



Cisco IOS XE 17 セグメントルーティング設定ガイド（アクセスルータおよびエッジルータ用）

最終更新：2024年10月22日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>



目次

第 1 章	最初にお読みください	1
	Short Description	2

第 2 章	MPLS データプレーンのセグメントルーティングの概要	3
	セグメントルーティングに関する機能情報	3
	MPLS データプレーンのセグメントルーティングの概要	4
	セグメントルーティングの仕組み	4
	セグメントルーティングの例	5
	セグメントルーティングの利点	7
	セグメントルーティング グローバルブロック	10
	隣接関係セグメント識別子	10
	プレフィックスセグメント識別子	10
	セグメントルーティングに関する追加情報	11

第 3 章	IS-IS v4 ノード SID によるセグメントルーティング	13
	IS-IS v4 ノード SID によるセグメントルーティングに関する機能情報	13
	IS-IS v4 ノード SID によるセグメントルーティングに関する制約事項	13
	IS-IS v4 ノード SID によるセグメントルーティングに関する情報	14
	セグメントルーティング IS-IS v4 ノード SID	14
	リモートルータからのラベルスイッチドパスで受信するプレフィックス SID	15
	セグメントルーティング隣接関係 SID アドバタイズメント	15
	隣接関係 (アジャセンシー) SID	16
	セグメントルーティング マッピング サーバー	16
	接続されたプレフィックス SID	16

SRGB 範囲の変更	16
SRGB の削除	17
インターフェイスでの MPLS 転送	17
セグメントルーティングと LDP の設定	17
セグメントルーティング トラフィック エンジニアリングの通知	17
IS-IS v4 ノード SID によるセグメントルーティングの設定方法	18
セグメントルーティングの設定	18
IS-IS ネットワークでのセグメントルーティングの設定	19
IS-IS のプレフィックス SID の設定	21
プレフィックス属性 N-Flag の設定	22
明示的 Null 属性の設定	23
セグメントルーティング Label Distribution Protocol 優先順位の設定	24
IS-IS SRMS の設定	25
IS-IS SRMS クライアントの設定	26
IS-IS SID バインド TLV ドメインフラッディングの設定	26
セグメントルーティングの設定例：IS-IS v4 ノード SID	26
例：IS-IS ネットワークでのセグメントルーティングの設定	26
例：明示的 Null 属性の設定	27
IS-IS v4 ノード SID によるセグメントルーティングに関する追加情報	27
第 4 章	
IS-IS リンク保護のトポロジに依存しないループフリー代替高速再ルーティング	29
IS-IS リンク保護のトポロジに依存しないループフリー代替高速再ルーティングの機能情報	29
IS-IS リンク保護のトポロジに依存しないループフリー代替高速再ルーティングの前提条件	30
IS-IS リンク保護のトポロジに依存しないループフリー代替高速再ルーティングについて	31
トポロジに依存しないループフリー代替	31
トポロジに依存しないループフリー代替タイプブレーク	32
インターフェイス高速再ルーティング タイプブレーカー	33
IS-IS リンク保護のトポロジに依存しないループフリー代替高速再ルーティングの設定方法	34
トポロジに依存しないループフリー代替高速再ルーティングの設定	34

マッピング サーバーを使用したトポロジに依存しないループ フリー代替の設定	35
例 : IS-IS リンク保護のトポロジに依存しないループ フリー代替高速再ルーティングの設定	38
タイブレーカーの確認	40
プライマリおよび修復パスの確認	40
IS-IS セグメント ルーティングの設定の確認	41
IS-IS トポロジに依存しないループ フリー代替トンネルの確認	42
トポロジに依存しないループ フリー代替構成によるセグメント ルーティング トラフィック エンジニアリングの確認	42

第 5 章

IS-IS のセグメント ルーティング トラフィック エンジニアリング 45

IS-IS によるセグメント ルーティング トラフィック エンジニアリングに関する機能情報	45
IS-IS によるセグメント ルーティング トラフィック エンジニアリングに関する制約事項	46
IS-IS によるセグメント ルーティング トラフィック エンジニアリングに関する情報	46
SR-TE LSP のインスタンス化	47
SR-TE LSP の明示的ヌル	47
SR-TE LSP のパス検証	47
SR-TE トラフィックのロード バランシング	50
SR-TE トンネルの再最適化	51
ロックダウンオプション付き SR-TE	52
SR-TE トンネル保護	52
アンナンバード サポート	53
IS-IS によるセグメント ルーティング トラフィック エンジニアリングの設定方法	54
TE トンネルのパスオプションの設定	54
SR 明示パス ホップの設定	54
インターフェイスのアフィニティの設定	55
使用例 : セグメント ルーティング トラフィック エンジニアリングの基本設定	55
明示パス SR-TE トンネル 1	57
明示パス SR-TE トンネル 2	57
明示パス SR-TE トンネル 3	58
動的パス SR-TE トンネル 4	58

動的パス SR-TE トンネル 5	58
SR-TE トンネルの構成の確認	59
トンネル 1 の確認	59
トンネル 2 の確認	59
トンネル 3 の確認	60
トンネル 4 の確認	61
トンネル 5 の確認	61
Verbatim パス サポートの確認	62

第 6 章

OSPFv2 ノード SID のセグメント ルーティング	63
OSPFv2 ノード SID のセグメント ルーティングに関する機能情報	63
OSPFv2 ノード SID のセグメント ルーティングに関する情報	64
リモートルータからのラベルスイッチドパスで受信されたプレフィックス SID	64
セグメントルーティング隣接関係 SID アドバタイズメント	65
複数の隣接関係 SID	65
セグメントルーティングマッピングサーバー	65
接続されたプレフィックス SID	66
SRGB 範囲の変更	66
インターフェイスでの MPLS 転送	66
SID エントリの競合処理	66
OSPFv2 ノード SID のセグメントルーティングの設定方法	67
OSPF のセグメントルーティングの設定	67
OSPF ネットワークでのセグメントルーティングの設定	69
OSPF のプレフィックス SID の設定	70
プレフィックス属性 N-flag-clear の設定	71
OSPF での明示的ヌル属性の設定	72
OSPF のセグメントルーティング Label Distribution Protocol 優先順位の設定	74
OSPF SRMS の設定	75
OSPF SRMS クライアントの設定	75
OSPFv2 ノード SID のセグメントルーティングに関する追加情報	76

OSPFv2 リンク保護のトポロジに依存しないループフリー代替高速再ルーティング 77

OSPFv2 リンク保護のトポロジに依存しないループフリー代替高速再ルーティングの機能情報 77

トポロジに依存しないループフリー代替高速再ルーティングの制約事項 78

OSPFv2 リンク保護のトポロジに依存しないループフリー代替高速再ルーティングについて 79

IP 高速再ルーティングおよびリモート ループフリー代替 79

トポロジに依存しない高速再ルーティング 80

トポロジに依存しないループフリー代替 80

トポロジに依存しないループフリー代替タイプブレイク 81

P スペース 82

Q スペース 82

コンバージェンス後のパス 82

宛先ごとのリンク保護 83

インターフェイスごとのループフリー代替の使用可能性 83

プレフィックス処理 83

エニーキャストプレフィックス処理 84

プレフィックスごとのループフリー代替タイプブレイク 84

ノード保護 86

共有リスク リンク グループ保護 86

ノード共有リスク リンク グループ保護 87

トポロジに依存しないループフリー代替高速再ルーティングの設定方法 88

トポロジに依存しないループフリー代替高速再ルーティングの有効化 88

トポロジに依存しないループフリー代替高速再ルーティングの設定 88

トポロジに依存しない高速再ルーティング タイブレーカーの設定 89

トポロジに依存しない高速再ルーティング トンネルの確認 91

トポロジに依存しないループフリー代替高速再ルーティングのデバッグ 92

例：OSPFv2 リンク保護のトポロジに依存しないループフリー代替高速再ルーティング 93

例：トポロジに依存しないループフリー代替高速再ルーティングの設定 93

OSPF のセグメント ルーティング トラフィック エンジニアリング	95
OSPF のセグメント ルーティング トラフィック エンジニアリングの機能情報	95
OSPF のセグメント ルーティング トラフィック エンジニアリングの制約事項	96
OSPF のセグメント ルーティング トラフィック エンジニアリングに関する情報	96
OSPF のセグメント ルーティング トラフィック エンジニアリングを使用する利点	97
OSPFv2 セグメント ルーティング トラフィック エンジニアリング機能	97
保護された隣接関係 SID	98
トラフィック エンジニアリング インターフェイス	98
アンナンバード サポート	98
隣接関係転送のためのセグメント ルーティング トラフィック エンジニアリング サポート	98
自動ルート アナウンスのためのセグメント ルーティング トラフィック エンジニアリング サポート	99
自動ルート アナウンス IP2MPLS	99
SR-TE LSP のインスタンス化	99
トンネルパス アフィニティの検証	100
SR-TE トラフィックのロード バランシング	100
ポート チャネル TE リンクのロード バランシング	100
単一トンネルでのロード バランシング	100
複数トンネルでのロード バランシング	100
SR-TE トンネルの再最適化	101
ロックダウンオプション付き SR-TE	102
SR-TE トンネル保護	102
IP-FRR ローカル修復保護	103
トンネルパス保護	103
SR TE LSP のパス検証	103
トポロジパスの検証	104
SR SID の検証	104
LSP 出力インターフェイス	105
IP 到達可能性の検証	105

トンネルパス リソース回避の検証	105
SR-TE LSP の明示的ヌル	106
Verbatim パス サポート	106
OSPF のセグメントルーティング トラフィック エンジニアリングの設定方法	106
OSPF のセグメントルーティング トラフィック エンジニアリングの有効化	106
TE トンネルのパスオプションの設定	107
SR 明示パス ホップの設定	107
トンネルパス アフィニティの検証の設定	108
インターフェイスのアフィニティの設定	108
OSPF のセグメントルーティング トラフィック エンジニアリングの設定	109
エリア内トンネルの設定	109
エリア間トンネルの設定	112
SR-TE トンネルの構成の確認	114
トンネル 1 の確認	114
トンネル 2 の確認	115
トンネル 3 の確認	115
トンネル 4 の確認	116
トンネル 5 の確認	117

 第 9 章

BGP ダイナミック セグメントルーティング トラフィック エンジニアリング	119
BGP ダイナミック セグメントルーティング トラフィック エンジニアリングの機能情報	119
セグメントルーティングの制約事項：トラフィック エンジニアリング ダイナミック BGP	120
セグメントルーティングに関する情報：トラフィック エンジニアリング ダイナミック BGP	120
TE ラベルスイッチドパス属性セット	121
TE ラベルスイッチドパス属性セットの設定方法	122
TE ラベルスイッチドパス属性セットの設定	122

 第 10 章

L3/L3VPN 用のセグメントルーティング オン デマンド ネクスト ホップ	125
L3/L3VPN のセグメントルーティング オン デマンド ネクスト ホップに関する機能情報	125

L3/L3VPN のセグメント ルーティング オンデマンド SR PFP ODN 自動ステアリング (PCE 委任) に関する制約事項	126
L3/L3VPN のセグメント ルーティング オンデマンド SR PFP ODN 自動ステアリング (PCE 委任) に関する情報	126
L3/L3VPN のセグメント ルーティング オンデマンド ネクスト ホップの設定方法	127
L3/L3VPN のセグメント ルーティング オンデマンド ネクスト ホップの設定	127
L3/L3VPN のセグメント ルーティング オンデマンド ネクスト ホップの確認	131

第 11 章

L2VPN/VPWS のセグメント ルーティング オンデマンド 137

L2VPN/VPWS のセグメント ルーティング オンデマンド ネクスト ホップに関する機能情報	137
L2VPN/VPWS のセグメント ルーティング オンデマンド ネクスト ホップの制約事項	138
L2VPN/VPWS のセグメント ルーティング オンデマンド ネクスト ホップに関する情報	138
AToM マネージャ	139
エリア間 L2VPN ODN	139
L2VPN/VPWS のセグメント ルーティング オンデマンド ネクスト ホップの設定方法	139
Pesudowire インターフェイス コマンドを使用した、L2VPN/VPWS のオンデマンドネクスト ホップでのセグメント ルーティングの設定	140
テンプレート コマンドを使用した L2VPN/VPWS のセグメント ルーティング オンデマンドネクスト ホップの設定	141
前に付加オプションを使用した L2VPN/VPWS のセグメント ルーティング オンデマンドネクスト ホップの設定	141
L2VPN/VPWS のセグメント ルーティング オンデマンド ネクスト ホップの優先パスの設定	142
L2VPN/VPWS のセグメント ルーティング オンデマンド ネクスト ホップの自動ルート宛先の設定	142
L2VPN/VPWS のセグメント ルーティング オンデマンド ネクスト ホップの確認	143

第 12 章

高速コンバージェンスのデフォルト最適化 147

高速コンバージェンスのデフォルト最適化の機能情報	147
高速コンバージェンスのデフォルト最適化に関する情報	148
IS-IS のデフォルト最適化値	148
OSPF のデフォルト最適化値	149

第 13 章	ルーティング情報ベースのサポート	153
	ルーティング情報ベースのサポートの機能情報	153
	ルート再配布のためのルーティング情報ベースのサポート	154
	OSPF ノード SID 再配布のサポート	154
	OSPF ノード SID 再配布のサポートに関する情報	155
	NSSA ASBR	155
	非 NSSA ASBR	155
	プレフィックスの再配布	155
	OSPF ノード SID 再配布の確認	156
	オンデマンドネクストホップのためのルーティング情報ベースのサポート	157
第 14 章	SR-TE オンデマンド LSP	159
	SR-TE オンデマンド LSP の機能情報	159
	SR-TE オンデマンド LSP の制約事項	160
	SR-TE オンデマンド LSP に関する情報	160
	SR-TE : スタティックルートとして LSP をセットアップする	160
	アンナンバードインターフェイス上のスタティック SRTE	161
	SR-TE オンデマンド LSP の設定方法	161
	スタティックルートとしての LSP の設定	162
	セグメントルーティング自動トンネルスタティックルートの有効化	162
	セグメントルーティング自動トンネルスタティックルートの確認	162
	スタティックルーティング向けネイティブ UCMP の設定	165
	ローカル UCMP	165
	ネイティブ UCMP	165
	設定例	165
第 15 章	セグメントルーティング MPLS OAM のサポート	167
	セグメントルーティング OAM サポートの機能情報	167
	セグメントルーティング OAM MPLS サポートの制約事項	168
	セグメントルーティング MPLS OAM サポートに関する情報	168

セグメントルーティング OAM サポート	168
セグメントルーティング OAM サポートの利点	169
セグメントルーティング MPLS Ping	169
セグメントルーティング MPLS Traceroute	170
Nil FEC ターゲットに対する LSP Ping 操作	170
LSP Ping およびトレース ルート Nil FEC ターゲットを使用してセグメントルーティングを 診断する方法	170
Nil FEC ターゲットに対する LSP Ping の使用	170
Nil FEC ターゲットに対する LSP Traceroute の使用	171
LSP Ping Nil FEC ターゲットのサポートの例	171
セグメントルーティング ネットワークのパス検証	173
IGP プレフィックス SID FEC タイプ用の MPLS Ping および Traceroute	173
IGP 隣接セグメント ID 用の MPLS Ping および Traceroute	175
MPLS Ping および Traceroute 用のセグメントルーティング MPLS トラフィック エンジニア リングの設定	175
MPLS Ping および Traceroute 用のセグメントルーティング MPLS IGP の設定	176
<hr/>	
第 16 章	セグメントルーティングでのシームレス BFD の使用 177
セグメントルーティングでのシームレス BFD に関する機能情報	177
セグメントルーティングでのシームレス BFD 使用の制約事項	178
セグメントルーティングでのシームレス BFD に関する情報	178
双方向フォワーディング検出とシームレス双方向フォワーディング検出 (S-BFD)	178
イニシエータとリフレクタ	179
セグメントルーティングでのシームレス BFD の設定方法	180
セグメントルーティングのシームレス双方向フォワーディング検出 (S-BFD) の設定	180
リフレクタ ノードでのシームレス双方向フォワーディング検出 (S-BFD) の有効化	180
イニシエータ ノードでのシームレス双方向フォワーディング検出 (S-BFD) の有効化	180
シームレス双方向フォワーディング (S-BFD) でのセグメントルーティングトラフィッ ク エンジニアリング トンネルの有効化	180
S-BFD 設定の確認	181
セグメントルーティングでのシームレス BFD に関する追加情報	182

第 17 章

セグメント ルーティングでの SSPF の使用 183

セグメント ルーティングでの SSPF に関する機能情報 183

セグメント ルーティングでの SSPF に関する情報 184

厳格な最短パス優先 184

厳格な最短パス優先を設定するためのアプローチ 184

セグメント ルーティングでの SSPF の設定方法 185

厳格な最短パス優先 (SPF) の設定 185

connect-prefix-sid-map コマンドを使用した厳格な最短パス優先の有効化 185

セグメント ルーティング マッピング サーバーを使用した厳格な最短パス優先の有効化
185

セグメント ルーティングでの SSPF の追加情報 187

第 18 章

ダイナミック PCC 189

ダイナミック PCC に関する情報 189

パス計算要素プロトコル関数 189

冗長パス計算要素 190

ダイナミック PCC の設定方法 190

ダイナミック PCC のグローバルな設定 190

インターフェイスでのダイナミック PCC の設定 190

Verbatim パス オプションを使用したダイナミック PCC の設定 191

ダイナミック PCC の確認 191

ダイナミック PCC を使用した Verbatim パス オプションの確認 194

ダイナミック PCC の機能情報 195

第 19 章

SR : PCE 開始の LSP 197

SR の前提条件 : PCE 開始の LSP 197

SR の制約事項 : PCE 開始の LSP 197

SR に関する情報 : PCE 開始の LSP 197

パス計算要素プロトコルの概要 197

SR : PCE 開始の LSP 198

単一および冗長 PCE 操作	198
SR の設定方法 : PCE 開始の LSP	199
PCC との PCEP セッションの確立	199
ネットワークでの LSP のアドバタイジング	199
PCC に対する PCE の優先順位の指定	199
LSP 構成の確認	200
SR の追加情報 : PCE 開始の LSP	205
SR の機能情報 : PCE 開始の LSP	205

第 20 章

ISIS - SR : uLoop 回避 207

ISIS - SR の前提条件 : uLoop 回避	207
ISIS - SR の制約事項 : uLoop 回避	207
ISIS - SR に関する情報 : uLoop 回避	208
マイクロループ	208
セグメントルーティングとマイクロループ	211
セグメントルーティングがマイクロループを防ぐ仕組み	211
ISIS - SR を有効にする方法 : uLoop 回避	212
マイクロループ回避の有効化	212
マイクロループ回避の確認	212
ISIS - SR の追加情報 : uLoop 回避	213
ISIS - SR の機能情報 : uLoop 回避	214

第 21 章

BGP-SR : BGP プレフィックス SID の再配布 215

BGP - SR の前提条件 : BGP プレフィックス SID の再配布	215
BGP - SR に関する情報 : BGP プレフィックス SID の再配布	215
セグメントルーティングと BGP	215
ローカルソースルートのセグメントルーティング	216
受信したプレフィックスのセグメントルーティング	216
再配布ルートのセグメントルーティング	216
BGP--MFI インタラクション	217
BGP - SR を有効にする方法 : BGP プレフィックス SID の再配布	217

BGP-Prefix-SID の有効化	217
セグメントルーティング用の BGP の有効化	217
BGP - SR の確認 : BGP プレフィックス SID の再配布	217
BGP - SR の追加情報 : BGP プレフィックス SID の再配布	218
BGP - SR の機能情報 : BGP プレフィックス SID の再配布	218

第 22 章

IS-IS および OSPF によって最大 SID 深度を BGP-LS にアダプタイズする	221
IS-IS および OSPF による最大 SID 深度の BGP-LS へのアダプタイズに関する制約事項	221
IS-IS および OSPF による最大 SID 深度の BGP-LS へのアダプタイズに関する情報	222
最大 SID 深度	222
ノードの最大 SID 深度のアダプタイズメント	222
ハードウェアからのノード MSD の取得	223
BGP LS への MSD のアダプタイジング	223
IS-IS および OSPF による最大 SID 深度の BGP-LS へのアダプタイズの確認	224
IS-IS および OSPF による最大 SID 深度の BGP-LS へのアダプタイズに関する機能情報	224

第 23 章

セグメントルーティングトラフィックエンジニアリング AutoTunnel を使用した RSVP-TE の保護	227
セグメントルーティングトラフィックエンジニアリング AutoTunnel を使用した RSVP-TE の保護に関する機能情報	227
セグメントルーティングトラフィックエンジニアリング AutoTunnel を使用した RSVP-TE の保護に関する前提条件	228
セグメントルーティングトラフィックエンジニアリング AutoTunnel を使用した RSVP-TE の保護に関する制約事項	229
セグメントルーティングトラフィックエンジニアリング AutoTunnel を使用した RSVP-TE の保護に関する情報	229
セグメントルーティングトラフィックエンジニアリング AutoTunnel を使用した RSVP-TE の保護の利点	229
バックアップ AutoTunnel	229
セグメントルーティングトラフィックエンジニアリング AutoTunnel を使用した RSVP-TE の保護の設定方法	232
ポイントツーポイント ネットワーク タイプの明示パスの設定	232

FRR での明示的 RSVP-TE トンネルの設定 233

セグメントルーティングトラフィックエンジニアリング AutoTunnel を使用した RSVP-TE
の保護の確認 234

第 24 章

ISIS 手動隣接関係 SID 237

ISIS 手動隣接関係 SID の機能情報 237

ISIS 手動隣接関係 SID に関する情報 238

手動隣接関係 SID 238

隣接関係 SID のアドバタイズメント 239

隣接関係 SID のフォワーディング 239

設定要件 239

手動隣接関係 SID の設定 240

手動隣接関係 SID の確認 240

第 25 章

OSPF 手動隣接関係 (アジャセンシー) SID 243

OSPF 手動隣接関係 (アジャセンシー) SID に関する機能情報 243

OSPF 手動隣接関係 (アジャセンシー) SID に関する情報 244

OSPF 手動隣接関係 (アジャセンシー) SID の前提条件 244

OSPF 手動隣接関係 (アジャセンシー) SID に関する制約事項 244

手動隣接関係 (アジャセンシー) SID 245

手動隣接関係 (アジャセンシー) SID のアドバタイズメント 245

手動隣接関係 (アジャセンシー) SID の転送 245

OSPF 手動隣接関係 (アジャセンシー) SID の設定方法 246

セグメントルーティング ローカルブロック範囲の変更 246

OSPF 手動隣接関係 (アジャセンシー) SID の設定 246

OSPF 手動隣接関係 (アジャセンシー) SID の確認 246

第 26 章

OSPFv2 セグメントルーティングの厳格な SPF 249

OSPFv2 セグメントルーティングの厳格な SPF に関する機能情報 249

OSPFv2 セグメントルーティングの厳格な SPF の制約事項 250

OSPFv2 セグメントルーティングの厳格な SPF に関する情報 250

厳格な SPF を使用する理由	251
厳格な SPF 機能のアドバタイズメント	251
拡張プレフィックス LSA での厳格な SPF SID アドバタイズメント	251
SR-TE およびルータ情報ベースとのインタラクション	252
OSPFv2 セグメント ルーティングの厳格な SPF の有効化および無効化	252
OSPFv2 セグメント ルーティングの厳格な SPF SID の設定	253
OSPFv2 セグメント ルーティングの厳格な SPF の確認	253

第 27 章

セグメント ルーティング OSPFv2 マイクロループ回避	261
セグメント ルーティング OSPFv2 マイクロループ回避に関する機能情報	261
セグメント ルーティング OSPFv2 マイクロループ回避に関する情報	262
マイクロループ	262
セグメント ルーティングを使用したマイクロループの防止	265
セグメント ルーティング OSPFv2 マイクロループ回避の前提条件	266
セグメント ルーティング OSPFv2 マイクロループ回避の制約事項	266
セグメント ルーティング OSPFv2 マイクロループ回避の設定	267
セグメント ルーティング OSPFv2 マイクロループ回避の確認	267

第 28 章

トラフィック エンジニアリングのパフォーマンス測定	269
トラフィック エンジニアリングのパフォーマンス測定に関する機能情報	269
トラフィック エンジニアリングのパフォーマンスメトリックに関する情報	270
リンク遅延測定の概要	270
計算間隔のリンク遅延メトリック	271
アドバタイズメントのリンク遅延メトリック	272
グローバルリンク遅延プロファイル	273
リンク遅延測定の利点	275
リンク遅延測定に関する制約事項	275
トラフィック エンジニアリングのパフォーマンス測定の設定方法	275
グローバルリンク遅延プロファイルの設定	275
インターフェイスのリンク遅延測定の設定	276
モニタリングモードの有効化	277

リンク遅延設定の確認	277
インターフェイスのリンク遅延情報の表示	278
その他のコマンド	279
その他の参考資料	281

第 29 章

パフォーマンス測定の設定 283

リンク遅延測定	284
リンク遅延に関する PM の制約事項および使用上のガイドライン	285
PM リンク遅延：さまざまなパラメータのデフォルト値	285
設定例：リンク遅延の PM	286
検証：PM リンク遅延設定	287
エンドツーエンド遅延測定	289
設定例：エンドツーエンドの遅延管理用の PM	290
検証：PM エンドツーエンド遅延管理設定	292
一方向リンク損失測定	293
一方向リンク損失測定に関する情報	293
一方向リンク損失測定に関する制約事項	294
一方向リンク損失測定でサポートされるプラットフォーム	294
GRE-IPSec トンネルのデュアルカラー損失測定	294
リンク損失測定に関する IGP IS-IS アドバタイズメント	296
設定例：一方向リンク損失測定	296
設定例：SR-MPLS ポリシーの設定	297
検証：一方向リンク損失測定	298
一方向リンク損失測定のデバッグとトラブルシューティング	302
show コマンドの例	303

第 30 章

IP エンドポイントの遅延測定および活性モニタリング 309

IP エンドポイントのパフォーマンス遅延測定および活性モニタリングに関する情報	309
IP エンドポイントのパフォーマンス遅延測定および活性モニタリングの利点	309
IP エンドポイントのパフォーマンス遅延測定および活性モニタリングの制約事項	310

IP エンドポイントのパフォーマンス遅延測定および活性モニタリングでサポートされるプラットフォーム	310
IP エンドポイントのパフォーマンス遅延測定のユースケース	311
ユースケース 1: グローバルルーティング テーブルで到達可能な IP エンドポイントへの遅延測定プローブ	311
ユースケース 2: ユーザー指定の VRF で到達可能な IP エンドポイントへの遅延測定プローブ	312
IP エンドポイントのパフォーマンス遅延測定の設定方法	312
使用上のガイドラインと制限事項	312
パフォーマンス遅延測定を行う IP エンドポイントの設定	313
IP エンドポイントのパフォーマンス遅延測定プロファイルの設定	315
IP エンドポイントのパフォーマンス遅延測定の設定例	318
設定例: IP エンドポイントのパフォーマンス遅延測定の設定 (グローバル コンフィギュレーション)	319
設定例: IP エンドポイントのパフォーマンス遅延測定の設定 (VRF 設定)	320
IP エンドポイントのパフォーマンス遅延測定の検証	320
例	321
show performance-measurement summary	321
show performance-measurement profile	321
show performance-measurement endpoint session	322
show performance-measurement counters endpoint	323
show performance-measurement history endpoint	323
IP エンドポイントの遅延測定および活性モニタリングの機能情報	324
第 31 章	
SR-TE フロー別 (クラス) ODN と自動化されたステアリング (PCE 委任)	327
SR-TE フロー別 (クラス) ODN と自動化されたステアリング (PCE 委任) に関する機能情報	328
SR-TE フロー別 (クラス) ODN と自動化されたステアリング (PCE 委任) に関する情報	330
SR-TE フロー別 (クラス) ODN と自動化されたステアリング (PCE 委任) に関する制約事項	330
BGP カラー拡張コミュニティと VRF プレフィックスのカラーリング	331
サポートされるプラットフォーム	332

カラー拡張コミュニティのアタッチ	332
RIB パスによる PFP のサポート	334
例：RIB パスによる PFP の設定	334
SR-TE フロー別クラス (ODN) と自動化されたステアリング (PCE 委任) の設定	335
SR-TE フロー別クラス (ODN) と自動化されたステアリング (PCE 委任) の確認	337

第 32 章

複数の ISIS ドメインでの境界ルータのループバックプレフィックス SID のアダプタイズメント 339

複数の ISIS ドメインでの境界ルータのループバックプレフィックス SID のアダプタイズメントに関する機能情報	339
複数の ISIS ドメインでの境界ルータのループバックプレフィックス SID のアダプタイズメントに関する情報	340
複数の ISIS ドメインでの境界ルータのループバックプレフィックス SID のアダプタイズメントの概要	340
複数の ISIS ドメインでの境界ルータのループバックプレフィックス SID のアダプタイズメントの設定方法	341
複数の ISIS ドメインでの境界ルータのループバックプレフィックス SID のアダプタイズメントの設定	341
複数の ISIS ドメインでの境界ルータのループバックプレフィックス SID のアダプタイズメントの確認	341
例：複数の ISIS ドメインでの BR のループバックプレフィックス SID の設定	342

第 33 章

無効なパスのドロップによるトラフィックステアリング 345

無効なパスのドロップによるトラフィックステアリングに関する機能情報	345
概要	346
はじめる前に	346
利点	346
機能制限	347
無効なパスのドロップによるトラフィックステアリングの設定方法	347
PCC プロファイルの設定	347
静的ポリシーの設定	347
SR-TE ポリシーのオンデマンドネクストホップの設定	347

コマンドの表示 347

第 34 章

Cisco IS-IS ローカル不等コストマルチパス (UCMP) の設定 349

不等コストマルチパス (UCMP) ローカルの設定 350

不等コストマルチパス (UCMP) ローカルの確認 350

例 : show コマンド 350

debug コマンド 351

セグメントルーティングに関する機能情報 : IS-IS UCMP 351

第 35 章

セグメント ルーティング フレキシブル アルゴリズムの有効化 353

機能の履歴 354

フレキシブルアルゴリズムの前提条件 355

フレキシブルアルゴリズムに関する制約事項 356

セグメント ルーティング フレキシブル アルゴリズムの構成要素 356

フレキシブルアルゴリズムの定義 356

フレキシブルアルゴリズムのサポートのアドバタイズメント 356

フレキシブルアルゴリズムの定義のアドバタイズメント 356

フレキシブルアルゴリズムのプレフィックス SID のアドバタイズメント 357

フレキシブルアルゴリズム パスの計算 357

フレキシブルアルゴリズム パスの転送エントリの組み込み 358

フレキシブルアルゴリズムのプレフィックス SID の再配布 358

アルゴリズム情報の表示 359

フレキシブルアルゴリズムのプレフィックス メトリック アドバタイズメント 359

フレキシブルアルゴリズムの設定 360

IS-IS フレキシブルアルゴリズムの設定 363

IS-IS の再配布 365

SRTE-ODN の関連付けの設定 365

フレキシブルアルゴリズム用のインターフェイスの設定 365

BGP の設定 366

選択的なパスのフィルタ処理の設定 366

PCE 委任による SR ポリシーの設定 366

フレキシブルアルゴリズムの設定の確認 367

第 36 章

SR-TE 優先パス上の L2VPN 373

機能制限 374

フレキシブルアルゴリズムでの SR-TE 優先パスを使用した L2VPN トラフィックステアリングの設定 374

設定例 1 : SR-TE 優先パス上の VPWS 疑似回線 376

設定例 2 : SR-TE 優先パス上の VPWS 疑似回線 376

設定例 3 : SR-TE 優先パス上の VPLS 疑似回線 377

SR-TE 優先パス上の L2VPN の設定確認 377

第 37 章

IGP 自動ルート通知により COE-PCE が開始する SR ポリシー 381

COE-PCE が開始する SR ポリシー 382

PCE が開始する SR ポリシーに関する制約事項 382

SR-TE を介した ECMP 383

SR-TE ポリシーを介した ECMP に関する制約事項 383

ローカル輻輳の緩和 384

ロード バランシング 386

自動ルート通知 386

スタティック ルートの設定 387

SR ポリシー内のネクストホップ ECMP 387

IGP 自動ルート通知により の の設定 387

自動ルート通知による SR ポリシーの確認 387

IGP の ISIS 自動ルートの確認 388

SR ポリシーのトンネル ID の確認 388

第 38 章

Cisco ACI から SR-MPLS ハンドオフにおける DC-PE ルータ 391

前提条件 391

機能制限 391

ACI から SR-MPLS ハンドオフにおける DC-PE ルータに関する情報 392

サポートされるプラットフォーム 393

DC-PE ルータの設定方法	393
DC-PE ルータでの VRF の設定	393
DC-PE ルータでの BGP の設定	395
DC-PE ルータ設定の確認	401
ACI からの IPv4 および IPv6 ルートの確認	401
WAN からの IPv4 および IPv6 ルートの確認	402
トラブルシューティングとデバッグ	404
Cisco ACI から SR-MPLS ハンドオフにおける DC-PE ルータの機能情報	405

第 39 章

IPv6 を介したセグメントルーティング	407
IPv6 を介したセグメントルーティング	408
機能情報	408
SRv6 に関する制約事項	409
SRv6 に関する情報	409
SRv6 マイクロセグメント (uSID)	410
SRv6 の導入	411
サポートされるプラットフォーム	412
SRv6 の設定	413
SRv6 の設定	413
SPv6 の設定の確認	414
IS-IS での SRv6	417
IS-IS での SRv6	417
IS-IS での SRv6 に関する情報	417
IS-IS での SRv6 の設定	417
SRv6 IS-IS の設定の確認	418
SRv6 BGP ベースのサービス	419
SRv6 BGP ベースのサービス	419
SRv6 BGP ベースのサービスに関する制約事項	419
SRv6 BGP ベースのサービスに関する情報	420
SRv6 ベースの L3VPN	421
SRv6 ベースの L3VPN の設定	421

BGP MPLS と SRv6 の共存	423
L3VPN の MPLS と SRv6 の共存設定	423
SRv6 の状態の確認	423
SRv6 BGP のトラブルシューティングとデバッグ	429
BGP SRv6 L3VPN オンデマンドネクストホップ	429
BGP SRv6L3VPN オンデマンドネクストホップ	429
BGP SRv6 L3VPN ODN の前提条件	430
BGP SRv6L3VPN ODN に関する情報	430
SRv6 L3VPN ODN の設定	431
SRv6 ODN カラーテンプレートの設定	432
SRv6 L3VPN ODN 設定の確認	435
SRv6 L3VPN ODN 設定のデバッグ	439
SRv6 トラフィック エンジニアリング ポリシー	441
SRv6 トラフィック エンジニアリング ポリシー	441
SRv6-TE ポリシーに関する制約事項	441
SRv6-TE ポリシーに関する情報	441
SRv6-TE の設定	441
SRv6-TE の設定の確認	443
SRv6-TE のトラブルシューティングとデバッグ	446
SRv6 のパフォーマンス測定	447
SRv6 のパフォーマンス測定	447
SRv6 のパフォーマンス測定の活性	447
SRv6 の PM 活性の設定	447
SRv6 のパフォーマンス測定の確認	448
SRv6 OAM	453
SRv6 の運用、管理、およびメンテナンス	453
SRv6 に関する制約事項	453
SRv6 OAM に関する情報	454
SRv6 OAM の操作	454



第 1 章

最初にお読みください

重要事項



- (注) Cisco IOS XE Bengaluru 17.6.1a 以降のリリースでの CUBE 機能のサポート情報については、[Cisco Unified Border Element IOS-XE コンフィギュレーションガイド](#)を参照してください。



- (注) この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFPのドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

機能情報

機能のサポート、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.com のアカウントは必要ありません。

参考資料

- [Cisco IOS コマンドリファレンス、全リリース](#)

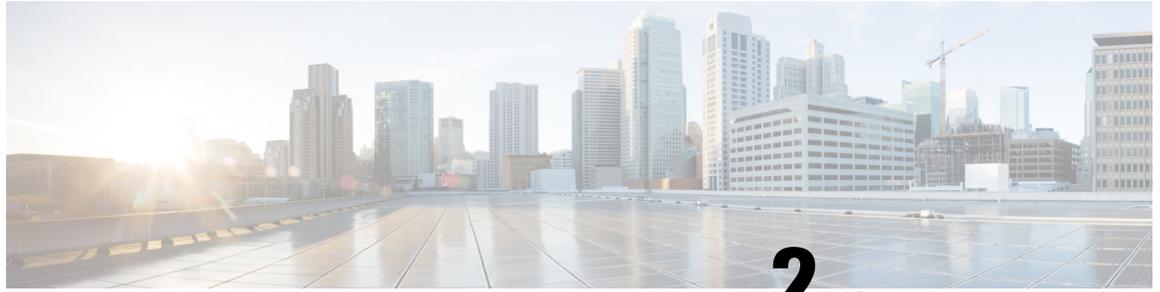
マニュアルの入手方法およびテクニカル サポート

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、[Cisco Services \[英語\]](#) にアクセスしてください。

- サービス リクエストを送信するには、[Cisco Support](#) [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco Marketplace](#) にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。
- [Short Description](#) (2 ページ)

Short Description

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)



第 2 章

MPLS データプレーンのセグメントルーティングの概要

この章では、セグメントルーティング（SR）の概念を次のセクションに分けて紹介します。

- [セグメントルーティングに関する機能情報（3 ページ）](#)
- [MPLS データプレーンのセグメントルーティングの概要（4 ページ）](#)
- [セグメントルーティングの仕組み（4 ページ）](#)
- [セグメントルーティングの例（5 ページ）](#)
- [セグメントルーティングの利点（7 ページ）](#)
- [セグメントルーティング グローバルブロック（10 ページ）](#)
- [セグメントルーティングに関する追加情報（11 ページ）](#)

セグメントルーティングに関する機能情報

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、<https://cfnnng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

表 1: セグメントルーティングに関する機能情報

機能名	リリース	機能情報
セグメントルーティングの概要	Cisco IOS XE Amsterdam 17.3.2	セグメントルーティング（SR）は、送信元ルーティングを実行するための柔軟でスケーラブルな方法です。

MPLS データプレーンのセグメントルーティングの概要

セグメントルーティング (SR) は、送信元ルーティングを実行するための柔軟でスケーラブルな方法です。送信元がパスを選択し、セグメントの番号付きリストとしてパケットヘッダー内で暗号化します。セグメントは、任意のタイプの命令の識別子です。各セグメントは、セグメント ID (SID) によって識別されます。次のようなセグメント命令があります。

- 最短パスを使用してノード N へ移動する。
- ノード M への最短パスを経由してノード N に移動し、次に特定のリンクセットをたどる。
- サービス S を適用する。

セグメントルーティングを使用すると、ネットワークでアプリケーションごとやフロー状態ごとに管理する必要がなくなります。代わりに、パケット内に指定されている転送命令に従います。

セグメントルーティングは、Intermediate System-to-Intermediate System (IS-IS) および Open Shortest Path First (OSPF) プロトコルの拡張機能に依存しています。MPLS (マルチプロトコルラベルスイッチング) データプレーンを使用して運用する場合、レイヤ 3 VPN (L3VPN)、仮想プライベートワイヤサービス (VPWS)、仮想プライベート LAN サービス (VPLS)、イーサネット VPN (EVPN) などの、さまざまなマルチサービス機能と統合されます。



(注) Cisco IOS XE Amsterdam 17.3.2 リリースは、IPv4 アドレスファミリの MPLS データプレーンのみをサポートします。

セグメントルーティングは、転送プレーンを変更することなく、マルチプロトコルラベルスイッチング (MPLS) アーキテクチャに直接適用できます。セグメントルーティングは従来の MPLS ネットワークよりも効率的にネットワーク帯域幅を利用し、遅延を低減します。セグメントは MPLS ラベルとしてエンコードされます。セグメントの番号付きリストはラベルのスタックとしてエンコードされます。処理するセグメントは、スタックの一番上にあります。セグメントの完了後に関連するラベルがスタックからポップします。

セグメントルーティングは自動トラフィック保護を提供しますが、トポロジ上の制約事項はありません。ネットワークがリンク障害やノード障害からトラフィックを保護し、ネットワーク内での追加シグナリングは必要ありません。既存の IP 高速再ルート (FRR) 技術と、セグメントルーティングの明示的なルーティング機能を組み合わせると、最適なバックアップパスを備えた完全な保護適用範囲が保証されます。トラフィック保護には、他のシグナリング要件は適用されません。

セグメントルーティングの仕組み

セグメントルーティング ネットワーク内のルータは、明示的な最短パスか、または内部ゲートウェイプロトコル (IGP) の計算された最短パスかどうかにかかわらず、トラフィックを転

送する任意のパスを選択できます。セグメントは、ネットワークの宛先への完全なパスを形成するためにルータを組み合わせることができるサブパスを表しています。各セグメントには識別子（セグメント識別子）があり、IGP 拡張機能を使用してネットワーク全体にアドバタイズされます。従来の MPLS ネットワークとは異なり、セグメントルータ ネットワーク内のルータに転送をサポートするための Label Distribution Protocol (LDP) や Resource Reservation Protocol - Traffic Engineering (RSVP-TE) は必要ありません。

各ルータ（ノード）と各リンク（隣接関係）には関連付けられたセグメント識別子（SID）があります。ノードセグメント識別子はグローバルに一意です。ネットワーク管理者は各ルータに予約済みブロックからノード ID を割り当てます。一方、隣接関係セグメント ID はアドバタイズノードにとってローカルで重要なものであり、出力インターフェイスなどの隣接ルータに固有の隣接関係を表します。ルータは、ノード ID に使用される予約済みブロック外の隣接関係識別子を自動的に生成します。MPLS ネットワークでは、セグメント識別子は MPLS ラベルスタック エントリとしてエンコードされます。セグメント ID は指定したパスに沿ってデータパケットを移動します。次の 2 種類のセグメント ID があります。

- **プレフィックス SID :**

ネットワーク内のノードに関連付けられた IP アドレスプレフィックスに関連付けられたセグメント ID。プレフィックス SID はグローバルに一意です。ノードセグメントは、ノードのループバックアドレスにバインドされる特別なプレフィックスセグメントです。これは、インデックスとしてノード固有の SR グローバルブロック (SRGB) にアドバタイズされます。

- **隣接 SID :**

2つのルータ間のリンクに関連付けられているセグメント ID。隣接関係 SID の範囲は特定のルータに限定されます。

ノードセグメントはマルチホップパスになり得ますが、隣接関係（アジャセンシー）セグメントは常にワンホップパスです。

セグメントルーティングの例

次の図は、セグメントルーティング、IS-IS、ノード ID 用に 16000 ~ 23999 のラベル範囲、および 200 以上の隣接 ID を使用する、5 台のルータを含む MPLS ネットワークについて示しています。IS-IS は、ネットワーク全体にセグメント ID (MPLS ラベル) とともに IP プレフィックスの到達可能性を配布します。

図 1: セグメントルーティングを使用する 5 台のルータを含む MPLS ネットワーク

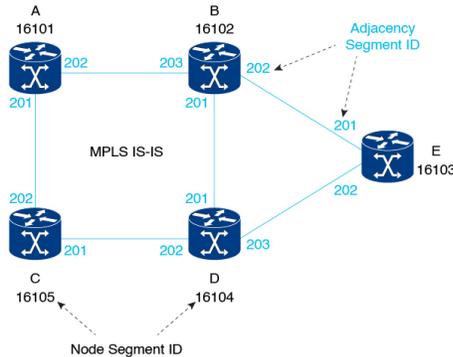
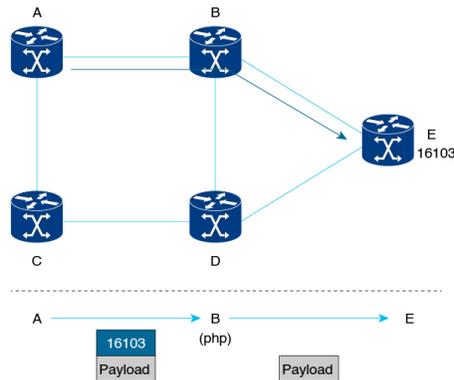


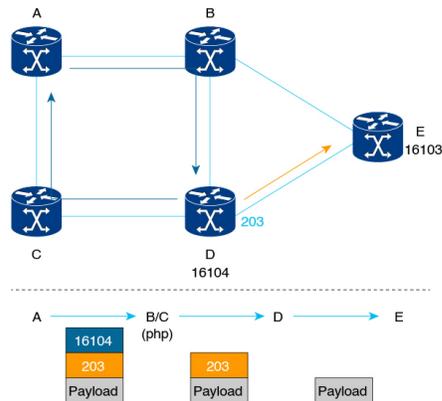
図 1 では、ルータ E にトラフィックを送信しているルータは、ラベル 16103（ルータ E ノードセグメント識別子）をプッシュし、IS-IS 最短パスを使用してトラフィックを転送します。各ホップでの MPLS ラベルスワッピング操作は、パケットが E に到着するまでラベル 16103 を保持します（図 2）。一方、隣接関係セグメントの動作は異なります。たとえば、パケットが 203（D 対 E の隣接関係セグメント識別子）のスタックトップの MPLS ラベルを持つルータ D に到着する場合、ルータ D はラベルをポップし、ルータ E にトラフィックを転送します。

図 2: MPLS ラベルスワッピング操作



セグメント識別子は、トラフィックエンジニアリングを実行するための順序付きリストとして組み合わせることができます。セグメントリストには、転送要件に応じて複数の隣接関係セグメント、複数のノードセグメント、または両方の組み合わせを含めることができます。前の例では、ルータ A は、ラベルスタック（16104、203）を代わりにプッシュし、最短パスとルータ D に該当するすべての ECMP を使用し、次に宛先への明示的なインターフェイスを通して、ルータ E に到達することができます（図 3）。ルータ A は新しいパスをシグナリングする必要がなく、状態情報はネットワーク内で一定に保たれます。ルータ A は、最終的に特定のパス経由でルータ E 宛てのどのフローを切り替えるかを決定する転送ポリシーを適用します。

図 3: ルータ E の宛先パス



セグメントルーティングの利点

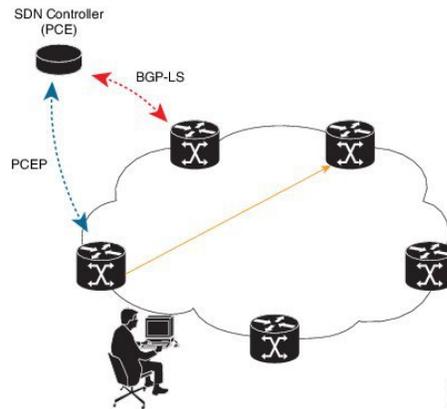
- SDNの準備**：セグメントルーティングは、ソフトウェア定義型ネットワーク（SDN）の採用を構想した魅力的なアーキテクチャであり、アプリケーション対応ルーティング（AER）の基盤です。これは、自動リンクおよびノード保護などのネットワークベースの分散インテリジェンスと、トラフィック最適化などのコントローラベースの集中型インテリジェンスとの間のバランスをとります。

厳格なネットワークパフォーマンス保証、ネットワークリソースの効率的な使用、およびアプリケーションベースのトランザクションに対する非常に高いスケーラビリティを提供することができます。ネットワークは、これらの要件を満たすために最小限の状態情報を使用します。セグメントルーティングは、コントローラベースのSDNアーキテクチャと簡単に統合できます。

次の図は、コントローラが帯域幅アドミSSIONコントロールなどの集中最適化を実行するSDNシナリオの例を示しています。このシナリオでは、コントローラがネットワークトポロジとフローの全体像をもっています。ルータは、遅延、帯域幅、ダイバーシティなど、特定の特性を持つ宛先へのパスを要求できます。コントローラは最適なパスを計算し、MPLSラベルスタックなどの対応するセグメントリストを要求元ルータに返します。その時点で、ルータはネットワークに追加のシグナリングなしでセグメントリストとともにトラフィックを注入できます。

さらに、セグメントリストを使用すると、ネットワークにアプリケーションの状態を追加することなく、完全なネットワーク仮想化を実現できます。状態は、セグメントのリストとしてパケットにエンコードされます。ネットワークはセグメント状態を維持するだけなので、ネットワークに負荷をかけることなく、大量で高頻度のトランザクションベースのアプリケーション要求をサポートできます。

図 4: SDN コントローラ



• 運用のシンプル化 :

- MPLS データプレーンに適用された場合、セグメントルーティングは、IGP (ISIS または OSPF) 以外のプロトコルを使用せずに、入力プロバイダーエッジから出力プロバイダーエッジへの MPLS サービス (VPN、VPLS、および VPWS) をトンネリングする機能を提供します。
- ラベル配布用に別のプロトコルを使用しない単純な動作です (たとえば LDP や RSVP が不要)。
- トラブルシューティングを行うための複雑な LDP または IGP 同期はありません。
- ECMP に対応した最短パス転送 (ノードセグメント ID を使用) により、設置済みインフラストラクチャの使用率を向上し、設備投資 (CapEx) を削減します。

- **高速再ルーティング (FRR) のサポート** : 任意のトポロジに対して自動化 FRR を提供します。ネットワーク内でリンクまたはノード障害が発生した場合、MPLS は FRR メカニズムを使用してコンバージェンスを行います。セグメントルーティングでは、コンバージェンス時間は 50 ミリ秒以下です。

• 大規模データセンター :

- セグメントルーティングでは、ボーダー ゲートウェイ プロトコル (BGP) RFC 3107 (トップオブブラック/リーフ/スパインスイッチ間の IPv4 ラベル付きユニキャスト) を使用して、MPLS 対応のデータセンター設計を簡素化します。
- BGP は、IGP ノード SID と同等のノードセグメント ID を配布します。
- トポロジ内のノードは、同じスイッチに同じ BGP セグメントを割り当てます。
- IGP ノード SID : ECMP および自動 FRR (BGP PIC (プレフィックス独立コンバージェンス)) の場合と同じ利点を提供されます。
- これは、トラフィック エンジニアリング (SR TE データセンター ファブリックの最適化) のためのビルディングブロックです。

• デュアルプレーン ネットワーク :

- セグメントルーティングは、プレーンが分割されていない限り、特定のプレーンからエッジの宛先へのルートがプレーン内に留まるデュアルプレーン ネットワークでのディスジョイントネスを強制するための簡単なソリューションを提供します。
- 追加の SID エニーキャストセグメント ID により、「ノード Z に向けてノード A に投入されたフロー 1 は、プレーン 1 を経由しなければならない」、「ノード Z に向けてノード A に投入されたフロー 2 は、プレーン 2 を経由しなければならない」といったマクロポリシーの表現が可能になります。

• 集中型トラフィック エンジニアリング :

- コントローラとオーケストレーション プラットフォームは、WAN 最適化などの集中型の最適化のために、セグメントルーティング トラフィック エンジニアリングと対話することができます。
- 輻輳などのネットワーク変更により、アプリケーションがセグメントルーティング トラフィック エンジニアリング トンネルの配置を最適化（再計算）することをトリガーできます。
- セグメントルーティング トンネルは、PCE のようなサウスバウンドプロトコルを使用してオーケストレータからネットワーク上に動的にプログラムされます。
- セグメントルーティング トンネルは中間点およびテールエンドルータでのシグナリングおよびフローごとの状態を必要としないため、アジャイル ネットワーク プログラミングが可能です。

• 出力ピアリング トラフィック エンジニアリング (EPE) :

- セグメントルーティングは集中型 EPE を可能にします。
- コントローラは、特定の出力プロバイダーのエッジと特定の外部インターフェイスを使用して宛先に到達するように、入力プロバイダーのエッジとコンテンツソースに指示します。
- BGP ピアリングセグメント ID は、ソースルーティングされたドメイン間パスを表すために使用されます。
- コントローラは、BGP リンクの状態 (BGP-LS) EPE ルートを介して、BGP ピアリング SID と出力境界ルータの外部トポロジを学習します。
- コントローラは、必要なパスを使用して入力ポイントをプログラムします。

- **プラグアンドプレイ展開** : セグメントルーティング トンネルは、既存の MPLS コントローラプレーンおよびデータプレーンと相互運用可能で、既存の展開に実装できます。

セグメントルーティンググローバルブロック

セグメントルーティンググローバルブロック (SRGB) は、セグメントルーティングのグローバルスコープの SID に予約されたラベルの範囲のことです。SRGB は、セグメントルーティングノードのローカルプロパティです。MPLS アーキテクチャでは、SRGB はグローバルセグメントに予約済みの一連のローカルラベルです。セグメントルーティングでは、各ノードを異なる SRGB で設定できます。そのため、IGP プレフィックスセグメントに関連付けられた絶対 SID はノードごとに変更できます。

SRGB のデフォルト範囲は 16000 ~ 23999 です。SRGB は、次のように設定できます。

```
Device(config)# segment-routing mpls
Device(config-srmppls)#segment-routing global-block 45000 55000
```

SRGB ラベル値は、次のようにホップバイホップで計算されます。

- ノード SID は、ローカル SRGB へのインデックスとしてアドバタイズされます。
- IGP は、ネクストホップによってアドバタイズされた SRGB にインデックスを追加することで、ノード SID に関連付けられた適切な MPLS ラベルを計算します。
- プラットフォームには、SRGB の下限と上限に特定の制限がある場合があります。これらの境界は、segment-routing global-block コマンドに関連付けられたヘルプ文字列に表示されます。例：

```
Router(config-srmppls)#global-block ?
<16-1048575> SR GB/LB Label Range Start
```

隣接関係セグメント識別子

隣接関係セグメント識別子 (adj-SID) は、パケットの方向を特定のインターフェイスとネクストホップに指定するローカルラベルです。adj-SID を有効にするために必要な特定の設定はありません。隣接関係 SID は、すべてのネイバーに対して IGP によって自動的に割り当てられます。

プレフィックスセグメント識別子

プレフィックスセグメント識別子 (SID) は、プレフィックスによって表される宛先にトラフィックを転送するために使用されます。

プレフィックス SID は、セグメントルーティンググローバルブロック (SRGB) へのインデックスです。インデックスはローカル MPLS ラベルにマッピングされます。このラベルの値は、ローカルにアドバタイズされた SRGB の開始値にインデックス値を追加することによって、ノードごとに計算されます。次に例を示します。

- ノードが 16000 ~ 23999 の SRGB 範囲をアドバタイズする場合、SID インデックス 100 は MPLS ラベル 16100 にマッピングされます。

- ノードが 25000 ～ 39999 の SRGB 範囲をアドバタイズする場合、SID インデックス 100 は MPLS ラベル 25100 にマッピングされます。

セグメントルーティングに関する追加情報

関連資料

関連項目	マニュアルタイトル
動画	<ul style="list-style-type: none">• シスコセグメントルーティングの概要 (YouTube)• シスコセグメントルーティングの概要 (CCO)



CHAPTER 3

IS-IS v4 ノード SID によるセグメントルーティング

この章では、セグメントルーティング（SR）が IS-IS でどのように機能するかについて、次のセクションに分けて説明します。

- IS-IS v4 ノード SID によるセグメントルーティングに関する機能情報, on page 13
- IS-IS v4 ノード SID によるセグメントルーティングに関する制約事項, on page 13
- IS-IS v4 ノード SID によるセグメントルーティングに関する情報（14 ページ）
- IS-IS v4 ノード SID によるセグメントルーティングの設定方法, on page 18
- セグメントルーティングの設定例：IS-IS v4 ノード SID, on page 26
- IS-IS v4 ノード SID によるセグメントルーティングに関する追加情報, on page 27

IS-IS v4 ノード SID によるセグメントルーティングに関する機能情報

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、<https://cfng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

IS-IS v4 ノード SID によるセグメントルーティングに関する制約事項

- ルーティング プロトコルの構成をそのルータ構成のサブ モードで許可する前に、セグメントルーティングを最上位レベルで設定する必要があります。

- IS-IS プロトコルの SR コマンドは、トポロジごと（IPv4 アドレス ファミリ）に基づいています。
- 有効な Cisco IOS-XE リリース 3.16 では、ISIS は IPv4 に対してのみセグメントルーティングをサポートしています。

IS-IS v4 ノード SID によるセグメントルーティングに関する情報

セグメントルーティング IS-IS v4 ノード SID

セグメントルーティングは、シスコの Intermediate System-to-Intermediate System (IS-IS) および Open Shortest Path First (OSPF) プロトコルのいくつかの拡張機能に依存しています。ルーティングプロトコルインスタンスのセグメントルーティングを有効にするには、2つのレベルの構成が必要です。セグメントルーティングインフラストラクチャコンポーネントによって管理される最上位のセグメントルーティング構成では、セグメントルーティングが可能になり、一方、ルータレベルでのセグメントルーティング構成では、ルーティングプロトコルインスタンスの特定のアドレスファミリに対してセグメントルーティングが可能になります。セグメントルーティングの状態には、次の3つがあります。

- SR_NOT_CONFIGURED
- SR_DISABLED
- SR_ENABLED

IGP 下のセグメントルーティング構成は、SR の状態が SR_DISABLED または SR_ENABLED のいずれかである場合にのみ許可されます。SR_ENABLED 状態は、少なくとも MFI によって正常に予約済みの有効な SRGB 範囲にあることを示します。コマンドを使用して、ルータ設定サブモードで IGP のセグメントルーティングを有効にすることができます。ただし、IGP セグメントルーティングは、グローバル SR が設定された後にのみ有効になります。

SR_ENABLED は、SR を有効にするためにすべてのプロトコルに必要な状態ですが、プロトコルインスタンスの SR を有効にするには十分ではありません。その理由は、IS-IS にセグメントルーティンググローバルブロック (SRGB) 情報に関する情報がまだないことです。SRGB に関する情報を受信する要求が正常に処理されると、IS-IS SR の動作状態が有効になります。

セグメントルーティングでは、各ルータが、セグメントルーティングデータプレーン機能と、グローバル SID が割り当てられている場合にセグメントルーティングに使用される MPLS ラベル値の範囲をアドバタイズする必要があります。データプレーン機能とラベル範囲は、RFC4971 で定義されている、IS-IS ルータ機能 TLV-242 に挿入される SR 機能サブ TLV を使用してアドバタイズされます。

ISIS SR 機能サブ TLV には、すべての予約済み SRGB 範囲が含まれます。ただし、シスコの実装でサポートされる SRGB 範囲は1つだけです。サポートされている IPv4 プレフィックス SID サブ TLV は、TLV-135 および TLV-235 です。

リモートルータからのラベルスイッチドパスで受信するプレフィックス SID

到達可能性 TLV (TLV 135 および 235) を使用してラベルスイッチドパス (LSP) で受信したプレフィックス SID は、次の条件が満たされている場合にのみ、プレフィックス VPN ラベルごとの BGP ダウンロードと同じ方法でルーティング情報ベース (RIB) にダウンロードされません。

- トポロジとアドレスファミリに対してセグメントルーティングが有効。
- プレフィックス SID が有効。
- MFI へのローカルラベルのバインドが成功している。



Note

- 指定された SID 範囲に収まらない SID の場合、RIB の更新時にラベルは使用されません。SID が SID の範囲内には収まるが、ネクストホップのネイバー SID の範囲には収まらない場合は、そのパスに関連付けられているリモートラベルはインストールされません。
- 到達可能性 TLV (TLV 135 および 235) を使用して LSP で受信されたノード SID は、対応するアドレスファミリでセグメントルーティングが有効になっている場合にのみ RIB にダウンロードされます。
- 複数のベストネクストホップの場合は、すべてのネクストホップがセグメントルーティングをサポートしていないと、ISIS は同じプレフィックスに割り当てられた一致しないラベルに類似したインスタンスを処理します。つまり、IS-IS がラベルを無視し、すべての ECMP パスについてラベルのないパスをグローバル RIB にインストールすることを意味します。

セグメントルーティング隣接関係 SID アドバタイズメント

Cisco IOS XE リリース 3.17 では、IS-IS によるセグメントルーティング隣接関係 SID のアドバタイズメントのサポートが有効です。隣接関係セグメント識別子 (Adj-SID) は、セグメントルーティングにおけるルータ隣接関係を表します。

セグメントルーティング対応ルータは、隣接関係ごとに Adj-SID を割り当てることができ、この SID を隣接関係 TLV で伝送するように Adj-SID サブ TLV が定義されます。IS-IS 隣接関係は、次のいずれかのネイバー TLV を使用してアドバタイズされます。

- TLV-22 [RFC5305]
- TLV-23 [RFC5311]

IS-IS は、IS-IS 隣接関係状態がアップであり、IS-IS セグメントルーティングの内部動作状態が有効になっている場合にのみ、IS-IS ネイバーごとに隣接関係 SID を割り当てます。ラベルリソースの不足が原因で隣接関係 SID の割り当てに失敗した場合、IS-IS は、デフォルトの間隔 (30 秒) で定期的に Adj-SID の割り当てを再試行します。

隣接関係（アジャセンシー）SID

Cisco IOS XE リリース 3.18 では、複数の隣接関係 SID がサポートされています。保護された P2P/LAN 隣接関係のそれぞれに対して、IS-IS は 2 つの Adj-SID を割り当てます。バックアップ Adj-SID は、インターフェイス上で FRR（ローカル LFA）が有効になっているときにのみ割り当てられ、アドバタイズされます。FRR が無効になっている場合は、バックアップ隣接関係 SID が解放されます。フォワーディングプレーンでの保護された adj-SID の永続化はサポートされません。プライマリリンクがダウンしている場合、IS-IS は、遅延タイマーが期限切れになるまでバックアップ Adj-SID の解放を遅らせます。これにより、フォワーディングプレーンは、ルータがコンバージされるまで、バックアップパスを経由してトラフィックを転送し続けることができます。

Cisco IOS XE リリース 3.18 では、フォワーディングプレーンがプロトコル固有のレベルを認識しないので、IS-IS Adj-SID はレベルごとに変更されます。割り当てられ、アドバタイズされたバックアップ Adj-SID は、**show isis neighbor detail** および **show isis data verbose** コマンドの出力で表示できます。

セグメントルーティング マッピング サーバー

セグメントルーティング マッピング サーバー（SRMS）を使用すると、プレフィックス SID マッピング ポリシー エントリの構成と保守を行うことができます。Cisco IOS XE リリース 3.17 では、IGP は SRMS のアクティブ ポリシーを使用して、フォワーディングプレーンのプログラミング時に SID 値を決定します。

SRMS は、ネットワークの SID/ラベル マッピング ポリシーにプレフィックスを提供します。一方、IGP は、プレフィックス SID/ラベル バインディング TLV を介して SID/ラベル マッピング ポリシーにプレフィックスをアドバタイズする役割を担います。アクティブ ポリシー情報と変更は、アクティブ ポリシー情報を使用して転送情報を更新する IGP に通知されます。

接続されたプレフィックス SID

場合によってはルータは、LSP にアドバタイズするものとは異なる SID を持つプレフィックスをインストールすることがあります。たとえば、複数のプロトコルまたは複数の IGP インスタンスが、異なる SID を持つ同じプレフィックスを SRMS にアナウンスしている場合、SRMS は競合を解決し、ローカルインスタンスと同じでない可能性がある競合に勝ったプレフィックスと SID をアナウンスします。その場合、IGP は、常にソース LSP から学習した内容をアドバタイズしますが、その LSP で学習したものとは異なる可能性がある SID のインストールを試みます。これは IGP が別のプロトコルまたは別のプロトコル インスタンスから SID を再配布することを防ぐために行われます。

SRGB 範囲の変更

IS-IS セグメントルーティングが設定されている場合、IS-IS は、IS-IS SR の動作状態を有効にする前に SRGB とのインタラクションを要求する必要があります。SRGB 範囲が作成されていない場合、IS-IS は有効になりません。

SRGB 変更イベントが発生した場合、IS-IS は、そのサブブロック エントリで対応する変更を行います。また IS-IS は、SR 機能サブ TLV で新しく作成または拡張された SRGB 範囲をアドバタイズし、プレフィックス SID サブ TLV アドバタイズメントを更新します。



Note Cisco IOS XE リリース 3.16 では、変更に対して 1 つの SRGB 範囲と SRGB 拡張機能のみがサポートされます。

SRGB の削除

IS-IS が SRGB 削除イベントを受信すると、IS-IS は、IS-IS SRGB キューのリストで SRGB エントリを検索します。SRGB エントリが存在しない場合、IS-IS は保留中の SRGB が作成されたイベントがないことを確認します。保留中の SRGB 作成イベントが見つかった場合、IS-IS は SRGB 作成イベントを削除し、SRGB の削除処理を完了します。

IS-IS SRGB キューで SRGB エントリが見つかった場合、IS-IS は SRGB をロックし、RIB を再配布し、保留中の削除 SRGB 範囲内の SID の値を持つすべてのプレフィックス SID をアドバタイズせず、SR 機能サブ TLV から SRGB 範囲をアドバタイズしません。IS-IS は SRGB の削除処理を完了すると、SRGB のロックを解除し、その SR サブブロック エントリから SRGB を削除します。

SRGB の削除後に有効な SRGB がない場合、IS-IS SR の動作状態が無効になります。

インターフェイスでの MPLS 転送

セグメントルーティングがインターフェイスを使用する前に、MPLS 転送を有効にする必要があります。IS-IS は、インターフェイスでの MPLS 転送を有効にする役割を担います。

セグメントルーティングが IS-IS トポロジに対して有効になっている場合、または IS-IS セグメントルーティングの動作状態が有効になっている場合、IS-IS は、IS-IS トポロジがアクティブである任意のインターフェイスに対して MPLS を有効にします。同様に、IS-IS トポロジのセグメントルーティングが無効になっている場合、IS-IS は、そのトポロジのすべてのインターフェイスで MPLS 転送を無効にします。

セグメントルーティングと LDP の設定

コマンド `sr-label-preferred` により、転送インターフェイスは、トポロジ内のすべてのプレフィックスに対して、セグメントルーティングラベルを LDP ラベルより優先させることができます。

セグメントルーティングトラフィックエンジニアリングの通知

IS-IS は、少なくとも 1 つのレベルに対して IS-IS SR と TE の両方が有効になっていることを検出した場合、セグメントルーティング情報を TE に通知します。IS-IS は、TE が設定されているレベルから取得された情報のみをアナウンスします。

同様に IS-IS は、セグメントルーティングが有効になっていないこと、または TE がどのレベルでも設定されていない状態になったことを検出した場合、すべての通知を削除するように TE に指示します。

IS-IS v4 ノード SID によるセグメントルーティングの設定方法

セグメントルーティングの設定

Before you begin

セグメントルーティングをサポートするように IS-IS を設定する前に、最初にグローバル コンフィギュレーション モードでセグメントルーティング機能を設定する必要があります。

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **segment-routing mpls**
4. **connected-prefix-sid-map**
5. **address-family ipv4**
6. **10.1.1.1/32 index 100 range 1**
7. **exit-address-family**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	enable Example: Device# enable	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	configure terminal Example: 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	segment-routing mpls Example: Device(config-sr)# segment-routing mpls	MPLS データ プレーンを使用してセグメント機能を有効にします。

	Command or Action	Purpose
ステップ 4	connected-prefix-sid-map Example: Device(config-srmppls)# connected-prefix-sid-map	ローカルプレフィックスと SID のアドレスファミリ固有のマッピングを設定できるサブモードを開始します。
ステップ 5	address-family ipv4 Example: Device(config-srmppls-conn)# address-family ipv4	IPv4 アドレスプレフィックスを指定します。
ステップ 6	10.1.1.1/32 index 100 range 1 Example: Device(config-srmppls-conn-af)# 10.1.1.1/32 100 range 1	SID 100 にアドレス 1.1.1.1/32 を関連付けます。
ステップ 7	exit-address-family Example: Device(config-srmppls-conn-af)# exit-address-family	アドレスファミリを終了します。

IS-IS ネットワークでのセグメントルーティングの設定

始める前に

IS-IS ネットワークでセグメントルーティングを設定するには、その前にネットワークで IS-IS をイネーブルにする必要があります。

手順の概要

1. **router isis**
2. **net network-entity-title**
3. **metric-style wide**
4. **segment-routing mpls**
5. **exit**
6. **show isis segment-routing**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	router isis 例： Device(config-router)# router isis	IS-IS ルーティング プロトコルをイネーブルにし、ルータ 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	net network-entity-title 例： Device(config-router)# net 49.0000.0000.0003.00	ルーティング インスタンスの Network Entity Title (NET) を設定します。
ステップ 3	metric-style wide 例： Device(config-router)# metric-style wide	ワイドリンク メトリックだけを生成および受け入れるようにデバイスを設定します。
ステップ 4	segment-routing mpls 例： Device(config-router)# segment-routing mpls	セグメントルーティングの動作状態を設定します。
ステップ 5	exit 例： Device(config-router)# exit	セグメントルーティングモードを終了し、コンフィギュレーション 端末モードに戻ります。
ステップ 6	show isis segment-routing 例： Device# show is-is segment-routing	(任意) IS-IS セグメント ルーティングの現在の状態を表示します。

例

次の例は、IS-IS のセグメントルーティングに関する **show isis segment-routing state** コマンドからの出力を示しています。

```
Device# show isis segment-routing
```

```
ISIS protocol is registered with MFI
ISIS MFI Client ID:0x63
Tag 1 - Segment-Routing:
  SR State:SR_ENABLED
  Number of SRGB:1
  SRGB Start:16000, Range:8000, srgb_handle:0x4500AED0, srgb_state: created
```

```
Address-family IPv4 unicast SR is configured
Operational state:Enabled
```

IS-IS のプレフィックス SID の設定

このセクションでは、各インターフェイスでプレフィックスセグメント識別子 (SID) のインデックスを設定する方法について説明します。

始める前に

セグメントルーティングを対応するアドレスファミリでイネーブルにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **segment-routing mpls**
4. **connected-prefix-sid-map**
5. **address-family ipv4**
6. **10.1.1.1/32 index 100 range 1**
7. **exit**

手順の詳細

手順

	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	segment-routing mpls 例 : Device(config)# segment-routing mpls	セグメントルーティング MPLS モードを設定します。
ステップ 4	connected-prefix-sid-map 例 : Device(config-srmppls)# connected-prefix-sid-map	ローカルプレフィックスと SID のアドレスファミリ固有のマッピングを設定できるサブモードを開始します。

プレフィックス属性 N-Flag の設定

	コマンドまたはアクション	目的
ステップ 5	address-family ipv4 例： Device(config-srmppls-conn)# address-family ipv4	IPv4 アドレス ファミリを指定し、ルータ アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 6	10.1.1.1/32 index 100 range 1 例： Device(config-srmppls-conn-af)# 10.1.1.1/32 100 range 1	SID 100 にアドレス 1.1.1.1/32 を関連付けます。
ステップ 7	exit 例： Device(config-router)# exit	セグメントルーティングモードを終了し、コンフィギュレーション端末モードに戻ります。

プレフィックス属性 N-Flag の設定

デフォルトでは、ループバックアドレスに関連付けられた SID をアドバタイズするときに、IS-IS によって N-flag と呼ばれるフラグが設定されます。このフラグをクリアするには、明示的な設定を追加します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface loopback3**
4. **isis prefix n-flag-clear**

手順の詳細

手順

	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。パスワードを入力します（要求された場合）。
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。

	コマンドまたはアクション	目的
ステップ 3	interface loopback3 例 : Device(config)# interface loopback3	インターフェイス ループバックを指定します。
ステップ 4	isis prefix n-flag-clear 例 : Device(config-if)# isis prefix n-flag-clear	プレフィックス N-flag をクリアします。

明示的 Null 属性の設定

penultimate-hop-popping (PHP) を無効にし、明示的ヌル ラベルを追加するには、explicit-null オプションを指定する必要があります。オプションを指定すると、IS-IS は、プレフィックス SID サブ TLV に E フラグを設定します。

デフォルトでは、ループバック アドレスに関連付けられたプレフィックス SID をアドバタイズするときに、IS-IS によって E-flag (明示的ヌルフラグ) と呼ばれるフラグが 0 に設定されます。このフラグを設定するには、明示的な設定を追加します。

SUMMARY STEPS

1. enable
2. configure terminal
3. segment-routing mpls
4. set-attributes
5. address-family ipv4
6. explicit-null
7. exit-address-family

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	enable Example: Device# enable	特権 EXEC モードを有効にします。パスワードを入力します (要求された場合)。
ステップ 2	configure terminal Example: 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。

	Command or Action	Purpose
ステップ 3	segment-routing mpls Example: Device(config)# segment-routing mpls	セグメントルーティング MPLS モードを設定します。
ステップ 4	set-attributes Example: Device(config-srmppls)# set-attributes	属性を設定します。
ステップ 5	address-family ipv4 Example: Device(config-srmppls-attr)# address-family ipv4	IPv4 アドレス ファミリを指定し、ルータ アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 6	explicit-null Example: Device(config-srmppls-attr-af)# explicit-null	explicit-null ラベルを有効化します。
ステップ 7	exit-address-family Example: Device(config-srmppls-attr-af)# exit-address-family	アドレス ファミリを終了します。

セグメントルーティング Label Distribution Protocol 優先順位の設定

手順の概要

1. enable
2. configure terminal
3. segment-routing mpls
4. set-attributes
5. address-family ipv4
6. sr-label-preferred
7. exit-address-family

手順の詳細

手順

	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。パスワードを入力します（要求された場合）。
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	segment-routing mpls 例 : Device(config)# segment-routing mpls	セグメント ルーティング MPLS モードを設定します。
ステップ 4	set-attributes 例 : Device(config-srmpls)# set-attributes	属性を設定します。
ステップ 5	address-family ipv4 例 : Device(config-srmpls-attr)# address-family ipv4	IPv4 アドレス ファミリを指定し、ルータ アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 6	sr-label-preferred 例 : Device(config-srmpls-attr-af)# sr-label-preferred	LDP より優先される SR ラベルを指定します。
ステップ 7	exit-address-family 例 : Device(config-srmpls-attr-af)# exit-address-family	アドレス ファミリを終了します。

IS-IS SRMS の設定

次のコマンドは、IS-IS SRMS を有効にして、IS-IS がローカルマッピング エントリをアドバタイズできるようにします。IS-IS は、SRMS ライブラリにリモート エントリを送信しません。

ただし、IS-ISは、ローカルに設定されたマッピングエントリのみに基づいて計算されるSRMSアクティブポリシーを使用します。

```
[no] segment-routing prefix-sid-map advertise-local
```

IS-IS SRMS クライアントの設定

デフォルトでは、IS-IS SRMS クライアントモードが有効になっています。IS-ISは、常にSRMSにLSPを通じて受信したリモートプレフィックスSIDマッピングエントリを送信します。SRMSアクティブポリシーは、ローカルおよびリモートのマッピングエントリに基づいて計算されます。

次のコマンドを実行すると、プレフィックスSIDマッピングクライアント機能が無効になり、受信者側で設定されます。

```
segment-routing prefix-sid-map receive [disable]
```

IS-IS SID バインド TLV ドメインフラッディングの設定

デフォルトでは、IS-IS SRMS サーバーは、ルーティングドメイン内のSIDバインディングエントリをフラッディングしません。Cisco IOS-XE リリース3.18以降、IS-IS SRMS サーバーモードコマンドにオプションのキーワード **domain-wide** が追加され、SIDおよびラベルバインドTLVフラッディング機能が有効になります。

```
segment-routing prefix-sid-map advertise-local [domain-wide]
```

キーワード **domain-wide** を使用すると、IS-IS SRMS サーバーは、ルーティングドメイン全体でSIDバインドTLVをアドバタイズできます。



Note このオプションは、IS-IS SRMS が SRMS サーバー モードで実行する場合にのみ有効です。

セグメントルーティングの設定例：IS-IS v4 ノード SID

例：IS-IS ネットワークでのセグメントルーティングの設定

次の例では、各インターフェイスでプレフィックスセグメントID (SID) を設定する方法について説明します。

```
Device(config)#segment-routing mpls
Device(config-srmppls)#connected-prefix-sid-map
Device(config-srmppls-conn)#address-family ipv4
Device(config-srmppls-conn-af)#10.1.2.2/32 index 2 range 1
```

```
Device(config-srmppls-conn-af)#exit-address-family
Device(config-srmppls-conn-af)#end
```

例：明示的 Null 属性の設定

明示的な Null 属性を設定する例を次に示します。

```
Device(config)# segment-routing mpls
Device(config-srmppls)# set-attributes
Device(config-srmppls-attr)# address-family ipv4
Device(config-srmppls-attr-af)# explicit-null
Device (config-srmppls-attr-af)# exit-address-family
```

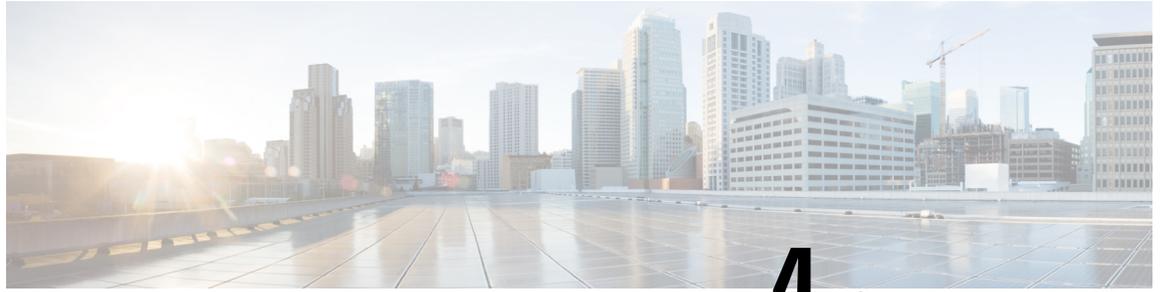
IS-IS v4 ノード SID によるセグメントルーティングに関する追加情報

関連資料

関連項目	マニュアルタイトル
IP ルーティング ISIS コマンド	Cisco IOS IP ルーティング ISIS コマンド

RFC

RFC	タイトル
RFC4971	『Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information』
RFC5305	『IS-IS Extensions for Traffic Engineering』。IPv4 用のルータ ID のアドバタイズメントを定義します。
RFC6119	『IPv6 Traffic Engineering in IS-IS』。IPv6 用のルータ ID のアドバタイズメントを定義します。



第 4 章

IS-IS リンク保護のトポロジに依存しないループフリー代替高速再ルーティング

このドキュメントでは、セグメントルーティング（SR）のトポロジに依存しないループフリー代替（TI-LFA）リンク保護を使用した IP 高速再ルーティング機能（IPFRR）の機能性と IS-IS の実装について説明します。

- [IS-IS リンク保護のトポロジに依存しないループフリー代替高速再ルーティングの機能情報（29 ページ）](#)
- [IS-IS リンク保護のトポロジに依存しないループフリー代替高速再ルーティングの前提条件, on page 30](#)
- [IS-IS リンク保護のトポロジに依存しないループフリー代替高速再ルーティングについて（31 ページ）](#)
- [IS-IS リンク保護のトポロジに依存しないループフリー代替高速再ルーティングの設定方法（34 ページ）](#)

IS-IS リンク保護のトポロジに依存しないループフリー代替高速再ルーティングの機能情報

表 2: IS-IS リンク保護のトポロジに依存しないループフリー代替高速再ルーティングの機能情報

機能名	リリース	機能情報
IS-IS リンク保護のトポロジに依存しないループフリー代替高速再ルーティング	Cisco IOS XE Amsterdam 17.3.2	次のコマンドが導入または変更されました。 fast-reroute ti-lfa {level-1 level-2} [maximum-metric value] 、 isis fast-reroute ti-lfa protection level-1 disable 、 isis fast-reroute ti-lfa protection {level-1 level-2} [maximum-metric value] 、 show running all section interface interface-name 、 show running all section router isis 。

IS-IS リンク保護のトポロジに依存しないループフリー代替高速再ルーティングの前提条件

- すべてのノードで TI-LFA を有効にしてから、TI-LFA 用の SR-TE を設定してください。

```

mpls traffic-eng tunnels
!
segment-routing mpls
connected-prefix-sid-map
  address-family ipv4
    10.1.1.1/32 index 11 range 1
  exit-address-family
!
interface Loopback1
  ip address 10.1.1.1 255.255.255.255
  ip router isis 1
!
interface Tunnel1
  ip unnumbered Loopback1
  tunnel mode mpls traffic-eng
  tunnel destination 10.6.6.6
  tunnel mpls traffic-eng autoroute announce
  tunnel mpls traffic-eng path-option 10 explicit name IP_PATH segment-routing
!
interface GigabitEthernet2
  ip address 192.168.1.1 255.255.255.0
  ip router isis 1
  negotiation auto
  mpls traffic-eng tunnels
  isis network point-to-point
!
interface GigabitEthernet3
  ip address 192.168.2.1 255.255.255.0
  ip router isis 1
  negotiation auto
  mpls traffic-eng tunnels
  isis network point-to-point
!
router isis 1
  net 49.0001.0010.0100.1001.00
  is-type level-1
  metric-style wide
  log-adjacency-changes
  segment-routing mpls
  fast-reroute per-prefix level-1 all
  fast-reroute ti-lfa level-1
  mpls traffic-eng router-id Loopback1
  mpls traffic-eng level-1
!
ip explicit-path name IP_PATH enable
  next-address 10.4.4.4
  next-address 10.5.5.5
  next-address 10.6.6.6

```

- プライマリとセカンダリのパス切り替えの場合で、ルータ間でマイクロループが作成された場合は、コンバージェンス時間を減らす必要があります。**microloop avoidance** **rib-update-delay** コマンドを使用して、コンバージェンス時間を減らします。

```
router isis ipfrr
net 49.0001.0120.1201.2012.00
is-type level-2-only
metric-style wide
log-adjacency-changes
segment-routing mpls
segment-routing prefix-sid-map advertise-local
fast-reroute per-prefix level-2 all
fast-reroute ti-lfa level-2
microloop avoidance rib-update-delay 10000
```

- 高可用性 (HA) 切り替え後のトラフィック損失を削減または最小化するために、MPLS-TE ノンストップルーティング (NSR) と IS-IS ノンストップフォワーディング (NSF) を有効にします。グローバル EXEC モードで **mpls traffic-eng nsr** コマンドを使用します。

```
mpls traffic-eng nsr
```

IS-IS で **nsf** コマンドを使用します。

```
router isis
nsf cisco
nsf interval 0
```

IS-IS リンク保護のトポロジに依存しないループフリー代替高速再ルーティングについて

ローカル LFA およびリモート LFA が有効になっている場合、保護すべきプレフィックスのカバレッジは良好になります。ただし、PQ インターセクトノードを持たないいくつかのまれなトポロジでは、ローカルおよびリモート LFA のどちらも、失敗したリンクを保護するために解放ノードを見つけることに失敗します。さらに、2つのアルゴリズムには LFA のコンバージェンス後の特性についての知識がないため、コンバージェンス後の経路を優先する方法はありません。

上記の制限を克服するために、有効な Cisco IOS-XE リリース 3.18 では、トポロジに依存しない LFA (TI-LFA) が SR 対応ネットワークでサポートされます。

トポロジに依存しないループフリー代替

TI-LFA は以下のためのサポートを提供します。

- リンク保護：LFA はリンクの障害のための修復パスを提供します。
- ローカル LFA：コンバージェンス後のパスのローカル LFA が利用可能であるときはいつでも、ローカル LFA は修復パスのための追加 SID を必要としないので、TI LFA より優先されます。つまり、PQ ノードのラベルは、リリース ノードには必要ありません。
- 拡張 P スペースのローカル LFA：拡張 P スペースのノードの場合、ローカル LFA は今でも修復パスのための最も経済的な方法です。この場合、TI-LFA は選択されません。

- PQ 交差ノードへのトンネル：これは、修復パスが TI-LFA を使用してコンバージェンス後のパスで保証されることを除いて、リモート LFA と類似しています。
- PQ 分離ノードへのトンネル：ローカルおよびリモート LFA が修復パスを見つけられない場合には、この機能は TI-LFA に固有です。
- プラットフォームのサポートされている最大ラベル数までの、複数の交差または分離 PQ ノードを通過するトンネル：TI-LFA は、すべてのプレフィックスの完全なカバレッジを提供します。
- 保護されたリンクのための P2P インターフェイス：TI-LFA は P2P インターフェイスを保護します。
- 非対称リンク：ネイバー間の ISIS メトリックは同じではありません。
- マルチホーム（エニーキャスト）プレフィックス保護：同じプレフィックスが複数のノードによって発信される場合があります。
- 保護されたプレフィックスのフィルタリング：ルートマップは、保護するプレフィックスのリストと、リリースノードまでの最大修復距離を制限するオプションを含めるかまたは除外します。
- タイブレーカー：TI-LFA に適用可能な既存のタイブレーカーのサブセットがサポートされています。

トポロジに依存しないループフリー代替タイブレーク

ローカルおよびリモート LFA は、プレフィックスを保護するために複数のパスがある場合、デフォルトまたはユーザー設定のヒューリスティックを使用してタイブレークします。この属性は、ロードバランシングの前に、TI-LFA リンク保護計算の終了時に修復パスの数を削減するために使用されます。ローカル LFA およびリモート LFA は次のタイブレーカーをサポートします。

- Linecard-disjoint：ラインカード分離修復パスを優先します
- Lowest-backup-path-metric：最小の合計メトリックを持つ修復パスを優先します
- Node-protecting：修復パスを保護するノードを優先します
- SRLG-disjoint：SRLG 分離修復パスを優先します
- Load-sharing：リンクとプレフィックスの間で均等に修復パスを分配します

特定のプレフィックスに対して2つの修復パスがある場合、プライマリポートのものとは異なるラインカードの出力ポートであるパスが、修復パスとして選択されます。TI-LFA リンク保護の場合、次のタイブレーカーがサポートされています。

- Linecard-disjoint：ラインカード分離修復パスを優先します。
- LC disjoint index：修復パスの両方がプライマリパスのものと同じラインカード上にある場合、両方のパスが候補と見なされます。パスの1つが別のラインカード上にある場合は、そのパスが修復パスとして選択されます。
- SRLG index：両方の修復パスがプライマリパスのものと同じ SRLG ID を持つ場合、両方のパスが候補と見なされます。パスの1つが異なる srlg id を持つ場合、そのパスが修復パスとして選択されます。

- **Node-protecting** : TI-LFA ノード保護の場合、コンバージェンス後の最短パスを計算するときに保護ノードが削除されます。修復パスは、保護されたノードの周囲のトラフィックを指示する必要があります。

SRLG ID は、各インターフェイスに対して構成できます。プレフィックスに対して2つの修復パスがある場合、修復パスに設定された SRLG ID は、プライマリパス SRLG ID のものと比較されます。セカンダリパスの SRLG ID がプライマリのものとは異なる場合、そのパスが修復パスとして選択されます。このポリシーが有効になるのは、プライマリパスが SRLG ID で構成されている場合のみです。同じインターフェイスまたは同じプロトコルインスタンスに対して、ノードと SRLG の両方の保護モードを設定することができます。その場合、追加の TI-LFA ノード SRLG の組み合わせ保護アルゴリズムが実行されます。TI-LFA ノード SRLG の組み合わせアルゴリズムは、コンバージェンス後の SPT を計算するときに、保護されたノードと、同じ SRLG グループを持つインターフェイスのすべてのメンバーを削除します。

インターフェイス高速再ルーティング タイブレーカー

インターフェイス高速再ルーティング (FRR) タイブレーカーは、TI-LFA ノードおよび SRLG 保護にも必要です。インターフェイスおよびプロトコルインスタンス FRR タイブレーカーの両方が設定されている場合、インターフェイス FRR タイブレーカーはプロトコルインスタンスよりも優先されます。インターフェイス FRR タイブレーカーが設定されていない場合、インターフェイスは、プロトコルインスタンス FRR タイブレーカーを継承します。

以下のインターフェイス FRR タイブレーカー コマンドは、特定のインターフェイスにのみ適用されます。

```
isis fast-reroute tie-break
[level-1 | level-2] linecard-disjoint
priority
isis fast-reroute tie-break
[level-1 | level-2] lowest-backup-metric
priority
isis fast-reroute tie-break
[level-1 | level-2] node-protecting
priority
isis fast-reroute tie-break
[level-1 | level-2] srlg-disjoint
priority
isis fast-reroute tie-break
[level-1 | level-2] default
```

同じインターフェイス上のタイブレーカーのデフォルトと明示的なタイブレーカーは、相互に排他的です。

以下のタイブレーカーは、すべての LFA でデフォルトで有効になっています。

- linecard-disjoint
- lowest-backup-metric
- srlg-disjoint

Cisco IOS XE リリース 3.18 では、ノード保護タイブレーカーはデフォルトで無効になっています。

IS-IS リンク保護のトポロジに依存しないループフリー代替高速再ルーティングの設定方法

リンク保護のトポロジに依存しないループフリー代替高速再ルーティングを設定するには、以下のステップを実行します。

トポロジに依存しないループフリー代替高速再ルーティングの設定

次の2つの方法のいずれかを使用して、TI-LFA を有効にすることができます。

1. **プロトコルの有効化**：すべてのIS-IS インターフェイスに対してルータ isis モードで TI-LFA を有効にします。必要に応じて、インターフェイス コマンドを使用して、TI-LFA を無効にするインターフェイスを除外します。

たとえば、すべての IS-IS インターフェイスに対して TI-LFA を有効にするには次を実行します。

```
router isis 1
fast-reroute per-prefix {level-1 | level-2}
fast-reroute ti-lfa {level-1 | level-2} [maximum-metric value]
```



Note `isis fast-reroute protection level-x` コマンドはローカル LFA を有効にし、TI-LFA の有効化を要求されます。

2. **インターフェイスの有効化**：各インターフェイスで TI-LFA を選択的に有効にします。

```
interface interface-name
isis fast-reroute protection {level-1 | level-2}
isis fast-reroute ti-lfa protection {level-1 | level-2} [maximum-metric value]
```

maximum-metric オプションは、ノードがリリース ノードとして適格であると見なされる最大修復距離を指定します。

インターフェイスとプロトコルの両方で TI-LFA が有効になっている場合、インターフェイス設定はプロトコル設定より優先されます。TI-LFA はデフォルトでは無効になっていません。

特定のインターフェイスで TI-LFA を無効にするには、次のコマンドを使用します。

```
interface interface-name
isis fast-reroute ti-lfa protection level-1 disable
```

マッピングサーバーを使用したトポロジに依存しないループフリー代替の設定

構成を理解するために、次のトポロジを検討してください。



- IXIA-2 は ISIS のプレフィックスを注入し、IXIA-1 は一方向のトラフィックを IXIA-2 に送ります
- .
- R1 10,000 プレフィックスはセグメントルーティングマッピングサーバーで設定されます。

R1 の設定は次のとおりです。

```

configure terminal
segment-routing mpls
global-block 16 20016
!
connected-prefix-sid-map
address-family ipv4
10.11.11.11/32 index 11 range 1
exit-address-family
!
!
mapping-server
!
prefix-sid-map
address-family ipv4
10.0.0.0/24 index 2 range 1 attach
203.0.113.1/24 index 1 range 1 attach
192.168.0.0/24 index 100 range 10000 attach
exit-address-family
!
!
!
!
interface Loopback0
ip address 10.11.11.11 255.255.255.255
ip router isis ipfrr
!
interface GigabitEthernet0/1/0
ip address 10.14.0.1 255.255.255.0
ip router isis ipfrr
negotiation auto
isis network point-to-point
!
interface GigabitEthernet0/1/2
ip address 10.0.0.1 255.255.255.0
ip router isis ipfrr
negotiation auto
isis network point-to-point
!

```

```

interface GigabitEthernet0/1/4
ip address 203.0.113.2 255.255.255.0
ip router isis ipfrr
negotiation auto
isis network point-to-point
!
router isis ipfrr
net 49.0001.0110.1101.1011.00
is-type level-2-only
metric-style wide
log-adjacency-changes
nsf cisco
segment-routing mpls
segment-routing prefix-sid-map advertise-local
fast-reroute per-prefix level-2 all
fast-reroute ti-lfa level-2
microloop avoidance rib-update-delay 10000

```

R2 の設定は次のとおりです。

```

configure terminal
!
!
segment-routing mpls
!
connected-prefix-sid-map
address-family ipv4
10.12.12.12/32 index 12 range 1
exit-address-family
!
!
interface Loopback0
ip address 10.12.12.12 255.255.255.255
ip router isis ipfrr
!
interface GigabitEthernet0/1/0
ip address 10.12.0.1 255.255.255.0
ip router isis ipfrr
negotiation auto
isis network point-to-point
!
interface GigabitEthernet0/1/1
ip address 10.11.0.2 255.255.255.0
ip router isis ipfrr
negotiation auto
isis network point-to-point
!
router isis ipfrr
net 49.0001.0120.1201.2012.00
is-type level-2-only
metric-style wide
log-adjacency-changes
nsf cisco
segment-routing mpls
segment-routing prefix-sid-map advertise-local
fast-reroute per-prefix level-2 all
fast-reroute ti-lfa level-2
microloop avoidance rib-update-delay 10000
!

```

R3 の設定は次のとおりです。

```

configure terminal

```

```
!  
mpls traffic-eng tunnels  
!  
segment-routing mpls  
!  
connected-prefix-sid-map  
address-family ipv4  
10.13.13.13/32 index 13 range 1  
exit-address-family  
!  
!  
interface Loopback0  
ip address 10.13.13.13 255.255.255.255  
ip router isis ipfrr  
!  
interface GigabitEthernet0/0/4  
ip address 10.13.0.1 255.255.255.0  
ip router isis ipfrr  
load-interval 30  
speed 1000  
no negotiation auto  
isis network point-to-point  
!  
interface GigabitEthernet0/0/5  
ip address 10.12.0.2 255.255.255.0  
ip router isis ipfrr  
negotiation auto  
isis network point-to-point  
!  
router isis ipfrr  
net 49.0001.0130.1301.3013.00  
is-type level-2-only  
metric-style wide  
log-adjacency-changes  
nsf cisco  
segment-routing mpls  
segment-routing prefix-sid-map advertise-local  
fast-reroute per-prefix level-2 all  
fast-reroute ti-lfa level-2  
microloop avoidance rib-update-delay 10000  
!
```

R4 の設定は次のとおりです。

```
configure terminal  
!  
mpls traffic-eng tunnels  
!  
segment-routing mpls  
!  
connected-prefix-sid-map  
address-family ipv4  
10.14.14.14/32 index 14 range 1  
exit-address-family  
!  
!  
interface Loopback0  
ip address 10.14.14.14 255.255.255.255  
ip router isis ipfrr  
!  
interface GigabitEthernet0/0/0  
ip address 10.14.0.2 255.255.255.0  
ip router isis ipfrr  
negotiation auto
```

例：IS-IS リンク保護のトポロジに依存しないループフリー代替高速再ルーティングの設定

```

isis network point-to-point
!
interface GigabitEthernet0/0/3
ip address 10.13.0.2 255.255.255.0
ip router isis ipfrr
speed 1000
no negotiation auto
isis network point-to-point
!
interface GigabitEthernet0/0/5
ip address 10.120.0.1 255.255.255.0
ip router isis ipfrr
speed 1000
no negotiation auto
isis network point-to-point
!
router isis ipfrr
net 49.0001.0140.1401.4014.00
is-type level-2-only
metric-style wide
log-adjacency-changes
nsf cisco
segment-routing mpls
segment-routing prefix-sid-map advertise-local
fast-reroute per-prefix level-2 all
fast-reroute ti-lfa level-2
microloop avoidance rib-update-delay 10000
!

```

例：IS-IS リンク保護のトポロジに依存しないループフリー代替高速再ルーティングの設定

例1：次の例では、ローカル LFA が linecard-disjoint と srlg-disjoint タイブレーカーで設定されています。Linecard-disjoint は、srlg-disjoint (11) よりも低い優先順位値 (10) で優先されます。

```

router isis access
net 49.0001.2037.0685.b002.00
metric-style wide
fast-flood 10
max-lsp-lifetime 65535
lsp-refresh-interval 65000
spf-interval 5 50 200
prc-interval 5 50 200
lsp-gen-interval 5 5 200
log-adjacency-changes
nsf ietf
segment-routing mpls
fast-reroute per-prefix level-1 all - configures the local LFA
fast-reroute per-prefix level-2 all
fast-reroute remote-lfa level-1 mpls-ldp - enables rLFA (optional)
fast-reroute remote-lfa level-2 mpls-ldp
fast-reroute ti-lfa level-1 - enables TI-LFA
microloop avoidance rib-update-delay 10000
bfd all-interfaces

```

例2：優先度 100 のすべての ISIS レベル 2 インターフェイスで、TI-LFA node-protecting タイブレーカーを有効にします。その他のタイブレーカーはすべて無効になります。

```
router isis
fast-reroute per-prefix level-2 all
fast-reroute ti-lfa level-2
fast-reroute tie-break level-2 node-protecting 100
```

例 3：すべての IS-IS レベル 2 インターフェイスで、優先度 100 の TI-LFA node-protecting タイブレーカーと、優先度 200 の TI-LFA SRLG 保護を有効にします。node-protecting タイブレーカーが設定されているため、他のすべてのタイブレーカーは無効になります。

```
router isis
fast-reroute per-prefix level-2 all
fast-reroute ti-lfa level-2
fast-reroute tie-break level-2 node-protecting 100
fast-reroute tie-break level-2 srlg-disjoint 200
```

例 4：Ethernet0/0 を除くすべての IS-IS レベル 2 インターフェイスで、優先度 100 の TI-LFA node-protecting タイブレーカーを有効にします。これらの IS-IS インターフェイスでは、他のすべてのタイブレーカーは無効になります。Ethernet0/0 は継承を上書きし、linecard-disjoint、lowest-backup-path-metric、srlg-disjoint を有効にしたタイブレーカーのデフォルトセットを使用します。

```
router isis
fast-reroute per-prefix level-2 all
fast-reroute ti-lfa level-2
fast-reroute tie-break level-2 node-protecting 100
!
interface ethernet0/0
ip router isis
isis fast-reroute tie-break level-2 default
```

例 5：Ethernet0/0 以外のすべての IS-IS インターフェイスで、デフォルトのタイブレーカーを使用して TI-LFA を有効にします。Ethernet0/0 で、優先度 100 の TI-LFA node-protecting を有効にし、他のすべてのタイブレーカーを無効にします。

```
router isis
fast-reroute per-prefix level-2 all
fast-reroute ti-lfa level-2
!
interface ethernet0/0
ip router isis
isis fast-reroute tie-break level-2 node-protecting 100
```

例 6：すべての IS-IS レベル 2 インターフェイスで、優先度 200 の TI-LFA node-protecting タイブレーカーおよび優先度 100 の linecard-disjoint tie-breaker タイブレーカーを有効にします。その他のタイブレーカーはすべて無効になります。

```
router isis
fast-reroute per-prefix level-2 all
fast-reroute ti-lfa level-2
fast-reroute tie-break level-2 linecard-disjoint 100
fast-reroute tie-break level-2 node-protecting 200
```

タイブレーカーの確認

インターフェイスで有効になっているタイブレーカーを表示するには、次のコマンドを使用します。

```
show running all | section interface interface-name
```

ルータ モードで有効になっているタイブレーカーを表示するには、次のコマンドを使用します。

```
show running all | section router isis
```

プライマリおよび修復パスの確認

この例では、10.1.1.1 は保護ネイバーであり、10.4.4.4 は保護リンク上のネイバーです。

```
Router#
show ip cef 10.1.1.1
10.1.1.1/32
  nexthop 10.1.1.1 GigabitEthernet0/2/0 label [explicit-null|explicit-null]() - slot 2
is primary interface
  repair: attached-nexthop 10.24.0.2 TenGigabitEthernet0/3/0 - slot 3 is repair interface

  nexthop 10.24.0.2 TenGigabitEthernet0/3/0 label [explicit-null|explicit-null]()
  repair: attached-nexthop 10.1.1.1 GigabitEthernet0/2/0
Router#
show ip cef 10.4.4.4
10.4.4.4/32
  nexthop 10.4.4.4 GigabitEthernet0/2/3 label [explicit-null|16004]() - slot 2 is primary interface
  repair: attached-nexthop 10.5.5.5 MPLS-SR-Tunnel2
Router# show ip cef 10.4.4.4 int
10.4.4.4/32, epoch 3, RIB[I], refcnt 6, per-destination sharing
sources: RIB, Adj, LTE
feature space:
  IPRM: 0x00028000
  Broker: linked, distributed at 4th priority
  LFD: 10.4.4.4/32 2 local labels
  dflt local label info: global/877 [0x3]
  sr local label info: global/16004 [0x1B]
  contains path extension list
  dflt disposition chain 0x46654200
  label implicit-null
  FRR Primary
    <primary: IP adj out of GigabitEthernet0/2/3, addr 10.4.4.4>
  dflt label switch chain 0x46654268
  label implicit-null
  TAG adj out of GigabitEthernet0/2/3, addr 10.4.4.4
  sr disposition chain 0x46654880
  label explicit-null
  FRR Primary
    <primary: TAG adj out of GigabitEthernet0/2/3, addr 10.4.4.4>
  sr label switch chain 0x46654880
  label explicit-null
  FRR Primary
    <primary: TAG adj out of GigabitEthernet0/2/3, addr 10.4.4.4>
subblocks:
  Adj source: IP adj out of GigabitEthernet0/2/3, addr 10.4.4.4 464C6620
  Dependent covered prefix type adjfib, cover 10.0.0.0/0
```

```

ifnums:
  GigabitEthernet0/2/3(11): 10.4.4.4
  MPLS-SR-Tunnel2(1022)
  path list 3B1FC930, 15 locks, per-destination, flags 0x4D [shble, hvsh, rif, hwcn]
    path 3C04D5E0, share 1/1, type attached nexthop, for IPv4, flags [has-rpr]
      MPLS short path extensions: [rib | lblmrg | srlbl] MOI flags = 0x21 label
explicit-null
  nexthop 10.4.4.4 GigabitEthernet0/2/3 label [explicit-null|16004](), IP adj out
of GigabitEthernet0/2/3, addr 10.4.4.4 464C6620
  repair: attached-nexthop 10.5.5.5 MPLS-SR-Tunnel2 (3C04D6B0)
    path 3C04D6B0, share 1/1, type attached nexthop, for IPv4, flags [rpr, rpr-only]
      MPLS short path extensions: [rib | lblmrg | srlbl] MOI flags = 0x1 label 16004
      nexthop 10.5.5.5 MPLS-SR-Tunnel2 label 16004(), repair, IP midchain out of
MPLS-SR-Tunnel2 46CE2440
  output chain:
    label [explicit-null|16004]()
    FRR Primary (0x3B209220)
    <primary: TAG adj out of GigabitEthernet0/2/3, addr 10.4.4.4 464C6480> - primary
path
  <repair: TAG midchain out of MPLS-SR-Tunnel2 46CE22A0
    label 16()
    label 16003()
    TAG adj out of TenGigabitEthernet0/3/0, addr 10.24.0.2 46CE25E0> - repair
path

```

IS-IS セグメントルーティングの設定の確認

```

Router# show isis segment-routing
ISIS protocol is registered with MFI
ISIS MFI Client ID:0x63
Tag Null - Segment-Routing:
  SR State:SR_ENABLED
  Number of SRGB:1
  SRGB Start:14000, Range:1001, srgb_handle:0xE0934788, srgb_state: created
  Address-family IPv4 unicast SR is configured
  Operational state: Enabled

```

コマンドでキーワード **global-block** を指定すると、SRGB と、LSP の範囲を表示します。

```

Router# show isis segment-routing global-block
IS-IS Level-1 Segment-routing Global Blocks:
System ID          SRGB Base      SRGB Range
nevada             20000          4001
arizona            * 16000         1000
utah               40000          8000

```

show isis segment-routing prefix-sid-map コマンドでキーワード **advertise** を指定すると、ルータがアドバタイズするプレフィックス SID マップを表示します。

```

Router# show isis segment-routing prefix-sid-map adv
IS-IS Level-1 advertise prefix-sid maps:
Prefix             SID Index      Range          Flags
10.16.16.16/32    101            1              Attached
10.16.16.17/32    102            1              Attached

```

show isis segment-routing prefix-sid-map コマンドでキーワード **receive** を指定すると、ルータが受信するプレフィックス SID マップを表示します。

```
Router #sh isis segment-routing prefix-sid-map receive
IS-IS Level-1 receive prefix-sid maps:
Host          Prefix          SID Index  Range      Flags
utah          10.16.16.16/32  101       1          Attached
              10.16.16.17/32  102       1          Attached
```

LSPで見つかった、マッピングサーバーコンポーネントに渡される接続SIDを表示するには、**show isis segment-routing connected-sid** コマンドを使用します。

```
Router# show isis segment-routing connected-sid
IS-IS Level-1 connected-sids
Host          Prefix          SID Index  Range      Flags
nevada        * 10.1.1.2/32   1002      1          Attached
              10.2.2.2/32    20        1          Attached
              10.1.1.10/32   10        1          Attached
colorado      10.1.1.3/32    33        1          Attached
              10.1.1.6/32    6         1          Attached
IS-IS Level-2 connected-sids
Host          Prefix          SID Index  Range      Flags
```

IS-IS トポロジに依存しないループフリー代替トンネルの確認

```
Router# show isis fast-reroute ti-lfa tunnel
Fast-Reroute TI-LFA Tunnels:
Tunnel  Interface  Next Hop      End Point      Label      End Point Host
MP1     Et1/0      10.30.1.4    10.1.1.2      41002     nevada
MP2     Et0/0      10.19.1.6    10.1.1.6      60006     colorado
              10.1.1.2    16         nevada
MP3     Et0/0      10.19.1.6    10.1.1.6      60006     colorado
              10.1.1.2    16         nevada
              10.1.1.5    70005     wyoming
```

トポロジに依存しないループフリー代替構成によるセグメントルーティングトラフィックエンジニアリングの確認

```
Router# show mpls traffic-eng tunnels tunnell1
Name: PE1 (Tunnell1) Destination: 10.6.6.6
Status:
  Admin: up      Oper: up      Path: valid      Signalling: connected
  path option 10, (SEGMENT-ROUTING) type explicit IP_PATH (Basis for Setup)
Config Parameters:
  Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  Path Selection:
  Protection: any (default)
  Path-invalidation timeout: 45000 msec (default), Action: Tear
  AutoRoute: enabled LockDown: disabled Loadshare: 0 [0] bw-based
  auto-bw: disabled
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
History:
  Tunnel:
  Time since created: 4 hours, 25 minutes
```

```

    Time since path change: 4 hours, 21 minutes
    Number of LSP IDs (Tun_Instances) used: 37
    Current LSP: [ID: 37]
    Uptime: 4 hours, 21 minutes
    Tun_Instance: 37
    Segment-Routing Path Info (isis level-1)
    Segment0[Node]: 10.4.4.4, Label: 16014
    Segment1[Node]: 10.5.5.5, Label: 16015
    Segment2[Node]: 10.6.6.6, Label: 16016
Router# show isis fast-reroute ti-lfa tunnel

Tag 1:
Fast-Reroute TI-LFA Tunnels:
Tunnel Interface Next Hop          End Point      Label      End Point Host
MP1      Gi2      192.168.1.2    10.6.6.6      16016      SR_R6
MP2      Gi3      192.168.2.2    10.6.6.6      16016      SR_R6
Router# show frr-manager client client-name ISIS interfaces detail
TunnelI/F : MP1
Type : SR
Next-hop : 192.168.1.2
End-point : 10.6.6.6
OutI/F : Gi2
Adjacency State : 1
Prefix0 : 10.6.6.6(Label : 16016)
TunnelI/F : MP2
Type : SR
Next-hop : 192.168.2.2
End-point : 10.6.6.6
OutI/F : Gi3
Adjacency State : 1
Prefix0 : 10.6.6.6(Label : 16016)
Router# show ip cef 10.6.6.6 internal

10.6.6.6/32, epoch 2, RIB[I], refcnt 6, per-destination sharing
sources: RIB, LTE
feature space:
  IPRM: 0x00028000
  Broker: linked, distributed at 1st priority
  LFD: 10.6.6.6/32 1 local label
  sr local label info: global/16016 [0x1A]
  contains path extension list
  sr disposition chain 0x7FC6B0BF2AF0
    label implicit-null
    IP midchain out of Tunnel1
    label 16016
    FRR Primary
    <primary: label 16015
      TAG adj out of GigabitEthernet3, addr 192.168.2.2>
  sr label switch chain 0x7FC6B0BF2B88
    label implicit-null
    TAG midchain out of Tunnel1
    label 16016
    FRR Primary
    <primary: label 16015
      TAG adj out of GigabitEthernet3, addr 192.168.2.2>
ifnums:
  Tunnel1(13)
  path list 7FC6B0BDDDE0, 3 locks, per-destination, flags 0x49 [shble, rif, hwn]
  path 7FC7144D4300, share 1/1, type attached nexthop, for IPv4
  MPLS short path extensions: [rib | prfmfi | lblmrg | srlbl] MOI flags = 0x3 label
implicit-null
  nexthop 10.6.6.6 Tunnel1, IP midchain out of Tunnel1 7FC6B0BBB440
output chain:
  IP midchain out of Tunnel1 7FC6B0BBB440

```

```

label [16016|16016]
FRR Primary (0x7FC714515460)
  <primary: label 16015
    TAG adj out of GigabitEthernet3, addr 192.168.2.2 7FC6B0BBB630>
  <repair: label 16015
    label 16014
    TAG midchain out of MPLS-SR-Tunnell 7FC6B0BBAA90
    label 16016
    TAG adj out of GigabitEthernet2, addr 192.168.1.2 7FC6B0BBBA10>

```



Note TI-LFA を使用して 50 ミリ秒未満のトラフィック保護を保証するには、ダイナミック パス オプションを指定した SR-TE でバックアップ隣接関係 SID を使用する必要があります。

ダイナミック パス オプションを指定して SR-TE を作成するには、トポロジ内のすべてのルータで次の設定を使用します。

```

router isis 1
fast-reroute per-prefix level-1 all

```

トンネルのヘッドエンドルータ：

```

interface Tunnell
ip unnumbered Loopback1
tunnel mode mpls traffic-eng
tunnel destination 10.6.6.6
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 1 dynamic segment-routing
tunnel mpls traffic-eng path-selection segment-routing adjacency protected

```



CHAPTER 5

IS-IS のセグメントルーティングトラフィックエンジニアリング

この章では、IS-IS を使用してセグメントルーティングトラフィックエンジニアリング (SR-TE) を導入する方法について、次のセクションに分けて説明します。

- IS-IS によるセグメントルーティングトラフィックエンジニアリングに関する機能情報 (45 ページ)
- IS-IS によるセグメントルーティングトラフィックエンジニアリングに関する制約事項, on page 46
- IS-IS によるセグメントルーティングトラフィックエンジニアリングに関する情報 (46 ページ)
- IS-IS によるセグメントルーティングトラフィックエンジニアリングの設定方法 (54 ページ)

IS-IS によるセグメントルーティングトラフィックエンジニアリングに関する機能情報

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、<https://cfnnng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

表 3: IS-IS によるセグメントルーティングトラフィック エンジニアリングに関する機能情報

機能名	リリース	機能情報
IS-IS によるセグメントルーティングトラフィックエンジニアリング	Cisco IOS XE Amsterdam 17.3.2	次のコマンドが導入または変更されました。 <ul style="list-style-type: none"> • <code>mpls traffic-eng nsr</code> • <code>show mpls traffic-eng tunnels tunnel1</code> • <code>show isis fast-reroute ti-lfa tunnel</code> • <code>show fr- manager client client-name ISIS interfaces detail</code> • <code>show ip cef 6.6.6.6 internal</code>

IS-IS によるセグメントルーティングトラフィック エンジニアリングに関する制約事項

- SR-TE は、ブロードキャストインターフェイスではサポートされていません。ポイントツーポイントインターフェイスのみサポートしています。
- 特定の時点で、TE に対して有効にする必要があるプロトコルのインスタンスは1つだけです。
- `verbatim` キーワードは、明示パスオプションが設定されたラベルスイッチドパス (LSP) だけで使用できます。
- `verbatim LSP` では、再最適化はサポートされていません。

IS-IS によるセグメントルーティングトラフィック エンジニアリングに関する情報

トラフィック エンジニアリング (TE) トンネルは、トンネルの入力とトンネルの宛先との間でインスタンス化された TE LSP のコンテナです。TE トンネルは、同じトンネルに関連付けられた1つ以上の SR-TE LSP をインスタンス化できます。SR-TE LSP パスが宛先ノードへの同じ IGP パスに必ずしも従うとは限りません。この場合、SR-TE パスは、プレフィックス SID のセット、またはノードの隣接関係 SID、あるいはその両方と、SR-TE LSP によってトラバースされるリンクによって指定することができます。

ヘッドエンドは、トンネルを通して伝送される発信パケットに、対応する MPLS ラベルスタックを課します。SR-TE LSP パスに沿った各通過ノードは、パケットが最終的な宛先に到達するまで、着信トップラベルを使用してネクストホップを選択し、ラベルをポップまたはスワップし、ラベルスタックの残りの部分を使用して次のノードにパケットを転送します。SR-TE LSP

パスを定義するホップまたはセグメントのセットは、演算子によってプロビジョニングされません。

SR-TE LSP のインスタンス化

トラフィック エンジニアリング (TE) トンネルは、1 つ以上のインスタンス化された TE LSP のコンテナです。SR-TE LSP は、TE トンネルのパスオプションで「segment-routing」を設定することによってインスタンス化されます。トンネルにマップされたトラフィックは、プライマリ SR-TE のインスタンス化 LSP を介して転送されます。

同じトンネルの下で複数のパスオプションを設定することもできます。各パスオプションには、プリファレンスインデックスまたはパスオプションインデックスが割り当てられていて、プライマリ LSP をインスタンス化するためのより有利なパスオプションを決定するために使用されます。パスオプションのプリファレンスインデックスが低いほど、パスオプションがより有利になります。同じ TE トンネルにおける他のあまり有利ではないパスオプションは、セカンダリパスオプションと見なされ、(たとえば、パス上の障害が原因で) 現在使用されているパスオプションが無効になった場合に使用されることがあります。



Note フォワーディング ステートは、プライマリ LSP に対してのみ維持されます。

SR-TE LSP の明示的ヌル

MPLS-TE トンネルのヘッドエンドは、スタックの最下部に明示的ヌルを課しません。penultimate hop popping (PHP) が SR プレフィックス SID に対して有効になっている場合、または隣接関係 SID が SR-TE LSP の最後のホップである場合、パケットはトランスポート ラベルなしでテールエンドに到着する可能性があります。ただし、場合によっては、パケットが明示的ヌルラベルでテールエンドに到着することが望ましいため、このような場合、ヘッドエンドはラベルスタックの最上部に明示的ヌル ラベルを課することになります。

SR-TE LSP のパス検証

SR-TE トンネル機能では、ヘッドエンドがトンネルパスの初期検証と、その後のトンネルテールエンドおよび通過セグメントの到達可能性の追跡を実行する必要があります。

SR-TE LSP パスのパス検証は、トポロジの変更または SR SID の更新について MPLS-TE で通知されるたびにトリガーされます。

SR-TE LSP 検証手順は、以下のチェックで構成されています。

トポロジ パスの検証

ヘッドエンドは、TE トポロジに対する接続性について SR-TE LSP のパスを検証します。MPLS-TE ヘッドエンドは、隣接関係 SID に対応するリンクが TE トポロジで接続されているかどうかをチェックします。

新たにインスタンス化された SR-TE LSP の場合、ヘッドエンドが SR-TE パスの任意のリンクで不連続性を検出すると、そのパスは無効であると見なされ、使用されません。有効なパスを持つ他のパスオプションがトンネルにある場合、これらのパスを使用してトンネル LSP をインスタンス化します。

既存のインスタンス化された SR-TE LSP がある TE トンネルでは、ヘッドエンドがリンク上の不連続性を検出すると、ヘッドエンドはそのリンクで障害が発生したと見なします。この場合、IP FRR などのローカル修復保護が有効になります。隣接関係がしばらく失われた後、IGP は保護された隣接関係ラベルと関連付けられた転送を維持し続けます。これにより、同じ障害の影響を受けない別のパスにトンネルを再ルーティングするのに十分な時間が、ヘッドエンドで可能になります。ヘッドエンドは、リンク障害を検出した後、有効なパスを持つ他の使用可能パスオプションにトンネルの再ルーティングを試みるために、トンネル無効化タイマーを開始します。

TE トンネルが、障害の影響を受けない検証済みの他のパスオプションを使用して設定されている場合、ヘッドエンドは、これらのパスオプションの1つを使用して、影響を受けないパスを使用してトンネルの新しいプライマリ LSP をインスタンス化することによって、トンネルを再ルーティングします。

同じトンネルの下に他の有効なパスオプションが存在しない場合、または TE トンネルが障害の影響を受けるパスオプションを1つだけで設定されている場合、ヘッドエンドは無効タイマーを開始し、その後トンネルの状態を「ダウン」にします。このアクションにより、影響を受ける SR-TE LSP 上を流れるトラフィックとともに Null ルートが送信されるのを回避でき、トンネルを通過するサービスはヘッドエンドで利用できる異なるパスを経由して再ルーティングできるようになります。無効化ドロップ構成は、トンネルを「アップ」のままにしますが、無効化タイマーが満了したときにトラフィックをドロップします。

エリア内 SR-TE LSP では、ヘッドエンドは LSP パス上で完全な可視性を持ち、最終的な LSP 宛先へのパスを検証します。ただし、エリア間 LSP の場合、ヘッドエンドには LSP パスに対する部分的な可視性があります（最初の ABR までのみ）。この場合、ヘッドエンドは、入力から最初の ABR へのパスのみを検証できます。最初の ABR ノードを超える LSP に沿った障害は、ヘッドエンドからは見えず、LSP を介した BFD など、そのような障害を検出するその他のメカニズムが想定されます。

SR SID の検証

SR-TE LSP の SID ホップは TE トンネルの SR-TE LSP を介して運ばれる発信パケットに課される発信 MPLS ラベル スタックを決定するために使用されます。グローバルおよびローカルの隣接関係 SID のデータベースは、IGP から受信した情報から取り込まれ、MPLS-TE で維持されます。MPLS TE データベースで利用できない SID を使用すると、明示的パスを使用するパスオプションが無効になります。この場合、パスオプションは、SR TE LSP のインスタンス化には使用されません。また、MPLS の SID データベースで SID を取り消す、追加する、または変更すると、MPLS-TE ヘッドエンドは、SR パスオプション（使用中またはセカンダリ）を持つすべてのトンネルを確認し、適切な処理を呼び出します。

LSP 出力インターフェイス

SR-TE LSP が最初のパス ホップの隣接関係の SID を使用するとき、TE は隣接関係 SID および SR-TE LSP が出力するノードに関連付けられているインターフェイス状態および IGP 隣接関係

状態を監視します。インターフェイスまたは隣接関係がダウンした場合、TE は SR-TE LSP パスで障害が発生したと仮定し、前のセクションで説明したのと同じリアクティブアクションを実行できます。



Note SR-TE LSP が最初のホップのプレフィックス SID を使用するとき、TE はトンネルが出力するインターフェイスを直接推測できません。TE は、プレフィックスの IP 到達可能性情報に基づいて、最初のホップへの接続が維持されるかどうかを判断します。

IP 到達可能性の検証

MPLS-TE では、SR パスを有効と宣言する前に、プレフィックス SID に対応するノードが IP 到達可能であることを検証します。MPLS-TE は、SR-TE LSP パスの隣接関係またはプレフィックス SID に対応する IP プレフィックスのパス変更を検出します。リンクまたはノードの障害が原因で、特定の SID をアナウンスするノードが IP の到達可能性を失う場合、MPLS-TE はパス変更（パスなし）の通知を受けます。MPLS-TE は、現在の SR-TE LSP パスを無効にすることによって反応し、もしあれば有効なパスを持つ他のパスオプションを使用して新しい SR-TE LSP をインスタンス化する場合があります。



Note IP-FRR は（SR-TE LSP パスに沿ったプレフィックス SID の失敗など）SR-TE LSP が通過しているノードの障害に対する保護を提供しないため、ヘッドエンドは、トンネル状態を「ダウン」に設定することによってプレフィックス SID ノードの IP ルートの到達可能性の損失にすぐに反応し、影響を受けるトンネルに対して有効なパスを持つパスオプションが他にない場合は、トンネル転送エントリを削除します。

トンネルパス アフィニティの検証

トンネルパスのアフィニティは、トンネルインターフェイスで `tunnel mpls traffic-eng affinity` コマンドを使用して指定することができます。

ヘッドエンドは、指定された SR パスが設定されたアフィニティに準拠していることを検証します。これにより、SR パスの各セグメントのパスは、指定された制約に照らして検証される必要があります。パスの少なくとも1つのセグメントが設定されているアフィニティを満たさない場合、そのパスは設定されているアフィニティ制約に対して無効として宣言されます。

トンネルパス リソース回避の検証

SR-TE トンネルパケットの通過から除外されたことを検証するアドレスのセットを指定できます。これを実現するために、ヘッドエンドはセグメントごとの検証チェックを実行し、指定されたノード、プレフィックス、またはリンクアドレスが SR パスのトンネルから実際に除外されていることを検証します。以下のコマンドを使用して、トンネルリソース回避チェックをパスごとに有効にすることができます。除外されるアドレスのリストが定義され、リストの名前がパスオプションで参照されます。

```
interface tunnel100
```

```
tunnel mpls traffic-eng path-option 1 explicit name EXCLUDE segment-routing
ip explicit-path name EXCLUDE enable
exclude-address 192.168.0.2
exclude-address 192.168.0.4
exclude-address 192.168.0.3
!
```

Verbatim パス サポート

通常、MPLS TE LSP を使用する場合は、ネットワーク内のすべてのノードで TE の IGP 拡張がサポートされていて、TE が認識されるように設定されている必要があります。ただし、TE の IGP 拡張をサポートしないが、TE の RSVP 拡張はサポートするノードを通過する TE LSP を構築する機能を必要とするネットワーク管理者もいます。Verbatim LSP は、ネットワーク内のすべてまたは一部の中間ノードで TE の IGP 拡張がサポートされていない場合に役立ちます。

この機能をイネーブルにすると、IP 明示パスの TE トポロジデータベースに対するチェックは行われません。TE トポロジデータベースの検証が行われなため、IP 明示パス情報を持つ Path メッセージは、IP ルーティング用の Shortest Path First (SPF) アルゴリズムを使用してルーティングされます。

SR-TE トラフィックのロード バランシング

SR-TE トンネルは、次のロードバランシング オプションをサポートします。

ポートチャネル TE リンクのロードバランシング

ポートチャネルインターフェイスは SR-TE LSP トラフィックを運びます。このトラフィック負荷は、ポートチャネルメンバーリンクと、SR-TE LSP の先頭または中間のバンドルインターフェイス上でバランスをとります。

単一トンネルでのロードバランシング

同じコストのマルチパスプロトコル (ECMP) を使用している間、特定のプレフィックス SID へのパスが複数のネクストホップを指す場合があります。さらに、SR-TE LSP パスが、ECMP を持つ 1 つ以上のプレフィックス SID を通過する場合、SR-TE LSP トラフィック負荷は、SR-TE LSP パスに沿ってヘッドエンドまたは中間点の通過したノードから通過した各プレフィックス SID の ECMP パスでバランスをとります。

複数トンネルでのロードバランシング

スタティック ルートを設定するか、同じ宛先に対して複数の並列トンネルを自動ルートアナウンスをすると、複数の TE トンネルを特定の IP プレフィックスへのルーティングのためのネクストホップパスとして使用することができます。このような場合、トンネルはトラフィック負荷を均等に共有するか、複数の並列トンネル上でトラフィックをロードバランシングします。トンネルヘッドエンドでトンネルごとの明示的な設定を使用して不等なロードバランシング (UELB) を許可することも可能です。この場合、トンネルのロードシェアは MPLS-TE からフォワーディングプレーンに渡されます。

トンネルのロードシェア機能は、SR-TE LSP をインスタンス化する TE トンネルで引き続き機能します。

SR-TE トンネルの再最適化

TE トンネルの再最適化は、ヘッドエンドが、現在使用しているパスよりも最適な利用できるパスがあると判断した場合に発生します。たとえば、SR-TE LSP パスに沿って障害が発生した場合、ヘッドエンドは再最適化をトリガーすることによって、より最適なパスを検出し復帰することができます。

SR-TE LSP をインスタンス化するトンネルは、トンネルを通して運ばれるトラフィックに影響を与えずに再最適化できます。

再最適化は、次の理由で発生します。

- プライマリ SR-TE LSP 明示的のパスによって使用される明示的なパスホップが変更された。
- トポロジパスが切断されているか、明示的のパスで指定されている SID データベースで SID が見つからないため、現在使用しているパスオプションは無効であるとヘッドエンドが判断した。
- より有利なパスオプション（より低いインデックス）が利用可能になった。

ヘッドエンドは、SR-TE LSP が通過する保護された SR 隣接関係 SID で障害を検出すると、無効化タイマーを開始します。タイマーが期限切れになり、別のパスで再ルーティングできないために失敗したパスをヘッドエンドがまだ使用している場合、Null のルートがトラフィックとともに送信されないように、トンネル状態が「ダウン」になります。トンネルがダウンすると、トンネル上のサービスは、異なるパスを使用するために収束します。

次に手動の再最適化の例で出力されるサンプルを示します。この例では、パスオプションが **10** から **20** に変更されます。

```
Router# mpls traffic-eng reoptimize tunnel 1 path-option 20
The targeted path-option is not in lock down mode. Continue? [no]: yes
Router# show mpls traffic-eng tunnels tunnel1
Name: R1_t1 (Tunnel1) Destination: 10.6.6.6
Status:
  Admin: up      Oper: up      Path: valid      Signalling: connected
  path option 20, (SEGMENT-ROUTING) type explicit IP_PATH (Basis for Setup)
  path option 10, (SEGMENT-ROUTING) type dynamic
Config Parameters:
  Bandwidth: 0 kbps (Global) Priority: 6 6 Affinity: 0x0/0xFFFF
  Metric Type: IGP (interface)
  Path Selection:
    Protection: any (default)
  Path-invalidation timeout: 45000 msec (default), Action: Tear
  AutoRoute: enabled LockDown: disabled Loadshare: 10 [200000000]
  auto-bw: disabled
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: explicit path option 20 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
History:
  Tunnel:
    Time since created: 6 days, 19 hours, 9 minutes
    Time since path change: 14 seconds
    Number of LSP IDs (Tun_Instances) used: 1819
  Current LSP: [ID: 1819]
    Uptime: 17 seconds
    Selection: reoptimization
```

```

Prior LSP: [ID: 1818]
  ID: path option unknown
  Removal Trigger: reoptimization completed
Tun_Instance: 1819
Segment-Routing Path Info (isis level-1)
  Segment0[Node]: 10.4.4.4, Label: 114
  Segment1[Node]: 10.5.5.5, Label: 115
  Segment2[Node]: 10.6.6.6, Label: 116

```

ロックダウンオプション付き SR-TE

lockdown オプションは、SR-TE がより良いパスに再最適化することを防ぎます。ただし、新しいパスの存在をシグナリングすることは防げません。

```

interface Tunnell
ip unnumbered Loopback1
tunnel mode mpls traffic-eng
tunnel destination 10.6.6.6
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 6 6
tunnel mpls traffic-eng path-option 10 segment-routing lockdown
tunnel mpls traffic-eng path-selection metric igp
tunnel mpls traffic-eng load-share 10 (Tunnell) Destination:
10.6.6.6
Status:
  Admin: up      Oper: up      Path: valid      Signalling: connected
  path option 10, (LOCKDOWN) type segment-routing (Basis for Setup)
Config Parameters:
  Bandwidth: 0      kbps (Global)  Priority: 6 6  Affinity: 0x0/0xFFFF
  Metric Type: IGP (interface)
  Path Selection:
    Protection: any (default)
    Path-invalidation timeout: 45000 msec (default), Action: Tear
    AutoRoute: enabled LockDown: enabled Loadshare: 10 [200000000]
    auto-bw: disabled
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: segment-routing path option 10 is active
  BandwidthOverride: disabled LockDown: enabled Verbatim: disabled
History:
  Tunnel:
    Time since created: 6 days, 19 hours, 22 minutes
    Time since path change: 1 minutes, 26 seconds
    Number of LSP IDs (Tun_Instances) used: 1822
  Current LSP: [ID: 1822]
    Uptime: 1 minutes, 26 seconds
    Selection: reoptimization
  Prior LSP: [ID: 1821]
    ID: path option unknown
    Removal Trigger: configuration changed
  Tun_Instance: 1822
  Segment-Routing Path Info (isis level-1)
    Segment0[Node]: 10.6.6.6, Label: 116

```

SR-TE トンネル保護

SR TE トンネルの保護は、次のいずれかの代替手段で行うことができます。

IP-FRR ローカル修復保護

SR-TE LSP ヘッドエンドまたはミッドポイント ノードでは、IP-FRR はプレフィックス SID または隣接関係 SID ラベルのためのバックアップ保護パスを計算し、プログラムするのに使用されます。

IP-FRR を使用すると、バックアップ修復パスは、リンクまたはノードの障害が発生する前に IGP によって事前に計算されプログラムされます。リンクが失敗すると、TE トポロジからの即時の取り消し（リンクアダプタイズメントの取り消し）がトリガーされます。これにより、ヘッドエンドは、失敗した隣接関係 SID を通過する SR-TE LSP の障害を検出することができます。

保護された隣接関係 SID が失敗した場合、失敗した隣接関係 SID ラベルとそれに関連する転送は、すべての SR-TE トンネルのヘッドエンドが障害を検出して対応できるように、指定した時間（5～15分）機能し続けます。隣接関係 SID ラベルを使用するトラフィックは、バックアップ修復パスを変更するその後のトポロジ更新がある場合でも、FRR 保護され続けます。この場合、IGP は FRR がアクティブになっている間にバックアップ修復パスを更新し、新しく計算されたバックアップパス上のトラフィックを再ルーティングします。

保護されたプレフィックス SID のプライマリ パスが失敗すると、PLR はバックアップパスに経路を再ルーティングします。ヘッドエンドは障害に対してトランスペアレントなままであり、引き続き SR-TE LSP を有効なパスとして使用します。

IP-FRR は、リンク障害に対してのみ隣接関係およびプレフィックス SID を保護します。

トンネルパス保護

パス保護とは、単一の TE トンネルのプライマリ LSP の障害から保護するために、1つまたは複数のスタンバイ LSP をインスタンス化することです。

パス保護では、同じトンネルのプライマリパスオプションによってさまざまな障害のセカンダリパスを事前に計算し、事前プロビジョニングすることで、障害から保護します。この保護は、プライマリ LSP が通過するプレフィックス SID および隣接関係 SID を除外するパスを計算するか、またはプライマリ SR-TE LSP パスの SRLG を除外するパスを計算することによって実現します。

プライマリ SR-TE LSP に障害が発生した場合、トンネルには少なくとも1台のスタンバイ SR-TE LSP が使用されます。複数のセカンダリパスオプションをスタンバイ SR-TE LSP パスとして使用するように設定できます。

アンナンバード サポート

アンナンバードリンクの IS-IS の説明には、リモート インターフェイス ID 情報は含まれません。アンナンバードリンクのリモートインターフェイス ID には、SR-TE トンネルの一部としてアンナンバードリンクを含める必要があります。

IS-IS によるセグメントルーティングトラフィック エンジニアリングの設定方法

次の手順を実行して、IS-IS でのセグメントルーティングトラフィック エンジニアリング (SR-TE) を設定します。

TE トンネルのパスオプションの設定

稼働中の SR トンネルのパスオプションタイプが SR から非 SR (たとえば **dynamic**) に変更されると、トンネルの既存の転送エントリが削除されます。

セグメントルーティングは、既存のセカンダリまたは使用中のパスオプションで有効または無効にすることができます。トンネルでシグナリングされた **RSVP-TE** の明示的パスオプションが使用され、そのトンネルでセグメントルーティングが有効になっている場合、**RSVP-TE LSP** は切断され、**SR-TE LSP** が同じパスオプションを使用してインスタンス化されます。逆に、プライマリ LSP によって使用されているパスオプションでセグメントルーティングが無効になっている場合、トンネルは断続的にダウンし、新しい **RSVP-TE LSP** は同じ明示的パスを使用してシグナリングされます。

セグメントルーティングパスオプションがセカンダリパスオプションで有効になっている (すなわち、トンネルのプライマリ LSP によって使用されていない) 場合、新しく指定された **SR-TE LSP** パスオプションが有効で、トンネルのプライマリ LSP に使用するのがより有利であるかどうかを評価するためにトンネルがチェックされます。

```
Device(config)# interface tunnel 100
Device(config-if)# tunnel mpls traffic-eng path-option 1 explicit name foo segment-routing
Device(config-if)# tunnel mpls traffic-eng path-option 2 dynamic segment-routing
Device(config-if)# tunnel mpls traffic-eng path-option 3 segment-routing
```

SR 明示パス ホップの設定

SR-TE では次の明示的パスホップがサポートされています。

- IP アドレス
- MPLS ラベル
- IP アドレスと MPLS ラベルの混在

エリア内 LSP では、明示的パスを IP アドレスのリストとして指定できます。

```
Device(config)# ip explicit-path name foo
Device(config-ip-expl-path)# index 10 next-address 10.1.1.1 node address
Device(config-ip-expl-path)# index 20 next-address 10.12.12.2 link address
```



Note IP アンナンバードインターフェイスを使用する場合、ネクストホップアドレスを明示的パスのインデックスとして指定することはできません。これは、ノードアドレスまたはラベルである必要があります。

明示的パスは、セグメントルーティング SID として指定することもできます。

```
Device(config)# ip explicit-path name foo
Device(config-ip-expl-path)# index 10 next-label 20
```

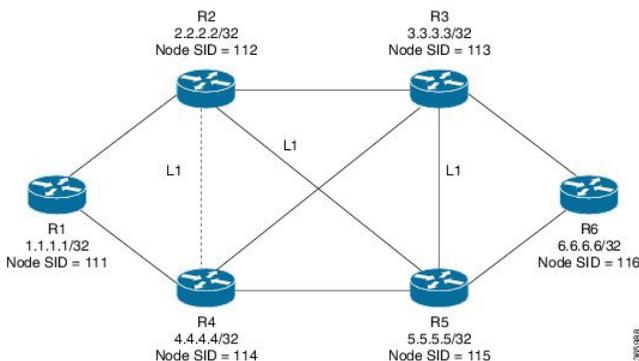
インターフェイスのアフィニティの設定

インターフェイスでアフィニティを設定するには、次の手順を実行します。

```
interface GigabitEthernet2
 ip address 192.168.2.1 255.255.255.0
 ip router isis 1
 negotiation auto
 mpls traffic-eng tunnels
 mpls traffic-eng attribute-flags 0x1
 isis network point-to-point
 ip rsvp bandwidth
```

使用例：セグメントルーティングトラフィック エンジニアリングの基本設定

SR-TE の構成を理解するには、次のトポロジを検討してください。



ヘッドエンド ルータで設定するには、R1 で次を実行します。

```
!
mpls traffic-eng tunnels
!
segment-routing mpls
connected-prefix-sid-map
 address-family ipv4
  10.1.1.1/32 index 111 range 1
```

```

    exit-address-family
  !
  set-attributes
    address-family ipv4
    sr-label-preferred
  exit-address-family
  !
  interface Loopback1
  ip address 10.1.1.1 255.255.255.255
  ip router isis 1
  !
  int gig0/0
  ip address 10.11.11.1 255.255.255.0
  ip router isis 1
  mpls traffic-eng tunnels
  isis network point-to-point
  !
  router isis 1
  net 49.0001.0010.0100.1001.00
  is-type level-1
  metric-style wide
  segment-routing mpls
  segment-routing prefix-sid-map advertise-local
  mpls traffic-eng router-id Loopback1
  mpls traffic-eng level-1
  !
end

```

SR-TE の明示的パス（ノードSIDベース）を有効にするには、R1 で次の CLI を有効にします。

```

Head end SR-TE configuration R1#
!
interface tunnel1
ip unnumbered Loopback1
tunnel mode mpls traffic-eng
tunnel destination 10.6.6.6
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 6 6
tunnel mpls traffic-eng path-option 10 explicit name Node_PATH segment-routing
!
ip explicit-path name Node_PATH
  next-label 16114
next-label 16115
next-label 16116

```

R1 上の SR-TE トンネル 1 の正常な動作を確認するには、次の CLI を有効にします。

```

Tunnel verification on (R1)# show mpls traffic-eng tun tun 1 detail
Name: R1_t1                               (Tunnel1) Destination: 10.6.6.6
  Status:
    Admin: up          Oper: up          Path: valid          Signalling: connected
    path option 10, (SEGMENT-ROUTING) type explicit Node_PATH (Basis for Setup)
  Config Parameters:
    Bandwidth: 0          kbps (Global) Priority: 6 6 Affinity: 0x0/0xFFFF
    Metric Type: IGP (interface)
  Verbatim: disabled
  Number of LSP IDs (Tun_Instances) used: 1815
    Current LSP: [ID: 1815]
    Uptime: 2 seconds
  Removal Trigger: configuration changed
    Segment-Routing Path Info (isis level-1)
    Segment0[Node]: 10.4.4.4, Label: 16114

```

```
Segment1[Node]: 10.5.5.5, Label: 16115
Segment2[Node]: 10.6.6.6, Label: 16116
```

テールエンド ルータで設定するには、R6 で次を実行します。

```
interface GigabitEthernet2
ip address 10.101.1.1 255.255.255.0
ip router isis 1
negotiation auto
mpls traffic-eng tunnels
router isis 1
net 49.0001.0060.0600.6006.00
 ispf level-1
 metric-style wide
 log-adjacency-changes
 segment-routing mpls

segment-routing prefix-sid-map advertise-local
mpls traffic-eng router-id Loopback1
mpls traffic-eng level-1
```

明示パス SR-TE トンネル 1

トンネル 1 を IP アドレスのみに基づいて考慮します。

```
ip explicit-path name IP_PATH1
next-address 10.2.2.2
next-address 10.3.3.3
next-address 10.6.6.6
!
interface Tunnel1
 ip unnumbered Loopback1
 tunnel mode mpls traffic-eng
 tunnel destination 10.6.6.6
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 6 6
 tunnel mpls traffic-eng path-option 10 explicit name IP_PATH1 segment-routing
 tunnel mpls traffic-eng path-selection metric igp
 tunnel mpls traffic-eng load-share 10
end
```

明示パス SR-TE トンネル 2

トンネル 2 をノードの SID に基づいて考慮します

```
ip explicit-path name IA_PATH
next-label 114
next-label 115
next-label 116
!
interface Tunnel2
 ip unnumbered Loopback1
 tunnel mode mpls traffic-eng
 tunnel destination 10.6.6.6
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 6 6
 tunnel mpls traffic-eng bandwidth 10000 class-type 1
 tunnel mpls traffic-eng path-option 10 explicit name IA_PATH segment-routing
 tunnel mpls traffic-eng path-selection metric igp
```

```
tunnel mpls traffic-eng load-share 10
end
```

明示パス SR-TE トンネル 3

トンネル 3 は IP アドレスとラベルの組み合わせに基づいていることを考慮します

```
ip explicit-path name MIXED_PATH enable
next-address 10.2.2.2
next-address 10.3.3.3
next-label 115
next-label 116
!
interface Tunnel3
ip unnumbered Loopback1
tunnel mode mpls traffic-eng
tunnel destination 10.6.6.6
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 6 6
tunnel mpls traffic-eng path-option 10 explicit name MIXED_PATH segment-routing
tunnel mpls traffic-eng path-selection metric igp
tunnel mpls traffic-eng load-share 10
```



Note パスが混在している場合、パスでノード SID を使用した後に IP ネクストホップを使用することはできません。次のパスは有効ではありません。

```
ip explicit-path name MIXED_PATH enable
next-label 115
next-label 116
next-address 10.2.2.2
```

動的パス SR-TE トンネル 4

トンネル 4is は隣接関係 SID に基づいていることを考慮します

```
interface Tunnel4
ip unnumbered Loopback1
tunnel mode mpls traffic-eng
tunnel destination 10.6.6.6
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 6 6
tunnel mpls traffic-eng bandwidth 10000 class-type 1
tunnel mpls traffic-eng path-option 10 dynamic segment-routing
tunnel mpls traffic-eng path-selection metric igp
tunnel mpls traffic-eng load-share 10
end
```

動的パス SR-TE トンネル 5

トンネル 5 はノード SID に基づいていることを考慮します

```
interface Tunnel5
ip unnumbered Loopback1
tunnel mode mpls traffic-eng
tunnel destination 10.6.6.6
```

```
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 6 6
tunnel mpls traffic-eng path-option 10 segment-routing
tunnel mpls traffic-eng path-selection metric igp
tunnel mpls traffic-eng load-share 10
```

SR-TE トンネルの構成の確認

`show mpls traffic-eng tunnels tunnel-number` コマンドを使用して、SR-TE トンネルの構成を確認します。

トンネル 1 の確認

```
Name: R1_t1                               (Tunnel1) Destination: 10.6.6.6
Status:
  Admin: up           Oper: up           Path: valid           Signalling: connected
  path option 10, (SEGMENT-ROUTING) type explicit IP_PATH (Basis for Setup)
Config Parameters:
  Bandwidth: 0        kbps (Global) Priority: 6 6 Affinity: 0x0/0xFFFF
  Metric Type: IGP (interface)
  Path Selection:
    Protection: any (default)
  Path-invalidation timeout: 45000 msec (default), Action: Tear
  AutoRoute: enabled LockDown: disabled Loadshare: 10 [200000000]
  auto-bw: disabled
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
History:
  Tunnel:
    Time since created: 6 days, 19 hours
    Time since path change: 2 seconds
    Number of LSP IDs (Tun_Instances) used: 1814
    Current LSP: [ID: 1814]
    Uptime: 2 seconds
    Selection: reoptimization
    Prior LSP: [ID: 1813]
    ID: path option unknown
    Removal Trigger: configuration changed
Tun_Instance: 1814
Segment-Routing Path Info (isis level-1)
  Segment0 [Node]: 10.4.4.4, Label: 114
  Segment1 [Node]: 10.5.5.5, Label: 115
  Segment2 [Node]: 10.6.6.6, Label: 116
```

トンネル 2 の確認

```
Name: R1_t2                               (Tunnel1) Destination: 10.6.6.6
Status:
  Admin: up           Oper: up           Path: valid           Signalling: connected
  path option 10, (SEGMENT-ROUTING) type explicit IA_PATH (Basis for Setup)
Config Parameters:
  Bandwidth: 0        kbps (Global) Priority: 6 6 Affinity: 0x0/0xFFFF
  Metric Type: IGP (interface)
  Path Selection:
    Protection: any (default)
  Path-invalidation timeout: 45000 msec (default), Action: Tear
```

```

AutoRoute: enabled LockDown: disabled Loadshare: 10 [200000000]
auto-bw: disabled
Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
State: explicit path option 10 is active
BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
History:
Tunnel:
Time since created: 6 days, 19 hours, 1 minutes
Time since path change: 1 seconds
Number of LSP IDs (Tun_Instances) used: 1815
Current LSP: [ID: 1815]
Uptime: 1 seconds
Prior LSP: [ID: 1814]
ID: path option unknown
Removal Trigger: configuration changed
Tun_Instance: 1815
Segment-Routing Path Info (isis level-1)
Segment0[ - ]: Label: 114
Segment1[ - ]: Label: 115
Segment2[ - ]: Label: 116

```

トンネル3の確認

```

Name: R1_t3 (Tunnell) Destination: 10.6.6.6
Status:
Admin: up Oper: up Path: valid Signalling: connected
path option 10, (SEGMENT-ROUTING) type explicit MIXED_PATH (Basis for Setup)
Config Parameters:
Bandwidth: 0 kbps (Global) Priority: 6 6 Affinity: 0x0/0xFFFF
Metric Type: IGP (interface)
Path Selection:
Protection: any (default)
Path-invalidation timeout: 45000 msec (default), Action: Tear
AutoRoute: enabled LockDown: disabled Loadshare: 10 [200000000]
auto-bw: disabled
Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
State: explicit path option 10 is active
BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
History:
Tunnel:
Time since created: 6 days, 19 hours, 2 minutes
Time since path change: 2 seconds
Number of LSP IDs (Tun_Instances) used: 1816
Current LSP: [ID: 1816]
Uptime: 2 seconds
Selection: reoptimization
Prior LSP: [ID: 1815]
ID: path option unknown
Removal Trigger: configuration changed
Tun_Instance: 1816
Segment-Routing Path Info (isis level-1)
Segment0[Node]: 10.2.2.2, Label: 112
Segment1[Node]: 10.3.3.3, Label: 113
Segment2[ - ]: Label: 115
Segment3[ - ]: Label: 116

```

トンネル4の確認

```

Name: R1_t4                                     (Tunnell) Destination: 10.6.6.6
Status:
  Admin: up           Oper: up           Path: valid           Signalling: connected
  path option 10, (SEGMENT-ROUTING) type dynamic (Basis for Setup, path weight 30)
Config Parameters:
  Bandwidth: 0           kbps (Global) Priority: 6 6   Affinity: 0x0/0xFFFF
  Metric Type: IGP (interface)
  Path Selection:
    Protection: any (default)
  Path-invalidation timeout: 45000 msec (default), Action: Tear
  AutoRoute: enabled LockDown: disabled Loadshare: 10 [200000000]
  auto-bw: disabled
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: dynamic path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
History:
  Tunnel:
    Time since created: 6 days, 19 hours
    Time since path change: 2 seconds
    Number of LSP IDs (Tun_Instances) used: 1813
  Current LSP: [ID: 1813]
    Uptime: 2 seconds
  Prior LSP: [ID: 1806]
    ID: path option unknown
    Removal Trigger: configuration changed
Tun_Instance: 1813
Segment-Routing Path Info (isis level-1)
  Segment0[Link]: 192.168.2.1 - 192.168.2.2, Label: 17
  Segment1[Link]: 192.168.4.2 - 192.168.4.1, Label: 25
  Segment2[Link]: 192.168.8.1 - 192.168.8.2, Label: 300

```

トンネル5の確認

```

Name: R1_t5                                     (Tunnell) Destination: 10.6.6.6
Status:
  Admin: up           Oper: up           Path: valid           Signalling: connected
  path option 10, type segment-routing (Basis for Setup)
Config Parameters:
  Bandwidth: 0           kbps (Global) Priority: 6 6   Affinity: 0x0/0xFFFF
  Metric Type: IGP (interface)
  Path Selection:
    Protection: any (default)
  Path-invalidation timeout: 45000 msec (default), Action: Tear
  AutoRoute: enabled LockDown: disabled Loadshare: 10 [200000000]
  auto-bw: disabled
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: segment-routing path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
History:
  Tunnel:
    Time since created: 6 days, 19 hours, 4 minutes
    Time since path change: 14 seconds
    Number of LSP IDs (Tun_Instances) used: 1817
  Current LSP: [ID: 1817]
    Uptime: 14 seconds
    Selection: reoptimization
  Prior LSP: [ID: 1816]

```

```

ID: path option unknown
Removal Trigger: configuration changed
Tun_Instance: 1817
Segment-Routing Path Info (isis level-1)
Segment0[Node]: 10.6.6.6, Label: 116

```

Verbatim パス サポートの確認

適切な動作と SR-TE トンネル状態を確認するには、次の CLI を使用します。

```

R6#sh mpl traffic-eng tunnels tunnel 4

Name: R6_t4                               (Tunnel4) Destination: 10.11.11.11
Status:
  Admin: up           Oper: up           Path: valid           Signalling: connected
  path option 1, (SEGMENT-ROUTING) type explicit (verbatim) multihop (Basis for Setup)

Config Parameters:
  Bandwidth: 0          kbps (Global) Priority: 7 7  Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  Path Selection:
    Protection: any (default)
  Path-selection Tiebreaker:
    Global: not set Tunnel Specific: not set Effective: min-fill (default)
  Hop Limit: disabled [ignore: Verbatim Path Option]
  Cost Limit: disabled
  Path-invalidation timeout: 10000 msec (default), Action: Tear
  AutoRoute: disabled LockDown: disabled Loadshare: 0 [0] bw-based
  auto-bw: disabled
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: explicit path option 1 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: enabled

History:
  Tunnel:
    Time since created: 16 minutes, 40 seconds
    Time since path change: 13 minutes, 6 seconds
    Number of LSP IDs (Tun_Instances) used: 13
  Current LSP: [ID: 13]
    Uptime: 13 minutes, 6 seconds
    Selection: reoptimization
  Prior LSP: [ID: 12]
    ID: path option unknown
    Removal Trigger: configuration changed (severe)
Tun_Instance: 13
Segment-Routing Path Info (IGP information is not used)
Segment0[First Hop]: 10.0.0.0, Label: 16003
Segment1[ - ]: Label: 16002
Segment2[ - ]: Label: 16001

```



第 6 章

OSPFv2 ノード SID のセグメントルーティング

この章では、セグメントルーティングが OSPFv2 ノード SID でどのように機能するかについて説明します。

- [OSPFv2 ノード SID のセグメントルーティングに関する機能情報 \(63 ページ\)](#)
- [OSPFv2 ノード SID のセグメントルーティングに関する情報 \(64 ページ\)](#)
- [OSPFv2 ノード SID のセグメントルーティングの設定方法 \(67 ページ\)](#)
- [OSPFv2 ノード SID のセグメントルーティングに関する追加情報 \(76 ページ\)](#)

OSPFv2 ノード SID のセグメントルーティングに関する機能情報

表 4: OSPFv2 ノード SID のセグメントルーティングに関する機能情報

機能名	リリース	機能情報
OSPF によるセグメントルーティング	Cisco IOS XE Amsterdam 17.3.2	セグメントルーティング OSPFv2 ノード SID 機能は、OSPF ネットワークでのセグメントルーティングのサポートを提供します。 次のコマンドが導入または変更されました。 connected-prefix-sid-map 、 show ip ospf 10 segment-routing 、 sr-label-preferred 、 ip ospf prefix-attributes n-flag-clear

OSPFv2 ノード SID のセグメントルーティングに関する情報

セグメントルーティングは、Open Shortest Path First (OSPF) プロトコルのいくつかの拡張機能に依存しています。ルーティングプロトコルインスタンスのセグメントルーティングを有効にするには、2つのレベルの構成が必要です。セグメントルーティングインフラストラクチャコンポーネントによって管理される最上位のセグメントルーティング構成では、セグメントルーティングが可能になり、一方、ルータ ospf レベルでのセグメントルーティング構成では、ospf インスタンスに対してセグメントルーティングが可能になります。セグメントルーティングの状態には、次の3つがあります。

- SR_NOT_CONFIGURED
- SR_DISABLED
- SR_ENABLED

IGP 下のセグメントルーティング構成は、SR の状態が SR_DISABLED または SR_ENABLED のいずれかである場合にのみ許可されます。SR_ENABLED 状態は、少なくとも予約済みの有効な SRGB 範囲にあることを示します。コマンドを使用して、ルータ設定サブモードで IGP のセグメントルーティングを有効にすることができます。ただし、IGP セグメントルーティングは、グローバル SR が設定された後にのみ有効になります。

SR_ENABLED は、SR を有効にするためにすべてのプロトコルに必要な状態ですが、プロトコルインスタンスの SR を有効にするには十分ではありません。その理由は、OSPF にセグメントルーティンググローバルブロック (SRGB) 情報に関する情報がまだないことです。SRGB に関する情報を受信する要求が正常に処理されると、OSPF SR の動作状態が有効になります。

セグメントルーティングでは、各ルータが、セグメントルーティングデータプレーン機能と、グローバル SID が割り当てられている場合にセグメントルーティングに使用される MPLS ラベル値の範囲をアダプタイズする必要があります。データプレーン機能とラベル範囲は、OSPF ルータ情報不透明 LSA に挿入される SR 機能サブ TLV を使用してアダプタイズされます。

OSPF SR 機能サブ TLV には、すべての予約済み SRGB 範囲が含まれます。ただし、シスコの実装でサポートされる SRGB 範囲は1つだけです。

リモートルータからのラベルスイッチドパスで受信されたプレフィックス SID

OSPF は、その不透明な拡張プレフィックス LSA 内の拡張プレフィックスサブ TLV を使用して、接続されたプレフィックスに関連付けられたプレフィックス SID を送信します。到達可能性のある LSA で受信したプレフィックス SID は、次の条件が満たされている場合にのみ、プレフィックス VPN ラベルごとの BGP ダウンロードと同じ方法でルーティング情報ベース (RIB) にダウンロードされます。

- トポロジとアドレスファミリに対してセグメントルーティングが有効。

- プレフィックス SID が有効。
- MFI へのローカル ラベルのバインドが成功している。



(注) 指定された SID 範囲に収まらない SID の場合、RIB の更新時にラベルは使用されません。SID が SID の範囲内には収まるが、ネクストホップのネイバー SID の範囲には収まらない場合は、そのパスに関連付けられているリモート ラベルはインストールされません。

セグメントルーティング隣接関係 SID アドバタイズメント

Cisco IOS XE リリース 3.17 では、OSPF によるセグメントルーティング隣接関係 SID のアドバタイズメントのサポートが有効です。隣接関係セグメント識別子 (Adj-SID) は、セグメントルーティングにおけるルータ隣接関係を表します。

セグメントルーティング対応ルータは、隣接関係ごとに Adj-SID を割り当てることができ、この SID を拡張不透明リンク LSA で伝送するように Adj-SID サブ TLV が定義されます。

OSPF は、OSPF 隣接関係が 2 つの方法または完全な状態にある場合、各 OSPF ネイバーに隣接関係 SID を割り当てます。OSPF は、セグメントルーティングが有効になっている場合にのみ隣接関係 SID を割り当てます。隣接関係 SID のラベルは、システムによって動的に割り当てられます。これにより、ローカルでしか有効でないため、設定ミスの可能性がなくなります。

複数の隣接関係 SID

Cisco IOS XE リリース 16.3 では、複数の隣接関係 SID がサポートされています。OSPF の隣接関係ごとに、OSPF は拡張リンク LSA で伝送される隣接関係 SID、非保護および保護された Adj-SID を割り当てます。保護された隣接関係 SID (またはバックアップ Adj-SID) は、ルータで FRR が有効になっている場合のみ、また SR がシステムで有効になっているインターフェイスでのみ、割り当てられてアドバタイズされます。FRR または SR が無効になっている場合、保護された Adj-SID は解放されます。

フォワーディングプレーンでの保護された adj-SID の永続化はサポートされます。プライマリリンクがダウンしている場合、OSPF は、遅延タイマー (30 秒) が期限切れになるまでバックアップ Adj-SID の解放を遅らせます。これにより、フォワーディングプレーンは、ルータがコンバージされるまで、バックアップパスを経由してトラフィックを転送し続けることができます。

割り当てられ、アドバタイズされたバックアップ Adj-SID は、`show ip ospf neighbor detail` および `show ip ospf segment-routing protected-adjacencies command` の出力で表示できます。

セグメントルーティング マッピング サーバー

セグメントルーティング マッピング サーバー (SRMS) を使用すると、プレフィックス SID マッピング ポリシー エントリの構成と保守を行うことができます。Cisco IOS XE リリース 3.17

では、IGP は SRMS のアクティブ ポリシーを使用して、フォワーディング プレーンのプログラミング時に SID 値を決定します。

SRMS は、ネットワークの SID/ラベル マッピング ポリシーにプレフィックスを提供します。一方、IGP は、プレフィックス SID/ラベル バインディング TLV を介して SID/ラベル マッピング ポリシーにプレフィックスをアドバタイズする役割を担います。

アクティブ ポリシー情報と変更は、アクティブ ポリシー情報を使用して転送情報を更新する IGP に通知されます。

接続されたプレフィックス SID

ルータが LSP にアドバタイズしたものと異なる SID を持つプレフィックスをインストールする場合、たとえば、複数のプロトコルまたは複数の IGP インスタンスが、異なる SID を持つ同じプレフィックスを SRMS にアナウンスしている場合、SRMS は競合を解決し、ローカル インスタンスと同じでない可能性がある競合に勝ったプレフィックスと SID をアナウンスします。その場合、IGP は、常にソース LSP から学習した内容をアドバタイズしますが、その LSP で学習したものと異なる可能性がある SID のインストールを試みます。これは IGP が別のプロトコルまたは別のプロトコルインスタンスから SID を再配布することを防ぐために行われます。

SRGB 範囲の変更

OSPF セグメント ルーティングが設定されている場合、OSPF は、OSPF SR の動作状態を有効にする前に SRGB とのインタラクションを要求する必要があります。SRGB 範囲が作成されていない場合、OSPF は有効になりません。

SRGB 変更イベントが発生した場合、OSPF は、そのサブブロック エントリで対応する変更を行います。また OSPF は、SR 機能サブ TLV で新しく作成または拡張された SRGB 範囲をアドバタイズし、プレフィックス SID サブ TLV アドバタイズメントを更新します。

インターフェイスでの MPLS 転送

セグメントルーティングがインターフェイスを使用する前に、MPLS 転送を有効にする必要があります。OSPF は、インターフェイスでの MPLS 転送を有効にする役割を担います。

セグメントルーティングが OSPF トポロジに対して有効になっている場合、または OSPF セグメントルーティングの動作状態が有効になっている場合、OSPF は、OSPF トポロジがアクティブである任意のインターフェイスに対して MPLS を有効にします。同様に、OSPF トポロジのセグメントルーティングが無効になっている場合、OSPF は、そのトポロジのすべてのインターフェイスで MPLS 転送を無効にします。

SID エントリの競合処理

SID エントリと関連付けられているプレフィックス エントリの間には競合がある場合は、次のいずれかの方法を使用して競合を解決します。

- システムが同じプレフィックスに対して2つの SID エントリを受信すると、より高いルータ ID で受信したプレフィックスが、プレフィックスに対応する SID として扱われます。プレフィックスは、上位のルータ ID によってアドバタイズされた SID エントリを使用してインストールされます。
- システムが、1つは OSPF プロトコル、他方は IS-IS プロトコルによる2つの SID エントリを受信すると、OSPF プロトコルによって受信した SID エントリが有効な SID として扱われます。プレフィックスは、OSPF プロトコルによって受信した SID エントリを使用してインストールされます。
- 2つのプレフィックスが同じ SID エントリでアドバタイズされると、上位のルータ ID によってアドバタイズされたプレフィックスが SID エントリを使用してインストールされ、もう一方のプレフィックスは SID エントリなしでインストールされます。

理想的な状況では、各プレフィックスに一意の SID エントリが割り当てられている必要があります。

OSPFv2 ノード SID のセグメントルーティングの設定方法

OSPFv2 ノード SID を使用してセグメントルーティングを設定するには、次の手順を実行します。

OSPF のセグメントルーティングの設定

始める前に

セグメントルーティングをサポートするように OSPF を設定する前に、最初にグローバル コンフィギュレーション モードでセグメントルーティング機能を設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **segment-routing mpls**
4. **connected-prefix-sid-map**
5. **address-family ipv4**
6. **10.1.1.1/32 index 100 range 1**
7. **exit-address-family**

手順の詳細

手順

	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。 <ul style="list-style-type: none">パスワードを入力します (要求された場合)。
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	segment-routing mpls 例 : Device(config-sr)# segment-routing mpls	mpls データプレーンを使用してセグメント機能を有効にします。
ステップ 4	connected-prefix-sid-map 例 : Device(config-srmppls)# connected-prefix-sid-map	ローカルプレフィックスと SID のアドレスファミリー固有のマッピングを設定できるサブモードを開始します。
ステップ 5	address-family ipv4 例 : Device(config-srmppls-conn)# address-family ipv4	IPv4 アドレスプレフィックスを指定します。
ステップ 6	10.1.1.1/32 index 100 range 1 例 : Device(config-srmppls-conn-af)# 10.1.1.1/32 100 range 1	SID 100 にアドレス 1.1.1.1/32 を関連付けます。
ステップ 7	exit-address-family 例 : Device(config-srmppls-conn-af)# exit-address-family	アドレスファミリーを終了します。

OSPF ネットワークでのセグメントルーティングの設定

始める前に

OSPF ネットワークでセグメントルーティングを設定する前に、ネットワーク上で OSPF を有効にする必要があります。

手順の概要

1. **router ospf 10**
2. **router-id <id>**
3. **segment-routing mpls**
4. **segment-routing area <area id> mpls**
5. **show ip ospf 10 segment-routing**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	router ospf 10 例： Device(config)# router ospf 10	OSPF モードを有効にします。
ステップ 2	router-id <id> 例： Device(config-router)# router-id 10.0.0.0	OSPF ルートを設定します。
ステップ 3	segment-routing mpls 例： Device(config-router)# segment-routing mpls	セグメントルーティング MPLS モードを設定します。
ステップ 4	segment-routing area <area id> mpls 例： Device(config-router) # segment-routing area 0 mpls	特定の領域にセグメントルーティング MPLS モードを設定します。
ステップ 5	show ip ospf 10 segment-routing 例： Device# show ip ospf 10 segment-routing	OSPF の下で SR を設定するための出力を示します。 次の例は、OSPF のセグメントルーティングに対する show ip ospf segment-routing state コマンドからの出力を表しています。

	コマンドまたはアクション	目的
		<pre> Device#show ip ospf 10 segment-routing OSPF Router with ID (10.0.0.1) (Process ID 10) Global segment-routing state: Enabled Segment Routing enabled: Area Topology name Forwarding ----- 0 Base MPLS 1 Base MPLS SR Attributes Prefer non-SR (LDP) Labels Do not advertise Explicit Null Local MPLS label block (SRGB): Range: 16000 - 23999 State: Created Registered with SR App, client handle: 3 Connected map notifications active (handle 0x4), bitmask 0x1 Active policy map notifications active (handle 0x5), bitmask 0xC Registered with MPLS, client-id: 100 Bind Retry timer not running Adj Label Bind Retry timer not running </pre>

OSPF のプレフィックス SID の設定

ここでは、各インターフェイスでプレフィックスセグメント ID (SID) を設定する方法について説明します。

始める前に

セグメントルーティングを対応するアドレスファミリでイネーブルにする必要があります。

手順の概要

1. enable
2. configure terminal
3. segment-routing mpls
4. connected-prefix-sid-map
5. address-family ipv4
6. 10.1.1.1/32 index 100 range 1
7. exit

手順の詳細

手順

	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	グローバル設定モードを開始します。
ステップ 3	segment-routing mpls 例： Device(config)# segment-routing mpls	セグメントルーティング MPLS モードを設定します。
ステップ 4	connected-prefix-sid-map 例： Device(config-srmppls)# connected-prefix-sid-map	ローカルプレフィックスと SID のアドレスファミリー固有のマッピングを設定できるサブモードを開始します。
ステップ 5	address-family ipv4 例： Device(config-srmppls-conn)# address-family ipv4	IPv4 アドレスファミリーを指定し、ルータアドレスファミリー コンフィギュレーションモードを開始します。
ステップ 6	10.1.1.1/32 index 100 range 1 例： Device(config-srmppls-conn-af)# 10.1.1.1/32 100 range 1	SID 100 にアドレス 1.1.1.1/32 を関連付けます。
ステップ 7	exit 例： Device(config-router)# exit	セグメントルーティングモードを終了し、コンフィギュレーション端末モードに戻ります。

プレフィックス属性 N-flag-clear の設定

OSPF は、その不透明 LSA に拡張プレフィックス TLV を介してプレフィックス SID をアドバタイズします。これはプレフィックスのフラグを伝送します。そのうちの1つはNフラグ（ノード）で、プレフィックスに沿って送信されたトラフィックが、LSAを発信するルータ宛てであ

ることを示します。このフラグは通常、ルータのループバックのホスト ルートをマークします。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface loopback3**
4. **ip ospf prefix-attributes n-flag-clear**

手順の詳細

手順

	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。 <ul style="list-style-type: none">• パスワードを入力します（要求された場合）。
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	interface loopback3 例： Device(config)# interface loopback3	インターフェイス ループバックを指定します。
ステップ 4	ip ospf prefix-attributes n-flag-clear 例： Device(config-if)# ip ospf prefix-attributes n-flag-clear	プレフィックス N-flag をクリアします。

OSPF での明示的ヌル属性の設定

penultimate-hop-popping (PHP) を無効にし、明示的ヌル ラベルを追加するには、explicit-null オプションを指定する必要があります。このオプションを指定すると、OSPF は、拡張プレフィックス SID TLV の E フラグをその LSA に設定します。

デフォルトでは、ループバック アドレスに関連付けられたプレフィックス SID をアドバタイズするときに、OSPF によって E-flag (明示的ヌルフラグ) と呼ばれるフラグが 0 に設定されます。このフラグを設定するには、明示的な設定を追加します。

手順の概要

1. **enable**
2. **configure terminal**
3. **segment-routing mpls**
4. **set-attributes**
5. **address-family ipv4**
6. **explicit-null**
7. **exit-address-family**

手順の詳細

手順

	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。 • パスワードを入力します (要求された場合)。
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	segment-routing mpls 例 : Device(config)# segment-routing mpls	セグメント ルーティング MPLS モードを設定します。
ステップ 4	set-attributes 例 : Device(config-srmppls)# set-attributes	属性を設定します。
ステップ 5	address-family ipv4 例 : Device(config-srmppls-attr)# address-family ipv4	IPv4 アドレス ファミリを指定し、ルータ アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 6	explicit-null 例 : Device(config-srmppls-attr-af)# explicit-null	明示的ヌルを指定します。

	コマンドまたはアクション	目的
ステップ 7	exit-address-family 例 : Device (config-srmppls-attr-af) # exit-address-family	アドレス ファミリを終了します。

OSPF のセグメントルーティング Label Distribution Protocol 優先順位の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **segment-routing mpls**
4. **set-attributes**
5. **address-family ipv4**
6. **sr-label-preferred**
7. **exit-address-family**

手順の詳細

手順

	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。 • パスワードを入力します (要求された場合)。
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	segment-routing mpls 例 : Device (config) # segment-routing mpls	セグメントルーティング MPLS モードを設定します。
ステップ 4	set-attributes 例 : Device (config-srmppls) # set-attributes	属性を設定します。

	コマンドまたはアクション	目的
ステップ 5	address-family ipv4 例 : Device(config-srmppls-attr)# address-family ipv4	IPv4 アドレス ファミリを指定し、ルータ アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 6	sr-label-preferred 例 : Device(config-srmppls-attr-af)# sr-label-preferred	LDP より優先される SR ラベルを指定します。
ステップ 7	exit-address-family 例 : Device(config-srmppls-attr-af)# exit-address-family	アドレス ファミリを終了します。

OSPF SRMS の設定

次のコマンドは、OSPF SRMS を有効にして、OSPF がローカル マッピング エントリをアドバタイズできるようにします。OSPF は、SRMS ライブラリにリモート エントリを送信しません。ただし、OSPF は、ローカルに設定されたマッピング エントリのみに基づいて計算される SRMS アクティブ ポリシーを使用します。

```
[no] segment-routing prefix-sid-map advertise-local
```

OSPF SRMS クライアントの設定

デフォルトでは、OSPF SRMS クライアント モードが有効になっています。OSPF は、常に SRMS に LSA を通じて受信したリモート プレフィックス SID マッピング エントリを送信します。SRMS アクティブ ポリシーは、ローカルおよびリモートの両方のマッピング エントリに基づいて計算されます。

次のコマンドを実行すると、プレフィックス SID マッピング クライアント機能が無効になります。これは受信側で設定されます。

```
segment-routing prefix-sid-map receive [disable]
```

OSPFv2 ノード SID のセグメントルーティングに関する追加情報

関連資料

関連項目	マニュアルタイトル
IP ルーティング ISIS コマンド	Cisco IOS IP ルーティング ISIS コマンド



第 7 章

OSPFv2 リンク保護のトポロジに依存しないループフリー代替高速再ルーティング

このドキュメントでは、TI-LFA（トポロジに依存しないループフリー代替）を使用した IP 高速再ルーティング機能（IP FRR）の OSPFv2 の実装について説明します。

- [OSPFv2 リンク保護のトポロジに依存しないループフリー代替高速再ルーティングの機能情報（77 ページ）](#)
- [トポロジに依存しないループフリー代替高速再ルーティングの制約事項（78 ページ）](#)
- [OSPFv2 リンク保護のトポロジに依存しないループフリー代替高速再ルーティングについて（79 ページ）](#)
- [トポロジに依存しないループフリー代替高速再ルーティングの設定方法（88 ページ）](#)
- [トポロジに依存しないループフリー代替高速再ルーティングのデバッグ（92 ページ）](#)
- [例：OSPFv2 リンク保護のトポロジに依存しないループフリー代替高速再ルーティング（93 ページ）](#)

OSPFv2 リンク保護のトポロジに依存しないループフリー代替高速再ルーティングの機能情報

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、<https://cfnnng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

表 5: OSPFv2 リンク保護のトポロジに依存しないループフリー代替高速再ルーティングの機能情報

機能名	リリース	機能情報
OSPFv2 リンク保護のトポロジに依存しないループフリー代替高速再ルーティング	Cisco IOS XE Amsterdam 17.3.2	<p>トポロジに依存しないループフリー代替 (TI-LFA) は、セグメントルーティングを使用して、他の高速再ルーティング技術が保護を提供できないトポロジでリンク、ノード、および共有リスク リンク グループ (SRLG) 保護を提供します。TI-LFA の目的は、リンク障害によるトポロジ変更後にルータがコンバージェンスする間に結果として生じるパケット損失を減らすことです。</p> <p>次のコマンドが導入または変更されました。</p> <p>fast-reroute per-prefix ti-lfa [area <area> [disable]], fast-reroute per-prefix tie-break node-protecting index <index>, fast-reroute per-prefix tie-break node-protecting required index <index>, fast-reroute per-prefix tie-break srlg index <index>, fast-reroute per-prefix tie-break srlg required index <index>, ip ospf fast-reroute per-prefix protection disable, ip ospf fast-reroute per-prefix candidate disable, show ip ospf fast-reroute ti-lfa tunnels.</p>

トポロジに依存しないループフリー代替高速再ルーティングの制約事項

- TI-LFA は OSPFv2 でのみサポートされています。
- TI-LFA トンネルは、ルータが SR をサポートし、プレフィックス SID を使用して設定されている場合だけ作成されます。プレフィックス (または) ノード SID は、接続された SID として設定 (または) SRMS (セグメントルーティング マッピング サーバー) を使用してアドバタイズできます。
- TI-LFA は、マルチポイント インターフェイスへの OSPF ポイントではサポートされません。
- TI-LFA は、マルチ トポロジルーティング (MTR) をサポートしません。
- TI-LFA は、仮想リンク、シャムリンク (または) TE トンネルを使用して修復パスを作成しません。
- TI-LFA トンネルは、トンネルが通過する必要があるノード (または) 修復ノードのセットを明示的に指定することによって構築され、プログラムされます。

OSPFv2 リンク保護のトポロジに依存しないループフリー代替高速再ルーティングについて

トポロジに依存しないループフリー代替 (TI-LFA) は、セグメントルーティングを使用して、RLFA (リモートループフリー代替) などの他の高速再ルーティング技術が保護を提供できないトポロジでリンク、ノード、および共有リスク リンク グループ (SRLG) 保護を提供します。TI-LFA の目的は、リンク障害によるトポロジ変更後にルータがコンバージェンスする間に結果として生じるパケット損失を減らすことです。急速な障害修復 (50 ミリ秒未満) は、分散ネットワーク コンバージェンス プロセスが完了するまで、ループフリーで安全に使用できる事前計算済みのバックアップパスを使用することによって達成されます。

TI-LFA を使用する主な利点を次に示します。

- すべてのプレフィックスの 100% のカバレッジと 50 ミリ秒以内のリンクおよびノードの保護を提供します。
- コンバージェンス後のパスを活用することで、一時的な輻輳と最適でないルーティングを防ぎます。
- ラベル配布プロトコル (LDP) と IP トラフィックも保護します。

IP 高速再ルーティングおよびリモート ループフリー代替

IP 高速再ルーティング (FRR) は、ネットワーク内の障害が発生したリンクまたは障害が発生したノードの周囲の IP トラフィックを、非常に短時間 (50 ミリ秒未満) で再ルーティングできるようにする一連の手法です。使用される手法の 1 つは、OSPF プロトコルを使用して実装されるループフリー代替 (LFA) です。OSPF は現在、プレフィックスごとの直接接続された LFA およびリモート LFA (RLFA) をサポートします。これらの LFA アルゴリズムの問題はトポロジ依存性です。LFA アルゴリズムはすべてのトポロジに対してネットワークを通してループフリー代替パスを見つけることはできません。

プレフィックスごとの直接接続された LFA (DLFA としても知られています) はほとんどの三角形のトポロジに対してループフリー代替パスを提供しますが、長方形または円形のトポロジに対しては優れたカバレッジを提供しません。再ルーティングされたトラフィックを中間ノードにトンネリングするために LDP シグナリングとともに MPLS フォワーディングを使用するリモート LFA 実装 (RLFA) は、リングまたは長方形トポロジの IPFRR カバレッジを拡張します。各リンクについて、RLFA は P スペース (保護対象リンクを横断せずに計算ノードから到達可能なノードのセット) と Q スペース (保護対象リンク自体を横断せずに保護されたリンク上のネイバーに到達できるノードのセット) を定義します。P および Q スペースの両方に属するノードは、PQ ノードと呼ばれ、保護対象トラフィックの中間ノードとして使用できます。RLFA は、PQ ノードを対象にした LDP セッションを形成し、RLFA トンネルを構成します。ただし、P スペースと Q スペースが分離されているトポロジでは、R-LFA はそれらのプレフィックスを保護しません。

トポロジに依存しない高速再ルーティング

トポロジに依存しない高速再ルーティング (TI-FRR) は、トポロジ内のリンクのメトリックが対称であると仮定して、セグメントルーティングを使用して任意のトポロジでリンク保護を提供する技法です。TI-LFA は、単一リンクの帯域幅が非対称である場合のバックアップを保証しません。TI-LFA は、コンバージェンス後のパス上にあるループフリー修復パスのみを考慮します。これは、ネットワークのより優れたキャパシティ計画を行うのに役立ちます。

TI-LFA アルゴリズムは、ネットワークを通して完全な明示的パスを作成することを可能にします。完全に指定されたパスを使用すると、パスに沿ったセグメントの数が原因で、大きなトポロジで問題が発生する可能性があります。ただし、パス全体を指定する必要はなく、トラフィックを保護ノードにループバックしない中間ノード (リリースノード) にトラフィックを伝送するために必要なのはパスのサブセットのみです。TI-LFA アルゴリズムは、修復パスとして SR トンネルを構築します。TI-LFA トンネルは、トンネルが通過する必要があるノード (または) 修復ノードのセットを明示的に指定することによって構築され、プログラムされます。トラフィックは (プライマリパスが失敗した場合) トンネルで伝送され、コンバージェンス後パスでも伝送されます。

トポロジに依存しないループフリー代替

ローカル LFA およびリモート LFA が有効になっている場合、保護すべきプレフィックスのカバレッジは良好になります。ただし、PQ インターセクト ノードを持たないいくつかのまれなトポロジでは、ローカルおよびリモート LFA のどちらも、失敗したリンクを保護するために解放ノードを見つけることに失敗します。さらに、2つのアルゴリズムには LFA のコンバージェンス後の特性についての知識がないため、コンバージェンス後の経路を優先する方法はありません。

上記の制限を克服するために、トポロジに依存しない LFA (TI-LFA) が SR 対応ネットワークでサポートされ、次のサポートを提供します。

- **リンク保護** : LFA はリンクの障害のための修復パスを提供します。
- **ローカル LFA** : コンバージェンス後のパスのローカル LFA が利用可能であるときはいつでも、ローカル LFA は修復パスのための追加 SID を必要としないので、TI LFA より優先されます。つまり、PQ ノードのラベルは、リリース ノードには必要ありません。
- **拡張 P スペースのローカル LFA** : 拡張 P スペースのノードの場合、ローカル LFA は今でも修復パスのための最も経済的な方法です。この場合、TI-LFA は選択されません。
- **PQ 交差ノードへのトンネル** : これは、修復パスが TI-LFA を使用してコンバージェンス後のパスで保証されることを除いて、リモート LFA と類似しています。
- **PQ 分離ノードへのトンネル** : ローカルおよびリモート LFA が修復パスを見つけられない場合には、この機能は TI-LFA に固有です。
- **複数の交差または分離 PQ ノードを通過するトンネル** : TI-LFA は、プラットフォームのサポートされている最大ラベル数まで、すべてのプレフィックスの完全なカバレッジを提供します。
- **保護対象リンクのための P2P およびブロードキャスト インターフェイス** : TI-LFA は P2P およびブロードキャスト インターフェイスを保護します。

- **非対称リンク**：ネイバー間の OSPF メトリックは同じではありません。
- **マルチホーム（エニーキャスト）プレフィックス保護**：同じプレフィックスが複数のノードによって発信される可能性があり、TI-LFA はコンバージェンス後の修復パスを提供することによってエニーキャストプレフィックスも保護します。
- **保護されたプレフィックスのフィルタリング**：ルートマップは、保護するプレフィックスのリストと、リリースノードまでの最大修復距離を制限するオプションを含めるかまたは除外します。
- **タイブレーカー**：TI-LFA に適用可能な既存のタイブレーカーのサブセットがサポートされています。

トポロジに依存しないループフリー代替タイブレーク

ローカルおよびリモート LFA は、プレフィックスを保護するために複数のパスがある場合、デフォルトまたはユーザー設定のヒューリスティックを使用してタイブレークします。この属性は、ロード バランシングの前に、TI-LFA リンク保護計算の終了時に修復パスの数を削減するために使用されます。

ローカル LFA およびリモート LFA は次のタイブレーカーをサポートします。

- **Linecard-disjoint**：ラインカード分離修復パスを優先します。
- **Node-protecting**：修復パスを保護するノードを優先します。
- **SRLG-disjoint**：SRLG 分離修復パスを優先します。
- **Load-sharing**：リンクとプレフィックスの間で均等に修復パスを分配します。

特定のプレフィックスに対して2つの修復パスがある場合、プライマリポートのものとは異なるラインカードの出力ポートであるパスが、修復パスとして選択されます。

- **LC-disjoint-index**：修復パスの両方がプライマリパスのものと同じラインカード上にある場合、両方のパスが候補と見なされます。パスの1つが別のラインカード上にある場合は、そのパスが修復パスとして選択されます。
- **SRLG-disjoint**：SRLG 分離修復パスを優先します。

SRLG ID は、各インターフェイスに対して構成できます。プレフィックスに対して2つの修復パスがある場合、修復パスに設定された SRLG ID は、プライマリパス SRLG ID のものと比較されます。セカンダリパスの SRLG ID がプライマリのものとは異なる場合、そのパスが修復パスとして選択されます。

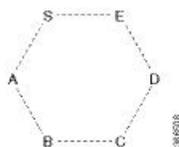
Cisco IOS XE リリース 3.18 では、ノード保護タイブレーカーはデフォルトで無効になっています。同じインターフェイス上のタイブレーカーのデフォルトと明示的なタイブレーカーは、相互に排他的です。以下のタイブレーカーは、すべての LFA でデフォルトで有効になっています。

- linecard-disjoint
- lowest-backup-metric
- SRLG-disjoint

Pスペース

S-E を通過せずに最短パス ツリー上の S から到達できるルータのセットは、リンク S-E に関して、S の P スペースと呼ばれます。

図 5: 単純なリングトポロジ



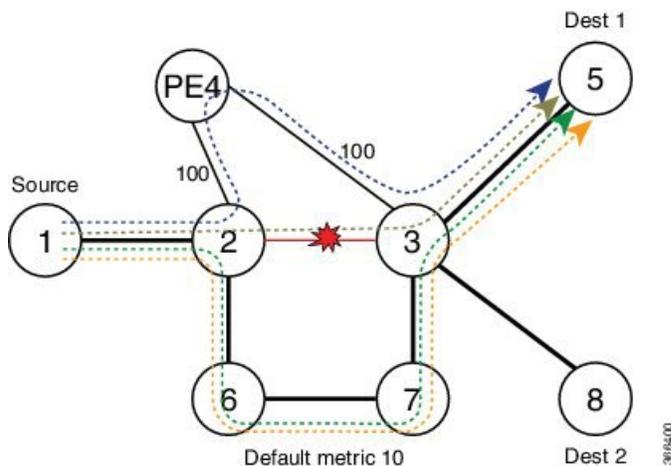
Qスペース

リンク S-E を通過することなく通常のフォワーディングによってノード E に到達できるルータのセットは、リンク S-E に関して、E の Q スペースと呼ばれます。

コンバージェンス後のパス

コンバージェンス後のパスは、OSPF がリンク障害の後に使用するパスです。TI-LFA は常に、コンバージェンス後のパスである修復パスを計算します。障害発生時にトラフィックを伝送するために、コンバージェンス後のパスを計画してサイズを合わせることができます。TI-LFA は、コンバージェンス後のパスをセグメントのリストとしてエンコーディングすることによって適用します。次の図は、コンバージェンス後のパスを使用した TI-LFA の例を示しています。

図 6: コンバージェンス後のパスを使用した TI-LFA

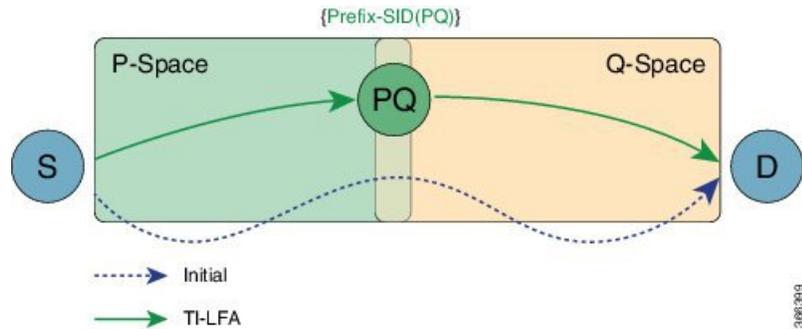


- これは、リンク 2-3 の障害に対してノード 2 の宛先ノード 5 を保護します。
- ノード 2 は、コアリンクを介してノード 5 宛てのすべてのトラフィックをスイッチします。

宛先ごとのリンク保護

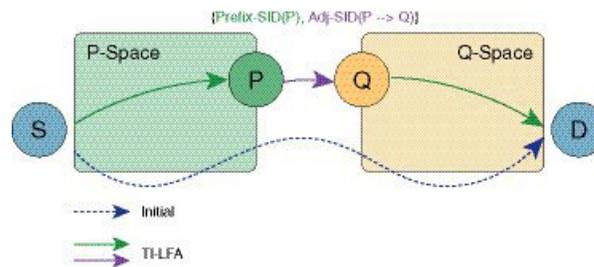
TI-LFA の実装は、基盤となるハードウェアによってサポートされるセグメント（ラベル）の数で宛先ごとのリンク保護を提供します。次の図は、TI-LFA の実装を示しています。

図 7: TI-LFA : {プレフィックス SID (PQ)} }



PQ が S の直接ネイバーである場合、追加セグメントをプッシュする必要はありません。

図 8: TI-LFA : {プレフィックス SID (P)、隣接関係 SID (P->Q)} }



インターフェイスごとのループフリー代替の使用可能性

- TI-LFA は、エリアごとに有効にすることができます。
- TI-LFA バックアップパスが計算されるのは、保護対象のプライマリ インターフェイスで TI-LFA 保護が有効になっている場合だけです。デフォルトでは、すべてのインターフェイスで保護が有効です。
- TI-LFA 修復パスは、ハードウェアによってサポートされるラベルの数によって制限されます。ハードウェアが2つのラベルだけをサポートする場合、TI-LFA 修復パスは、2つ以下のセグメントによって保護できるそれらのプレフィックスだけを保護できます。2つ以上のセグメントを必要とするそれらのプレフィックスは、未保護のままになります。

プレフィックス処理

すべてのリンクについて TI-LFA パスが計算されると、プレフィックス処理が開始されます。デフォルトでは、エリア内およびエリア間のプレフィックスのみが保護されます。外部プレ

フィックスを保護するには、OSPF レベルでグローバルにセグメントルーティングを有効にする必要があります。

プライマリパスと修復パスは、保護されているプレフィックスと同じルートタイプである必要があります。つまり、エリア内を保護する必要がある場合、TI-LFA 修復パスは、プレフィックスが一意であっても（または）エニーキャストプレフィックスであっても、同じエリア内プレフィックスについても計算します。

エニーキャストプレフィックス処理

また OSPF TI-LFA は、エニーキャストプレフィックスのための修復パスを計算します。エニーキャストプレフィックス（または）デュアルホームのプレフィックスは、複数のルータによってアドバタイズされたプレフィックスです。エリア内、エリア間、またはエリア外プレフィックスである可能性があります。エニーキャストプレフィックスのための TI-LFA 修復パスの計算は以下のとおりです。

- プレフィックス P1 がルータ R1 および R2 によってアドバタイズされると仮定します。両方のルータによってアドバタイズされたプレフィックスは、同じルートタイプである必要があります。つまり、R1 と R2 の両方で、プレフィックスをエリア内プレフィックス（またはエリア内もしくはエリア外）としてアドバタイズする必要があります。
- プライマリパスは、コストが低いため R1 に向けて計算されます。
- TI-LFA がバックアップパスを計算するときに、コンバージェンス後のパスを計算します。したがって、コンバージェンス後のパスは R1 向けである必要はありません。R2（コンバージェンス後）に到達するためのコストがより短い場合、TI-LFA アルゴリズムは R2 向けのコンバージェンス後パスを選択します。TI-LFA トンネルは R2 に向けて形成されません。
- R2 がプレフィックスをアドバタイズしない場合、TI-LFA アルゴリズムは R1 向けの修復パスについて再計算されます。

プレフィックスごとのループフリー代替タイブレーク

IP FRR には、以下に示す順序で下記のタイブレークルールがあります。最適なパスを選択できる複数の修復パスがある場合は、次のタイブレークルールが適用されます。複数のパスがすべてのタイブレークルールに一致する場合、すべてのパスが修復パスとして使用されます。

- **Post Convergence** : コンバージェンス後のパスであるバックアップパスを優先します。これはデフォルトで有効になっていて、ユーザーはこれを変更できません。
- **Primary-path** : ECMP セットからのバックアップパスを優先します。
- **Interface-disjoint** : ポイントツーポイントインターフェイスには、プライマリゲートウェイで障害が発生した場合、再ルーティングのための代替のネクストホップはありません。interface-disjoint 属性を設定すると、このような修復パスの選択を防ぐことができるため、インターフェイスが保護されます。

- **Lowest-backup-metric** : 最小の合計メトリックを持つバックアップパスを優先します。TI-LFA は常に最低のコストであるバックアップパスを選択するので、これは TI-LFA には適用されません。
- **LC-disjoint** : プライマリパスとは異なるラインカードにあるバックアップパスを優先します。
- **Broadcast-interface-disjoint** : LFA 修復パスは、修復パスと保護されたプライマリパスが異なるネクストホップインターフェイスを使用するときにリンクを保護します。ただし、ブロードキャストインターフェイスでは、LFA 修復パスがプライマリパスと同じインターフェイスを介して計算され、ネクストホップゲートウェイが異なる場合、ノードは保護されますがリンクは保護されないことがあります。**broadcast-interface-disjoint** 属性を設定すると、プライマリパスがポイントするブロードキャストネットワークを修復パスが経由しない（つまり、インターフェイスと、これに接続されるブロードキャストネットワークを使用できない）ように指定することができます。
- **Load Sharing** : 上記のルールに一致する修復パスが複数ある場合は、バックアップパスをロードシェアします。このルールは、ユーザーが変更することもできます。



(注) ユーザーは、要件に応じてタイプブレイクルールを変更および定義できます。このようにして、ユーザーはシーケンスの優先順位を変更したり、必要のないタイプブレイクインデックスの一部を削除したりすることができます。



(注) TI-LFA は常に最低コストのバックアップパスのみを選択するので、Lowest-backup-metric ポリシーは TI-LFA には適用されません。

上記のルールは、次のコマンドを使用して確認できます。

```
R2#show ip ospf fast-reroute
      OSPF Router with ID (10.2.2.200) (Process ID 10)
Microloop avoidance is enabled for protected prefixes, delay 5000 msec
Loop-free Fast Reroute protected prefixes:
      Area          Topology name  Priority  Remote LFA Enabled  TI-LFA Enabled
      0              Base           Low       No                    Yes
AS external        Base           Low       No                    Yes

Repair path selection policy tiebreaks (built-in default policy):
  0  post-convergence
 10  primary-path
 20  interface-disjoint
 30  lowest-metric
 40  linecard-disjoint
 50  broadcast-interface-disjoint
256  load-sharing
```

```
OSPF/RIB notifications:
  Topology Base: Notification Enabled, Callback Registered
```

```
Last SPF calculation started 17:25:51 ago and was running for 3 ms.
```

TI-LFA の導入によって、次の 2 つのタイブレーク ルールが拡張されます。

- node-protection
- srlg-protection

上記の 2 つのタイブレークルールは、デフォルトでは有効になっていません。ユーザーは、前述のタイブレーク ポリシーを設定する必要があります。

ノード保護

TI-LFA ノード保護は、ノード障害からの保護を提供します。ノードを保護する TI-LFA は、特定のネクストホップへのリンクだけでなく、特定のネクストホップの障害に対して保護するコンバージョン後の修復パスの計算を試みます。

ノード保護は、ローカル LFA の実装でもタイブレーカーとして使用されます。ただし、これが TI-LFA と組み合わせられると、バックアップパスはノード保護パスとのコンバージョン後に計算されます。プレフィックスごとの TI-LFA ノード保護はデフォルトで無効になっています。IPFRR TI-LFA ノード保護機能は、対応するタイブレークが TI-LFA 機能とともに有効になると有効になります。つまり、

```
router ospf 10
  [no] fast-reroute per-prefix ti-lfa [area <area> [disable]]
  [no] fast-reroute per-prefix tie-break node-protecting index <index>
  [no] fast-reroute per-prefix tie-break node-protecting required index <index>
```

ノード保護を有効にする場合、他のすべてのタイブレーク ルールも手動で設定する必要があります。ノード保護はリンク保護上に構築されます。

node-protecting と **node-protecting required** の違いは、バックアップパスの選択です。

node-protecting required を設定すると、選択されたバックアップは、ノード（保護しているリンクの一部）を通過しないパスでなければなりません。このようなパスが使用できない場合は、バックアップパスとしてパスが選択されません。

共有リスク リンク グループ保護

共有リスクリンクグループ (SRLG) は、同時に障害が発生する可能性が高い修復パスおよび保護されたプライマリパスのネクストホップインターフェイスのグループです。OSPFv2 ループフリー Fast Reroute 機能では、コンピューティングルータでローカルに設定された SRLG のみがサポートされます。TI LFA の導入によって、SRLG グループ ID をプライマリパスインターフェイスと共有しないコンバージョン後のパスが選択されます。このようにして、プライマリリンクが失敗するたびに、ユーザーは SRLG 保護を確認します。

IPFRR TI-LFA SRLG 保護機能は、対応するタイブレークが TI-LFA 機能とともに有効になると有効になります。つまり、

```
router ospf 10
  [no] fast-reroute per-prefix ti-lfa [area <area> [disable]]
  [no] fast-reroute per-prefix tie-break srlg index <index>
  [no] fast-reroute per-prefix tie-break srlg required index <index>
```

SRLG 保護を有効にすると、他のすべてのタイブレイクルールを手動で設定する必要があります。**srlg-protecting** と **srlg-protecting required** の違いは、バックアップパスの選択です。**srlg-protecting required** を設定すると、選択されたバックアップは、保護されているプライマリリンクと SRLG ID を共有しないパスでなければなりません。このようなパスが使用できない場合は、バックアップパスとしてパスが選択されません。

一方、**srlg-protecting** を単独で設定すると、SRLG 保護パスが使用できない場合は、リンク保護パスがバックアップパスとして選択されます。SRLG 保護パスが使用可能な場合、SRLG 保護パスへのスイッチオーバーが行われます。

ノード共有リスク リンク グループ保護

ノードと SRLG の保護タイブレイクの両方を一緒に設定できます。これは、バックアップパスがノード保護と SRLG 保護の両方の基準を満たす必要があることを意味します。その場合、追加の TI-LFA ノード SRLG の組み合わせ保護アルゴリズムが実行されます。TI-LFA ノード SRLG の組み合わせアルゴリズムは、コンバージェンス後の最短パスツリー (SPT) を計算するときに、保護されたノードと、同じ SRLG グループを持つインターフェイスのすべてのメンバーを削除します。

ノードおよび SRLG の保護タイブレイクを一緒に有効にするには、次のコマンドを使用します。

```
router ospf 10
  [no] fast-reroute per-prefix ti-lfa [area <area> [disable]]
  [no] fast-reroute per-prefix tie-break node-protecting index <index>
  [no] fast-reroute per-prefix tie-break srlg index <index>
```

次の show コマンドは、タイブレイクポリシーを表示するために使用されます。

```
R3#show ip ospf fast-reroute

      OSPF Router with ID (10.3.3.33) (Process ID 10)

Loop-free Fast Reroute protected prefixes:

      Area          Topology name  Priority  Remote LFA Enabled  TI-LFA Enabled
      ---          -
          0          Base           Low       No                   No
          1          Base           Low       No                   No
        1000          Base           Low       No                   No
AS external          Base           Low       No                   No

Repair path selection policy tiebreaks:
  0 post-convergence
  60 node-protecting
  70 srlg
  256 load-sharing

OSPF/RIB notifications:
Topology Base: Notification Disabled, Callback Not Registered
```

Last SPF calculation started 00:00:06 ago and was running for 2 ms.

トポロジに依存しないループフリー代替高速再ルーティングの設定方法

トポロジに依存しないループフリー代替高速再ルーティングの有効化

デフォルトでは、TI-LFA は無効になっています。プロトコルの有効化を使用して、TI-LFA を有効にすることができます。

プロトコルの有効化：すべての OSPF エリアに対して、ルータ OSPF モードで TI-LFA を有効にします。TI-LFA FRR を有効にするには、次の手順を実行します。

```
[no] fast-reroute per-prefix ti-lfa [ area <area> disable]
```

```
router ospf <process>
fast-reroute per-prefix enable area <area> prefix-priority {low | high}
fast-reroute per-prefix ti-lfa [ area <area> disable]
```

また、インターフェイス コマンドを使用して、特定のインターフェイスで IP FRR を有効または無効にすることもできます。

```
interface <interface>
ip ospf fast-reroute per-prefix protection disable
ip ospf fast-reroute per-prefix candidate disable
ip ospf fast-reroute per-prefix protection ti-lfa [disable]
```



- (注)
- TI-LFA が OSPF ルータおよび広域で設定されるとき、エリア特定の設定が優先します。
 - 外部プレフィックスを保護するには、TI-LFA はグローバルに有効にする必要があります。

トポロジに依存しないループフリー代替高速再ルーティングの設定

このタスクでは、リンク、ノード、および SRLG の障害に関するトラフィック フローを収束させるために、プレフィックスごとのトポロジに依存しないループフリー代替 (TI-LFA) の計算を有効にする方法について説明します。TI-LFA は、より低いレベルによって継承されたインスタンスまたはエリア レベルで設定することができます。TI-LFA にも適用されるインターフェイス レベルごとのプレフィックス FRR ごとに有効または無効にできます。

設定を開始する前に、次のトポロジ要件を満たしていることを確認してください。

- ルータ インターフェイスがトポロジごとに設定されている。
- ルータが OSPF で設定されている。

- セグメントルーティングが OSPF レベルでもグローバルでも有効である。

1. 指定されたルーティング プロセスの OSPF ルーティングを有効にして、ルータ コンフィギュレーション モードを開始します。

```
Device(config)# router ospf 10
```

2. FRR を有効にします。

```
Device(config-router)# fast-reroute per-prefix enable prefix-priority low
```

3. TI-LFA を有効にします。

```
Device(config-router)# fast-reroute per-prefix ti-lfa
```

4. 特定のエリアで TI-LFA を有効にします。

```
Device(config-router)# fast-reroute per-prefix ti-lfa area 0
```

5. TI-LFA モードを終了します。

```
Device(config-router)# exit
```

6. インターフェイス モードに入ります。

```
Device(config)#interface ethernet 0/0
```

7. 特定のインターフェイスで FRR を有効にしたいくない場合は、`protection disable` コマンドを使用します。

```
Device(config-if)#ip ospf fast-reroute per-prefix protection disable
```

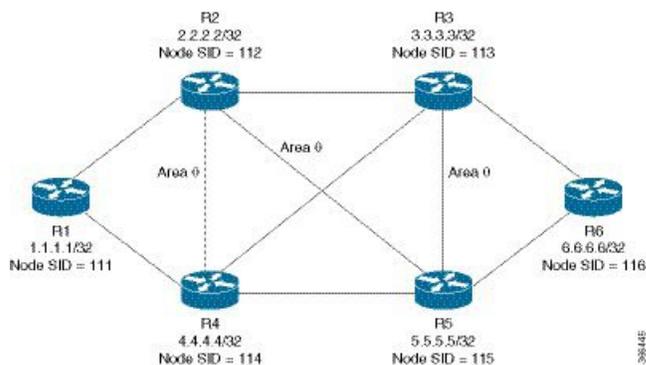
8. 特定のインターフェイスを修復パスとして有効にしたいくない場合は、`candidate disable` コマンドを使用します。

```
Device(config-if)#ip ospf fast-reroute per-prefix candidate disable
```

トポロジに依存しない高速再ルーティング タイブレーカーの設定

すべてのノードのプレフィックス SID が設定されているすべてのルータで、セグメントルーティングを有効にする必要があります。構成を理解するには、次のトポロジを参照として使用してください。

図 9: 設定例



R2 と R3 の間のリンクを保護するデバイス R2 を考えます。R2 での設定：

```
router ospf 10
fast-reroute per-prefix enable prefix-priority low
fast-reroute per-prefix ti-lfa
segment-routing mpls
segment-routing area 0 mpls
fast-reroute per-prefix enable prefix-priority low
fast-reroute per-prefix ti-lfa
fast-reroute per-prefix ti-lfa area 0
fast-reroute per-prefix tie-break node-protecting index 60
fast-reroute per-prefix tie-break srlg index 70
mpls traffic-eng router-id Loopback1
mpls traffic-eng area 0

interface GigabitEthernet4 //interface connecting to the router 4
ip address 10.101.4.4 255.255.255.0
ip ospf 10 area 0
ip ospf network point-to-point
srlg gid 10
negotiation auto

interface GigabitEthernet3 //interface connecting to the router 3
ip address 10.101.3.3 255.255.255.0
ip ospf 10 area 0
ip ospf network point-to-point
srlg gid 10
negotiation auto

interface GigabitEthernet5 //interface connecting to the router 2
ip address 10.101.5.5 255.255.255.0
ip ospf 10 area 0
ip ospf network point-to-point
srlg gid 20
negotiation auto

interface loopback2
ip address 10.2.2.2/32
ip ospf 10 area 0
```



(注) 他のすべてのデバイスでは、セグメントルーティングの構成と、接続されたプレフィックス SID の割り当てを行う必要があります。

ノード保護の仕組み：例として同じトポロジを使用し、R2 と R3 の間のリンクと R6 からのプレフィックスも保護している場合を考えてみましょう。その場合、プレフィックスのプライマリパスが R2-R3 経由であると想定してみましょう。したがってプライマリパスは R2---R3---R6 であり、リンク R2---R3 を保護しています。

このシナリオでは、リンク保護のみが設定され、有効になっています。OSPF プロセスの下で TI-LFA を有効にすると、すべてのパスのコストが等しいという条件で次のパスが得られます。

R2---R4---R5---R6

R2---R5---R3---R6

R2---R5---R6

リンク保護のみを設定している場合は、3つのパスがすべて選択され、それらの間で負荷が共有されます。

ノード保護を構成する場合は、バックアップパスに保護対象のノードが含まれないようにバックアップが計算されます。この例では、バックアップのノード R3 は必要ありません。その結果、次の2つのパスのみがバックアップパスとして選択されます。

R2---R4---R5---R6

R2---R5---R6

R2---R5---R3---R6 のコストは上記の2つのパスよりも小さい可能性があります。しかし、ノード保護が設定されているため、上記の2つのパスのみが考慮されます。

SRLG 保護の仕組み：SRLG 保護は、プライマリパスとバックアップが同じ SRLG ID を共有しないような方法で、バックアップパスをさらに排除します。次のバックアップパスが使用可能であるとしています。

R2---R4---R5---R6

R2---R5---R6

次に、(R2---R4) と (R2---R5) の SRLG ID が、10 であるプライマリ インターフェイス (R2---R3) と比較されます。インターフェイス R2---R5 のみが、異なる SRLG ID である 20 を持つことに注意します。したがって、バックアップパス R2---R5---R6 のみが選択されます。

トポロジに依存しない高速再ルーティング トンネルの確認

次のコマンドを使用して、TILFA トンネルを確認することができます。

```
Device#show ip ospf fast-reroute ti-lfa tunnels
```

```
OSPF Router with ID (10.2.2.200) (Process ID 10)
```

```
Area with ID (0)
```

```
Base Topology (MTID 0)
```

Tunnel	Interface	Next Hop	Mid/End Point	Label
MPLS-SR-Tunnel2	Et1/1	10.7.0.7	10.1.1.1	16020
MPLS-SR-Tunnel6	Et0/3	10.8.0.0	10.3.3.3	16003
MPLS-SR-Tunnel7	Et1/1	10.7.0.7	10.1.1.1	16020
			10.5.5.5	16005
			10.3.3.3	16003
MPLS-SR-Tunnel5	Et0/3	10.8.0.0	10.5.5.5	16005
MPLS-SR-Tunnel11	Et1/1	10.7.0.7	10.1.1.1	16020
			10.5.5.5	16005
MPLS-SR-Tunnel13	Et1/1	10.7.0.7	10.6.6.6	16006

次のコマンドを使用して、プライマリおよび修復パスを持つ OSPF ルーティングテーブル内のルートを確認できます。

```

Device#show ip ospf rib 10.6.6.6

          OSPF Router with ID (10.2.2.200) (Process ID 10)

          Base Topology (MTID 0)

OSPF local RIB
Codes: * - Best, > - Installed in global RIB
LSA: type/LSID/originator

*> 10.6.6.6/32, Intra, cost 31, area 0
    SPF Instance 19, age 02:12:11
      contributing LSA: 10/10.0.0.0/10.6.6.6 (area 0)
    SID: 6
    CSTR Local label: 0
    Properties: Sid, LblRegd, SidIndex, N-Flag, TeAnn
    Flags: RIB, HiPrio
      via 10.7.0.7, Ethernet1/1 label 16006
        Flags: RIB
        LSA: 1/10.6.6.6/10.6.6.6
    PostConvrq repair path via 10.3.3.3, MPLS-SR-Tunnel6 label 16006, cost 81, Lbl cnt
    1
      Flags: RIB, Repair, PostConvrq, IntfDj, LC Dj
      LSA: 1/10.6.6.6/10.6.6.6

```

次のコマンドを使用して、IP ルーティング テーブルにルートを表示できます。

```

Device#show ip route 10.6.6.6
Routing entry for 10.6.6.6/32
  Known via "ospf 10", distance 110, metric 31, type intra area
  Last update from 10.7.0.7 on Ethernet1/1, 00:25:14 ago
  SR Incoming Label: 16006
  Routing Descriptor Blocks:
    * 10.7.0.7, from 10.6.6.6, 00:25:14 ago, via Ethernet1/1, merge-labels
      Route metric is 31, traffic share count is 1
      MPLS label: 16006
      MPLS Flags: NSF
      Repair Path: 10.3.3.3, via MPLS-SR-Tunnel6

```

トポロジに依存しないループフリー代替高速再ルーティングのデバッグ

次のコマンドを使用して、TI-LFA FRR をデバッグすることができます。

```

debug ip ospf fast-reroute spf
debug ip ospf fast-reroute spf detail
debug ip ospf fast-reroute rib
debug ip ospf fast-reroute rib [<access-list>]

```

例：OSPFv2 リンク保護のトポロジに依存しないループフリー代替高速再ルーティング

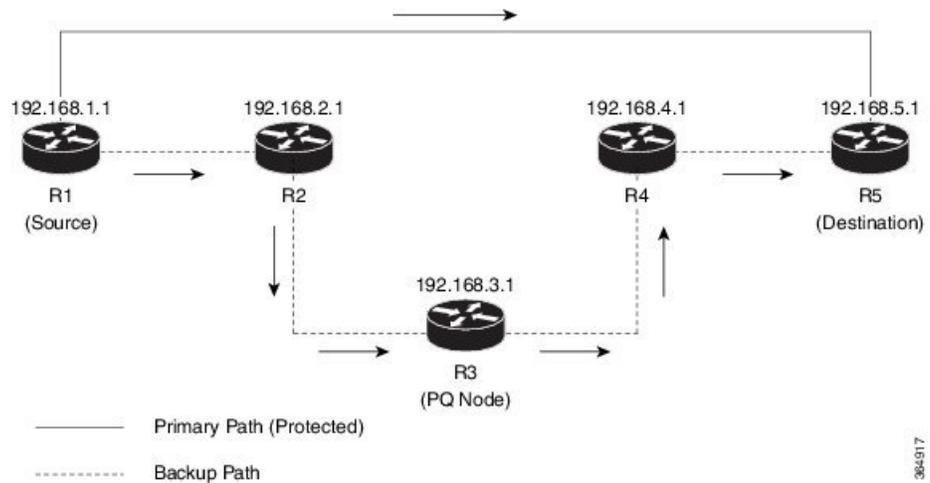
OSPFv2 リンク保護 TI-LFA FRR の例を次に示します。

例：トポロジに依存しないループフリー代替高速再ルーティングの設定

この例では、単一またはディスジョイントの PQ ノードを使用してセグメントルーティング TE トンネルに TI-LFA を設定する方法を示します。次に、使用される 2 つのトポロジを示します。

- トポロジ 1：単一の PQ ノードであり、2 つの SID を持ちます。送信元ルータ R1 から PQ ノードを経由して宛先ルータ R5 に送信されます。

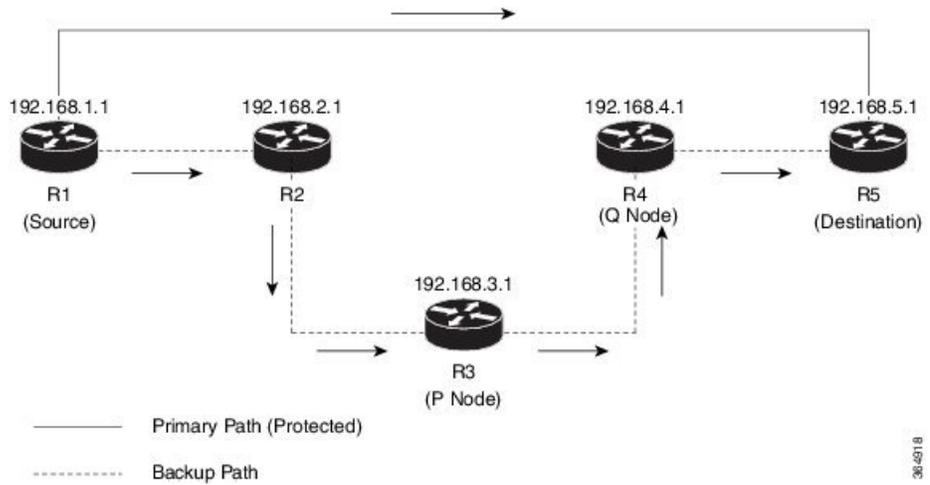
図 10: トポロジ 1: 単一の PQ ノード



- トポロジ 2：ディスジョイント PQ ノードであり、3 つの SID で構成されます。送信元ルータ R1 から P ノードおよび Q ノードを介して宛先ルータ R5 に送信されます。

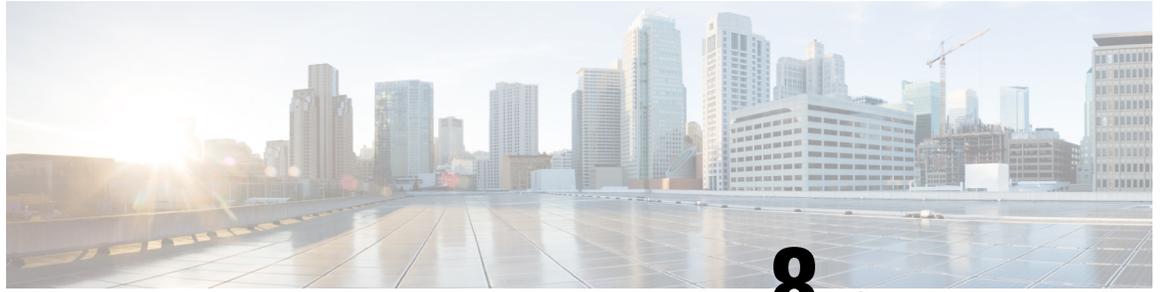
例：トポロジに依存しないループフリー代替高速再ルーティングの設定

図 11: トポロジ 2: ディスジョイント PQ ノード



宛先ルータ（R5）に接続する送信元ルータ（R1）インターフェイスで OSPF 用に TI-LFA を設定します。

```
Device(config)# router ospf 10
Device(config-router)# fast-reroute per-prefix enable prefix-priority low
Device(config-router)# fast-reroute per-prefix ti-lfa
Device(config-router)# fast-reroute per-prefix ti-lfa area 0
Device(config-router)# exit
```



第 8 章

OSPF のセグメントルーティングトラフィックエンジニアリング

この章では、OSPF を使用してセグメントルーティングトラフィックエンジニアリングを実装する方法について説明します。

- OSPF のセグメントルーティングトラフィックエンジニアリングの機能情報 (95 ページ)
- OSPF のセグメントルーティングトラフィックエンジニアリングの制約事項 (96 ページ)
- OSPF のセグメントルーティングトラフィックエンジニアリングに関する情報 (96 ページ)
- OSPF のセグメントルーティングトラフィックエンジニアリングの設定方法 (106 ページ)
- SR-TE トンネルの構成の確認, on page 114

OSPF のセグメントルーティングトラフィックエンジニアリングの機能情報

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、<https://cfng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

表 6: OSPFのセグメントルーティングトラフィックエンジニアリングの機能情報

機能名	リリース	機能情報
OSPFのセグメントルーティングトラフィックエンジニアリング	Cisco IOS XE Amsterdam 17.3.2	<p>トラフィックエンジニアリング (TE) トンネルは、トンネルの入力とトンネルの宛先との間でインスタンス化されたTE LSPのコンテナです。TE トンネルは、同じトンネルに関連付けられた1つ以上のSR-TE LSPをインスタンス化できます。</p> <p>次のコマンドが追加または修正されました。</p> <p>show mpls traffic-eng tunnels、 tunnel mpls traffic-eng path-option 10 dynamic segment-routing、 tunnel mpls traffic-eng path-option 10 segment-routing、 tunnel mpls traffic-eng path-option 10 explicit name MIXED_PATH segment-routing、 tunnel mpls traffic-eng path-option 10 explicit name IP_PATH1 segment-routing、 tunnel mpls traffic-eng path-option 10 explicit name NODE_PATH segment-routing。</p>

OSPFのセグメントルーティングトラフィックエンジニアリングの制約事項

- セグメントルーティングトラフィックエンジニアリングは、OSPFv2でのみサポートされています。
- SR-TEは、ブロードキャストインターフェイスではサポートされていません。ポイントツーポイントインターフェイスのみサポートしています。
- 特定の時点で、TEに対して有効にする必要があるプロトコルのインスタンスは1つだけです。

OSPFのセグメントルーティングトラフィックエンジニアリングに関する情報

トラフィックエンジニアリング (TE) トンネルは、トンネルの入力とトンネルの宛先との間でインスタンス化されたTE LSPのコンテナです。TE トンネルは、同じトンネルに関連付けられた1つ以上のSR-TE LSPをインスタンス化できます。SR-TE LSPパスが宛先ノードへの同じIGPパスに必ずしも従うとは限りません。この場合、SR-TEパスには、SR-TE LSPが通過するノードおよび/またはリンクのプレフィックスSIDおよび/または隣接関係SIDのセットを指定することができます。

ヘッドエンドは、トンネルを通して伝送される発信パケットに、対応するMPLSラベルスタックを課します。SR-TE LSPパスに沿った各通過ノードは、パケットが最終的な宛先に到達するまで、着信トップラベルを使用してネクストホップを選択し、ラベルをポップまたはスワップし、ラベルスタックの残りの部分を使用して次のノードにパケットを転送します。OSPFは、トポロジおよびSRに関連する情報をTEに提供します。SR関連情報には、ネットワーク内でSRが有効になっているすべてのノード/リンクのSRGB/プレフィックス/隣接関係SIDが含まれます。

OSPFのセグメントルーティングトラフィックエンジニアリングを使用する利点

セグメントルーティングトラフィックエンジニアリングは、次のような役に立つすべての最適化と制約を包括的にサポートしています。

- 遅延
- 帯域幅
- ディスジョイントネス
- リソース回避

OSPFv2は、SR-TEに以下の機能を提供します。

- OSPFv2は、TEモジュールにSR情報とともにTEトポロジ情報を提供します。
- TEでは、この情報を使用し、プレフィックスおよび/または隣接関係セグメントの組み合わせを使用して、1つ以上のセグメントで構成されるSR TEパス/トンネルを構築します。
- TEが関連するプレフィックスの場合、OSPFはフォワーディングプレーンをセットアップするためのファーストホップの解決策を提供します。
- また、SR TE トンネルは、SR-TE トンネル上のトラフィックを即転送するためにOSPF (RSVP TE トンネルなど) に再度アダプタイズされます。

OSPFv2 セグメントルーティングトラフィックエンジニアリング機能

OSPFv2は、SR-TEのために以下の機能を実行します。

- OSPFv2は、TEモジュールにSR情報とともにTEトポロジ情報を提供します。
- TEでは、この情報を使用し、プレフィックスおよび/または隣接関係セグメントの組み合わせを使用して、1つ以上のセグメントで構成されるSR TEパス/トンネルを構築します。
- TEが関連するプレフィックスの場合、OSPFはフォワーディングプレーンをセットアップするためのファーストホップの解決策を提供します。
- また、SR TE トンネルは、SR-TE トンネル上のトラフィックを即転送するためにOSPF (RSVP TE トンネルなど) に再度アダプタイズされます。

保護された隣接関係 SID

セグメントルーティングは、ポイントツーポイントインターフェイスおよびブロードキャストインターフェイスに対して保護された隣接関係 SID を作成します。セグメントルーティングは、それらを保護されていない隣接関係 SID とともに、拡張リンクステートアドバタイズメント (LSA) にアドバタイズします。保護された隣接関係 SID は修復パスを持つことができますが、修復パスを持つことが保証されるわけではありません。

トラフィック エンジニアリング インターフェイス

SR-TE 機能をサポートするため、TE は、TE トポロジに関する情報を配布および受信するためのさまざまなコンポーネントや IGP (OSPF および ISIS) と連携します。SR-TE サポートの場合、OSPF は、さまざまな LSA を通じて受信した SR 情報を TE に追加で提供する必要があります。

- ルータ情報 LSA
- 拡張プレフィックス LSA
- 拡張リンク LSA

TE インターフェイスは、TE 用に設定されたリンクに関連付けられた、帯域幅リソース、制約、機能、その他の属性などの情報を配布します。リンク情報は、不透明な LSA を使用して他のルータに配布され、TE によってローカルトポロジデータベースを作成するために使用されます。トポロジデータベースは、TE が LSP を確立するための適切な制約ベースのパスを計算できるようにするための鍵となる要素です。TE は IGP とも連携し、ルーティングパケット用に TE ヘッドエンドインターフェイスを考慮できる場合に通知します。

アンナンバード サポート

アンナンバードリンクの IS-IS の説明には、リモートインターフェイス ID 情報は含まれません。アンナンバードリンクのリモートインターフェイス ID には、SR-TE トンネルの一部としてアンナンバードリンクを含める必要があります。

隣接関係転送のためのセグメントルーティングトラフィックエンジニアリング サポート

MPLS TE 転送隣接機能は、OSPF でサポートされます。この場合、TE トンネルは IGP ネットワーク内のリンクと見なされます。TE トンネルインターフェイスは、他のリンクと同様に、IGP ネットワーク内にアドバタイズされます。その後、ルータはこれらのリンクを使用して最短パスツリー (SPT) を計算できます。



(注) この機能は、SR-TE トンネルではサポートされていません。

自動ルート アナウンスのためのセグメントルーティングトラフィックエンジニアリング サポート

MPLS TE 自動ルートアナウンス機能は、TE トンネルをファーストホップとして使用する OSPF によって、ノードがそのトンネル経由で到達可能な場合にサポートされます。これにより、TE トンネルのテールエンドへ向かう下流方向のノードへのトラフィックがトンネルを通して流れます。OSPF では、RSVP を使用した MPLS TE トンネル設定と同様に、SR-TE トンネル上での自動ルートをサポートします。

SR-TE LSP をインスタンス化する TE トンネルは、IGP のショートカットとして IGP (OSPF および ISIS) に自動ルートアナウンス (AA) することができます。IGP はネクストホップとして TE トンネルを使用し、最短パスが TE トンネルの宛先よりも遅くなるすべての IP プレフィックスに対して RIB にルートをインストールします。TE トンネルの自動ルートアナウンスは、IPv4 プレフィックスを運ぶためにサポートされています。

自動ルート アナウンス IP2MPLS

SR トンネルのための自動ルート IP2MPLS 機能は、SR-TE トンネルのヘッドエンド/入力と、ヘッドエンド/入力にパケットを指定/ルーティングして戻すノードとの間で、潜在的なパケットが無限にループするのを回避するために導入されました。

このソリューションは、SR-TE トンネルにマッピングされるプレフィックスに対して2セットのパスを転送するヘッドエンドプログラミングで構成されています。1つ目は、発信インターフェイスをトンネルインターフェイスとして持ち、マッピングされているプレフィックスの純粋な IP ルートです。これにより、IP トラフィックをトンネル経由で直接マッピングできます。2つ目は、トンネルにマップされたプレフィックスの MPLS パスです。この場合プレフィックス SID ラベルは IGP の最短パス発信インターフェイス、つまり非トンネル出力インターフェイスでプログラムされます。

SR-TE LSP のインスタンス化

トラフィックエンジニアリング (TE) トンネルは、1つ以上のインスタンス化された TE LSP のコンテナです。SR-TE LSP は、TE トンネルのパスオプションで「segment-routing」を設定することによってインスタンス化されます。トンネルにマップされたトラフィックは、プライマリ SR-TE のインスタンス化 LSP を介して転送されます。

同じトンネルの下で複数のパスオプションを設定することもできます。各パスオプションには、プリファレンスインデックスまたはパスオプションインデックスが割り当てられていて、プライマリ LSP をインスタンス化するためのより有利なパスオプションを決定するために使用されます。パスオプションのプリファレンスインデックスが低いほど、パスオプションがより有利になります。同じ TE トンネルにおける他のあまり有利ではないパスオプションは、セカンダリパスオプションと見なされ、(たとえば、パス上の障害が原因で) 現在使用されているパスオプションが無効になった場合に使用されることがあります。



Note フォワーディングステートは、プライマリ LSP に対してのみ維持されます。

トンネルパスアフィニティの検証

トンネルパスのアフィニティは、トンネルインターフェイスで **tunnel mpls traffic-eng affinity** コマンドを使用して指定することができます。

ヘッドエンドは、指定された SR パスが設定されたアフィニティに準拠していることを検証します。これにより、SR パスの各セグメントのパスは、指定された制約に照らして検証される必要があります。パスの少なくとも1つのセグメントが設定されているアフィニティを満たさない場合、そのパスは設定されているアフィニティ制約に対して無効として宣言されます。

SR-TE トラフィックのロードバランシング

SR-TE トンネルは、次のロードバランシング オプションをサポートします。

ポートチャネルTEリンクのロードバランシング

ポートチャネルインターフェイスは SR-TE LSP トラフィックを運びます。このトラフィック負荷は、ポートチャネルメンバーリンクと、SR-TE LSP の先頭または中間のバンドルインターフェイス上でバランスをとります。

単一トンネルでのロードバランシング

同じコストのマルチパスプロトコル (ECMP) を使用している間、特定のプレフィックス SID へのパスが複数のネクストホップを指す場合があります。さらに、SR-TE LSP パスが、ECMP を持つ1つ以上のプレフィックス SID を通過する場合、SR-TE LSP トラフィック負荷は、SR-TE LSP パスに沿ってヘッドエンドまたは中間点の通過したノードから通過した各プレフィックス SID の ECMP パスでバランスをとります。

複数トンネルでのロードバランシング

スタティックルートを設定するか、同じ宛先に対して複数の並列トンネルを自動ルートアナウンスをすると、複数の TE トンネルを特定の IP プレフィックスへのルーティングのためのネクストホップパスとして使用することができます。このような場合、トンネルはトラフィック負荷を均等に共有するか、複数の並列トンネル上でトラフィックをロードバランシングします。トンネルヘッドエンドでトンネルごとの明示的な設定を使用して不等なロードバランシング (UELB) を許可することも可能です。この場合、トンネルのロードシェアは MPLS-TE からフォワーディングプレーンに渡されます。

トンネルのロードシェア機能は、SR-TE LSP をインスタンス化する TE トンネルで引き続き機能します。

SR-TE トンネルの再最適化

TE トンネルの再最適化は、ヘッドエンドが、現在使用しているパスよりも最適な利用できるパスがあると判断した場合に発生します。たとえば、SR-TE LSP パスに沿って障害が発生した場合、ヘッドエンドは再最適化をトリガーすることによって、より最適なパスを検出し復帰することができます。

SR-TE LSP をインスタンス化するトンネルは、トンネルを通して運ばれるトラフィックに影響を与えずに再最適化できます。

再最適化は、次の理由で発生します。

- プライマリ SR-TE LSP 明示的パスによって使用される明示的なパスホップが変更された。
- トポロジパスが切断されているか、明示的パスで指定されている SID データベースで SID が見つからないため、現在使用しているパスオプションは無効であるとヘッドエンドが判断した。
- より有利なパスオプション（より低いインデックス）が利用可能になった。

ヘッドエンドは、SR-TE LSP が通過する保護された SR 隣接関係 SID で障害を検出すると、無効化タイマーを開始します。タイマーが期限切れになり、別のパスで再ルーティングできないために失敗したパスをヘッドエンドがまだ使用している場合、Null のルートがトラフィックとともに送信されないように、トンネル状態が「ダウン」になります。トンネルがダウンすると、トンネル上のサービスは、異なるパスを使用するために収束します。

次に手動の再最適化の例で出力されるサンプルを示します。この例では、パスオプションが **10** から **20** に変更されます。

```
Router# mpls traffic-eng reoptimize tunnel 1 path-option 20
The targeted path-option is not in lock down mode. Continue? [no]: yes
Router# show mpls traffic-eng tunnels tunnel1
Name: R1_t1 (Tunnel1) Destination: 10.6.6.6
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 20, (SEGMENT-ROUTING) type explicit IP_PATH (Basis for Setup)
  path option 10, (SEGMENT-ROUTING) type dynamic
Config Parameters:
  Bandwidth: 0 kbps (Global) Priority: 6 6 Affinity: 0x0/0xFFFF
  Metric Type: IGP (interface)
  Path Selection:
    Protection: any (default)
  Path-invalidation timeout: 45000 msec (default), Action: Tear
  AutoRoute: enabled LockDown: disabled Loadshare: 10 [200000000]
  auto-bw: disabled
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: explicit path option 20 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
History:
  Tunnel:
    Time since created: 6 days, 19 hours, 9 minutes
    Time since path change: 14 seconds
    Number of LSP IDs (Tun_Instances) used: 1819
    Current LSP: [ID: 1819]
    Uptime: 17 seconds
```

```

    Selection: reoptimization
  Prior LSP: [ID: 1818]
    ID: path option unknown
  Removal Trigger: reoptimization completed
Tun_Instance: 1819
Segment-Routing Path Info (isis level-1)
  Segment0[Node]: 10.4.4.4, Label: 114
  Segment1[Node]: 10.5.5.5, Label: 115
  Segment2[Node]: 10.6.6.6, Label: 116

```

ロックダウンオプション付き SR-TE

lockdown オプションは、SR-TE がより良いパスに再最適化することを防ぎます。ただし、新しいパスの存在をシグナリングすることは防げません。

```

interface Tunnel1
 ip unnumbered Loopback1
 tunnel mode mpls traffic-eng
 tunnel destination 10.6.6.6
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 6 6
 tunnel mpls traffic-eng path-option 10 segment-routing lockdown
 tunnel mpls traffic-eng path-selection metric igp
 tunnel mpls traffic-eng load-share 10 (Tunnel1) Destination:
10.6.6.6
 Status:
   Admin: up      Oper: up      Path: valid      Signalling: connected
   path option 10, (LOCKDOWN) type segment-routing (Basis for Setup)
 Config Parameters:
   Bandwidth: 0      kbps (Global) Priority: 6 6 Affinity: 0x0/0xFFFF
   Metric Type: IGP (interface)
   Path Selection:
     Protection: any (default)
     Path-invalidation timeout: 45000 msec (default), Action: Tear
     AutoRoute: enabled LockDown: enabled Loadshare: 10 [200000000]
     auto-bw: disabled
     Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
 Active Path Option Parameters:
   State: segment-routing path option 10 is active
   BandwidthOverride: disabled LockDown: enabled Verbatim: disabled
 History:
   Tunnel:
     Time since created: 6 days, 19 hours, 22 minutes
     Time since path change: 1 minutes, 26 seconds
     Number of LSP IDs (Tun_Instances) used: 1822
   Current LSP: [ID: 1822]
     Uptime: 1 minutes, 26 seconds
     Selection: reoptimization
   Prior LSP: [ID: 1821]
     ID: path option unknown
     Removal Trigger: configuration changed
 Tun_Instance: 1822
 Segment-Routing Path Info (isis level-1)
   Segment0[Node]: 10.6.6.6, Label: 116

```

SR-TE トンネル保護

SR TE トンネルの保護は、次のいずれかの代替手段で行うことができます。

IP-FRR ローカル修復保護

SR-TE LSP ヘッドエンドまたはミッドポイント ノードでは、IP-FRR はプレフィックス SID または隣接関係 SID ラベルのためのバックアップ保護パスを計算し、プログラムするのに使用されます。

IP-FRR を使用すると、バックアップ修復パスは、リンクまたはノードの障害が発生する前に IGP によって事前に計算されプログラムされます。リンクが失敗すると、TE トポロジからの即時の取り消し（リンクアダタイズメントの取り消し）がトリガーされます。これにより、ヘッドエンドは、失敗した隣接関係 SID を通過する SR-TE LSP の障害を検出することができます。

保護された隣接関係 SID が失敗した場合、失敗した隣接関係 SID ラベルとそれに関連する転送は、すべての SR-TE トンネルのヘッドエンドが障害を検出して対応できるように、指定した時間（5～15分）機能し続けます。隣接関係 SID ラベルを使用するトラフィックは、バックアップ修復パスを変更するその後のトポロジ更新がある場合でも、FRR 保護され続けます。この場合、IGP は FRR がアクティブになっている間にバックアップ修復パスを更新し、新しく計算されたバックアップパス上のトラフィックを再ルーティングします。

保護されたプレフィックス SID のプライマリ パスが失敗すると、PLR はバックアップパスに経路を再ルーティングします。ヘッドエンドは障害に対してトランスペアレントなままであり、引き続き SR-TE LSP を有効なパスとして使用します。

IP-FRR は、リンク障害に対してのみ隣接関係およびプレフィックス SID を保護します。

トンネルパス保護

パス保護とは、単一の TE トンネルのプライマリ LSP の障害から保護するために、1 つまたは複数のスタンバイ LSP をインスタンス化することです。

パス保護では、同じトンネルのプライマリパスオプションによってさまざまな障害のセカンダリパスを事前に計算し、事前プロビジョニングすることで、障害から保護します。この保護は、プライマリ LSP が通過するプレフィックス SID および隣接関係 SID を除外するパスを計算するか、またはプライマリ SR-TE LSP パスの SRLG を除外するパスを計算することによって実現します。

プライマリ SR-TE LSP に障害が発生した場合、トンネルには少なくとも 1 台のスタンバイ SR-TE LSP が使用されます。複数のセカンダリパスオプションをスタンバイ SR-TE LSP パスとして使用するように設定できます。

SR-TE LSP のパス検証

SR-TE トンネル機能では、ヘッドエンドがトンネルパスの初期検証と、その後のトンネルテールエンドおよび通過セグメントの到達可能性の追跡を実行する必要があります。

SR-TE LSP パスのパス検証は、トポロジの変更または SR SID の更新について MPLS-TE で通知されるたびにトリガーされます。

SR-TE LSP 検証手順は、以下のチェックで構成されています。

トポロジパスの検証

ヘッドエンドは、TE トポロジに対する接続性について SR-TE LSP のパスを検証します。MPLS-TEヘッドエンドは、隣接関係SIDに対応するリンクがTE トポロジで接続されているかどうかをチェックします。

新たにインスタンス化された SR-TE LSP の場合、ヘッドエンドが SR-TE パスの任意のリンクで不連続性を検出すると、そのパスは無効であると見なされ、使用されません。有効なパスを持つ他のパスオプションがトンネルにある場合、これらのパスを使用してトンネルLSPをインスタンス化します。

既存のインスタンス化された SR-TE LSP がある TE トンネルでは、ヘッドエンドがリンク上の不連続性を検出すると、ヘッドエンドはそのリンクで障害が発生したと見なします。この場合、IP FRR などのローカル修復保護が有効になります。隣接関係がしばらく失われた後、IGP は保護された隣接関係ラベルと関連付けられた転送を維持し続けます。これにより、同じ障害の影響を受けない別のパスにトンネルを再ルーティングするのに十分な時間が、ヘッドエンドで可能になります。ヘッドエンドは、リンク障害を検出した後、有効なパスを持つ他の使用可能パスオプションにトンネルの再ルーティングを試みるために、トンネル無効化タイマーを開始します。

TE トンネルが、障害の影響を受けない検証済みの他のパスオプションを使用して設定されている場合、ヘッドエンドは、これらのパスオプションの1つを使用して、影響を受けないパスを使用してトンネルの新しいプライマリ LSP をインスタンス化することによって、トンネルを再ルーティングします。

同じトンネルの下に他の有効なパスオプションが存在しない場合、または TE トンネルが障害の影響を受けるパスオプションを1つだけで設定されている場合、ヘッドエンドは無効タイマーを開始し、その後トンネルの状態を「ダウン」にします。このアクションにより、影響を受ける SR-TE LSP 上を流れるトラフィックとともに Null ルートが送信されるのを回避でき、トンネルを通過するサービスはヘッドエンドで利用できる異なるパスを経由して再ルーティングできるようになります。無効化ドロップ構成は、トンネルを「アップ」のままにしますが、無効化タイマーが満了したときにトラフィックをドロップします。

エリア内 SR-TE LSP では、ヘッドエンドは LSP パス上で完全な可視性を持ち、最終的な LSP 宛先へのパスを検証します。ただし、エリア間 LSP の場合、ヘッドエンドには LSP パスに対する部分的な可視性があります（最初の ABR までのみ）。この場合、ヘッドエンドは、入力から最初の ABR へのパスのみを検証できます。最初の ABR ノードを超える LSP に沿った障害は、ヘッドエンドからは見えず、LSP を介した BFD など、そのような障害を検出するその他のメカニズムが想定されます。

SR SID の検証

SR-TE LSP の SID ホップは TE トンネルの SR-TE LSP を介して運ばれる発信パケットに課される発信 MPLS ラベル スタックを決定するために使用されます。グローバルおよびローカルの隣接関係 SID のデータベースは、IGP から受信した情報から取り込まれ、MPLS-TE で維持されます。MPLS TE データベースで利用できない SID を使用すると、明示的パスを使用するパスオプションが無効になります。この場合、パスオプションは、SR TE LSP のインスタンス化には使用されません。また、MPLS の SID データベースで SID を取り消す、追加する、または

変更すると、MPLS-TE ヘッドエンドは、SR パスオプション（使用中またはセカンダリ）を持つすべてのトンネルを確認し、適切な処理を呼び出します。

LSP 出カインターフェイス

SR-TE LSP が最初のパス ホップの隣接関係の SID を使用するとき、TE は隣接関係 SID および SR-TE LSP が出力するノードに関連付けられているインターフェイス状態および IGP 隣接関係状態を監視します。インターフェイスまたは隣接関係がダウンした場合、TE は SR-TE LSP パスで障害が発生したと仮定し、前のセクションで説明したのと同じリアクティブアクションを実行できます。



Note SR-TE LSP が最初のホップのプレフィックス SID を使用するとき、TE はトンネルが出力するインターフェイスを直接推測できません。TE は、プレフィックスの IP 到達可能性情報に基づいて、最初のホップへの接続が維持されるかどうかを判断します。

IP 到達可能性の検証

MPLS-TE では、SR パスを有効と宣言する前に、プレフィックス SID に対応するノードが IP 到達可能であることを検証します。MPLS-TE は、SR-TE LSP パスの隣接関係またはプレフィックス SID に対応する IP プレフィックスのパス変更を検出します。リンクまたはノードの障害が原因で、特定の SID をアナウンスするノードが IP の到達可能性を失う場合、MPLS-TE はパス変更（パスなし）の通知を受けます。MPLS-TE は、現在の SR-TE LSP パスを無効にすることによって反応し、もしあれば有効なパスを持つ他のパスオプションを使用して新しい SR-TE LSP をインスタンス化する場合があります。



Note IP-FRR は（SR-TE LSP パスに沿ったプレフィックス SID の失敗など）SR-TE LSP が通過しているノードの障害に対する保護を提供しないため、ヘッドエンドは、トンネル状態を「ダウン」に設定することによってプレフィックス SID ノードの IP ルートの到達可能性の損失にすぐに反応し、影響を受けるトンネルに対して有効なパスを持つパスオプションが他にない場合は、トンネル転送エントリを削除します。

トンネルパス リソース回避の検証

SR-TE トンネルパケットの通過から除外されたことを検証するアドレスのセットを指定できます。これを実現するために、ヘッドエンドはセグメントごとの検証チェックを実行し、指定されたノード、プレフィックス、またはリンクアドレスが SR パスのトンネルから実際に除外されていることを検証します。以下のコマンドを使用して、トンネルリソース回避チェックをパスごとに有効にすることができます。除外されるアドレスのリストが定義され、リストの名前がパスオプションで参照されます。

```
interface tunnel100
 tunnel mpls traffic-eng path-option 1 explicit name EXCLUDE segment-routing
 ip explicit-path name EXCLUDE enable
```

```
exclude-address 192.168.0.2
exclude-address 192.168.0.4
exclude-address 192.168.0.3
!
```

SR-TE LSPの明示的ヌル

MPLS-TEトンネルのヘッドエンドは、スタックの最下部に明示的ヌルを課しません。penultimate hop popping (PHP) が SR プレフィックス SID に対して有効になっている場合、または隣接関係 SID が SR-TE LSP の最後のホップである場合、パケットはトランスポートラベルなしでテールエンドに到着する可能性があります。ただし、場合によっては、パケットが明示的ヌルラベルでテールエンドに到着することが望ましいため、このような場合、ヘッドエンドはラベルスタックの最上部に明示的ヌルラベルを課することになります。

Verbatim パス サポート

通常、MPLS TE LSP を使用する場合は、ネットワーク内のすべてのノードで TE の IGP 拡張がサポートされていて、TE が認識されるように設定されている必要があります。ただし、TE の IGP 拡張をサポートしないが、TE の RSVP 拡張はサポートするノードを通過する TE LSP を構築する機能を必要とするネットワーク管理者もいます。Verbatim LSP は、ネットワーク内のすべてまたは一部の中間ノードで TE の IGP 拡張がサポートされていない場合に役立ちます。

この機能をイネーブルにすると、IP 明示パスの TE トポロジデータベースに対するチェックは行われません。TE トポロジデータベースの検証が行われなかったため、IP 明示パス情報を持つ Path メッセージは、IP ルーティング用の Shortest Path First (SPF) アルゴリズムを使用してルーティングされます。

OSPFのセグメントルーティングトラフィックエンジニアリングの設定方法

次の手順を実行して、OSPF でのセグメントルーティングトラフィックエンジニアリングを設定します。

OSPFのセグメントルーティングトラフィックエンジニアリングの有効化

OSPF セグメントルーティングトラフィックエンジニアリングは、mpls トラフィックエンジニアリングとともにセグメントルーティングが有効になっている場合に有効になります。エリア内で SR と MPLS TE を有効にした場合、そのエリア内で SR-TE のサポートがオンになります。

```
router ospf 10
router-id 10.10.10.2
segment-routing mpls
mpls traffic-eng area 0
```

TE トンネルのパスオプションの設定

稼働中の SR トンネルのパスオプションタイプが SR から非 SR（たとえば **dynamic**）に変更されると、トンネルの既存の転送エントリが削除されます。

セグメントルーティングは、既存のセカンダリまたは使用中のパスオプションで有効または無効にすることができます。トンネルでシグナリングされた **RSVP-TE** の明示的パスオプションが使用され、そのトンネルでセグメントルーティングが有効になっている場合、**RSVP-TE LSP** は切断され、**SR-TE LSP** が同じパスオプションを使用してインスタンス化されます。逆に、プライマリ **LSP** によって使用されているパスオプションでセグメントルーティングが無効になっている場合、トンネルは断続的にダウンし、新しい **RSVP-TE LSP** は同じ明示的パスを使用してシグナリングされます。

セグメントルーティングパスオプションがセカンダリパスオプションで有効になっている（すなわち、トンネルのプライマリ **LSP** によって使用されていない）場合、新しく指定された **SR-TE LSP** パスオプションが有効で、トンネルのプライマリ **LSP** に使用するのがより有利であるかどうかを評価するためにトンネルがチェックされます。

```
Device(config)# interface tunnel 100
Device(config-if)# tunnel mpls traffic-eng path-option 1 explicit name foo segment-routing
Device(config-if)# tunnel mpls traffic-eng path-option 2 dynamic segment-routing
Device(config-if)# tunnel mpls traffic-eng path-option 3 segment-routing
```

SR 明示パス ホップの設定

SR-TE では次の明示的パスホップがサポートされています。

- IP アドレス
- MPLS ラベル
- IP アドレスと MPLS ラベルの混在

エリア内 **LSP** では、明示的パスを IP アドレスのリストとして指定できます。

```
Device(config)# ip explicit-path name foo
Device(config-ip-expl-path)# index 10 next-address 10.1.1.1 node address
Device(config-ip-expl-path)# index 20 next-address 10.12.12.2 link address
```



Note IP アンナウンサードインターフェイスを使用する場合、ネクストホップアドレスを明示的パスのインデックスとして指定することはできません。これは、ノードアドレスまたはラベルである必要があります。

明示的パスは、セグメントルーティング **SID** として指定することもできます。

```
Device(config)# ip explicit-path name foo
Device(config-ip-expl-path)# index 10 next-label 20
```

トンネルパスアフィニティの検証の設定

トンネルパスのアフィニティは、トンネルインターフェイスで **tunnel mpls traffic-eng affinity** コマンドを使用して指定することができます。

ヘッドエンドは、指定されたSRパスが設定されたアフィニティに準拠していることを検証します。これにより、SRパスの各セグメントのパスは、指定された制約に照らして検証される必要があります。パスの少なくとも1つのセグメントが設定されているアフィニティを満たさない場合、そのパスは設定されているアフィニティ制約に対して無効として宣言されます。

```
interface Tunnell
no ip address
tunnel mode mpls traffic-eng
tunnel destination 10.5.5.5
tunnel mpls traffic-eng priority 5 5
tunnel mpls traffic-eng bandwidth 100
tunnel mpls traffic-eng affinity 0x1 mask 0xFFFF
tunnel mpls traffic-eng path-option 10 dynamic segment-routing
Router# show tunnel ??
Name: R1_t1                               (Tunnell) Destination: 10.5.5.5
Status:
  Admin: up          Oper: up          Path: valid          Signalling: connected
  path option 10, (SEGMENT-ROUTING) type dynamic (Basis for Setup, path weight 20)
Config Parameters:
  Bandwidth: 100      kbps (Global) Priority: 5 5  Affinity: 0x1/0xFFFF
  Metric Type: TE (default)
  Path Selection:
    Protection: any (default)
  Path-selection Tiebreaker:
    Global: not set Tunnel Specific: not set Effective: min-fill (default)
  Hop Limit: disabled
  Cost Limit: disabled
  Path-invalidation timeout: 10000 msec (default), Action: Tear
  AutoRoute: disabled LockDown: disabled Loadshare: 100 [0] bw-based
  auto-bw: disabled
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: dynamic path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
Node Hop Count: 2
History:
  Tunnel:
    Time since created: 10 minutes, 54 seconds
    Time since path change: 34 seconds
    Number of LSP IDs (Tun_Instances) used: 55
  Current LSP: [ID: 55]
    Uptime: 34 seconds
  Prior LSP: [ID: 49]
    ID: path option unknown
    Removal Trigger: tunnel shutdown
Tun_Instance: 55
Segment-Routing Path Info (isis level-1)
  Segment0[Link]: 192.168.2.1 - 192.168.2.2, Label: 46
  Segment1[Link]: 192.168.4.2 - 192.168.4.1, Label: 49
```

インターフェイスのアフィニティの設定

インターフェイスでアフィニティを設定するには、次の手順を実行します。

```
interface GigabitEthernet2
ip address 192.168.2.1 255.255.255.0
ip router isis 1
negotiation auto
mpls traffic-eng tunnels
mpls traffic-eng attribute-flags 0x1
isis network point-to-point
ip rsvp bandwidth
```

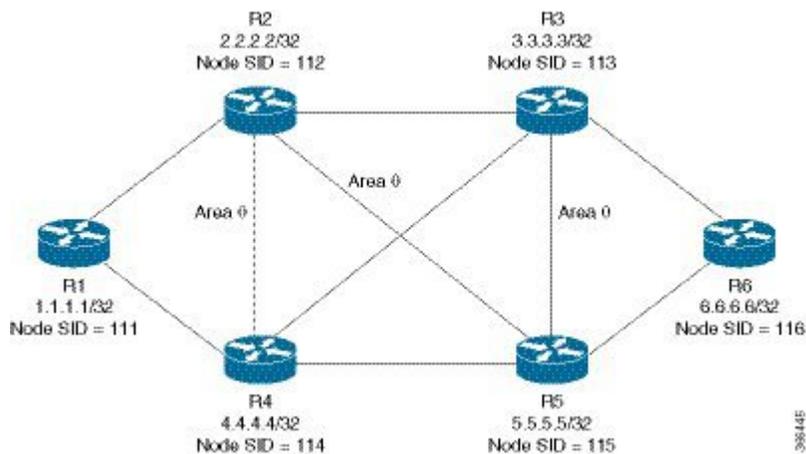
OSPFのセグメントルーティングトラフィックエンジニアリングの設定

OSPFでSR-TEを設定するには、次のエリア間およびエリア内の使用例を考慮してください。

エリア内トンネルの設定

エリア内トンネルを設定するには、次のトポロジを検討してください。

図 12: エリア内トンネル



すべてのルータは、同じエリアである、エリア 0 内で設定されています。

ヘッドエンドルータ R1 の構成

```
router ospf 10
fast-reroute per-prefix enable prefix-priority low
fast-reroute per-prefix ti-lfa
segment-routing mpls
mpls traffic-eng router-id Loopback1
mpls traffic-eng area 0

interface GigabitEthernet2 //interface connecting to the router 2
ip address 10.101.1.1 255.255.255.0
ip ospf 10 area 0
ip ospf network point-to-point
negotiation auto
mpls traffic-eng tunnels

interface GigabitEthernet4 //interface connecting to the router 4
ip address 10.101.1.1 255.255.255.0
```

明示パス SR-TE トンネル 1

```

ip ospf 10 area 0
ip ospf network point-to-point
negotiation auto
mpls traffic-eng tunnels

interface loopback1
ip address 10.1.1.1/32
ip ospf 10 area 0

```

テールエンド ルータ R6 の構成

```

router ospf 10
fast-reroute per-prefix enable prefix-priority low
fast-reroute per-prefix ti-lfa
segment-routing mpls
mpls traffic-eng area 0
mpls traffic-eng router-id Loopback1
interface GigabitEthernet2 //interface connecting to the router 3
ip address 10.101.2.1 255.255.255.0
ip ospf 10 area 0
ip ospf network point-to-point
negotiation auto
mpls traffic-eng tunnels

interface GigabitEthernet4 //interface connecting to the router 5
ip address 10.101.2.1 255.255.255.0
ip ospf 10 area 0
ip ospf network point-to-point
negotiation auto
mpls traffic-eng tunnels

interface loopback1
ip address 10.6.6.6/32
ip ospf 10 area 0

```

明示パス SR-TE トンネル 1

トンネル 1 を IP アドレスのみに基づいて考慮します。

```

ip explicit-path name IP_PATH1
next-address 10.2.2.2
next-address 10.3.3.3
next-address 10.6.6.6
!
interface Tunnel1
ip unnumbered Loopback1
tunnel mode mpls traffic-eng
tunnel destination 10.6.6.6
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 6 6
tunnel mpls traffic-eng path-option 10 explicit name IP_PATH1 segment-routing
tunnel mpls traffic-eng path-selection metric igp
tunnel mpls traffic-eng load-share 10
end

```

明示パス SR-TE トンネル 2

トンネル 2 をノードの SID に基づいて考慮します

```

ip explicit-path name IA_PATH
next-label 114
next-label 115

```

```

next-label 116
!
interface Tunnel2
 ip unnumbered Loopback1
 tunnel mode mpls traffic-eng
 tunnel destination 10.6.6.6
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 6 6
 tunnel mpls traffic-eng bandwidth 10000 class-type 1
 tunnel mpls traffic-eng path-option 10 explicit name IA_PATH segment-routing
 tunnel mpls traffic-eng path-selection metric igp
 tunnel mpls traffic-eng load-share 10
end

```

明示パス SR-TE トンネル 3

トンネル 3 は IP アドレスとラベルの組み合わせに基づいていることを考慮します

```

ip explicit-path name MIXED_PATH enable
next-address 10.2.2.2
next-address 10.3.3.3
next-label 115
next-label 116
!
interface Tunnel3
 ip unnumbered Loopback1
 tunnel mode mpls traffic-eng
 tunnel destination 10.6.6.6
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 6 6
 tunnel mpls traffic-eng path-option 10 explicit name MIXED_PATH segment-routing
 tunnel mpls traffic-eng path-selection metric igp
 tunnel mpls traffic-eng load-share 10

```



Note パスが混在している場合、パスでノード SID を使用した後に IP ネクストホップを使用することはできません。次のパスは有効ではありません。

```

ip explicit-path name MIXED_PATH enable
next-label 115
next-label 116
next-address 10.2.2.2

```

動的パス SR-TE トンネル 4

トンネル 4is は隣接関係 SID に基づいていることを考慮します

```

interface Tunnel4
 ip unnumbered Loopback1
 tunnel mode mpls traffic-eng
 tunnel destination 10.6.6.6
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 6 6
 tunnel mpls traffic-eng bandwidth 10000 class-type 1
 tunnel mpls traffic-eng path-option 10 dynamic segment-routing
 tunnel mpls traffic-eng path-selection metric igp
 tunnel mpls traffic-eng load-share 10
end

```

動的パス SR-TE トンネル 5

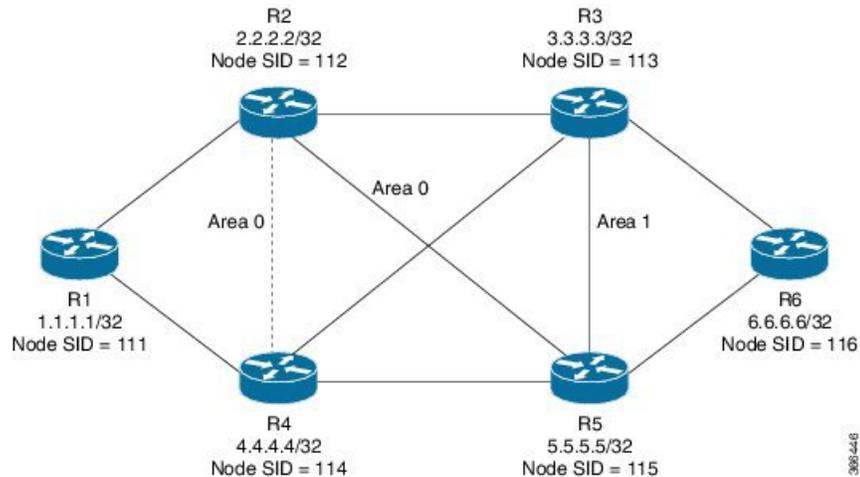
トンネル 5 はノード SID に基づいていることを考慮します

```
interface Tunnel5
ip unnumbered Loopback1
tunnel mode mpls traffic-eng
tunnel destination 10.6.6.6
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 6 6
tunnel mpls traffic-eng path-option 10 segment-routing
tunnel mpls traffic-eng path-selection metric igp
tunnel mpls traffic-eng load-share 10
```

エリア間トンネルの設定

エリア間トンネルを設定するには、次のトポロジを検討してください。

図 13: エリア間トンネル



エリア 1 内で設定されている R6 を除き、すべてのルータは同エリアであるエリア 0 内で設定されています。

ヘッドエンド ルータ R1 の構成

```
router ospf 10
fast-reroute per-prefix enable prefix-priority low
fast-reroute per-prefix ti-lfa
segment-routing mpls
mpls traffic-eng router-id Loopback1
mpls traffic-eng area 0

interface GigabitEthernet2 //interface connecting to the router 2
ip address 10.101.1.1 255.255.255.0
ip ospf 10 area 0
ip ospf network point-to-point
negotiation auto
mpls traffic-eng tunnels

interface GigabitEthernet4 //interface connecting to the router 4
ip address 10.101.1.1 255.255.255.0
```

```

ip ospf 10 area 0
ip ospf network point-to-point
negotiation auto
mpls traffic-eng tunnels

interface loopback1
ip address 10.1.1.1/32
ip ospf 10 area 0

```

テールエンド ルータ R6 の構成

```

router ospf 10
fast-reroute per-prefix enable prefix-priority low
fast-reroute per-prefix ti-lfa
segment-routing mpls
mpls traffic-eng area 1
mpls traffic-eng router-id Loopback1
interface GigabitEthernet2 //interface connecting to the router 3
ip address 10.101.2.1 255.255.255.0
ip ospf 10 area 1
ip ospf network point-to-point
negotiation auto
mpls traffic-eng tunnels

interface GigabitEthernet4 //interface connecting to the router 5
ip address 10.101.2.1 255.255.255.0
ip ospf 10 area 1
ip ospf network point-to-point
negotiation auto
mpls traffic-eng tunnels

interface loopback1
ip address 10.6.6.6/32
ip ospf 10 area 1

```

エリア間トンネルの設定に関する制約事項

エリア間トンネルの設定に関する制約事項は次のとおりです。

- ノードおよび隣接関係 SID を持つ動的オプションはサポートされていません。
- ラベルのみおよび/または IP アドレスとラベルを含む明示的パスを使用して、エリア間トンネルを設定できます。



(注) IPアドレスは、エリア境界ルータ (ABR) までのみ使用でき、その後はラベルのみを指定する必要があります。

明示パス SR-TE トンネル 1

トンネル 2 はノード SID に基づいていることを考慮します。

```

ip explicit-path name IA_PATH
next-label 114
next-label 115
next-label 116
!

```

```

interface Tunnel2
ip unnumbered Loopback1
tunnel mode mpls traffic-eng
tunnel destination 10.6.6.6
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 6 6
tunnel mpls traffic-eng bandwidth 10000 class-type 1
tunnel mpls traffic-eng path-option 10 explicit name NODE_PATH segment-routing
tunnel mpls traffic-eng path-selection metric igp
tunnel mpls traffic-eng load-share 10
end

```

明示パス SR-TE トンネル 2

トンネル 3 は IP アドレスとラベルの組み合わせに基づいていることを考慮します。

```

ip explicit-path name MIXED_PATH enable
next-address 10.2.2.2
next-address 10.3.3.3
next-label 115
next-label 116
!

interface Tunnel3
ip unnumbered Loopback1
tunnel mode mpls traffic-eng
tunnel destination 10.6.6.6
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 6 6
tunnel mpls traffic-eng path-option 10 explicit name MIXED_PATH segment-routing
tunnel mpls traffic-eng path-selection metric igp
tunnel mpls traffic-eng load-share 10

```

SR-TE トンネルの構成の確認

show mpls traffic-eng tunnels *tunnel-number* コマンドを使用して、SR-TE トンネルの構成を確認します。

トンネル 1 の確認

```

Name: R1_t1                               (Tunnel1) Destination: 10.6.6.6
Status:
  Admin: up          Oper: up          Path: valid          Signalling: connected
  path option 10, (SEGMENT-ROUTING) type explicit IP_PATH (Basis for Setup)
Config Parameters:
  Bandwidth: 0          kbps (Global) Priority: 6 6  Affinity: 0x0/0xFFFF
  Metric Type: IGP (interface)
  Path Selection:
    Protection: any (default)
  Path-invalidation timeout: 45000 msec (default), Action: Tear
  AutoRoute: enabled  LockDown: disabled Loadshare: 10 [200000000]
  auto-bw: disabled
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled

```

```

History:
  Tunnel:
    Time since created: 6 days, 19 hours
    Time since path change: 2 seconds
    Number of LSP IDs (Tun_Instances) used: 1814
    Current LSP: [ID: 1814]
    Uptime: 2 seconds
    Selection: reoptimization
    Prior LSP: [ID: 1813]
    ID: path option unknown
    Removal Trigger: configuration changed
  Tun_Instance: 1814
Segment-Routing Path Info (ospf 10 area 0)
  Segment0[Node]: 10.4.4.4, Label: 114
  Segment1[Node]: 10.5.5.5, Label: 115
  Segment2[Node]: 10.6.6.6, Label: 116

```

.

トンネル2の確認

```

Name: R1_t2                               (Tunnel) Destination: 10.6.6.6
Status:
  Admin: up           Oper: up           Path: valid           Signalling: connected
  path option 10, (SEGMENT-ROUTING) type explicit IA_PATH (Basis for Setup)
Config Parameters:
  Bandwidth: 0           kbps (Global) Priority: 6 6 Affinity: 0x0/0xFFFF
  Metric Type: IGP (interface)
  Path Selection:
    Protection: any (default)
  Path-invalidation timeout: 45000 msec (default), Action: Tear
  AutoRoute: enabled LockDown: disabled Loadshare: 10 [200000000]
  auto-bw: disabled
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
History:
  Tunnel:
    Time since created: 6 days, 19 hours, 1 minutes
    Time since path change: 1 seconds
    Number of LSP IDs (Tun_Instances) used: 1815
    Current LSP: [ID: 1815]
    Uptime: 1 seconds
    Prior LSP: [ID: 1814]
    ID: path option unknown
    Removal Trigger: configuration changed
  Tun_Instance: 1815
Segment-Routing Path Info (ospf 10 area 0)
  Segment0[ - ]: Label: 114
  Segment1[ - ]: Label: 115
  Segment2[ - ]: Label: 116

```

トンネル3の確認

```

Name: R1_t3                               (Tunnel) Destination: 10.6.6.6
Status:
  Admin: up           Oper: up           Path: valid           Signalling: connected
  path option 10, (SEGMENT-ROUTING) type explicit MIXED_PATH (Basis for Setup)

```

```

Config Parameters:
  Bandwidth: 0          kbps (Global)  Priority: 6 6  Affinity: 0x0/0xFFFF
  Metric Type: IGP (interface)
  Path Selection:
    Protection: any (default)
  Path-invalidation timeout: 45000 msec (default), Action: Tear
  AutoRoute: enabled  LockDown: disabled Loadshare: 10 [200000000]
  auto-bw: disabled
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
History:
  Tunnel:
    Time since created: 6 days, 19 hours, 2 minutes
    Time since path change: 2 seconds
    Number of LSP IDs (Tun_Instances) used: 1816
  Current LSP: [ID: 1816]
    Uptime: 2 seconds
    Selection: reoptimization
  Prior LSP: [ID: 1815]
    ID: path option unknown
    Removal Trigger: configuration changed
Tun_Instance: 1816
Segment-Routing Path Info (ospf 10 area 0)
  Segment0[Node]: 10.2.2.2, Label: 112
  Segment1[Node]: 10.3.3.3, Label: 113
  Segment2[ - ]: Label: 115
  Segment3[ - ]: Label: 116

```

トンネル4の確認

```

Name: R1_t4          (Tunnel1) Destination: 10.6.6.6
Status:
  Admin: up          Oper: up          Path: valid          Signalling: connected
  path option 10, (SEGMENT-ROUTING) type dynamic (Basis for Setup, path weight 30)
Config Parameters:
  Bandwidth: 0          kbps (Global)  Priority: 6 6  Affinity: 0x0/0xFFFF
  Metric Type: IGP (interface)
  Path Selection:
    Protection: any (default)
  Path-invalidation timeout: 45000 msec (default), Action: Tear
  AutoRoute: enabled  LockDown: disabled Loadshare: 10 [200000000]
  auto-bw: disabled
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: dynamic path option 10 is active
  BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
History:
  Tunnel:
    Time since created: 6 days, 19 hours
    Time since path change: 2 seconds
    Number of LSP IDs (Tun_Instances) used: 1813
  Current LSP: [ID: 1813]
    Uptime: 2 seconds
  Prior LSP: [ID: 1806]
    ID: path option unknown
    Removal Trigger: configuration changed
Tun_Instance: 1813
Segment-Routing Path Info (ospf 10 area 0)
  Segment0[Link]: 192.168.2.1 - 192.168.2.2, Label: 17

```

```
Segment1[Link]: 192.168.4.2 - 192.168.4.1, Label: 25
Segment2[Link]: 192.168.8.1 - 192.168.8.2, Label: 300
```

トンネル5の確認

```
Name: R1_t5 (Tunnell) Destination: 10.6.6.6
Status:
  Admin: up      Oper: up      Path: valid      Signalling: connected
  path option 10, type segment-routing (Basis for Setup)
Config Parameters:
  Bandwidth: 0      kbps (Global) Priority: 6 6  Affinity: 0x0/0xFFFF
  Metric Type: IGP (interface)
  Path Selection:
    Protection: any (default)
  Path-invalidation timeout: 45000 msec (default), Action: Tear
  AutoRoute: enabled LockDown: disabled Loadshare: 10 [200000000]
  auto-bw: disabled
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: segment-routing path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
History:
  Tunnel:
    Time since created: 6 days, 19 hours, 4 minutes
    Time since path change: 14 seconds
    Number of LSP IDs (Tun_Instances) used: 1817
  Current LSP: [ID: 1817]
    Uptime: 14 seconds
    Selection: reoptimization
  Prior LSP: [ID: 1816]
    ID: path option unknown
    Removal Trigger: configuration changed
Tun_Instance: 1817
Segment-Routing Path Info (ospf 10 area 0)
  Segment0[Node]: 10.6.6.6, Label: 116
```




第 9 章

BGP ダイナミック セグメント ルーティング トラフィック エンジニアリング

ボーダー ゲートウェイ プロトコル (BGP) はデータセンター (DC) ネットワークのルーティングプロトコルとして一般的な選択となっています。BGPによって開始されるセグメントルーティングトラフィックエンジニアリング (SR-TE) パスを設定する機能により、DC ネットワークの動作が簡素化されます。

- [BGP ダイナミック セグメント ルーティング トラフィック エンジニアリングの機能情報 \(119 ページ\)](#)
- [セグメントルーティングの制約事項：トラフィック エンジニアリング ダイナミック BGP \(120 ページ\)](#)
- [セグメントルーティングに関する情報：トラフィック エンジニアリング ダイナミック BGP \(120 ページ\)](#)
- [TE ラベル スイッチドパス属性セットの設定方法 \(122 ページ\)](#)

BGP ダイナミック セグメント ルーティング トラフィック エンジニアリングの機能情報

表 7: BGP ダイナミック セグメントルーティングトラフィック エンジニアリングの機能情報

機能名	リリース	機能情報
BGP ダイナミック セグメントルーティング トラフィック エンジニアリング	Cisco IOS XE Amsterdam 17.3.2	BGP ダイナミック SR-TE では、定義済みの基準とポリシーが満たされると、ラベルスイッチドパス (LSP) がオンデマンドで有効になります。 次のコマンドが導入または変更されました。 mpls traffic-eng lsp attribute name

セグメントルーティングの制約事項：トラフィック エンジニアリング ダイナミック BGP

- エニーキャストの場合、BGP-TEを動作させるためにSIDサポートで前に付加（Prepend）機能を設定する必要があります。
- BGP ダイナミック SR-TE では、SR-TE で障害が発生した場合、フォワーディングが中断されます。

セグメントルーティングに関する情報：トラフィック エンジニアリング ダイナミック BGP

BGP ダイナミック SR-TE では、定義済みの基準とポリシーが満たされ、それが手動で有効になっている SR-TE と BGP ダイナミック SR-TE 間の主な違いである場合、ラベル スイッチドパス（LSP）がオンデマンドで有効になります。たとえば、低遅延パス、最小コストパスなどのポリシーは、BGPによって伝送され、特定の顧客プレフィックスで一致します。自動検出とシグナリングのためにBGPを使用するL3VPNまたは仮想プライベートLANサービス（VPLS）に使用されるSR-TE トンネルは、BGP-TE ダイナミックと呼ばれます。

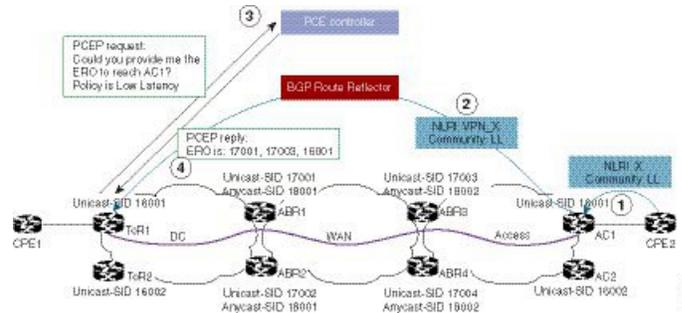
BGP SR-TE ダイナミックは、オンデマンドの自動トンネルが単一のIGP ドメインに存在することを前提としています。この場合、パスの計算はIGPを介して行われます。BGPからの要求に基づいて作成されたSR-TE自動トンネルはダイナミックSR-TEトンネルです。つまり、トンネルパス情報またはラベルスタックが、BGPネクストホップおよびTE属性設定に基づいて計算されます。BGPダイナミックSR-TEは、オンデマンドLSP（自動トンネル）をトリガーする機能を備えています。機能は次のとおりです。

- ルートマップ設定を介してコミュニティ（コミュニティリスト）を使用して、顧客プレフィックス（IPv4 または L3VPN VRF）にタグを付けます。
- 各コミュニティをTEの属性セットまたはプロファイルに関連付けます。

SR-TE プロファイルは、遅延、分離パスなどの特定のSR-TEパラメータを定義するために、属性設定でローカルに設定されます。BGP顧客プレフィックスがSR-TEプロファイルにマップされると、プレフィックスと関連付けられている指定された各BGPネクストホップおよび属性セットのペアに対して、属性セットで定義されたパラメータを使用してトンネルが動的に作成されます（自動トンネルまたはオンデマンドラベルスイッチドパス（LSP））。バインディングSIDは、各SR-TE自動トンネルに関連付けられていて、BGPに渡されます。バインディングSIDまたはバインディングラベルは、ルーティング情報ベース（RIB）および転送情報ベース（FIB）にインストールされます。FIBは、オンデマンドSR-TE自動トンネルを経由して転送するバインディングSIDまたはバインディングラベルによってBGPパスを解決します。バインディングSIDは、SR-TE LSP上の顧客トラフィックを制御するためにも使用されます。

BGP はこの場合は SR-TE ポリシーのみを伝送し、パスの計算は単一の IGP ドメインで IGP を介して行われることに注意する必要があります。単一の IGP ドメインでは、ヘッドエンドノードはエンドツーエンドパスとトポロジエンジニアリング データベース（トラフィック エンジニアリング データベースまたは TED）の完全な可視性を持っています。また、BGP 動的 SR-TE ですべてのノードが単一の AS と単一の IGP ドメイン内に存在することを前提とします。

図 14: BGP-TE ダイナミック ワークフロー



上の図は、複数のルーティング ドメインを使用した BGP-TE ダイナミック ワークフローの使用例を示しています。

1. 顧客宅内機器 2 (CPE) は、プレフィックス X に対して BGP アップデートを送信し、LL コミュニティ (100:333 など) を追加します。
2. AC1 は LL コミュニティを持つプレフィックス X のための VPN ルートをアナウンスします。
3. VPN ルート マッチング コミュニティ LL の BGP アップデートを受信した後、ToR1 は低遅延の TE ポリシーを使用して AC1 に向かう LSP パスに対して PCE コントローラに要求を送信します。
4. パス計算要素 (PCE) コントローラは、ラベルスタックで応答します (たとえば、17003、1600)。
5. ToR1 は SR-TE 自動トンネルを作成し、この VPN の VRF のプレフィックス X のためのルートをインストールします。

TE ラベルスイッチドパス属性セット

TE-LSP 属性セットは、LSP のプロパティを設定するために使用されます。これは、オートトンネルを作成するために使用される、帯域幅、アフィニティの包含と除外、リンク/ノード/SRLG の包含と除外、メトリック、パスの分離度、グループなどの TE プロファイルまたはポリシーについて記述します。

TE ラベルスイッチドパス属性セットの設定方法

TE ラベルスイッチドパス属性セットの設定

コマンド `mpls traffic-eng lsp attribute <name>` を使用して、TE-LSP 属性を設定することができます。次のオプションを使用できます。

```
Mpls traffic-eng lsp attribute name
  affinity          Specify attribute flags for links comprising LSP
  lockdown         Lockdown the LSP--disable reoptimization
  priority         Specify LSP priority
```

TE-LSP 属性コマンドは、拡張して2つのオプション `pce` と `path-selection` の設定をサポートすることができます。次のように設定できます。

```
mpls traffic-eng lsp attribute name <test>
  path-selection
    metric <te/igp>
    invalidation <time-out> <drop/tear>
    segment-routing adjacency <protected/unprotected>
```

- `pce` オプションが TE 属性で設定されている場合、ダイナミック パスは `pce` によって計算されます。それ以外の場合、パスは TE PCALC (パス計算) エンティティによってローカルに計算されます。後者の場合、IGP を設定する必要があり、BGP ネクストホップが IGP によってアドバタイズされ、IGP ルートを経由してローカルノードから到達可能である必要があります。
- オプションの `path-selection` メトリックは、パスの計算が TE のメトリックまたは IGP メトリックに基づいているかどうかを示します。このオプションが設定されていない場合は、`mpls traffic-eng path-selection` メトリックで設定されたグローバル値が使われます。
- オプションの `path-selection invalidation` は、LSP がネットワークからのソフト障害にどのように反応するかを設定します。LSP パスにリンクまたはノード障害に対する IGP からの保護パスがある場合、リンクまたはノードへの障害はソフト障害と見なされます。
- オプション `path-selection segment-routing adjacency` は、LSP ラベルスタックを計算する際に、IGP 保護の有無にかかわらず隣接関係 SID を選択するかどうかを示します。
- オプション `pce disjoint-path` は、トンネル LSP が `disjoint-path` グループのメンバーであることを示します。同じ `disjoint-path` グループ内の LSP は、そのパス内のリンク、ノード、または SRLG などの同じリソースを通過しません。これは、分離パスを持つ2つ以上のトンネル LSP を作成するために使用されます。

BGP-TE ダイナミックの場合、TE 属性名は次のように BGP ルートマップセット拡張に関連付けられます。

```
route-map <name>
  match community <name>
    set attribute-set <name>
```

BGP は文字列 **attribute-set** *<name>* をその BGP ネクストホップとともに使用して、SR-TE 自動トンネルを要求します。



第 10 章

L3/L3VPN 用のセグメントルーティング オンデマンドネクストホップ

ドメイン全体にルーティング情報を再配布すると、マルチドメインサービス（L2VPN と L3VPN）のプロビジョニングにそれ自体の複雑性と拡張性の問題が発生します。オンデマンドネクストホップ（ODN）は、再配布を行わずに制約やポリシーなど、PCE コントローラへのエンドツーエンド LSP の計算の委任をトリガーします。次に、サービスが Forwarding Information Base（FIB）へ移行する間に応答されたマルチドメイン LSP をインストールします。

- [L3/L3VPN のセグメントルーティング オンデマンドネクストホップに関する機能情報（125 ページ）](#)
- [L3/L3VPN のセグメントルーティング オンデマンド SR PFP ODN 自動ステアリング（PCE 委任）に関する制約事項（126 ページ）](#)
- [L3/L3VPN のセグメントルーティング オンデマンド SR PFP ODN 自動ステアリング（PCE 委任）に関する情報（126 ページ）](#)
- [L3/L3VPN のセグメントルーティング オンデマンドネクストホップの設定方法（127 ページ）](#)
- [L3/L3VPN のセグメントルーティング オンデマンドネクストホップの確認（131 ページ）](#)

L3/L3VPN のセグメントルーティング オンデマンドネクストホップに関する機能情報

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、<https://cfng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

表 8: L3/L3VPN のセグメントルーティング オンデマンドネクストホップに関する機能情報

機能名	リリース	機能情報
L3/L3VPN用のセグメントルーティング オンデマンドネクストホップ	Cisco IOS XE Amsterdam 17.3.2	<p>オンデマンドネクストホップ (ODN) は、再配布を行わずに制約やポリシーなど、PCE コントローラへのエンドツーエンド LSP の計算の委任をトリガーします。</p> <p>次のコマンドが導入または変更されました。</p> <p>route-map BGP_TE_MAP permit、mpls traffic-eng tunnels、sh bgp li li summary、sh pce client peer、sh pce ipv4 peer、sh ip route vrf sr、sh ip bgp vpnv4 vrf sr、sh ip cef label-table、sh mpls traffic-eng tunnels、sh pce client lsp brief、sh pce lsp summ、sh pce lsp det、routing-default-optimize</p>

L3/L3VPN のセグメントルーティング オンデマンド SR PFP ODN 自動ステアリング (PCE 委任) に関する制約事項

- オンデマンドネクストホップ (ODN) エニーキャスト SID はサポートされていません。
 - IPv6 の ODN はサポートされていません。
 - SR ODN トンネルは、BGP ノンストップルーティング (NSR) ではサポートされていません。BGP ノンストップフォワーディング (NSF) でのみサポートされています。
- BGP NSF を有効にするには、次のコマンドを使用します。

```

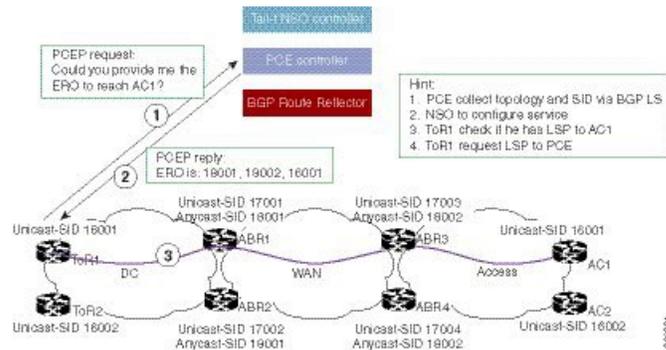
bgp grace-full restart
neighbor 10.0.0.2 ha-mode graceful-restart

```

L3/L3VPN のセグメントルーティング オンデマンド SR PFP ODN 自動ステアリング (PCE 委任) に関する情報

オンデマンドの SR PFP ODN 自動ステアリング (PCE 委任) は、BGP ダイナミック SR-TE 機能を活用し、要件に基づいてエンドツーエンドパスを検索しダウンロードするパス計算 (PCE) 機能を追加します。ODN は定義された BGP ポリシーに基づいて SR-TE 自動トンネルをトリガーします。下の図に示すように、ToR1 と AC1 間のエンドツーエンドパスは、低遅延あるいは VRF (L3VPN) または IPv4 サービスの他の基準に基づいて両端から確立できます。ODN のワークフローは次のようにまとめられます。

図 15: ODN 操作



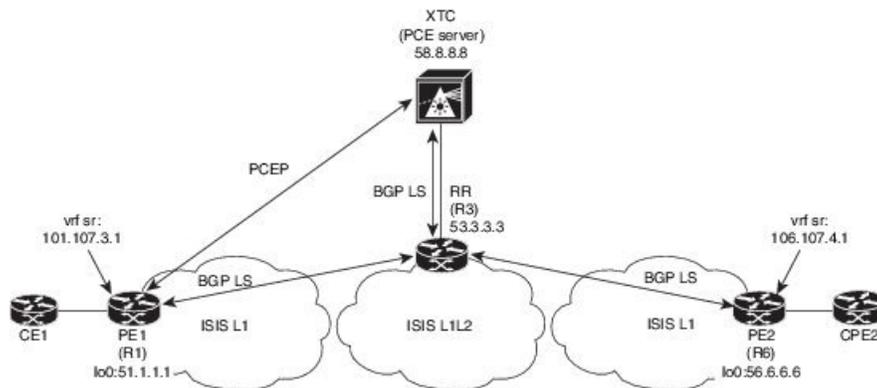
1. PCE コントローラは、BGP リンク ステート (BGP-LS) を介してトポロジと SID の情報を収集します。BGP-LS の詳細については、「[BGP Link-State](#)」を参照してください。
2. NSO コントローラが有効になっている場合、L3VPN VRF または IPv4 プレフィックスが設定され、要求が ToR1 および AC1 に送信されます。
3. ToR1 と AC1 は、お互いに対する LSP が存在するかどうかをチェックします。ない場合は、PCE コントローラに要求が送信され、BGP 経由で伝送される SR-TE ポリシーに一致する SR-TE パスが計算されます。
4. PCE コントローラはパスを計算し、ラベルスタック (ToR1 の例では 18001、18002、16001) で応答します。
5. ToR1 と AC1 は、SR-TE の自動トンネルを作成し、VRF または IPv4 用の LSP がアップであり稼働中であることを示す返信を NSO コントローラに返します。

L3/L3VPN のセグメント ルーティング オン デマンド ネクスト ホップ の設定方法

L3/L3VPN のセグメント ルーティング オン デマンド ネクスト ホップ の設定

SR-TE のオンデマンドネクストホップを設定するには、次のステップを実行します。設定ステップを説明するため、次の図を参考として使用します。

図 16: ODN 自動トンネル セットアップ



1. VRF インターフェイスを使用してルータ (R6 テールエンド) を設定します。

```
interface GigabitEthernet0/2/2
 vrf forwarding sr
 ip address 10.0.0.1 255.0.0.0
 negotiation auto
```

```
interface Loopback0
 ip address 192.168.0.1 255.255.0.0
 ip router isis 1
```

2. R6 (テールエンド) での BGP コミュニティを持つ VRF プレフィックスをタグ付けします。

```
route-map BGP_TE_MAP permit 9
 match ip address traffic
 set community 3276850
```

```
ip access-list extended traffic
 permit ip 10.0.0.1 255.255.0.0 any
```

3. R6 (テールエンド) および R1 (ヘッドエンド) 上の BGP を有効にして VRF SR プレフィックスをアドバタイズおよび受信し、R6 (テールエンド) 上のコミュニティ設定で一致させます。

```
router bgp 100
 bgp router-id 172.16.0.1
 bgp log-neighbor-changes
 bgp graceful-restart
 no bgp default ipv4-unicast
 neighbor 10.0.0.2 remote-as 100
 neighbor 10.0.0.2 update-source Loopback0
```

```
address-family ipv4
 neighbor 10.0.0.2 activate
 neighbor 10.0.0.2 send-community both
 neighbor 10.0.0.2 next-hop-self
 exit-address-family
```

```
address-family vpnv4
 neighbor 10.0.0.2 activate
 neighbor 10.0.0.2 send-community both
```

```
neighbor 10.0.0.2 route-map BGP_TE_MAP out
exit-address-family

address-family link-state link-state
neighbor 10.0.0.2 activate
exit-address-family

address-family ipv4 vrf sr
redistribute connected
exit-address-family

route-map BGP_TE_MAP permit 9
match ip address traffic
set community 3276850

ip access-list extended traffic
permit ip 10.0.0.1 255.255.0.0 any

router bgp 100
bgp router-id 192.168.0.2
bgp log-neighbor-changes
bgp graceful-restart
no bgp default ipv4-unicast
neighbor 10.0.0.2 remote-as 100
neighbor 10.0.0.2 update-source Loopback0

address-family ipv4
neighbor 10.0.0.2 activate
neighbor 10.0.0.2 send-community both
neighbor 10.0.0.2 next-hop-self
exit-address-family

address-family vpnv4
neighbor 10.0.0.2 activate
neighbor 10.0.0.2 send-community both
neighbor 10.0.0.2 route-map BGP_TE_MAP in
exit-address-family

address-family link-state link-state
neighbor 10.0.0.2 activate
exit-address-family

address-family ipv4 vrf sr
redistribute connected
exit-address-family

route-map BGP_TE_MAP permit 9
match community 1
set attribute-set BGP_TE5555

ip community-list 1 permit 3276850

mpls traffic-eng lsp attributes BGP_TE5555
path-selection metric igp
pce
```

4. R1 で PCE および自動トンネル設定を有効にします。

```
mpls traffic-eng tunnels
mpls traffic-eng pcc peer 10.0.0.3 source 10.0.0.4 precedence 255
mpls traffic-eng auto-tunnel p2p tunnel-num min 2000 max 5000
```

5. SR-TE 構成ですべてのコアリンクを有効にし、ポイントツーポイントインターフェイスとして有効になっていることを確認します。

```

mpls traffic-eng tunnels

interface GigabitEthernet0/2/0
 ip address 10.102.6.1 255.255.255.0
 ip router isis 1
 mpls traffic-eng tunnels
 isis network point-to-point

interface GigabitEthernet0/3/1
 vrf forwarding sr
 ip address 10.107.3.1 255.255.255.0
 negotiation auto

end

```

6. R3 (RR) を有効にして、BGP-LS によって TED を PCE サーバーにアドバタイズします。

```

router isis 1
 net 49.0002.0000.0000.0003.00
 ispf level-1-2
 metric-style wide
 nsf cisco
 nsf interval 0
 distribute link-state
 segment-routing mpls
 segment-routing prefix-sid-map advertise-local
 redistribute static ip level-1-2
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-1
 mpls traffic-eng level-2

router bgp 100
 bgp router-id 10.0.0.2
 bgp log-neighbor-changes
 bgp graceful-restart
 no bgp default ipv4-unicast
 neighbor 10.0.0.3 remote-as 100
 neighbor 10.0.0.3 update-source Loopback0

address-family ipv4
 neighbor 10.0.0.3 activate
 exit-address-family

```

7. PCE サーバーの設定を有効にし、RR によって BGP-LS セッションが正しく確立されていることを確認します。

```

Device# sh bgp li li summary
BGP router identifier 10.0.0.3, local AS number 100
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0 RD version: 1436
BGP main routing table version 1436
BGP NSR Initial initsync version 1 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs
BGP is operating in STANDALONE mode.
Process      RcvTblVer  bRIB/RIB  LabelVer  ImportVer  SendTblVer  StandbyVer
Speaker      1436      1436      1436      1436      1436      1436
0

```

```

Neighbor      Spk    AS MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down  St/PfxRcd
10.0.0.2      0      100  19923     17437   1436    0    0
 1w2d        103

Device# sh pce ipv4 topo | b Node 3
Node 3
  TE router ID: 10.0.0.2
  Host name: R3
  ISIS system ID: 0000.0000.0003 level-1

  ISIS system ID: 0000.0000.0003 level-2
  Prefix SID:
    Prefix 10.0.0.2, label 20011 (regular)

```

L3/L3VPN のセグメントルーティング オン デマンド ネクスト ホップの確認

ODN の検証は、L3VPN VRF プレフィックスに基づいています。

1. R1 (ヘッドエンドと PCE サーバー) 間の PCEP セッションが確立されていることを確認します。

```

Device# sh pce client peer
PCC's peer database:
-----
Peer address: 10.0.0.3 (best PCE)
  State up
  Capabilities: Stateful, Update, Segment-Routing

```

2. すべてのピア間 (PCC) で PCEP セッションが確立されていることを確認します。

```

Device# sh pce ipv4 peer
PCE's peer database:
-----
Peer address: 10.0.0.4
  State: Up
  Capabilities: Stateful, Segment-Routing, Update
Peer address: 172.16.0.5
  State: Up
  Capabilities: Stateful, Segment-Routing, Update

```

3. R1 (ヘッドエンド) に、R6 ループバックアドレスへの可視性がないことを確認します。

```

Device# sh ip route 192.168.0.1
% Network not in table

```

4. VRF プレフィックスが R1 VRF SR ルーティング テーブルの MP-BGP によって注入されることを確認します。

```

Device# sh ip route vrf sr
Routing Table: sr
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

```

```

a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is not set
  10.0.0.6/8 is variably subnetted, 2 subnets, 2 masks
C    10.0.0.7/24 is directly connected, GigabitEthernet0/3/1
L    10.0.0.7/32 is directly connected, GigabitEthernet0/3/1
    10.0.0.8/24 is subnetted, 1 subnets
B    10.0.0.9 [200/0] via binding label: 865, 4d21h

```

5. BGP がポリシーとバインディング SID を VRF プレフィックスと正しく関連付けていることを確認します。

```

Device# sh ip bgp vpv4 vrf sr 10.107.4.0
BGP routing table entry for 100:100:10.107.4.0/24, version 3011
Paths: (1 available, best #1, table sr)
  Not advertised to any peer
  Refresh Epoch 4
  Local
    192.168.0.1 (metric 10) (via default) from 10.0.0.2 (10.0.0.2)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Community: 3276850
      Extended Community: RT:100:100
      Originator: 192.168.0.1, Cluster list: 10.0.0.2
      mpls labels in/out nolabel/1085
      binding SID: 865 (BGP_TE5555)
      rx pathid: 0, tx pathid: 0x0

```

6. バインディング ラベルの VRF プレフィックスとの関連付けを確認します。

```

Device# sh ip route vrf sr 10.107.4.0
Routing Table: sr
Routing entry for 10.107.4.0/24
  Known via "bgp 100", distance 200, metric 0, type internal
  Routing Descriptor Blocks:
    * Binding Label: 865, from 10.0.0.2, 4d22h ago
      Route metric is 0, traffic share count is 1
      AS Hops 0
      MPLS label: 1085
      MPLS Flags: NSF

```

7. VRF プレフィックスが ODN 自動トンネルによって転送されることを確認します。

```

Device# sh ip cef label-table
Label          Next Hop          Interface
0              no route
865           attached         Tunnel2000

Device# sh ip cef vrf sr 10.107.4.0 detail
10.0.0.8/24, epoch 15, flags [rib defined all labels]
  recursive via 865 label 1085
  attached to Tunnel2000

```

8. ODN 自動トンネルの状態を確認します。

```

Device# sh mpls traffic-eng tunnels
P2P TUNNELS/LSPs:
Name: R1_t2000 (Tunnel2000) Destination: 192.168.0.1 Ifhandle:
0x6F5 (auto-tunnel for BGP TE)
Status:
  Admin: up      Oper: up      Path: valid      Signalling: connected---□
auto-tunnel 2000
  path option 1, (SEGMENT-ROUTING) (PCE) type dynamic (Basis for Setup, path
weight 10)
Config Parameters:
  Bandwidth: 0      kbps (Global)  Priority: 7 7    Affinity: 0x0/0xFFFF

```

```

Metric Type: IGP (interface)
Path Selection:
  Protection: any (default)
Path-selection Tiebreaker:
  Global: not set   Tunnel Specific: not set   Effective: min-fill (default)
Hop Limit: disabled
Cost Limit: disabled
Path-invalidation timeout: 10000 msec (default), Action: Tear
AutoRoute: disabled LockDown: disabled Loadshare: 0 [0] bw-based
auto-bw: disabled
Attribute-set: BGP_TE5555--- attribute-set
Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: dynamic path option 1 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
PCEP Info:
  Delegation state: Working: yes   Protect: no
Working Path Info:
  Request status: processed
  Created via PCR message from PCE server: 10.0.0.3--- via PCE server
  PCE metric: 30, type: IGP
Reported paths:
  Tunnel Name: Tunnel2000_w
  LSPs:
  LSP[0]:
    source 10.0.0.4, destination 192.168.0.1, tunnel ID 2000, LSP ID 1
    State: Admin up, Operation active
    Binding SID: 865
    Setup type: SR
    Bandwidth: requested 0, used 0
    LSP object:
      PLSP-ID 0x807D0, flags: D:0 S:0 R:0 A:1 O:2
    Metric type: IGP, Accumulated Metric 0
    ERO:
      SID[0]: Adj, Label 2377, NAI: local 10.102.6.1 remote 10.0.0.10
      SID[1]: Unspecified, Label 17, NAI: n/a
      SID[2]: Unspecified, Label 20, NAI: n/a
History:
  Tunnel:
    Time since created: 4 days, 22 hours, 21 minutes
    Time since path change: 4 days, 22 hours, 21 minutes
    Number of LSP IDs (Tun_Instances) used: 1
    Current LSP: [ID: 1]
    Uptime: 4 days, 22 hours, 21 minutes
  Tun_Instance: 1
Segment-Routing Path Info (isis level-1)
  Segment0[Link]: 10.102.6.1 - 10.0.0.10, Label: 2377
  Segment1[ - ]: Label: 17
  Segment2[ - ]: Label: 20

```

9. R1 (ヘッドエンド) で ODN 自動トンネル LSP の状態を確認します。

```

Device# sh pce client lsp brief
PCC's tunnel database:
-----
Tunnel Name: Tunnel2000_w
LSP ID 1
Tunnel Name: Tunnel2000_p

R1# sh pce client lsp detail
PCC's tunnel database:
-----
Tunnel Name: Tunnel2000_w
LSPs:

```

```
LSP[0]:
source 10.0.0.4, destination 192.168.0.1, tunnel ID 2000, LSP ID 1
State: Admin up, Operation active
Binding SID: 865
Setup type: SR
Bandwidth: requested 0, used 0
LSP object:
  PLSP-ID 0x807D0, flags: D:0 S:0 R:0 A:1 O:2
Metric type: IGP, Accumulated Metric 0
ERO:
  SID[0]: Adj, Label 2377, NAI: local 10.102.6.1 remote 10.0.0.10
  SID[1]: Unspecified, Label 17, NAI: n/a
  SID[2]: Unspecified, Label 20, NAI: n/a
```

10. PCE サーバーで ODN LSP の状態を確認します。

```
Device# sh pce lsp summ

PCE's LSP database summary:
-----
All peers:
Number of LSPs:          1
Operational: Up:         1 Down:           0
Admin state: Up:        1 Down:           0
Setup type: RSVP:       0 Segment routing: 1

Peer 10.0.0.4:
Number of LSPs:          1
Operational: Up:         1 Down:           0
Admin state: Up:        1 Down:           0
Setup type: RSVP:       0 Segment routing: 1
```

11. PCE サーバーで詳細な LSP 情報を確認します。

```
Device# sh pce lsp det
PCE's tunnel database:
-----
PCC 10.0.0.4:
Tunnel Name: Tunnel2000_w
LSPs:
LSP[0]:
source 10.0.0.4, destination 192.168.0.1, tunnel ID 2000, LSP ID 48
State: Admin up, Operation active
Binding SID: 872
PCEP information:
  plsp-id 526288, flags: D:1 S:0 R:0 A:1 O:2
Reported path:
  Metric type: IGP, Accumulated Metric 0
  SID[0]: Adj, Label 885, Address: local 10.0.0.9 remote 10.0.0.10
  SID[1]: Unknown, Label 17,
  SID[2]: Unknown, Label 20,
Computed path:
  Computed Time: Tue Dec 20 13:12:57 2016 (00:11:53 ago)
  Metric type: IGP, Accumulated Metric 30
  SID[0]: Adj, Label 885, Address: local 10.0.0.9 remote 10.0.0.10
  SID[1]: Adj, Label 17, Address: local 10.0.0.12 remote 10.0.0.13
  SID[2]: Adj, Label 20, Address: local 10.0.0.14 remote 10.0.0.14
Recorded path:
  None
```

12. VRF SR に接続されているインターフェイスをシャットダウンして、プレフィックスが MP-BGP によってアドバタイズされなくなるようにします。

```
Device# int gig0/2/2
Device(config-if)#shut
```

13. VRF プレフィックスが R6 (テールエンド) を介して R1 (ヘッドエンド) にアドバタイズされなくなったことを確認します。

```
Device# sh ip route vrf sr
Routing Table: sr
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        a - application route
        + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is not set
  10.0.0.6/8 is variably subnetted, 2 subnets, 2 masks
C       10.0.0.7/24 is directly connected, GigabitEthernet0/3/1
L       10.0.0.8/32 is directly connected, GigabitEthernet0/3/1
```

14. ODN 自動トンネルが存在しないことを確認します。

```
Device# sh mpls traffic-eng tunnels
P2P TUNNELS/LSPs:
P2MP TUNNELS:
P2MP SUB-LSPS:
```




第 11 章

L2VPN/VPWS のセグメントルーティング オンデマンド

レイヤ2 VPN (L2VPN) のためのオンデマンドネクストホップ (ODN) は、セグメントルーティング (SR) トラフィックエンジニアリング (TE) 自動トンネルを作成し、擬似回線データプレーンのために自動トンネルを使用します。

- [L2VPN/VPWS のセグメントルーティングオンデマンドネクストホップに関する機能情報 \(137 ページ\)](#)
- [L2VPN/VPWS のセグメントルーティングオンデマンドネクストホップの制約事項 \(138 ページ\)](#)
- [L2VPN/VPWS のセグメントルーティングオンデマンドネクストホップに関する情報 \(138 ページ\)](#)
- [L2VPN/VPWS のセグメントルーティングオンデマンドネクストホップの設定方法 \(139 ページ\)](#)
- [前に付加オプションを使用した L2VPN/VPWS のセグメントルーティングオンデマンドネクストホップの設定 \(141 ページ\)](#)
- [L2VPN/VPWS のセグメントルーティングオンデマンドネクストホップの優先パスの設定 \(142 ページ\)](#)
- [L2VPN/VPWS のセグメントルーティングオンデマンドネクストホップの自動ルート宛先の設定 \(142 ページ\)](#)
- [L2VPN/VPWS のセグメントルーティングオンデマンドネクストホップの確認 \(143 ページ\)](#)

L2VPN/VPWS のセグメントルーティングオンデマンド ネクストホップに関する機能情報

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 9: L2VPN/VPWS のセグメントルーティング オン デマンド ネクスト ホップに関する機能情報

機能名	リリース	機能情報
L2VPN/VPWS のセグメント ルーティング オン デマンド ネクスト ホップ	Cisco IOS XE Amsterdam 17.3.2	L2VPN の ODN は、SR TE 自動トンネルを作成し、擬似回線データプレーンの自動トンネルを使用します。ピア IP アドレスはトンネルの宛先であり、TE LSP 属性によってトンネルのパスが決定されます。 次のコマンドが追加または修正されました。 sh mpls l2 vc、sh mpls l2 vc detail、sh l2vpn atom preferred-path、sh l2vpn atom vc、sh mpls traffic-eng tun tun 2000、sh mpls ldp discovery、sh mpls ldp nei、sh int pseudowire 4243、sh xconnect all。

L2VPN/VPWS のセグメント ルーティング オン デマンド ネクスト ホップの制約事項

- レイヤ 2 VPN/VPWS (仮想プライベート ワイヤ サービス) オン デマンド ネクスト ホップ (ODN) は擬似回線 (PW) クラスではサポートされません。
- L2VPN または VPWS のためのオン デマンドのセグメント ルーティングは、BGP シグナル/ADVPWS または仮想プライベート LAN サービス (VPLS) ではサポートされません。
- 属性セットを使用して L2VPN 用にサポートおよび作成されるのは、セグメント ルーティング TE トンネルのみです。
- TE の属性セットが設定されている場合、L2VPN 優先パス帯域幅関連の設定は有効になりません。
- LDP シグナリングを使用した L2-VPN ODN VPWS のみがサポートされています。

L2VPN/VPWS のセグメント ルーティング オン デマンド ネクスト ホップに関する情報

L2VPN のオン デマンド ネクスト ホップ (ODN) は SR TE 自動トンネルを作成し、擬似回線データプレーンの自動トンネルを使用します。ピア IP アドレスはトンネルの宛先であり、TE LSP 属性によってトンネルのパスが決定されます。場合によっては、擬似回線接続は複数の内

部ゲートウェイプロトコル (IGP) エリアにまたがる必要がありますが、LDP はシグナリングプロトコルとして使用されます。擬似回線エンドポイントプロバイダー エッジ (PE) のループバックアドレスは、IGP エリアの境界を越えて配布されません。この場合、ある PE がその RIB 内に擬似回線接続のピア PE に到達するためのデフォルト ルート (または完全一致ルート) を持たない可能性があります。したがって、擬似回線接続は LDP によってシグナルを受けることができません。この問題に対処するために、LSP 属性の下に新しいオプション **autoroute destination** が導入されました。この **autoroute destination** コマンドを使用して LSP 属性が設定されている場合、自動トンネルは LSP 属性を使用して、自動トンネルインターフェイスをネクストホップとしてトンネル宛先のスタティック ルートを自動的に作成します。このスタティック ルートにより、LDP は LDP セッションを確立し、2 つの擬似回線エンドポイント間でラベルマッピングメッセージを交換することができます。



(注) LDP シグナリング L2VPN によって使用される LSP 属性の設定にのみ **autoroute destination** コマンドを使用します。これは BGP シグナリング レイヤ 3 VPN ODN には必要ありません。

AToM マネージャ

Any Transport over MPLS (AToM) マネージャは、属性セットとピア IP アドレスのペアで自動トンネルのデータベースを維持します。AToM マネージャは擬似回線インターフェイス (VC) の SR TE 自動トンネルを追加または削除できます。

同じ属性セットまたはピアで設定された VC は、同じ自動トンネルを使用します。すべての擬似回線インターフェイスで属性セットまたはピアのペアが使用されなくなった場合、TE サービスを使用して自動トンネルをデータベースから削除できます。

エリア間 L2VPN ODN

LDP がシグナリングプロトコルとして使用され、擬似回線接続が複数の内部ゲートウェイプロトコル (IGP) にまたがる場合、擬似回線エンドポイント PE のループバックアドレスは IGP エリア境界を越えて配布されません。この場合、ある PE がその RIB 内に擬似回線接続のピア PE に到達するためのデフォルト ルート (または完全一致ルート) を持たない可能性があります。したがって、擬似回線接続は LDP によってシグナルを受けることができません。

L2VPN/VPWS のセグメントルーティング オン デマンド ネクストホップの設定方法

L2VPN/VPWS を設定するには、擬似回線インターフェイス コマンドまたはテンプレートメソッドのいずれかを使用できます。

Pesudowire インターフェイス コマンドを使用した、L2VPN/VPWS のオン デマンド ネクスト ホップでのセグメントルーティングの設定

1. ヘッドエンド ノード (R1) で次のコマンドを実行します。

```
R1#
!
mpls traffic-eng auto-tunnel p2p tunnel-num min 2000 max 2002
!
interface GigabitEthernet0/3/1
  no ip address
  negotiation auto
  service instance 300 ethernet
  encapsulation dot1q 300
!
interface pseudowire4243
  encapsulation mpls
  neighbor 10.6.6.6 300
  preferred-path segment-routing traffic-eng attribute-set L2VPNODN
!
l2vpn xconnect context foobar
  member GigabitEthernet0/3/1 service-instance 300
  member pseudowire4243
!
mpls traffic-eng lsp attributes L2VPNODN
  priority 7 7
  path-selection metric te
!
end
```

2. テール エンド (R2) で次のコマンドを実行します。

```
R2#
!
mpls traffic-eng auto-tunnel p2p tunnel-num min 2000 max 2002

interface pseudowire4243
  encapsulation mpls
  neighbor 10.1.1.1 300
  preferred-path segment-routing traffic-eng attribute-set L2VPNODN
!
interface GigabitEthernet0/2/2
  no ip address
  negotiation auto
  service instance 300 ethernet
  encapsulation dot1q 300
!
l2vpn xconnect context foobar
  member GigabitEthernet0/3/1 service-instance 300
  member pseudowire4243
!
mpls traffic-eng lsp attributes L2VPNODN
  priority 7 7
  path-selection metric te
!
end
```

テンプレートコマンドを使用した L2VPN/VPWS のセグメントルーティング オン デマンド ネクストホップの設定

1. ヘッドエンド ノード (R1) で次のコマンドを実行します。

```
R1#
template type pseudowire test
  encapsulation mpls
  preferred-path segment-routing traffic-eng attribute-set L2VPNODN
!
interface GigabitEthernet0/3/1
  no ip address
  negotiation auto
  service instance 400 ethernet
  encapsulation dot1q 400
!
l2vpn xconnect context foobar2
  member 10.6.6.6 400 template test
  member GigabitEthernet0/3/1 service-instance 400
```

2. テール エンド (R2) で次のコマンドを実行します。

```
R2#
!
template type pseudowire test
  encapsulation mpls
  preferred-path segment-routing traffic-eng attribute-set L2VPNODN
!
interface GigabitEthernet0/2/2
  no ip address
  negotiation auto
  service instance 400 ethernet
  encapsulation dot1q 400
!
l2vpn xconnect context foobar2
  member 10.1.1.1 400 template test
  member GigabitEthernet0/2/2 service-instance 400
!
end
```

前に付加オプションを使用した L2VPN/VPWS のセグメントルーティング オン デマンド ネクストホップの設定

LSP のパスを制御するために前に付加 (Prepend) オプションを有効にすることができます。前に付加オプションは、エリア内でのみサポートされ、ラベル付きパスのみをサポートします。前に付加オプションを有効にするには、次の CLI を使用します。

```
R1(config-lsp-attr)#path-selection segment-routing prepend
R1(config-lsp-attr-sr-prepend)#?
Segment-routing label prepend commands:
  exit    Exist from segment-routing prepend config mode
  index   Specify the next entry index to add, edit or delete
```

```
list    List all prepend entries
no      Delete a specific entry index
R1(config-lsp-attr-sr-prepend)#index ?
<1-10> Entry index number
last-hop    Indicates the end of label list
next-label  Specify the next MPLS label in the path
```



(注) ラストホップ オプションがテールエンドノードを示している場合。このオプションを使用する場合は、LSP パスの制御を行うことはできません。

L2VPN/VPWS のセグメントルーティング オン デマンド ネクストホップの優先パスの設定

パスが失敗したか、コマンドが削除されたことが原因である、LSPに障害が発生した場合に仮想回線 (VC) をダウンさせるには、フォールバック モードを無効にします。

```
preferred-path segment-routing traffic-eng attribute-set L2VPNODN
disable-fallback disable fall back to alternative route
```

L2VPN/VPWS のセグメントルーティング オン デマンド ネクストホップの自動ルート宛先の設定

エリア間宛先の場合、IPアドレスがヘッドエンドにインストールされていない可能性があります。L2-VPN VPWS の対象となる LDP セッションを有効にするには、宛先 IP アドレスがインストールされている必要があります。L2VPN VPWS の対象となる LDP セッションを有効にするには、属性セットの下に自動ルートの宛先を設定します。

```
Device#
mpls traffic-eng lsp attributes L2VPNODN
  priority 7 7
  path-selection metric te
  pce
  autoroute destination
!
```

宛先アドレスはスタティックルートとして L2-VPNODN LSP によってインストールされます。

次のコマンドを実行して、自動ルート宛先の設定を確認します。

```
Device#sh ip route 10.6.6.6
Routing entry for 10.6.6.6/32
  Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:
```

```
* directly connected, via Tunnel2000-----□ L2-VPN ODN LSP
  Route metric is 0, traffic share count is 1

Device#sh mpls for 10.6.6.6
Local      Outgoing      Prefix      Bytes Label  Outgoing  Next Hop
Label      Label           or Tunnel Id  Switched     interface
25         [T] Pop Label   10.6.6.6/32  0            Tu2000    point2point
```

L2VPN/VPWS のセグメントルーティング オン デマンド ネクストホップの確認

1. sh mpls l2 vc

```
Device#sh mpls l2 vc
Local intf    Local circuit      Dest address      VC ID      Status
-----
Gi0/3/1      Eth VLAN 300      10.6.6.6         300        UP
```

2. sh mpls l2 vc detail

```
Device# sh mpls l2 vc detail
Local interface: Gi0/3/1 up, line protocol up, Eth VLAN 300 up
  Interworking type is Ethernet
  Destination address: 10.6.6.6, VC ID: 300, VC status: up
  Output interface: Tu2000, imposed label stack {23 17 20}----□ 20 is the VC label
  assigned by R6
  Preferred path: Tunnel2000, active
  Default path: ready
  Next hop: point2point
  Create time: 00:15:48, last status change time: 00:15:38
  Last label FSM state change time: 00:15:38
  Signaling protocol: LDP, peer 10.6.6.6:0 up
  Targeted Hello: 10.1.1.1(LDP Id) -> 10.6.6.6, LDP is UP
  Graceful restart: not configured and not enabled
  Non stop routing: not configured and not enabled
  Status TLV support (local/remote) : enabled/supported
  LDP route watch : enabled
  Label/status state machine : established, LruRru
  Last local dataplane status rcvd: No fault
  Last BFD dataplane status rcvd: Not sent
  Last BFD peer monitor status rcvd: No fault
  Last local AC circuit status rcvd: No fault
  Last local AC circuit status sent: No fault
  Last local PW i/f circ status rcvd: No fault
  Last local LDP TLV status sent: No fault
  Last remote LDP TLV status rcvd: No fault
  Last remote LDP ADJ status rcvd: No fault
  MPLS VC labels: local 2032, remote 20
  Group ID: local 20, remote 25
  MTU: local 1500, remote 1500
  Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  SSO Descriptor: 10.6.6.6/300, local label: 2032
```

```
Dataplane:
  SSM segment/switch IDs: 10198/6097 (used), PWID: 1001
VC statistics:
  transit packet totals: receive 0, send 0
  transit byte totals:   receive 0, send 0
  transit packet drops: receive 0, seq error 0, send 0
```

3. sh l2vpn atom preferred-path

```
Device# sh l2vpn atom preferred-path
Tunnel interface      Bandwidth Tot/Avail/Resv      Peer ID      VC ID
-----
Tunnel2000
  300
!
end
```

4. sh l2vpn atom vc

```
Device# sh l2vpn atom vc
Interface Peer ID      VC ID      Type      Name      Status
-----
pw4243   10.6.6.6      300        p2p       foobar     UP
!
end
```

5. sh mpl traffic-eng tun tun 2000

```
Device# sh mpl traffic-eng tun tun 2000
Name: R1_t2000 (Tunnel2000) Destination: 10.6.6.6 Ifhandle: 0x7EE
(auto-tunnel for atom)
Status:
  Admin: up      Oper: up      Path: valid      Signalling: connected
  path option 1, (SEGMENT-ROUTING) (PCE) type dynamic (Basis for Setup, path weight
  30)
Config Parameters:
  Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (interface)
  Path Selection:
  Protection: any (default)
  Path-selection Tiebreaker:
  Global: not set Tunnel Specific: not set Effective: min-fill (default)
  Hop Limit: disabled
  Cost Limit: disabled
  Path-invalidation timeout: 10000 msec (default), Action: Tear
  AutoRoute: disabled LockDown: disabled Loadshare: 0 [0] bw-based
  auto-bw: disabled
  Attribute-set: L2VPNODN
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: dynamic path option 1 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
PCEP Info:
  Delegation state: Working: yes Protect: no
  Delegation peer: 10.8.8.8
Working Path Info:
  Request status: processed
  Created via PCRep message from PCE server: 10.8.8.8
  PCE metric: 30, type: TE
```

```

Reported paths:
Tunnel Name: Tunnel2000_w
LSPs:
LSP[0]:
  source 10.1.1.1, destination 10.6.6.6, tunnel ID 2000, LSP ID 4
  State: Admin up, Operation active
  Binding SID: 20
  Setup type: SR
  Bandwidth: requested 0, used 0
  LSP object:
    PLSP-ID 0x807D0, flags: D:0 S:0 R:0 A:1 O:2
  Metric type: TE, Accumulated Metric 30
  ERO:
    SID[0]: Adj, Label 19, NAI: local 10.104.1.1 remote 10.104.1.2
    SID[1]: Adj, Label 23, NAI: local 10.104.12.2 remote 10.104.12.1
    SID[2]: Adj, Label 17, NAI: local 10.106.13.1 remote 10.106.13.2
  PLSP Event History (most recent first):
    Tue Jun 20 10:04:48.514: PCRpt create LSP-ID:4, SRP-ID:0, PST:1,
METRIC_TYPE:2, REQ_BW:0, USED_BW:0
    Tue Jun 20 10:04:48.511: PCRpt RP-ID:9
    Tue Jun 20 10:04:48.505: PCRpt RP-ID:9, LSP-ID:4, REQ_BW:0
History:
Tunnel:
  Time since created: 18 minutes, 26 seconds
  Time since path change: 17 minutes, 9 seconds
  Number of LSP IDs (Tun_Instances) used: 4
  Current LSP: [ID: 4]
  Uptime: 17 minutes, 9 seconds
Tun_Instance: 4
Segment-Routing Path Info (isis level-2)
Segment0[Link]: 10.104.1.1 - 10.104.1.2, Label: 19-----□ will not be shown
in sh mpls l2 vc output
Segment1[Link]: 10.104.12.2 - 10.104.12.1, Label: 23
Segment2[Link]: 10.106.13.1 - 10.106.13.2, Label: 17
!
end

```

6. sh mpls ldp discovery

```

Device# sh mpls ldp discovery
Local LDP Identifier:
  10.1.1.1:0
Discovery Sources:
Targeted Hellos:
  10.1.1.1 -> 10.6.6.6 (ldp): active/passive, xmit/rcv
  LDP Id: 10.6.6.6:0

```

7. sh mpls ldp nei

```

Device# sh mpls ldp nei
Peer LDP Ident: 10.6.6.6:0; Local LDP Ident 10.1.1.1:0
TCP connection: 10.6.6.6.38574 - 10.1.1.1.646
State: Oper; Msgs sent/rcvd: 43/42; Downstream
Up time: 00:19:33
LDP discovery sources:
  Targeted Hello 10.1.1.1 -> 10.6.6.6, active, passive
Addresses bound to peer LDP Ident:
  10.106.2.2      10.106.13.2      10.6.6.6
!

```

8. sh int pseudowire 4243



第 12 章

高速コンバージェンスのデフォルト最適化

高速コンバージェンスのデフォルトの最適化機能は、すべてのプロトコルのデフォルトの設定を、高速コンバージェンスの推奨されるデフォルト値に変更します。

- [高速コンバージェンスのデフォルト最適化の機能情報 \(147 ページ\)](#)
- [高速コンバージェンスのデフォルト最適化に関する情報 \(148 ページ\)](#)

高速コンバージェンスのデフォルト最適化の機能情報

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、<https://cfng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

表 10: 高速コンバージェンスのデフォルト最適化の機能情報

機能名	リリース	機能情報
高速コンバージェンスのデフォルト最適化	Cisco IOS XE Amsterdam 17.3.2	高速コンバージェンスのデフォルトの最適化機能は、すべてのプロトコルのデフォルトの設定を、高速コンバージェンスの推奨されるデフォルト値に変更します。 新しく追加または変更されたコマンドはありません。

高速コンバージェンスのデフォルト最適化に関する情報

高速コンバージェンスのデフォルトの最適化機能は、すべてのプロトコルのデフォルトの設定を、高速コンバージェンスの推奨されるデフォルト値に変更します。IS-ISおよびOSPFの両方についてデフォルトを事前の高速コンバージェンス設定に戻すには、**no routing-default-optimize** コマンドを使用します。このコマンドは、信号をその IS-IS および OSPF に送信し、これらのプロトコルのデフォルト設定を変更します。

デフォルトでは、高速コンバージェンス設定が有効になっているため、ソフトウェアをアップグレードすると、新しい動作が自動的に表示されます。これにより、マルチベンダー展開でのデバイスの統合が容易になり、コンバージェンスの低下によるサポートケースが減少します。

デフォルトの最適化を無効にすると、既存のプロトコルのデフォルト設定が使用されます。デフォルトの最適化を有効にすると、新しいプロトコルのデフォルト値が使用されます。**show running configurations** は、デフォルト設定が使用されている場合でも、デフォルト設定の設定行を表示しません。

プロトコルの設定はデフォルトよりも優先されますが、デフォルトの最適化への変更は設定を上書きしません。

次に、IS-IS での **spf-interval** コマンドの出力例を示します。

```
Device(config-if)# router isis
Device(config-router)# spf-interval 10 5500 5500
```

デフォルト値以外が設定されている場合は、**show running configuration** の出力に表示されます。

```
Device(config-router)# spf-interval 5 50 200
Device(config-router)# do show run | inc spf-interval
  spf-interval 5 50 200
```

デフォルト値を設定するか、デフォルト以外の設定を削除することによって、デフォルト値に戻すことができます。

IS-IS のデフォルト最適化値

次の表は、デフォルト最適化の影響を受ける設定の概要を示します。

IS-IS コマンド	パラメータ	デフォルト最適化が無効	デフォルト最適化が有効
fast-flood			
	# of lsps flooded back-back	無効	10
spf-interval			

IS-IS コマンド	パラメータ	デフォルト最適化が無効	デフォルト最適化が有効
	初期 (ミリ秒)	5500	50
	セカンダリ (ミリ秒)	5500	200
	最大 (秒)	10	5
pre-interval			
	初期 (ミリ秒)	2000	50
	セカンダリ (ミリ秒)	5000	200
	最大 (秒)	5	5
lsp-gen-interval			
	初期 (ミリ秒)	50	50
	セカンダリ (ミリ秒)	5000	200
	最大 (秒)	5	5
log-adjacency-changes		disabled	enabled

OSPF のデフォルト最適化値

次の表は、OSPFv2/v3 のデフォルト最適化の影響を受ける設定の概要を示します。

OSPF コマンド	パラメータ	デフォルト最適化が無効	デフォルト最適化が有効
timers throttle spf			
	初期 (ミリ秒)	5000	50
	セカンダリ (ミリ秒)	10000	200
	最大 (ミリ秒)	10	5
timers throttle lsa all			
	初期 (ミリ秒)	0	50
	セカンダリ (ミリ秒)	5000	200
	最大 (ミリ秒)	5	5
timers lsa arrival			

OSPF コマンド	パラメータ	デフォルト最適化が無効	デフォルト最適化が有効
	milliseconds	1000	100

以下は、デフォルト最適化値を使用した OSPFv2 の **show ip ospf** コマンドの出力例です。

```
Device# show ip ospf
Routing Process "ospf 10" with ID 10.1.1.1
Start time: 00:00:01.471, Time elapsed: 03:00:34.706
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 3101)
Supports Database Exchange Summary List Optimization (RFC 5243)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 50 msec
Minimum hold time between two consecutive SPFs 200 msec
Maximum wait time between two consecutive SPFs 5000 msec
Incremental-SPF disabled
Initial LSA throttle delay 50 msec
Minimum hold time for LSA throttle 200 msec
Maximum wait time for LSA throttle 5000 msec
Minimum LSA arrival 100 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
EXCHANGE/LOADING adjacency limit: initial 300, process maximum 300
Number of external LSA 18. Checksum Sum 0x075EB2
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps
  Area BACKBONE(0)
    Number of interfaces in this area is 4 (2 loopback)
    Area has RRR enabled
    Area has no authentication
    SPF algorithm last executed 02:27:23.736 ago
    SPF algorithm executed 20 times
    Area ranges are
    Number of LSA 94. Checksum Sum 0x321DCF
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
```

以下は、デフォルト最適化値を使用した OSPFv3 の **show ospf** コマンドの出力例です。

```
Device# show ospfv3
OSPFv3 10 address-family ipv6
Router ID 10.11.11.11
Supports NSSA (compatible with RFC 3101)
```

```
Supports Database Exchange Summary List Optimization (RFC 5243)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 50 msec
Minimum hold time between two consecutive SPF's 200 msec
Maximum wait time between two consecutive SPF's 5000 msec
Initial LSA throttle delay 50 msec
Minimum hold time for LSA throttle 200 msec
Maximum wait time for LSA throttle 5000 msec
Minimum LSA arrival 100 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Retransmission limit dc 24 non-dc 24
EXCHANGE/LOADING adjacency limit: initial 300, process maximum 300
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Graceful restart helper support enabled
Reference bandwidth unit is 100 mbps
RFC1583 compatibility enabled
  Area BACKBONE(0)
    Number of interfaces in this area is 2
    SPF algorithm executed 7 times
    Number of LSA 3. Checksum Sum 0x012426
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
```




第 13 章

ルーティング情報ベースのサポート

ルーティング情報ベース（RIB）拡張は、ルート再配布およびオンデマンドネクストホップ要件をサポートします。

- ルーティング情報ベースのサポートの機能情報（153 ページ）
- ルート再配布のためのルーティング情報ベースのサポート（154 ページ）
- OSPF ノード SID 再配布のサポート（154 ページ）
- オンデマンドネクストホップのためのルーティング情報ベースのサポート（157 ページ）

ルーティング情報ベースのサポートの機能情報

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、<https://cfng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

表 11: ルーティング情報ベースのサポートの機能情報

機能名	リリース	機能情報
ルーティング情報ベースのサポート	Cisco IOS XE Amsterdam 17.3.2	ルーティング情報ベース（RIB）拡張は、ルート再配布およびオンデマンドネクストホップ要件をサポートします。 新しく追加または変更されたコマンドはありません。

機能名	リリース	機能情報
OSPF ノード SID 再配布のサポート	Cisco IOS XE Amsterdam 17.3.2	<p>以前のケースとは異なり、OSPF が他の IGP から再配布されたプレフィックスを受信した場合、およびその逆の場合は、プレフィックスのセグメント識別子 (SID) もアドバタイズされます。IGP ドメイン間で SID を学習するには、BGP LS (または) セグメントルーティングマッピングサーバー (SRMS) のサポートが必要です。</p> <p>この機能のために、show ip ospf rib redistribution detail、show ip ospf segment-routing local-prefix、show ip ospf segment-routing sid-database、show ip route 3.3.3.3 コマンドが導入または変更されました。</p>

ルート再配布のためのルーティング情報ベースのサポート

Cisco IOS XE Everest 16.5.1 では、プレフィックスに関連付けられたラベルを再配布するための要件が導入されています。再配布の要件をサポートするために、プレフィックスごとのローカルラベルのストレージが RIB でサポートされます。

異なる SRGB を使用する可能性のあるさまざまなプロトコルでの使用を容易にするために、SID の代わりにローカルラベルが保存されます。宛先プロトコルによって割り当てられた SID は、送信元プロトコルに関連付けられた SID と同じではない場合があります。

プレフィックス到達可能性アドバタイズメントまたは SRMS アドバタイズメントは、SID のソースです。SRMS アドバタイズでは、再配布の宛先プロトコルは、アドバタイズメントのソースが SRMS ではないことを他のネットワーク ノードで示すことによって競合の解決を変更するため、そのプレフィックス到達可能性アドバタイズメントで SID をアドバタイズしません。

OSPF ノード SID 再配布のサポート

Cisco IOS XE 16.7.1 では以前のケースとは異なり、OSPF が他の IGP から再配布されたプレフィックスを受信し、その逆にプレフィックスセグメント識別子 (SID) もアドバタイズされます。IGP ドメイン間で SID を学習するには、BGP LS (または) セグメントルーティングマッピングサーバー (SRMS) のサポートが必要でした。

ユーザーが OSPF で再配布を有効にすると、プレフィックス エントリに関連付けられたプレフィックス SID エントリが OSPF に提供されます。これは OSPF によってそのすべてのネイバーにアドバタイズされます。OSPF のアドバタイズ方法は、ネットワーク内の OSPF の役割によって異なります。

OSPF ノード SID 再配布のサポートに関する情報

NSSA ASBR

Not-So-Stubby Area 自律システム境界ルータ (NSSA ASBR) の OSPF で **redistribute ISIS instance ip** を有効にすると、SID エントリとともに IS-IS で学習された IP ルーティング情報ベース (RIB) からのすべてのプレフィックスを取得します。OSPF は、エリアとして範囲と、プレフィックスの RTYPE_NSSA1 または RTYPE_NSSA2 としてルートタイプを持つ拡張プレフィックス LSA (EPL) を生成し、そのすべてのネイバーにアドバタイズします。同様に、再配布が設定されていない場合 (または) プレフィックスが使用できなくなったときに、OSPF は EPL を取り消します。再配布されたルートが非接続ルートである場合、OSPF は No-PHP フラグを設定しますが、明示的な NULL フラグは設定されません。ただし、再配布されたルートが接続済みルートである場合、OSPF は、SR ポリシーで行われた設定に従って明示的な NULL および No-PHP フラグを設定します。

NSSA ABR が EPL を受信すると、ABR は LSA を不透明 AS EPL に変換し、そのすべてのネイバーにフラッドします。

ABR でも ASBR でもない NSSA ルータが EPL を受信すると、SID エントリとともにプレフィックスを学習し、同じエリア内のすべてのネイバーにフラッドします。

非 NSSA ASBR

通常の ASBR ルータである OSPF でユーザーが **redistribute ISIS instance ip** を有効にすると、SID エントリとともに IS-IS によって学習された IP RIB からのすべてのプレフィックスを取得します。OSPF は、自律システム (AS) として範囲と、プレフィックスの RTYPE_EXTERN1 または RTYPE_EXTERN2 としてルートタイプを持つ EPL を生成し、そのすべてのネイバーにアドバタイズします。同様に、再配布が設定されていない場合 (または) プレフィックスが使用できなくなったときに、OSPF は再び EPL を AS 範囲とともに取り消します。再配布されたルートが非接続ルートである場合、OSPF は No-PHP フラグを設定しますが、明示的な NULL フラグは設定されません。ただし、再配布されたルートが接続済みルートである場合、OSPF は、SR ポリシーで行われた設定に従って明示的な NULL および No-PHP フラグを設定します。ルータは AS 範囲を持つ EPL を受信すると、SID エントリとともにプレフィックスを学習し、すべてのエリアのすべてのネイバーにフラッドします。

プレフィックスの再配布

IS-IS で OSPF ルートの再配布が有効になっている場合、プレフィックスが SID 情報とともに与えられ、プレフィックスが SID 値を持つ他のドメインに到達するようになります。他のドメインへの OSPF プレフィックスの再配布を理解するには、以下のトポロジを参照してください。

図 17: OSPF プレフィックスの再配布



R1 および R2 は OSPF が有効になっています。R2 および R3 は IS-IS が有効になっています。IS-IS および OSPF の両方ともセグメントルーティングが有効になっています。R2 では、IS-IS

および OSPF の両方とも設定されています。設定されているプレフィックスは次のとおりです。

1. R1 の 10.1.1/32 (SID 1 による OSPF に対して有効)
2. R2 の 10.2.2/32 (SID 2 による OSPF に対して有効)
3. R3 の 10.3.3/32 (ISIS SID 3 に対して有効)

R2 で SID 再配布を有効にすると、プレフィックス 10.3.3.3/32 が R1 に再配布されます。したがって、R1 はプレフィックス R3 に到達する SID を知っています。

```
conf trouter isis 10 net 49.0001.0000.0000.0001.00 metric-style wide distribute link-state
segment-routing mpls router ospf 10 router-id 10.2.2.2 segment-routing mpls distribute
link-state
```

OSPF ルートへの ISIS の再配布を有効にするには次を実行します。

```
conf t router ospf 10 redistribute isis 10 ip
```

OSPF ノード SID 再配布の確認

show ip ospf rib redistribution detail コマンドを使用して、OSPF が IS-IS からプレフィックスを再配布しているかどうかを確認します。



(注) C8xxx=C8200/C8300/C8500 または C8000v

```
c8xxx# show ip ospf rib redistribution detail
OSPF Router with ID (10.2.2.2) (Process ID 10)

Base Topology (MTID 0)

OSPF Redistribution
10.3.3.3/32, type 2, metric 20, tag 0, from IS-IS Router
Attributes 0x1000000, event 1, PDB Index 4, PDB Mask 0x0
Source route metric 20, tag 0
SID 1003, SID Flags NP-bit, EPX Flags None
via 10.9.0.9, Ethernet0/0
```

show ip ospf segment-routing local-prefix コマンドを使用して、SID エントリがそのネイバーにアドバタイズされているかどうかを確認します。

```
c8xxx# show ip ospf segment-routing local-prefix

OSPF Router with ID (10.2.2.2) (Process ID 10)

Area 0:
Prefix:          Sid:    Index:          Type:          Source:
10.2.2.2/32      2      10.0.0.0        Intra          Loopback0
AS external:
Prefix:          Sid:    Index:          Type:          Source:
10.3.3.3/32      3      10.0.0.1        External      Redist
```

show ip ospf segment-routing sid-database コマンドを使用して、SID が受信されているかどうかを確認します。

```
Device# show ip ospf segment-routing sid-database
```

```
OSPF Router with ID (10.1.1.1) (Process ID 10)
OSPF Segment Routing SIDs
```

```
Codes: L - local, N - label not programmed,
M - mapping-server
```

SID	Prefix	Adv-Rtr-Id	Area-Id	Type
1	10.1.1.1/32	10.1.1.1	0	Intra
2	10.2.2.2/32	10.2.2.2	0	Intra
3	10.3.3.3/32	10.2.2.2	-	External

show ip route 10.3.3.3 コマンドを使用して、再配送されたルートに対して IP ルーティング エントリが設定されているかどうかを確認します。

```
c8xxx# show ip route 10.3.3.3
Routing entry for 10.3.3.3/32
  Known via "ospf 10", distance 110, metric 20, type extern 2, forward metric 20
  Last update from 10.2.0.2 on Ethernet0/1, 00:00:01 ago
  SR Incoming Label: 16003
  Routing Descriptor Blocks:
  * 10.3.1.3, from 10.2.2.2, 00:00:01 ago, via Ethernet1/1, merge-labels
    Route metric is 20, traffic share count is 1
    MPLS label: 16003
    MPLS Flags: NSF
```

オンデマンドネクストホップのためのルーティング情報ベースのサポート

オンデマンドネクストホップ (ODN) 要件の場合、RIBは、ルーティングプロトコル (BGP) をサポートすることによって提供されるバインディング ラベルと呼ばれるネクスト ホップをサポートします。FIBは、バインディング ラベルを使用してネクスト ホップを動的に解決します。

ルートプロデューサは、ネクストホップに関連付けられたODNトンネルパスを識別するローカルバインディングラベルをインストールします。ラベル付きトラフィックは、トンネルを介して送信され、ラベルは既存のアウトラベルとは区別されます。

次に、各ネクストホップがバインディングラベルを表示するように更新される **show ip route** コマンドの出力例を示します。

```
Device# show ip route 10.10.10.2
```

```
Routing entry for 10.10.10.2/32
  Known via "isis", distance 115, metric 10, type level-1
  Redistributing via isis
  Last update from 10.200.200.2 on Ethernet0/0, 00:00:14 ago
  Incoming Label: 16100
  Routing Descriptor Blocks:
  * 10.200.200.2, from 10.10.10.2, 00:00:14 ago, via Ethernet0/0
    Route metric is 10, traffic share count is 1
```

```
* Binding Label 4020, from 10.2.2.2, 00:00:14 ago,  
Route metric is 10, traffic share count is 1
```



(注) 受信ラベルは、SID の再配布が有効になった後にのみ表示されます。



第 14 章

SR-TE オン デマンド LSP

SR-TE オン デマンド LSP 機能は、宛先へのスタティックルートを経由してメトロ アクセス リングを接続する機能を提供します。スタティックルートは明示的なパスにマップされ、宛先へのオン デマンド LSP をトリガーします。SR-TE オン デマンド LSP 機能は、メトロ アクセス リング間の VPN サービスの転送に使用されます。

- [SR-TE オン デマンド LSP の機能情報 \(159 ページ\)](#)
- [SR-TE オン デマンド LSP の制約事項 \(160 ページ\)](#)
- [SR-TE オン デマンド LSP に関する情報 \(160 ページ\)](#)
- [SR-TE オン デマンド LSP の設定方法 \(161 ページ\)](#)
- [スタティック ルーティング向けネイティブ UCMP の設定 \(165 ページ\)](#)

SR-TE オン デマンド LSP の機能情報

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、<https://cfng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

表 12: SR-TE オン デマンド LSP の機能情報

機能名	リリース	機能情報
SR-TE オン デマ ンド LSP	Cisco IOS XE Amsterdam 17.3.2	SR-TE オン デマンド LSP 機能は、宛先へのスタティックルートを経由してメトロ アクセス リングを接続する機能を提供します。スタティックルートは明示的なパスにマップされ、宛先へのオン デマンド LSP をトリガーします。SR-TE オン デマンド LSP 機能は、メトロ アクセス リング間の VPN サービスの転送に使用されます。 mpls traffic-eng auto-tunnel コマンドが変更されました。

SR-TE オン デマンド LSP の制約事項

- セグメントルーティング自動トンネル スタティック ルートは ECMP をサポートしていません。
- IP 明示的パスのメトリクスおよび自動トンネル SRTE スタティック ルートのアドミニストレーティブ ディスタンスの変更はサポートされていません。
- MPLS トラフィック エンジニアリング (TE) ノンストップルーティング (NSR) は、ステートフル スイッチオーバー (SSO) のためにアクティブ ルート プロセッサ (RP) で設定する必要があります。これは、スタティック ルート自動トンネル設定を削除して再設定しない限り、SSO の後に SR スタティック自動トンネルが起動しなくなるためです。
- IP アンナナード インターフェイスは動的パスをサポートしません。
- IP アンナナード インターフェイスを使用する場合、ネクスト ホップ アドレスを明示的パスのインデックスとして指定することはできません。これは、ノードアドレスまたはラベルである必要があります。

SR-TE オン デマンド LSP に関する情報

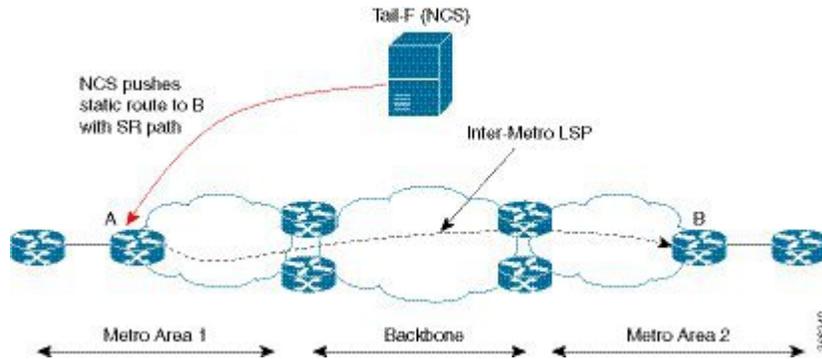
SR TE オン デマンド LSP 機能は、宛先へのスタティック ルートを經由してメトロ アクセス リングを接続する機能を提供します。

SR-TE : スタティック ルートとして LSP をセットアップする

アジャイル キャリア イーサネット (ACE) ソリューションは、統合 VPN サービスのためにセグメントルーティングベースのトランスポートを活用します。メトロ リングアーキテクチャでは、アクセス リングはルーティング トポロジを互いに共有しません。

SR TE オン デマンド LSP 機能は、宛先へのスタティック ルートを經由してメトロ アクセス リングを接続する機能を提供します。スタティック ルートは明示的なパスにマップされ、宛先へのオン デマンド LSP をトリガーします。SR TE オン デマンド LSP 機能は、メトロ アクセス リング間の VPN サービスの転送に使用されます。

図 18: ACE ソリューションにおけるメトロ間 LSP



メトロ間 LSP には、次のような側面があります。

- 送信元パケットが宛先デバイスの IP アドレスを知らない可能性があります。
- 既存のセグメントルーティング機能を LSP に適用できます。

バインディング SID は、SR-TE トンネル内のトラフィックをステアリングするのに役立ちます。つまり、バインディング SID を持つ入力 MPLS パケットは、特定の SR-TE トンネルを介して転送されます。

アンナンバードインターフェイス上のスタティック SRTE

前のセクションで説明したように、LSP をスタティック ルートとして設定して、IP 明示的パスを指定することで自動トンネルを作成できます。

明示パスとは、IP アドレス（または）IP アドレスとラベルの組み合わせです。また、アンナンバードインターフェイス上でスタティック SRTE トンネルを設定することもできます。ナンバードインターフェイスに対するアンナンバードインターフェイスの制限はほとんどありません。

- IP 明示パス オプションでネクストホップインターフェイスアドレスではなく、ノードの IP アドレスを指定する必要があります。
- 明示パス オプションで隣接関係 SID を指定することはできません。つまり、明示パス オプションには、ノードの IP アドレス (/32 マスク) とプレフィックス SID ラベルのみが含まれている必要があります。

SR-TE オンデマンド LSP の設定方法

SR-TE のオンデマンド LSP を設定するには、次のステップを実行します。

スタティックルートとしての LSP の設定

SR TE による RP スイッチオーバー後のパケットドロップを回避するには、次のコマンドを使用することをお勧めします。

```
mpls traffic-eng nsr
```

ISIS が設定されている場合は、次のコマンドを使用します。

```
router isis
 nsf cisco
 nsf interval 0
```

セグメントルーティング自動トンネルスタティックルートの有効化

このタスクを実行して、次のように自動トンネルスタティックルートを設定します。

- IP 明示パスを設定します
- IP 明示パスを持つ自動トンネルをスタティックルートに関連付けます
- ピアツーピア (P2P) 自動トンネルサービスを有効にします

```
ip explicit-path name path1
 index 1 next-label 16002
 index 2 next-label 16006
 exit
ip route 172.16.0.1 255.240.0.0 segment-routing mpls path name path1
mpls traffic-eng auto-tunnel p2p
mpls traffic-eng auto-tunnel p2p config unnumbered-interface loopback0
mpls traffic-eng auto-tunnel p2p tunnel-num min 10 max 100
```

セグメントルーティング自動トンネルスタティックルートの確認

コマンド **show mpls traffic-eng service summary** は、TE 自動トンネルを使用するすべての登録済み TE サービスクライアントおよび統計を表示します。

```
Device# show mpls traffic-eng service summary
```

```
Service Clients Summary:
Client: BGP TE
  Client ID                :0
  Total P2P tunnels        :1
  P2P add requests         :6
  P2P delete requests      :5
  P2P add falis            :0
  P2P delete falis         :0
  P2P notify falis         :0
  P2P notify succs         :12
  P2P replays              :0
Client: ipv4static
  Client ID                :1
  Total P2P tunnels        :1
  P2P add requests         :6
  P2P delete requests      :5
  P2P add falis            :0
  P2P delete falis         :0
  P2P notify falis         :0
```

```
P2P notify succs      :85
P2P replays           :0
```

コマンド **show mpls traffic-eng auto-tunnel p2p** は、ピアツーピア (P2P) 自動トンネルの設定と操作状態を表示します。

```
Device# show mpls traffic-eng auto-tunnel p2p
```

```
State: Enabled
p2p auto-tunnels: 2 (up: 2, down: 0)
Default Tunnel ID Range: 62336 - 64335
Config:
  unnumbered-interface: Loopback0
  Tunnel ID range: 1000 - 2000
```

コマンド **show mpls traffic-eng tunnel summary** は、P2P 自動トンネルの状態を表示します。

```
Device# show mpls traffic-eng tunnel summary
```

```
Signalling Summary:
LSP Tunnels Process:      running
Passive LSP Listener:    running
RSVP Process:            running
Forwarding:              enabled
auto-tunnel:
  p2p   Enabled (1), id-range:1000-2000
Periodic reoptimization:  every 3600 seconds, next in 1265 seconds
Periodic FRR Promotion:   Not Running
Periodic auto-bw collection: every 300 seconds, next in 66 seconds
SR tunnel max label push: 13 labels
P2P:
  Head: 11 interfaces, 5234 active signalling attempts, 1 established
        5440 activations, 206 deactivations
        1821 failed activations
        0 SSO recovery attempts, 0 SSO recovered
  Midpoints: 0, Tails: 0
P2MP:
  Head: 0 interfaces, 0 active signalling attempts, 0 established
        0 sub-LSP activations, 0 sub-LSP deactivations
        0 LSP successful activations, 0 LSP deactivations
        0 SSO recovery attempts, LSP recovered: 0 full, 0 partial, 0 fail
  Midpoints: 0, Tails: 0
Bidirectional Tunnel Summary:
Tunnel Head: 0 total, 0 connected, 0 associated, 0 co-routed
LSPs Head: 0 established, 0 proceeding, 0 associated, 0 standby
LSPs Mid: 0 established, 0 proceeding, 0 associated, 0 standby
LSPs Tail: 0 established, 0 proceeding, 0 associated, 0 standby

AutoTunnel P2P Summary:
ipv4static:
  Tunnels: 1 created, 1 up, 0 down
Total:
  Tunnels: 1 created, 1 up, 0 down
```

コマンド **show mpls traffic-eng tunnel auto-tunnel** は、TE サービス自動トンネルのみを表示します。

```
Device# show mpls traffic-eng tunnel auto-tunnel detail
```

```
P2P TUNNELS/LSPs:
```

```

Name: R1_t1000 (Tunnel1000) Destination: 10.0.0.0 Ifhandle:
0x17 (auto-tunnel for ipv4static)
Status:
  Admin: up      Oper: up      Path: valid      Signalling: connected
  path option 1, (SEGMENT-ROUTING) type explicit (verbatim) path202 (Basis for Setup)

Config Parameters:
  Bandwidth: 0      kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  Path Selection:
    Protection: any (default)
  Path-selection Tiebreaker:
    Global: not set Tunnel Specific: not set Effective: min-fill (default)
  Hop Limit: disabled [ignore: Verbatim Path Option]
  Cost Limit: disabled
  Path-invalidation timeout: 10000 msec (default), Action: Tear
  AutoRoute: disabled LockDown: disabled Loadshare: 0 [0] bw-based
  auto-bw: disabled
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: explicit path option 1 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: enabled

History:
  Tunnel:
    Time since created: 33 days, 20 hours, 29 minutes
    Time since path change: 10 days, 19 hours, 45 minutes
    Number of LSP IDs (Tun_Instances) used: 1646
  Current LSP: [ID: 1646]
    Uptime: 10 days, 19 hours, 45 minutes
  Prior LSP: [ID: 1645]
    ID: path option unknown
    Removal Trigger: signalling shutdown
  Tun_Instance: 1646
  Segment-Routing Path Info (IGP information is not used)
    Segment0[First Hop]: 10.0.0.0, Label: 16002
    Segment1[ - ]: Label: 16006

```

コマンド **show mpls traffic-eng tunnel brief** は、自動トンネルの情報を表示します。

```

Device# show mpls traffic-eng tunnel brief

Signalling Summary:
  LSP Tunnels Process:      running
  Passive LSP Listener:    running
  RSVP Process:            running
  Forwarding:              enabled
  auto-tunnel:
    p2p      Enabled (2), id-range:1000-2000

  Periodic reoptimization:  every 3600 seconds, next in 406 seconds
  Periodic FRR Promotion:   Not Running
  Periodic auto-bw collection: every 300 seconds, next in 107 seconds
  SR tunnel max label push: 13 labels

P2P TUNNELS/LSPs:
TUNNEL NAME      DESTINATION      UP IF      DOWN IF      STATE/PROT
R1_t1            10.66.66.66     -          -            up/down
R1_t2            10.66.66.66     -          -            up/up
R1_t3            10.66.66.66     -          -            up/up
R1_t10           10.66.66.66     -          -            up/up
SBFD tunnel      10.33.33.33     -          -            up/up

```

SBFD Session configured: 1

SBFD sessions UP: 1

スタティック ルーティング向けネイティブ UCMP の設定

トラフィックが2つ以上のリンクで負荷分散されているネットワークでは、リンク上で等価メトリックを設定すると、Equal Cost Multipath (ECMP; 等コスト マルチパス) ネクスト ホップが作成されます。ロードバランシング中にリンクの帯域幅が考慮されないため、より高い帯域幅のリンクが十分に活用されません。この問題を回避するには、より高い帯域幅のリンクがリンクの容量に比例してトラフィックを伝送するように、不等コスト マルチパス (UCMP) をローカル (ローカル UCMP) またはネイティブ (ネイティブ UCMP) で設定できます。UCMP は、IPv4 および IPv6 のスタティック VRF ルートをサポートしています。

ローカル UCMP

静的ルートはすべて同じリンクメトリックで設定されます。スタティック IGP は、リンクの帯域幅に基づいて負荷メトリックを計算し、リンク上のトラフィックを負荷分散します。ただし、ローカル UCMP では、(複数ホップ離れた) 宛先に近いリンク間のロードバランシング時に帯域幅を考慮しません。

ネイティブ UCMP

より高い帯域幅のリンク上の静的ルートは、より低いリンクメトリックで設定し、より低い帯域幅のリンク上のルートより優先されるようにします。スタティック IGP は、リンクの帯域幅に基づいて負荷メトリックを計算し、より高い帯域幅のリンクおよびより低い帯域幅のリンクから出るトラフィックの割合を決定します。設定されたリンクメトリックとエンドツーエンドの使用可能な帯域幅を照合することで、ネイティブ UCMP は、(複数ホップ離れた) 宛先に近いリンク間でトラフィックを効果的に負荷分散できます。

設定例

次の図のトポロジについて考えます。ルータ A1 からのトラフィックのロードバランシングでは、ローカル UCMP が使用されている場合、10G と 100G の両方のリンクには等しいリンクメトリックが設定されます。負荷メトリックが高いため、スタティック IGP は 100G リンクからより多くのトラフィックを送信することを決定します。ただし、ルータ A2 からのトラフィックのロードバランシングでは、ローカル UCMP はルータ C1 および C2 へのリンク上でのみ機能します。ルータ C1 からルータ A1 およびルータ C2 からルータ A1 へのトラフィックのロードバランシングでは、ネイティブ UCMP が推奨されます。その結果、ローカル UCMP はシングルホップの宛先でのみ使用され、ネイティブ UCMP はマルチホップの宛先で使用されます。



第 15 章

セグメント ルーティング MPLS OAM のサポート

セグメントルーティング保守運用管理 (OAM) は、ネットワークの障害検出とトラブルシューティングに役立ちます。これを使用することで、サービス プロバイダーはラベル スイッチドパス (LSP) をモニターしてフォワーディングの問題を迅速に隔離できます。セグメントルーティング OAM 機能では、Nil-FEC (フォワーディング等価クラス) LSP Ping および Traceroute、IGP プレフィックス SID FEC タイプ、および SR-TE 機能のための部分的な IGP 隣接関係 SID FEC タイプのサポートを提供します。

- [セグメントルーティング OAM サポートの機能情報 \(167 ページ\)](#)
- [セグメントルーティング OAM MPLS サポートの制約事項 \(168 ページ\)](#)
- [セグメントルーティング MPLS OAM サポートに関する情報 \(168 ページ\)](#)
- [LSP Ping およびトレース ルート Nil FEC ターゲットを使用してセグメントルーティングを診断する方法 \(170 ページ\)](#)
- [LSP Ping Nil FEC ターゲットのサポートの例 \(171 ページ\)](#)
- [セグメントルーティング ネットワークのパス検証 \(173 ページ\)](#)
- [MPLS Ping および Traceroute 用のセグメント ルーティング MPLS トラフィック エンジニアリングの設定 \(175 ページ\)](#)
- [MPLS Ping および Traceroute 用のセグメントルーティング MPLS IGP の設定 \(176 ページ\)](#)

セグメント ルーティング OAM サポートの機能情報

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 13:セグメントルーティング OAM サポートの機能情報

機能名	リリース	機能情報
セグメントルーティング OAM サポート	Cisco IOS XE Amsterdam 17.3.2	セグメントルーティング OAM 機能では、Nil-FEC (転送等価クラス) LSP Ping および Traceroute 機能のサポートを提供します。 Nil-FEC LSP ping および traceroute の操作は、単に通常の MPLS ping および traceroute の拡張機能です。

セグメントルーティング OAM MPLS サポートの制約事項

- Ping と traceroute は、SR-TE スタティック自動トンネル、BGP ダイナミック TE、およびオンデマンドネクストホップ自動トンネルではサポートされていません。
- Strict-SID オプションは、OSPF によってインストールされたパスではサポートされません。
- MPLS traceroute は、1 つのノードで 2 つの明示的ヌルラベルのポップをサポートしません。
- IP ルーティングの宛先が MPLS FEC ではないため、レイヤ 3 VPN を使用せずに、MPLS セグメント経由で IP へのパスを再ルーティングすることはサポートされていません。

セグメントルーティング MPLS OAM サポートに関する情報

セグメントルーティング OAM サポート

Nil-FEC LSP ping および traceroute の操作は、通常の MPLS ping および traceroute の拡張機能です。Nil-FEC LSP Ping/Trace 機能は、セグメントルーティングと MPLS スタティックをサポートしています。また、他のすべての LSP タイプに対する追加の診断ツールとしても機能します。この機能は、オペレータがラベルスタックをテストして以下を指定できるようにします。

- ラベルスタック
- 発信インターフェイス
- ネクストホップアドレス

セグメントルーティングの場合、ルーティングパスに沿った各セグメントノードラベルおよび隣接関係ラベルは、イニシエータのラベルスイッチルータ (LSR) からのエコー要求メッ

セージのラベルスタックに入れられます。MPLS データプレーンは、このパケットをラベルスタックターゲットに転送し、ラベルスタックターゲットはエコーメッセージを送り返します。

セグメントルーティング OAM サポートの利点

- この機能により、トラフィックが SR-TE トンネルまたはネイティブ SR フォワーディングを介してエンジニアリングされるセグメントルーティングネットワークの MPLS OAM 機能が有効になります。
- 従来の MPLS ネットワークでは、ソースノードは、LDP または RSVP-TE のようなホップバイホッピングナリングプロトコルに基づいてパスを選択します。セグメントルーティングネットワークでは、パスは IGP プロトコル（現在は OSPF および ISIS）によってアドバタイズされるセグメントのセットによって指定されます。
- SR を使用して提供されるサービスの量が増加するため、オペレータが本質的に SR アーキテクチャの接続検証と障害分離を行うことができることが重要です。
- セグメントの割り当ては、従来の MPLS ネットワークのようにホップバイホップのプロトコルに基づいていないため、切断された中継ノードによって Null ルートが生まれ、望ましくないトラフィック動作を引き起こす可能性があります。
- SR と SR-TE はどちらもロードバランシングをサポートしていて、ソースルータとターゲットルータの間で利用可能なすべての ECMP パスをトレースすることが重要です。この機能は、TE とネイティブ SR パスの両方に対してマルチパスの traceroute をサポートします。
- セグメントルーティング OAM サポートの主な利点は次のとおりです。
 - **運用**：ネットワークのモニタリングおよび障害管理。
 - **管理**：ネットワークの検出と計画。
 - **メンテナンス**：訂正および予防のアクティビティにより、障害の発生と影響を最小限に抑えます。

セグメントルーティング MPLS Ping

MPLS ping および traceroute は設計によって拡張可能です。SR サポートを追加するには、新しい FEC および/または追加の検証手順を定義します。MPLS ping は MPLS データパスを検証し、次を実行します。

- エコー要求パケットを MPLS ラベルにカプセル化します。
- 低密度ラウンドトリップ時間を測定します。
- 低密度ラウンドトリップ遅延を測定します。

セグメントルーティング MPLS Traceroute

MPLS ping および traceroute は設計によって拡張可能です。SR サポートを追加するには、新しい転送等価クラス (FEC) および/または追加の検証手順を定義します。MPLS traceroute は、LSP の各ホップでフォワーディングプレーンおよびコントロールプレーンを検証して、障害を切り分けます。traceroute は、TTL 1 から始まり単調増加する存続可能時間 (TTL) で MPLS エコー要求を送信します。TTL の有効期限が過ぎると、中継ノードはソフトウェアで要求を処理し、ターゲット FEC と目的の中継ノードへの LSP があるかどうかを確認します。中継ノードは、検証が成功した場合、ネクストホップに到達するための上記の検証とラベルスタックの結果を指定するリターンコードと、宛先に向かうネクストホップの ID を含むエコー応答を送信します。発信元は、TTL + 1 を含む次のエコー要求をビルドするためにエコー応答を処理します。宛先が FEC の出力であると応答するまで、プロセスが繰り返されます。

Nil FEC ターゲットに対する LSP Ping 操作

LSP Ping/Traceroute は LSP 破損の識別に使用されます。nil-fec ターゲット型は、既知のラベルスタックの接続性をテストするために使用できます。既存の LSP ping 手順に従います (詳細については、「[MPLS Lsp ping/Traceroute](#)」を参照してください)。ただし以下を変更します。

- 指定されたラベルスタックを使用してエコー要求パケットをビルドします。
- ラベルスタックの下部に明示的 null ラベルを追加します。
- ターゲットの FEC NilFEC とラベルの値が明示的 null であるラベルスタックの下部のラベルに設定されているエコー要求 FTS TLV をビルドします。

LSP Ping およびトレースルート NilFEC ターゲットを使用してセグメントルーティングを診断する方法

Nil FEC ターゲットに対する LSP Ping の使用

Nil FEC LSP の ping および traceroute の運用は、単に通常の MPLS の ping および traceroute の拡張機能です。ping mpls コマンドに **nil-fec labels <label, label...>** が追加されています。このコマンドは、指定に応じて MPLS ラベルスタックを使用してエコー要求メッセージを送信し、スタックの最下部に別の明示的ヌルを追加します。

```
ping mpls nil-fec labels <comma separated labels> output interface <tx-interface> nexthop
  <nexthop ip addr>
[repeat <count>]
[size <size> | sweep <min_size> <max_size> <increment>]
[timeout <seconds>]
[interval <milliseconds>]
[destination <addr_start> [<addr_end> [<addr_incr_mask> | <addr_incr>]]]
[source <addr>]
[exp <exp-value>]
```

```
[pad <pattern>]
[ttl <ttl>]
[reply [mode [ipv4 | router-alert | no-reply]]]
[dscp <dscp-bits>]
[pad-tlv]]
[verbose]
[force-disposition ra-label]
{dsmap | dmap [l2ecmp]} [hashkey {none | {ipv4 | ipv4-label-set {bitmap <bitmap_size>}}}]
```

詳細については、「[ping mpls](#)」を参照してください。

Nil FEC ターゲットに対する LSP Traceroute の使用

```
trace mpls nil-fec labels <comma separated labels> output interface <tx-interface>
nexthop <nexthop ip addr>
[timeout <seconds>]
[destination <addr_start> [<addr_end> [<addr_incr_mask> | <addr_incr>]]]
[source <addr> ]
[exp <exp-value>]
[ttl <ttl-max>]
[reply [mode [ipv4 | router-alert | no-reply]]]
[dscp <dscp-bits>]
[pad-tlv]]
[flags {fec | ttl}]
[hashkey ipv4 | ipv4-label-set {bitmap <bitmap_size>}]
```

詳細については、「[traceroute mpls](#)」を参照してください。

LSP Ping Nil FEC ターゲットのサポートの例

```
Node loopback IP address: 10.1.1.3                10.1.1.4                10.1.1.5
                        1.1.1.7
Node label:                16004                16005
                        16007
Nodes:                Arizona ----- Utah ----- Wyoming
----- Texas
Interface:                Eth1/0                Eth1/0
Interface IP address:    10.30.1.3                10.30.1.4
```

```
Device#sh mpls forwarding-table
Local   Outgoing  Prefix          Bytes Label  Outgoing  Next Hop
Label   Label    or Tunnel Id   Switched    interface
16      Pop Label 3333.3333.0000-Et1/0-10.30.1.3  \
        0        Et1/0         10.30.1.3
17      Pop Label 5555.5555.5555-Et1/1-10.90.1.5  \
        0        Et1/1         10.90.1.5
18      Pop Label 3333.3333.0253-Et0/2-102.102.102.2 \
        0        Et0/2         10.102.102.2
19      Pop Label 10.9.9.4/32    0           Et0/2         10.102.102.2
20      Pop Label 10.1.1.5/32    0           Et1/1         10.90.1.5
21      Pop Label 10.1.1.3/32    0           Et1/0         10.30.1.3
22      Pop Label 10.16.16.16/32 0           Et1/0         10.30.1.3
23      Pop Label 10.16.16.17/32 0           Et1/0         10.30.1.3
24      Pop Label 10.17.17.17/32 0           Et1/0         10.30.1.3
25      20        10.9.9.3/32    0           Et1/0         10.30.1.3
26      21        10.1.1.6/32    0           Et1/0         10.30.1.3
27      24        10.1.1.2/32    0           Et1/0         10.30.1.3
```

	28	10.1.1.2/32	0	Et1/1	10.90.1.5	
28	18	10.1.1.7/32	0	Et1/1	10.90.1.5	
29	27	10.9.9.7/32	0	Et1/1	10.90.1.5	
30	Pop Label	10.55.1.0/24	0	Et1/1	10.90.1.5	
31	Pop Label	10.19.1.0/24	0	Et1/0	10.30.1.3	
Local	Outgoing	Prefix	Bytes	Label	Outgoing	Next Hop
Label	Label	or Tunnel Id	Switched	interface		
32	Pop Label	10.1.1.0/24	0	Et1/0	10.30.1.3	
33	Pop Label	10.100.100.0/24	0	Et1/0	10.30.1.3	
34	Pop Label	10.1.1.0/24	0	Et1/0	10.30.1.3	
35	28	10.1.1.0/24	0	Et1/0	10.30.1.3	
36	29	10.101.101.0/24	0	Et1/0	10.30.1.3	
37	29	10.65.1.0/24	0	Et1/1	10.90.1.5	
38	33	10.104.104.0/24	0	Et1/0	10.30.1.3	
	39	10.104.104.0/24	0	Et1/1	10.90.1.5	
39	30	10.103.103.0/24	0	Et1/1	10.90.1.5	
16005	Pop Label	10.1.1.5/32	1782	Et1/1	10.90.1.5	
16006	16006	10.1.1.6/32	0	Et1/0	10.30.1.3	
16007	16007	10.1.1.7/32	0	Et1/1	10.90.1.5	
16017	16017	10.17.17.17/32	0	Et1/0	10.30.1.3	
16250	16250	10.9.9.3/32	0	Et1/0	10.30.1.3	
16252	16252	10.9.9.7/32	0	Et1/1	10.90.1.5	
16253	Pop Label	10.9.9.4/32	0	Et0/2	10.102.102.2	
17000	17000	10.16.16.16/32	0	Et1/0	10.30.1.3	
17002	17002	10.1.1.2/32	0	Et1/0	10.30.1.3	
	17002	10.1.1.2/32	0	Et1/1	10.90.1.5	

```
Device#ping mpls nil-fec labels 16005,16007 output interface ethernet 1/0 nexthop 10.30.1.4
repeat 1
```

```
Sending 1, 72-byte MPLS Echos with Nil FEC labels 16005,16007,
timeout is 2 seconds, send interval is 0 msec:
```

```
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'l' - Label switched with FEC change, 'd' - see DDMAP for return code,
'X' - unknown return code, 'x' - return code 0
```

```
Type escape sequence to abort.
```

```
!
```

```
Success rate is 100 percent (1/1), round-trip min/avg/max = 1/1/1 ms
Total Time Elapsed 0 ms
```

```
Device#traceroute mpls nil-fec labels 16005,16007 output interface ethernet 1/0 nexthop
10.30.1.4
```

```
Tracing MPLS Label Switched Path with Nil FEC labels 16005,16007, timeout is 2 seconds
```

```
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'l' - Label switched with FEC change, 'd' - see DDMAP for return code,
'X' - unknown return code, 'x' - return code 0
```

```
Type escape sequence to abort.
```

```
0 10.30.1.3 MRU 1500 [Labels: 16005/16007/explicit-null Exp: 0/0/0]
L 1 10.30.1.4 MRU 1500 [Labels: implicit-null/16007/explicit-null Exp: 0/0/0] 1 ms
L 2 10.90.1.5 MRU 1500 [Labels: implicit-null/explicit-null Exp: 0/0] 1 ms
```

! 3 10.55.1.7 1 ms

セグメントルーティング ネットワークのパス検証

MPLS OAM メカニズムは、MPLS エコー要求パケットで運ばれて FEC 検証のためにレスポンスによって使用されるさまざまなターゲット FEC スタックサブ TLV の使用によって、MPLS データプレーン パスのための障害検出および分離に役立ちます。新しいサブ TLV をセグメントルーティングに割り当てる必要があることは明らかですが、セグメントルーティングアーキテクチャの固有の性質により、パスの検証に関して追加の運用上の考慮が必要になります。

隣接関係セグメント ID の転送セマンティックは、セグメント ID をポップし、特定のリンクを介して特定のネイバーにパケットを送信することです。誤動作しているノードは、隣接関係セグメント ID を使用して、誤ったネイバーへまたは誤ったリンク上でパケットを転送することがあります。（誤って転送された隣接関係セグメント ID の）リスクにさらされているセグメント ID では、目的の厳格なトラバースが壊れているにもかかわらず、パケットが目的の宛先に到達できる可能性があります。MPLS traceroute はそのような逸脱の検出の役に立つ場合があります。

次のセグメント ID サブ TLV の形式は、ラベルスタック内の各ラベルに対応する FEC を運ぶターゲット FEC スタック TLV の原理に従います。これにより、ターゲット FEC スタック TLV に要求先ノードで受信したラベルスタックよりも多くの FEC が含まれている場合に LSP ping/traceroute 操作を機能させることができます。ターゲット FEC スタック TLV (タイプ 1)、リバースパスターゲット FEC スタック TLV (タイプ 16)、および応答パス TLV (タイプ 21) には、3 つの新しいサブ TLV が定義されています。

sub-Type	Value Field
34	IPv4 IGP-Prefix Segment ID
35	IPv6 IGP-Prefix Segment ID
36	IGP-Adjacency Segment ID

IGP プレフィックス SID FEC タイプ用の MPLS Ping および Traceroute

プレフィックス SID 用の MPLS ping および traceroute の操作は、次のようなさまざまな IGP シナリオでサポートされています。

- IS-IS レベルまたは OSPF エリア内
- IS-IS レベルまたは OSPF エリア間
- IS-IS から OSPF へ、および OSPF から IS-IS へのルート再配布

MPLS LSP ping 機能を使用して、LSP に沿った入力ラベルスイッチルータ (LSR) と出力 LSR 間の接続を確認します。MPLS LSP ping は、Internet Control Message Protocol (ICMP) のエコー要求メッセージと応答メッセージと同様に、LSP の検証に MPLS エコーの要求メッセージと応答メッセージを使用します。MPLS エコー要求パケットの宛先 IP アドレスは、ラベルスタックの選択に使用されるアドレスとは異なります。

MPLS LSP traceroute 機能を使用して、LSP の障害ポイントを隔離します。これはホップバイホップ エラーのローカリゼーションとパス トレースに使用されます。MPLS LSP traceroute 機能は、エコー要求を送送するパケットの存続可能時間 (TTL) 値の期限切れに依存します。MPLS エコー要求メッセージが中継ノードを見つけると TTL 値をチェックし、期限が切れている場合はコントロールプレーンにパケットが渡されます。それ以外の場合は、メッセージが転送されます。エコー メッセージがコントロールプレーンに渡されると、要求メッセージの内容に基づいて応答メッセージが生成されます。

MPLS LSP ツリー トレース (traceroute マルチパス) 操作は、IGP プレフィックス SID でもサポートされています。MPLS LSP ツリー トレースでは、LSP のすべての可能な等コスト マルチパス (ECMP) ルーティングパスを検出して宛先プレフィックス SID に到達する手段が提供されます。エコー要求パケットにエンコードされたマルチパスデータを使用して、ロードバランシング情報が照会されます。これにより、発信者は各 ECMP の実行を許可される場合があります。パケット TTL が応答ノードで期限切れになると、ノードはダウンストリーム パスのリストとマルチパス情報を返します。これにより、オペレータは MPLS エコー応答内の各パスを実行できるようになります。この操作は、すべての ECMP が検出されて検証されるまで、TTL 値が増加しながら各パスのホップごとに繰り返し実行されます。

MPLS エコー要求パケットは、ターゲット FEC スタック サブ TLV を伝送します。ターゲット FEC サブ TLV は、レスポндаによって FEC 検証のために使用されます。IGPIPv4 プレフィックス サブ TLV がターゲット FEC スタック サブ TLV に追加されました。IGP IPv4 プレフィックス サブ TLV には、プレフィックス SID、プレフィックス長、およびプロトコル (IS-IS または OSPF) が含まれています。

ノードセグメント ID をアドバタイズしたネットワーク ノードは、PHP (Penultimate Hop Popping) が有効かどうかに関係なく、ノードセグメント ID の pop 操作タイプを持つ FEC スタック変更サブ TLV を生成します。

IPv4 IGP プレフィックス セグメント ID の形式は次のとおりです。

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                                                 |
|                               IPv4 Prefix                       |
|                                                                 |
|Prefix Length | Protocol | Reserved |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

IPv6 IGP プレフィックス セグメント ID の形式は次のとおりです。

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                                                 |
|                               IPv6 Prefix                       |
|                                                                 |
|                                                                 |
|                                                                 |
+-----+-----+-----+-----+-----+-----+-----+-----+
|Prefix Length | Protocol | Reserved |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

IGP 隣接セグメント ID 用の MPLS Ping および Traceroute

隣接関係セグメント ID をアドバタイズしたノードのすぐ下流にあるネットワーク ノードは、隣接関係セグメント ID の「POP」操作のための FEC スタック変更サブ TLV を生成します。

IGP 隣接関係 SID の形式は次のとおりです。

```

0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
| Adj. Type | Protocol | Reserved |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Local Interface ID (4 or 16 octets) |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Remote Interface ID (4 or 16 octets) |
+-----+-----+-----+-----+-----+-----+-----+-----+
~
| Advertising Node Identifier (4 or 6 octets) |
+-----+-----+-----+-----+-----+-----+-----+-----+
~
| Receiving Node Identifier (4 or 6 octets) |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

MPLS Ping および Traceroute 用のセグメントルーティング MPLS トラフィック エンジニアリングの設定

```

ping mpls traffic-eng tunnel <tun-id>
[repeat <count>]
[size <size> | sweep <min_size> <max_size> <increment>]
[timeout <seconds>]
[interval <milliseconds>]
[destination <addr_start> [<addr_end> [<addr_incr_mask> | <addr_incr>]]]
[source <addr>]
[exp <exp-value>]
[pad <pattern>]
[ttl <ttl>]
[reply [mode [ipv4 | router-alert | no-reply]]]
[dscp <dscp-bits>]
[pad-tlv]
[verbose]
[output {interface <tx-interface>} [nexthop <nexthop ip addr>]]
[{{dmap | dmap [l2ecmp]} [hashkey {none | {ipv4 | ipv4-label-set {bitmap <bitmap_size>}}}}]

traceroute mpls [multipath] traffic-eng <tunnel-interface>
[timeout <seconds>]
[destination <addr_start> [<addr_end> [<addr_incr_mask> | <addr_incr>]]]
[source <addr> ]
[exp <exp-value>]
[ttl <ttl-max>]
[reply [mode [ipv4 | router-alert | no-reply]]]
[pad-tlv]
[output {interface <tx-interface>} [nexthop <nexthop ip addr>]]
[flags {fec | ttl}]
[hashkey ipv4 | ipv4-label-set {bitmap <bitmap_size>}]

```

MPLS Ping および Traceroute 用のセグメントルーティング MPLS IGP の設定

```
ping mpls ipv4 <prefix/prefix_length> [fec-type [ldp | bgp | generic | isis | ospf]]
[sr-path-type [ip | sid | strict-sid]]
[destination <addr_start> [<addr_end> [<addr_incr_mask> | <addr_incr>]]]
[source <addr>]
[exp <exp-value>]
[pad <pattern>]
[ttl <ttl>]
[reply [mode [ipv4 | router-alert | no-reply]]]
[dscp <dscp-bits>]
[pad-tlv]]
[verbose]
[output {interface <tx-interface>} [nexthop <nexthop ip addr>]]
[[dsmap | ddmmap [l2ecmp]] [hashkey {none | {ipv4 | ipv4-label-set {bitmap <bitmap_size>}}]]

traceroute mpls [multipath] ipv4 <prefix/prefix_length> [fec-type [ldp | bgp | generic
| isis | ospf]] [sr-path-type [ip | sid | strict-sid]]
[timeout <seconds>]
[destination <addr_start> [<addr_end> [<addr_incr_mask> | <addr_incr>]]]
[source <addr> ]
[exp <exp-value>]
[ttl <ttl-max>]
[reply [mode [ipv4 | router-alert | no-reply]]]
[pad-tlv]]
[output {interface <tx-interface>} [nexthop <nexthop ip addr>]]
[flags {fec | ttl}]
[hashkey ipv4 | ipv4-label-set {bitmap <bitmap_size>}]
```

- **fec-type** : IPv4 ターゲット FEC タイプ。デフォルトでヘッドエンド自動検出 FEC タイプを使用します。
- **sr-path-type** : セグメントルーティングパスのタイプの選択アルゴリズム。オプションが指定されている場合は、IP インポジションパスを使用します。



CHAPTER 16

セグメントルーティングでのシームレス BFD の使用

セグメントルーティング TE 機能は、シームレスな双方向フォワーディング検出 (S-BFD) のための情報サポートを提供します。

- セグメントルーティングでのシームレス BFD に関する機能情報, on page 177
- セグメントルーティングでのシームレス BFD 使用の制約事項 (178 ページ)
- セグメントルーティングでのシームレス BFD に関する情報, on page 178
- セグメントルーティングでのシームレス BFD の設定方法, on page 180
- セグメントルーティングでのシームレス BFD に関する追加情報, on page 182

セグメントルーティングでのシームレス BFD に関する機能情報

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、<https://cfng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

Table 14: セグメントルーティング TE 機能の機能情報

機能名	リリース	機能情報
セグメントルーティング TE の機能	Cisco IOS XE Amsterdam 17.3.2	シームレス双方向フォワーディング検出 (S-BFD) は、ネゴシエーションの側面の大部分が排除された BFD を使用する単純化されたメカニズムであり、迅速なプロビジョニング、ネットワークノードが開始するパスの監視の制御と柔軟性の向上などの利点を提供します。 次のコマンドが導入または変更されました。 address-family ipv4 strict-spf 、 bfd-template single-hop 、 index range 、 sbfd local-discriminator 、 show bfd neighbor 、 show isis segment-routing 、 show mpls forwarding-table 、 show mpls traffic tunnel 、 show mpls traffic-engineering 。

セグメントルーティングでのシームレス BFD 使用の制約事項

シームレス双方向フォワーディング (S-BFD) の制約事項

- シームレス双方向フォワーディング (S-BFD) は、セグメントルーティングトラフィックエンジニアリング (SR-TE) では IPv4 のみをサポートしています。IPv6 はサポートされていません。
- シングルホップの S-BFD セッションのみサポートされています。
- RSVP-TE は、S-BFD をサポートしていません。

セグメントルーティングでのシームレス BFD に関する情報

双方向フォワーディング検出とシームレス双方向フォワーディング検出 (S-BFD)

双方向フォワーディング検出 (BFD) は、すべてのメディアタイプ、カプセル化、トポロジ、およびルーティングプロトコルのために短時間で転送パス障害検出を提供するために設計された検出プロトコルです。

BFD は高速転送パス障害検出に加えて、ネットワーク管理者向けの整合性のある障害検出方法を提供します。ネットワーク管理者は BFD を使用して、ルーティングプロトコル毎に異なる hello

メカニズムの多様な検出時間でなく、一定の検出時間で転送パスの障害を検出できるため、ネットワークプロファイリングおよびプランニングが容易になります。また、再コンバージェンス時間の整合性が保たれ、予測可能になります。

シームレス双方向フォワーディング検出 (S-BFD) は、ネゴシエーションの側面の大部分が排除された BFD を使用する単純化されたメカニズムであり、迅速なプロビジョニング、ネットワーク ノードが開始するパスの監視の制御と柔軟性の向上などの利点を提供します。

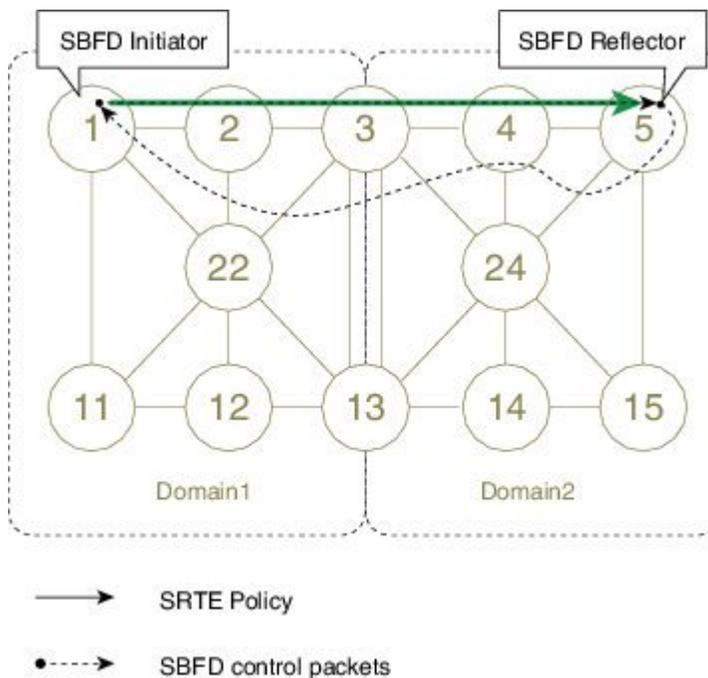
SBFDセッションが失敗した場合、S-BFDはSR-TEセッションをダウンさせます。また、S-BFDは、制御パケットの交換が少ないため、より高速なセッションの起動を提供します。S-BFDはSR-TEと関連付けられ、セッションを迅速に起動します。BFD状態はヘッドエンドでのみ維持され、それによってオーバーヘッドが減少します。

S-BFDは、セグメントルーティングでRFC 7880、RFC 7881のサポートを実装しています。

イニシエータとリフレクタ

SBFDはイニシエータとリフレクタを使用して非対称的な動作をします。次の図は、SBFDイニシエータとリフレクタの役割を示しています。

Figure 19: SBFD イニシエータとリフレクタ



イニシエータは、ネットワーク ノード上の SBFD セッションであり、SBFD パケットを送信することによってリモートエンティティへの連続性テストを実行します。イニシエータは、SBFD パケットをセグメントルーティングトラフィックエンジニアリング (SRTE) ポリシーに挿入します。イニシエータは、SBFD セッションをトリガーし、BFD 状態およびクライアントコンテキストを維持します。

リフレクタは、ローカルエンティティへの着信 SBFD 制御パケットをリッスンし、応答 SBFD 制御パケットを生成するネットワーク ノード上の SBFD セッションです。リフレクタはステートレスで、SBFD パケットのみをイニシエータに反映します。

ノードはイニシエータとリフレクタの両方になることができるため、異なる SBFD セッションを設定できます。

S-BFD は SR-TE IPv4 で有効でありサポート対象ですが、IPv6 はサポートされていません。SR-TE の場合、S-BFD 制御パケットは、前方向および逆方向にラベルスイッチされます。S-BFD の場合、テールエンドはリフレクタ ノードです。その他のノードをリフレクタにすることはできません。SR-TE で S-BFD を使用するとき、フォワードとリターンの方がラベルスイッチドパスである場合は、S-BFD をリフレクタ ノードで設定する必要はありません。

セグメントルーティングでのシームレス BFD の設定方法

セグメントルーティングのシームレス双方向フォワーディング検出 (S-BFD) の設定

S-BFD は、イニシエータとリフレクタの両方のノードで有効にする必要があります。



Note SR-TE で S-BFD を使用するとき、フォワードとリターンの方がラベルスイッチドパスである場合は、S-BFD をリフレクタ ノードで設定する必要はありません。

リフレクタ ノードでのシームレス双方向フォワーディング検出 (S-BFD) の有効化

リフレクタ ノードで S-BFD を設定するには、このタスクを実行します。

```
sbfd local-discriminator 10.55.55.55
```

イニシエータ ノードでのシームレス双方向フォワーディング検出 (S-BFD) の有効化

イニシエータ ノードで S-BFD を設定するには、このタスクを実行します。

```
bfd-template single-hop ABC
interval min-tx 300 min-rx 300 multiplier 10
```

シームレス双方向フォワーディング (S-BFD) でのセグメントルーティングトラフィック エンジニアリング トンネルの有効化

```
interface Tunnel56
 ip unnumbered Loopback11
 tunnel mode mpls traffic-eng
 tunnel destination 10.55.55.55 */IP address of Reflector node/*
 tunnel mpls traffic-eng path-option 1 dynamic segment-routing
 tunnel mpls traffic-eng bfd sbfd ABC
!
end
```

S-BFD 設定の確認

SUMMARY STEPS

1. `show mpls traffic-engineering tunnel tunnel-name`
2. `show bfd neighbors`

DETAILED STEPS

Procedure

ステップ 1 `show mpls traffic-engineering tunnel tunnel-name`

SR TE の状態と、S-BFD セッションの状態を確認します。

Example:

```
Router# sh mpls traffic-eng tunnel tunnel 56

Name: R1_t56                               (Tunnel56) Destination: 10.55.55.55
Status:
  Admin: up          Oper: up          Path: valid          Signalling: connected
  path option 1, (SEGMENT-ROUTING) type dynamic (Basis for Setup, path weight 12)

Config Parameters:
  Bandwidth: 0          kbps (Global) Priority: 7 7  Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  Path Selection:
    Protection: any (default)
  Path-selection Tiebreaker:
    Global: not set Tunnel Specific: not set Effective: min-fill (default)
  Hop Limit: disabled
  Cost Limit: disabled
  Path-invalidation timeout: 10000 msec (default), Action: Tear
  AutoRoute: disabled LockDown: disabled Loadshare: 0 [0] bw-based
  auto-bw: disabled
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No

SBFD configured with template: ABC
  Session type: CURRENT          State: UP          SBFD handle: 0x3
  LSP ID: 1
  Last uptime duration: 3 minutes, 35 seconds
  Last downtime duration: --
  Active Path Option Parameters:
  State: dynamic path option 1 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
Node Hop Count: 2
  History:
  Tunnel:
    Time since created: 4 minutes, 3 seconds
    Number of LSP IDs (Tun_Instances) used: 1
    Current LSP: [ID: 1]
    Uptime: 3 minutes, 36 seconds
Tun_Instance: 1
Segment-Routing Path Info (isis level-2)
  Segment0[Link]: 10.12.12.1 - 10.12.12.2, Label: 48
  Segment1[Link]: 10.25.25.2 - 10.25.25.5, Label: 35 !
```

ステップ 2 show bfd neighbors

BFD ネイバーが正しく確立されていることを確認します。

Example:

```
Router# show bfd neighbors
```

```
MPLS-TE SR Sessions
Interface      LSP ID(Type)          LD/RD          RH/RS          State
Tunnel56      1 (SR)                4097/926365495 Up              Up
```

セグメントルーティングでのシームレス BFD に関する追加情報

関連資料

関連項目	マニュアル タイトル
セグメントルーティング トラフィック エンジニアリングの設定	セグメントルーティング - トラフィック エンジニアリング

Table 15: 標準および RFC

標準/RFC	タイトル
draft-akiya-bfd-seamless-base-03	シームレス双方向フォワーディング検出 (S-BFD)
draft-ietf-isis-segment-routing-extensions-07	セグメント ルーティング対応の IS-IS 拡張
draft-ietf-spring-segment-routing-09	セグメント ルーティング アーキテクチャ
RFC 7880	シームレス双方向フォワーディング検出 (S-BFD)
RFC 7881	IPv4、IPv6、および MPLS 用のシームレス双方向フォワーディング検出 (S-BFD)



CHAPTER 17

セグメントルーティングでの SSPF の使用

セグメントルーティング TE 機能は、厳格な最短パス優先（SPF）の情報サポートを提供します。

- セグメントルーティングでの SSPF に関する機能情報, on page 183
- セグメントルーティングでの SSPF に関する情報, on page 184
- セグメントルーティングでの SSPF の設定方法, on page 185
- セグメントルーティングでの SSPF の追加情報, on page 187

セグメントルーティングでの SSPF に関する機能情報

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、<https://cfng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

Table 16: セグメントルーティング SSPF 機能の機能情報

機能名	リリース	機能情報
セグメントルーティング TE の機能	Cisco IOS XE Amsterdam 17.3.2	セグメントルーティング TE 機能は、厳格な最短パス優先（SPF）の情報サポートを提供します。 次のコマンドが導入または変更されました。 address-family ipv4 strict-spf、bfd-template single-hop、index range、sbfd local-discriminator、show bfd neighbor、show isis segment-routing、show mpls forwarding-table、show mpls traffic tunnel、show mpls traffic-engineering。

セグメントルーティングでの SSPF に関する情報

厳格な最短パス優先

セグメントルーティングは、次の 2 つのアルゴリズムをサポートします。

- **アルゴリズム 0**：これは、リンクメトリックに基づく最短パス優先 (SPF) アルゴリズムです。この最短パスアルゴリズムは、内部ゲートウェイプロトコル (IGP) によって計算されます。
- **アルゴリズム 1**：これは、リンクメトリックに基づく厳格な最短パス優先 (SSPF) アルゴリズムです。アルゴリズム 1 はアルゴリズム 0 と同じですが、パスに沿ったすべてのノードが SPF ルーティングの決定を遵守することを必要とします。ローカルポリシーは、転送の決定を変更しません。たとえば、パケットはローカルに設計されたパスを通じて転送されません。

アルゴリズムごとに異なる SID が同じプレフィックスに関連付けられます。

厳格な最短パス優先はデフォルトでサポートされていますが、厳格な SID を、セグメントルーティングをサポートする各ノードで少なくとも 1 つのノードアドレスに対して設定する必要があります。

厳格な最短パス優先を設定するためのアプローチ

厳格な SFP を設定するには、次の 2 つの方法があります。

- **connect-prefix-sid-map** コマンドを使用する：厳格な SFP はすべてのノードでグローバルに設定されます。ネットワークを厳格な SFP 対応にする（つまり、ISIS で厳格な SFP を入力するため）場合、すべてのノードをローカルの厳格な SFP SID で設定する必要があります。
- **セグメントルーティングマッピングサーバー**を使用する：ネットワーク内の 1 つのノードがマッピングサーバーとして設定され、残りのノードはクライアントとして機能します。

セグメントルーティングでの SSPF の設定方法

厳格な最短パス優先 (SPF) の設定

connect-prefix-sid-map コマンドを使用した厳格な最短パス優先の有効化

プロバイダーエッジデバイスでの最短パス優先の有効化

connect-prefix-sid-map コマンドを使用して厳格な最短パス優先を有効にする場合は、最初にプロバイダーエッジデバイスで、次にノードデバイスで、厳格な最短パス優先 (SPF) を設定する必要があります。次に示すのは、プロバイダーエッジデバイスで厳格な最短パス優先を有効にするための設定コード スニペットのサンプルです。

```
segment-routing mpls
connected-prefix-sid-map
  address-family ipv4
    10.10.10.10/32 index 100 range 1
  exit-address-family
  address-family ipv4 strict-spf
    10.10.10.10/32 index 1000 range 1 -----configure strict SPF locally
  exit-address-family
```

ノードデバイスでの最短パス優先の有効化

次に示すのは、ネットワーク内のノードで厳格な最短パス優先を有効にするための設定コード スニペットのサンプルで、ネットワーク内のすべてのノードで有効にする必要があります。

```
segment-routing mpls
connected-prefix-sid-map
  address-family ipv4
    10.20.20.20/32 index 110 range 1
  exit-address-family
  address-family ipv4 strict-spf
    10.20.20.20/32 index 1100 range 1
  exit-address-family
```

セグメントルーティング マッピング サーバーを使用した厳格な最短パス優先の有効化

セグメントルーティング マッピング サーバーとしてのノードの設定

次に示すのは、ノードをセグメントルーティング マッピング サーバーとして設定するための設定コード スニペットのサンプルです。

```
segment-routing mpls
mapping-server
  prefix-sid-map
    address-family ipv4
      10.10.10.10/32 index 100 range 1
      10.20.20.20/32 index 110 range 1
      10.30.30.30/32 index 120 range 1
      10.40.40.40/32 index 130 range 1
      10.50.50.50/32 index 140 range 1
```

ローカルプレフィックスをアドバタイズおよび受信するようにセグメントルーティングマッピングサーバーの設定

```

exit-address-family
address-family ipv4 strict-spf
 10.10.10.10/32 index 1000 range 1
 10.20.20.20/32 index 1100 range 1
 10.30.30.30/32 index 1200 range 1
 10.40.40.40/32 index 1300 range 1
 10.50.50.50/32 index 1400 range 1
 10.100.100.100/32 index 2000 range 1
exit-address-family

```

ローカルプレフィックスをアドバタイズおよび受信するようにセグメントルーティングマッピングサーバーの設定

次に示すのは、ローカルプレフィックスをアドバタイズおよび受信するようにセグメントルーティングマッピングサーバーを設定するための設定コードスニペットのサンプルです。

```

router isis SR
segment-routing mpls
  segment-routing prefix-sid-map advertise-local
  segment-routing prefix-sid-map receive

```

ISIS の SID のアドバタイズの確認

次に示すのは、ISIS が SID をアドバタイズしていることを確認するための設定コードスニペットのサンプルです。

```

Router# show isis segment-routing prefix-sid-map advertise strict-spf
Tag SR:
IS-IS Level-1 advertise prefix-sid maps:
Prefix          SID Index  Range  Flags
10.10.10.10/32  1000      1
10.20.20.20/32  1100      1
10.30.30.30/32  1200      1
10.40.40.40/32  1300      1
10.50.50.50/32  1400      1
10.100.100.100/32 2000      1
Tag SR:
IS-IS Level-2 advertise prefix-sid maps:
Prefix          SID Index  Range  Flags
10.10.10.10/32  1000      1
10.20.20.20/32  1100      1
10.30.30.30/32  1200      1
10.40.40.40/32  1300      1
10.50.50.50/32  1400      1
10.100.100.100/32 2000      1

```

次に示すのは、プロバイダーエッジデバイスが SRMS サーバーから厳格な最短パス優先の SID を受信することを確認するための設定コードスニペットのサンプルです。

```

Router# show isis segment-routing prefix-sid-map receive strict-spf
Tag SR:
IS-IS Level-1 receive prefix-sid maps:
Host          Prefix          SID Index  Range  Flags
P1            10.10.10.10/32  1000      1
              10.20.20.20/32  1100      1
              10.30.30.30/32  1200      1
              10.40.40.40/32  1300      1
              10.50.50.50/32  1400      1
              10.100.100.100/32 2000      1
Tag SR:
IS-IS Level-2 receive prefix-sid maps:
Host          Prefix          SID Index  Range  Flags

```

P1	10.10.10.10/32	1000	1
	10.20.20.20/32	1100	1
	10.30.30.30/32	1200	1
	10.40.40.40/32	1300	1
	10.50.50.50/32	1400	1
	10.100.100.100/32	2000	1

セグメントルーティングでの SSPF の追加情報

関連資料

関連項目	マニュアルタイトル
セグメントルーティングトラフィックエンジニアリングの設定	セグメントルーティング - トラフィックエンジニアリング



第 18 章

ダイナミック PCC

ステートフルパス計算要素プロトコル (PCEP) により、ルータはステートフルパス計算要素 (PCE) に対して、Resource Reservation Protocol (RSVP) プロトコルまたはセグメントルーティングトラフィックエンジニアリング (SR-TE) のいずれかを使用して確立されたラベルスイッチドパス (LSP) をレポートし、必要に応じて委任することができます。

PCE に委任された LSP は、PCE によって更新でき、ステートフル PCE はパス計算クライアント (PCC) に LSP のパスを計算して提供することができます。

SR-TE および RSVP-TE LSP では、OSPF や ISIS などのリンクステートルーティングプロトコルによって、トラフィックエンジニアリングトポロジを配布および学習する必要があります。ステートフル PCE では、BGP リンクステートプロトコルを使用してトラフィックエンジニアリングトポロジを学習できます。ネットワーク内のすべてまたは一部の中間ノードで TE の IGP 拡張がサポートされていない場合は、verbatim パス オプションを使用できます。

- [ダイナミック PCC に関する情報 \(189 ページ\)](#)
- [ダイナミック PCC の設定方法 \(190 ページ\)](#)
- [ダイナミック PCC の確認 \(191 ページ\)](#)
- [ダイナミック PCC を使用した Verbatim パス オプションの確認 \(194 ページ\)](#)
- [ダイナミック PCC の機能情報 \(195 ページ\)](#)

ダイナミック PCC に関する情報

パス計算要素プロトコル関数

パス計算要素プロトコル (PCEP) セッションは、プロトコルメッセージを使用した PCC と PCE の間の TCP セッションです。PCEP 関数は PCC 関数に基づいて検証されます。構成と検証により、要求が受け入れられ、クライアントからの PCReq メッセージに基づいてパスの計算が提供されることが示されます。パッシブ レポートでは、ルータは PCE に委任するのではなく、トンネルをレポートすることができます。PCE は、トンネルを変更できなくてもトンネルを認識しています。

PCEP 関数は、ルータが制御するトンネルと PCE 委任トンネルの両方ともネットワークにある場合に便利です。PCE は両方のトンネルを認識し、パス計算の正確な決定を行うことができます。

冗長パス計算要素

冗長性のために、冗長 PCE サーバーの展開が必要になる場合があります。PCC は、LSP を委任するためにステータフルな PCE を選択するのに優先順位を使用します。優先順位は 0 から 255 の間の任意の値を取ることができます。デフォルトの優先順位は 255 です。アクティブな PCEP セッションを持つ複数のステータフル PCE がある場合、PCC は最も低い優先順位値を持つ PCE を選択します。プライマリ PCE サーバーセッションがダウンした場合、PCC ルータは次に利用可能な PCE サーバーにすべてのトンネルを再委任します。冗長 PCE の場合は、以下の CLI を使用できます。

```
R2(config)#mpls traffic-eng pcc peer 10.77.77.77 source 10.22.22.22 precedence 255
R2(config)#mpls traffic-eng pcc peer 10.88.88.88 source 10.22.22.22 precedence 100
!
```

上記の例では、IP アドレス 10.88.88.88 を持つ PCE サーバーは、優先順位値が低いため、プライマリ PCE サーバーです。

ダイナミック PCC の設定方法

ダイナミック PCC のグローバルな設定

ダイナミック PCC をグローバルに設定するには、次のタスクを実行します

```
enable
configure terminal
mpls traffic-eng tunnels
mpls traffic-eng pcc peer 10.0.0.1 ----(10.0.0.1 is the PCE server address)
mpls traffic-eng pcc report-all
end
```



(注) **mpls traffic-eng pcc report-all** は、PCE/PCC 基本運用委任トンネルに必須ではありません。ローカルで計算された LSP を PCE サーバーにレポートする必要があります。

インターフェイスでのダイナミック PCC の設定

インターフェイス上でダイナミック PCC を設定するには、次のタスクを実行します

```
interface Tunnell
ip unnumbered Loopback0
```

```
tunnel mode mpls traffic-eng
tunnel destination 10.7.7.7
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 5 5
tunnel mpls traffic-eng bandwidth 200
tunnel mpls traffic-eng path-option 10 dynamic pce segment-routing
end
```

Verbatim パス オプションを使用したダイナミック PCC の設定

verbatim パス オプションを使用してダイナミック PCC を有効にするには、SR-TE トンネル インターフェイスの下で次の CLI を使用します。

```
R1#
interface Tunnel2
ip unnumbered Loopback11
tunnel mode mpls traffic-eng
tunnel destination 10.66.66.66
tunnel mpls traffic-eng autoroute destination
tunnel mpls traffic-eng path-option 1 dynamic segment-routing pce verbatim
```

ダイナミック PCC の確認

次に、**show pce client peer detail** コマンドの出力例を示します。

```
Device# show pce client peer detail

PCC's peer database:
-----

Peer address: 10.1.1.1
State up
Capabilities: Stateful, Update, Segment-Routing
PCEP has been up for: 23:44:58
PCEP session ID: local 1, remote: 0
Sending KA every 30 seconds
Minimum acceptable KA interval: 20 seconds
Peer timeout after 120 seconds
Statistics:
  Keepalive messages: rx      2798 tx      2112
  Request messages:   rx         0 tx         32
  Reply messages:    rx        32 tx         0
  Error messages:    rx         0 tx         0
  Open messages:     rx         1 tx         1
  Report messages:   rx         0 tx         57
  Update messages:   rx        72 tx         0
```

次に、LSP の詳細を表示する **show mpls traffic-eng tunnels tunnel 1** コマンドの出力例を示します。

```
Device# show mpls traffic-eng tunnels tunnel 1

Name: dl_t1                               (Tunnel1) Destination: 10.7.7.7
Status:
```

```

Admin: up          Oper: up          Path: valid          Signalling: connected
path option 10, (SEGMENT-ROUTING) (PCE) type dynamic (Basis for Setup, path weight
0)

Config Parameters:
Bandwidth: 200      kbps (Global) Priority: 5 5 Affinity: 0x0/0xFFFF
Metric Type: TE (default)
Path Selection:
Protection: any (default)
Path-selection Tiebreaker:
Global: not set Tunnel Specific: not set Effective: min-fill (default)
Hop Limit: disabled
Cost Limit: disabled
Path-invalidation timeout: 10000 msec (default), Action: Tear
AutoRoute: enabled LockDown: disabled Loadshare: 200 [10000000] bw-based
auto-bw: disabled
Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
State: dynamic path option 10 is active
BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

PCEP Info:
Delegation state: Working: yes Protect: no
Current Path Info:
Request status: processed
Created via PCRep message from PCE server: 10.1.1.1
Reported paths:
Tunnel Name: csr551_t2001
LSPs:
LSP[0]:
source 10.2.2.2, destination 10.7.7.7, tunnel ID 1, LSP ID 5
State: Admin up, Operation active
Setup type: SR
Bandwidth: signaled 0
LSP object:
PLSP-ID 0x807D1, flags: D:0 S:0 R:0 A:1 O:2
Reported path:
Metric type: TE, Accumulated Metric 0

History:
Tunnel:
Time since created: 34 minutes, 3 seconds
Time since path change: 1 minutes, 44 seconds
Number of LSP IDs (Tun_Instances) used: 5
Current LSP: [ID: 5]
Uptime: 1 minutes, 44 seconds
Prior LSP: [ID: 3]
ID: path option unknown
Removal Trigger: path verification failed
Tun_Instance: 5
Segment-Routing Path Info (isis level-1)
Segment0[Node]: 10.3.3.3, Label: 20270
Segment1[Node]: 10.6.6.6, Label: 20120
Segment2[Node]: 10.7.7.7, Label: 20210

```

次に、**show pce client lsp detail** コマンドの出力例を示します。

```

Device# show pce client lsp detail

PCC's tunnel database:
-----
Tunnel Name: dl_t1
LSPs:

```

```
LSP[0]:
  source 10.2.2.2, destination 10.7.7.7, tunnel ID 1, LSP ID 5
  State: Admin up, Operation active
  Setup type: SR
  Bandwidth: signaled 0
  LSP object:
    PLSP-ID 0x807D1, flags: D:0 S:0 R:0 A:1 O:2
  Reported path:
    Metric type: TE, Accumulated Metric 0
```

次に、トンネルの委任を示す **show pce lsp detail** コマンドの出力例を示します。

```
Device# show pce lsp detail

Thu Jul  7 10:24:30.836 EDT

PCE's tunnel database:
-----
PCC 10.103.2.1:

Tunnel Name: dl_t1
LSPs:
LSP[0]:
  source 10.2.2.2, destination 10.7.7.7, tunnel ID 1, LSP ID 5
  State: Admin up, Operation active
  Binding SID: 0
  PCEP information:
    plsp-id 526289, flags: D:1 S:0 R:0 A:1 O:2
  Reported path:
    Metric type: TE, Accumulated Metric 0
    SID[0]: Node, Label 20270, Address 10.3.3.3
    SID[1]: Node, Label 20120, Address 10.6.6.6
    SID[2]: Node, Label 20210, Address 10.7.7.7
  Computed path:
    Metric type: TE, Accumulated Metric 30
    SID[0]: Node, Label 20270, Address 10.3.3.3
    SID[1]: Node, Label 20120, Address 10.6.6.6
    SID[2]: Node, Label 20210, Address 10.7.7.7
  Recorded path:
    None
```

次に、レポートされたトンネルについての **show pce client lsp detail** コマンドの出力例を示します。

```
Device# show pce client lsp detail

PCC's tunnel database:
-----
Tunnel Name: dl_t2
LSPs:
LSP[0]:
  source 10.2.2.2, destination 10.7.7.7, tunnel ID 2, LSP ID 1
  State: Admin up, Operation active
  Setup type: SR
  Bandwidth: signaled 0
  LSP object:
    PLSP-ID 0x807D2, flags: D:0 S:0 R:0 A:1 O:2
  Reported path:
    Metric type: TE, Accumulated Metric 30
```

次に、トンネルが委任されていないことを示す **show pce lsp detail** コマンドの出力例を示します。

```
Device# show pce lsp detail

Thu Jul  7 10:29:48.754 EDT

PCE's tunnel database:
-----
PCC 10.0.0.1:

Tunnel Name: dl_t2
LSPs:
LSP[0]:
  source 10.2.2.2, destination 10.7.7.7, tunnel ID 2, LSP ID 1
  State: Admin up, Operation active
  Binding SID: 0
  PCEP information:
    plsp-id 526290, flags: D:0 S:0 R:0 A:1 O:2
  Reported path:
    Metric type: TE, Accumulated Metric 30
    SID[0]: Adj, Label 74, Address: local 172.16.0.1 remote 172.16.0.2
    SID[1]: Adj, Label 63, Address: local 172.17.0.1 remote 172.17.0.2
    SID[2]: Adj, Label 67, Address: local 172.18.0.1 remote 172.18.0.2
    SID[3]: Node, Label unknownAddress 10.7.7.7
  Computed path:
    None
  Recorded path:
    None
```

ダイナミック PCC を使用した Verbatim パス オプションの確認

verbatim パス オプションを使用して適切な操作を確認するには、次のコマンドを使用します。

```
R1#sh mpls tr tun tun 2
Name: R1_t2 (Tunnel2) Destination: 10.66.66.66
Status:
  Admin: up      Oper: up      Path: valid      Signalling: connected
  path option 1, (SEGMENT-ROUTING) (PCE) type dynamic (verbatim) (Basis for Setup)

Config Parameters:
  Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (interface)
  Path Selection:
    Protection: any (default)
  Path-selection Tiebreaker:
    Global: not set Tunnel Specific: not set Effective: min-fill (default)
  Hop Limit: disabled [ignore: Verbatim Path Option]
  Cost Limit: disabled
  Path-invalidation timeout: 10000 msec (default), Action: Tear
  AutoRoute: disabled LockDown: disabled Loadshare: 0 [0] bw-based
  AutoRoute destination: enabled
  auto-bw: disabled
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
```

```

State: dynamic path option 1 is active
BandwidthOverride: disabled LockDown: disabled Verbatim: enabled

PCEP Info:
Delegation state: Working: yes Protect: no
Delegation peer: 10.77.77.77
Working Path Info:
Request status: processed
Created via PCRep message from PCE server: 10.77.77.77
PCE metric: 4, type: TE
Reported paths:
Tunnel Name: Tunnel2_w
LSPs:
LSP[0]:
source 10.11.11.11, destination 10.66.66.66, tunnel ID 2, LSP ID 1
State: Admin up, Operation active
Binding SID: 17
Setup type: SR
Bandwidth: requested 0, used 0
LSP object:
PLSP-ID 0x80002, flags: D:0 S:0 R:0 A:1 O:2
ERO:
SID[0]: Adj, Label 24, NAI: local 10.12.12.1 remote 10.12.12.2
SID[1]: Adj, Label 26, NAI: local 10.25.25.2 remote 10.25.25.5
SID[2]: Adj, Label 22, NAI: local 10.56.56.5 remote 10.56.56.6

History:
Tunnel:
Time since created: 39 days, 19 hours, 9 minutes
Time since path change: 1 minutes, 3 seconds
Number of LSP IDs (Tun_Instances) used: 1
Current LSP: [ID: 1]
Uptime: 1 minutes, 3 seconds
Tun_Instance: 1
Segment-Routing Path Info (IGP information is not used)
Segment0[Link]: 10.12.12.1 - 10.12.12.2, Label: 24
Segment1[Link]: 10.25.25.2 - 10.25.25.5, Label: 26
Segment2[Link]: 10.56.56.5 - 10.56.56.6, Label: 22
!
end

```

ダイナミック PCC の機能情報

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、<https://cfngn.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

表 17: ダイナミック PCC の機能情報

機能名	リリース	機能情報
ダイナミック PCC	Cisco IOS XE Amsterdam 17.3.2	<p>動的パス計算クライアント (PCC) 機能は、パス計算要素 (PCE) に委任された LSP をサポートします。ダイナミック PCC は、RSVP-TE と SR-TE の両方をサポートします。</p> <p>次のコマンドが追加または修正されました。</p> <p>show pce client peer detail、 show mpls traffic-eng tunnels tunnel 1、 show pce client lsp detail、 show pce lsp detail。</p>



CHAPTER 19

SR : PCE 開始の LSP

SR : PCE 開始の LSP 機能は、セグメントルーティング ネットワーク上のステートフル PCE モデルで PCE によって開始される LSP をサポートします。

- [SR の前提条件 : PCE 開始の LSP, on page 197](#)
- [SR の制約事項 : PCE 開始の LSP, on page 197](#)
- [SR に関する情報 : PCE 開始の LSP, on page 197](#)
- [SR の設定方法 : PCE 開始の LSP, on page 199](#)
- [SR の追加情報 : PCE 開始の LSP, on page 205](#)
- [SR の機能情報 : PCE 開始の LSP, on page 205](#)

SR の前提条件 : PCE 開始の LSP

- ダイナミック PCC 機能を設定する必要があります。
- 自動トンネルを PCC で有効にする必要があります。

SR の制約事項 : PCE 開始の LSP

- SR : PCE 開始 LSP 機能は、基本的な LSP の生成のみをサポートし、TE の属性をサポートしていません。

SR に関する情報 : PCE 開始の LSP

パス計算要素プロトコルの概要

draft-ietf-pce-stateful-pce-21 で説明されているステートフルパス計算要素プロトコル (PCEP) により、ルータはステートフルパス計算要素 (PCE) に対して、Resource Reservation Protocol (RSVP) プロトコルまたはセグメントルーティングトラフィックエンジニアリング (SR-TE) のいずれかを使用して確立されたラベルスイッチドパス (LSP) をレポートし、必要に応じて

委任することができます。PCE に委任された LSP は、PCE によって更新でき、ステートフル PCE はパス計算クライアント (PCC) に LSP のパスを計算して提供することができます。

ステートフル PCE モデル (**draft-ietf-pce-pce-initiated-lsp-11**) において PCE 開始 LSP 設定のための PCEP 拡張は、RFC4657 に準拠した PCEP セッション全体で TE LSP のステートフルな制御を可能にするために、PCEP に対する一連の拡張を規定しています。ステートフル PCE モデルで PCE 開始 LSP 設定のための PCEP 拡張は、次の情報を提供します。

- PCC での LSP の設定
- PCE への LSP の制御の委任

SR : PCE 開始の LSP

SR : PCE 開始 LSP 機能を使用すると、クライアントは PCE サーバーから LSP を作成、セットアップ、制御、削除することができます。これは PCE 開始メッセージを介して PCC 上で LSP の作成と削除を制御します。PCE 開始 LSP は、LSP を開始した PCE サーバーに自動的に委任されます。PCE クライアントは LSP 開始メッセージを処理します。LSP 開始メッセージを使用することにより、PCE クライアントは LSP を作成または削除することができます。

ルートプロセッサ (RP) でフェールオーバーが発生すると、フェールオーバーによって RP がネットワークから切断されます。接続を再確立するには、PCE サーバーは、クライアント上で PCE 開始 LSP を回収するために LSP 開始メッセージを再送する必要があり、そうしないとクライアントが作成した PCE 開始 LSP が自動的に削除されます。

PCC との PCEP セッションを確立するために **pce** コマンドを使用する必要があります。**force auto-route** コマンドは、自動ルート アナウンス メッセージを介してエリア内で、および自動ルート宛先メッセージを介してエリア間で LSP をアダプタイズするために使用されます。自動ルート アナウンスを使用するかまたは自動ルート宛先を使用するかは、宛先 IP アドレスに応じてデバイスによって実行されます。開始された LSP に対して **force auto-route** コマンドを有効にすると、スタティックルートを手動で設定してトラフィックをルーティングするのではなく、TE トンネル経由でトラフィックを自動的にルーティングできます。自動ルートアナウンス メッセージは、宛先ルータおよびダウンストリーム ルータによってアナウンスされたルート、トンネルを介して到達可能なヘッドエンド デバイスのルーティング テーブルにインストールします。

PCC 構成には、各 PCE の IP アドレス (プライマリとスタンバイの両方、またはさらにその他) が含まれます。各 PCE の優先順位を明示的に指定することができます。2 つの PCE の優先順位が同じである場合、小さい IP アドレスを持つ PCE の方が優先順位が高くなります。

単一および冗長 PCE 操作

SR : PCE 開始 LSP 機能は、単一および冗長 PCE 操作をサポートしています。単一 PCE 操作では、PCE が失敗すると、PCC は状態がタイムアウト (60 秒) するまで待ち、LSP を削除します。

冗長 PCE 操作では、タイマーの満了前に Representational state transfer (REST) 呼び出しがスタンバイ PCE に対して開始された場合は、開始された LSP が保持され、そうでない場合は LSP が削除されます。



Note プライマリ PCE が失敗した場合は、スタンバイ PCE に対して REST コールをもう一度開始する必要があります、コールにスタンバイ PCE の IP アドレスが含まれる必要があります。

冗長 PCE 操作では、PCC 構成は LSP のためのプライマリおよびスタンバイ IP アドレスの両方を含み、より低い優先順位の IP アドレスがプライマリ PCE になります。同じ優先順位の場合は IP アドレスが比較されます。

SR の設定方法 : PCE 開始の LSP

PCC との PCEP セッションの確立

このタスクを実行して、PCEP セッション PCE サーバー XR ベースの XTC サーバーを設定します。

```
configure terminal
pce
  address ipv4 192.0.2.1
end
```

IP アドレス 192.0.2.1 は、トランスポートコントローラの IP アドレスです。

ネットワークでの LSP のアドバタイジング

```
configure terminal
mpls traffic-eng pcc peer 192.0.2.1 source 203.0.113.1 force-autoroute
end
```

上のコードスニペットでは、192.0.2.1 は PCE IP アドレスで、203.0.113.1 は PCEP セッションを確立するための PCC 送信元アドレスです。

PCC に対する PCE の優先順位の指定

```
configure terminal
mpls traffic-eng pcc peer 192.0.2.1 source 203.0.113.1 force autoroute precedence 255
mpls traffic-eng pcc peer 192.0.2.2 source 203.0.113.1 force-autoroute precedence 100
end
```

上記のコードスニペットでは、100 はデフォルトの優先順位である 255 よりも低い優先順位です。したがって、IP アドレス 192.0.2.2 を持つデバイスがプライマリ PCE になり、192.0.2.1 を持つデバイスがスタンバイ PCE になります。

PCE サーバー優先順位の再評価のトリガー

PCE サーバーの優先順位の変更は、PCE サーバーの障害とは見なされません。したがって、優先順位の変更によって、再委託タイムアウトが発生したり、または PCC で PCE サーバーへの LSP 委任の再評価がトリガーされることはありません。

CLI 再構成後の PCE サーバーへの LSP 委任の再評価は、TE 再最適化タイマーによって制御されます。デフォルトでは、TE 再最適化タイマーは 3600 秒に設定されています。

PCE サーバーの優先順位を変更した後、または新しい PCE サーバーを追加した後で、PCC から PCE サーバーへの LSP 委任の再評価を高速化することができます。これを行うには、特権 EXEC モードで次のコマンドを使用して、TE 再最適化を手動でトリガーします。

```
mpls traffic-eng reoptimize
```

LSP 構成の確認

SUMMARY STEPS

1. **show pce ipv4 peer detail**
2. **show pce lsp detail**
3. **show pce client peer**
4. **show mpls traffic-eng tunnel tunnel *number***

DETAILED STEPS

Procedure

ステップ 1 show pce ipv4 peer detail

このコマンドを使用して、PCE で PCEP セッションの詳細を確認します。この例では、インスタンス化という用語は、PCE が開始された LSP をサポートすることを示します。

```
Device# show pce ipv4 peer detail
```

```
PCE's peer database:
```

```
-----
```

```
Peer address: 10.2.2.2----' PCC IP address
```

```
State: Up
```

```
Capabilities: Stateful, Segment-Routing, Update, Instantiation
```

ステップ 2 show pce lsp detail

このコマンドを使用して、PCE で開始された LSP を確認します。

```
Device# show pce lsp detail
```

```
PCE's tunnel database:
```

```
-----
```

```
PCC 10.52.2.2 ----' PCC IP address
```

```
Tunnel Name: Test1-----' tunnel name set by REST Call
```

```
LSPs:
```

```
LSP[0]:
```

```
source 10.52.2.2, destination 10.57.7.7, tunnel ID 2000, LSP ID 1
```

```
State: Admin up, Operation active
```

```
Binding SID: 26
```

```
PCEP information:
```

```
plsp-id 526288, flags: D:1 S:0 R:0 A:1 O:2 C:1
```

```
LSP Role: Single LSP
```

```
State-sync PCE: None
```

```
PCC: 10.52.2.2
```

```
LSP is subdelegated to: None
```

```
Reported path:
```

```
Metric type: TE, Accumulated Metric 2
```

```
SID[0]: Adj, Label 25, Address: local 10.105.3.1 remote 10.105.3.2
```

```
SID[1]: Adj, Label 24, Address: local 10.104.8.2 remote 10.104.8.1
```

```
SID[2]: Adj, Label 38, Address: local 10.107.10.1 remote 10.107.10.2
```

```
Computed path: (Local PCE)
```

```

None

Computed Time: Not computed yet

Recorded path:

None

Disjoint Group Information:

None

```

ステップ3 show pce client peer

このコマンドを使用して、PCC での PCEP セッション出力を確認し、**force-autoroute** コマンドが有効かどうかを確認します。

```

Device# show pce client peer

PCC's peer database:
-----

Peer address: 10.51.1.1, Precedence: 255

State up

Capabilities: Stateful, Update, Segment-Routing, Force-autoroute

```

ステップ4 show mpls traffic-eng tunnel tunnel number

このコマンドを使用して、PCC で開始された LSP トンネルの出力を確認します。

```

Device# show mpls traffic-eng tunnel tunnel 2000

Name: Test1 (Tunnel2000) Destination: 10.57.7.7 Ifhandle: 0x11E
(auto-tunnel for pce client)

Status:

Admin: up Oper: up Path: valid Signalling: connected

path option 1, (SEGMENT-ROUTING) (PCE) type dynamic (Basis for Setup)

```

Config Parameters:

Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF

Metric Type: TE (default)

Path Selection:

Protection: any (default)

Path-selection Tiebreaker:

Global: not set Tunnel Specific: not set Effective: min-fill (default)

Hop Limit: disabled

Cost Limit: disabled

Path-invalidation timeout: 10000 msec (default), Action: Tear

AutoRoute: enabled LockDown: disabled Loadshare: 0 [0] bw-based

auto-bw: disabled

Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No

Active Path Option Parameters:

State: dynamic path option 1 is active

BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

PCEP Info:

Delegation state: Working: yes Protect: no

Delegation peer: 10.51.1.1

Working Path Info:

Request status: delegated

SRP-ID: 1

Created via PCInitiate message from PCE server: 10.51.1.1-----' IP address

PCE metric: 2, type: TE

Reported paths:

Tunnel Name: Test1

LSPs:

LSP[0]:

source 10.52.2.2, destination 10.57.7.7, tunnel ID 2000, LSP ID 1

State: Admin up, Operation active

Binding SID: 26

Setup type: SR

Bandwidth: requested 0, used 0

LSP object:

PLSP-ID 0x807D0, flags: D:0 S:0 R:0 A:1 O:2

Metric type: TE, Accumulated Metric 2

ERO:

SID[0]: Adj, Label 25, NAI: local 10.105.3.1 remote 10.105.3.2

SID[1]: Adj, Label 24, NAI: local 10.104.8.2 remote 10.104.8.1

SID[2]: Adj, Label 38, NAI: local 10.107.10.1 remote 10.107.10.2

PLSP Event History (most recent first):

Mon Jul 17 08:55:04.448: PCRpt update LSP-ID:1, SRP-ID:1, PST:1, METRIC_TYPE:2, REQ_BW:0, USED_BW:0

Mon Jul 17 08:55:04.436: PCRpt create LSP-ID:1, SRP-ID:1, PST:1, METRIC_TYPE:2, REQ_BW:0, USED_BW:0

History:

Tunnel:

Time since created: 2 hours, 42 minutes

Time since path change: 2 hours, 42 minutes

Number of LSP IDs (Tun_Instances) used: 1

```

Current LSP: [ID: 1]

Uptime: 2 hours, 42 minutes

Tun_Instance: 1

Segment-Routing Path Info (isis level-2)

Segment0[Link]: 10.105.3.1 - 10.105.3.2, Label: 25

Segment1[Link]: 10.104.8.2 - 10.104.8.1, Label: 24

Segment2[Link]: 10.107.10.1 - 10.107.10.2, Label: 38

```

SR の追加情報 : PCE 開始の LSP

標準および RFC

標準/RFC	タイトル
draft-ietf-pce-pce-initiated-lsp-11	ステートフル <i>PCE</i> モデルでの <i>PCE</i> 開始 <i>LSP</i> 設定の <i>PCEP</i> 拡張機能
RFC 5440	パス計算要素 (<i>PCE</i>) 通信プロトコル (<i>PCEP</i>)
RFC 8231	パス計算要素 (<i>PCE</i>) 通信プロトコルの一般要件

SR の機能情報 : PCE 開始の LSP

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、<https://cfng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

Table 18: SR の機能情報 : PCE 開始の LSP

機能名	リリース	機能情報
SR : PCE 開始の LSP	Cisco IOS XE Amsterdam 17.3.2	SR : PCE 開始 LSP は、セグメントルーティング ネットワーク上のステートフル PCE モデルで PCE によって開始される LSP をサポートします。 次のコマンドが導入または変更されました。 mpls traffic-eng pcc、pce、show mpls traffic-eng tunnel、show pce client peer、show pce ipv4 peer、show pce lsp



CHAPTER 20

ISIS - SR : uLoop 回避

ISIS - SR : uLoop 回避機能により、ISIS ローカルマイクロループ保護機能が拡張され、リンクダウンイベントまたはリンクアップイベント後のネットワーク コンバージェンス時にマイクロループが発生するのを防ぐことができます。

- [ISIS - SR の前提条件 : uLoop 回避, on page 207](#)
- [ISIS - SR の制約事項 : uLoop 回避, on page 207](#)
- [ISIS - SR に関する情報 : uLoop 回避, on page 208](#)
- [ISIS - SR を有効にする方法 : uLoop 回避, on page 212](#)
- [ISIS - SR の追加情報 : uLoop 回避, on page 213](#)
- [ISIS - SR の機能情報 : uLoop 回避, on page 214](#)

ISIS - SR の前提条件 : uLoop 回避

- ISIS - SR : uLoop 回避機能はデフォルトで無効になっています。トポロジに依存しないループフリー代替 (TI-LFA) 機能が設定されている場合、この機能は自動的に有効になります。詳細については、IS-IS モジュールでのセグメントルーティングの使用の「トポロジに依存しない LFA」のセクションを参照してください。

ISIS - SR の制約事項 : uLoop 回避

- ISIS - SR : uLoop 回避機能は LAN ネットワークで同じサブネットの 2 ノードをサポートします。

ISIS - SR に関する情報 : uLoop 回避

マイクロループ

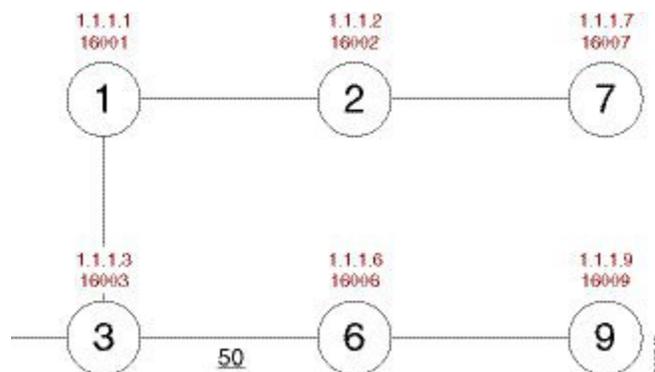
リンクまたはネットワーク デバイスで発生した障害や復旧のためにネットワーク トポロジに変更が生じると、IP Fast Reroute によって迅速なネットワーク コンバージェンスが行われます。このとき、定期的なコンバージェンス機能によってトラフィックが新しく計算されたベストパス（別名、ポスト コンバージェンス パス）へ移動されるまで、事前に計算されていたバックアップパスにトラフィックが移動されます。このネットワーク コンバージェンスにより、トポロジ内で直接または間接的に接続された2台のデバイス間で、マイクロループが短期間発生する可能性があります。マイクロループは、ネットワーク内の異なるノードが異なるタイミングで互いに別々に代替パスを計算したときに発生します。たとえば、あるノードがコンバージェンスを実行し、ネイバー ノードにトラフィックを送信したときに、そのネイバー ノードでまだコンバージョンが完了していないと、その2つのノードでトラフィックがループする可能性があります。

マイクロループによってトラフィックが損失する場合も、損失しない場合もあります。マイクロループが発生している期間が短ければ、つまりネットワークのコンバージェンスが迅速に行われれば、存続可能時間（TTL）が期限切れになるまでの短い期間、パケットがループする可能性があります。最終的には、パケットは宛先に転送されます。マイクロループの期間が長くなる、つまりネットワーク内のいずれかのルータでコンバージェンスに時間がかかっていると、パケットで TTL が期限切れになったり、パケット レートが帯域幅を超過したり、パケットの順番が狂ったり、パケットがドロップされたりする場合があります。

障害が発生したデバイスとそのネイバーとの間で形成されたマイクロループはローカル ユーループと呼ばれます。また複数ホップ離れたデバイスとの間で形成されるマイクロループはリモート ユーループと呼ばれます。ローカル ユーループは、通常はローカルのループフリー代替（LFA）パスが使用できないネットワークで見られます。このようなネットワークでは、リモート LFA によってネットワークのバックアップパスが提供されます。

上で説明した情報は、次の図に示すようにトポロジ例を参考にして示すことができます。

Figure 20: マイクロループのトポロジの例



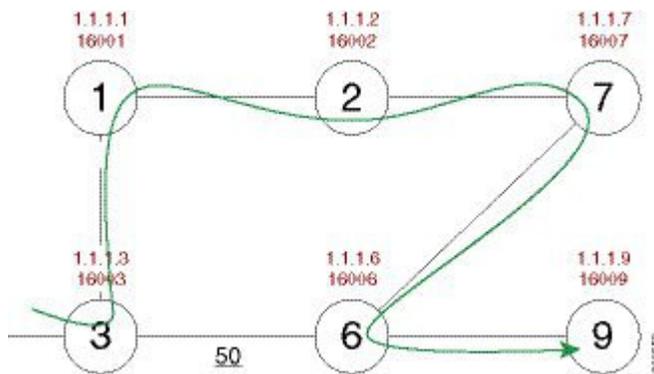
この例の前提条件は次のとおりです。

- デフォルトのメトリックは、メトリックが 50 であるノード 3 とノード 6 間のリンクを除き、各リンクごとに 10 です。各ノードでの SPF バックオフ遅延の収束順序は次のとおりです。
 - ノード 3 : 50 ミリ秒
 - ノード 1 : 500 ミリ秒
 - ノード 2 : 1 秒
 - ノード 7 : 1.5 秒

ノード 3 からノード 9 (宛先) に送信されたパケットは、ノード 6 経由で通過します。

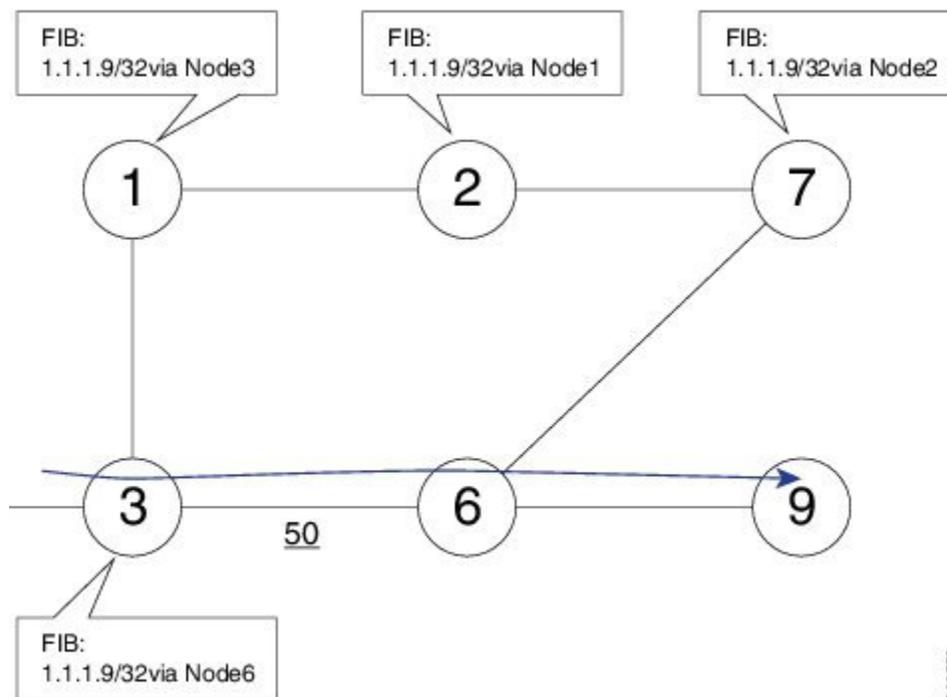
ノード 6 とノード 7 の間でリンクが確立されている場合、パケットが宛先であるノード 9 に到達する前のノード 3 からノード 9 へのパケットの最短パスは、ノード 1、ノード 2、ノード 7、およびノード 6 になります。

Figure 21: マイクロループのトポロジの例 : 最短パス



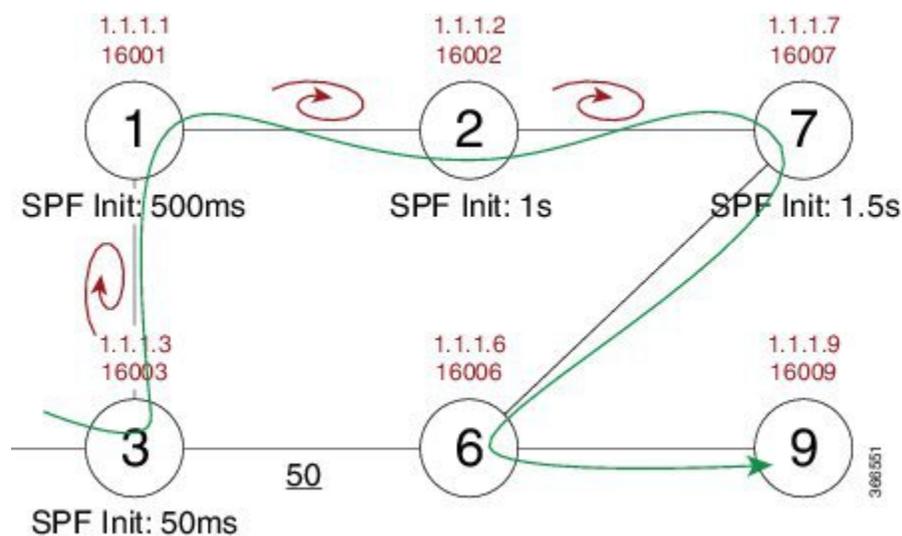
次の図は、ノード 6 とノード 7 間のリンクが確立される前の各ノードの転送情報ベース (FIB) テーブルを示しています。FIB エントリには、宛先ノード (ノード 9) のプレフィックスとネクスト ホップが含まれます。

Figure 22: マイクロループのトポロジの例 : FIB エントリ



ノード6とノード7間のリンクがアップすると、各ノードのコンバージェンスの順序に基づいて、マイクロループがリンクに対して発生します。この例では、ノード3は最初にノード1で収束し、その結果ノード3とノード1の間にマイクロループが発生します。その後、ノード1が次に収束し、その結果ノード1とノード2の間にマイクロループが発生します。次に、ノード2が次に収束し、その結果ノード2とノード7の間にマイクロループが発生します。最後に、次の図に示すように、ノード7はマイクロループの解決を収束し、パケットが宛先ノード9に到達します。

Figure 23: マイクロループのトポロジの例 : マイクロループ



SPF コンバージェンス遅延を追加すると、マイクロループは 1.5 秒間（ノード 7 に指定されたコンバージェンス期間）接続を失うことになります。

セグメントルーティングとマイクロループ

ISIS - SR : uLoop 回避機能は次のシナリオをサポートします。

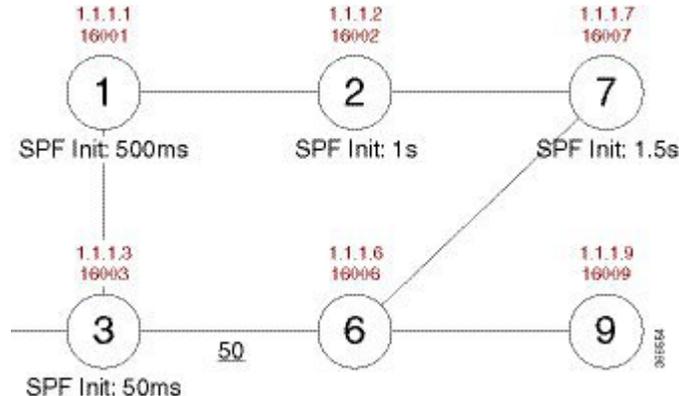
- ポイントツーポイント リンクのリンクアップまたはリンクダウンと 2 つのノードを持つ LAN セグメント
- オーバーロードビットが設定または設定解除されているためにノードがアップまたはダウンした場合のリンク コストの減少または増加

マイクロループを防ぐために、ノードで **microloop avoidance segment-routing** コマンドを有効にする必要があります。

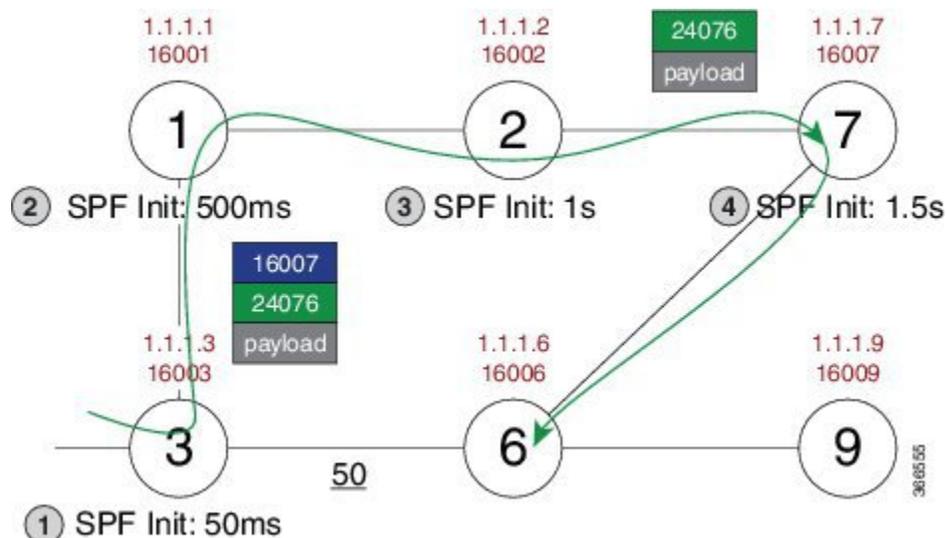
セグメントルーティングがマイクロループを防ぐ仕組み

このセクションでは、マイクロループの説明に使用した例を使用して、セグメントルーティングがマイクロループを防ぐ方法について説明します。この例のノード 3 は、**microloop avoidance segment-routing** コマンドで有効になっています。ノード 6 とノード 7 間のリンクがアップした後、ノード 3 はネットワーク上の新しいマイクロループを計算します。

Figure 24: マイクロループのトポロジの例 : セグメントルーティング



FIB テーブルを更新する代わりに、ノード 3 は、ノード 7 のプレフィックス セグメント ID (SID) である 16007 を含むセグメント ID のリストと、ノード 6 の隣接関係セグメント ID (SID) である 24076 を使用して、宛先（ノード 9）のダイナミックループフリー代替 (LFA) SR TE ポリシーを構築します。



したがって、SR TE ポリシーにより、ノード3からのパケットが宛先ノード9に到達することが可能になり、ネットワークが収束するまでマイクロループのリスクがなくなります。最後に、ノード3は新しいパスのFIBを更新します。

microloop avoidance segment-routing コマンドで **protected** キーワードを使用すると、保護するプレフィックスに対してのみマイクロループ回避が有効化されます。**microloop avoidance rib-update-delay milliseconds** コマンドを使用して、ノードのフォワーディングテーブルを更新する前にノードが待機する遅延時間をミリ秒単位で設定し、マイクロループ回避ポリシーの使用を停止することができます。RIB 遅延のデフォルト値は 5000 ミリ秒です。

ISIS - SR を有効にする方法 : uLoop 回避

マイクロループ回避の有効化

マイクロループ回避を有効にするための構成コード スニペットの例を次に示します。

```
router isis
  fast-reroute per-prefix level-2 all
  microloop avoidance segment-routing
  microloop avoidance rib-update-delay 3000
```

マイクロループ回避の確認

修復パスが存在するかどうかを確認するには、**show isis rib** および **show ip route** コマンドを使用します。

```
Router# show isis rib 10.20.20.0 255.255.255.0

IPv4 local RIB for IS-IS process sr

IPv4 unicast topology base (TID 0, TOPOID 0x0) =====
Repair path attributes:
```

```

DS - Downstream, LC - Linecard-Disjoint, NP - Node-Protecting
PP - Primary-Path, SR - SRLG-Disjoint

10.20.20.0/24 prefix attr X:0 R:0 N:0 prefix SID index 2 - Bound (ULOOP EP)
 [115/L2/130] via 10.77.77.77(MPLS-SR-Tunnel5), from 10.44.44.44, tag 0,
 LSP[2/5/29]
 prefix attr: X:0 R:0 N:0
 SRGB: 16000, range: 8000 prefix-SID index: None
 (ULOOP_EP) (installed)
 - - - - -
 [115/L2/130] via 10.16.16.6(Ethernet2/0), from 10.44.44.44, tag 0, LSP[2/5/29]
 prefix attr: X:0 R:0 N:0
 SRGB: 16000, range: 8000 prefix-SID index: None
 (ALT)

Router# show ip route 10.20.20.0

Routing entry for 10.20.20.0/24
Known via "isis", distance 115, metric 130, type level-2
Redistributing via isis sr
Last update from 10.77.77.77 on MPLS-SR-Tunnel5, 00:00:43 ago
SR Incoming Label: 16002 via SRMS
Routing Descriptor Blocks:
* 10.77.77.77, from 10.44.44.44, 00:00:43 ago, via MPLS-SR-Tunnel5,
* prefer-non-rib-labels, merge-labels
Route metric is 130, traffic share count is 1
MPLS label: 16002
MPLS Flags: NSF
    
```

ISIS - SR の追加情報 : uLoop 回避

関連資料

関連項目	マニュアルタイトル
「Segment Routing and IS-IS」	『Using Segment Routing with IS-IS』
IS-IS の概念の概要	『“IS-IS Overview and Basic Configuration” module in the IP Routing: ISIS Configuration Guide』
ISIS でのローカル マイクロループからの保護	『“ISIS Local Microloop Protection” module in the IP Routing: ISIS Configuration Guide』

標準/RFC

標準/RFC	タイトル
draft-francois-rtgwg-segment-routing-uloop-00	Loop avoidance using Segment Routing

ISIS - SR の機能情報 : uLoop 回避

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、<https://cfng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

Table 19: ISIS - SR の機能情報 : uLoop 回避

機能名	リリース	機能情報
ISIS - SR : uLoop 回避	Cisco IOS XE Amsterdam 17.3.2	ISIS - SR : uLoop 回避機能により、ISIS ローカル マイクロループ保護機能が拡張され、リンクダウン イベントまたはリンクアップ イベント後のネットワーク コンバージェンス時にマイクロループが発生するのを防ぐことができます。 次のコマンドが導入または変更されました。 microloop avoidance 、 microloop avoidance rib-update-delay 、 show mpls traffic tunnel 。



CHAPTER 21

BGP-SR : BGP プレフィックス SID の再配布

BGP - SR : BGP プレフィックス SID 再配布機能は、セグメントルーティング — BGP ネットワークにおいて IPv4 プレフィックスで BGP プレフィックス SID をサポートします。

- [BGP - SR の前提条件 : BGP プレフィックス SID の再配布, on page 215](#)
- [BGP - SR に関する情報 : BGP プレフィックス SID の再配布, on page 215](#)
- [BGP - SR を有効にする方法 : BGP プレフィックス SID の再配布, on page 217](#)
- [BGP - SR の追加情報 : BGP プレフィックス SID の再配布, on page 218](#)
- [BGP - SR の機能情報 : BGP プレフィックス SID の再配布, on page 218](#)

BGP - SR の前提条件 : BGP プレフィックス SID の再配布

- マルチプロトコル ラベル スイッチング (MPLS) が設定されている必要があります。

BGP - SR に関する情報 : BGP プレフィックス SID の再配布

セグメントルーティングと BGP

セグメントルーティングでは、マルチプロトコル ラベル スイッチング (MPLS) ラベルを使用して、ネットワーク内のパケットをガイドするパスを作成します。セグメントルーティングを使用すると、MPLS ラベル範囲は MPLS 転送インフラストラクチャ (MFI) で予約されます。このラベル範囲は、セグメントルーティング グローバルブロック (SRGB) と呼ばれます。プレフィックスに割り当てられたプレフィックス SID は、SRGB の拡張機能です。

セグメントルーティングをサポートするためには、Border Gateway Protocol (BGP) が BGP プレフィックスのセグメント ID (SID) をアドバタイズできなければなりません。BGP プレフィックス SID は、BGP ネットワークを使用したセグメントルーティングにおける BGP プレフィッ

クスセグメントのセグメント識別子です。また BGP プレフィックス SID は、BGP によって計算された ECMP 対応のベストパス上のパケットを関連するプレフィックスに転送する命令でもあります。BGP ノードがネットワーク内のネイバーノードと通信するとき、BGP アップデート（ネイバーノードに送信されるメッセージ）には、ラベル付きユニキャスト NLRI のプレフィックス SID ラベルと、プレフィックス SID 属性と呼ばれる新しい属性のプレフィックス SID インデックスが含まれます。

トラフィックエンジニアリングの転送パスをサポートするには、転送パスが最適パスと異なっていることが必要な場合があります。したがって、各 BGP ノードはネイバーにローカルラベルを割り当て、BGP -- リンク ステート アップデートによってローカルラベルを隣接関係 SID としてアドバタイズします。

BGP - SR : BGP プレフィックス SID 再配布機能は、セグメントルーティング MPLS コンフィギュレーションモードで **connected-prefix-sid-map** コマンドを使用して有効にすることができます。さらに、各アドレスファミリに対してルータ コンフィギュレーションモードでも **segment-routing mpls** コマンドを有効にする必要があります。



Note Cisco IOS XE Everest 16.6.1 では、IPv4 プレフィックスのみサポートされています。

ローカル ソース ルートのセグメントルーティング

ローカルノードで設定されたインターフェイスホストルートは、ローカルソースルートとして知られています。セグメントルーティングが有効になっている場合、BGP ノードは、プレフィックス SID ラベルおよびプレフィックス SID 属性として明示的または暗黙的 null を含み、プレフィックスをネイバーノードにアドバタイズします。

ネイバーに明示的 null が設定されていない場合、MPLS 暗黙的 Null ラベル (3) がネイバーノードにアドバタイズされます。ネイバーに明示的 null が設定されている場合、プレフィックスのアドレスファミリに対応する MPLS 明示的 Null ラベルがネイバーノードにアドバタイズされます (IPv4 の場合は 0)。

受信したプレフィックスのセグメントルーティング

通信を介してネイバーノードからプレフィックス SID 属性を受信する BGP ノードは、ルートが RIB に追加されたときに、プレフィックスとして発信ラベルにラベルを追加します。ローカルラベルおよびプレフィックス SID インデックスは RIB に含まれます。

再配布ルートのセグメントルーティング

BGP ノード上のソースプロトコルは、受信したプレフィックス SID インデックスおよびローカルノードで使用可能な SRGB に応じて、ローカルラベルを割り当てます。ソースプロトコルは、プレフィックス SID インデックスと派生したローカルラベルを RIB に提供します。BGP は、ネイバーノードに送信されるラベル付きユニキャスト更新のラベルとして RIB からのローカルラベルを使用します。

BGP--MFI インタラクション

BGP はクライアントとして MFI に登録し、プレフィックスのローカル ラベル（これを使用してトラフィックが到着することが予期される）として SID インデックスおよび SRGB から派生したラベルをバインドします。

BGP - SR を有効にする方法 : BGP プレフィックス SID の再配布

BGP-Prefix-SID の有効化

```
segment-routing mpls
  connected-prefix-sid-map */-----> Configures Prefix to SIDIndex Map that can be
  queried by BGP/IGP /*
  address-family ipv4
  10.0.0.1/255.0.0.0 index 10 range 10.11.0.1
```

セグメント ルーティング用の BGP の有効化

```
router bgp 2
  address-family-ipv4
  segment-routing mpls
```

BGP - SR の確認 : BGP プレフィックス SID の再配布

このセクションでは、ネットワーク例の助けを借りて、BGP - SR : BGP プレフィックス SID 再配布機能を確認する方法を示します。セグメントルーティングを使用して設定されているデバイスは、ボーダー ゲートウェイ プロトコル (BGP) を使用して設定されている 2 つのデバイスに接続されます。各デバイスで、**show segment-routing mpls** コマンドを使用して設定を表示します。

次に、セグメント ルーティングを使用して設定されているデバイスの構成を示します。

```
segment-routing mpls
global-block 10000 13000
!
connected-prefix-sid-map
  address-family ipv4
  10.12.1.1/32 index 3 range 1
  exit-address-family
!
segment-routing mpls

interface Loopback0
ip address 10.12.1.1 255.255.255.255

router bgp 1
neighbor 10.1.1.2 remote-as 2
!
```

```

address-family ipv4
  redistribute connected
  segment-routing mpls
  neighbor 10.1.1.2 activate
  neighbor 10.1.1.2 send-label
exit-address-family

```

次に、BGP を使用して設定されている最初のデバイスの設定を示します。

```

segment-routing mpls

router bgp 2
neighbor 10.1.1.1 remote-as 1
neighbor 10.11.1.2 remote-as 3
!
address-family ipv4
  redistribute connected
  neighbor 10.1.1.1 activate
  neighbor 10.1.1.1 send-label
  neighbor 10.11.1.2 activate
  neighbor 10.11.1.2 send-label
exit-address-family

```

次に、BGP を使用して設定されている 2 台目のデバイスの設定を示します。

```

segment-routing mpls

router bgp 3
neighbor 10.11.1.1 remote-as 2
!
address-family ipv4
  redistribute connected
  neighbor 10.11.1.1 activate
  neighbor 10.11.1.1 send-label
exit-address-family

```

BGP - SR の追加情報 : BGP プレフィックス SID の再配布

関連資料

標準および RFC

標準/RFC	タイトル
RFC3107	『 <i>Carrying Label Information in BGP-4</i> 』

BGP - SR の機能情報 : BGP プレフィックス SID の再配布

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 トレー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、特に断りが無い限り、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、<https://cfng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

Table 20: BGP - SR の機能情報 : BGP プレフィックス SID の再配布

機能名	リリース	機能情報
BGP-SR : BGP プレフィックス SID の再配布	Cisco IOS XE Amsterdam 17.3.2	BGP-SR : BGP プレフィックス SID 再配布機能は、セグメントルーティング — BGP ネットワークにおいて IPv4 プレフィックスで BGP プレフィックス SID をサポートします。 次のコマンドが導入または変更されました。 connected-prefix-sid-map 、 segment-routing 。



第 22 章

IS-IS および OSPF によって最大 SID 深度を BGP-LS にアドバタイズする

セグメントルーティング (SR) が有効になっているネットワークでは、SR トンネルをプログラムする集中型コントローラが、適切な深度の SID スタックをプッシュするために、ノードのヘッドエンドでサポートされる最大セグメント識別子 (SID) の深度 (MSD) および/またはリンクの細分性を認識する必要があります。MSD は、SR トンネルまたはバインディング SID アンカーノードのヘッドエンドに関連していて、バインディング SID の拡張によって新しい SID スタックが作成される可能性があります。

- [IS-IS および OSPF による最大 SID 深度の BGP-LS へのアドバタイズに関する制約事項 \(221 ページ\)](#)
- [IS-IS および OSPF による最大 SID 深度の BGP-LS へのアドバタイズに関する情報 \(222 ページ\)](#)
- [IS-IS および OSPF による最大 SID 深度の BGP-LS へのアドバタイズの確認 \(224 ページ\)](#)
- [IS-IS および OSPF による最大 SID 深度の BGP-LS へのアドバタイズに関する機能情報 \(224 ページ\)](#)

IS-IS および OSPF による最大 SID 深度の BGP-LS へのアドバタイズに関する制約事項

- IOS-XE ではラインカードがないため、リンク MSD はアドバタイズされません。

IS-IS および OSPF による最大 SID 深度の BGP-LS へのアドバタイズに関する情報



(注) この機能は、デフォルトで有効に設定されています。この機能を有効にするために固有の設定は不要です。

最大 SID 深度

次の方法により、IGP を使用して、ノードの MSD または集中型コントローラへのリンクをシグナリングすることができます。

- ノード - MSD をそのピアにアドバタイズする。
- MSD 情報を BGP-LS に提供する。

パス計算要素プロトコル (PCEP) SR 拡張は、SR PCE 能力 TLV の MSD およびメトリック オブジェクトをシグナリングします。ただし、PCEP が SR トンネルのヘッドエンドでサポート/設定されていないか、またはバインディング SID アンカー ノードとコントローラが IGP ルーティングに参加しない場合、ノードの MSD を学習する方法はありません。BGP-LS は、トポロジならびにそのトポロジ内のノードの関連する属性および機能を、集中型コントローラに公開する方法を定義します。通常、BGP-LS は、必ずしもヘッドエンドとして機能するとは限らない少数のノードで設定されます。ネットワーク内のすべての SR 対応ノードについて BGP-LS から MSD をシグナリングするために、MSD 機能をネットワーク内のすべての IGP ルータによってアドバタイズする必要があります。

判読可能なラベル深度機能 (RLDC) は、適切な深度でエントロピーラベル (EL) を挿入するためにヘッドエンドによって使用され、このためトランジットノードで読むことができます。MSD は逆に、特定の深度の SID のスタックをプッシュするために機能を通知します。

タイプ 1 の MSD (IANA レジストリ) は、ノードがパス計算要素/コントローラによって使用されるように課することができる SID の数を通知するために使用されます。これは、計算の結果として作成されたスタックの一部にのみ関係します。MSD は、サービス ラベルの数に関係なく、ノードが課することができるラベルの合計数をアドバタイズします。

ノードの最大 SID 深度のアドバタイズメント

ノード MSD TLV と呼ばれる本文内の新しいタイプ/長さ/値 (TLV) は、ルータ情報 (RI) リンク状態アドバタイズメント (LSA) を発信するルータのプロビジョニングされた SID 深度を伝送するために定義されます。ノード MSD は、ノードがサポートする最も低い MSD です。

OSPF のノードの最大 SID 深度のアドバタイズメント

```

0                               1                               2                               3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|   Type   |                               |   Length   |                               |
+-----+-----+-----+-----+-----+-----+-----+-----+
|   Sub-Type and Value ...
+-----+-----+-----+-----+-----+-----+ ...

```

この TLV のタイプ (2 バイト) は 12 です (これは IANA によって割り当てられることが推奨されている値です)。長さは可変 (最小 2、2 オクテットの倍数) であり、値フィールドの合計長を表します。値フィールドは 1 オクテットのサブタイプ (IANA レジストリ) と 1 オクテット値で構成されます。

サブタイプ 1、MSD、および値フィールドには、RILSA を発信するデバイスの最大 MSD が含まれます。ノードの最大 MSD は、0 ~ 254 の範囲内です。0 は、任意の深度の MSD をプッシュする能力がないことを表します。その他の値は、ノードのその能力を表します。この値は、ノードによってサポートされる最小値を表す必要があります。

IS-IS のノードの最大 SID 深度のアドバタイズメント

```

0                               1                               2                               3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|   Type   |   Length   |   Sub-Type and Value   |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

ノード MSD は、TLV 242 のサブ TLV です。このサブ TLV のタイプは 23 です。長さは可変です (最小値は 2、2 オクテットの倍数)。

サブタイプ 1、MSD、および値フィールドには、RILSA を発信するデバイスの最大 MSD が含まれます。ノードの最大 MSD は、0 ~ 254 の範囲内です。0 は、任意の深度の MSD をプッシュする能力がないことを表します。その他の値は、ノードのその能力を表します。この値は、ノードによってサポートされる最小値を表す必要があります。

ハードウェアからのノード MSD の取得

IS-IS および OSPF は、基盤となるハードウェアからのノードの最大 SID 深度について更新されます。IS-IS と OSPF はこれに基づいて、その TLV の値を更新します。

BGP LS への MSD のアドバタイジング

IGP は LSLIB に情報を送信して、MSD 情報を BGP-LS で使用できるようにします。これはノード MSD 情報またはリンク MSD 情報の可能性があります。また、MSD を動作させるためには、IS-IS で **distribute linkstate** を設定する必要があります。配布リンクの状態を設定するには、次の手順を実行します。

```
Device# configure terminal
```

```
Device(config)# router isis
Device(config-router)# distribute link-state
```

IS-IS および OSPF による最大 SID 深度の BGP-LS へのアドバタイズの確認

IS-IS を使用した最大 SID 深度のアドバタイズの確認

次の show コマンドはノード MSD TLV を確認するのに使用されます。

```
Device# show isis database verbose
Router CAP: 10.10.10.1, D:0, S:0
  Segment Routing: I:1 V:0, SRGB Base: 16000 Range: 8000
    Segment Routing Algorithms: SPF, Strict-SPF
  Router CAP: 10.2.2.2, D:0, S:0
  Segment Routing: I:1 V:0, SRGB Base: 16000 Range: 8000
  Segment Routing Algorithms: SPF, Strict-SPF
Node-MSD
  MSD: 16
```

OSPF を使用した最大 SID 深度のアドバタイズの確認

次の show コマンドはノード MSD TLV を確認するのに使用されます。

```
Device# show ip ospf database opaque-area type router-information
TLV Type: Segment Routing Node MSD
Length: 2
Sub-type: Node Max Sid Depth, Value: 16
```

IS-IS および OSPF による最大 SID 深度の BGP-LS へのアドバタイズに関する機能情報

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、<https://cfmng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

表 21: IS-IS および OSPF による最大 SID 深度の BGP-LS へのアダプタイズに関する機能情報

機能名	リリース	機能情報
IS-IS および OSPF によって最大 SID 深度を BGP-LS にアダプタイズする	Cisco IOS XE Amsterdam 17.3.2	<p>セグメントルーティング (SR) が有効になっているネットワークでは、SR トンネルをプログラムする集中型コントローラが、適切な深度の SID スタックをプッシュするために、ノードのヘッドエンドでサポートされる最大セグメント識別子 (SID) の深度 (MSD) および/またはリンクの細分性を認識する必要があります。MSD は、SR トンネルまたはバインディング SID アンカー ノードのヘッドエンドに関連していて、バインディング SID の拡張によって新しい SID スタックが作成される可能性があります。</p> <p>この機能により、次のコマンドが導入または変更されました。distributed link-state、show isis database verbose、show ip ospf database opaque-area type router-information</p>



第 23 章

セグメントルーティングトラフィックエンジニアリング **AutoTunnel** を使用した **RSVP-TE** の保護

このドキュメントでは、バックアップセグメントルーティングトラフィックエンジニアリング (SR-TE) 自動トンネルを使用した、ネクストホップ (NHOP) 保護とも呼ばれるリンク保護のサポートについて説明します。これは RSVP トラフィックエンジニアリング (RSVP-TE) トンネルが通過するリンクを保護します。

- [セグメントルーティングトラフィックエンジニアリング **AutoTunnel** を使用した RSVP-TE の保護に関する機能情報 \(227 ページ\)](#)
- [セグメントルーティングトラフィックエンジニアリング **AutoTunnel** を使用した RSVP-TE の保護に関する前提条件 \(228 ページ\)](#)
- [セグメントルーティングトラフィックエンジニアリング **AutoTunnel** を使用した RSVP-TE の保護に関する制約事項 \(229 ページ\)](#)
- [セグメントルーティングトラフィックエンジニアリング **AutoTunnel** を使用した RSVP-TE の保護に関する情報 \(229 ページ\)](#)
- [セグメントルーティングトラフィックエンジニアリング **AutoTunnel** を使用した RSVP-TE の保護の設定方法 \(232 ページ\)](#)
- [セグメントルーティングトラフィックエンジニアリング **AutoTunnel** を使用した RSVP-TE の保護の確認 \(234 ページ\)](#)

セグメントルーティングトラフィックエンジニアリング **AutoTunnel** を使用した **RSVP-TE** の保護に関する機能情報

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、<https://cfmng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

表 22:セグメントルーティングトラフィックエンジニアリング AutoTunnel を使用した RSVP-TE の保護に関する機能情報

機能名	リリース	機能情報
セグメントルーティングトラフィックエンジニアリング AutoTunnel を使用した RSVP-TE の保護	Cisco IOS XE Amsterdam 17.3.2	この機能は、バックアップセグメントルーティングトラフィックエンジニアリング (SR-TE) 自動トンネルを使用した、ネクストホップ (NHOP) 保護とも呼ばれるリンク保護をサポートします。これは RSVP トラフィックエンジニアリング (RSVP-TE) トンネルが通過するリンクを保護します。 この機能により、次のコマンドが導入されました。 ip explicit-path name path1 enable 、 show mpls traffic-eng tunnels tunnel 65436 、 show ip explicit-paths 、 show mpls traffic-eng tunnels tunnel 65436 show Segment-Routing Path Info 、 show mpls traffic-eng fast-reroute database 、 show ip rsvp fast-reroute sh mpls traffic-eng auto-tunnel backup 。

セグメントルーティングトラフィックエンジニアリング AutoTunnel を使用した RSVP-TE の保護に関する前提条件

SR-TEバックアップ自動トンネルを有効にする前に、セットアップで次のテクノロジーが構成されていることを確認してください。

- IS-IS ネットワーク ポイント ツー ポイント インターフェイス
- セグメントルーティング

さらに、次のテクノロジーに関する事前知識が必要です。

- MPLS トラフィックエンジニアリング
- RSVP トラフィックエンジニアリング
- Fast Reroute

セグメントルーティングトラフィックエンジニアリング AutoTunnel を使用した RSVP-TE の保護に関する制約事項

- SR-TE バックアップ自動トンネルは、帯域幅保護のために使用することはできません。
- SR-TE バックアップ自動トンネルは、RSVP-TE トンネル保護のバックアップとしてのみ使用できます。

セグメントルーティングトラフィックエンジニアリング AutoTunnel を使用した RSVP-TE の保護に関する情報

セグメントルーティングトラフィックエンジニアリング AutoTunnel を使用した RSVP-TE の保護の利点

ネットワークの複雑さが増すにつれて、複雑なシグナリングを伴う RSVP-TE トンネルのメンテナンスや、ネットワーク内のルータでの高いオーバーヘッドにより、スケーラビリティが問題になります。バックアップ自動トンネル機能は、セグメントルーティング (SR) ネットワークの複雑さを軽減するのに役立ちます。自動トンネルバックアップ機能には、次の利点があります。

- バックアップトンネルは自動的に構築されるため、ユーザーが各バックアップトンネルを事前に設定し、保護対象のインターフェイスにそのバックアップトンネルを割り当てる必要はありません。
- バックアップトンネルを設定すると、保護エリアが拡張されます。高速再ルーティング (FRR) は、TE トンネルを使用しない IP トラフィックや LDP ラベルの保護は行いません。
- バックアップ SR-TE 自動トンネルでは、RSVP-TE トンネルを通過する既存のトラフィックを中断することなく、SR ネットワークへの追加の移行手段が可能になります。

バックアップ AutoTunnel

ルータでのバックアップ自動トンネルは、必要に応じて動的バックアップトンネルを構築するのに役立ちます。これにより、静的 SR-TE トンネルの作成が防止されます。

静的 SR-TE トンネルが存在しない場合にラベルスイッチドパス (LSP) を保護するには、次の手順を実行する必要があります。

- 各バックアップ トンネルを事前に設定します。
- 保護対象のインターフェイスにバックアップ トンネルを割り当てます。

LSP は、次の状況でリソース予約プロトコル (RSVP) FRR からのバックアップ保護を要求します。

- 最初の RSVP Resv メッセージを受信した場合。
- LSP が保護属性なしで確立された後、保護属性付きの RSVP パス メッセージを受信した場合。
- レコードルート オブジェクト (RRO) の変更を検出した場合。

LSP で使用されているインターフェイスを保護するバックアップトンネルが存在しない場合、LSP は非保護のままになります。バックアップトンネルが利用できない理由には、次のようなものがあります。

- スタティック バックアップ トンネルが設定されていない。
- 静的バックアップトンネルは設定されているが、使用可能な帯域幅が不足しているか、トンネルが別のプールを保護しているか、またはトンネルが利用できないため、LSP を保護できない可能性があります。

バックアップトンネルが使用可能でない場合、次の2つのバックアップトンネルがダイナミックに作成されます。

- NHOP：リンク障害から保護
- NNHOP：ノード障害から保護

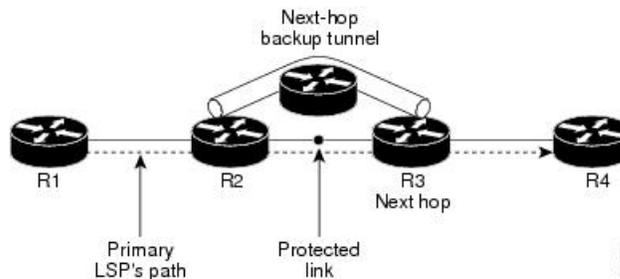


(注) 最後から2番めのホップには、NHOP バックアップ トンネルだけが作成されます。

リンク保護

LSP のパスの単一リンクだけをバイパスするバックアップトンネルが、リンク保護を提供します。パス上のリンクに障害が発生した場合、バックアップトンネルは、LSP のトラフィックをネクスト ホップにリルートする (障害の発生したリンクをバイパスする) ことによって LSP を保護します。これらは、障害ポイントの向こう側にある LSP のネクスト ホップで終端するため、NHOP バックアップ トンネルと呼ばれます。

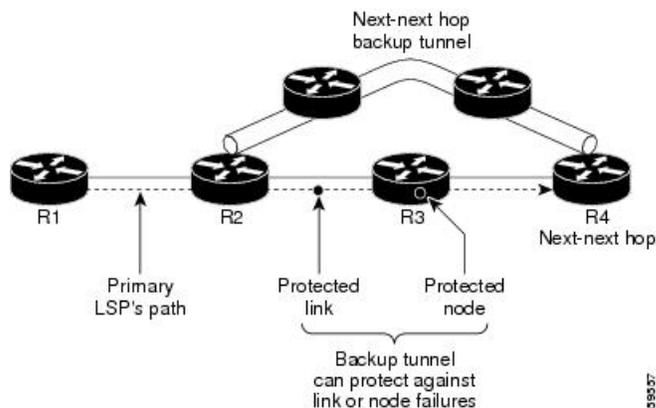
図 25: ネクストホップバックアップトンネル



ノード保護

LSP パスに沿ったネクストホップ ノードをバイパスするバックアップトンネルは、LSP のネクストホップ ノードの次のノードで終端して、結果としてネクストホップ ノードをバイパスするため、NNHOP バックアップトンネルと呼ばれます。リンク障害またはノード障害のノードアップストリームで、障害を避けて LSP とトラフィックがネクストホップ ノードにリルートされるようにすることにより、LSP が保護されます。また、NNHOP バックアップトンネルは、障害の発生したリンクおよびノードをバイパスするため、リンク障害からの保護も提供しています。

図 26: ネクストネクストホップバックアップトンネル



明示パス

明示パスを使用して、次のようにバックアップ自動トンネルが作成されます。

- NHOP では、保護されたリンクの IP アドレスが除外されます。
- NNHOP では、NHOP ルータ ID が除外されます。
- 明示パス名は、`_auto-tunnel_tunnelxxx` です。ここで、`xxx` は、動的に作成されたバックアップトンネル ID と一致します。

バックアップ自動トンネルの範囲

バックアップ自動トンネルのトンネル範囲は設定可能です。デフォルトでは、最後の100個のTEトンネルID（つまり、65,436～65,535）が使用されます。自動トンネルは、割り当てられている最も小さい番号で始まるトンネルIDを検出します。

たとえば、1000～1100の範囲内でトンネルを設定するとします。また、静的に設定されたTEトンネルも同じ範囲に入るため、ルータはこれらのIDを使用しません。これらのスタティックトンネルが削除されると、MPLS-TEダイナミックトンネルソフトウェアでこれらのIDを使用できるようになります。

セグメントルーティングトラフィックエンジニアリング AutoTunnel を使用した RSVP-TE の保護の設定方法

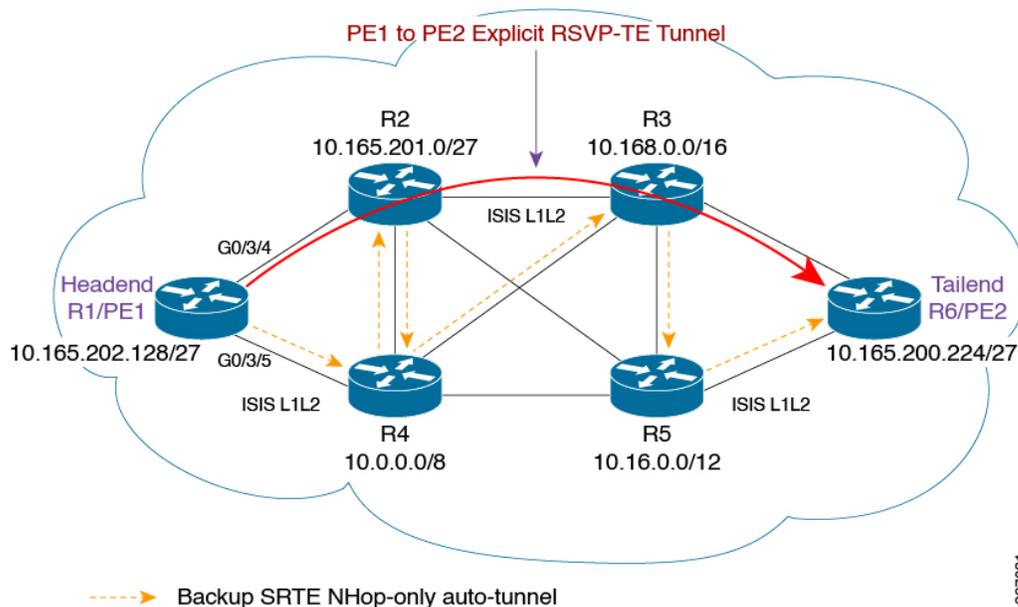
ポイントツーポイントネットワークタイプの明示パスの設定

SR-TE自動トンネルバックアップ機能を動作させるには、インターフェイスがポイントツーポイントネットワークタイプである必要があります。

```
interface Loopback0
 ip address 10.51.1.1 255.255.255.255
 ip router isis 1
end
!
interface GigabitEthernet0/2/0
 ip address 10.102.6.1 255.255.255.0
 ip router isis 1
 negotiation auto
 mpls traffic-eng tunnels
 isis network point-to-point
 ip rsvp bandwidth
end
!
interface GigabitEthernet0/2/4
 ip address 10.104.1.1 255.255.255.0
 ip router isis 1
 negotiation auto
 mpls traffic-eng tunnels
 isis network point-to-point
 ip rsvp bandwidth
end
```

FRR での明示的 RSVP-TE トンネルの設定

図 27: 明示的 RSVP-TE トンネル



1. ルータ R2 と R3 を通過する R1/PE1 から R6/PE2 への明示的パスを設定します。

```
ip explicit-path name path1 enable
index 1 next-address 10.165.202.128
index 2 next-address 10.165.201.0
index 3 next-address 10.168.0.0
index 4 next-address 10.165.200.224
```

2. 明示的 RSVP-TE トンネルを設定します。

```
interface Tunnell
ip unnumbered Loopback0
tunnel mode mpls traffic-eng
tunnel destination 10.165.200.224
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 10 explicit name path1
tunnel mpls traffic-eng record-route
end
```

3. プライマリ RSVP-TE トンネル1を FRR で設定して、保護プロセスをアクティブにします。

```
interface tunnel 1
tunnel mpls traffic-eng fast-reroute
```

4. SR-TE 自動トンネルを使用してリンク保護を有効にするには、グローバルコマンドを設定します。

```
mpls traffic-eng auto-tunnel backup segment-routing nhop-only
```

367031



(注) このコマンドは、リンク保護を必要とするすべてのノードで使用可能である必要があります。

プライマリ RSVP/TE トンネルは、ヘッドエンド R1/PE1 から宛先 R6/PE2 に初期化され、次のノード R2 などを通過するように保護する必要があります。この場合、R1/PE1 はローカル修復点 (PLR) であり、R2 は中間点 (MP) です。リンク保護によって、SR-TE バックアップ自動トンネルは、パス R1/PE1 -> R4 および R4 -> R2 を通過することによって R1/PE1 から R2 へのリンクに保護を提供するため、MP に収束します。

セグメントルーティングトラフィックエンジニアリング AutoTunnel を使用した RSVP-TE の保護の確認

show interfaces Tunnel コマンドを使用して、SR-TE 自動トンネルが生成され、アップになっているかどうかを確認します。

```
Device#show interfaces Tunnel65436
Tunnel65436 is up, line protocol is up
```

show mpls traffic-eng tunnels コマンドを使用して、バックアップ自動トンネルが SR-TE トンネルであるかどうかを確認します。

```
Device#show mpls traffic-eng tunnels tunnel 65436
Name: R1_t65436 (Tunnel65436) Destination: 10.165.201.0
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 1, (SEGMENT-ROUTING) type explicit __dynamic_tunnel65436 (Basis for
Setup, path weight 20)
```

show ip explicit-paths コマンドを使用して、SR-TE バックアップトンネルがノードに到達するためにセカンダリパスを使用しているかどうかを確認します。

```
Device#show ip explicit-paths
PATH __dynamic_tunnel65436 (strict source route, path complete, generation 49, status
non-configured)
1: exclude-address 10.102.5.1
```

show mpls traffic-eng tunnels tunnel 65436 | s Segment-Routing Path Info コマンドを使用して、バックアップトンネルがパス R1/PE1 から R4 へ、および最終的に中間点である宛先 R2 を通過しているかどうかを確認します。

```
Device#show mpls traffic-eng tunnels tunnel 65436 | s Segment-Routing Path Info
Segment-Routing Path Info (isis level-1)
Segment0[Link]: 10.104.1.1 - 10.104.1.2, Label: 19
Segment1[Link]: 10.104.6.2 - 10.104.6.1, Label: 18
```

show mpls traffic-eng auto-tunnel backup コマンドを使用して、自動トンネルバックアップの状態が正しいかどうかを確認します。

```
Device#show mpls traffic-eng auto-tunnel backup
State: Enabled
Auto backup tunnels: 1 (up: 1, down: 0)
Tunnel ID Range: 65436 - 65535
Create Nhop Only: Yes
Check for deletion of unused tunnels every: 3600 Sec
SRLG: Not configured

Config:
unnumbered-interface: Loopback0
Affinity/Mask: 0x0/0xFFFF
```

show mpls traffic-eng fast-reroute database コマンドを使用して、RSVP-TE LSP が通過するプライマリ リンクが保護されているかどうかを確認します。

```
Device#show mpls traffic-eng fast-reroute database
P2P Headend FRR information:
Protected tunnel In-label Out intf/label FRR intf/label Status
-----
Tunnell Tun hd Gi0/3/4:30 Tu65436:30 ready

Device#show ip rsvp fast-reroute
P2P Protect BW Backup
Protected LSP I/F BPS:Type Tunnel:Label State Level Type
-----
Rl_t1 Gi0/3/4 0:G Tu65436:28 Ready any-unl Nhop
```




第 24 章

ISIS 手動隣接関係 SID

統合された Intermediate System-to-Intermediate System (IS-IS) の手動隣接関係 SID 機能は、手動でプロビジョニングされた隣接関係 SID に関する情報を提供します。

- [ISIS 手動隣接関係 SID の機能情報 \(237 ページ\)](#)
- [ISIS 手動隣接関係 SID に関する情報 \(238 ページ\)](#)
- [手動隣接関係 SID の設定 \(240 ページ\)](#)
- [手動隣接関係 SID の確認 \(240 ページ\)](#)

ISIS 手動隣接関係 SID の機能情報

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、<https://cfng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

表 23: ISIS 手動隣接関係 SID の機能情報

機能名	リリース	機能情報
ISIS 手動隣接関係 SID	Cisco IOS XE Amsterdam 17.3.2	統合された Intermediate System-to-Intermediate System (IS-IS) の手動隣接関係 SID 機能は、手動でプロビジョニングされた隣接関係 SID に関する情報を提供します。 この機能により、次のコマンドが追加されました。 adjacency-sid [absolute index]<value> [protected] 。 を参照してください。

ISIS 手動隣接関係 SID に関する情報

セグメントルーティング (SR) ネットワークでは、多くの場合、ネットワーク上で特定のトラフィックが通過するパスに影響を与えるために SR トラフィックエンジニアリング (SR-TE) を使用します。SR-TE トンネルはトンネルヘッドで手動でプロビジョニングできますが、多くの場合、中央コントローラによって計算およびプロビジョニングされます。多くの場合ネットワークのオペレータは、トラフィックに特定のノードやリンクを経由させたいと考えます。

SR ネットワーク オペレータの特定のノードをトラフィックに経由させるために、ノードによってアドバタイズされるプレフィックス SID を使用できます。多くの場合、複数のノードが同じプレフィックス SID を共有する特定の場所を通過するようにトラフィックに強制するエニーキャストプレフィックス SID が使用されます。

トラフィックに特定のリンク上を通過させるためには、隣接関係 SID (Adj-SID) が使用されます。既存の Adj-SID の実装の問題は、手動でプロビジョニングされたプレフィックス SID とは対照的に、動的に割り当てられた値であるということです。Adj-SID が動的に割り当てられているということは、一連の問題をもたらします。

- この値は、リロードまたはプロセスの再起動に対して永続的ではありません。
- この値は事前にわからないので、IGP によってフラッディングされた情報 (ネイティブまたは BGP-LS) にアクセスしない限り、コントローラが使用することはできません。
- 各リンクには一意の Adj-SID 値が割り当てられているため、複数のリンクで同じ Adj-SID を共有することはできません。

上記の問題に対処するために、adj-SID が拡張され、以下が可能になりました。

- リロードと再起動に対して永続的な、手動でプロビジョニングされた adj-SID をサポートします。
- 同じネイバーへの複数の隣接関係に対してプロビジョニングされる同じ adj-SID をサポートします。
- 異なるネイバーへの複数の隣接関係にプロビジョニングされる同じ adj-SID をサポートします。
- 1 つの隣接関係に対して複数の手動 Adj-SID を設定できます。

手動隣接関係 SID

新しい永続的な Adj-SID の要件をサポートするために、動的に割り当てられた Adj-SID に使用されている既存の IS-IS Adj-SID インフラストラクチャが拡張されます。新しい CLI コマンドも導入され、ポイントツーポイントリンクのために Adj-SID 値を手動で割り当てることができます。単一のポイントツーポイントインターフェイスで複数の Adj-SID をプロビジョニングできます。同じ Adj-SID を、同じまたは異なるネイバーにつながる複数のポイントツーポイントインターフェイスでプロビジョニングできます。

すべての手動 Adj-SID は、セグメントルーティング ローカルブロック (SRLB) と呼ばれるラベルの範囲から割り当てられます。デフォルトの SRLB の範囲は 15000 ~ 15999 です。

手動の Adj-SID は、インデックスまたは絶対値として設定できます。インデックスとして設定されている場合、絶対ラベルはインデックス + SRLB 開始ラベルとして計算されます。たとえば、56 を手動 Adj-SID のインデックスとして設定した場合、絶対ラベルは $15000 + 56 = 15056$ になります。絶対値として設定されている場合、ラベル自体が絶対値になります。たとえば、56 を絶対手動 Adj-SID として設定した場合、絶対ラベルは 56 のみになります。ラベル (インデックスと絶対の両方) は、保護または非保護として設定できます。デフォルトでは、すべてのラベルは非保護です。

隣接関係 SID のアドバタイズメント

手動で設定された adj-SID は、ISIS SR 拡張機能の草案で定義される既存の ISIS adj-SID サブ TLV を使用してアドバタイズされます。S フラグは、同じ Adj-SID 値が複数のインターフェイスにプロビジョニングされている場合に adj-SID サブ TLV に設定されます。手動で設定された SID の場合、P フラグは常に設定されます。

プロビジョニングされた adj-SID がプロテクトとして設定済みの場合は、B フラグも設定されます。

隣接関係 SID は常にラベル値としてアドバタイズされます。adj-SID の設定にインデックスが使用されている場合でも、インデックスとしてはアドバタイズされません。

隣接関係 SID のフォワーディング

adj-SID の値が 1 つのインターフェイスでのみ設定される場合、ISIS は手動で割り当てられた adj-SID のフォワーディング エントリをインストールします。任意の Adj-SID のプライマリパスは、Adj-SID が割り当てられているポイントツーポイント インターフェイス上の POP 操作です。割り当てられた adj-SID がバックアップの対象となり、バックアップパスが利用可能であれば、IS-IS はバックアップパスもプログラムします。Adj-SID のバックアップパスは、ネイバールータ ID アドレスに対して計算されたバックアップパスと同じです。

複数のリンクで同じ adj-SID 値が設定されている場合、次のような転送が発生します。

- この値を使用して adj-SID が設定されている各リンクを経由して、POP 操作を含むプライマリパスがインストールされます。
- 各プライマリパスについて、Adj-SID がプライマリインターフェイスで保護されるように設定されていて、バックアップが利用可能な場合、バックアップパスがインストールされます。バックアップパスは、ネイバールータ ID アドレスに関連付けられたバックアップパスとして表されます。

設定要件

- セグメントルーティングがグローバルに設定されていることを確認します。

- セグメントルーティングが IS-IS を使用して設定されていることを確認します。

手動隣接関係 SID の設定

```
Device#configure terminal
Device(config)#interface ethernet0/1
Device(config-if)#isis adjacency-sid [absolute | index] <value> [protected]
```

[index] : (オプション) 隣接関係 SID が SRLB 範囲のインデックスとして設定されている場合に使用されます。index キーワードが使用されていない場合、値はラベルの絶対値を表すことが期待されます。

[absolute] : (オプション) 隣接関係 SID が絶対値として設定されている場合に使用されます。

<value> : adj-SID ラベルの値またはインデックスを表します。プログラムおよびアドバタイズされる adj-SID では、値/インデックスは有効な SRLB の範囲である必要があります。

[protected] : (オプション) 手動の adj-SID を保護するために使用されます。デフォルトでは、手動 Adj-SID は保護されていません。

セグメントルーティング ローカル ブロック (SRLB) 範囲の変更

```
Device#configure terminal
Device(config)#segment-routing mpls
Device(config-srmpls)#local-block 7000 7999
```

手動隣接関係 SID の確認

SR アプリ データベースでのラベルの確認

```
Device#show segment-routing mpls lb assigned-sids
Adjacency SID Database
C=> In conflict
S=> Shared
R=> In range
SID STATE      PROTOCOL      TOPOID      LAN      PRO NEIGHBOR  INTERFACE
15378 R                ISIS          0           N         N   10.0.0.3      Ethernet0/1
```

MPLS 転送でのラベルの確認

```
Device# show mpls forwarding-table
Local      Outgoing      Prefix
Next Hop
Label      Label          or Tunnel Id  Switched      interface
15378      Pop Label      0.0.60.18-A  0              Et0/0
10.0.0.2  ☐== Configured only for interface e0/0
```

共有ラベルの確認

```
Device# show mpls forwarding-table
Local      Outgoing      Prefix          Bytes Label    Outgoing
Next Hop
Label      Label         or Tunnel Id   Switched       interface
15378     Pop Label     0.0.60.18-A   0              Et0/0
10.0.0.2  == Same Label is configured for 2 interfaces
          Pop Label     0.0.60.18-A   0              Et0/1
10.0.0.3  ==
```

ISIS LSP の確認

```
Device# sh isis database verbose R1.00-00
xxxxxx
xxxxxx
Adjacency SID Value:15378 F:0 B:0 V:1 L:1 S:1 P:1 Weight:0 == P (Persistent)
flag is always 1 if it is Manual Adj-SID
xxxxxx

P -> Persistent Flag (0 for Dynamic Adj-SID and 1 for Manual Adj-SID)
S -> Shared Flag (1 if label is shared by multiple adjacencies)
```




第 25 章

OSPF 手動隣接関係（アジャセンシー）SID

OSPF 手動隣接関係（アジャセンシー）SID 機能は、OSPFv2 によるセグメントルーティングの静的隣接関係 SID の設定をサポートしています。

- [OSPF 手動隣接関係（アジャセンシー）SID に関する機能情報（243 ページ）](#)
- [OSPF 手動隣接関係（アジャセンシー）SID に関する情報（244 ページ）](#)
- [OSPF 手動隣接関係（アジャセンシー）SID の設定方法（246 ページ）](#)

OSPF 手動隣接関係（アジャセンシー）SID に関する機能情報

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、<https://cfng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

表 24: OSPF 手動隣接関係（アジャセンシー）SID に関する機能情報

機能名	リリース	機能情報
OSPF 手動隣接関係（アジャセンシー）SID	Cisco IOS XE Amsterdam 17.3.2	OSPF 手動隣接関係（アジャセンシー）SID 機能は、OSPFv2 によるセグメントルーティングの静的隣接関係 SID の設定をサポートしています。 この機能により、次のコマンドが導入されました。 <code>adjacency-sid index 値 [protected]</code>

OSPF 手動隣接関係（アジャセンシー）SID に関する情報

セグメントルーティング（SR）ネットワークでは、多くの場合、ネットワーク上で特定のトラフィックが通過するパスに影響を与えるために SR トラフィック エンジニアリング（SR-TE）を使用します。SR-TE トンネルはトンネルヘッドエンドで手動でプロビジョニングできます。そうしない場合は、中央コントローラによって計算およびプロビジョニングされます。

トラフィック エンジニアリングの場合、ネットワークのオペレータは、トラフィックが特定のノードやリンクを経由するよう強制できる必要があります。トラフィックに SR ネットワーク上の特定のノードを経由させるために、オペレータはノードによってアドバタイズされるプレフィックス SID を使用できます。ユニキャストプレフィックス SID は、複数のノードが同じプレフィックス SID をアドバタイズする場合に、トラフィックを特定のノードにルーティングするために使用できます。

トラフィックに特定のリンクを経由させるために、オペレータはリンクの隣接関係（アジャセンシー）SID を使用できます。手動で設定する隣接関係 SID がサポートされていない場合、隣接関係 SID は動的に割り当てられます。動的に割り当てられた SID には、トラフィック エンジニアリングに関して次のような欠点があります。

- 動的な値は、リロードやプロセスの再起動を行うと維持されない。
- 動的な値は事前にわからないため、コントローラは（ネイティブにまたは BGP-LS を介して）IGP がフラッディングした情報にアクセスできない場合、これを使用できない。
- 各リンクには、一意の隣接 SID 値が割り当てられる。そのような割り当てでは、同じ隣接関係（アジャセンシー）SID を複数のリンクに割り当てることができない。

OSPF 手動隣接関係 SID 機能は、手動で設定する隣接関係 SID のサポートを導入します。手動で設定された静的隣接関係 SID では、

- プロビジョニングされた隣接関係 SID が、リロードや再起動を行っても維持されます。
- 1 つの隣接関係に対して複数の隣接関係 SID を設定できます。

OSPF 手動隣接関係（アジャセンシー）SID の前提条件

- セグメントルーティングはグローバルに設定する必要があります。
- セグメントルーティングは、OSPF インスタンスに対して設定する必要があります。

OSPF 手動隣接関係（アジャセンシー）SID に関する制約事項

- 静的隣接関係（アジャセンシー）SID は、ポイントツーポイントのリンクにのみ設定でき、ブロードキャストリンクには設定できません。
- 複数のリンクに同じ隣接関係 SID を割り当てないでください。グループ隣接関係 SID はサポートされていません。

- 複数の IGP または IGP インスタンスで同じ静的隣接関係 SID を設定しないでください。そのような設定はサポートされておらず、シナリオの競合処理メカニズムはまだ導入されていません。
- 静的隣接関係 SID をセグメントルーティング ローカルブロック (SRLB) のインデックスとして指定します。静的隣接関係 SID は、SRLB のラベルの絶対値として指定できません。

手動隣接関係 (アジャセンシー) SID

静的隣接関係 (アジャセンシー) SID は、OSPFv2 でポイントツーポイントのリンクに設定できます。

手動隣接関係 SID は、SRLB から割り当てる必要があります。デフォルトの SRLB ラベルの範囲は 15000 ~ 15999 です。 `local-block range-start range-end` コマンドを使用して SRLB 範囲を変更できます。

静的隣接関係 SID をインデックスとして SRLB に割り当てることができます。割り当てられたインデックスに基づいて、隣接関係 SID のラベルは、ラベル = `SRLB_range_start + index_value` として計算されます。

デフォルトでは、静的隣接関係 SID は保護されないため、設定時に静的隣接関係 SID を保護する必要があるかどうかを指定できます。

手動隣接関係 (アジャセンシー) SID のアドバタイズメント

静的隣接関係 (アジャセンシー) SID は、「セグメントルーティングの OSPF 拡張機能」で定義されているように、拡張リンク LSA の既存の Adj-SID Sub-TLV を使用してアドバタイズされます。

静的隣接関係 SID では、P フラグ (永続フラグ) が Adj-SID Sub-TLV に設定されます。

静的隣接関係 SID が保護されている場合、B フラグは Adj-SID Sub-TLV に設定されます。

静的隣接関係 SID は常にラベルとしてアドバタイズされます。静的隣接関係 SID がインデックスとして設定されている場合、ラベルの絶対値が計算され、ラベル値がアドバタイズされます。

手動隣接関係 (アジャセンシー) SID の転送

静的隣接関係 (アジャセンシー) SID がポイントツーポイント インターフェイスに設定されている場合、OSPFv2 は手動で割り当てられた隣接関係 SID の転送エントリをインストールします。隣接関係 SID のプライマリパスは、隣接関係 SID が割り当てられているポイントツーポイント インターフェイス上の POP 操作です。

手動で割り当てられた隣接関係 SID がバックアップの対象で、バックアップパスが利用できる場合、OSPFv2 はバックアップパスもプログラムします。手動で割り当てられた隣接関係 SID のバックアップパスは、ネイバールータに対して計算されるバックアップパスです。

OSPF 手動隣接関係（アジャセンシー）SID の設定方法

セグメントルーティング ローカル ブロック 範囲の変更

```
Device#configure terminal
Device(config)#segment-routing mpls
Device(config-srmppls)#local-block range-start range-end
```

range-start と *range-end* は、セグメントルーティング ローカルブロック（SRLB）の変更された範囲境界を示します。

OSPF は、ルータ情報（RI）Opaque LSA の SR ローカルブロック TLV で SRLB をアドバタイズします。

SRLB では 1 つの範囲のみがサポートされます。SR ローカルブロック TLV に複数の範囲がある場合、受信側ルータは TLV を無視します。

```
Device#configure terminal
Device(config)#segment-routing mpls
Device(config-srmppls)#local-block 7000 7999
```

OSPF 手動隣接関係（アジャセンシー）SID の設定

```
Device#configure terminal
Device(config)#interface <interface>
Device(config-if)#ip ospf adjacency-sid index <sid_value> [protected]
```

<sid_value> は SRLB に対するインデックスである必要があります。絶対ラベル値としての隣接関係（アジャセンシー）SID の設定はまだサポートされていません。

[protected]（オプション）：このキーワードは、手動隣接関係 SID を保護するために使用されます。デフォルトでは、手動隣接関係 SID は保護されません。

OSPF 手動隣接関係（アジャセンシー）SID の確認

コマンド **show ip ospf segment-routing adjacency-sid** および **show ip ospf segment-routing adjacency-sid detail** を使用して、隣接関係（アジャセンシー）に割り当てられた SID と、SID が静的か動的かを確認できます。いずれかのコマンドの出力には、隣接関係（アジャセンシー）を介してリンクされているネイバー、隣接関係が保護されているかどうか、保護されている隣接関係のバックアップネクストホップとインターフェイスなどの追加情報も表示されます。

```
• router#show ip ospf segment-routing adjacency-sid

                OSPF Router with ID (10.2.0.0) (Process ID 1)
                Flags: S - Static, D - Dynamic, P - Protected, U - Unprotected, G - Group, L -
                Adjacency Lost

Adj-Sid Neighbor ID      Interface      Neighbor Addr  Flags  Backup NextHop
Backup Interface
-----
-----
```

16	10.3.0.0	Et0/2.3	10.3.3.3	D U	
17	10.3.0.0	Et0/2.1	10.3.1.3	D U	
24	10.3.0.0	Et0/2.1	10.3.1.3	D P	10.3.2.3
	Et0/2.2				
25	10.1.0.0	Et0/0	10.2.0.1	D U	
26	10.1.0.0	Et0/0	10.2.0.1	D P	10.3.1.3
	Et0/2.1				
27	10.3.0.0	Et0/2.2	10.3.2.3	D U	
28	10.3.0.0	Et0/2	10.3.0.3	D U	
29	10.3.0.0	Et0/2	10.3.0.3	D P	10.4.0.4
	Et0/1				
30	10.4.0.0	Et0/1	10.4.0.4	D U	
34	10.4.0.0	Et0/1	10.4.0.4	D P	10.3.1.3
	Et0/2.1				
15010	10.1.0.0	Et0/0	10.2.0.1	S P	10.3.1.3
	Et0/2.1				
15210	10.1.0.0	Et0/0	10.2.0.1	S U	
15230	10.3.0.0	Et0/2	10.3.0.3	S P	10.4.0.4
	Et0/1				
15240	10.4.0.0	Et0/1	10.4.0.4	S U	
15800	10.3.0.0	Et0/2.1	10.3.1.3	S U	
15801	10.3.0.0	Et0/2.2	10.3.2.3	S U	
15802	10.3.0.0	Et0/2.3	10.3.3.3	S U	
15810	10.3.0.0	Et0/2.1	10.3.1.3	S P	10.3.2.3
	Et0/2.2				

• router#show ip ospf segment-routing adjacency-sid detail

```

      OSPF Router with ID (10.2.0.0) (Process ID 1)
Label 16, Paths 1, Dynamic
  Nbr id 10.3.0.0, via 10.3.3.3 on Et0/2.3, Unprotected
Label 17, Paths 1, Dynamic
  Nbr id 10.3.0.0, via 10.3.1.3 on Et0/2.1, Unprotected
Label 24, Paths 1, Dynamic
  Nbr id 10.3.0.0, via 10.3.1.3 on Et0/2.1, Protected, Nbr Prefix 10.33.33.33
  Primary path: via 10.3.1.3 on Et0/2.1, out-label 3
  Repair path: via 10.3.2.3 on Et0/2.2, out-label 3, cost 31, labels 0
Label 25, Paths 1, Dynamic
  Nbr id 10.1.0.0, via 10.2.0.1 on Et0/0, Unprotected
Label 26, Paths 1, Dynamic
  Nbr id 10.1.0.0, via 10.2.0.1 on Et0/0, Protected, Nbr Prefix 10.1.1.1
  Primary path: via 10.2.0.1 on Et0/0, out-label 3
  Repair path: via 10.3.1.3 on Et0/2.1, out-label 16001, cost 31, labels 0
Label 27, Paths 1, Dynamic
  Nbr id 10.3.0.0, via 10.3.2.3 on Et0/2.2, Unprotected
Label 28, Paths 1, Dynamic
  Nbr id 10.3.0.0, via 10.3.0.3 on Et0/2, Unprotected
Label 29, Paths 1, Dynamic
  Nbr id 10.3.0.0, via 10.3.0.3 on Et0/2, Protected, Nbr Prefix 10.3.3.3
  Primary path: via 10.3.0.3 on Et0/2, out-label 3
  Repair path: via 10.4.0.4 on Et0/1, out-label 16003, cost 21, labels 0
Label 30, Paths 1, Dynamic
  Nbr id 10.4.0.0, via 10.4.0.4 on Et0/1, Unprotected
Label 34, Paths 1, Dynamic
  Nbr id 10.4.0.0, via 10.4.0.4 on Et0/1, Protected, Nbr Prefix 10.4.4.4
  Primary path: via 10.4.0.4 on Et0/1, out-label 3
  Repair path: via 10.3.1.3 on Et0/2.1, out-label 16004, cost 31, labels 0
Label 15010, Paths 1, Static
  Nbr id 10.1.0.0, via 10.2.0.1 on Et0/0, Protected, Nbr Prefix 10.1.1.1
  Primary path: via 10.2.0.1 on Et0/0, out-label 3
  Repair path: via 10.3.1.3 on Et0/2.1, out-label 16001, cost 31, labels 0
Label 15210, Paths 1, Static
  Nbr id 10.1.0.0, via 10.2.0.1 on Et0/0, Unprotected
Label 15230, Paths 1, Static
  Nbr id 10.3.0.0, via 10.3.0.3 on Et0/2, Protected, Nbr Prefix 10.3.3.3

```

```
Primary path: via 10.3.0.3 on Et0/2, out-label 3
Repair path: via 10.4.0.4 on Et0/1, out-label 16003, cost 21, labels 0
Label 15240, Paths 1, Static
  Nbr id 10.4.0.0, via 10.4.0.4 on Et0/1, Unprotected
Label 15800, Paths 1, Static
  Nbr id 10.3.0.0, via 10.3.1.3 on Et0/2.1, Unprotected
Label 15801, Paths 1, Static
  Nbr id 10.3.0.0, via 10.3.2.3 on Et0/2.2, Unprotected
Label 15802, Paths 1, Static
  Nbr id 10.3.0.0, via 10.3.3.3 on Et0/2.3, Unprotected
Label 15810, Paths 1, Static
  Nbr id 10.3.0.0, via 10.3.1.3 on Et0/2.1, Protected, Nbr Prefix 10.33.33.33
  Primary path: via 10.3.1.3 on Et0/2.1, out-label 3
  Repair path: via 10.3.2.3 on Et0/2.2, out-label 3, cost 31, labels 0
```



第 26 章

OSPFv2 セグメント ルーティングの厳格な SPF

OSPFv2 セグメント ルーティングの厳格な最短パス優先 (SPF) 機能では、厳格な SPF セグメント識別子 (SID) に関する情報を提供します。

- [OSPFv2 セグメント ルーティングの厳格な SPF に関する機能情報 \(249 ページ\)](#)
- [OSPFv2 セグメント ルーティングの厳格な SPF の制約事項 \(250 ページ\)](#)
- [OSPFv2 セグメント ルーティングの厳格な SPF に関する情報 \(250 ページ\)](#)
- [OSPFv2 セグメント ルーティングの厳格な SPF の有効化および無効化 \(252 ページ\)](#)
- [OSPFv2 セグメント ルーティングの厳格な SPF SID の設定 \(253 ページ\)](#)
- [OSPFv2 セグメント ルーティングの厳格な SPF の確認 \(253 ページ\)](#)

OSPFv2 セグメント ルーティングの厳格な SPF に関する機能情報

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、<https://cfng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

表 25: OSPFv2 セグメントルーティングの厳格な SPF に関する機能情報

機能名	リリース	機能情報
OSPFv2 セグメントルーティングの厳格な SPF	Cisco IOS XE Amsterdam 17.3.2	OSPFv2 セグメントルーティングの厳格な SPF 機能は、厳格な最短パス アルゴリズムをサポートするためのプロビジョニングを提供します。パケットが SPF アルゴリズムに従って転送されることを強制し、SPF 決定を上書きする可能性のあるローカル ポリシーを無視するようにパス内のルータに指示します。 次のコマンドが追加または修正されました。 address-family ipv4 strict-spf。

OSPFv2 セグメントルーティングの厳格な SPF の制約事項

- OSPF エリア内のすべてのノードが厳格な SPF に対応していなければならない、セグメントルーティングトラフィック エンジニアリング (SR-TE) と連携する厳格な SPF ソリューションのために各ノードに少なくとも 1 つの厳格な SPF SID が必要です。
- 厳格な SPF SID の再配布はサポートされていません。

OSPFv2 セグメントルーティングの厳格な SPF に関する情報

セグメントルーティング (SR) アーキテクチャは、複数のプレフィックス SID アルゴリズムをサポートするためのプロビジョニングを提供します。現在、2 つのアルゴリズムが定義されています。

- **アルゴリズム 0**：これは最短パスアルゴリズムであり、デフォルトでサポートされています。
- **アルゴリズム 1**：これは厳格な最短パスアルゴリズムです。パケットが SPF アルゴリズムに従って転送されることを強制し、SPF 決定を上書きする可能性のあるローカルポリシーを無視するようにパス内のルータに指示します。厳格な最短パスアルゴリズムでアドバタイズされた SID により、パケットが取得しようとしているパスは、変更後の SPF パスではなく、予期したパスになります。セグメントルーティングをサポートする各ノードで、厳格な SPF SID を構成する必要があります。

アルゴリズム 1 はアルゴリズム 0 と同じですが、パスに沿ったすべてのノードが SPF ルーティングの決定を遵守することを必要とします。ローカルポリシーは、転送の決定を変更しません。たとえば、パケットはローカルに設計されたパスを通じて転送されません。

厳格な SPF を使用する理由

トンネルパスでリンクまたはノード障害が発生した場合、トラフィックが修復パスに即転送されると、SR-TE トンネルを介してルーティングされた MPLS トラフィックが中間チェーンからトンネルヘッドエンドに再ルーティングされる可能性があります。ヘッドエンドが SR-TE トンネル経由でこの MPLS トラフィックを再びルーティングした場合は、利用可能な宛先への代替 IGP 最短パスが存在する場合でも、同じ MPLS トラフィックが、TTL が満了するまでトンネルに沿ってループすることがあります。

厳格な SPF SID を使用すると、SR-TE トンネルを介したトラフィックのループを防ぐことができます。厳格な SPF のサポートにより、すべてのルータは、デフォルト SID、つまり SID0 と厳格な SPF SID、つまり SID1 の両方を持つように設定されます。トンネルトラフィックがヘッドエンドにルーティングされ戻された場合、アクティブ ラベルとして厳格な SPF SID を持つヘッドエンドに到着して非トンネル IGP 最短パス（ネイティブパス）経由で転送されるため、SR-TE トンネルに沿ってループを壊します。エリア/トンネルパス内のすべてのノードが厳格な SPF に対応している場合は、SRTE トンネルのデフォルトのプレフィックス SID よりも、厳格な SPF プレフィックス SID が優先されます。

厳格な SPF 機能のアドバイズメント

OSPF は、セグメントルーティングがグローバルまたは特定のエリアで有効になっている場合に、ルータ情報（RI）Opaque リンク状態アドバイズメント（LSA）の SR アルゴリズム TLV で厳格な SPF 機能をアドバイズします。OSPF には、SR アルゴリズム TLV のアルゴリズム 0（SPF）とアルゴリズム 1（厳格な SPF SID）の両方が含まれています。

受信されると、OSPF はルータ情報 Opaque LSA を解析して、SR アルゴリズム TLV を検出します。TLV が見つからないか、またはアルゴリズム 1 が TLV に含まれていない場合、OSPF はアドバイズメントルータからのすべての厳格な SPF SID アドバイズを無視します。

OSPF は引き続き単一の SRGB のみをサポートします。同じ SRGB が、通常の SID と厳格な SPF SID の両方に使用されます。通常の SID と同様に、OSPF では、SRGB 範囲の厳格な SPF SID を使用しないでください。

拡張プレフィックス LSA での厳格な SPF SID アドバイズメント

OSPF は、拡張プレフィックス Opaque LSA の OSPF 拡張プレフィックス TLV で 1 に設定されたアルゴリズムを使用して、プレフィックス SID サブ TLV の厳格な SPF SID 接続マップをアドバイズします。同じプレフィックスに対してデフォルト SID と厳格な SPF SID の両方が同じ LSA でアドバイズされます。OSPF は、通常の SID と厳格な SPF SID に対して、個別の明示的 NULL をアドバイズします。両方の SID は、同じアタッチフラグを共有します。

OSPF は、拡張プレフィックス Opaque LSA の OSPF 拡張プレフィックス範囲 TLV で、1 に設定されたアルゴリズムを使用して、プレフィックス SID サブ TLV の厳格な SPF SID マッピング サーバー エントリをアドバイズします。同じプレフィックスに対して、デフォルト SID と厳格な SPF SID の両方がアドバイズされる場合があります。同じプレフィックスに対して同じアルゴリズムの複数の SID がアドバイズされている場合、受信側のルータは最初のエン

コード済み SID を使用します。OSPF は、通常の SID と厳格な SPF SID に対して、個別の明示的 NULL をアドバタイズします。両方の SID は、同じアタッチ フラグを共有します。通常の SID では、アタッチ フラグの設定が異なる場合に優先順位を引き継ぎます。

SR アルゴリズム TLV が見つからないか、またはアルゴリズム 1 が TLV に含まれていない場合、OSPF はアドバタイズメント ルータからのすべての厳格な SPF SID アドバタイズを無視します。同じプレフィックスに対して同じアルゴリズムの複数の SID を受信した場合、受信側のルータは最初のエンコード済み SID を使用します。明示的 NULL およびアタッチ フラグがプレフィックスの受信 SID0 および SID1 と異なる場合、SID0 のフラグが優先順位を引き継ぎます。

SR-TE およびルータ情報ベースとのインタラクション

デフォルトの SID と同様に、厳格な SPF SID も、SR と TE の両方がそのエリアに対して有効になっている場合にのみ SR-TE と通信します。厳格な SPF SID に関連する SR-TE では、次の 3 つの形式の通信が発生する可能性があります。

- OSPF は、そのエリアが厳格な SPF に対応しているかどうかを SR-TE にアナウンスします。エリア内のすべてのノードが厳格な SPF に対応しているいて、各ノードに少なくとも 1 つの厳格 SPF SID が設定されている場合、そのエリアは厳格な SPF に対応しています。
- OSPF は、すべてのプレフィックスおよび登録されたプレフィックスパスについての厳格な SPF SID を SR-TE にアナウンスします。
- SR-TE は、ラベルスタックに対して厳格な SPF SID を優先します。OSPF は、自動ルート アナウンス トンネル リストのリストが変更されたときに、SR-TE からトンネル リストを受信します。各トンネルについて、SR-TE は、トンネルが厳格な SPF の SID またはデフォルトの SID を使用して作成されているかどうかを示します。OSPF は、更新されたトンネル リストが SR-TE から受信されるたびにフル SPF を実行し、トンネル エンドポイント 経由で到達可能なプレフィックスの RIB パスをトンネルのネクストホップに置き換えます。

厳格な SPF SID は、ルータ情報ベース (RIB) にはインストールされていません。RIB にインストールされているプレフィックスの発信ラベルとしてインストールされるのは、デフォルトの SID のみです。SR-TE トンネル タイプは両方とも RIB にインストールされています。

OSPFv2 セグメントルーティングの厳格な SPF の有効化および無効化

セグメントルーティング mpls が OSPF およびグローバル モードの下で設定される場合、厳格な SPF 機能はデフォルトで有効になっています。これを有効または無効にする個別の CLI はありません。

OSPFv2 セグメントルーティングの厳格な SPF SID の設定

OSPFv2 セグメントルーティングの厳格な SPF を設定するには、次の手順を実行します。

```
segment-routing mpls
connected-prefix-sid-map
address-family ipv4
  10.0.0.0/8 2
  172.16.0.0/8 3
address-family ipv4 strict-spf
  10.0.0.0/8 22
  172.16.0.0/8 23
exit-address-family
```

OSPFv2 セグメントルーティングの厳格な SPF の確認

次のコマンドを使用して、OSPFv2 セグメントルーティングの厳格な SPF を確認します。

OSPFv2 セグメントルーティングの厳格な SPF SID の確認

```
Device#show ip ospf database opaque-area type ext-prefix

          OSPF Router with ID (10.0.0.4) (Process ID 10)

          Type-10 Opaque Area Link States (Area 0)

LS age: 40
Options: (No TOS-capability, DC)
LS Type: Opaque Area Link
Link State ID: 10.7.0.3
Opaque Type: 7 (Extended Prefix)
Opaque ID: 3
Advertising Router: 10.0.0.2
LS Seq Number: 80000003
Checksum: 0xFB42
Length: 56

  TLV Type: Extended Prefix
  Length: 32
    Prefix      : 10.0.0.6/32
    AF          : 0
    Route-type: Intra
    Flags       : N-bit

  Sub-TLV Type: Prefix SID
  Length: 8
    Flags : None
    MTID  : 0
    Algo  : SPF
    SID   : 100

  Sub-TLV Type: Prefix SID
  Length: 8
    Flags : None
    MTID  : 0
```

```

Algo  : Strict SPF
SID   : 101

```

```
Device#show ip ospf segment-routing sid-database
```

```
OSPF Router with ID (10.0.0.4) (Process ID 10)
```

```
OSPF Segment Routing SIDs
```

```
Codes: L - local, N - label not programmed,
M - mapping-server
```

SID	Prefix	Adv-Rtr-Id	Area-Id	Type	Algo
2	10.0.0.2/32	10.0.0.2	0	Intra	0
4	(L) 10.0.0.4/32	10.0.0.4	0	Intra	0
7	10.0.0.7/32	10.0.0.5	0	Intra	0
9	10.0.0.8/32	10.0.0.2	0	Intra	0
20	10.0.2.20/32	10.2.2.2	0	Intra	0
21	10.0.22.21/32	10.2.2.2	0	Intra	1
22	(M) 10.0.2.22/32			Unknown	0
29	(M) 10.0.22.29/32			Unknown	1
33	10.0.33.33/32	10.3.3.3	0	Intra	1
38	(M) 10.0.3.38/32			Unknown	0
39	(M) 10.0.33.39/32			Unknown	1
77	10.77.77.77/32	10.5.5.5	0	Inter	0
92	(M) 10.1.2.92/32			Unknown	0
99	10.99.99.99/32	10.9.9.9	0	Intra	0
100	10.0.2.100/32	10.2.2.2	0	Intra	0
101	10.0.2.100/32	10.2.2.2	0	Intra	1
120	10.3.3.120/32	10.3.3.3	0	Intra	0
121	10.3.3.120/32	10.3.3.3	0	Intra	1

```
Device#show ip ospf segment-routing mapping-server
```

```
OSPF Router with ID (10.0.0.4) (Process ID 10)
```

```
Advertise local: Enabled
Receive remote: Enabled
```

```
Flags: i - sent to mapping-server, u - unreachable,
s - self-originated
```

```
10.0.2.22/32 (R), range size 1
```

Adv-rtr	Area	LSID	SID	Type	Algo
i 10.2.2.2	0	10.0.0.4	22	Intra	0
s 10.4.4.4	24	10.0.0.1	22	Inter	0

```
10.1.2.92/32 (R), range size 1
```

Adv-rtr	Area	LSID	SID	Type	Algo
i 10.2.2.2	0	10.0.0.5	92	Intra	0
s 10.4.4.4	24	10.0.0.2	92	Inter	0

```
10.0.3.38/32 (R), range size 1
```

Adv-rtr	Area	LSID	SID	Type	Algo
i 10.3.3.3	0	10.0.0.2	38	Intra	0
s 10.4.4.4	24	10.0.0.3	38	Inter	0

```
10.3.3.48/32 (R), range size 1
```

Adv-rtr	Area	LSID	SID	Type	Algo
i 10.3.3.3	0	10.0.0.3	48	Intra	0
s 10.4.4.4	24	10.0.0.4	48	Inter	0

```

10.0.22.29/32 (R), range size 1
  Adv-rtr      Area      LSID      SID      Type      Algo
i  10.2.2.2    0          10.0.0.6  29       Intra     1
s  10.4.4.4    24         10.0.0.5  29       Inter    1

10.1.22.99/32 (R), range size 1
  Adv-rtr      Area      LSID      SID      Type      Algo
i  10.2.2.2    0          10.0.0.7  99       Intra     1
s  10.4.4.4    24         10.0.0.6  99       Inter    1

10.0.33.39/32 (R), range size 1
  Adv-rtr      Area      LSID      SID      Type      Algo
i  10.3.3.3    0          10.0.0.4  39       Intra     1
s  10.4.4.4    24         10.0.0.7  39       Inter    1

10.3.33.49/32 (R), range size 1
  Adv-rtr      Area      LSID      SID      Type      Algo
i  10.3.3.3    0          10.0.0.5  49       Intra     1
s  10.4.4.4    24         10.0.0.8  49       Inter    1

Device#show ip ospf segment-routing local-prefix
                OSPF Router with ID (10.0.0.7) (Process ID 10)

Area 0:
  Prefix:      Sid:    Index:      Type:      Algo: Source:
10.2.2.2/32   2      10.0.0.0    Intra     0      Loopback0
              22     10.0.0.0    Intra     1      Loopback0
10.23.23.4/32 233    10.0.0.1    Intra     1      Loopback3

```

OSPFv2 セグメントルーティングの厳格な SPF 機能の確認

```

Device#show ip ospf database opaque-area type router-information self
                OSPF Router with ID (10.0.0.4) (Process ID 10)

                Type-10 Opaque Area Link States (Area 0)

LS age: 1692
Options: (No TOS-capability, DC)
LS Type: Opaque Area Link
Link State ID: 10.4.0.0
Opaque Type: 4 (Router Information)
Opaque ID: 0
Advertising Router: 10.4.4.4
LS Seq Number: 8000002
Checksum: 0x72B
Length: 60

TLV Type: Router Information
Length: 4
Capabilities:
  Graceful Restart Helper
  Stub Router Support
  Traffic Engineering Support

TLV Type: Segment Routing Algorithm
Length: 2
  Algorithm: SPF
  Algorithm: Strict SPF

TLV Type: Segment Routing Range
Length: 12

```

```

Range Size: 8000

Sub-TLV Type: SID/Label
Length: 3
Label: 16000

TLV Type: Segment Routing Node MSD
Length: 2
Sub-type: Node Max Sid Depth, Value: 10

```

OSPF ローカル RIB データベースで使用される厳格な SPF ラベルの確認

```

Device#show ip ospf rib 10.0.0.8

OSPF Router with ID (10.0.0.6) (Process ID 10)

Base Topology (MTID 0)

OSPF local RIB
Codes: * - Best, > - Installed in global RIB
LSA: type/LSID/originator

*> 10.0.2.100/32, Intra, cost 21, area 0
SPF Instance 28, age 00:01:19
contributing LSA: 10/10.7.0.3/10.2.2.2 (area 0)
SID: 100, Properties: Sid, LblRegd, SidIndex, N-Flag, TeAnn
Strict SPF SID: 101, Properties: Force, Sid, LblRegd, SidIndex, N-Flag
Flags: RIB, HiPrio
via 10.6.0.3, Ethernet0/1, label 16100, strict label 16101
Flags: RIB
LSA: 1/10.2.2.2/10.2.2.2
PostConvrq repair path via 10.6.0.5, Ethernet0/3, label 16100, strict label 16100,
cost 31
Flags: RIB, Repair, PostConvrq, IntfDj, BcastDj
LSA: 1/10.2.2.2/10.2.2.2

```

厳格な SPF TILFA トンネルの確認

```

Device#show ip ospf fast-reroute ti-lfa tunnels internal

OSPF Router with ID (10.0.0.2) (Process ID 10)

Area with ID (0)

Base Topology (MTID 0)

TI-LFA Release Node Tree:

TI-LFA Release Node 10.4.4.4 via 10.2.0.1 Ethernet0/0, instance 12, metric 20
Interface MPLS-SR-Tunnel2
Tunnel type: MPLS-SR (strict spf)
Tailend router ID: 10.4.4.4
Termination IP address: 10.4.4.4
Outgoing interface: Ethernet0/0
First hop gateway: 10.2.0.1
instance 12, refcount 1
rn-1: rtrid 10.4.4.4, addr 10.4.4.4, strict node-sid label 16044

TI-LFA Release Node 10.4.4.4 via 10.3.0.3 Ethernet0/1, instance 12, metric 20

```

```

Interface MPLS-SR-Tunnel1
  Tunnel type: MPLS-SR (strict spf)
  Tailend router ID: 10.4.4.4
  Termination IP address: 10.4.4.4
  Outgoing interface: Ethernet0/1
  First hop gateway: 10.3.0.3
  instance 12, refcount 1
    rn-1: rtrid 10.4.4.4, addr 10.4.4.4, strict node-sid label 16044

TI-LFA Node Tree:

TI-LFA Node 10.1.1.1 via 10.2.0.1 Ethernet0/0, abr, instance 12, rspt dist 0
  not-in-ext-p-space, in-q-space, interesting node 1
  Link Protect strict Path-1: via 10.3.0.3 Et0/1, parent 1/10.4.4.4, metric:30,
  rls-pt:10.4.4.4 at dist:20
  repair:y, rn-cnt:1, first-q:10.4.4.4, rtp-flags:Repair, PostConvrq, IntfDj
  rn-1: rtrid 10.4.4.4, addr 10.4.4.4, strict node-sid label 16044
  Protected by: MPLS-SR-Tunnel1, tailend 10.4.4.4, rls node 10.4.4.4
  instance 12, metric 20, refcount 1

TI-LFA Node 10.3.3.3 via 10.3.0.3 Ethernet0/1, instance 12, rspt dist 0
  not-in-ext-p-space, in-q-space, interesting node 1
  Link Protect strict Path-1: via 10.2.0.1 Et0/0, parent 1/10.4.4.4, metric:30,
  rls-pt:10.4.4.4 at dist:20
  repair:y, rn-cnt:1, first-q:10.4.4.4, rtp-flags:Repair, PostConvrq, IntfDj
  rn-1: rtrid 10.4.4.4, addr 10.4.4.4, strict node-sid label 16044
  Protected by: MPLS-SR-Tunnel2, tailend 10.4.4.4, rls node 10.4.4.4
  instance 12, metric 20, refcount 1

TI-LFA Node 10.4.4.4 via 10.2.0.1 Ethernet0/0, abr, instance 12, rspt dist 10
  in-ext-p-space, in-q-space, interesting node 1
  Link Protect strict Path-1: via 10.3.0.3 Et0/1, parent 1/10.3.3.3, metric:20,
  rls-pt:10.3.3.3 at dist:10
  repair:y, rn-cnt:0, first-q:10.4.4.4, rtp-flags:Repair, PostConvrq, IntfDj, PrimPath
  Protected by: directly connected TI-LFA

TI-LFA Node 10.4.4.4 via 10.3.0.3 Ethernet0/1, abr, instance 12, rspt dist 10
  in-ext-p-space, in-q-space, interesting node 1
  Link Protect strict Path-1: via 10.2.0.1 Et0/0, parent 1/10.1.1.1, metric:20,
  rls-pt:10.1.1.1 at dist:10
  repair:y, rn-cnt:0, first-q:10.4.4.4, rtp-flags:Repair, PostConvrq, IntfDj, PrimPath
  Protected by: directly connected TI-LFA

TI-LFA Protected neighbors:

Neighbor 10.2.0.1 Ethernet0/0, ID 10.1.1.1, Dist 10, instance 12
  TI-LFA Required, TI-LFA Computed, RLFA not Required
  TI-LFA protection Required: link

Neighbor 10.3.0.3 Ethernet0/1, ID 10.3.3.3, Dist 10, instance 12
  TI-LFA Required, TI-LFA Computed, RLFA not Required
  TI-LFA protection Required: link

```

厳格な SPF SR-TE トンネルの確認

```

Device#show mpls traffic-eng segment-routing ospf summary
IGP Area[1]: ospf 10 area 0, Strict SPF Enabled:
Nodes:

```

```

IGP Id: 10.1.1.20, MPLS TE Id: 10.1.1.1, OSPF area 0
  2 links with segment-routing adjacency SID
IGP Id: 10.2.0.0, MPLS TE Id: 10.2.2.2, OSPF area 0
  2 links with segment-routing adjacency SID
IGP Id: 10.3.0.0, MPLS TE Id: 10.3.3.3, OSPF area 0
  3 links with segment-routing adjacency SID
IGP Id: 10.4.4.4, MPLS TE Id: 10.4.4.4, OSPF area 0
  3 links with segment-routing adjacency SID
IGP Id: 10.5.0.0, MPLS TE Id: 10.5.5.5, OSPF area 0
  2 links with segment-routing adjacency SID
Prefixes:
10.1.1.1/32, SID index: 1, Strict SID index: 11
10.2.0.2/32
10.2.2.2/32, SID index: 2, Strict SID index: 22
10.2.2.22/32, SID index: 222, Strict SID index: 2222
10.3.3.3/32, SID index: 3, Strict SID index: 34
10.3.3.33/32, SID index: 333, Strict SID index: 1333
10.4.4.4/32, SID index: 4, Strict SID index: 444
10.5.5.5/32, SID index: 5, Strict SID index: 555
10.6.6.6/32, SID index: 6
10.7.7.7/32, SID index: 7
Total:
  Node Count      : 5
  Adjacency-SID Count: 17
  Prefix-SID Count : 10
Grand Total:
  Node Count      : 5
  Adjacency-SID Count: 17
  Prefix-SID Count : 10
  IGP Areas Count : 1

```

厳格な SPF 修復パスを使用して保護された adj-SID の確認

```
Device#sh ip ospf segment-routing protected-adjacencies detail
```

```
OSPF Router with ID (10.0.0.0) (Process ID 10)
```

```
Area with ID (0)
```

```

Nbr id 10.0.0.1, via 10.0.0.2 on Ethernet0/1, Label 26
  Primary path: via 10.0.0.2 on Et0/1, out-label 3
  Repair path: via 10.0.0.3 on Et0/2, out-label 13222, cost 31, labels 0
  Nbr Prefix 10.0.0.4, Strict
Nbr id 10.0.0.5, via 10.0.0.3 on Ethernet0/2, Label 25
  Primary path: via 10.0.0.3 on Et0/2, out-label 3
  Repair path: via 10.0.0.2 on Et0/1, out-label 12333, cost 21, labels 0
  Nbr Prefix 10.0.0.5, Strict

```

セグメントルーティング グローバル ブロックの確認

```
Device#show ip ospf segment-routing global-block
```

```
OSPF Router with ID (10.0.0.0) (Process ID 10)
```

```
OSPF Segment Routing Global Blocks in Area 0
```

Router ID:	SR Capable:	SR Algorithm:	SRGB Base:	SRGB Range:	SID/Label:
*10.0.0.0	Yes	SPF,StrictSPF	16000	8000	Label
10.0.0.1	Yes	SPF,StrictSPF	16000	8000	Label
10.0.0.2	Yes	SPF,StrictSPF	16000	8000	Label

10.0.0.3	Yes	SPF	16000	8000	Label
10.0.0.4	Yes	SPF,StrictSPF	16000	8000	Label
10.0.0.5	No				
10.0.0.6	Yes	SPF	16000	8000	Label

Device#



第 27 章

セグメントルーティング OSPFv2 マイクロループ回避

この機能により、IS-IS や OSPF などのリンクステートルーティングプロトコルを使用して、トポロジ変更後のネットワークコンバージェンス中に発生するマイクロループを防止または回避することができます。

- セグメントルーティング OSPFv2 マイクロループ回避に関する機能情報 (261 ページ)
- セグメントルーティング OSPFv2 マイクロループ回避に関する情報 (262 ページ)
- セグメントルーティング OSPFv2 マイクロループ回避の前提条件 (266 ページ)
- セグメントルーティング OSPFv2 マイクロループ回避の制約事項 (266 ページ)
- セグメントルーティング OSPFv2 マイクロループ回避の設定 (267 ページ)
- セグメントルーティング OSPFv2 マイクロループ回避の確認 (267 ページ)

セグメントルーティング OSPFv2 マイクロループ回避に関する機能情報

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、<https://cfng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

表 26: セグメントルーティング OSPFv2 マイクロループ回避に関する機能情報

機能名	リリース	機能情報
セグメントルーティング OSPFv2 マイクロループ回避	Cisco IOS XE Amsterdam 17.3.2	セグメントルーティングマイクロループ回避により、IS-IS や OSPF などのリンクステートルーティングプロトコルを使用して、トポロジ変更後のネットワークコンバージェンス中に発生するマイクロループを防止または回避することができます。 この機能により、次のコマンドが導入または変更されました。 microloop avoidance segment-routing 。

セグメントルーティング OSPFv2 マイクロループ回避に関する情報

マイクロループは、トポロジの変更（リンクダウン、リンクアップ、またはメトリック変更イベント）後にネットワークで発生する短いパケットループです。マイクロループは、ネットワーク内の異なるノードの非同時コンバージェンスによって引き起こされます。ノードが収束し、収束していないネイバーノードにトラフィックを送信すると、これら2つのノード間でトラフィックがループし、パケット損失、ジッター、および順不同パケットが発生する可能性があります。

セグメントルーティングマイクロループ回避機能によってトポロジの変更が検出されると、セグメントのリストを使用して宛先へのループフリーパスが作成されます。

マイクロループ

リンクまたはネットワークデバイスで発生した障害や復旧のためにネットワークトポロジに変更が生じると、IP Fast Reroute によって迅速なネットワークコンバージェンスが行われます。このとき、定期的なコンバージェンス機能によってトラフィックが新しく計算されたベストパス（別名、ポストコンバージェンスパス）へ移動されるまで、事前に計算されていたバックアップパスにトラフィックが移動されます。このネットワークコンバージェンスにより、トポロジ内で直接または間接的に接続された2台のデバイス間で、マイクロループが短期間発生する可能性があります。マイクロループは、ネットワーク内の異なるノードが異なるタイミングで互いに別々に代替パスを計算したときに発生します。たとえば、あるノードがコンバージェンスを実行し、ネイバーノードにトラフィックを送信したときに、そのネイバーノードでまだコンバージェンスが完了していないと、その2つのノードでトラフィックがループする可能性があります。

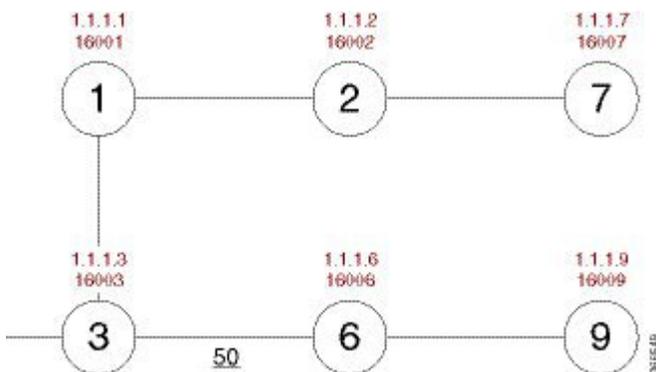
マイクロループによってトラフィックが損失する場合も、損失しない場合もあります。マイクロループが発生している期間が短ければ、つまりネットワークのコンバージェンスが迅速に行われれば、存続可能時間（TTL）が期限切れになるまでの短い期間、パケットがループする可能性があります。最終的には、パケットは宛先に転送されます。マイクロループの期間が長く

なる、つまりネットワーク内のいずれかのルータでコンバージェンスに時間がかかっていると、パケットで TTL が期限切れになったり、パケットレートが帯域幅を超過したり、パケットの順番が狂ったり、パケットがドロップされたりする場合があります。

障害が発生したデバイスとそのネイバーとの間で形成されたマイクロループはローカルユーロープと呼ばれます。また複数ホップ離れたデバイスとの間で形成されるマイクロループはリモートユーロープと呼ばれます。ローカルユーロープは、通常はローカルのループフリー代替 (LFA) パスが使用できないネットワークで見られます。このようなネットワークでは、リモート LFA によってネットワークのバックアップパスが提供されます。

上で説明した情報は、トポロジ例を参考にして示すことができます。

図 28: マイクロループのトポロジの例



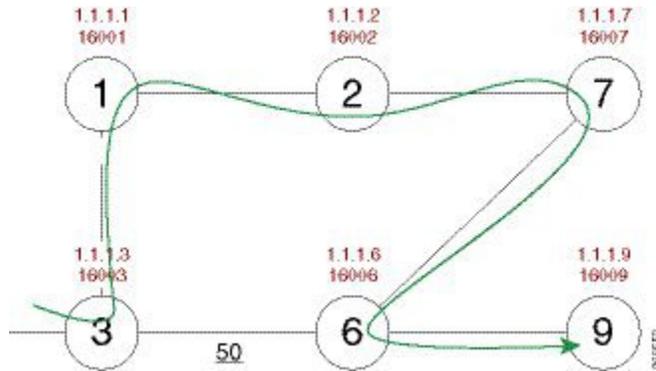
この例の前提条件は次のとおりです。

- デフォルトのメトリックは、メトリックが 50 であるノード 3 とノード 6 間のリンクを除き、各リンクごとに 10 です。各ノードでの SPF バックオフ遅延の収束順序は次のとおりです。
 - ノード 3 : 50 ミリ秒
 - ノード 1 : 500 ミリ秒
 - ノード 2 : 1 秒
 - ノード 7 : 1.5 秒

ノード 3 からノード 9 (宛先) に送信されたパケットは、ノード 6 経由で通過します。

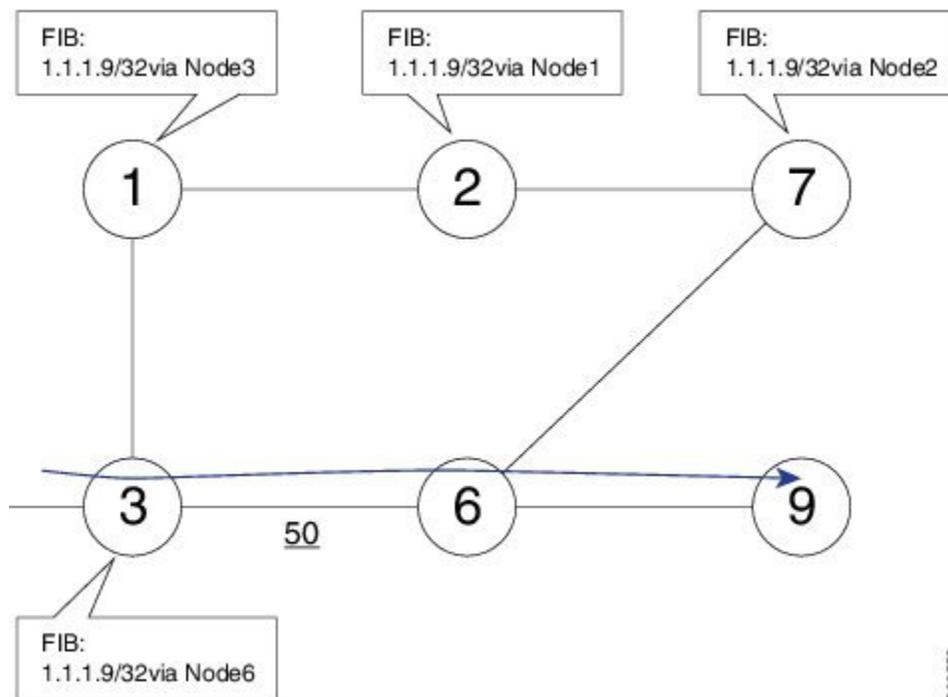
ノード 6 とノード 7 の間でリンクが確立されている場合、パケットが宛先であるノード 9 に到達する前のノード 3 からノード 9 へのパケットの最短パスは、ノード 1、ノード 2、ノード 7、およびノード 6 になります。

図 29: マイクロループのトポロジの例: 最短パス



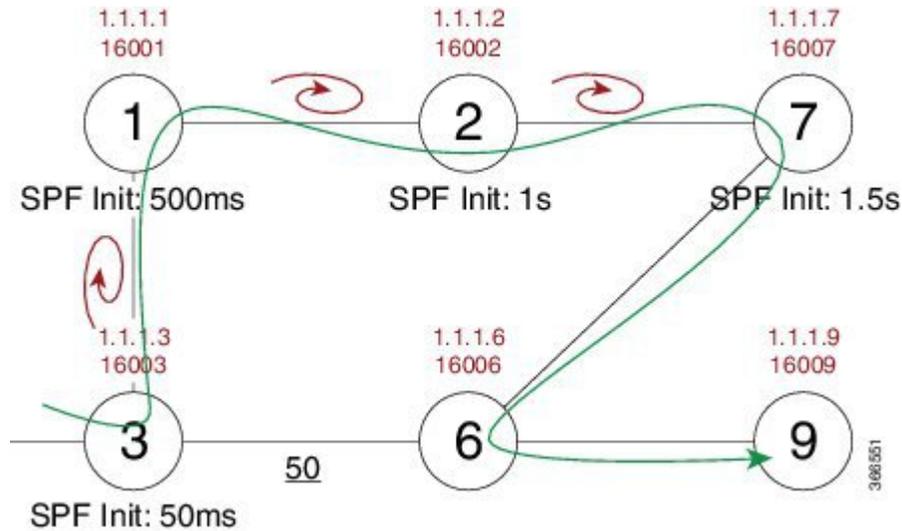
次の図は、ノード6とノード7間のリンクが確立される前の各ノードの転送情報ベース（FIB）テーブルを示しています。FIB エントリには、宛先ノード（ノード9）のプレフィックスとネクスト ホップが含まれます。

図 30: マイクロループのトポロジの例: FIB エントリ



ノード6とノード7間のリンクがアップすると、各ノードのコンバージェンスの順序に基づいて、マイクロループがリンクに対して発生します。この例では、ノード3は最初にノード1で収束し、その結果ノード3とノード1の間にマイクロループが発生します。その後、ノード1が次に収束し、その結果ノード1とノード2の間にマイクロループが発生します。次に、ノード2が次に収束し、その結果ノード2とノード7の間にマイクロループが発生します。最後に、次の図に示すように、ノード7はマイクロループの解決を収束し、パケットが宛先ノード9に到達します。

図 31: マイクロループのトポロジの例: マイクロループ

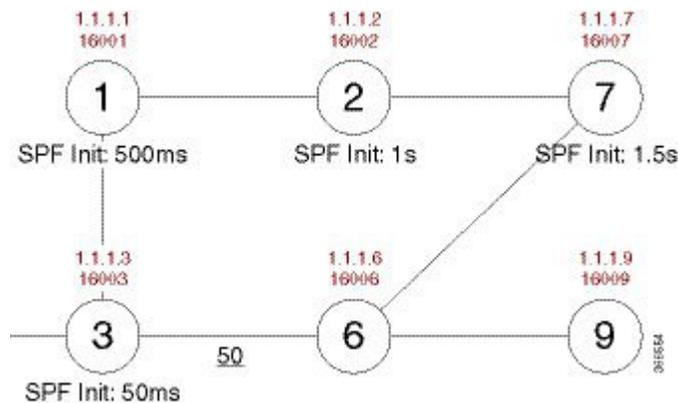


SPF コンバージェンス遅延を追加すると、マイクロループは 1.5 秒間（ノード 7 に指定されたコンバージェンス期間）接続を失うことになります。

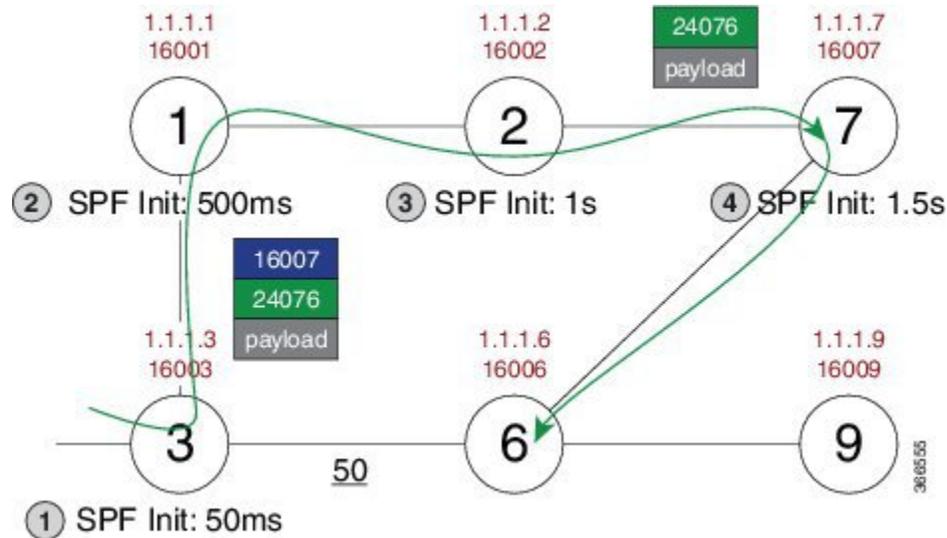
セグメントルーティングを使用したマイクロループの防止

このセクションでは、例を使用して、セグメントルーティングがマイクロループを防ぐ方法について説明します。この例のノード 3 は、**microloop avoidance segment-routing** コマンドで有効になっています。

図 32: マイクロループのトポロジの例: セグメントルーティング



FIB テーブルを更新する代わりに、ノード 3 は、ノード 7 のプレフィックスセグメント ID (SID) である 16007 を含むセグメント ID のリストと、ノード 6 の隣接関係セグメント ID (SID) である 24076 を使用して、宛先（ノード 9）のダイナミックループフリーパスを構築します。



したがって、ノード3からのパケットが宛先ノード9に到達することが可能になり、ネットワークが収束するまでマイクロループのリスクがなくなります。最後に、ノード3は新しいパスでFIBを更新します。

セグメントルーティング OSPFv2 マイクロループ回避の前提条件

SR マイクロループ回避を設定する前に、セグメントルーティングがOSPF ルータ モードでグローバルに設定されていることを確認してください。

```
router ospf process
segment-routing mpls
```

セグメントルーティング OSPFv2 マイクロループ回避の制約事項

- セグメントルーティング OSPFv2 マイクロループ回避は、マルチトポロジルーティング (MTR) をサポートしていません。MTID 0 のみをサポートしています。
- コンバージェンス後のパスに沿ったセグメント ID のリストは、リスト内のノードが SR に対応していて、ノード SID が少なくとも1つある場合にのみ使用されます。それ以外の場合、OSPF はコンバージェンス後のパスをただちにインストールします。
- SR マイクロループ回避は、ポイントツーポイント インターフェイスと2つのネイバーのみのブロードキャスト インターフェイスのリンク アップ、リンク ダウン、およびリンク メトリック変更イベントに使用されます。

- SR マイクロループ回避は、1つのトポロジ変更に対してのみ使用できます。複数のトポロジ変更が発生すると、OSPF はコンバージェンス後のパスをすぐにインストールします。

セグメントルーティング OSPFv2 マイクロループ回避の設定

すべてのプレフィックスのセグメントルーティング マイクロループ回避を有効にします。

```
router ospf
  microloop avoidance segment-routing
  microloop avoidance rib-update-delay delay-time
```

microloop avoidance rib-update-delay delay-time コマンドを使用して、ノードのフォワーディングテーブルを更新する前にノードが待機する遅延時間をミリ秒単位で設定し、マイクロループ回避の使用を停止します。RIB 遅延のデフォルト値は 5000 ミリ秒です。

セグメントルーティング OSPFv2 マイクロループ回避の確認

show ip ospf segment-routing microloop avoidance コマンドを使用して、SR マイクロループ回避が有効かどうかを確認します。



第 28 章

トラフィックエンジニアリングのパフォーマンス測定

パケット損失、遅延、遅延変動（ジッター）、帯域幅使用率などのメトリックは、ネットワークのパフォーマンスを評価するのに役立ちます。これらのメトリックをトラフィックエンジニアリング（TE）の入力として使用し、サービスレベル契約（SLA）に準拠するようにネットワークを通過するトラフィックのフローを誘導できます。この機能を使用すると、TE のリンク遅延メトリックの測定とアダプタイズメントを設定できます。

- [トラフィック エンジニアリングのパフォーマンス測定に関する機能情報（269 ページ）](#)
- [トラフィック エンジニアリングのパフォーマンスメトリックに関する情報（270 ページ）](#)
- [トラフィック エンジニアリングのパフォーマンス測定の設定方法（275 ページ）](#)
- [その他の参考資料（281 ページ）](#)

トラフィック エンジニアリングのパフォーマンス測定に関する機能情報

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 27: トラフィック エンジニアリングのパフォーマンス測定に関する機能情報

機能名	リリース	機能情報
リンク遅延測定	Cisco IOS XE Bengaluru 17.4	パケット損失、遅延、遅延変動（ジッター）、帯域幅使用率などのメトリックは、ネットワークのパフォーマンスを評価するのに役立ちます。これらのメトリックをトラフィックエンジニアリング（TE）の入力として使用し、サービスレベル契約（SLA）に準拠するようにネットワークを通過するトラフィックのフローを誘導できます。この機能を使用すると、TE のリンク遅延メトリックの測定とアダプタイズメントを設定できます。

トラフィック エンジニアリングのパフォーマンスメトリックに関する情報

リンク遅延測定の概要

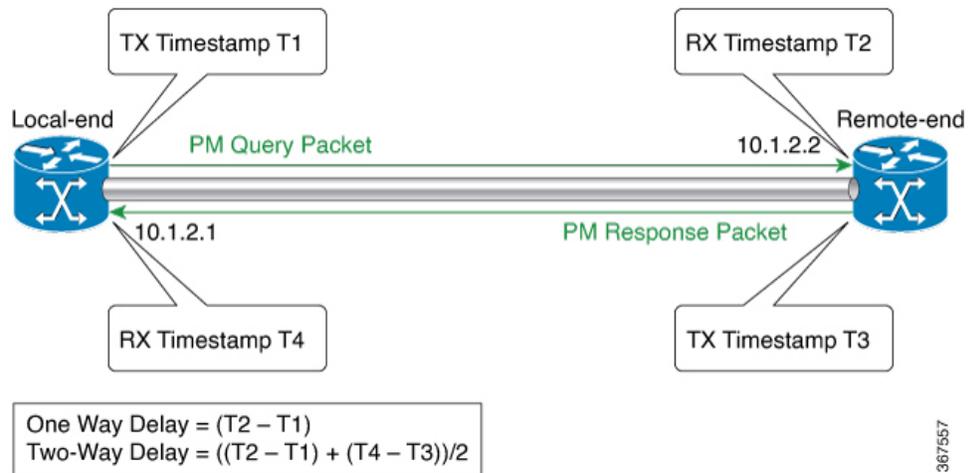
リンク遅延は、RFC 6374 で定義されている形式の PM クエリパケットを使用して測定されます。パケット形式をサポートするには、リモートラインカードが MPLS 対応である必要があります。



(注) 双方向リンク遅延測定のみがサポートされています。

リンク遅延測定では、MPLS マルチキャスト MAC アドレスを使用して、遅延測定プローブパケットをネクストホップに送信します。リンクのネクストホップのアドレスを設定する必要はありません。リモート側のラインカードは、MPLS マルチキャスト MAC アドレスをサポートしている必要があります。

次の図は、PM クエリおよび応答パケットを使用したリンク遅延の測定を示しています。



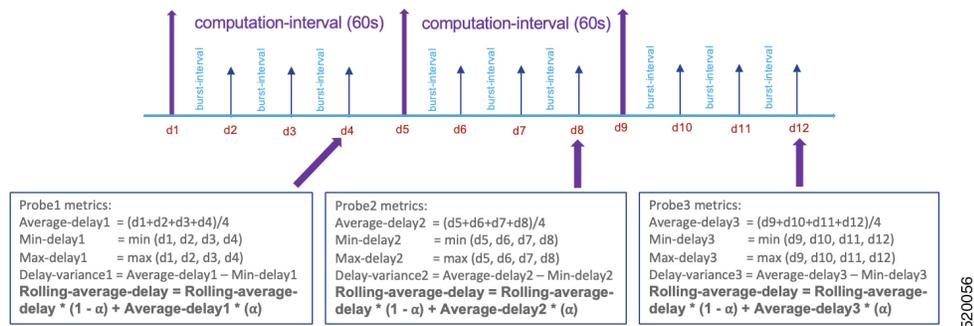
1. ローカルエンドルータは、設定されたインターバルでリモートエンドルータに PM Query パケットのバーストを送信します。パケットには、送信前にタイムスタンプ (T1) が付けられます。
2. リモートエンドルータでは、受信時にパケットにタイムスタンプ (T2) が付けられます。
3. リモートエンドルータは、タイムスタンプ (T1 および T2) を含む PM パケットをローカルエンドルータに送り返します。パケットには、送信前にタイムスタンプ (T3) が付けられます。
4. ローカルエンドルータでは、受信時にパケットにタイムスタンプ (T4) が付けられます。
5. ローカルエンドルータでは、PM パケットのタイムスタンプを使用して双方向リンク遅延が測定されます。

計算間隔のリンク遅延メトリック

ローカルエンドルータは、設定されたバースト間隔で、設定された数の PM クエリパケットをリモートエンドルータに送信します。ローカルエンドルータは、リモートエンドルータに送信してタイムスタンプとともに返される PM クエリパケットのバーストごとに、双方向リンク遅延を測定します。

設定されたプローブまたは計算間隔ごとに、PM パケットの複数のバーストが送信され、リンク遅延が測定されます。そのインターバルについて、最小、最大、平均のリンク遅延、および遅延バリエーションが計算されます。これらのメトリックは、インターバル中に送信されたバーストについて測定されたリンク遅延を使用して計算されます。

次の図は、計算間隔の遅延メトリックの計算を示しています。この例では、計算間隔は 60 秒で、バースト間隔は 15 秒です。



アドバタイズメントのリンク遅延メトリック

遅延メトリックの計算とアドバタイズメントは、定期的、高速、またはその両方で設定できます。リンク遅延メトリックのアドバタイズメントは、ISIS、OSPF、およびBGP-LSプロトコルでサポートされます。ISIS、OSPF、およびBGP-LSプロトコルを介してリンク遅延メトリックをフラッディングするために、追加の設定は必要ありません。

定期アドバタイズメント

定期アドバタイズメントはデフォルトで有効になっています。定期アドバタイズメントのインターバルは、1つ以上の計算またはプローブ間隔で構成されます。リンク遅延メトリックは、各計算間隔の終了時に計算されます。定期アドバタイズメントのインターバルでは、最後の計算間隔の後、リンクについて計算した最小遅延が以前にアドバタイズした値と比較されます。値の変動が設定された制限を超えている場合、リンクのすべての遅延メトリックがアドバタイズされます。値の変動が設定された制限内にある場合、リンクの遅延メトリックはアドバタイズされません。

- 定期アドバタイズメントのインターバルがN個の計算間隔で構成されているとすると、計算間隔*i*の終了時に、次のメトリックが計算されます。
 - ローリング平均遅延

$$\text{ローリング平均遅延} = \text{ローリング平均遅延}(i-1) * 0.5 + \text{平均遅延}(i) * 0.5$$
 - Minimum delay

$$\text{最小遅延} = \text{最小} [\text{最小遅延} (1) , \dots , \text{最小遅延} (i-1) , \text{最小遅延} (i)]$$
 - 最大遅延

$$\text{最大遅延} = \text{最大} [\text{最大遅延} (1) , \dots , \text{最大遅延} (i-1) , \text{最大遅延} (i)]$$
 - 遅延バリエーション

$$\text{遅延バリエーション} = \text{平均} [\text{遅延バリエーション} (1) , \dots , \text{遅延バリエーション} (i-1) , \text{遅延バリエーション} (i)]$$
- 定期アドバタイズメントのインターバルの最後の計算間隔の後、リンクの最小遅延は、その前の間隔の後にアドバタイズした値と比較されます。

- ケース 1 : 2 つの値の間の変化が、設定したしきい値と最小変化を超えている。この場合、最新の定期アドバタイズメントのインターバルの後にリンクについて計算したすべての遅延メトリックがアドバタイズされます。
- ケース 2 : 2 つの値の間の変化が、設定したしきい値と最小変化の範囲内である。この場合、遅延メトリックはアドバタイズされません。

高速アドバタイズメント

デフォルトでは、高速アドバタイズメントは無効になっています。高速アドバタイズメントを有効にすると、計算間隔の後にリンクについて計算した最小リンク遅延が、その前にアドバタイズした値と比較されます。値の変動が設定された制限を超えている場合、リンクのすべての遅延メトリックがアドバタイズされます。値の変動が設定された制限内にある場合、リンクの遅延メトリックはアドバタイズされません。

リンク遅延メトリックが高速でアドバタイズされると、定期アドバタイズメントのインターバルがリセットされます。このリセットにより、最新のアドバタイズメントと次の定期アセスメントの間に設定された時間間隔が確保されます。

リンクの状態が変化した場合のリンク遅延メトリック

リンクが DOWN 状態になると、リンク遅延メトリックが最大値でアドバタイズされます。最小、最大、平均のリンク遅延と遅延バリエーションは、16.7 秒 (0xFFFFF) の値でアドバタイズされます。最大メトリック値がアドバタイズされると、リンクが UP 状態になったときに、ルーティングおよび SR-TE パス計算で古いメトリック値が使用されることはありません。

グローバルリンク遅延プロファイル

リンク遅延メトリックの測定用にグローバルプロファイルを設定できます。プロファイルは、リンク遅延メトリックの計算とアドバタイズメントを制御するパラメータを定義し、デフォルト設定を置き換えます。グローバルであるため、プロファイルはすべてのインターフェイスのリンク遅延測定に適用されます。

グローバルプロファイルの一部として次のパラメータを設定できます。

表 28: グローバルリンク遅延プロファイルのパラメータ

項目	パラメータ	説明
プローブ	間隔	デフォルトのプローブまたは計算間隔は30秒です。範囲は30～3600秒です。
	protocol	プローブの送信に使用されるプロトコル。デフォルトであり、かつサポートされる唯一のプロトコルは pm-mpls です。MPLS カプセル化を使用した RFC 6374 に基づくリンク遅延測定です。
バースト	count	デフォルト値は10で、範囲は1～30です。
	間隔	デフォルト値は3000ミリ秒で、範囲は30～15000ミリ秒です。
定期アドバタイズメント	間隔	デフォルト値は120秒で、インターバルの範囲は30～3600秒です。
	threshold	定期アドバタイズメントのしきい値のデフォルト値は10%です。
	minimum-change	デフォルト値は1000マイクロ秒で、範囲は0～10000マイクロ秒です。
	無効	定期アドバタイズメントはデフォルトで有効になっています。
高速アドバタイズメント	threshold	デフォルト値は20%で、範囲は0～100%です。
	minimum-change	デフォルト値は1000マイクロ秒で、範囲は1～100000マイクロ秒です。

リンク遅延測定の利点

平均遅延、最小遅延、最大遅延、遅延バリエーションなどのリンク遅延メトリックを使用して、ネットワーク遅延を判断できます。リンク遅延メトリックを使用すると、遅延問題のトラブルシューティングや、サービスレベル契約（SLA）を満たすためのトラフィックエンジニアリング（TE）ソリューションの適用ができます。たとえば次のようなことができます。

- 遅延が許容可能な SR ポリシーの設定
- 提供している SR ポリシーの遅延パフォーマンスが許容限度を超えて低下した場合の、代替 SR ポリシーを介したトラフィックのステアリング

リンク遅延測定に関する制約事項

IOS XE リリース 17.1.x の制約事項

- 双方向リンク遅延の測定のみがサポートされています。
- PM リンク遅延測定は RFC 6374 に基づいており、PM パケットは MPLS/GAL カプセル化を使用します。
- しきい値チェックには、最小遅延値のみが使用されます。
- リンク遅延プローブプロトコルパケットのパケットサイズおよび TOS/DSCP/EXP は設定できません。
- 2 秒を超えるリンク遅延値は廃棄されます。

トラフィック エンジニアリングのパフォーマンス測定の設定方法

グローバルリンク遅延プロファイルの設定

インターフェイス遅延プロファイルモードを開始して、グローバルリンク遅延プロファイルのパラメータを設定します。

```
performance-measurement
  delay-profile
    interfaces    ---> Global default profile for link delay measurement
    probe
      computation-interval <seconds> (range:30-3600 seconds; default:30 seconds)
      burst-interval <milliseconds> (range:30-15000 milliseconds; default: 3000 milliseconds)

    protocol
      pm-mpls      Link delay measurement using RFC6374 with MPLS encapsulation
      twamp-light  Link delay measurement using RFC5357 [Default]
    advertisement
```

```

periodic (default: enabled)
  disabled
  interval <seconds> (range:30-3600 seconds; default:120 seconds)
  threshold <percentage> (range:0-100%; default:10%)
  minimum-change <microseconds> (range:0-100000 microseconds; default: 1000 microseconds)
accelerated (default: disabled)
  threshold <percentage> (range:0-100%; default: 20%)
  minimum-change <microseconds> (range:0-100000 microseconds; default: 1000 microseconds)

```



(注) PM リンク遅延セッションの数が 500 セッションを超える拡張シナリオでは、burst-interval を最大値の 15000 ミリ秒に増やすことをお勧めします。

インターフェイスのリンク遅延測定の設定

インターフェイスのリンク遅延測定の有効化

次のように、インターフェイスの遅延測定を有効にします。

```

performance-measurement
  interface <interface-name>
    delay-measurement

```

インターフェイスのリンク遅延測定の無効化

次のように、インターフェイスの遅延測定を無効にします。

```

performance-measurement
  interface <interface-name>
    no delay-measurement

```

インターフェイスのリンク遅延の設定

インターフェイスのリンク遅延を次のように設定します。

```

performance-measurement
  interface <interface-name>
    delay-measurement
      advertise-delay <microseconds> (range: 0-16777215 microseconds)

```

アドバタイズ遅延がインターフェイスに設定されている場合、

- 関連付けられたリンクの最小、最大、および平均遅延が、アドバタイズ遅延値に設定されます
- リンクの遅延バリエーションはゼロに設定されます
- リンク遅延メトリックはすぐにアドバタイズされます

計算間隔中に、PM クエリおよび応答パッケージが交換され、リンク遅延メトリックが計算されます。これらのメトリックは履歴バッファに保存され、コマンド **show performance-measurement history interfaces [name interface-name] [adv | aggr | probe]**。ただし、アドバタイズ遅延が設定されている場合、しきい値チェックは実行されません。したがって、計算されたメトリックはアドバタイズされません。

次のように、インターフェイスのリンク遅延設定を削除します。

```
performance-measurement
  interface <interface-name>
    delay-measurement
      no advertise-delay <microseconds>    (range: 0-16777215 microseconds)
```

インターフェイスのリンク遅延設定が削除されると、

- 遅延メトリックは、IGP から TLV を削除することで非公開になります。
- その後のアドバタイズメントのインターバル終了時に、しきい値チェックが実行されます。しきい値チェックに基づいて、必要に応じてリンク遅延メトリックがアドバタイズされます。

モニタリングモードの有効化

モニタリングモードでは、計算された遅延メトリックは、履歴バッファに保存されます。ただし、メトリックはIGPまたはBGP-LSによってアドバタイズされません。履歴バッファ内のメトリックは、**show performance-measurement history interfaces [name interface-name] [adv | aggr | probe]** コマンドを使用して表示できます。

モニタリングモードを有効にするには、リンク遅延メトリックの定期アドバタイズメントと高速アドバタイズメントの両方を無効にします。



(注) 高速アドバタイズメントはデフォルトで無効になっています。

次のように、定期アドバタイズメントを無効にします。

```
performance-measurement
  delay-profile
    interfaces ---> Global default profile for link delay measurement
    advertisement
      periodic (default: enabled)
      disabled
```

モニタリングモードを有効にすると、

- リンク遅延メトリックは、システムのインターフェイスマネージャ属性を介して公開されません。
- リンク遅延メトリックは、IGPによってネットワーク内でフラッディングされたり、BGP-LSによってアドバタイズされたりすることはありません。

リンク遅延設定の確認

リンク遅延の設定を表示するには、**show performance-measurement summary [detail]** コマンドを使用します。

例

```

router#show performance-measurement summary
Total interfaces          : 2
Maximum PPS              : 100 pkts/sec

Interface Delay-Measurement:
Total sessions           : 2
Profile configuration:
  Measurement Type       : Two-Way
  Probe interval         : 30 seconds
  Burst interval         : 3000 mSec
  Burst count            : 10 packets
  Protocol                : MPLS RFC6374
  HW Timestamp Supported : Yes
  Periodic advertisement : Enabled
  Interval                : 120 (effective: 120) sec
  Threshold               : 10%
  Minimum-Change         : 1000 uSec
  Advertisement accelerated : Disabled
  Threshold crossing check : Minimum-delay
Counters:
Packets:
  Total sent              : 289588
  Total received          : 289588
Errors:
  Total sent errors       : 23
  Total received errors   : 21
  .
  .
  .

```

インターフェイスのリンク遅延情報の表示

インターフェイスのリンク遅延測定に関する情報を表示するには、**show performance-measurement interfaces [name interface-name] [detail]** コマンドを使用します。

例

```

router#show performance-measurement interfaces name gigabitEthernet 0/0/7 detail
Interface Name: GigabitEthernet0/0/7 (ifh: 0xF)
Delay-Measurement      : Enabled
Local IPV4 Address     : 10.100.1.1
Local IPV6 Address     : ::
State                  : Up

Delay Measurement session:
  Session ID           : 1

Last advertisement:
  Advertised at: 13:53:11 28 2019 (434548 seconds ago)
  Advertised reason: Periodic timer, min delay threshold crossed
  Advertised delays (uSec): avg: 4011, min: 4033, max: 4050, variance: 4

Next advertisement:
  Check scheduled in 2 more probes (roughly every 120 seconds)
  Aggregated delays (uSec): avg: 4040, min: 4035, max: 4054, variance: 5
  Rolling average (uSec): 4040

Current Probe:
  Started at 14:35:38 02 2019 (1 second ago)
  Packets Sent: 1, received: 1
  Measured delays (uSec): avg: 4035, min: 4035, max: 4035, variance: 0
  Probe samples:
    Packet Rx Timestamp Measured Delay

```

```

14:35:38 02 2019 4035081
Next probe scheduled at 14:36:08 02 2019 (in 29 seconds)
Next burst packet will be sent in 2 seconds

```

その他のコマンド

show コマンド

表 29: ローカルエンドルータ（クエリア）の **show** コマンド

コマンド	説明
show performance-measurement summary [detail]	設定、セッションデータ、カウンタなど、PM リンク遅延情報を表示します。
show performance-measurement interfaces [name interface-name] [detail]	インターフェイスの PM リンク遅延情報を表示します。
show performance-measurement history interfaces [name interface-name] [adv aggr probe]	<ul style="list-style-type: none"> • probe : インターフェイスの PM リンク遅延プローブ履歴を表示します。 • adv : インターフェイスの PM リンク遅延アダプタイズメント履歴を表示します。リンク遅延メトリックのアダプタイズされる値は、ISIS、OSPF、またはBGPを使用してフラグディングされた値です。 • aggr : インターフェイスの PM リンク遅延集約履歴を表示します。
show performance-measurement counters interfaces [name interface-name] [detail]	PM リンク遅延セッションカウンタを表示します。
show performance-measurement sessions interface [session-id] [detail]	リモート側からプローブクエリを受信したインターフェイスに関する情報を表示します。

表 30: リモートエンドルータ（レスポнда）の **show** コマンド

コマンド	説明
show performance-measurement responder summary	リモートエンドルータ（レスポнда）のリンク遅延サマリーの PM を表示します。
show performance-measurement responder interfaces [name interface-name]	リモートエンドルータ上のインターフェイスの PM リンク遅延設定情報を表示します。
show performance-measurement responder counters interface [name interface-name]	リモートエンドルータ上の PM リンク遅延セッションカウンタを表示します。

clear コマンド表 31: ローカルエンドルータ (クエリア) の **clear** コマンド

コマンド	説明
clear performance-measurement all	アドバタイズされた遅延メトリックを含む、すべてのパフォーマンス測定データをクリアします。このコマンドを使用すると、IGP または BGP を使用してフラッディングされたすべての遅延メトリックが取り消されます。
clear performance-measurement delay interfaces [name <i>interface-name</i>]	インターフェイスの PM 遅延情報をクリアします。 (注) このコマンドを使用すると、クリアされたインターフェイスの以前にアドバタイズされた遅延が取り消されます。このコマンドの使用には注意が必要です。
clear performance-measurement counters interfaces [name <i>interface-name</i>]	PM インターフェイスカウンタをクリアします。
clear performance-measurement counters summary	PM サマリーカウンタをクリアします。

表 32: リモートエンドルータ (レスポнда) の **clear** コマンド

コマンド	説明
clear performance-measurement responder counters interfaces [name <i>interface-name</i>]	レスポндаの PM インターフェイスカウンタをクリアします。
clear performance-measurement responder counters summary	レスポндаの PM サマリーカウンタをクリアします。

debug コマンド表 33: ローカルエンドルータ (クエリア) の **debug** コマンド

コマンド	説明
debug performance-measurement query [errors entry packet-errors packets queues timers]	クエリアでデバッグメッセージを有効化します。

表 34: リモートエンドルータ（レスポнда）の *debug* コマンド

コマンド	説明
debug performance-measurement responder [errors entry packet-errors packets queues timers]	クエリアでデバッグメッセージを有効化します。

show tech-support コマンド

コマンド	説明
show tech-support perf_measure	パフォーマンス測定関連情報を表示します。
show tech-support monitor event-trace perf_measure	パフォーマンス測定に関連するトレース情報を表示します。

その他の参考資料

標準および RFC

標準/RFC	タイトル
RFC 6374	MPLS ネットワークのパケット損失と遅延の測定



第 29 章

パフォーマンス測定の設定

表 35: 機能の履歴

機能名	リリース情報	説明
RFC5357 (TWAMP ライト) を使用したセグメントルーティング パフォーマンス測定 の遅延測定	Cisco IOS XE Bengaluru 17.4	この機能により、ハードウェアタイムスタンプが有効になります。リンク遅延のパフォーマンス測定 (PM) は、RFC 5357 の付録 I で定義されている IP および UDP を介した双方向アクティブ測定プロトコル (TWAMP) の軽量バージョンを使用します。TWAMP は、RFC 6374 を使用していない場合の相互運用性の代替手段を提供します。
GRE-IPSec トンネルのセグメントルーティング絶対的一方 向リンク損失測定	Cisco IOS XE Dublin 17.10.1a	この機能は、指定した損失基準を満たすパスを識別するために、ポイントツーポイント GRE-IPSec トンネルのリンク損失測定メカニズムを提供します。

パケット損失、遅延、遅延変動、帯域幅使用率などのネットワーク評価指標は、サービスプロバイダー ネットワーク内のトラフィック エンジニアリング (TE) の重要な評価基準です。これらの評価指標は、パフォーマンス評価のためにネットワークの特性に関する情報をネットワークオペレータに提供し、サービスレベル契約に準拠するようにします。サービスプロバイダーのサービスレベル契約 (SLA) は、これらのネットワーク評価指標を測定および監視する能力によって異なります。ネットワークオペレータは、パフォーマンス測定 (PM) 機能を使用して、リンクのネットワークメトリックとともに、エンドツーエンドの TE ラベルスイッチドパス (LSP) もモニターできます。

次の表では、リンクまたは SR ポリシーの遅延を測定するためにパフォーマンス測定機能でサポートされている機能について説明します。

表 36: パフォーマンス測定機能

機能	詳細 (Details)
プローブとバーストのスケジューリング	プローブをスケジュールし、遅延測定用のメトリックアダプタイズメントパラメータを設定します。
メトリック アダプタイズメント	設定されたしきい値を使用して測定メトリックを定期的にあダプタイズします。また、設定されたしきい値を使用した高速アダプタイズメントもサポートします。
測定履歴とカウンタ	パケットの遅延および損失の測定履歴と、セッションカウンタおよびパケットアダプタイズメントカウンタも維持します。

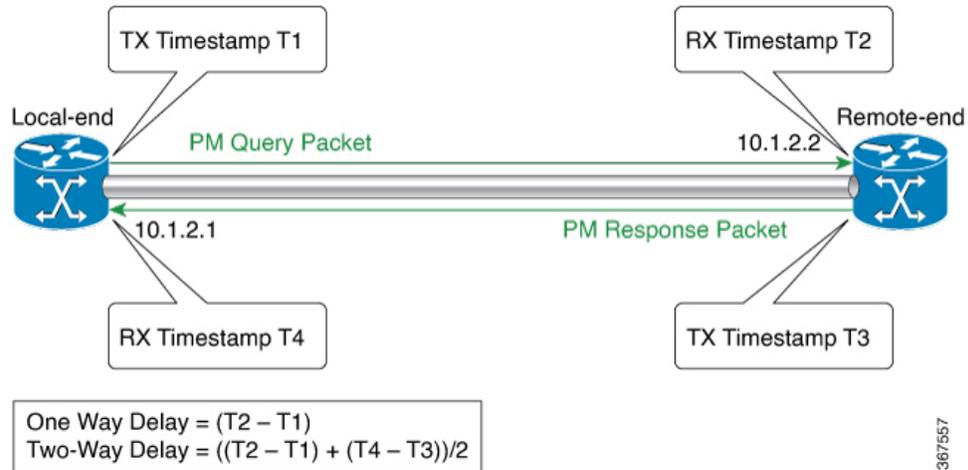
- [リンク遅延測定 \(284 ページ\)](#)
- [エンドツーエンド遅延測定 \(289 ページ\)](#)
- [一方向リンク損失測定 \(293 ページ\)](#)
- [show コマンドの例, on page 303](#)

リンク遅延測定

リンク遅延の PM は、RFC 5357 の付録 I で定義されている、IP および UDP を介した Two-Way Active Measurement Protocol (TWAMP) の軽量バージョンを使用します。したがって、TWAMP テストセッションのみが実装され、TWAMP 制御プロトコルは実装されません。TWAMP は、RFC 6374 を使用していない場合の相互運用性の代替手段を提供します。TWAMP パケットは、IP および UDP を介して伝送されます。したがって、MPLS データプレーンへの依存関係が解消されます。

次の図で、リンク遅延の PM クエリと応答について説明します。

図 33: リンク遅延のパフォーマンス測定



リンク遅延の PM クエリと応答は、次の手順で説明できます。

1. ローカルエンドルータは、ルータの出力ラインカードがパケットにタイムスタンプを適用すると、リモート側に PM クエリパケットを定期的送信します。
2. リモートエンドルータの入力ラインカードは、それを受信するとすぐにパケットにタイムスタンプを適用します。
3. リモートエンドルータは、タイムスタンプを含む PM パケットをローカルエンドルータに送り返します。リモートエンドルータは、双方向測定のため、パケットを送信する直前にパケットにタイムスタンプを付けます。

リンク遅延に関する PM の制約事項および使用上のガイドライン

異なるリンクのリンク遅延機能の PM には、次の制約とガイドラインが適用されます。

- ブロードキャストリンクでは、ポイントツーポイント (P2P) リンクのみがサポートされます。値のフラッドイングには、IGP での P2P 設定が必要です。
- ASR 1000 プラットフォームは PTP 1588v2 クロックをサポートしていないため、(T2-T1) を使用して一方向遅延値を計算することはできません。したがって、双方向遅延値を 2 で除算して一方向遅延値を計算します。
 - 双方向遅延 = (T2 - T1) + (T4 - T3)
 - 一方向遅延 = ((T2 - T1) + (T4 - T3))/2

PM リンク遅延：さまざまなパラメータのデフォルト値

リンク遅延に関する PM のさまざまなパラメータのデフォルト値は次のとおりです。

- probe : プロブのデフォルトモードは双方向遅延測定です。

- **interval** : デフォルトのプローブ間隔は 30 秒です。範囲は 30 ~ 3600 秒です。
- **burst count** : デフォルト値は 10 で、範囲は 1 ~ 30 です。
- **burst interval** : デフォルト値は 3000 ミリ秒で、範囲は 30 ~ 15000 ミリ秒です。
- **periodic advertisement** : 定期的なアドバタイズメントはデフォルトで有効になっています。
- **periodic-advertisement interval** : デフォルト値は 120 秒で、インターバルの範囲は 30 ~ 3600 秒です。
- **periodic-advertisement threshold** : 定期的なアドバタイズメントのしきい値のデフォルト値は 10% です。
- **periodic-advertisement minimum** : デフォルト値は 1000 マイクロ秒 (usec) で、範囲は 0 ~ 100000 マイクロ秒です。
- **accelerated advertisement** : 拡張アドバタイズメントはデフォルトで無効になっています。
- **accelerated-advertisement threshold** : デフォルト値は 20% で、範囲は 0 ~ 100% です。
- **accelerated-advertisement minimum** : デフォルト値は 1000 マイクロ秒で、範囲は 1 ~ 100000 マイクロ秒です。

設定例：リンク遅延の PM

この例では、リンク遅延のパフォーマンス測定機能をグローバルデフォルトプロファイルとして設定する方法を示します。

```
R1 (config) #performance-measurement
R1 (config-perf-meas) # delay-profile interfaces

R1 (config-pm-dm-intf) #advertisement
R1 (config-pm-dm-intf-adv) # accelerated // Default: Disabled
R1 (config-pm-dm-intf-adv-acc) #threshold 40 //Default 20%
R1 (config-pm-dm-intf-adv-acc) #minimum-change 1000 //Default 1000uSec
R1 (config-pm-dm-intf-adv) #periodic
R1 (config-pm-dm-intf-adv-per) #interval 100 //Default 120seconds
R1 (config-pm-dm-intf-adv-per) #threshold 40 //Default 10%
R1 (config-pm-dm-intf-adv-per) #minimum-change 1000 //Default 1000 uSec
R1 (config-pm-dm-intf) #probe

R1 (config-pm-dm-intf-probe) #computation-interval 40 // Def: 30s
R1 (config-pm-dm-intf-probe) #burst-interval 40 // Def: 3000 mSec
R1 (config-perf-meas) #delay-profile sr-policy
R1 (config-pm-dm-srpol) #advertisement
R1 (config-pm-dm-sr-adv) #accelerated // Default: Disabled
R1 (config-pm-dm-sr-adv-acc) #threshold 40 //Default 40%
R1 (config-pm-dm-sr-adv-acc) #minimum-change 4000 // Def: 500 uSec
R1 (config-pm-dm-sr-adv) #periodic

R1 (config-pm-dm-srpol-adv-per) #interval 100 // Def: 120 sec
R1 (config-pm-dm-srpol-adv-per) #threshold 40 // Def: 10%
R1 (config-pm-dm-srpol-adv-per) #minimum-change 2000 // Def: 500 uSec
R1 (config-pm-dm-srpol) #probe
R1 (config-pm-dm-srpol-probe) #computation-interval 40 // Def: 30s
```

```

R1(config-pm-dm-srpol-probe)#burst-interval 40 // Def: 3000 mSec
R1(config-pm-dm-srpol-probe)#exit

R1(config-pm-dm-srpol)#exit

R1(config-pm-dm-srpol-adv-per)#exit
R1 R1(config-pm-dm-intf-probe)#exit
R1(config-pm-dm-intf-adv)#exit

R1(config-pm-dm-intf)#exit

R1(config-perf-meas)#exit

```

この例では、インターフェイス上のリンク遅延に対して PM を有効にする方法を示します。

```

R1(config)#performance-measurement
R1(config-perf-meas)#interface GigabitEthernet 0/0/1
R1(config-pm-intf)#delay-measurement
R1(config-pm-intf-dm)#exit
R1(config-pm-intf-dm)#next-hop ipv4 10.50.62.1
R1(config-pm-intf)#exit

```

検証：PM リンク遅延設定

この例では、**show performance-measurement summary [detail]** コマンドを使用してリンク遅延設定の PM を確認する方法を示します。

```

R1#show performance-measurement summary detail
Total interfaces                : 3
Maximum PPS                     : 100 pkts/sec

Interface Delay-Measurement:
Total sessions                   : 3
Profile configuration:
  Measurement Type               : Two-Way
  Computation interval           : 30 seconds
  Burst interval                 : 3000 mSec
  Burst count                    : 10 packets
  Protocol                       : TWAMP-Lite Unauth
  HW Timestamp Supported         : No
  Periodic advertisement         : Enabled
  Interval                       : 30 (effective: 30) sec
  Threshold                      : 100%
  Minimum-Change                 : 100000 uSec
  Accelerated advertisement      : Enabled
  Threshold                      : 100%
  Minimum-Change                 : 100000 uSec
  Threshold crossing check       : Minimum-delay
Counters:
Packets:
  Total sent                     : 293020
  Total received                 : 293016
Errors:
  TX:
  Total interface down           : 0
  Total no MPLS caps             : 0
  Total no IP address            : 0
  Total other                     : 19
  RX:
  Total negative delay            : 144

```

```

Total delay threshold exceeded      : 0
Total missing TX timestamp          : 0
Total missing RX timestamp          : 0
Total probe full                    : 0
Total probe not started             : 0
Total control code error            : 0
Total control code notif            : 0
Probes:
  Total started                     : 29306
  Total completed                   : 29155
  Total incomplete                   : 148
  Total advertisements              : 3

Global Delay Counters:
  Total packets sent                : 293020
  Total query packets received      : 293016
  Total invalid session id          : 0
  Total no session                  : 0

HW Support for MPLS-GAL [RFC6374] timestamp : No
HW Support for TWAMP [RF5357] timestamp    : No
HW Support for 64 bit timestamp          : No
HW Support for IPv4 UDP Cheksum          : No

```

この例では、**show performance-measurement interfaces** [*interface-name*] [*detail*] コマンドを使用してリンク遅延設定の PM を確認する方法を示します。

```

R1#show performance-measurement interfaces detail
Interface Name: GigabitEthernet0/2/3 (ifh: 0xA)
  Delay-Measurement      : Enabled
  Local IPV4 Address     : 10.50.62.2
  Local IPV6 Address     : ::
  State                  : Up

Delay Measurement session:
  Session ID             : 1

Last advertisement:
  Advertised at: 09:21:08 12 2019 (439879 seconds ago)
  Advertised reason: Advertise delay config
  Advertised delays (uSec): avg: 2000, min: 2000, max: 2000, variance: 0

Next advertisement:
  Check scheduled at the end of the current probe (roughly every 30 seconds)
  No probes completed
  Rolling average (uSec): 3146

Current Probe:
  Started at 11:32:17 17 2019 (10 seconds ago)
  Packets Sent: 4, received: 4
  Measured delays (uSec): avg: 1999, min: 1500, max: 2499, variance: 499
  Probe samples:
    Packet Rx Timestamp Measured Delay
    11:32:17 17 2019 1999999
    11:32:20 17 2019 1500000
    11:32:23 17 2019 2499999
    11:32:26 17 2019 1999999
  Next probe scheduled at 11:32:46 17 2019 (in 19 seconds)
  Next burst packet will be sent in 1 seconds

R1#

```

次のコマンドを使用して、ローカルエンドルータのリンク遅延の PM を確認することもできます。

コマンド	説明
show performance-measurement history interfaces [nameinterface-name] probe	インターフェイスの PM リンク遅延プローブ履歴を表示します。
show performance-measurement history interfaces [nameinterface-name] aggr	インターフェイスの PM リンク遅延集約履歴を表示します。
show performance-measurement counters interface [nameinterface-name] [detail]	PM リンク遅延セッションカウンタを表示します。
show performance-measurement responder interfaces [nameinterface-name]	リモートエンドルータ上のインターフェイスのリンク遅延の PM を表示します。
show performance-measurement responder counters interface [nameinterface-name]	リモートエンドルータ上の PM リンク遅延セッションカウンタを表示します。

エンドツーエンド遅延測定

表 37: 機能の履歴

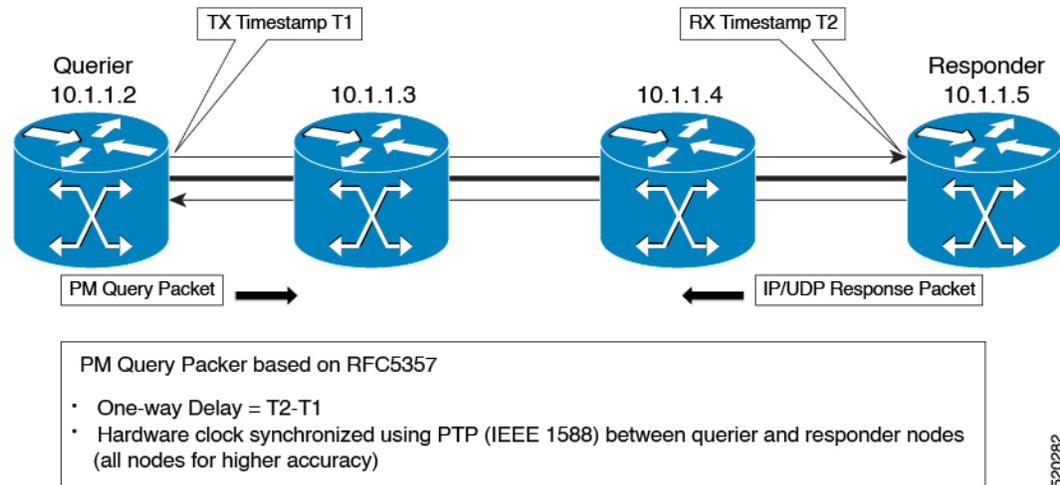
機能名	リリース情報	説明
セグメントルーティングパフォーマンス測定のエンドツーエンド遅延測定	Cisco IOS XE Bengaluru 17.4	この機能を使用すると、セグメントルーティングポリシーを介して送信されるトラフィックで発生するエンドツーエンド遅延をモニターできます。この機能により、遅延が指定したしきい値を超えたり、SLA に違反したりすることがなくなります。この機能を使用して、拡張 TE リンク遅延メトリック（最小遅延値）を適用し、最適化メトリックまたは累積遅延境界としてセグメントルーティングポリシーのパスを計算します。

Cisco IOS XE リリース 17.4.1 以降、セグメントルーティングパフォーマンス管理にエンドツーエンド遅延測定機能が導入されています。この機能を使用して、セグメントルーティングポリシーを介して送信されるトラフィックで発生するエンドツーエンド遅延をモニターします。この機能により、遅延が指定したしきい値を超えたり、SLA に違反したりすることがなくなります。転送テーブル内のセグメントルーティングポリシーの候補パスやセグメントリストを

アクティブにする前に、エンドツーエンド遅延値を確認できます。また、エンドツーエンド遅延値を使用して、転送テーブル内のセグメントルーティングポリシーのアクティブな候補パスやセグメントリストを非アクティブにすることもできます。この機能を使用して、拡張 TE リンク遅延メトリック（最小遅延値）を適用し、最適化メトリックまたは累積遅延境界としてセグメントルーティングポリシーのパスを計算します。

次の図は、エンドツーエンド遅延測定のパフォーマンス測定について説明しています。

図 34: エンドツーエンド遅延測定のパフォーマンス測定



エンドツーエンド遅延測定のパフォーマンス測定は、次の手順で説明できます。

1. ルータの出力ラインカードがパケットにタイムスタンプを適用すると、クエリアルータは PM クエリパケットをレスポンスルータに定期的送信します。
2. レスポンスルータの入力ラインカードは、受信時にパケットにタイムスタンプを適用します。
3. SR ポリシーのエンドツーエンド遅延値は、ルータ内のキューイング遅延などのいくつかの要因により、パス計算結果（TE リンク遅延メトリックの合計）とは異なります。
4. リモートエンドルータは、タイムスタンプを含む PM パケットをローカルエンドルータに送り返します。リモートエンドルータは、双方向測定のため、パケットを送信する直前にパケットにタイムスタンプを付けます。
5. ローカルエンドルータは、双方向測定のため、パケットを受信するとすぐにパケットにタイムスタンプを付けます。

設定例：エンドツーエンドの遅延管理用の PM

下記の例では、エンドツーエンドの遅延管理用のオンデマンドセグメントルーティングポリシーを設定する方法を示します。

```
#show running-config | s on-demand color 800
on-demand color 800 -----> SR ODN
```

```

Policy
authorize
performance-measurement -----> SR PM CLI
delay-measurement -----> SR PM CLI
candidate-paths
preference 1
constraints
segments
dataplane mpls
!
!
dynamic
pcep
metric
type delay
!
!
!
#

#show segment-routing traffic-eng policy name *10.216.216.216|800

Name: *10.216.216.216|800 (Color: 800 End-point: 10.216.216.216)
Owners : BGP
Status:
Admin: up, Operational: up for 01:27:24 (since 11-29 04:41:36.053)
Candidate-paths:
Preference 1 (BGP):
Dynamic (pce 10.12.12.12) (active)
Weight: 0, Metric Type: DELAY
Metric Type: DELAY, Path Accumulated Metric: 330
16011 [Prefix-SID, 10.205.205.205]
1133 [Adjacency-SID, 10.50.72.1 - 10.50.72.2]
16009 [Prefix-SID, 10.216.216.216]
Attributes:
Binding SID: 1218
Allocation mode: dynamic
State: Programmed
IPv6 caps enabled
#

```

この例では、エンドツーエンドの遅延管理のパフォーマンス測定機能をグローバルデフォルトプロファイルとして設定する方法を示します。

```

R1(config)#performance-measurement
R1(config-perf-meas)#delay-profile sr-policy

R1(config-pm-dm-srpol)#probe
R1(config-pm-dm-srpol-probe)#computation-interval 40

R1(config-pm-dm-srpol-probe)#burst-interval 40

R1(config-pm-dm-srpol-probe)#protocol twamp-light
R1(config-pm-dm-srpol-probe-protocol)#exit

R1(config-pm-dm-srpol-probe)#exit
R1(config-pm-dm-srpol)#advertisement periodic

R1(config-pm-dm-srpol-adv-per)#interval 100
R1(config-pm-dm-srpol-adv-per)#threshold 20

R1(config-pm-dm-srpol-adv-per)#minimum-change 500

```

```

R1 (config-pm-dm-srpol-adv-per) #exit

R1 (config-pm-dm-sr-adv) #exit

R1 (config-pm-dm-srpol) #advertisement accelerated

R1 (config-pm-dm-sr-adv-acc) #threshold 40

R1 (config-pm-dm-sr-adv-acc) #minimum-change 1000

R1 (config-pm-dm-sr-adv-acc) #exit
R1 (config-pm-dm-sr-adv) #exit

R1 (config-pm-dm-srpol) #exit

R1 (config-perf-meas) #exit

```

検証：PM エンドツーエンド遅延管理設定

この例では、**show performance-measurement summary** コマンドを使用してエンドツーエンド遅延管理設定の PM を確認する方法を示します。

```

R1#show performance-measurement summary
Total interfaces                : 6
Total SR Policies               : 1
Maximum PPS                    : 1000 pkts/sec

SR Policy Delay-Measurement:
Total sessions                  : 1
Profile configuration:
  Measurement Type              : Two-Way
  Computation interval          : 30 seconds
  Burst interval                 : 3000 mSec
  Burst count                   : 10
  Protocol                      : TWAMP-Lite Unauth
  HW Timestamp Supported        : Yes
  Periodic advertisement        : Enabled
  Interval                      : 30 (effective: 30) sec
  Threshold                     : 15%
  Minimum-Change                : 600 uSec
  Accelerated advertisement     : Enabled
  Threshold                     : 25%
  Minimum-Change                : 900 uSec
  Threshold crossing check      : Minimum-delay
Counters:
Packets:
  Total sent                    : 334
  Total received                 : 0
Errors:
  Total sent errors              : 0
  Total received errors         : 0
Probes:
  Total started                 : 33
  Total completed                : 0
  Total incomplete               : 33
  Total advertisements          : 0

Global Delay Counters:
Total packets sent              : 1251
Total query packets received   : 917

```

```

Total invalid session id          : 0
Total no session                  : 0

HW Support for MPLS-GAL [RFC6374] timestamp : No
HW Support for TWAMP [RF5357] timestamp    : Yes
HW Support for 64 bit timestamp           : Yes
HW Support for IPv4 UDP Cheksum           : No
R1#

```

一方向リンク損失測定

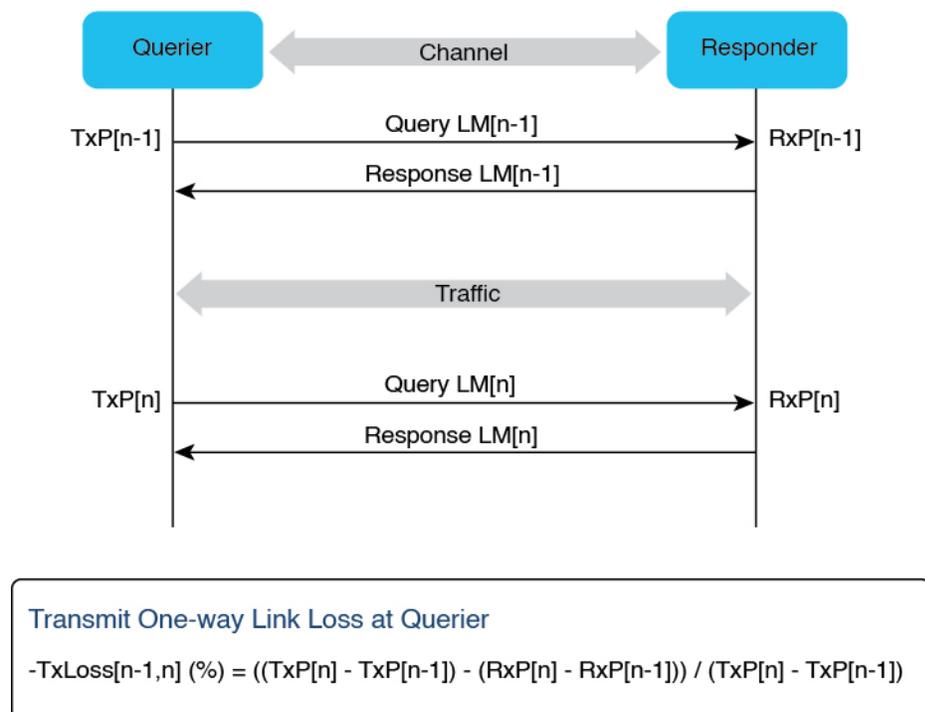
Cisco IOS XE リリース 17.10.1a 以降、ポイントツーポイント GRE-IPSec トンネルのリンク損失を測定するために、デュアルカラー損失測定メカニズムが実装されています。

一方向リンク損失測定に関する情報

ネットワーク全体で計算されるパスは、特定の SLA を達成するために、指定された損失要件を満たす必要があります。一方向リンク損失測定機能は、既存のネットワークパフォーマンス測定機能を拡張して、リンク損失を測定し、SLA の損失要件を満たすための基準として使用します。

これを実現するために、ユーザー データグラム プロトコル (UDP) による IP を介した [シンプル](#)な双方向直接損失測定 (SDLM) の基本プロトコルを活用する、絶対一方向パッシブメカニズムが導入されています。

図 35: 一方向リンク損失測定の概要



一方向リンク損失測定に関する制約事項

- デュアルカラーの GRE 一方向リンク損失測定のみがサポートされます。
- デュアルカラーの損失測定メカニズムは、ポイントツーポイント GRE-IPSec トンネルリンク損失の測定にのみ使用できます。
- クエリアとレスポンドは、同じ querier-dst-port UDP ポートを使用する必要があります。
- 設定するクエリア宛先ポート (querier-dst-port) とクエリア送信元ポート (querier-src-port) は異なっている必要があります。
- オーバーレイ宛先 IP アドレスは、測定された GRE-IPSec トンネルのネクストホップとして設定する必要があります。
- すべての測定対象インターフェイスは、クエリア側とレスポンド側の両方で同じ GRE を使用する必要があります。
- サポートされる最大セッション数は下記のとおりです。
 - BFD および IS-IS を使用した GRE-IPSec トンネル : 500
 - パフォーマンスの測定 : 500
- 内部ゲートウェイプロトコル (IGP) としてサポートされるのは IS-IS のみです。

一方向リンク損失測定でサポートされるプラットフォーム

Cisco IOS XE 17.10.1a 以降、一方向リンク損失測定は次のプラットフォームで使用できます。

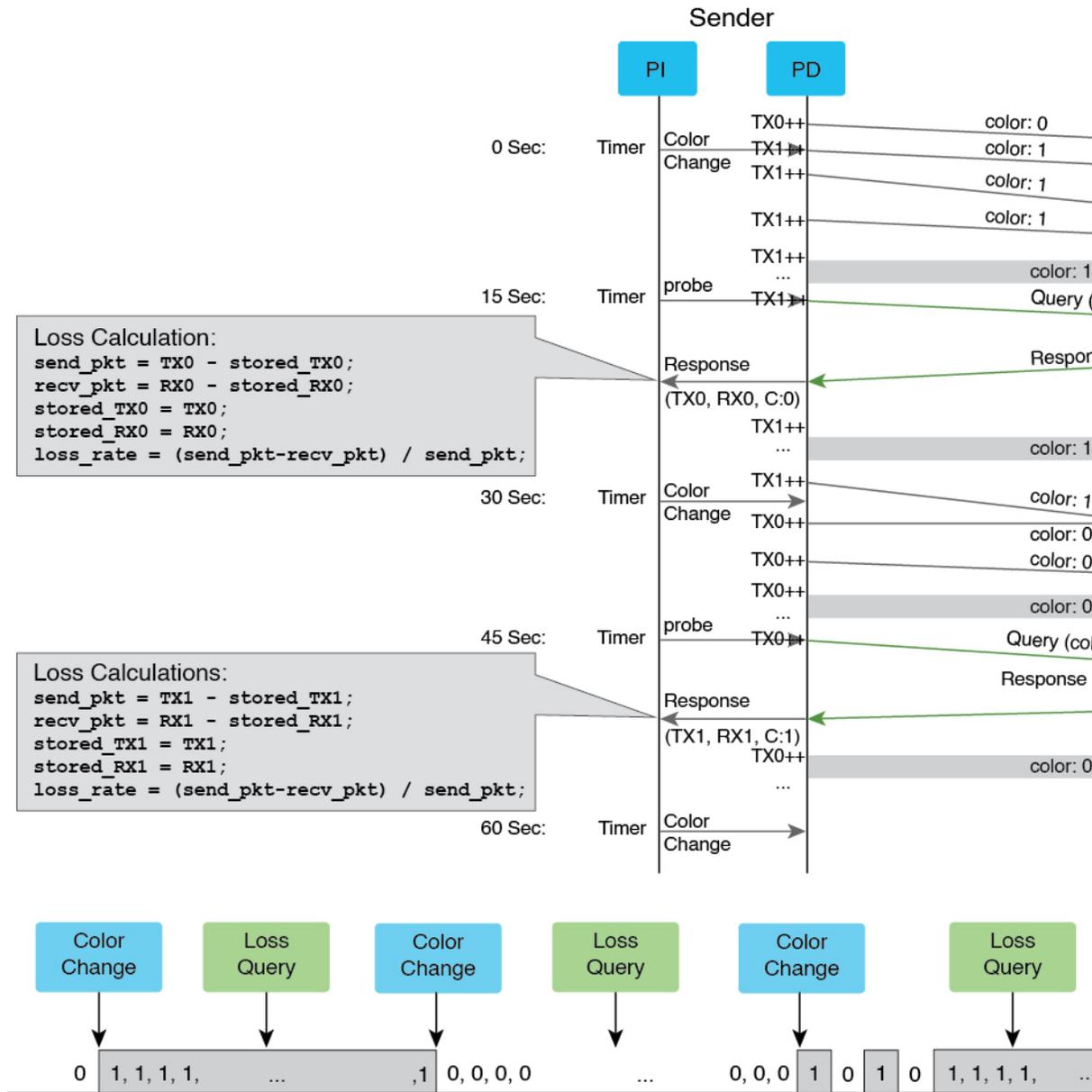
- Cisco 1000 シリーズ アグリゲーション サービス ルータ (ASR)
- Cisco Catalyst 8300 シリーズ エッジ プラットフォーム
- Cisco Catalyst 8500 シリーズ エッジ プラットフォーム
- Cisco Catalyst 8000V Edge ソフトウェア

GRE-IPSec トンネルのデュアルカラー損失測定

デュアルカラー損失測定メカニズムは、リアルタイムトラフィックの GRE-IPSec トンネルリンク損失を測定するために導入されています。未使用のビット ([フラグ (Flags)] フィールドの 9~12) の1つを、デュアルカラーリング用の GRE ヘッダー (RFC 1701) の [カラー (Color)] フィールドとして使用します。明示的に設定されていない場合、デフォルト値は 9 です。

デュアルカラー損失測定メカニズムを実装するため、**color-type** コマンドに新しいキーワード (**dual-color gre**) が導入されます。

図 36:デュアルカラー損失測定メカニズム



デュアルカラーメカニズムは次のように実装されます。

- トラフィックは、GREヘッダーの[カラー (Color)]フィールドのカラー値 (0または1) でタグ付けされ、カラー値は一定の間隔で0と1が交互に切り替わります。
- カラー付きのトラフィックがインターフェイスごとにカラー別でカウントされます。
- UDPプロトコルによるIP経路の非認証SDLM形式は、SDLMプローブパケットとSDLM応答プローブパケットをエンコードするために使用されます。これらのパケットは、非アクティブなTXまたはRXカウンタを伝送し、クエリア側で損失を計算します。

リンク損失測定に関する IGP IS-IS アドバタイズメント

IGP は、セグメントルーティング パフォーマンス測定 (SR-PM) からの A ビットの有無にかかわらず、拡張トラフィック エンジニアリング リンク損失メトリックをパーセンテージでアドバタイズします。このアドバタイズメントを有効化するために IS-IS で追加の設定を行う必要はありません。

- SR-PM が測定したリンク損失値が、設定したしきい値と最小変更値に違反した場合、SR-PM は値をパーセンテージとして IS-IS に送信し、この値は IS-IS ドメインでアドバタイズされます。
- 異常 (A) ビットは、設定した下限値と上限値をチェックすることで測定されたリンク損失値をアドバタイズする新しい方法を提供するために導入されています。
 - 測定されたリンク損失値が上限値を超えており、A ビットが設定されていない場合、SR-PM はアドバタイズのために、A ビットが設定された状態でその値をパーセンテージとして IS-IS に送信します。
 - 測定されたリンク損失値が下限値を下回っており、A ビットが設定されている場合、SR-PM はアドバタイズのために、A ビットが設定されていない状態でその値をパーセンテージとして IS-IS に送信します。

測定されたリンク損失に対する IGP IS-IS メトリック ペナルティ オプション

IS-IS は、ISIS インターフェイスの下に新しい CLI を追加することでメトリックペナルティのメカニズムを導入し、A ビットが設定されている場合に測定されたリンクの IGP、TE、または IGP と TE の両方のリンクメトリックを増やす、あるいは A ビットが設定されていない場合にそれを減らすというオプションを提供します。

```
isis metric fallback anomaly loss <options>
```

設定例：一方向リンク損失測定

クエリアでの設定

次に、GRE-IPSec トンネルに対してリンク損失測定を有効にし、ネクストホップを設定したクエリア側の設定の例を示します。測定したリンク損失値を IGP にアドバタイズする定期間隔は 120 秒に設定され、プローブ間隔は 30 秒に設定されます。異常基準の下限と上限は、デフォルト設定では 0.5 と 1.0 に設定され、サンプル設定では 1.0 と 2.0 に設定されます。

デフォルトの損失測定プローブのカラータイプは単色です。次に、損失測定機能を有効にするようにデュアルカラー GRE を設定する例を示します。IS-IS 損失異常ペナルティは、[増分 (Increment)]、[最大 (Maximum)]、[乗数 (Multiplier)] のいずれかのオプションに設定できます。

デフォルト設定

```
loss-profile interfaces
  advertisement
    periodic
      interval 120
```

```

    threshold 10.000000
    minimum-change 0.100000
    anomaly-check
      lower-bound 0.500000 upper-bound 1.000000
    !
  probe
    tx-interval 30
    color-type
    dual-color gre
  !

```

設定例

```

performance-measurement
  protocol sdlm-light
  measurement loss
    unauthenticated
      querier-dst-port 6634
  dual-color gre-flags bit-position 9
  interface Tunnel155
    loss-measurement
      loss-profile name Profile1
    loss-profile name Profile1
  advertisement
    periodic
      interval 120
      threshold 10.0
      minimum-change 0.1
    anomaly-check
      lower-bound 1.0 upper-bound 2.0
  probe
    tx-interval 30
    color-type
    dual-color gre

interface Tunnel155
  ip address 10.0.0.10 10.255.255.0
  ip router isis 1
  mpls ip
  mpls traffic-eng tunnels
  tunnel source GigabitEthernet3
  tunnel destination 10.0.0.20
  tunnel protection ipsec profile gre_profile
  isis metric fallback anomaly loss maximum level-1

```

レスポンスの設定

次の例は、レスポンス側の設定を示しています。

```

performance-measurement
  protocol sdlm-light
  measurement loss
    unauthenticated
      querier-dst-port 6634
  dual-color gre-flags bit-position 9

```

設定例：SR-MPLS ポリシーの設定

次の例で、静的セグメントルーティングポリシーとオンデマンドセグメントルーティングポリシーの設定方法を示します。

```

segment-routing traffic-eng
  policy static-policy

```

```

color 100 end-point 10.12.12.12
candidate-paths
  preference 100
  constraints
    segments
      dataplane mpls
    !
  !
  dynamic
    metric
      type igp
    !
  !
  !
  !
on-demand color 100
candidate-paths
  preference 100
  constraints
    segments
      dataplane mpls
    !
  !
  dynamic
    metric
      type igp
    !
  !
  !
  !

```



(注) 静的またはオンデマンドセグメントルーティングポリシーのいずれかを設定できます。

検証：一方向リンク損失測定

リンク損失測定設定のパフォーマンス測定パラメータに関する情報を提示するには、クエリア側で **show performance-measurement summary** コマンドを使用します。

```

show performance-measurement summary
Total interfaces                               : 1
Total SR Policies                             : 0
Total endpoints                               : 0
Maximum PPS                                  : 2000 pkts/sec
Dual-color gre bit-position                   : 9

Interface Delay-Measurement:
Total sessions                               : 0
Counters:
  Packets:
    Total sent                               : 0
    Total received                           : 0
  Errors:
    Total sent errors                         : 0
    Total received errors                    : 0
  Probes:
    Total started                             : 0

```

```

Total completed                : 0
Total incomplete                : 0
Total advertisements            : 0

SR Policy Delay-Measurement:
Total sessions                  : 0
Counters:
  Packets:
    Total sent                  : 0
    Total received              : 0
  Errors:
    Total sent errors           : 0
    Total received errors       : 0
  Probes:
    Total started               : 0
    Total completed             : 0
    Total incomplete            : 0
    Total advertisements        : 0

Endpoint Delay-Measurement:
Total sessions                  : 0
Counters:
  Packets:
    Total sent                  : 0
    Total received              : 0
  Errors:
    Total sent errors           : 0
    Total received errors       : 0
  Probes:
    Total started               : 0
    Total completed             : 0
    Total incomplete            : 0
    Total advertisements        : 0

Interface Loss-Measurement:
Total sessions                  : 1
Counters:
  Packets:
    Total sent                  : 22
    Total received              : 10
  Errors:
    Total sent errors           : 0
    Total received errors       : 0
  Probes:
    Total started               : 6
    Total completed             : 2
    Total incomplete            : 3
    Total advertisements        : 6

Global Counters:
Total packets sent              : 22
Total query packets received    : 10
Total invalid session id        : 0
Total no session                : 0

HW Support for MPLS-GAL [RFC6374] timestamp : Yes
HW Support for IPv4 TWAMP [RF5357] timestamp : Yes
HW Support for IPv6 TWAMP [RF5357] timestamp : Yes
HW Support for 64 bit timestamp          : No
HW Support for IPv4 UDP Cheksum          : Yes

```

リンク損失測定設定のパフォーマンス測定セッションに関する詳細情報を提示するには、**show performance-measurement sessions detail** コマンドを使用します。

```

show performance-measurement sessions detail
Transport type           :Interface
Measurement type        :Loss Measurement
Interface name          :Tunnel100
Nexthop                 :100.0.0.2

Loss Measurement session:
  Session ID             :1
  Profile name           :loss1

Last advertisement:
  Advertised at: 17:48:05 10-25 2022 (14 seconds ago)
  Advertised reason: First advertisement
  Advertised anomaly: INACTIVE
  Advertised loss(%) [Capped @ 50.331642%]: avg: 0.000000, min: 0.000000, max: 0.000000,
variance: 0.000000

Next advertisement:
  Check scheduled at the end of the current probe (roughly every 40 seconds)
  No probes completed
  Rolling average (%): 0.000000

Current Probe:
  Started at 17:48:05 10-25 2022 (14 seconds ago)
  Packets Sent: 1, received: 1
  Measured loss(%) [Capped @ 50.331642%]: avg: 0.000000, min: 0.000000, max: 0.000000,
variance: 0.000000

Probe samples:
Rx Timestamp           Last TX      TX           Last RX      RX           Co Loss(0-100%)
17:48:10 10-25 2022   677         680         11          14          0 0.000000

Next probe scheduled at 17:48:45 10-25 2022 (in 26 seconds)
  Next burst packet will be sent in 1 seconds

Liveness Detection:
  Session Creation Timestamp :10-25 17:32:00.699
  Session State: Up
  Last State Change Timestamp :10-25 17:47:40.761
  Missed count [consecutive] :0
  Received count [consecutive] :5
  Backoff                   :1
  Unique Path Name          :Path-1
  Loss in Last Interval     :0 % [TX: 1 RX: 1]

```

インターフェイスのパフォーマンス測定プロファイルの損失を表示するには、クエリア側で **show performance-measurement profile loss interface** コマンドを使用します。

```

show performance-measurement profile loss interface
Default Interface Loss Measurement:
  Profile configuration:
    Measurement Type           : One-Way
    Tx interval                 : 10 sec
    Protocol                    : SDLM-Lite Unauth
    ToS DSCP value              : 48
  Anomaly-check:
    lower-bound                 : 0.500000%
    upper-bound                 : 5.000000%
  Color-type:
    Dual-color:
      gre                       : Enabled
  Periodic advertisement
    Interval                    : 120 (effective: 120) sec

```

```

Threshold                               : 15.000000%
Minimum-Change                           : 0.200000

```

特定のインターフェイスのリンク損失や遅延などのパフォーマンス測定の詳細を表示するには、クエリア側で **show performance-measurement interfaces name <name> detail** コマンドを使用します。

```
show performance-measurement interfaces name tunnel100 detail
```

```

sh performance-measurement interfaces name Tunnel100 det
Interface Name: Tunnel100 (ifh: 0x11)
Delay-Measurement           : Disabled
Loss-Measurement            : Enabled
Local IPV4 Address          : 100.0.0.1
Local IPV6 Address           : ::
State                       : Up

Loss Measurement session:
Session ID                   : 1
Profile name                  : Not configured

Last advertisement:
Advertised at: 10:23:40 10-25 2022 (32 seconds ago)
Advertised reason: Periodic timer, avg loss threshold crossed
Advertised anomaly: ACTIVE
Advertised loss(%) [Capped @ 50.331642%]: avg: 9.458820, min: 9.997998, max:
10.002333, variance: 0.002499

Next advertisement:
Check scheduled at the end of the current probe (roughly every 40 seconds)
No probes completed
Rolling average (%): 9.458820

Current Probe:
Started at 10:23:40 10-25 2022 (32 seconds ago)
Packets Sent: 3, received: 3
Measured loss(%) [Capped @ 50.331642%]: avg: 6.667149, min: 0.000000, max: 10.002120,
variance: 6.667149

Probe samples:
Rx Timestamp      Last TX   TX       Last RX   RX       Col  Loss(0-100%)
10:24:05 10-25 2022 153911   153917   138520   138526   0    0.000000
10:23:55 10-25 2022 149505   177779   134556   160002   1    10.002120
10:23:45 10-25 2022 123899   153911   111509   138520   0    9.999333

Next probe scheduled at 10:24:20 10-25 2022 (in 8 seconds)
Next burst packet will be sent in 3 seconds

Liveness Detection:
Session Creation Timestamp: 10-25 10:09:56.898
Session State: Up
Last State Change Timestamp: 10-25 10:19:05.803
Missed count [consecutive]: 0
Received count [consecutive]: 32
Backoff           : 1
Unique Path Name   : Path-1
Loss in Last Interval : 0 % [TX: 3 RX: 3]

```

設定したインターフェイスのパフォーマンス測定プローブ履歴を表示するには、クエリア側で **show performance-measurement history interfaces probe** コマンドを使用します。

```
show performance-measurement history interfaces probe
```

```

Interface Name: Tunnell (ifh: 0x10)
Loss-Measurement history (%):
  Session ID: 1
  Probe Start Timestamp      Pkt (TX/RX) Average   Min       Max
23:28:56 08-04 2022         4/4         0.000000 0.000000 0.000000
23:28:16 08-04 2022         4/4         0.000000 0.000000 0.000000
23:27:36 08-04 2022         4/4         0.000000 0.000000 0.000000
23:26:56 08-04 2022         4/4         0.000000 0.000000 0.000000
23:26:16 08-04 2022         4/4         0.000000 0.000000 0.000000
23:25:36 08-04 2022         4/4         0.000000 0.000000 0.000000
23:24:56 08-04 2022         4/4         0.000000 0.000000 0.000000
23:24:16 08-04 2022         4/4         0.000000 0.000000 0.000000
23:23:36 08-04 2022         4/4         0.000000 0.000000 0.000000
23:22:56 08-04 2022         4/4         0.000000 0.000000 0.000000
23:22:16 08-04 2022         4/4         0.000000 0.000000 0.000000
23:21:36 08-04 2022         4/4         0.000000 0.000000 0.000000
23:20:56 08-04 2022         4/4         0.000000 0.000000 0.000000
23:20:16 08-04 2022         4/4         0.000000 0.000000 0.000000
23:19:36 08-04 2022         4/4         0.000000 0.000000 0.000000
23:18:56 08-04 2022         4/4         0.000000 0.000000 0.000000
23:18:16 08-04 2022         4/4         0.000000 0.000000 0.000000
23:17:36 08-04 2022         4/4         0.000000 0.000000 0.000000
23:16:56 08-04 2022         4/4         0.000000 0.000000 0.000000
23:16:16 08-04 2022         4/4         0.000000 0.000000 0.000000
23:15:36 08-04 2022         4/4         0.000000 0.000000 0.000000
23:14:56 08-04 2022         4/4         0.000000 0.000000 0.000000
23:14:16 08-04 2022         4/4         0.000000 0.000000 0.000000
23:13:36 08-04 2022         4/4         0.000000 0.000000 0.000000
23:12:56 08-04 2022         4/4         0.000000 0.000000 0.000000
23:12:16 08-04 2022         4/4         0.000000 0.000000 0.000000
23:11:36 08-04 2022         4/4         0.000000 0.000000 0.000000
23:10:56 08-04 2022         4/4         0.000000 0.000000 0.000000
23:10:16 08-04 2022         4/4         0.000000 0.000000 0.000000
23:09:36 08-04 2022         4/4         0.000000 0.000000 0.000000

```

IS-IS トラフィック エンジニアリング アプリケーション情報を表示するには、**show isis teapp** コマンドを使用します。

```

show isis teapp

Tag 200:
Tag 100:
Tag 1:
  ISIS TE Attr PM Information:
    Tu100: IDB num:14 Min:0 Max:0 Min-max-anomaly:0 Avg:0 Avg-anomaly:0 Var:0
    Is-Loss-set:1, Loss:533333 Loss-anomaly:1
    Tu200: IDB num:15 Min:0 Max:0 Min-max-anomaly:0 Avg:0 Avg-anomaly:0 Var:0
    Is-Loss-set:1, Loss:633333 Loss-anomaly:1

```

その他の show コマンドを表示するには、[検証：PM リンク遅延設定（287ページ）](#) を参照してください。

一方向リンク損失測定デバッグとトラブルシューティング

- INPUT_PM_DUAL_COLOR_LM（レスポンド側）および OUTPUT_PM_DUAL_COLOR_LM（クエリア側）が有効になっているかどうかを確認するには、`show platform hardware qfp active interface if-name <interface name> | i PM` コマンドを使用します。
- GRE ビット位置を確認するには、`show platform hardware qfp active feature sr client grebit-pos` コマンドを使用します。

- 送信元および宛先 UDP ポートを確認するには、`show platform hardware qfp active feature sr client udp-ports` コマンドを使用します。
- 現在のカラーを確認するには、`show platform hardware qfp active feature sr client dualcolor <interface name>` コマンドを使用します。
- パフォーマンス測定の設定とデータをクリアするには、次のコマンドを使用します。

```
clear performance-measurement
all clear all data
counters clear pm querier counters
delay clear pm querier delay
errors clear internal errors
loss clear pm querier loss
responder clear responder data
```

- パフォーマンス測定の設定をデバッグするには、次のコマンドを使用します。

```
debug performance-measurement
all Performance Measurements all categories
global Global
ha HA
query Query debugs
responder Responder debugs
```

show コマンドの例

```
R1#show performance-measurement interfaces detail
Interface Name: GigabitEthernet2 (ifh: 0x8)
Delay-Measurement : Enabled
Local IPV4 Address : 10.0.0.74
Local IPV6 Address : ::
State : Up
Delay Measurement session:
Session ID : 2
Last advertisement:
Advertised at: 06:45:50 02 2020 (214 seconds ago)
Advertised reason: First advertisement
Advertised delays (uSec): avg: 227, min: 198, max: 263, variance: 29
Next advertisement:
Check scheduled in 1 more probe (roughly every 160 seconds)
Aggregated delays (uSec): avg: 250, min: 208, max: 301, variance: 38
Rolling average (uSec): 254
Current Probe:
Started at 06:49:14 02 2020 (10 seconds ago)
Packets Sent: 3, received: 3
Measured delays (uSec): avg: 243, min: 230, max: 265, variance: 13
Probe samples:
Packet Rx Timestamp Measured Delay
06:49:22 02 2020 265500
06:49:18 02 2020 230000
06:49:14 02 2020 233500
Next probe scheduled at 06:49:54 02 2020 (in 30 seconds)
Next burst packet will be sent in 2 seconds

R1#show performance-measurement history interfaces name Gi2 probe
Interface Name: GigabitEthernet2 (ifh: 0x8)
Delay-Measurement history (uSec):
  Probe Start Timestamp Pkt(TX/RX) Average   Min     Max
    06:48:34 02 2020 10/10      254    216    301
```

```

06:47:54 02 2020 10/10      246      208      282
06:47:14 02 2020 10/10      262      182      380
06:46:34 02 2020 10/10      278      201      360
06:45:54 02 2020 10/10      274      202      364
06:45:14 02 2020 10/10      227      198      263

```

```

R1#show performance-measurement history interfaces name Gi2 aggr
Interface Name: GigabitEthernet2 (ifh: 0x8)
Delay-Measurement history (uSec):
Aggregation Timestamp Average   Min       Max       Action
06:47:50 02 2020 259           182       380       NONE

```

```

R1#show performance-measurement counters interface name Gi2 detail
Interface Name: GigabitEthernet2 (ifh: 0x8)
Delay-Measurement:
Packets:
  Total sent                : 67
  Total received            : 67
Errors:
TX:
  Total interface down      : 0
  Total no MPLS caps        : 0
  Total no IP address       : 0
  Total other                : 0
RX:
  Total negative delay      : 0
  Total delay threshold exceeded : 0
  Total missing TX timestamp : 0
  Total missing RX timestamp : 0
  Total probe full          : 0
  Total probe not started   : 0
  Total control code error   : 0
  Total control code notif   : 0
Probes:
  Total started             : 6
  Total completed           : 6
  Total incomplete          : 0
  Total advertisements      : 1

```

```

R1#show segment-routing traffic-eng policy all
Name: *10.2.2.2|100 (Color: 100 End-point: 10.2.2.2)
Owners : BGP
Status:
  Admin: up, Operational: up for 03:14:11 (since 12-02 03:36:05.290)
Candidate-paths:
  Preference 100 (BGP):
    Dynamic (active)
      Metric Type: TE, Path Accumulated Metric: 30
      16002 [Prefix-SID, 10.2.2.2]
Attributes:
  Binding SID: 40
  Allocation mode: dynamic
  State: Programmed
IPv6 caps enabled

```

```

R1#show performance-measurement sr-policy name *10.2.2.2|100 detail
SR Policy name: *10.2.2.2|100
Color                : 100
Endpoint              : 10.2.2.2
Source                : 10.9.9.9
Number of candidate-paths : 1
Candidate-Path:

```

```

Preference                               : 100
Protocol-origin                           : BGP
Discriminator                             : 0
Active:                                    : Yes
Number of segment-lists                   : 1
Number of atomic paths                    : 1
Max Pkts per Burst                        : 4000
Max Pkts per Probe                        : 40000
AP Min Run per Probe                      : 3
Round-robin bursts                        : 1
Round-robin probes                        : 1
Last advertisement:
  Advertised at: 06:45:52 02 2020 (271 seconds ago)
  Advertised delays (uSec): avg: 860, min: 740, max: 946, variance: 120
Next advertisement:
  Check scheduled in 1 more probe (roughly every 160 seconds)
  Aggregated delays (uSec): avg: 935, min: 795, max: 1146, variance: 140
Last probe:
  Packets Sent: 10, received: 10
  Measured delays (uSec): avg: 910, min: 844, max: 1013, variance: 66
Current Probe:
  Packets Sent: 8, received: 8
  Measured delays (uSec): avg: 949, min: 851, max: 1065, variance: 98

Segment-List:
Name                                       : SegmentList0
Number of atomic paths                    : 1
Last advertisement:
  Advertised at: 06:45:52 02 2020 (271 seconds ago)
  Advertised delays (uSec): avg: 860, min: 740, max: 946, variance: 120
Next advertisement:
  Aggregated delays (uSec): avg: 935, min: 795, max: 1146, variance: 140
Last probe:
  Packets Sent: 10, received: 10
  Measured delays (uSec): avg: 910, min: 844, max: 1013, variance: 66
Current probe:
  Packets Sent: 8, received: 8
  Measured delays (uSec): avg: 949, min: 851, max: 1065, variance: 98

R1#show performance-measurement sr-policy name *10.2.2.2|100 private
SR Policy name: *10.2.2.2|100
Color                                       : 100
Endpoint                                   : 10.2.2.2
Source                                     : 10.9.9.9
Number of candidate-paths                  : 1

Candidate-Path:
Preference                               : 100
Protocol-origin                           : BGP
Discriminator                             : 0
Active:                                    : Yes
Number of segment-lists                   : 1
Number of atomic paths                    : 1
Max Pkts per Burst                        : 4000
Max Pkts per Probe                        : 40000
AP Min Run per Probe                      : 3
Round-robin bursts                        : 1
Round-robin probes                        : 1
Last advertisement:
  Advertised at: 06:45:52 02 2020 (284 seconds ago)
  Advertised delays (uSec): avg: 860, min: 740, max: 946, variance: 120
Next advertisement:
  Check scheduled in 4 more probes (roughly every 160 seconds)
  Aggregated delays (uSec): avg: 935, min: 795, max: 1146, variance: 140

```

```

Last probe:
  Packets Sent: 10, received: 10
  Measured delays (uSec): avg: 963, min: 851, max: 1083, variance: 112
Current Probe:
  Packets Sent: 1, received: 1
  Measured delays (uSec): avg: 925, min: 925, max: 925, variance: 0

R1#show performance-measurement sr-policy name *10.2.2.2|100 verbose
SR Policy name: *10.2.2.2|100
  Color : 100
  Endpoint : 10.2.2.2
  Source : 10.9.9.9
  Number of candidate-paths : 1

Candidate-Path:
  Preference : 100
  Protocol-origin : BGP
  Discriminator : 0
  Active: : Yes
  Number of segment-lists : 1
  Number of atomic paths : 1
  Max Pkts per Burst : 4000
  Max Pkts per Probe : 40000
  AP Min Run per Probe : 3
  Round-robin bursts : 1
  Round-robin probes : 1
Last advertisement:
  Advertised at: 06:45:52 02 2020 (290 seconds ago)
  Advertised delays (uSec): avg: 860, min: 740, max: 946, variance: 120
Next advertisement:
  Check scheduled in 4 more probes (roughly every 160 seconds)
  Aggregated delays (uSec): avg: 935, min: 795, max: 1146, variance: 140
Last probe:
  Packets Sent: 10, received: 10
  Measured delays (uSec): avg: 963, min: 851, max: 1083, variance: 112
Current Probe:
  Packets Sent: 3, received: 3
  Measured delays (uSec): avg: 911, min: 882, max: 925, variance: 29

PE3#show performance-measurement history sr-policy name *10.2.2.2|100 probe
SR Policy name: *10.2.2.2|100
Candidate-Path:
  Preference : 100
  Protocol-origin : BGP
  Discriminator : 0
  Active : Yes
  Probe Start Timestamp Pkt(TX/RX) Average Min Max
    06:49:54 02 2020 10/10 963 851 1083
    06:49:14 02 2020 10/10 910 844 1013
    06:48:34 02 2020 10/10 896 795 1019
    06:47:54 02 2020 10/10 1000 882 1146
    06:47:14 02 2020 10/10 990 909 1135
    06:46:34 02 2020 10/10 931 735 1080
    06:45:54 02 2020 10/10 911 768 1087
    06:45:14 02 2020 10/10 860 740 946
Segment-list:
  Name : SegmentList0
  Probe Start Timestamp Pkt(TX/RX) Average Min Max
    06:49:54 02 2020 10/10 963 851 1083
    06:49:14 02 2020 10/10 910 844 1013
    06:48:34 02 2020 10/10 896 795 1019
    06:47:54 02 2020 10/10 1000 882 1146
    06:47:14 02 2020 10/10 990 909 1135
    06:46:34 02 2020 10/10 931 735 1080
    06:45:54 02 2020 10/10 911 768 1087

```

```

06:45:14 02 2020 10/10      860      740      946
Atomic path:
  Hops          : 10.2.2.2
  Labels       : 16002
  Outgoing Interface : GigabitEthernet2
  Next Hop     : 10.0.0.73
  Destination  : 10.2.2.2
  Session ID   : 1
  Probe Start Timestamp Pkt(TX/RX) Average  Min      Max
    06:49:54 02 2020 10/10      963      851     1083
    06:49:14 02 2020 10/10      910      844     1013
    06:48:34 02 2020 10/10      896      795     1019
    06:47:54 02 2020 10/10     1000      882     1146
    06:47:14 02 2020 10/10      990      909     1135
    06:46:34 02 2020 10/10      931      735     1080
    06:45:54 02 2020 10/10      911      768     1087
    06:45:14 02 2020 10/10      860      740     946

R1#show performance-measurement history sr-policy name *10.2.2.2|100 aggr
SR Policy name: *10.2.2.2|100
Candidate-Path:
  Preference          : 100
  Protocol-origin     : BGP
  Discriminator       : 0
  Active              : Yes
  Aggregation Timestamp Average  Min      Max      Action
    06:50:32 02 2020 942      795     1146    NONE
    06:47:52 02 2020 922      735     1135    NONE
Segment-list:
  Name                : SegmentList0
  Aggregation Timestamp Average  Min      Max      Action
    06:50:32 02 2020 942      795     1146    NONE
    06:47:52 02 2020 922      735     1135    NONE
Atomic path:
  Hops          : 10.2.2.2
  Labels       : 16002
  Outgoing Interface : GigabitEthernet2
  Next Hop     : 10.0.0.73
  Destination  : 10.2.2.2
  Session ID   : 1
  Aggregation Timestamp Average  Min      Max      Action
    06:50:32 02 2020 942      795     1146    NONE
    06:47:52 02 2020 922      735     1135    NONE

```




第 30 章

IP エンドポイントの遅延測定および活性モニタリング

このモジュールでは、エンドツーエンドの遅延を測定し、指定された IP エンドポイントへの活性をモニターする IP エンドポイント機能のパフォーマンス測定について説明します。

- [IP エンドポイントのパフォーマンス遅延測定および活性モニタリングに関する情報 \(309 ページ\)](#)
- [IP エンドポイントのパフォーマンス遅延測定のユースケース \(311 ページ\)](#)
- [IP エンドポイントのパフォーマンス遅延測定の設定方法 \(312 ページ\)](#)
- [IP エンドポイントのパフォーマンス遅延測定の設定例 \(318 ページ\)](#)
- [IP エンドポイントのパフォーマンス遅延測定の検証 \(320 ページ\)](#)
- [IP エンドポイントの遅延測定および活性モニタリングの機能情報 \(324 ページ\)](#)

IP エンドポイントのパフォーマンス遅延測定および活性モニタリングに関する情報

IP エンドポイント機能のパフォーマンス測定は、指定された IP エンドポイントに対するエンドツーエンドの遅延を動的に測定します。IP エンドポイントは、グローバルルーティングテーブルまたは VRF にあります。

IP エンドポイントのパフォーマンス遅延測定および活性モニタリングの利点

- パフォーマンス値（遅延メトリックと活性状態）は、Two-Way Active Measurement Protocol (TWAMP) Light を使用して計算されます。
- グローバルルーティングテーブルの IP アドレス、IPv4 VRF、および IPv6 VRF を使用した TWAMP 測定をサポートします。

- ヒストグラムを含むパフォーマンス値は、手動のデータ収集手法ではなく、プッシュベースのデータ収集手法であるストリーミングテレメトリを使用して送信されます。

IP エンドポイントのパフォーマンス遅延測定および活性モニタリングの制約事項

- MPLS-Path を使用した IP エンドポイントのパフォーマンス遅延測定はサポートされていません。
- ループバックモードでの IP エンドポイントのパフォーマンス遅延測定はサポートされていません。
- TWAMP のプラットフォーム パント ポリサーは、スケーリング展開用に設定することをお勧めします。
- デフォルトのバースト間隔（3 秒）を変更すると、パフォーマンス測定機能によって送信される pps の数に直接影響するため、注意してください。
- 送信側と応答側の両方に対する TWAMP Light のサポート。
- 双方向（必須） および一方向（オプション） の遅延測定がサポートされています。双方向遅延測定を使用することを強く推奨します。
- 一方向の測定は、遅延が数十ミリ秒または数百ミリ秒のオーダーであると予想され、パスが非対称であることがわかっている場合にのみ使用してください。この測定では、ソースデバイスとターゲットデバイスのクロックを同期させる必要があります。
- クロック同期には Network Time Protocol (NTP) を使用することを強く推奨します。
- 最小 2500 pps（それぞれ 10 pps で設定された 250 のプローブ/セッション）。
- 期待される精度は IP-SLA と同様です。
- TWAMP-light プローブの TOS/DSCP の設定がサポートされています。
- パケットサイズの設定がサポートされています。
- パディングサイズを変更すると、CPU 使用率が増加します。

IP エンドポイントのパフォーマンス遅延測定および活性モニタリングでサポートされるプラットフォーム

IP エンドポイントの遅延測定および活性モニタリング機能は、次のプラットフォームで使用できます。

- Cisco Catalyst 8500 シリーズ エッジプラットフォーム
- Cisco Catalyst 8200 シリーズ エッジプラットフォーム

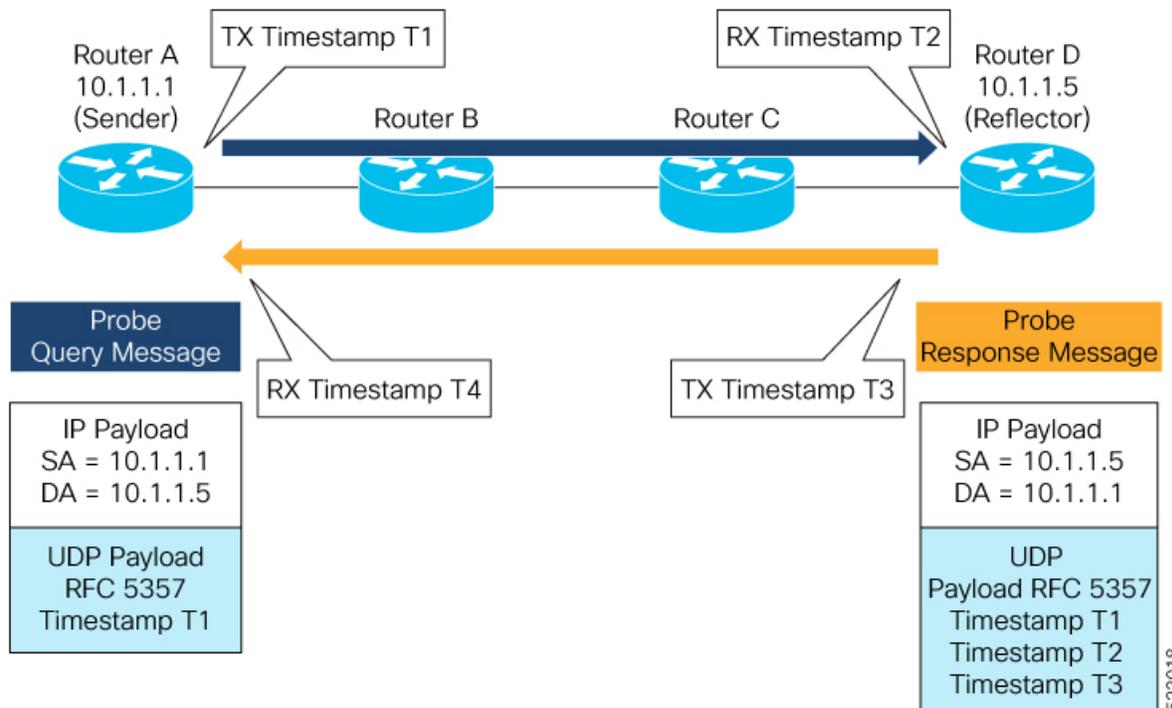
- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ
- Cisco Catalyst 8000V Edge ソフトウェア

IP エンドポイントのパフォーマンス遅延測定の実用例

次の実用例は、IP エンドポイントの遅延測定と活性検出を展開するさまざまな方法を示しています。

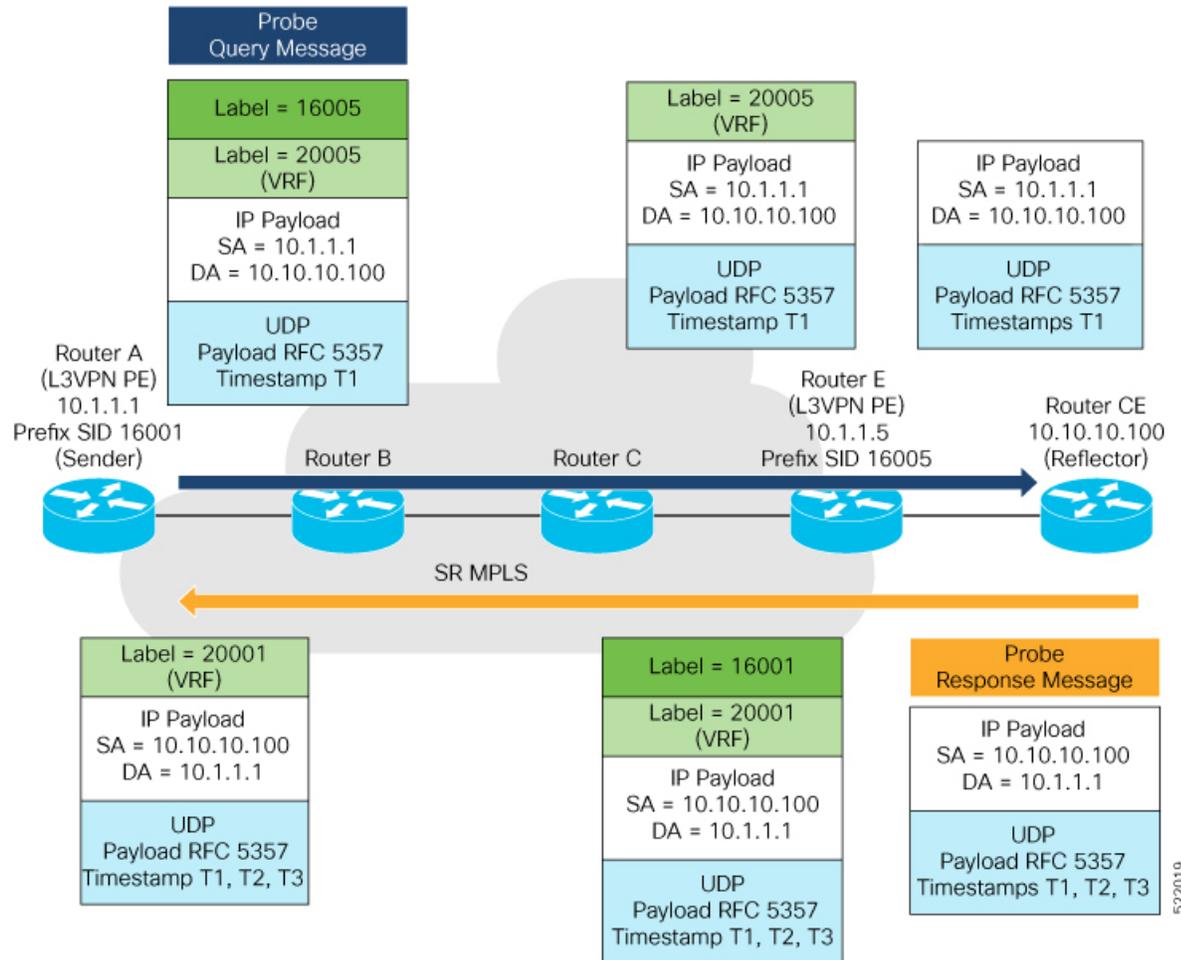
実用例 1：グローバルルーティングテーブルで到達可能な IP エンドポイントへの遅延測定プローブ

次の図は、グローバルルーティングテーブルで到達可能な IP エンドポイントに対する遅延測定プローブを示しています。送信者とリフレクタを相互接続するネットワークは、プレーン IP 接続を提供します。



ユースケース 2: ユーザー指定の VRF で到達可能な IP エンドポイントへの遅延測定プローブ

次の図は、ユーザー指定の L3VPN の VRF ルーティングテーブルで到達可能な IP エンドポイントに対する遅延測定プローブを示しています。L3VPN 入力 PE (ルータ A) は送信者として機能します。リフレクタは、L3VPN 出力 PE (ルータ E) の背後にある CE デバイスにあります。L3VPN PE を相互接続するネットワークは、セグメントルーティングとの MPLS 接続を提供します。



IP エンドポイントのパフォーマンス遅延測定の設定方法

使用上のガイドラインと制限事項

- プローブのエンドポイントは IP アドレスで指定されます。IPv4 および IPv6 エンドポイントアドレスがサポートされています。

- プローブのエンドポイントには、送信者が到達可能な任意の IP アドレスを指定できます。たとえば、オペレータのネットワーク内にある、または VRF を介して到達可能なローカルインターフェイス、リモートノードまたはホストなどです。
- エンドポイントの IP アドレスは、グローバルルーティングテーブルまたはユーザー指定の VRF ルーティングテーブルで見つけることができます。
- VRF 認識により、オペレータは次のシナリオでプローブを展開できます。
- 管理対象の顧客機器 (CE) のシナリオ：
 - PE to CE プローブ
 - CE to CE プローブ
- 管理対象外の顧客機器 (CE) のシナリオ：
 - PE to PE プローブ
 - PE to PE (PE-CE インターフェイスからの送信元) プローブ
- プローブの IPv6 エンドポイントとしての SRv6 ロケータプレフィックスおよび VRF SRv6 ロケータ/機能 (uDT4/uDT6) はサポートされていません。
- エンドポイントの IP アドレスには、IP パス、MPLS LSP、または IP トンネル (GRE) を介して到達できます。
- エンドポイントが MPLS LSP (SR、LDP、RSVP-TE、SR ポリシーなど) を使用して到達可能である場合、転送段階で対応する MPLS トランスポートラベルが適用されます。
- エンドポイントが MPLS ネットワーク内の VRF 経由で到達可能である場合、転送段階で対応する MPLS サービスラベルが適用されます。転送パスでは、送信者ノードはエンドポイントアドレスに設定された VRF を使用します。リターンパスでは、リフレクタノードは、プローブパケットを受信した着信 VRF ラベルに基づいて VRF を取得します。

パフォーマンス遅延測定を行う IP エンドポイントの設定

パフォーマンス遅延測定を行う IP エンドポイントを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **performance-measurement**
4. **endpoint *endpoint-name***
5. **vrf *vrf-name***
6. **source-address ipv4 *source_ip_address***
7. **destination-address ipv4 *destination_ip_address***
8. **delay-measurement**

9. profile *profile-name*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	configureterminal 例： Router# 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	performance-measurement 例： RouterA(config)# performance-measurement	パフォーマンス遅延測定モードを開始します。
ステップ 4	endpoint <i>endpoint-name</i> 例： RouterA(config-perf-meas)# endpoint test-ipv4-1	IP エンドポイントの名前を指定します。
ステップ 5	vrf <i>vrf-name</i> 例： RouterA(config-pm-ep)# vrf VPN-1	VRF インスタンスの名前を指定します。
ステップ 6	source-address ipv4 <i>source_ip_address</i> 例： RouterA(config-pm-ep)# source-address ipv4 1.1.1.1	送信元 IP アドレスを指定します。
ステップ 7	destination-address ipv4 <i>destination_ip_address</i> 例： RouterA(config-pm-ep)# destination-address ipv4 1.1.1.4	宛先 IP アドレスを指定します。
ステップ 8	delay-measurement 例： RouterA(config-pm-ep)#delay-measurement	IP エンドポイントで遅延測定を有効にします。
ステップ 9	profile <i>profile-name</i> 例： RouterA(config-pm-ep-dm)#profile test-profile	プロファイル名を指定します。

IP エンドポイントのパフォーマンス遅延測定プロファイルの設定

IP エンドポイントのパフォーマンス遅延測定プロファイルを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **performance-measurement**
4. **delay-profile endpoint name** *endpoint-name*
5. **probe**
6. **measurement-mode** {**one-way** | **two-way**}
7. **computation-interval** *seconds*
8. **burst-interval** *milliseconds*
9. **padding-size** *size*
10. **tos-dscp** *value*
11. **exit**
12. **liveness-detection**
13. **multiplier** *value*
14. **exit**
15. **advertisement**
16. **threshold-check** {**average-delay** | **maximum-delay** | **minimum-delay**}
17. **exit**
18. **periodic** {**disabled** | **interval** *seconds* | **minimum-change** *microseconds* | **threshold** *value*}
19. **exit**
20. **accelerated** {**minimum-change** *microseconds* | **threshold** *value*}
21. **exit**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	configureterminal 例： Router# 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	performance-measurement 例：	パフォーマンス遅延測定モードを開始します。

IP エンドポイントのパフォーマンス遅延測定プロファイルの設定

	コマンドまたはアクション	目的
	RouterA(config)# performance-measurement	
ステップ 4	delay-profile endpoint name <i>endpoint-name</i> 例： RouterA(config-perf-meas)#delay-profile endpoint name test-profile	関連付ける遅延プロファイル名を指定します。
ステップ 5	probe 例： RouterA(config-pm-dm-ep)#probe	プローブ コンフィギュレーション モードに入ります。
ステップ 6	measurement-mode { one-way two-way } 例： RouterA(config-pm-dm-ep-probe)# measurement-mode two-way	間隔測定モードを指定します。デフォルト値は双方向測定モードです。
ステップ 7	computation-interval <i>seconds</i> 例： RouterA(config-pm-dm-ep-probe)# computation-interval 60	メトリック計算の間隔を指定します。有効な範囲は 1 ~ 3600 秒です。デフォルト値は 30 秒です。
ステップ 8	burst-interval <i>milliseconds</i> 例： RouterA(config-pm-dm-ep-probe)#burst-interval 3000	プローブパケットを送信する間隔を指定します。指定できる範囲は 30 ~ 15000 ミリ秒です。デフォルト値は 3000 ミリ秒です。
ステップ 9	padding-size <i>size</i> 例： RouterA(config-pm-dm-ep-probe)#padding-size 0	パケットパディングサイズを指定します。範囲は 0 ~ 8000 です。 (注) 1500 を超えるパディングサイズを設定することは推奨されません。パディングサイズを大きくすると、フラグメンテーションとリアセンブルが発生し、システムパフォーマンスと IP エンドポイント PM 遅延の精度に影響を与える可能性があります。
ステップ 10	tos-dscp <i>value</i> 例： RouterA(config-pm-dm-ep-probe)# tos-dscp 48	タイプオブサービス DSCP を指定します。指定できる範囲は 0 ~ 63 です。デフォルト値は IP/UDP で DSCP 48 です。
ステップ 11	exit 例： RouterA(config-pm-dm-ep-probe)#exit	プローブ コンフィギュレーション モードを終了します。

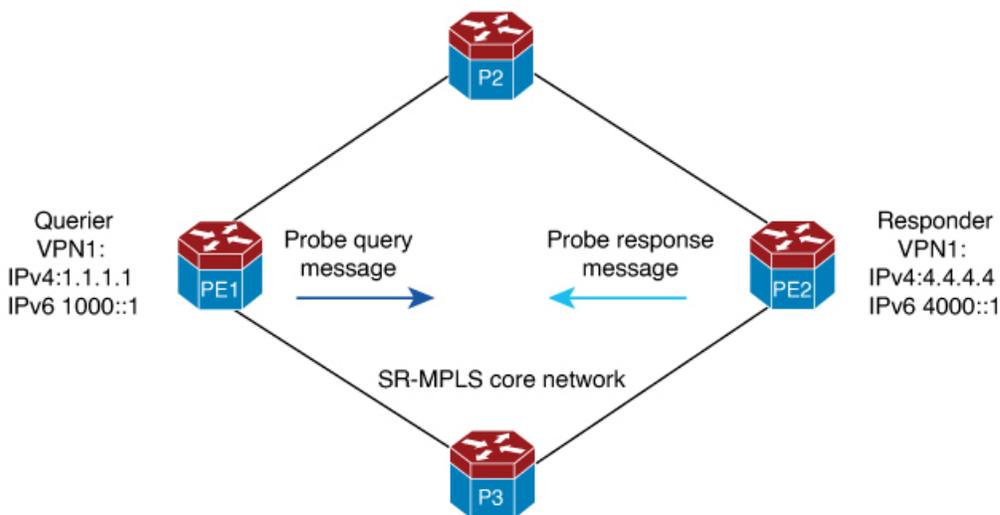
	コマンドまたはアクション	目的
ステップ 12	liveness-detection 例： RouterA(config-pm-dm-ep)#liveness-detection	エンドポイント活性検出コンフィギュレーションモードを開始します。
ステップ 13	multiplier value 例： RouterA(config-pm-dm-ep-live)#multiplier 3	ヘッドエンドノードがエンドポイントの活性セッション状態がダウンであると見なす前に送信される、プローブパケットの数を指定します。範囲は2～10です。
ステップ 14	exit 例： RouterA(config-pm-dm-ep-live)#exit	エンドポイント活性検出コンフィギュレーションモードを終了します。
ステップ 15	advertisement 例： RouterA(config-pm-dm-ep)#advertisement	アドバタイズメント コンフィギュレーション モードに入ります。
ステップ 16	threshold-check {average-delay maximum-delay minimum-delay} 例： RouterA(config-pm-dm-ep-adv)#threshold-check maximum-delay	しきい値チェックアドバタイズメントコンフィギュレーションモードを開始します。高速アドバタイズメントのしきい値超過の遅延メトリック変更値を確認します。デフォルト値は average-delay です。
ステップ 17	exit 例： RouterA(config-pm-dm-ep-adv-threshold-check)#exit	しきい値チェックアドバタイズメントコンフィギュレーションモードを終了します。
ステップ 18	periodic {disabled interval seconds minimum-change microseconds threshold value} 例： RouterA(config-pm-dm-ep-adv)# periodic interval 120	定期アドバタイズメント コンフィギュレーションモードを開始します。 disabled ：定期的なアドバタイズメントを無効にします。 interval ：定期的なアドバタイズメントとメトリックの集約間隔。範囲は30～3600秒です。デフォルト値は120秒です。 minimum-change ：定期的なアドバタイズメントの最小変更値。指定できる範囲は0～1000000マイクロ秒です。デフォルト値は500マイクロ秒です。 threshold ：定期的なアドバタイズメントのしきい値超過の最小遅延メトリック変更値を指定します。有効値は0～100パーセントです。デフォルト値は10%です。

	コマンドまたはアクション	目的
		(注) 最小変更値としきい値の両方を超えた場合に、アダプタイズメントが発生します。
ステップ 19	exit 例： RouterA(config-pm-dm-ep-adv-per) #exit	定期アダプタイズメント コンフィギュレーション モードを終了します。
ステップ 20	accelerated {minimum-change <i>microseconds</i> threshold <i>value</i>} 例： RouterA(config-pm-dm-ep-adv) #accelerated minimum-change 1000	高速アダプタイズメント コンフィギュレーション モードを開始します。 minimum-change : 定期的なアダプタイズメントの最小変更値。指定できる範囲は1～1000000 マイクロ秒です。デフォルト値は 500 マイクロ秒です。 threshold : 定期的なアダプタイズメントのしきい値超過の最小遅延メトリック変更値を指定します。有効値は0～100 パーセントです。デフォルト値は 20 パーセントです。
ステップ 21	exit 例： RouterA(config-pm-dm-ep-adv-acc) #exit	高速アダプタイズメント コンフィギュレーション モードを終了します。

IP エンドポイントのパフォーマンス遅延測定の設定例

次に、IP エンドポイントのパフォーマンス遅延測定の設定例を示します。

設定例：IP エンドポイントのパフォーマンス遅延測定の設定（グローバル コンフィギュレーション）



実行コンフィギュレーション

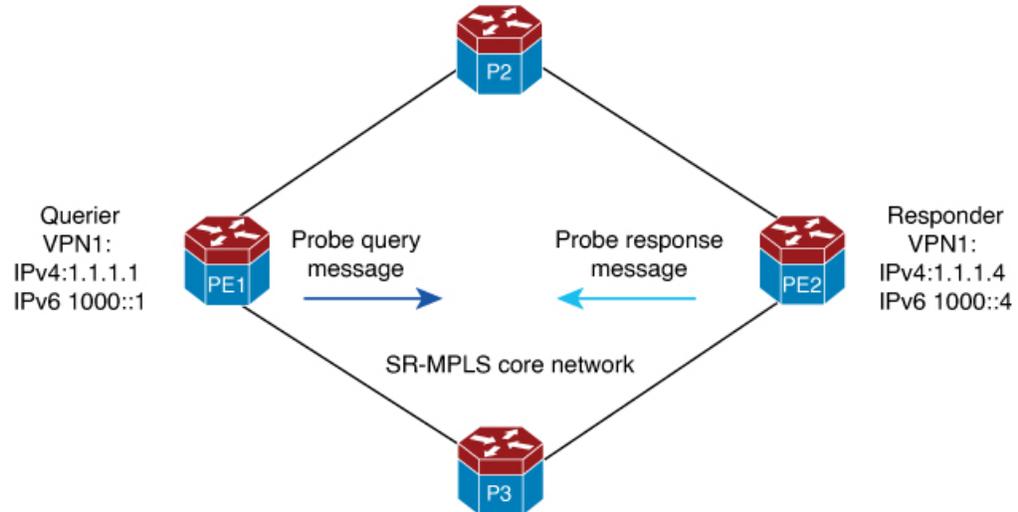
クエリア（送信者）の設定：

```
performance-measurement
delay-profile endpoint name test-profile
probe
burst-interval 95
tos-dscp 24
!
endpoint test-ipv4-1
source-address ipv4 1.1.1.1
destination-address ipv4 4.4.4.4
delay-measurement
profile test-profile
performance-measurement
!
endpoint test-ipv6-1
source-address ipv6 1000::1
destination-address ipv6 4000::1
delay-measurement
profile test-profile
```

クエリア（送信者）の設定：

```
performance-measurement
```

設定例：IP エンドポイントのパフォーマンス遅延測定の設定（VRF 設定）



実行コンフィギュレーション

クエリア（送信者）の設定：

```
performance-measurement
delay-profile endpoint name test-profile
probe
burst-interval 95
tos-dscp 24
!
endpoint test-ipv4-1
vrf VPN-1
source-address ipv4 1.1.1.1
destination-address ipv4 1.1.1.4
delay-measurement
profile test-profile
!
performance-measurement
!
endpoint test-ipv6-1
vrf VPN-1
source-address ipv6 1000::1
destination-address ipv6 1000::4
delay-measurement
profile test-profile
```

クエリア（送信者）の設定：

```
performance-measurement
```

IP エンドポイントのパフォーマンス遅延測定の検証

次の show コマンドを使用して、IP エンドポイントのパフォーマンス遅延測定を確認できます。

- **show performance-measurement counters endpoint filter name pm-name detail**
- **show performance-measurement endpoint filter name pm-name detail**
- **show performance-measurement history endpoint adv**
- **show performance-measurement history endpoint aggr**
- **show performance-measurement history endpoint filter name liveness-notification**
- **show performance-measurement history endpoint filter name pm-name adv**
- **show performance-measurement history endpoint filter name pm-name aggr**
- **show performance-measurement history endpoint filter name probe**
- **show performance-measurement profile endpoint**
- **show performance-measurement responder counters interface**
- **show performance-measurement responder summary**
- **show performance-measurement summary**

例

次に、IP エンドポイントのパフォーマンス遅延測定を確認するための show コマンドの出力例を示します。

show performance-measurement summary

```
pel#show performance-measurement summary
Total interfaces : 1
Total SR Policies : 0
Total endpoints : 250
Maximum PPS : 2000 pkts/sec
Dual-color gre bit-position : 9
Endpoint Delay-Measurement:
  Total sessions : 250
  Counters:
    Packets:
      Total sent : 12816719
      Total received : 11443853
    Errors:
      Total sent errors : 0
      Total received errors : 172421
  Probes:
    Total started : 40959
    Total completed : 35208
    Total incomplete : 5751
    Total advertisements : 33
```

show performance-measurement profile

```
pel#show performance-measurement profile endpoint name test-profile
test-profile Endpoint Delay Measurement:
  Profile configuration:
    Measurement Type : Two-Way
    Computation interval : 30 (effective : 30) seconds
```

show performance-measurement endpoint session

```

Burst interval : 95 mSec
Burst count : 316
Protocol : TWAMP-Lite Unauth
ToS DSCP value : 48
Destination sweeping mode : Disabled
Periodic advertisement : Enabled
    Interval : 120 (effective: 120) sec
    Threshold : 10%
    Minimum-Change : 500 uSec
Accelerated advertisement : Disabled
Threshold crossing check : Average-delay
Liveness-detection multiplier : 3

```

show performance-measurement endpoint session

```

PE#show performance-measurement endpoint filter name test-ipv6-2000 detail
Endpoint name: test-ipv6-2000
Source address          : 1412::1
Destination address     : 1412::4
Delay Measurement      : Enabled
VRF                    : Not configured
Profile name           : test-profile
Forward SID List       : Not configured
Reverse SID List       : Not configured

Delay Measurement session:
Session ID              : 6
Profile name            : test-profile

Last advertisement:
Advertised at: 15:00:52 11-01 2023 (30 seconds ago)
Advertised reason: Periodic timer, avg delay threshold crossed
Advertised anomaly: INACTIVE
Advertised delays (uSec): avg: 4265, min: 2902, max: 5999, variance: 986

Next advertisement:
Check scheduled in 3 more probes (roughly every 120 seconds)
No probes completed
Rolling average (uSec): 4378

Current Probe:
Started at 15:00:52 11-01 2023 (30 seconds ago)
Packets Sent: 311, received: 311
Measured delays (uSec): avg: 5004, min: 4010, max: 5977, variance: 994
Probe samples:
  Packet Rx Timestamp      Measured Delay (nsec)
  15:01:23 11-01 2023      5093944
  15:01:23 11-01 2023      5092502
  15:01:23 11-01 2023      5110069
  15:01:23 11-01 2023      5365350
  15:01:23 11-01 2023      5365940
Next probe scheduled at 15:01:22 11-01 2023 (in 0 seconds)
Burst completed

Liveness Detection:
Session Creation Timestamp: 11-01 14:50:29.937
Session State: Up
Last State Change Timestamp: 11-01 14:51:56.110
Missed count [consecutive]: 0
Received count [consecutive]: 5691
Backoff : 0
Unique Path Name : Path-6
Loss in Last Interval : 0 % [TX: 313 RX: 313]

```

show performance-measurement counters endpoint

```

pel#show performance-measurement counters endpoint filter name test-ipv6-100 detail
Endpoint name: test-ipv6-100
Source address : 1000::100
Destination address : 6000::100
Delay Measurement : Enabled
VRF : Not configured
Profile name : test-profile
Forward SID List : Not configured
Reverse SID List : Not configured
Delay-Measurement:
  Packets:
    Total sent : 771804
    Total received : 741831
  Errors:
    TX:
      Total interface down : 0
      Total no MPLS caps : 0
      Total no IP address : 0
      Total other : 0
    RX:
      Total negative delay : 1762
      Total delay threshold exceeded : 0
      Total missing TX timestamp : 0
      Total missing RX timestamp : 0
      Total probe full : 0
      Total probe not started : 1
      Total control code error : 0
      Total control code notif : 0
  Probes:
    Total started : 2487
    Total completed : 2358
    Total incomplete : 128
    Total advertisements : 1

```

show performance-measurement history endpoint

```

pel#show performance-measurement history endpoint filter name test-ipv6-100 probe
Endpoint name: test-ipv6-100
Source address : 1000::100
Destination address : 6000::100
Delay Measurement : Enabled
VRF : Not configured
Profile name : test-profile
Forward SID List : Not configured
Reverse SID List : Not configured
Delay-Measurement history (uSec):

```

Probe Start Timestamp	Pkt (TX/RX)	Average	Min	Max
03:52:25 01-18 2024	313/313	30	16	314
03:51:54 01-18 2024	313/313	29	13	47
03:51:22 01-18 2024	313/313	30	15	349
03:38:16 01-18 2024	10/10	42	29	101
<snip>				
03:37:46 01-18 2024	10/10	37	28	45
03:37:16 01-18 2024	10/10	37	29	47
03:36:46 01-18 2024	10/10	38	31	46
03:36:16 01-18 2024	10/10	39	28	48

IP エンドポイントの遅延測定および活性モニタリングの機能情報

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 38: IP エンドポイントの遅延測定および活性モニタリングの機能情報

機能名	リリース	機能情報
IP エンドポイントの遅延測定 および活性モニタリング	IOS XE 17.14.1a	<p>この機能を使用すると、エンドツーエンドの遅延を測定し、指定した IPv4 または IPv6 エンドポイントのいずれかに対する活性をモニターできます。</p> <p>この機能は、次のプラットフォームに導入されています。</p> <ul style="list-style-type: none"> • Cisco Catalyst 8500 シリーズ エッジプラットフォーム • Cisco Catalyst 8200 シリーズ エッジプラットフォーム • Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ • Cisco Catalyst 8000V Edge ソフトウェア <p>Cisco IOS XE 17.14.1a 以降では、performance-measurement endpoint および performance-measurement delay-profile endpoint コマンドを使用してこの機能を設定できます。</p>



第 31 章

SR-TE フロー別（クラス）ODN と自動化されたステアリング（PCE 委任）

この章では、セグメントルーティングトラフィックエンジニアリング（SR-TE）がフロー別ポリシー（PFP）のオンデマンドネクストホップ（ODN）および自動ステアリング（フロー別 ODN/AS）メカニズムと連携する仕組みについて説明します。この章は、次の項で構成されています。

- [SR-TE フロー別（クラス）ODN と自動化されたステアリング（PCE 委任）に関する機能情報（328 ページ）](#)
- [SR-TE フロー別（クラス）ODN と自動化されたステアリング（PCE 委任）に関する情報（330 ページ）](#)
- [BGP カラー拡張コミュニティと VRF プレフィックスのカラーリング（331 ページ）](#)
- [RIB パスによる PFP のサポート, on page 334](#)
- [SR-TE フロー別クラス（ODN）と自動化されたステアリング（PCE 委任）の設定（335 ページ）](#)
- [SR-TE フロー別クラス（ODN）と自動化されたステアリング（PCE 委任）の確認（337 ページ）](#)

SR-TE フロー別（クラス）ODN と自動化されたステアリング（PCE 委任）に関する機能情報

表 39: 機能の履歴

機能名	リリース	説明
RIB パスによる PFP のサポート	Cisco IOS XE 17.9.1a	この機能により、ルーティング情報ベース（RIB）パスオプションを使用して、フローごとのポリシーで転送クラスを設定できます。宛先ごとのポリシーを設定する代わりに、RIB オプションはポリシーの宛先への IGP 最短パスを使用します。

機能名	リリース	説明
BGP VRF への拡張カラーコミュニティのアタッチ	Cisco IOS XE 17.7.1a Cisco IOS XE 17.11.1a	<p>この機能は、拡張カラーコミュニティをプレフィックスにアタッチする新しい方法を導入します。カラーコミュニティは、プレフィックスに送信されるトラフィックの帯域幅または遅延レベルのインジケータです。それらをプレフィックスにアタッチする新しい方法は次のとおりです。</p> <ul style="list-style-type: none"> • VRF エクスポートのカラーリング • VRF インポートのカラーリング • BGP でのルート再配布のカラーリング • ネイバー着信のカラーリング <p>Cisco IOS XE 17.11.1a 以降、この機能は次のプラットフォームに拡張されています。</p> <ul style="list-style-type: none"> • Cisco Catalyst 8300 シリーズエッジプラットフォーム • Cisco Catalyst 8500 シリーズエッジプラットフォーム • Cisco Catalyst 8000V Edge ソフトウェア
SR-TE フロー別（クラス）ODN と自動化されたステアリング（PCE 委任）	Cisco IOS XE Amsterdam 17.4	<p>この機能を使用すると、パケットの QoS マーキングに基づき SR-TE PFP を使用してトラフィックをステアリングできます。トラフィックはその後、パケットの転送クラスに基づいて適切なパスにスイッチされます。</p>

SR-TE フロー別（クラス）ODN と自動化されたステアリング（PCE 委任）に関する情報

自動ステアリング（フロー別 ODN/AS）によるセグメントルーティングトラフィックエンジニアリング（SR-TE）フロー別ポリシー（PFP）オンデマンドネクストホップ（ODN）は、パケットの属性に基づくセグメントルーティングポリシーでのトラフィックのステアリングを可能にするメカニズムです。自動ステアリング（フロー別 ODN/AS）による SR-TE PFP ODN は、パケットの属性に基づく SR ポリシーでのトラフィックのステアリングを可能にするメカニズムです。パケットはシスコのモジュラ QoS CLI（MQC）フレームワークを使用して分類され、転送クラス（FC）と呼ばれる内部タグを使用してマークされます。PFP はその後、FC とそれに対応するパス間のマッピングに基づく、マークされたパケットのルーティングに使用されます。これは、トラフィックがその QoS マーキングに基づいてステアリングされ、パケットの FC に基づいて適切なパスにスイッチされることを意味します。

PFP は <color, endpoint> によって識別されます。これは、最大 8 つのエントリを含むフロー別転送クラステーブルで設定され、各エントリは FC によってインデックスが付けられ、宛先別ポリシー（PDP）を指し示します。



（注） サポートされる機能は次のとおりです。

- 250 PFP+PDP（組み合わせ）
- 6 PE および 6 VPE
- 10k VPNV4 プレフィックス制限
- SR PFP の L3VPN Inter AS オプション B
- PFP を介した IPv6

SR-TE フロー別（クラス）ODN と自動化されたステアリング（PCE 委任）に関する制約事項

- Quality of Service（QoS）ポリシーの動的変更はサポートされていません。
- SR-TE トンネルの PIC エッジを介した PIC コアはサポートされていません。
- SR-TE を介した VPLS はサポートされていません。
- 設定転送クラスを 0 に設定して、非転送クラスのデフォルトパスを取得します。
- BGP ラベル付きユニキャスト（BGP-LU）（RFC 3107）は、SR ODN PFP 自動ステアリングではサポートされていません。

- PFP トンネルを介した L2VPN はサポートされていません。
- PFP を介したパフォーマンス測定はサポートされていません。
- PFP を介した MPLS の Ping または Traceroute はサポートされていません。
- PFP または PDP を介した自動ルート通知はサポートされていません。
- PIC は PFP ではサポートされていません。

BGP カラー拡張コミュニティと VRF プレフィックスのカラーリング

セグメントルーティングトラフィックエンジニアリングメカニズムでは、SR-TE ルーティングパスを必要とするプレフィックスは、カラー拡張コミュニティ（プレフィックスにカラーを割り当てる属性）に関連付けられます。BGPには現在、neighbor コマンドのルートマップアウトバウンド設定のみに基づいてカラー拡張コミュニティをアタッチする機能があります。送信元 VRF、宛先 VRF、CE ネイバー、送信元プロトコルなどの属性に基づいてプレフィックスをカラーリングするために、カラーをアタッチする次のような方法が導入されています。

- VRF エクスポートのカラーリング
- VRF インポートのカラーリング
- BGP へのルート再配布カラーリング
- ネイバー インバウンド カラーリング

さらに、17.7.1a より前の Cisco IOS XE リリースでは、プレフィックスにアタッチされた新しいカラー拡張コミュニティが、プレフィックスで使用可能な既存のカラー拡張コミュニティを置き換えます。置き換えるのではなく、新しいカラー拡張コミュニティをカラー拡張コミュニティの既存のリストに追加できるように、Cisco IOS XE 17.7.1a の一部としてキーワード **additive** が **route-map** コマンドに追加されています。

```
route-map SRTE-color-map permit  
set extcommunity color < 1-4294967295> [additive]
```



- (注) 複数のカラー拡張コミュニティを含む BGP アップデートを受信すると、リスト内の最高のカラー値が SR ポリシーの作成に使用され、その SR ポリシーに対応するバインディング SID が、受信した BGP パスのルーティングパスとして使用されます。最高のカラーに対応する SR ポリシーが使用できない場合、BGP はアップデートのルーティングパスとしてインターフェイスを使用します。

サポートされるプラットフォーム

Cisco IOS XE 17.7.1a 以降、この機能は下記でサポートされます。

- Cisco ASR 1000 シリーズ プラットフォーム

Cisco IOS XE 17.11.1a 以降、この機能は下記でサポートされます。

- Cisco Catalyst 8300 シリーズ エッジ プラットフォーム
- Cisco Catalyst 8500 シリーズ エッジ プラットフォーム
- Cisco Catalyst 8000V Edge ソフトウェア

カラー拡張コミュニティのタッチ

カラー拡張コミュニティをタッチするには、次の方法を使用できます。

- **VRF エクスポートカラーリング**：次の設定では、VRF に関連付けられたエクスポートルートマップのカラー拡張コミュニティにしたがって、カラー拡張コミュニティを VPN プレフィックスにタッチします。これにより、VPN プレフィックスの送信元 VRF に基づいてカラー拡張コミュニティの関連付けができます。

```
route-map SRTE-color-map permit
set extcommunity color < 1-4294967295> [additive]
vrf def SRTE-VRF
rd 1:1
!
address-family ipv4
export map SRTE-color-map
exit-address-family
!
address-family ipv6
export map SRTE-color-map
exit-address-family
```

- **VRF インポートカラーリング**：次の設定では、VRF に関連付けられたインポートルートマップのカラー拡張コミュニティにしたがって、カラー拡張コミュニティをインポートされた VRF プレフィックスにタッチします。これにより、プレフィックスがインポートされる VRF に基づいて、カラー拡張コミュニティをプレフィックスにタッチできます。

```
route-map SRTE-color-map permit
set extcommunity color < 1-4294967295> [additive]
vrf def SRTE-VRF
rd 1:1
!
address-family ipv4
import map SRTE-color-map
exit-address-family
!
address-family ipv6
import map SRTE-color-map
exit-address-family
```

- **BGP へのルート再配布カラーリング**：次の設定では、再配布ルートの一部としてカラー拡張コミュニティを BGP にタッチします。これにより、プレフィックスを所有する送信

元プロトコルに基づいて、カラー拡張コミュニティがプレフィックスに関連付けられます。

```
route-map SRTE-color-map permit
set extcommunity color < 1-4294967295> [additive]
router bgp <ASnum>
address-family ipv4
redistribute <source-protocol> route-map SRTE-color-map
or
network <address> mask <network-mask> route-map SRTE-color-map
exit-address-family
!
address-family ipv4 vrf <vrf-name>
redistribute <source-protocol> route-map SRTE-color-map
or
network <address> mask <network-mask> route-map SRTE-color-map
exit-address-family
!
address-family ipv6
redistribute <source-protocol> route-map SRTE-color-map
or
network <address>/masklen route-map SRTE-color-map
exit-address-family
!
address-family ipv6 vrf <vrf-name>
redistribute <source-protocol=> route-map SRTE-color-map
or
network <address>/masklen route-map SRTE-color-map
exit-address-family
```

- **ネイバー インバウンド カラーリング** : 次の設定では、ネイバーにアタッチされているインバウンドルートマップ処理の一部として、カラー拡張コミュニティをアタッチします。これにより、プレフィックスをアドバタイズするネイバーに基づいてカラー拡張コミュニティがアタッチされます。

```
route-map SRTE-color-map permit
set extcommunity color < 1-4294967295> [additive]
router bgp <ASnum>
address-family ipv4
neighbor <address> route-map SRTE-color-map in
exit-address-family
!
address-family vpv4
neighbor <address> route-map SRTE-color-map in
exit-address-family
!
address-family ipv4 vrf <vrf-name>
neighbor <address> route-map SRTE-color-map in
exit-address-family
!
address-family ipv6
neighbor <address> route-map SRTE-color-map in
exit-address-family
!
address-family vpv6
neighbor <address> route-map SRTE-color-map in
exit-address-family
!
address-family ipv6 vrf <vrf-name>
neighbor <address> route-map SRTE-color-map in
exit-address-family
```

RIB パスによる PFP のサポート

PFP はバンドル出力チェーン要素（OCE）で構成され、バンドル OCE の各ハッシュは PDP ポリシー（PDP トンネル）で構成されます。このシナリオでは、デフォルトの IGP または RIB 学習パスに対して PDP ポリシーが作成されます。つまり、デフォルトの IGP または RIB 学習パスごとに個別の PDP ポリシーが作成されます。したがって、この実装は最終的にポリシーの数を増やすものであり、拡張するものではありません。

Cisco IOS XE 17.9.1a 以降では、RIB パスオプションを使用して PFP で転送クラスを設定できます。PDP を設定する代わりに、RIB オプションはポリシー宛先への IGP 最短パスを使用します。

PFP には、PDP と同様のバインディング SID があります。トラフィックステアリングのメカニズムも PDP と同じで、BSID または RIB のいずれかを紹介します。

PFP は、次の条件に基づいて動作状態が UP になります。

- デフォルトの FC が PDP で設定されており、その動作状態が UP である。
- デフォルトの FC が RIB パスで設定され、解決されている。



Note デフォルト以外の FC の状態は、PFP の状態に影響しません。

パケットが PFP でステアリングされた後、入力時にモジュラ QoS CLI（MQC）によってマークされた FC に従って、次のシナリオはパケットのパスを示します。

- PFP が Down 状態の場合、パケットはドロップされます。
- パケットに FC がアタッチされていない場合、パケットは PFP のデフォルト FC を使用して転送されます。
- 解決された RIB パスまたは動作可能な PDP を指すパケットに FC がアタッチされている場合、パケットはそこに転送されます。
- パケットにアタッチされている FC が、存在しない未解決の RIB パスまたは動作していない PDP を指している場合、パケットはデフォルトの FC に転送されます。

例：RIB パスによる PFP の設定

次の例で、RIB パスとカラーの両方を使用して PFP を設定する方法を示します。

```
segment-routing traffic-eng
policy PERFLOW
color 10 end-point 1.1.1.1
binding-sid mpls 15001
candidate-path
preference 1
per-flow
```

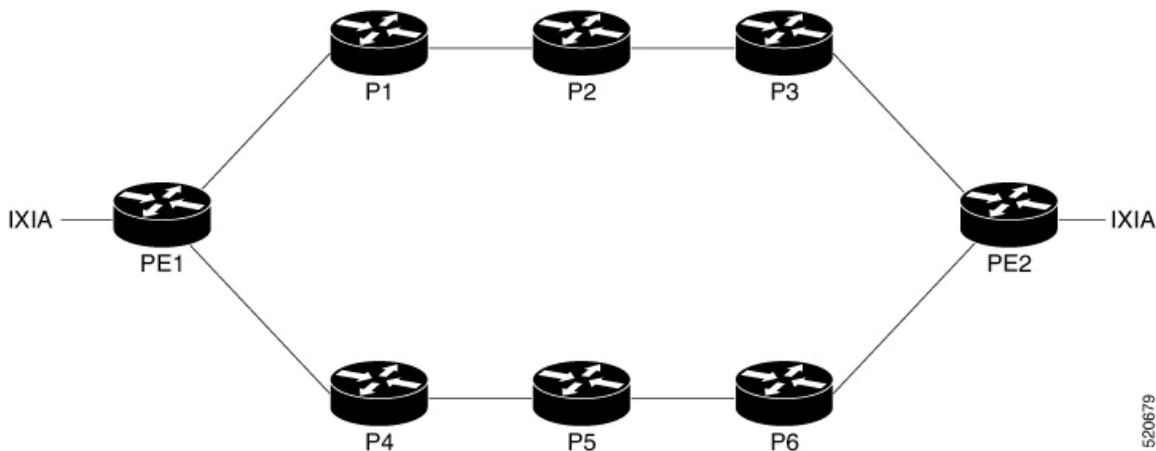
```
forward-class 0 rib
forward-class 1 color 20
forward-class 2 color 30
```

次の例で、RIB パスとカラーの両方を使用して ODN PFP を設定する方法を示します。

```
segment-routing traffic-eng
on-demand color 10
candidate-path
preference 1
per-flow
forward-class 0 rib
forward-class 1 color 20
forward-class 2 color 30
```

SR-TE フロー別クラス (ODN) と自動化されたステアリング (PCE 委任) の設定

次のトポロジを検討します。



PFP の ODN を設定するには、次の手順を実行します。

1. PE1 で QoS を設定します。

```
class-map DSCP
match DSCP AF41
```

- クラスマップで転送クラスを設定します。

```
policy-map per-flow
class DSCP
set forward-class 1
```

- 対応するインターフェイスにポリシーマップをアタッチします。

```
interface GigabitEthernet0/0/3
service-policy type epbr input PFP
```

2. PE1 で SR-TE PFP を設定します。

- PFP で転送クラスを設定します。

```
on-demand color 4500
  authorized
candidate-paths
  preference 2
  per-flow
    forward-class 0 color 100
    forward-class 0 rib
    forward-class 2 color 102
```

- セグメントリストを PDP にアタッチします。

```
policy perflow_pdp
color 100 end-point 10.5.5.5
candidate-paths
  preference 2
  explicit segment-list srtel weight 10
  !
constraints
  segments
    dataplane mpls
```

- セグメントリストを SR-TE に設定します。

```
segment-routing traffic-eng
  segment-list name srtel
    index 1 mpls label 16002
    index 2 mpls label 16005
```

3. PE2 で SR-TE PFP を設定します。

```
ip prefix-list pfp seq 5 permit 10.35.0.0/16 le 32
```

- ルートマップを PFP にアタッチします。

```
route-map pfp permit 10
  match ip address prefix-list pfp
  set extcommunity color 4500
```

- BGP ルートをアクティブにします。

```
router bgp 100
!
address-family vpnv4
  neighbor 10.1.1.1 activate
  neighbor 10.1.1.1 send-community extended
  neighbor 10.1.1.1 route-map pfp out
```

4. PFP の出力を表示します。

```
show segment-routing traffic-eng policy name *6.6.6.6|4090 detail

Name: *6.6.6.6|4090 (Color: 4090 End-point: 6.6.6.6)
Owners : BGP
Status:
Admin: up, Operational: up for 01:29:41 (since 06-21 14:09:05.510)
Candidate-paths:
Preference 1 (BGP):
Per-flow Information (active):
Forward PDP PDP BSID RW
Class Color Status Status
-----
0 rib n/a n/a
```

```

1 129 up Done
2 130 up Done
3 131 up Done
4 132 up Done
Default Forward Class: 0
Attributes:
Binding SID: 39
Allocation mode: dynamic
State: Programmed
IPv6 caps enabled
Tunnel ID: 65568 (Interface Handle: 0x26)
Per owner configs:
BGP
Binding SID: dynamic
Stats:
5 minute output rate 0 bits/sec, 0 packets/sec
Packets: 500524 Bytes: 88056352

Event history:
Timestamp Client Event type Context: Value
-----:-----:-----:-----:-----:-----
06-21 14:09:05.489 BGP Policy created Name: BGP
06-21 14:09:05.490 BGP Set colour Colour: 4090
06-21 14:09:05.490 BGP Set end point End-point: 6.6.6.6
06-21 14:09:05.490 BGP Set dynamic pce Path option: per flow
06-21 14:09:05.510 BGP BSID allocated FWD: label 39
06-21 14:09:05.510 FH Resolution Policy state UP Status: PFP RESOLVED CP: 1
06-21 14:09:05.551 FH Resolution REOPT triggered Status: REOPTIMIZED CP: 1
06-21 14:09:05.576 FH Resolution REOPT triggered Status: REOPTIMIZED CP: 1
06-21 14:09:05.602 FH Resolution REOPT triggered Status: REOPTIMIZED CP: 1
06-21 14:09:05.626 FH Resolution REOPT triggered Status: REOPTIMIZED CP: 1

```

SR-TE フロー別クラス (ODN) と自動化されたステアリング (PCE 委任) の確認

SR-TE フロー別クラス (ODN) と自動化されたステアリング (PCE 委任) を確認するには、次のコマンドを使用します。

```

show segment-routing traffic-eng policy name *10.5.5.5|4500

Name: *10.5.5.5|4500 (Color: 4500 End-point: 10.5.5.5)
Owners : BGP
Status:
Admin: up, Operational: up for 00:03:50 (since 09-07 16:07:02.938)
Candidate-paths:
Preference 2 (BGP):
Per-flow Information (active):
Forward PDP PDP BSID RW
Class Color Status Status
-----:-----:-----:-----:-----:-----
0 100 up Done
1 101 up unknown Pending
2 102 up unknown Pending
Default Forward Class: 0
Attributes:
Binding SID: 72
Allocation mode: dynamic
State: Programmed
IPv6 caps enabled

```

```
Tunnel ID: 65675 (Interface Handle: 0x2D)
Per owner configs:
BGP
Binding SID: dynamic
Stats:
5 minute output rate 0 bits/sec, 0 packets/sec
Packets: 9 Bytes: 584
```



第 32 章

複数の ISIS ドメインでの境界ルータのルー プバックプレフィックス SID のアドバタイ ズメント

境界ルータは、複数の ISIS ドメインの同じループバック インターフェイス プレフィックスおよび関連するプレフィックスセグメント識別子 (SID) をアドバタイズできます。

- [複数の ISIS ドメインでの境界ルータのループバックプレフィックス SID のアドバタイズメントに関する機能情報 \(339 ページ\)](#)
- [複数の ISIS ドメインでの境界ルータのループバックプレフィックス SID のアドバタイズメントに関する情報 \(340 ページ\)](#)
- [複数の ISIS ドメインでの境界ルータのループバックプレフィックス SID のアドバタイズメントの設定方法 \(341 ページ\)](#)
- [例：複数の ISIS ドメインでの BR のループバックプレフィックス SID の設定 \(342 ページ\)](#)

複数の ISIS ドメインでの境界ルータのループバックプレ フィックス SID のアドバタイズメントに関する機能情報

表 40: トラフィック エンジニアリングのパフォーマンス測定に関する機能情報

機能名	リリース	機能情報
複数の ISIS ドメインでの境界ルータのループバックプレフィックス SID のアドバタイズメント	Cisco IOS XE Amsterdam 17.3.2	境界ルータは、複数の ISIS ドメインのループバック インターフェイス プレフィックスおよび関連するプレフィックスセグメント識別子 (SID) をアドバタイズできます。このようなアドバタイズメントにより、関連付けられた各ドメイン内のルータは、同じプレフィックスとプレフィックス SID を使用して境界ルータと通信できます。

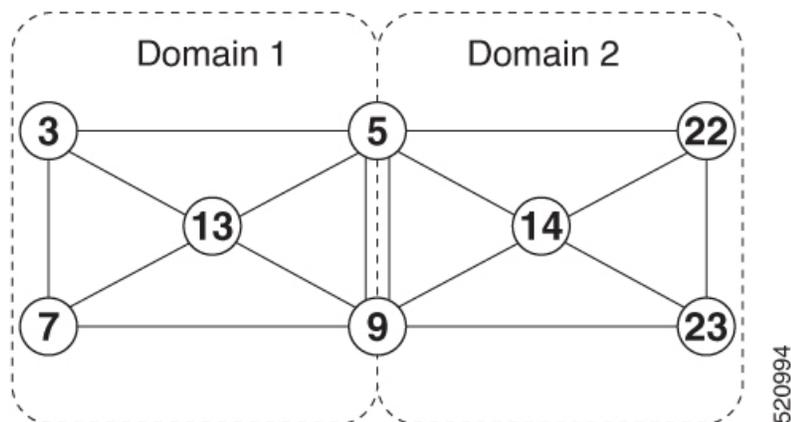
複数の ISIS ドメインでの境界ルータのループバックプレフィックス SID のアドバタイズメントに関する情報

複数の ISIS ドメインでの境界ルータのループバックプレフィックス SID のアドバタイズメントの概要

複数の ISIS ドメインを持つセグメントルーティング展開では、境界ルータが、関連付けられた各ドメインのループバック インターフェイス プレフィックスとプレフィックス SID をアドバタイズすると便利です。このようなアドバタイズメントにより、関連付けられた各ドメイン内のルータは、同じプレフィックスとプレフィックス SID を使用して境界ルータと通信できます。

この機能により、境界ルータは、プレフィックスとプレフィックス SID を複数の ISIS ルーティングプロセスにアドバタイズすることで、さらにそれを関連する各ドメインにアドバタイズできるようになります。

たとえば、次の図に示すトポロジでは、境界ルータであるルータ 5 とルータ 9 は、ドメイン 1 とドメイン 2 の両方でプレフィックスとプレフィックス SID をアドバタイズできます。ルータ 3 のようなドメイン 1 のルータとルータ 22 のようなドメイン 2 のルータは、同じプレフィックス SID を使用してトラフィックを送信し、いずれかの境界ルータにトラフィックを送信できます。



520994

複数の ISIS ドメインでの境界ルータのループバックプレフィックス SID のアドバタイズメントの設定方法

複数の ISIS ドメインでの境界ルータのループバックプレフィックス SID のアドバタイズメントの設定

複数の ISIS ドメインの境界ルータのループバックプレフィックスおよびプレフィックス SID をアドバタイズするには、境界ルータで、各ドメインの ISIS ルーティングプロセスに `passive-interface loopback-interface-name` コマンドを発行します。

```
router isis 1
  passive-interface loopback 0
router isis 2
  passive-interface loopback 0
```

複数の ISIS ドメインでの境界ルータのループバックプレフィックス SID のアドバタイズメントの確認

```
Router#show isis database verbose
```

```
Tag 1:
IS-IS Level-1 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime/Rcvd  ATT/P/OL
Router.00-00   * 0x00000013  0xDCD8       469/*              0/0/0
Area Address: 49.0001
NLPID:         0xCC
Router CAP:    10.0.0.0, D:0, S:0
Segment Routing: I:1 V:0, SRGB Base: 16000 Range: 8000
Segment Routing Local Block: SRLB Base: 15000 Range: 1000
Segment Routing Algorithms: SPF, Strict-SPF
Node-MSD
MSD: 16
Hostname: Router
Metric: 0      IP 10.2.2.2/32
Prefix-attr: X:0 R:0 N:0
Metric: 0      IP 10.1.1.1/32
Prefix-attr: X:0 R:0 N:0
Prefix-SID Index: 1, Algorithm:SPF, R:0 N:1 P:0 E:0 V:0 L:0
IS-IS Level-2 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime/Rcvd  ATT/P/OL
Router.00-00   * 0x00000014  0xDAD9       469/*              0/0/0
Area Address: 49.0001
NLPID:         0xCC
Router CAP:    10.0.0.0, D:0, S:0
Segment Routing: I:1 V:0, SRGB Base: 16000 Range: 8000
Segment Routing Local Block: SRLB Base: 15000 Range: 1000
Segment Routing Algorithms: SPF, Strict-SPF
Node-MSD
MSD: 16
Hostname: Router
Metric: 0      IP 10.2.2.2/32
Prefix-attr: X:0 R:0 N:0
```

例：複数の ISIS ドメインでの BR のループバックプレフィックス SID の設定

```

Metric: 0          IP 10.1.1.1/32
Prefix-attr: X:0 R:0 N:0
Prefix-SID Index: 1, Algorithm:SPF, R:0 N:1 P:0 E:0 V:0 L:0

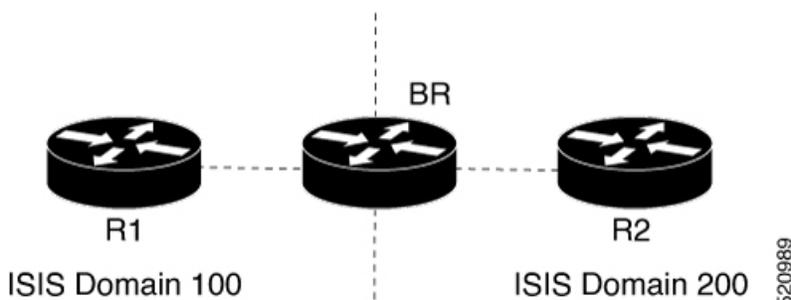
Tag 2:
IS-IS Level-1 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime/Rcvd  ATT/P/OL
Router.00-00   * 0x00000012  0xC68A        1179/*              0/0/0
Area Address: 39.0002
NLPID:         0xCC
Router CAP:    10.1.1.1, D:0, S:0
Segment Routing: I:1 V:0, SRGB Base: 16000 Range: 8000
Segment Routing Local Block: SRLB Base: 15000 Range: 1000
Segment Routing Algorithms: SPF, Strict-SPF
Node-MSD
MSD: 16
Hostname: Router
IP Address:    10.1.1.1
Metric: 0          IP 10.1.1.1/32
Prefix-attr: X:0 R:0 N:1
Prefix-SID Index: 1, Algorithm:SPF, R:0 N:1 P:0 E:0 V:0 L:0
IS-IS Level-2 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime/Rcvd  ATT/P/OL
Router.00-00   * 0x00000011  0xC889        1184/*              0/0/0
Area Address: 39.0002
NLPID:         0xCC
Router CAP:    10.1.1.1, D:0, S:0
Segment Routing: I:1 V:0, SRGB Base: 16000 Range: 8000
Segment Routing Local Block: SRLB Base: 15000 Range: 1000
Segment Routing Algorithms: SPF, Strict-SPF
Node-MSD
MSD: 16
Hostname: Router
IP Address:    10.1.1.1
Metric: 0          IP 10.1.1.1/32
Prefix-attr: X:0 R:0 N:1
Prefix-SID Index: 1, Algorithm:SPF, R:0 N:1 P:0 E:0 V:0 L:0

```

例：複数の ISIS ドメインでの BR のループバックプレフィックス SID の設定

次の例で、複数のドメインで BR およびプレフィックス SID の関連付けを設定する方法を示します。

2つの異なる ISIS ドメインにルータ R1 と R2 があり、両方のドメインに属する境界ルータ BR がある次のトポロジについて考えます。



デバイス	ループバック アドレス	プレフィックス SID
R1	10.1.1.1/32	101
R2	10.2.2.2/32	202
BR	10.3.3.3/32	303

境界ルータ BR で次の設定を行うと、ルータは、接続されている両方の ISIS ドメインのループバック インターフェイス アドレスおよび関連するプレフィックス SID をアドバタイズします。この設定例は、ループバック インターフェイスの定義、プレフィックス SID とループバック インターフェイスの関連付け、およびループバック インターフェイス アドレスのアドバタイズメントと、ISIS ドメインの ISIS 100 および ISIS 200 で関連付けられているプレフィックス SID を示しています。

```
BR>enable
BR#configure terminal
BR(config)#interface loopback 0
BR(config-if)#ip address 10.3.3.3 255.255.255.255
BR(config-if)#exit
BR(config)#segment-routing mpls
BR(config-srmppls)#connected-prefix-sid-map
BR(config-srmppls-conn)#address-family ipv4
BR(config-srmppls-conn-af)#10.3.3.3/32 index 303 range 1
BR(config-srmppls-conn-af)#exit-address-family
BR(config-srmppls-conn-af)#end
BR#configure terminal
BR(config)#router isis 100
BR(config-router)#passive-interface loopback 0
BR(config-router)#exit
BR(config)#router isis 200
BR(config-router)#passive-interface loopback 0
BR(config-router)#end
```

例：複数の ISIS ドメインでの BR のループバックプレフィックス SID の設定



第 33 章

無効なパスのドロップによるトラフィックステアリング

SR-TE ポリシーに有効なパスが定義されていない場合、パスはドロップされ、ポリシーを介してステアリングされているトラフィックはデフォルト（制約のない IGP）の転送パスにフォールバックします。また、ベストエフォート型トラフィックを伝送する SR-TE ポリシーに障害が発生すると、トラフィックは再ルーティングされ、プレミアムトラフィックの SLA（サービスレベル契約）に影響します。

SR-TE ポリシーの障害の問題を解決するために、データプレーンのトラフィックはドロップされますが、コントロールプレーンには保持されます。したがって、プレミアムトラフィックを伝送している可能性がある他のセグメントルーティングポリシーは影響を受けません。

- [無効なパスのドロップによるトラフィックステアリングに関する機能情報（345 ページ）](#)
- [無効なパスのドロップによるトラフィックステアリングの設定方法（347 ページ）](#)

無効なパスのドロップによるトラフィックステアリングに関する機能情報

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 41: トラフィック エンジニアリングのパフォーマンス測定に関する機能情報

機能名	リリース	機能情報
無効なパスのドロップによるトラフィックステアリング	Cisco IOS XE Bengaluru 17.5	SR-TE ポリシーに不具合があると、データプレーンのトラフィックはドロップされますが、コントロールプレーンに保持されます。したがって、プレミアムトラフィックを伝送する可能性のある他のセグメントルーティングポリシーは影響を受けません。

概要

SR-TE ポリシーに有効なパスが定義されていない場合、パスはドロップされ、ポリシーを介してステアリングされているトラフィックはデフォルト（制約のないIGP）の転送パスにフォールバックします。また、ベストエフォート型トラフィックを伝送する SR-TE ポリシーに障害が発生すると、トラフィックは再ルーティングされ、プレミアムトラフィックの SLA（サービレベル契約）に影響します。

SR-TE ポリシーの障害の問題を解決するために、データプレーンのトラフィックはドロップされますが、コントロールプレーンには保持されます。したがって、プレミアムトラフィックを伝送している可能性がある他のセグメントルーティングポリシーは影響を受けません。

この機能は、**path-invalidation drop** コマンドを使用して設定できます。

はじめる前に

セグメントルーティング BFD またはパフォーマンス活性モニタリングをすでに設定している場合は、この機能を有効にしないでください。この機能が有効になっている場合、セグメントルーティング BFD やパフォーマンス活性通知は無視されます。このようなシナリオでは、セグメントルーティング BFD またはパフォーマンス活性イベントのロギングや syslog 通知は生成されません。

SR-TE ポリシーが DOWN 状態でこの機能が設定されている場合、SR-TE ポリシーの状態は影響を受けないことに注意してください。

利点

- この機能を設定すると、プレミアムトラフィックをルーティングするように設定されている他のセグメントルーティングポリシーが影響を受けなくなり、その結果 SLA ガイドラインが影響を受けなくなります。

機能制限

- この機能は、セグメントルーティング BFD またはパフォーマンスモニタリング活性チェックと組み合わせて有効にすることはできません。

無効なパスのドロップによるトラフィックステアリングの設定方法

PCC プロファイルの設定

この設定により、PCE が開始したポリシーで、設定された値と一致するプロファイル ID でインスタンス化されたポリシーに対してパス無効化機能が有効になります。

```
segment-routing traffic-eng
  pcc
    profile <number >
      steering
        path-invalidation drop
```

静的ポリシーの設定

この設定により、セグメントルーティング静的ポリシーのパス検証ドロップが設定されます。

```
segment-routing traffic-eng
  policy <name>
    steering
      path-invalidation drop
```

SR-TE ポリシーのオンデマンドネクストホップの設定

この設定により、特定のカラーのオンデマンドセグメントルーティングポリシーの設定パス検証ドロップが発生します。

```
segment-routing traffic-eng
  on-demand color <>
    steering
      path-invalidation drop
```

コマンドの表示

パス無効化イベントのタイプおよび無効化ドロップのステータスを表示するには、**show segment-routing traffic-eng policy name** コマンドを使用します。

```
device#show segment-routing traffic-eng policy name foo detail
Name: foo (Color: 10 End-point: 192.168.0.8)
Owners : CLI
Status:
  Admin: up, Operational: up for 00:00:08 (since 09-17 10:19:54.536)
```

```

Candidate-paths:
  Preference 100 (CLI):
    Dynamic (active)
      Status: Invalidation drop
      Metric Type: TE
Attributes:
  Binding SID: 20
  Allocation mode: dynamic
  State: Programmed
  Autoroute:
    Include all
Tunnel ID: 65536 (Interface Handle: 0x9)
Per owner configs:
  CLI
  Binding SID: dynamic
Stats:
  5 minute output rate 0 bits/sec, 0 packets/sec
  Packets: 0 Bytes: 0

Event history:
  Timestamp          Client          Event type          Context: Value
  -----          -
  09-17 10:19:54.536 CLI             Policy created      Name: CLI
  09-17 10:19:54.537 CLI             Path Invalidation  Drop: Configured
  09-17 10:19:58.744 CLI             Set colour         Colour: 10
  09-17 10:19:58.744 CLI             Set end point      End-point:
192.168.0.8
  09-17 10:19:58.752 CLI             Set dynamic        Path option:
dynamic
  09-17 10:19:58.753 CLI             BSID allocated     FWD: label 20
  09-17 10:19:58.755 FH Resolution    Policy state UP     Status: PATH
RESOLVED CP: 100
  09-17 10:19:58.760 FH Resolution    REOPT triggered    Status: REOPTIMIZED
CP: 100
  09-17 10:19:58.780 CLI             Path Invalidation  Drop: Unconfigured

  09-17 10:19:59.537 CLI             Path Invalidation  Drop: Set
  09-17 10:20:00.853 FH Resolution    Path Invalidation  Status: Drop
  09-17 10:20:01.853 FH Resolution    Path Invalidation  Status: No Drop
  09-17 10:20:02.853 FH Resolution    Path Invalidation  Status: Drop

```



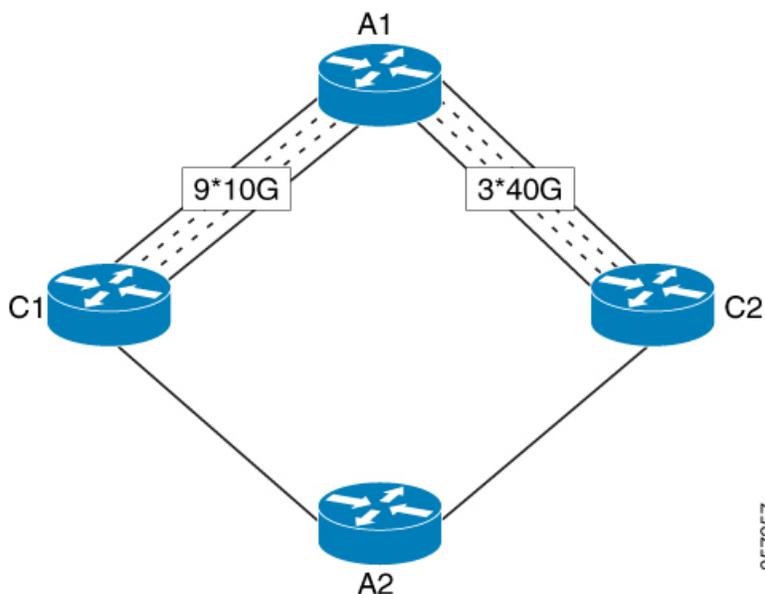
第 34 章

Cisco IS-IS ローカル不等コストマルチパス (UCMP) の設定

Cisco IOS XE ISIS ローカル UCMP 機能を使用すると、ネットワーク内の A1-C1 および A1-C2 からのすべてのリンク間で、A1 から A2 へのトラフィックのロードバランシングができます。すべてのリンクで同じメトリックを設定すると、等コストマルチパス (ECMP) パスが作成されます。ただし、高帯域幅リンクが低帯域幅リンクと同じトラフィックを伝送するため、高帯域幅リンクが十分に活用されません。この問題を回避するために、すべてのリンクで設定されたメトリックが同じであっても、帯域幅に基づいてリンク全体にトラフィックが均等に分散されるように、すべてのリンクを設定できます。

次の図で、トポロジについて説明します。

図 37: ローカル不等コストマルチパストポロジ



- 不等コストマルチパス (UCMP) ローカルの設定 (350 ページ)
- 不等コストマルチパス (UCMP) ローカルの確認 (350 ページ)

- [debug コマンド \(351 ページ\)](#)
- [セグメントルーティングに関する機能情報 : IS-IS UCMP \(351 ページ\)](#)

不等コストマルチパス (UCMP) ローカルの設定

ucmp local を設定するには、次のタスクを実行します。

```
router isis
 ucmp local [prefix-list <prefix-list-name>]
router isis
 address-family ipv6
 ucmp local [prefix-list <prefix-list-name>]
```

不等コストマルチパス (UCMP) ローカルの確認

この機能を確認するには、次の show コマンドを使用します。

- **show interface <name> counters**
- **show ip route**
- **show ipv6 route**
- **show ip cef**
- **show mpls forwarding-table labels detail**
- **show mpls infrastructure lfd lte**

例 : show コマンド

次に、不等コストマルチパス (UCMP) ローカルの show ip route の出力例を示します。

```
Device#show ip route 10.138.1.3
Routing entry for 10.138.1.0/24
Known via "isis", distance 115, metric 50, type level-1
Redistributing via isis Ring#1
Advertised by isis Ring#1 (self originated)
Last update from 10.148.1.1 on FortyGigabitEthernet0/5/1, 00:24:51
ago
Routing Descriptor Blocks:
* 10.198.1.1, from 10.1.1.1, 00:24:51 ago, via GigabitEthernet0/0/0
  Route metric is 50, traffic share count is 6
  10.148.1.1, from 10.1.1.1, 00:24:51 ago, via
  FortyGigabitEthernet0/5/1
  Route metric is 50, traffic share count is 25
```



(注) トラフィック共有数がインターフェイス帯域幅にしたがって計算されているかどうかを確認する必要があります。

次に、不等コストマルチパス (UCMP) ローカルの show interface counter の出力例を示します。

```
Device#show interface fo0/5/1 counters
Port      InOctets   InUcastPkts InMcastPkts InBcastPkts
Fo0/5/1   22883      0            17           0
Port      OutOctets   OutUcastPkts OutMcastPkts OutBcastPkts
Fo0/5/1   16242883   57513        17           0
PE12#show interface gi0/0/0 counters
Port      InOctets   InUcastPkts InMcastPkts InBcastPkts
Gi0/0/0   26388      26           19           0
Port      OutOctets   OutUcastPkts OutMcastPkts OutBcastPkts
Gi0/0/0   81944464   264216       195          0
```



(注) 計算されたトラフィック共有数にしたがって発信トラフィックが分割されているかどうかを確認できます。

debug コマンド

ローカル UCMP に関する問題をトラブルシュートするには、次のデバッグコマンドを使用します。

- `debug isis mfi`
- `debug ip routing detail`
- `debug ipv6 routing`

セグメントルーティングに関する機能情報 : IS-IS UCMP

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 トレー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、<https://cfng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

表 42: セグメントルーティングに関する機能情報 : IS-IS UCMP

機能名	リリース	機能情報
セグメントルーティング : IS-IS UCMP	Cisco IOS XE 17.5.1	セグメントルーティング : IS-IS UCMP 機能を使用すると、インターフェイスの帯域幅に比例して、すべての IGP ECMP パス間で発信トラフィックのロードバランシングを行うことができます。



第 35 章

セグメントルーティングフレキシブルアルゴリズムの有効化

セグメントルーティングフレキシブルアルゴリズムを使用すると、オペレータは、独自のニーズに応じてIGP最短パス計算をカスタマイズできます。オペレータは、リンクコストベースのSPFよりも優れた転送を実現するために、カスタムのSRプレフィックスSIDを割り当てることができます。結果として、フレキシブルアルゴリズムにより、IGPから到達可能なあらゆる宛先へのトラフィックエンジニアリングに基づくパスをIGPで自動的に計算できます。

SRアーキテクチャでは、パスの計算方法を定義するアルゴリズムにプレフィックスSIDが関連付けられます。フレキシブルアルゴリズムにより、ユーザーが定義したメトリックタイプと制約の組み合わせに基づいてIGPでパスを計算する、ユーザー定義のアルゴリズムを実現できます。

- [機能の履歴 \(354 ページ\)](#)
- [フレキシブルアルゴリズムの前提条件 \(355 ページ\)](#)
- [フレキシブルアルゴリズムに関する制約事項 \(356 ページ\)](#)
- [セグメントルーティングフレキシブルアルゴリズムの構成要素 \(356 ページ\)](#)
- [フレキシブルアルゴリズムのプレフィックスSIDの再配布, on page 358](#)
- [フレキシブルアルゴリズムのプレフィックスメトリックアドバタイズメント \(359 ページ\)](#)
- [フレキシブルアルゴリズムの設定 \(360 ページ\)](#)
- [フレキシブルアルゴリズムの設定の確認 \(367 ページ\)](#)

機能の履歴

表 43: 機能の履歴

機能名	リリース情報	機能説明
IS-IS フレキシブルアルゴリズムの TE メトリックサポート	Cisco IOS XE Dublin 17.11.1a	フレキシブルアルゴリズムにより、内部ゲートウェイプロトコル (IGP) がメトリックタイプ (パス最適化の目的) と制約のユーザー定義による組み合わせに基づいてパスを計算する、ユーザー定義のアルゴリズムを実現できます。この機能により、IS-IS フレキシブルアルゴリズム機能のメトリックタイプとしての TE メトリックのサポートが追加されます。これにより、最短パスの計算を実行するときに、IGP および遅延メトリックとともに TE メトリックを使用できるようになります。
セグメントルーティングフレキシブルアルゴリズムのプレフィックス SID 再配布	Cisco IOS XE Cupertino 17.8.1	この機能を使用すると、プレフィックスが再配布されるときに、サポートされているすべてのアルゴリズムに対してプレフィックス SID が提供されます。この機能は、厳格な、またはフレキシブルなアルゴリズムの SID を使用するルートの再配布を設定すると、自動的に有効になります。

機能名	リリース情報	機能説明
アフィニティサポートを含む IS-IS フレキシブルアルゴリズム	Cisco IOS XE Bengaluru 17.6.1	この機能は、IS-IS で include-any および include-all アフィニティをサポートしています。Cisco IOS XE Bengaluru 17.6.1 リリースより前は、フレキシブルアルゴリズムのアフィニティ exclude-any のみがサポートされていました。
セグメントルーティングフレキシブルアルゴリズム	Cisco IOS XE Bengaluru 17.4.1	TI LFA および uLoop 回避：ループフリー代替 (LFA) パスの計算を可能にします。IS-IS 向けの、フレキシブルアルゴリズムのプライマリパスの計算と同じ制約を使用する TI-LFA バックアップパスです。
セグメントルーティングフレキシブルアルゴリズム	Cisco IOS XE Amsterdam 17.3.1	セグメントルーティングフレキシブルアルゴリズムを使用すると、オペレータは、独自のニーズに応じて IGP 最短パス計算をカスタマイズできます。オペレータは、リンクコストベースの SPF よりも優れた転送を実現するために、カスタムの SR プレフィックス SID を割り当てることができます。結果として、フレキシブルアルゴリズムにより、IGP から到達可能なあらゆる宛先へのトラフィック エンジニアリングに基づくパスを IGP で自動的に計算できます。 アフィニティ exclude-any をサポートしています。

フレキシブルアルゴリズムの前提条件

フレキシブルアルゴリズム機能をアクティブ化する前に、ルータでセグメントルーティングを有効にする必要があります。

フレキシブルアルゴリズムに関する制約事項

- 最大 20 の IS-IS フレキシブルアルゴリズム セッションがサポートされます。
- IS-IS では、フレキシブルアルゴリズム アフィニティ「exclude-any」、「include-any」、および「include-all」がサポートされています。

セグメントルーティングフレキシブルアルゴリズムの構成要素

このセクションでは、IS-IS および OSPF で SR フレキシブルアルゴリズム機能をサポートするために必要な構成要素について説明します。

フレキシブルアルゴリズムの定義

ネットワーク上のパスを計算するために、考えられる多くの制約が使用される可能性があります。一部のネットワークは複数のプレーンを使用して展開されます。単純な形の制約は、特定のプレーンを使用することである場合もあります。より洗練された形の制約には、[RFC8570] で説明されているように、遅延など、一部の拡張メトリックが含まれる可能性があります。さらに高度なケースでは、パスを制限し、特定のアフィニティを持つリンクを回避することも考えられます。また、これらを組み合わせて使用することも可能です。最大限の柔軟性を得られるように、ユーザーは、アルゴリズム値とその意味の間のマッピングを定義できます。ドメイン内のすべてのルータで、特定のアルゴリズム値が持つ意味について共通の認識が確立されている場合、アルゴリズムの計算は一貫性のあるものとなり、トラフィックがループすることはありません。つまり、アルゴリズムの意味が標準によってではなく、ユーザーによって定義されるため、フレキシブルアルゴリズムと呼ばれます。

フレキシブルアルゴリズムのサポートのアドバタイズメント

アルゴリズムは、IGP によるベストパスの計算方法を定義します。ルータは、ノード機能としてアルゴリズムのサポートをアドバタイズします。プレフィックス SID もアルゴリズム値とともにアドバタイズされ、アルゴリズム自体と密接に結び付けられます。

アルゴリズムは 1 つのオクテット値です。128 ~ 255 までの値が、ユーザー定義の値用に予約されており、フレキシブルアルゴリズムの表現に使用されます。

フレキシブルアルゴリズムの定義のアドバタイズメント

特定のフレキシブルアルゴリズムで計算されたパスについてループフリーの転送を実現するためには、ネットワーク内のすべてのルータでフレキシブルアルゴリズムの同じ定義を共有する必要があります。これは、各フレキシブルアルゴリズムの定義をアドバタイズする専用ルータ

によって実現されます。このようなアドバタイズメントでは、優先度を設定して、フレキシブルアルゴリズムごとに一貫した1つの定義がすべてのルータで適用されるようにします。

フレキシブルアルゴリズムの定義には以下が含まれます。

- メトリックタイプ
- アフィニティ制約

特定のフレキシブルアルゴリズムの定義をルータからアドバタイズできるようにするには、**advertise-definition** コマンドを使用します。エリア内の少なくとも1つのルータ、または可能であれば冗長性を確保するために2つのルータで、フレキシブルアルゴリズム定義をアドバタイズする必要があります。有効な定義がアドバタイズされない場合、フレキシブルアルゴリズムは機能しません。

フレキシブルアルゴリズムのプレフィックス SID のアドバタイズメント

フレキシブルアルゴリズム固有のパスでトラフィックを転送するため、フレキシブルアルゴリズムに参加するすべてのルータは、フレキシブルアルゴリズム固有のプレフィックス SID の MPLS ラベル付きパスをインストールします。このフレキシブルアルゴリズム固有のプレフィックス SID は、プレフィックスに対してアドバタイズされます。フレキシブルアルゴリズム固有のプレフィックス SID がアドバタイズされるプレフィックスだけが、フレキシブルアルゴリズム固有の転送の対象となります。

エリア間リーク

Cisco IOS XE Bengaluru 17.4.1 では、フレキシブルアルゴリズムの SID とプレフィックスが IS-IS エリア間でリークされます。ただし、レベル1またはレベル2のパスによって到達可能なプレフィックスのみがリークされます。同様に、特定のフレキシブルアルゴリズムで到達可能な SID のみがリークされます。

たとえば、以下のようなプレフィックス P があるとします。

- レベル1で発生し、レベル2にリークされる
- フレキシブルアルゴリズム 128 での SID 値 = 128、フレキシブルアルゴリズム 129 での SID 値 = 129
- レベル1パスが SID 値 = 128 にのみ存在し、SID 値 = 129 には存在しない

上記の条件の結果として、SID 128 のみがレベル1からレベル2にリークされ、SID 129 はリークされません。

フレキシブルアルゴリズムパスの計算

ルータは、複数のフレキシブルアルゴリズムのパスを計算できます。このようなフレキシブルアルゴリズムのパスを計算する前に、特定のフレキシブルアルゴリズムをサポートするように

ルータを設定する必要があります。このようなフレキシブルアルゴリズムを使用する場合は、あらかじめ、フレキシブルアルゴリズムの有効な定義をルータで確立しておく必要があります。

特定のフレキシブルアルゴリズムの最短パスツリーを計算する場合は、次のようなプロセスになります。

- このようなフレキシブルアルゴリズムのサポートをアドバタイズしないすべてのノードは、トポロジからブルーニングされます。
- 除外されるアフィニティがフレキシブルアルゴリズム定義に含まれている場合、そのようなアフィニティのいずれかがアドバタイズされるすべてのリンクは、トポロジからブルーニングされます。
- ルータは、フレキシブルアルゴリズム定義の一部であるメトリックを使用します。特定のリンクに対してメトリックがアドバタイズされていない場合、そのリンクはトポロジからブルーニングされます。

OSPFおよびIS-ISでは、フレキシブルアルゴリズムのループフリー代替（LFA）パスとTI-LFAバックアップパスは、そのフレキシブルアルゴリズムのプライマリパスの計算と同じ制約を使用して計算されます。これらのパスでは、特にそのフレキシブルアルゴリズム用にアドバタイズされたプレフィックスSIDを使用してバックアップパスを適用します。

フレキシブルアルゴリズムパスの転送エントリの組み込み

フレキシブルアルゴリズム用にアドバタイズされたプレフィックスSIDを使用して、あらゆるプレフィックスに対するフレキシブルアルゴリズムパスを転送エントリにインストールする必要があります。フレキシブルアルゴリズムのプレフィックスSIDが不明な場合は、そのプレフィックスの転送にフレキシブルアルゴリズムパスはインストールされません。

フレキシブルアルゴリズムパスのMPLSからMPLSへのエントリのみが組み込まれます。IPからIPへのエントリまたはIPからMPLSへのエントリは組み込まれません。これらは、デフォルトのアルゴリズムと通常のIGPメトリックに基づいて計算されたネイティブIPGパスに従います。

configuration コマンド `distribute-list filter name in` を使用して、MFIにインストールされているパスを選択的にフィルタ処理できます。設定例については、[選択的なパスのフィルタ処理の設定](#)を参照してください。この機能は、IS-ISフレキシブルアルゴリズムに対してのみサポートされます。

フレキシブルアルゴリズムのプレフィックスSIDの再配布

Cisco IOS XE 17.8 より前では、プロトコル間でプレフィックスが再配布される場合、SRアルゴリズム0（通常のSPF）のプレフィックスSIDのみが使用可能でした。

Cisco IOS XE 17.8 では、プレフィックスが再配布される場合、サポートされているすべてのアルゴリズムのプレフィックス SID を提供するためのサポートが追加されています。この機能は、セグメントルーティングフレキシブルアルゴリズムのプレフィックス SID 再配布と呼ばれます。この機能は、厳格な、またはフレキシブルなアルゴリズムの SID を使用するルートの再配布を設定すると、自動的に有効になります。

OSPF が ISIS に再配布する場合は、すべてのアルゴリズムプレフィックスを再配布し、ISIS がそれを処理します。ISIS が OSPF に再配布する場合は、基本的なアルゴリズムプレフィックスだけが OSPF によって処理されます。その他のフレキシブルアルゴリズムのプレフィックスの再配布は、OSPF ではサポートされていません。たとえば、OSPF 10 は ISIS 30 に再配布され、厳格な SID とフレキシブルアルゴリズムの SID は ISIS によって処理されます。しかし、ISIS 30 が OSPF 10 に再配布される場合は、厳格な SID のみが OSPF によって処理されます。

OSPF は、厳格な SPF とフレキシブルアルゴリズムをサポートしています。ただし、再配布はサポートしていません。たとえば、OSPF 10 と OSPF 20 は、厳格な SPF とフレキシブルアルゴリズムを持つ 2 つのインスタンスです。OSPF 10 が OSPF 20 に再配布される場合、OSPF 20 は OSPF 10 の厳格な SID とフレキシブルアルゴリズムの SID を処理しません。

アルゴリズム情報の表示

`show mpls forwarding-table` コマンドを使用すると、ゼロ以外のアルゴリズム固有のプレフィックス SID ラベル MPLS 転送情報を表示できます。コマンド構文は次のとおりです。

```
show mpls forwarding <ip> <mask> [algo <algo-number>]
```

詳細については、[フレキシブルアルゴリズムの設定の確認, on page 367](#)を参照してください。

フレキシブルアルゴリズムのプレフィックスメトリックアドバタイズメント

セグメントルーティングのフレキシブルアルゴリズムプレフィックスメトリックを使用すると、オペレータは、プレフィックスのレベル間リンクまたはドメイン間再配布中に、特定のフレキシブルアルゴリズムで計算されたメトリックをプレフィックスに関連付けることができます。これは、最適なレベル間またはドメイン間パスを計算するのに役立ちます。プレフィックスメトリックをサポートするようにフレキシブルアルゴリズムを設定すると、ISIS フレキシブルアルゴリズム定義フラグのサブ TLV でプレフィックスメトリックフラグ (M フラグ) がアドバタイズされます。サブ TLV は、レベル 1 およびレベル 2 ルータによってのみアドバタイズされます。プレフィックスメトリックフラグ (M フラグ) を表示するには、`show isis database verbose` コマンドを使用します。詳細については、[フレキシブルアルゴリズムの設定の確認 \(367 ページ\)](#)を参照してください。

特定の Flex Algo アルゴリズム (128 ~ 255) で Flex Algo プレフィックスメトリック (FAPM) の使用が指定されている場合、プレフィックスに関連付けられたメトリックは、そのプレフィックスを他のレベル/エリアにアドバタイズする ABR が、そのアルゴリズム固有の FAPM サブ TLV を使用してアドバタイズする必要があります。フレキシブルアルゴリズム定義で FAPM

(M フラグ) の使用が指定されている場合、アルゴリズム固有の FAPM アドバタイズメントを持つプレフィックスのみが、アルゴリズム固有のトポロジで到達可能と見なされます。



(注) Cisco IOS XE は、プレフィックスのレベル間リーク時にのみフレキシブルアルゴリズムのプレフィックスメトリック挿入をサポートし、ドメイン間再配布時はサポートしません。

ISIS フレキシブルアルゴリズム プレフィックス メトリック サブ TLV は、特定のプレフィックスアドバタイズメントに関連付けられたフレキシブルアルゴリズム固有のプレフィックスメトリックのアドバタイズメントをサポートしています。

フレキシブルアルゴリズム プレフィックス メトリックのアドバタイズメントを有効にするには、次のコマンドを使用します。

```
router isis 1
flex-algo 128
  advertise-definition
  prefix-metric

# show isis 1 rib redistribution level-2
IPv4 redistribution RIB for IS-IS process 1
IPV4 unicast base topology (TID 0, TOPOID 0x0) =====
===== Level 2 =====
10.1.1.1/32
 [ISIS/20] isis prefix-SID index: 1, R:1 N:1 P:1 E:0 V:0 L:0
 flex-algo 128 SID index: 11, R:0 N:1 P:0 E:0 V:0 L:0 map 0x0
 prefix-metric: 20, advertised
```

このコマンドの出力では、有効になっている場合のみプレフィックスメトリックがアドバタイズされることがわかります。

フレキシブルアルゴリズムの設定

このセクションでは、SR フレキシブルアルゴリズム機能をサポートするために必要となるさまざまな設定について説明します。

表 44: フレキシブルアルゴリズムの設定

タスク	プロトコル	モード	コマンド
フレキシブルアルゴリズムの設定	IS-IS および OSPF	IS-IS および OSPF 設定のサブモード	<code>flex-algo algorithm number</code> <code>algorithm number : 128</code> ～ 255 の値

タスク	プロトコル	モード	コマンド
メトリックタイプの設定	IS-IS および OSPF	フレキシブルアルゴリズムのサブモード	<p>[IS-IS]</p> <pre>metric type {delay te}</pre> <p>(注) デフォルトでは、通常の IGP メトリックが使用されます。遅延メトリックが有効になっている場合、リンク上でアドバタイズされた遅延が、フレキシブルアルゴリズム計算のメトリックとして使用されます。</p> <p>TE メトリックが有効になっている場合、リンク上でアドバタイズされる TE メトリックがフレキシブルアルゴリズム計算のメトリックとして使用されます。</p> <p>[OSPF]</p> <pre>metric-type {delay te-metric igp-metric}</pre>

タスク	プロトコル	モード	コマンド
アフィニティの設定	IS-IS および OSPF	フレキシブルアルゴリズムのサブモード	<p>[IS-IS]</p> <pre>affinity {exclude-any include-any include-all} name affinity-name</pre> <p>[OSPF]</p> <pre>affinity {exclude-any include-any include-all} name affinity-name</pre> <p><i>affinity-name</i> : アフィニティマップの名前</p>
優先順位の設定	IS-IS および OSPF	フレキシブルアルゴリズムのサブモード	<p>[IS-IS および OSPF]</p> <pre>priority priority value</pre> <p><i>priority-value</i> : フレキシブルアルゴリズム定義の選択時に使用される優先順位</p>
IS-IS および OSPF でフレキシブルアルゴリズム定義のアドバタイズメントを有効にします。 アフィニティマップは、拡張管理者グループのビットマスク内の特定のビット位置に名前を関連付けます。	IS-IS および OSPF		<p>[IS-IS]</p> <pre>affinity-map affinity-name bit-position bit number</pre> <p>[OSPF]</p> <pre>affinity-map name affinity-name bit-position bit number</pre> <p><i>affinity-name</i> : アフィニティマップの名前</p> <p><i>bit number</i> : 拡張管理者グループのビットマスク内のビット位置</p>

タスク	プロトコル	モード	コマンド
アフィニティのインターフェイスへの関連付け	IS-IS および OSPF		<p>[IS-IS]</p> <pre>isis affinity flex-algo name affinity-name</pre> <p>[OSPF]</p> <pre>ip ospf affinity flex-algo name affinity-name</pre> <p><i>affinity-name</i> : アフィニティマップの名前</p>

Cisco IOS XE リリース 17.11.1a 以降、IS-IS フレキシブルアルゴリズムに新しいメトリック **TE** が導入されています。このメトリックには、**isis flex-algo metric-type** コマンドの新しいキーワードが含まれています。

```
isis instance flex-algo algo metric-type {delay | te}
```

このキーワードは、Cisco ASR 1000 シリーズのプラットフォームで使用できます。



- (注) デフォルトでは、IGP メトリックはフレキシブルアルゴリズム計算に使用されます。遅延または TE メトリックが有効になっている場合、リンク上でアドバタイズされる遅延または TE メトリックは、フレキシブルアルゴリズム計算のメトリックとして使用されます。

フレキシブルアルゴリズム設定でのプレフィックス SID のコマンド

特定のフレキシブルアルゴリズムに関連付けられたプレフィックス SID を定義するために、接続されたプレフィックス SID マップとマッピングサーバーの両方に関して、セグメントルーティングの下に新しいコマンドが追加されています。

```
segment-routing mpls
connected-prefix-sid-map
address-family ipv4algorithmflex-algo
ip addressmask [index | absolute] sid range range of SIDs

segment-routing mpls
mapping-server
prefix-sid-map
address-family ipv4algorithmflex-algo
ip addressmask [index | absolute] sid range range of SIDs
```

IS-IS フレキシブルアルゴリズムの設定

次に、IS-IS フレキシブルアルゴリズムの設定例を示します。

```
router isis 1
net 49.0002.0000.0001.00
is-type level-1
metric-style wide
```

```

log-adjacency-changes
nsf cisco
distribute link-state
segment-routing mpls
segment-routing prefix-sid-map advertise-local
affinity-map blue bit-position 8
affinity-map green bit-position 201
affinity-map red bit-position 65

fast-reroute per-prefix level-1 all
fast-reroute tie-break level-1 node-protecting 100
fast-reroute tie-break level-1 srlg-disjoint 50
fast-reroute ti-lfa level-1
fast-reroute ti-lfa level-2
microloop avoidance segment-routing
microloop avoidance rib-update-delay 10000

flex-algo 129
  advertise-definition
  metric-type delay
  priority 120
  affinity
  exclude-any
  name red
!
```



(注) TI LFA を無効にするには、**fast-reroute disable** コマンドを使用します。

次の例で、メトリックタイプを TE として IS-IS フレキシブルアルゴリズムを設定する方法を示します。

```

router isis 1
net 49.0002.0000.0001.00
is-type level-1
metric-style wide
log-adjacency changes
nsf cisco
distribute link-state
segment-routing mpls
segment-routing prefix-sid-map advertise-local
affinity-map blue bit-position 8
affinity-map green bit-position 201
affinity-map red bit-position 65

fast-reroute per-prefix level-1 all
fast-reroute tie-break level-1 node-protecting 100
fast-reroute tie-break level-1 srlg-disjoint 50
fast-reroute ti-lfa level-1
fast-reroute ti-lfa level-2
microloop avoidance segment-routing
microloop avoidance rib-update-delay 10000

flex-algo 129 advertise-definition
metric-type te
  priority 120
affinity exclude-any name red
!
```

次の例で、インターフェイスに IS-IS TE メトリックを設定する方法を示します。

```
interface Ethernet0/0
ip address 10.12.12.1 255.255.255.0
ip router isis 1
ipv6 address 2001:20::1/112
ipv6 router isis 1
isis network point-to-point
isis te-metric flex-algo 500
```

IS-IS の再配布

次の例で IS-IS を再配布する方法を示します。

```
router isis 2
router-id Loopback0
metric-style wide
segment-routing mpls
segment-routing prefix-sid-map advertise-local
flex-algo 128
advertise-definition
redistribute isis 1 ip level2 <-----
passive-interface Loopback0
mpls traffic-eng level-1
mpls traffic-eng level-2
```

SRTE-ODN の関連付けの設定

次の例で、SR トラフィック エンジニアリングと ODN の関連付けを設定する方法を示します。

```
segment-routing traffic-eng
on-demand color 100
  authorize
  candidate-paths
  preference 100
  constraints
    segments
      dataplane mpls
      algorithm 129
  !
!
dynamic
  metric
    type delay
!
!
```

フレキシブルアルゴリズム用のインターフェイスの設定

次の例で、フレキシブルアルゴリズム用のインターフェイスを設定する方法を示します。

```
interface GigabitEthernet0/0/6
ip address 10.11.11.1 255.255.255.0
ip router isis 1
mpls ip
mpls traffic-eng tunnels
bfd template pw_bfd
isis network point-to-point
isis affinity flex-algo
  name red
!
```

BGP の設定

次の例で、BGPを設定する方法を示します。

```
router bgp 100
  bgp router-id 10.1.1.1
  bgp log-neighbor-changes
  bgp graceful-restart
  neighbor 10.2.2.2 remote-as 100
  neighbor 10.2.2.2 ha-mode sso
  neighbor 10.2.2.2 update-source Loopback1
  !
  address-family ipv4
    neighbor 10.2.2.2 activate
  exit-address-family
  !
  address-family vpnv4
    neighbor 10.2.2.2 activate
    neighbor 10.2.2.2 send-community both
    neighbor 10.2.2.2 route-map BGP_TE_MAP out
  exit-address-family
  !
  address-family ipv4 vrf SR
    redistribute connected
    neighbor 10.132.1.1 remote-as 101
    neighbor 10.132.1.1 activate
  exit-address-family
  !
```

選択的なパスのフィルタ処理の設定

次の例で、MPLS 転送インフラストラクチャ（MFI）にインストールされているパスを選択的にフィルタ処理する方法を示します。

```
Prefix-source
=====
interface Loopback1
ip address 10.1.1.1 255.255.255.255
ip router isis
  isis tag 111

Remote router configured for selective path filtering
=====
route-map block deny 10
match tag 111
!
route-map block permit 100
!
router isis 1
!
flex-algo 135
!
distribute-list route-map block in
```

PCE 委任による SR ポリシーの設定

次の例で、パス計算要素（PCE）委任を使用して SR ポリシーを設定する方法を示します。

```
policy p-delay
  color 1111 end-point 10.6.6.6
  candidate-paths
  preference 1
  constraints
  segments
  dataplane mpls
  algorithm 128
  !
  !
  dynamic
  pcep
```

フレキシブルアルゴリズムの設定の確認

次に、IS-IS フレキシブルアルゴリズムに関するすべての情報を表示する **show isis flex-algo value** コマンドの出力例を示します。

```
show isis flex-algo 129
Tag 1:
IS-IS Flex-Algo Database
  Flex-Algo count: 7

Flex-Algo 129:
  IS-IS Level-1
    Definition Priority: 222
    Definition Source: R2-RSP3-2015.00, (Local)
    Definition Equal to Local: Yes
    Definition Metric Type: Delay
    Definition Flex-Algo Prefix Metric: No
    Disabled: No
    Microloop Avoidance Timer Running: No
  Local Priority: 222
  FRR Disabled: No
  Microloop Avoidance Disabled: No
```

次に、メトリックタイプ TE を表示する **show isis flex-algo** コマンドの出力例を示します。

```
show isis flex-algo 129 Tag 1:
IS-IS Flex-Algo Database Flex-Algo count: 7

Flex-Algo 129:
IS-IS Level-1
Definition Priority: 222
Definition Source: R2-RSP3-2015.00, (Local) Definition Equal to Local: Yes
Definition Metric Type: TE
Definition Flex-Algo Prefix Metric: No Disabled: No
Microloop Avoidance Timer Running: No Local Priority: 222
FRR Disabled: No
Microloop Avoidance Disabled: No
```

次に、すべての IS-IS ローカル RIB 情報を表示する **show isis rib flex-algo value** コマンドの出力例を示します。

```
show isis rib flex-algo 129
IPv4 local RIB for IS-IS process 1

IPv4 unicast topology base (TID 0, TOPOID 0x0) ===== Repair path attributes:
DS - Downstream, LC - Linecard-Disjoint, NP - Node-Protecting PP - Primary-Path, SR -
```

```
SRLG-Disjoint

Flex-algo 129

10.1.1.1/32 prefix attr X:0 R:0 N:1 source router id: 10.1.1.1 SID index 38 - Bound
[115/L1/113] via 10.11.11.1(GigabitEthernet0/4/6) R1-ASR920-2011.00-00, from 10.1.1.1,
tag 0
LSP 6/6/351(351), prefix attr: X:0 R:0 N:1 Source router id: 10.1.1.1
Prefix-SID index: 38, R:0 N:1 P:0 E:0 V:0 L:0
label: implicit-null
repair path: 10.20.20.2 (GigabitEthernet0/4/7) metric: 117 (DS,SR) local LFA
label: implicit-null
repair source: R1-ASR920-2011, LSP 6

10.2.2.2/32 prefix attr X:0 R:0 N:1 source router id: 10.2.2.2 SID index 39 - Bound
[115/L1/24] via 10.13.13.2(GigabitEthernet0/1/5) R4-RSP3-2036.00-00, from 10.2.2.2, tag
0
LSP 2/3/345(345), prefix attr: X:0 R:0 N:1 Source router id: 10.2.2.2
Prefix-SID index: 39, R:0 N:1 P:0 E:0 V:0 L:0
label: 17039
repair path: 10.4.4.4 (MPLS-SR-Tunnel4) metric: 170 (DS,NP,SR) next-hop: 10.20.20.2
(GigabitEthernet0/4/7)
TI-LFA node/SRLG-protecting, SRLG-protecting
SRGB: 17000, range: 7000 prefix-SID index: 39, R:0 N:1 P:0 E:0 V:0 L:0
label: 17039
P node: R3-RSP2-2013[10.4.4.4], label: 17221
repair source: R6-RSP3-2038, LSP 3

10.4.4.4/32 prefix attr X:0 R:0 N:1 source router id: 10.4.4.4 SID index 221 - Bound

[115/L1/172] via 10.13.13.2(GigabitEthernet0/1/5) R4-RSP3-2036.00-00, from 10.4.4.4, tag
0
LSP 2/7/24(24), prefix attr: X:0 R:0 N:1 Source router id: 10.4.4.4
Prefix-SID index: 221, R:0 N:1 P:0 E:0 V:0 L:0
label: 17221
repair path: 10.20.20.2 (GigabitEthernet0/4/7) metric: 184 (DS,NP,SR) local LFA
label: 17221
repair source: R3-RSP2-2013, LSP 7

10.5.5.5/32 prefix attr X:0 R:0 N:1 source router id: 10.5.5.5 SID index 222 - Bound
[115/L1/17] via 10.13.13.2(GigabitEthernet0/1/5) R4-RSP3-2036.00-00, from 10.5.5.5, tag
0
LSP 2/2/347(347), prefix attr: X:0 R:0 N:1 Source router id: 10.5.5.5
Prefix-SID index: 222, R:0 N:1 P:0 E:0 V:0 L:0
label: implicit-null
repair path: 10.4.4.4 (MPLS-SR-Tunnel4) metric: 170 (DS,SR) next-hop: 10.20.20.2
(GigabitEthernet0/4/7)
TI-LFA SRLG-protecting
SRGB: 17000, range: 7000 prefix-SID index: 222, R:0 N:1 P:0 E:0 V:0 L:0
label: 17222
P node: R3-RSP2-2013[10.4.4.4], label: 17221
repair source: R4-RSP3-2036, LSP 2

10.6.6.6/32 prefix attr X:0 R:0 N:1 source router id: 10.6.6.6 SID index 333 - Bound
[115/L1/122] via 10.13.13.2(GigabitEthernet0/1/5) R4-RSP3-2036.00-00, from 10.6.6.6, tag
0
LSP 2/4/351(351), prefix attr: X:0 R:0 N:1 Source router id: 10.6.6.6
Prefix-SID index: 333, R:0 N:1 P:0 E:0 V:0 L:0
label: 17333
repair path: 10.4.4.4 (MPLS-SR-Tunnel4) metric: 170 (DS,NP,SR) next-hop: 10.20.20.2
(GigabitEthernet0/4/7)
TI-LFA node/SRLG-protecting, SRLG-protecting
```

```
SRGB: 17000, range: 7000 prefix-SID index: 333, R:0 N:1 P:0 E:0 V:0 L:0
label: 17333
P node: R3-RSP2-2013[10.4.4.4], label: 17221
repair source: R5-ASR920-2012, LSP 4
```

次に、中間システムへの IS-IS パスに関する情報を表示する **show isis topo flex-algo value** コマンドの出力例を示します。

```
show isis topo flex-algo 129
Tag 1:
IS-IS TID 0 paths to level-1 routers
Flex-algo 129
System Id          Metric      Next-Hop          Interface         SNPA
920_1              3           RSP2_2           Gi0/15/0         e8ed.f3b8.f804
RSP3_R1           **
RSP2_1            2           RSP2_2           Gi0/15/0         e8ed.f3b8.f804
RSP3_R2           **
RSP2_2            1           RSP2_2           Gi0/15/0         e8ed.f3b8.f804
RSP3_R3           --
```

次に、IS-IS TI-LFA トンネルに関する情報を表示する **show isis fast-reroute ti-lfa tunnel** コマンドの出力例を示します。

```
show isis fast-reroute ti-lfa tunnel
Tag null:
Fast-Reroute TI-LFA Tunnels:
Tunnel Interface Next Hop          End Point          Label          End Point Host
Tag 1:
Fast-Reroute TI-LFA Tunnels:

Tunnel Interface Next Hop          End Point          Label          End Point Host
MP2      Gi0/0/6      10.12.12.2      10.2.2.2          17019         RSP3_R3
MP5      Gi0/0/5      10.11.11.2      10.2.2.2          17019         RSP3_R3
MP3      Gi0/0/6      10.12.12.2      10.6.6.6          17333         RSP2_2
          10.2.2.2          16           RSP3_R3
MP9      Gi0/0/5      10.11.11.2      10.2.2.2          17039         RSP3_R3
MP1      Gi0/0/6      10.12.12.2      10.6.6.6          20333         RSP2_2
          10.2.2.2          16           RSP3_R3
MP6      Gi0/0/5      10.11.11.2      10.2.2.2          17049         RSP3_R3
```

次に、リンクステートアドバタイズメント (LSA) からコンパイルされたノードとリンクの情報を表示する **show ip ospf topology** コマンドの出力例を示します。

```
R1#show ip ospf topology
      Process OSPF-10

Instance : global
Router ID : 10.1.1.1
Area : (8 nodes)
Node : 10.2.0.2 (pseudo) (2 links)
      Link : 10.1.1.1 10.0.0.0 Transit
      Link : 10.1.1.2 10.0.0.0 Transit
Node : 10.1.1.1 (root) (3 links) ABR
      Algos supported: 128, 129
```

```

Flex Algo Definition: 128
Flex Algo Definition: 129
Link : 10.1.1.6 10.0.0.2 Point-to-point
Link : 10.1.1.6 10.6.1.1 Point-to-point
Link : 10.2.0.2 10.2.0.1 Transit
Node : 10.1.1.2 (3 links)
Algos supported: 128
Link : 10.1.1.3 10.3.0.2 Point-to-point
Link : 10.1.1.54 10.5.0.2 Point-to-point
Link : 10.2.0.2 10.2.0.2 Transit
Node : 10.1.1.3 (2 links)
Algos supported: 128
Link : 10.1.1.2 10.3.0.3 Point-to-point
Link : 10.1.1.4 10.4.0.3 Point-to-point
Node : 10.1.1.4 (3 links) ABR, ASBR
Algos supported: 128, 129
Link : 10.1.1.3 10.4.0.4 Point-to-point
Link : 10.1.1.9 10.0.0.3 Point-to-point
Link : 10.1.1.54 10.5.0.4 Point-to-point
Node : 10.1.1.6 (4 links)
Algos supported: 129
Link : 10.1.1.1 10.0.0.2 Point-to-point
Link : 10.1.1.1 10.6.1.6 Point-to-point
Link : 10.1.1.54 10.6.0.6 Point-to-point
Link : 10.1.1.54 10.6.1.6 Point-to-point
Node : 10.1.1.9 (1 links) ABR
Link : 10.1.1.4 10.0.0.3 Point-to-point
Node : 10.1.1.54 (4 links)
Algos supported: 129
Link : 10.1.1.2 10.5.0.5 Point-to-point
Link : 10.1.1.4 10.5.0.5 Point-to-point
Link : 10.1.1.6 10.6.0.5 Point-to-point
Link : 10.1.1.6 10.6.1.5 Point-to-point
Area : (2 nodes)
Node : 10.1.1.1 (root) (1 links) ABR
Algos supported: 128, 129
Flex Algo Definition: 128
Flex Algo Definition: 129
Link : 10.1.1.8 10.8.0.1 Point-to-point
Node : 10.1.1.8 (1 links) ASBR
Link : 10.1.1.1 10.8.0.8 Point-to-point

```

次に、LSA からコンパイルされたノードとプレフィックスの情報を表示する **show ip ospf topology prefix** コマンドの出力例を示します。

```

R1#show ip ospf topology prefix
Process OSPF-10

Instance : global
Router ID : 10.1.1.1
Area : (8 nodes)
Node : 10.2.0.2 (pseudo) (2 links)
Node : 10.1.1.1 (root) (3 links) ABR
Algos supported: 128, 129
Flex Algo Definition: 128
Flex Algo Definition: 129
Node : 10.1.1.2 (3 links)
Algos supported: 128
Node : 10.1.1.3 (2 links)
Algos supported: 128
Prefix : 10.1.1.34/32
Node : 10.1.1.4 (3 links) ABR, ASBR
Algos supported: 128, 129
Prefix : 10.1.1.4/32

```

```

    Prefix : 10.1.1.34/32
    Prefix : 10.1.1.45/32
Node : 10.1.1.6 (4 links)
  Algos supported: 129
Node : 10.1.1.9 (1 links) ABR
Node : 10.1.1.54 (4 links)
  Algos supported: 129
  Prefix : 10.1.1.54/32
Area : (2 nodes)
Node : 10.1.1.1 (root) (1 links) ABR
  Algos supported: 128, 129
  Flex Algo Definition: 128
  Flex Algo Definition: 129
Node : 10.1.1.8 (1 links) ASBR

```

次に、ルート計算に基づいて計算されたルートのパス情報を表示する **show ip ospf topology route** コマンドの出力例を示します。

```

R1#show ip ospf topology route
Route Table of OSPF-10 with router ID 10.1.1.1 (VRF global)

10.1.1.4/32
  Algo 128, Metric 31, SID 132, Label 16132
    10.2.0.2, from 10.1.1.2, via Ethernet0/1
  Algo 129, Metric 31, SID 133, Label 16133
    10.1.1.6, from 10.1.1.6, via Ethernet0/0
    10.6.1.6, from 10.1.1.6, via Ethernet0/3
10.1.1.34/32
  Algo 128, Metric 21, SID 43, Label 16043
    10.2.0.2, from 10.1.1.2, via Ethernet0/1
10.1.1.45/32
  Algo 129, Metric 31, SID 4294967295, Label 1048577
    10.1.1.6, from 10.1.1.6, via Ethernet0/0
    10.6.1.6, from 10.1.1.6, via Ethernet0/3
10.1.1.54/32
  Algo 129, Metric 21, SID 45, Label 16045
    10.1.1.6, from 10.1.1.6, via Ethernet0/0
    10.6.1.6, from 10.1.1.6, via Ethernet0/3

```

次に、ゼロ以外のアルゴリズム固有のプレフィックス SID ラベル MPLS 転送情報を表示する **show mpls forwarding-table** コマンドの出力例を示します。

```

#show mpls forwarding-table 10.23.23.23 255.255.255.255 algo 20
Local   Outgoing Prefix          Bytes Label   Outgoing Next Hop
Label   Label    or Tunnel Id    Switched      interface
18      16023    0-10.23.23.23/32-4 (10:30:20:1) \
                                                0          Et1/1      10.1.1.2

```

プレフィックスまたはトンネル ID 列には、メトリックに関する情報 (0-10.6.6.6/32-4 (4:50:128:0) など) が表示されます。

プレフィックスの横にある 4 つの部分は次のとおりです。

- pdb-index=4
- metric 50
- algo=128
- via-srms=0

via-srms フィールドは、ラベルの送信元がプレフィックス到達可能性アドバタイズメント (0) またはマッピングサーバーアドバタイズメント (1) のどちらであるかを示します。再配布されたルートが再配布の宛先プロトコルによってアドバタイズされる場合、マッピングサーバーアドバタイズメントから取得したラベルはアドバタイズされません。

pdb-index フィールドは、プロトコルインスタンスを示します。次のコマンド出力は、さまざまなプロトコルとその値を示しています。

```
# show ip protocols summary
Index Process Name
0 connected
1 static
2 application
3 nat-route
4 isis 1
```

次に、再配布されたプレフィックスを表示する **show isis rib redistribution** コマンドの出力例を示します。

```
# show isis rib redistribution

IPV4 redistribution RIB for IS-IS process 1

IPV4 unicast base topology (TID 0, TOPOID 0x0) =====
===== Level 1 =====
===== Level 2 =====
10.3.3.3/32
  [Connected/0] prefix-SID index: 31, R:0 N:1 P:0 E:0 V:0 L:0
  strict-SPF SID index: 32, R:0 N:1 P:0 E:0 V:0 L:0
  flex-algo 128 SID index: 33, R:0 N:1 P:0 E:0 V:0 L:0 map 0x1
  prefix-metric: 0, not advertised
10.4.4.4/32
  [ISIS/0] external interarea prefix-SID index: 41, R:1 N:0 P:1 E:0 V:0 L:0
  strict-SPF SID index: 42, R:1 N:0 P:1 E:0 V:0 L:0
  flex-algo 128 SID index: 43, R:1 N:0 P:1 E:0 V:0 L:0 map 0x0
  prefix-metric: 40, not advertised
  prefix attr: X:1 R:0 N:0
```

この例では、厳格なSIDまたはフレキシブルアルゴリズムのプレフィックスSIDを確認できます。再配布されたプレフィックスはエリア間ルートとして示され、Xフラグが設定されます。

次に、ISISフレキシブルアルゴリズム定義フラグのサブTLVでアドバタイズされるプレフィックスメトリックフラグ (Mフラグ) を表示する **show isis database verbose** コマンドの出力例を示します。

```
# show isis database verbose
..
Router CAP: 10.1.1.1, D:0, S:0
  Segment Routing: I:1 V:0, SRGB Base: 16000 Range: 8000
  Segment Routing Local Block: SRLB Base: 15000 Range: 1000
  Node-MSD
    MSD: 16
  Flex algorithm: 150 Metric-Type: IGP Alg-type: SPF Priority: 128
  Segment Routing Algorithms: SPF, Strict-SPF, Flex-algo 128
  Segment Routing Algorithms: Flex-algo 150
  Flex algorithm: 128 Metric-Type: IGP Alg-type: SPF Priority: 128
  Flex-Algo Definition Flags:
    M:1.
```



第 36 章

SR-TE 優先パス上の L2VPN

表 45: 機能の履歴

機能名	リリース情報	説明
フレキシブルアルゴリズムでの SR-TE 優先パスを使用した L2VPN トラフィックステアリング	Cisco IOS XE Bengaluru 17.6.1	この機能により、フレキシブルアルゴリズムを使用して、SR ポリシーを VPWS または VPLS 疑似回線の優先パスとして設定できます。同じ PE 間の VPWS または VPLS 疑似回線は、要件に基づき異なる SR ポリシーを介してルーティングできます。このリリースより前は、IPv4 トラフィックを宛先疑似回線 (IGP または BGP-LU 経由) にルーティングするための SR ポリシーを使用してトラフィックをステアリングできるのみでした。

仮想プライベート LAN サービス (VPLS) により、企業では、サービスプロバイダーから提供されたインフラストラクチャを介して、複数のイーサネットベースの LAN をまとめてリンクすることが可能になります。

VPLS はサービスプロバイダーのコアを使用して企業の複数の接続回線をまとめ、仮想ブリッジをシミュレートします。VPLS のトポロジは、企業からは認識されません。すべてのカスタマーエッジ (CE) デバイスは、サービスプロバイダーのコアによってエミュレートされた論理ブリッジに接続されているように見えます。

Cisco IOS XE Bengaluru リリース 17.6.1 より前では、SR ポリシーを介した L2VPN (VPLS または VPWS) トラフィックをステアリングできませんでした。IPv4 トラフィックを宛先疑似回線 (IGP または BGP-LU 経由) にルーティングするための SR ポリシーを使用して、IPv4 トラフィックをステアリングできるのみでした。

次に、フレキシブルアルゴリズムを使用して、SR ポリシーをVPWS または VPLS 疑似回線の優先パスとして設定します。同じ PE 間の VPWS または VPLS 疑似回線は、異なる SR ポリシーを介してルーティングすることもできます。

フォールバックオプションの無効化

フォールバックの無効化オプションは、優先パスの SR ポリシーがダウンしたときに、ルータがデフォルトのパスを使用しないようにします。

- [機能制限 \(374 ページ\)](#)
- [フレキシブルアルゴリズムでの SR-TE 優先パスを使用した L2VPN トラフィックステアリングの設定 \(374 ページ\)](#)
- [設定例 1 : SR-TE 優先パス上の VPWS 疑似回線 \(376 ページ\)](#)
- [設定例 2 : SR-TE 優先パス上の VPWS 疑似回線 \(376 ページ\)](#)
- [設定例 3 : SR-TE 優先パス上の VPLS 疑似回線 \(377 ページ\)](#)
- [SR-TE 優先パス上の L2VPN の設定確認 \(377 ページ\)](#)

機能制限

- オンデマンド (ODN) ポリシーを優先パスに追加することはできません。
- SR-TE 優先パスを介した L2VPN は、SR 宛先別ポリシー (PDP) でのみサポートされ、SR フロー別ポリシー (FPF) ではサポートされません。
- SR-TE 優先パスを介した L2VPN は、疑似回線インターフェイスを使用してのみ設定できます。
- この機能は、IS-IS プロトコルでのみサポートされています。

フレキシブルアルゴリズムでの SR-TE 優先パスを使用した L2VPN トラフィックステアリングの設定

Flex Algo で IS-IS を設定するには、次の手順を実行します。

```
router isis 1

affinity-map green bit-position 0
affinity-map red bit-position 1
affinity-map yello bit-position 2
flex-algo 128
  advertise-definition
  metric-type delay
  priority 200
  affinity
    exclude-any
    name red
    name yellow
!
flex-algo 129
```

```

advertise-definition
priority 200
affinity
  exclude-any
    name green
    name red

interface Tunnell100
isis affinity flex-algo
  name green
!
interface Tunnell101
isis affinity flex-algo
  name yellow
!
interface Tunnell102
isis affinity flex-algo
  name red

segment-routing traffic-eng
policy p-2000
  color 2000 end-point 10.4.4.4
  performance-measurement
    delay-measurement
  candidate-paths
    preference 10
    constraints
      segments
        dataplane mpls
        algorithm 128
    !
    !
    !
  dynamic

```

MPLS ラベルの SR 静的ポリシーを作成するには、次の手順を実行します。

```

configure terminal segment-routing traffic-eng
segment-list name segment-name
index 1 mpls label first hop label
index 2 mpls label second hop label !
policy policy-name
color color-code end-point destination IP Address candidate-paths
preference preference
explicit segment-list segment-name
constraints
segments dataplane mpls

```

次の SR 静的ポリシーを作成することもできます。

- MPLS 隣接関係 (アジャセンシー)
- MPLS ブレフィックス

SR-TE 優先パスを介した L2VPN は、次の方法で設定できます。

- 非テンプレートベースの設定

- テンプレートベースの設定

非テンプレートベースの設定 :

- 疑似回線の作成

疑似回線を作成するには、次の手順を実行します。

```
interface pseudowire 1
 encapsulation mpls
 neighbor peer-address vc-id
```

- 優先パスを使用したポリシーのアタッチ

優先パスを使用してポリシーをアタッチするには、次の手順を実行します。

```
interface pseudowire1
 preferred-path segment-routing traffic-eng policy policy-name [disable-fallback]
```

テンプレートベースの設定 :

- テンプレートタイプの疑似回線の作成

テンプレートタイプの疑似回線を作成するには、次の手順を実行します。

```
template type pseudowire name
 encapsulation mpls
 preferred-path segment-routing traffic-eng policy name [disable-fallback]
```

- 優先パスを使用したポリシーのアタッチ

優先パスを使用してポリシーをアタッチするには、次の手順を実行します。

```
interface pseudowire 1
 source template type pseudowire name
```

設定例 1 : SR-TE 優先パス上の VPWS 疑似回線

```
!
interface
gi0/0/1
service instance 1000
ethernet encapsulation
dot1q 1000 !
template type pseudowire l2vpntest
 encapsulation mpls
 preferred-path Segment-Routing traffic-eng policy p106
l2vpn xconnect context l2vpn-test
member 10.6.6.6 1000 template
l2vpntest member gi0/0/1
service-instance 1000 !
```

設定例 2 : SR-TE 優先パス上の VPWS 疑似回線

```
!
!
interface gi0/0/1
```

```

service instance 1000 ethernet
  encapsulation dot1q 1000
  !
template type pseudowire
l2vpntest encapsulation mpls
preferred-path Segment-Routing traffic-eng policy p106 !

interface pseudowire1000
  source template type pseudowire l2vpntest
  encapsulation mpls neighbor 10.1.1.1 1000 !

l2vpn xconnect context l2vpn-test
member pseudowire 1000
member gi0/0/1 service-instance 1000

```

設定例 3 : SR-TE 優先パス上の VPLS 疑似回線

```

interface gi0/0/1

service instance 1000
ethernet encapsulation
dot1q 1000 !

interface pseudowire106
encapsulation mpls
neighbor 10.6.6.6 1000

preferred-path Segment-Routing traffic-eng policy p106 !
interface pseudowire104
encapsulation mpls
neighbor 10.4.4.4 1000

preferred-path Segment-Routing traffic-eng policy p104
!
l2vpn vfi context VC_1000 vpn id 1000 member
pseudowire106 member pseudowire104
!

bridge-domain 1000

member gi0/0/1 service-instance
1000 member vfi VC_1000

```

SR-TE 優先パス上の L2VPN の設定確認

ポリシー設定を確認するには、**show segment-routing traffic-eng policy name *policy name* detail** コマンドを使用します。

```

Router#show segment-routing traffic-eng policy name CE11-PE12 detail

Name: CE11-PE12 (Color: 50 End-point: 10.12.12.12)
Owners : CLI
Status:
  Admin: up, Operational: up for 70:04:00 (since 08-17 07:55:36.536)
Candidate-paths:
  Preference 100 (CLI):
    Explicit: segment-list IntraDomain (active)

```

```

Weight: 1, Metric Type: TE
16005
16008
16010
Attributes:
  Binding SID: 20
  Allocation mode: dynamic
  State: Programmed
Tunnel ID: 65538 (Interface Handle: 0x20)
Per owner configs:
  CLI
  Binding SID: dynamic
Stats:
  Packets: 0 Bytes: 0

Event history:
  Timestamp          Client          Event type      Context:
  Value
  -----
  -----: -----
  10-28 04:05:37.028    L2VPN          Policy created   Name:
L2VPN
  10-28 04:05:37.048    L2VPN          BSID allocated   FWD:
label 20
  10-28 04:05:37.494    L2VPN          Client removed   Owner:
Destroyed
  10-28 04:05:37.494    CLI            Set colour
Colour: 230
  10-28 04:05:37.494    CLI            Set end point
End-point: 12.12.12.12
  10-28 04:05:37.496    CLI            Set explicit path Path
option: IntraDomain
  10-28 04:08:22.873    FH Resolution   Policy state UP   Status:
PATH RESOLVED
  10-28 04:08:45.630    FH Resolution   REOPT triggered   Status:
REOPTIMIZED

```

show mpls l2transport vc 1000 detail コマンドを使用して、SR-TE 優先パスを介した L2VPN を確認します。

```

Router#show mpls l2transport vc 1000 detail
Local interface: VFI VC_1000 vfi up
Interworking type is Ethernet
Destination address: 10.12.12.12, VC ID: 1000, VC status: up
Output interface: tu65538, imposed label stack {16005 16008 16010 32}
Preferred path: not configured
Default path: active
Next hop: 10.168.1.1
Create time: 1w4d, last status change time: 22:50:57
Last label FSM state change time: 22:51:46
Signaling protocol: LDP, peer 10.1.1.1:0 up
Targeted Hello: 10.2.2.2(LDP Id) -> 10.1.1.1, LDP is UP
Graceful restart: not configured and not enabled
Non stop routing: not configured and not enabled
Status TLV support (local/remote) : enabled/supported
  LDP route watch : enabled
  Label/status state machine : established, LruRru
Last local dataplane status rcvd: No fault
Last BFD dataplane status rcvd: Not sent
Last BFD peer monitor status rcvd: No fault
Last local AC circuit status rcvd: No fault
Last local AC circuit status sent: No fault
Last local PW i/f circ status rcvd: No fault
Last local LDP TLV status sent: No fault

```

```
Last remote LDP TLV      status rcvd: No fault
Last remote LDP ADJ      status rcvd: No fault
MPLS VC labels: local 26, remote 21
Group ID: local n/a, remote 16
MTU: local 9000, remote 9000
Remote interface description:
MAC Withdraw: sent:0, received:301
Sequencing: receive disabled, send disabled
Control Word: On (configured: autosense)
```




第 37 章

IGP 自動ルート通知により COE-PCE が開始する SR ポリシー

表 46: 機能の履歴

機能名	リリース情報	機能説明
IGP 自動ルート通知により PCE が開始する SR ポリシー	Cisco IOS XE Bengaluru 17.7.1a Cupertino	この機能により、IGP がポリシーエンドポイントの宛先のダウンストリームにポリシーを自動的に使用するステアリングメカニズムが有効になります。

戦術的な TE ソリューションの一部として、パス計算要素 (PCE) は、セグメントルーティングトラフィックエンジニアリング (SR-TE) ポリシーをプロビジョニングしてリンクの輻輳を軽減できます。

自動ルート通知は、IGP がポリシーエンドポイントの宛先のダウンストリームにポリシーを自動的に使用するステアリングメカニズムです。自動ルート通知は、Cisco Crossworks Optimization Engine (COE) を使用して実行されます。COE は、リアルタイムでネットワークを最適化することで、オペレータがネットワーク使用率を効果的に最大化し、サービス速度を高められるようにします。

PCE はさまざまなネットワーク情報を収集し、リンク輻輳の原因となっているトラフィックフローを特定します。PCE は、それらのフローを迂回させて輻輳を軽減するための適切なパスを計算します。次に、PCE は SR-TE ポリシーを展開し、ステータフルなパス計算要素プロトコル (PCEP) を使用して輻輳の原因となるトラフィックを迂回させ、ポリシーをプロビジョニングします。輻輳が緩和されると、SR-TE ポリシーは削除されます。

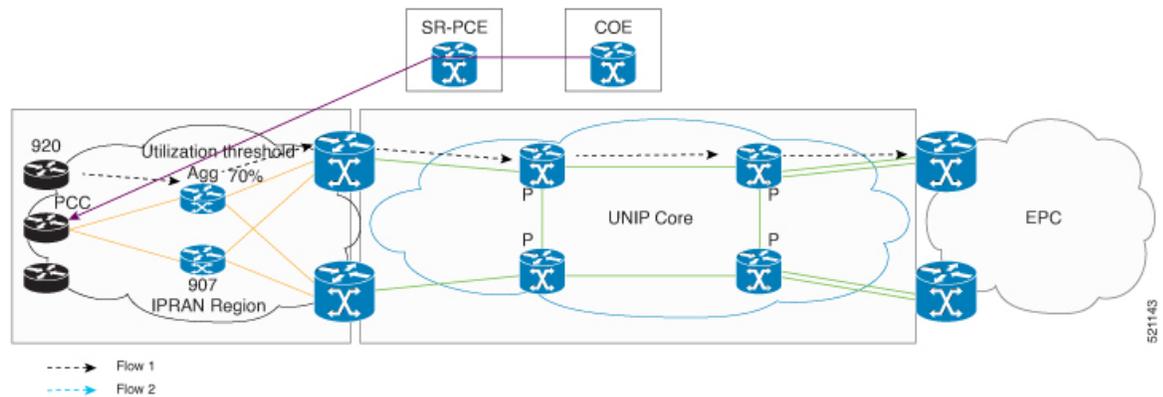
PCEP メッセージには、ヘッドエンドによって展開される SID リストが含まれています。パス計算クライアント (PCC) プロファイルでは、プロファイル ID を使用して、PCEP によってプロビジョニングされたポリシーに対する自動ルート通知をアクティブ化できます。PCE と PCC のプロファイル ID は一致する必要があります。一致しない場合、ポリシーはプロビジョニングされません。たとえば、PCE がプロファイル ID 1 のポリシーをプロビジョニングし、ポリシーがプロビジョニングされているヘッドエンドにも自動ルート通知が設定された PCC プロ

ファイルID1がある場合、COE-PCEが開始したSRポリシーはそのポリシーに対してアクティブ化されます。

- COE-PCE が開始する SR ポリシー (382 ページ)
- SR-TE を介した ECMP (383 ページ)

COE-PCE が開始する SR ポリシー

図 38: COE-PCE が開始する SR ポリシー



上記のトポロジは、SR-PCE ポリシーを COE から開始する仕組みを示しています。

- SR ポリシーは、プロファイル ID を使用して COE で設定されます。
- COE は SR ポリシーを PCE にプッシュし、PCE は SR ポリシーを PCC に転送します。
- PCC のプロファイル ID は、COE-PCE のプロファイル ID と一致します。
- IGP 自動ルート通知は PCC で設定されます。
- ポリシーがプロビジョニングされます。
- データトラフィックは、COE からプッシュされた SR ポリシーに準拠するようになりました。
- 完全な SR ポリシーの操作は、COE でのみ発生します。

PCE が開始する SR ポリシーに関する制約事項

- 最大 500 の ACE がサポートされます。
- ネイティブ COE のみがサポートされます。
- Cisco IOS XE Bengaluru 17.5.1 では、SR 戦略ポリシーに基づく帯域幅の最適化が RSP3 でサポートされています。
- COE を使用した帯域幅の最適化はサポートされていません。

- PIC コアは SR-TE トンネルではサポートされていません。
- SR-TE を介した PIC エッジはサポートされていません。
- Cisco IOS XE Bengaluru 17.5.1 では、SR-TE を介した ECMP が RSP3 でサポートされています。
- 6PE および 6VPE は、3 つおよび 4 つのトランスポートラベルではサポートされません。
- IPv6 はサポートされていません。
- 最大 10,000 の VPNv4 プレフィックス制限がサポートされています。
- BGP LU (RFC 3107) は、AS 内および AS 間ではサポートされません。

SR-TE を介した ECMP

表 47: 機能の履歴

機能名	リリース情報	機能説明
SR-TE ポリシーを介した ECMP	Cisco IOS XE Bengaluru 17.5.1	この機能を使用すると、SR-TE ポリシーを介した ECMP を設定できます。複数のパスの場合、この機能により、ロードバランシングによるローカル輻輳の緩和が可能になります。 この機能は、Cisco ASR 900 RSP3 モジュールのみでサポートされています。

次のセクションでは、ローカルの輻輳を軽減する方法と、ロードバランシングを実現するために SR-TE ポリシーを介して ECMP を展開する方法について説明します。



(注) 複数のパスでロードバランシングされるトラフィックは、HW ロードバランシングされます。

SR-TE ポリシーを介した ECMP に関する制約事項

Cisco ASR 900 RSP3 モジュールは、**sr_5_label_push_enable** および **sr_pfp_enable** テンプレートをサポートしています。さまざまなテンプレートの組み合わせには、次の制約が適用されます。

sr_5_label_push_enable テンプレートの場合：

- 3 つまたは 4 つの TE ラベルを持つ SR-TE トンネルを介した LB では、1 つのサービスラベルのみがサポートされます。このサービスラベルには、L3VPN、L2VPN、6PE、6VPE、および RFC 3107 BGP-LU ラベルが含まれます。
- 6PE および 6VPE は、3 つおよび 4 つの SR-TE トンネルラベルではサポートされません。
- セグメントルーティングは、**enable_portchannel_qos_multiple_active** テンプレートではサポートされません。
- L2VPN/EVPN の宛先に SR-TE トンネルを介して設定された静的ルートがある場合、L2VPN/EVPN サービスの HW ロードバランシングはサポートされません。

sr_pfp_enable テンプレートの場合：

- SR PM HW タイムスタンプはサポートされません。
- VLAN COS マーキングはサポートされません。
- HW ロードバランシングはサポートされません。
- 入力でのポリサーベースの階層型 QOS はサポートされません。
- ショートパイプ トンネリング モードはサポートされません。

その他の制約事項：

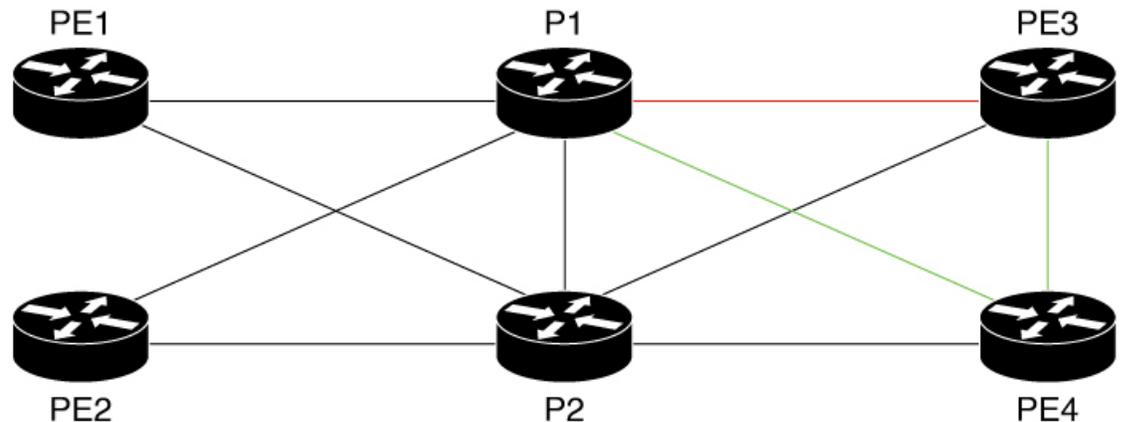
- SR-TE を介した ECMP は、COE ではサポートされません。
- SR-TE トンネルを介した PIC コアはサポートされません。
- SR TE トンネルを介した PIC エッジはサポートされません。
- SR TE トンネルを介した PIC エッジマルチパスはサポートされません。
- W-ECMP はサポートされません。
- ネクストホップ ECMP は SR ポリシー内ではサポートされません。
- ローカル輻輳緩和 (LCM) は、ベストエフォート型トラフィックにのみ適用されます。遅延の影響を受けやすい他のすべてのトラフィックは、安全な SID (Flex Algo 128) を使用します。遅延の影響を受けやすいトラフィックは、LCM トンネルを使用してリダイレクトされません。

ローカル輻輳の緩和

現在のネットワーク展開では、ネットワーク内のすべてのルータが、出入りするトラフィックの量に基づいて輻輳を回避するようにトラフィックをプロビジョニングする機能を備えていることが重要です。この輻輳緩和をプロビジョニングするには、ルータが等コストマルチパス (ECMP) のロードバランシングをサポートしている、つまり、宛先に到達するために使用可能なパスの数に基づいてトラフィックを分散している必要があります。

輻輳緩和は、ルータが戦術的 SR ポリシーを使用して、特定のトラフィックを現在のパスとは異なるパスに移動するのに役立ちます。リンク輻輳のしきい値を超えると、インターフェイスカウンタに基づいてリンクの輻輳をモニターする COE (Cisco Optimization Engine) は、PCE を使用してこれらの戦術的ポリシーをプッシュします。ローカル輻輳緩和 (LCM) に使用されるこれらの PCE 開始戦術ポリシーは、必要に応じて展開され、ベストエフォート型トラフィックのみがこれらの戦術的 SR-TE ポリシーでロードバランシングされます。

図 39: ローカル輻輳緩和の解説



521455

上記のトポロジで、PE1 および PE2 から宛先 PE3 に向かうベストエフォート型トラフィックが P1 に着信し、P1 と PE3 の間のリンクが輻輳していると仮定します。P1 と PE3 の間の輻輳を軽減するには、P1 と PE3 からの ECMP パスが必要です。これはセグメントルーティングでは、P1 から PE3 に複数の戦術的 SR ポリシーを展開し、1 つは直接接続されたリンク P1-PE3 を通し、もう 1 つはパス P1-PE4-PE3 を通すことで実現されます。これらのポリシーは戦術的ポリシーと呼ばれ、これらを介してベストエフォート型トラフィックのロードバランシングを行うことで、ローカル輻輳緩和を回避するために使用されます。LCM はベストエフォート型トラフィックにのみ適用されます。遅延の影響を受けやすい他のすべてのトラフィックは、安全な SID (Flex Algo 128) を使用します。遅延の影響を受けやすいトラフィックは、LCM トンネルを使用してリダイレクトされません。発信元トラフィックは非 LCM トンネルに送られ、safe-SID を持つ中継トラフィックは通常のラベルエントリトラフィックとして扱われ、それに応じて転送されます。

上記のトポロジでは、任意のノードが LCM の戦術的トンネルを展開し、特定のリンク上の輻輳を軽減する場合があります。これらのノードは、LCM トンネルのエンドポイントへ、さらにはトンネルのエンドポイントを越えて、トラフィックを中継したり、場合によっては発信したりします。

PE ノードがトラフィックを発信しており、P ノードが他の場所から発信されたトラフィックの中継ノードであると仮定します。これらの組み合わせに基づいて、考慮する必要があるトラフィックのタイプは次のとおりです。

PE ノードとして、

- L3VPN ベストエフォート型トラフィック
- L2VPN ベストエフォート型トラフィック

- グローバルトラフィック

P ノードとして、

- 非フレキシブルアルゴリズム 0 ラベルに着信するトラフィックは、ラベルルックアップのエントリスワップとして扱われます。
- フレキシブルアルゴリズム 0 ラベルに着信するトラフィックは、スワップケースとして扱われるか、輻輳に基づいてその発信リンク用に作成された LCM がある場合、ラベルのポップおよびプッシュスタックに変換される可能性があります。

LCM トンネルがプッシュする必要のある TE ラベルの数に基づいて、TE ラベルの外側のラベルの数は 1 または 2 のいずれかになります（サービ斯拉ベル）。

ロードバランシング

ヘッドエンドでロードバランシングの対象となるさまざまなタイプのトラフィックを下記に示します。ここでのトラフィックタイプには、ベストエフォートと遅延の影響を受けやすいものの両方が含まれます。

PE ノードとして、

- L3VPN トラフィック
- L2VPN トラフィック
- グローバルトラフィック

P ノードとして、

- 着信トラフィックは、ラベルルックアップに基づいて処理されます。

自動ルート通知

自動ルート通知または帯域幅最適化は、輻輳したリンクからトラフィックをステアリングし、ネットワークをより有効に活用するために使用します。

PCEP メッセージには、ヘッドエンドによって展開される SID リストが含まれています。パス計算クライアント (PCC) プロファイルでは、プロファイル ID を使用して、PCEP によってインスタンス化されたポリシーに対する自動ルート通知をアクティブ化できます。たとえば、PCE がプロファイル ID 1 のポリシーをインスタンス化し、ポリシーがインスタンス化されているヘッドエンドに自動ルート通知が設定された PCC プロファイル ID 1 がある場合、PCE が開始した SR ポリシーはそのポリシーに対してアクティブ化されます。

自動ルート通知は、厳密な SID で作成されたポリシーと厳密でない SID で作成されたポリシーの両方で設定できます。厳密な SID (A とする) と厳密でない SID (B とする) で作成されたポリシーでの自動ルーティング設定の主な違いは、A ではルックアップエントリが RIB でのみプログラムされるのに対し、B ではルックアップエントリが RIB と柔軟なアルゴリズムラベル 0 の LFIB でプログラムされることです。

スタティック ルートの設定

同じエンドポイントを持つ異なるトンネルを使用して同じ宛先への静的ルートを追加することで、設定したトンネルを介したルートのロードバランシングが形成されます。これは、すべてのタイプのトラフィックに適用されます。

SR ポリシー内のネクストホップ ECMP

一連の SID を持つ宛先に対して作成された SR ポリシーがあり、その SR ポリシーのヘッドエンドにネクストホップに到達するための複数の等しいパスがある場合、SR ポリシー内のネクストホップに到達するための ECMP は形成されません。

IGP 自動ルート通知により の の設定

```
pce
  address ipv4 10.13.13.13
  segment-routing traffic-eng
  peer ipv4 10.1.1.1
  segment-list name ssl

  policy 100
  binding-sid mpls 15999
  color 100 end-point ipv4 10.12.12.12
  candidate-paths
  preference 10
  dataplane mpls
profile-id 100
```

ここで、PCE が開始した OSPF 自動ルート通知を PCE から PCC にプッシュするには、PCE と PCC のプロファイル ID を一致させる必要があります。次の設定は PCC 設定を示しており、プロファイル ID が PCE と一致しているため、自動ルート通知が有効になっています。

```
segment-routing traffic-eng

  pcc
  pce address 10.13.13.13 source-address 10.1.1.1
profile 100
  autoroute
  include all
```

自動ルート通知による SR ポリシーの確認

```
ASR903-R1#show segment-routing traffic-eng policy all

Name: *10.12.12.12|100 (Color: 100 End-point: 10.12.12.12)
Owners : PCEP
Status:
Admin: up, Operational: up for 66:41:16 (since 09-18 16:56:50.444)
Candidate-paths:
Preference 10 (PCEP):
PCC profile: 100
Dynamic (pce 10.13.13.13) (active)
Metric Type: TE, Path Accumulated Metric: 5
16003 [Prefix-SID, 10.3.3.3]
16012 [Prefix-SID, 10.12.12.12]
Attributes:
Binding SID: 15999
```

```

Allocation mode: explicit
State: Programmed
Autoroute:
Include all

```

IGP の ISIS 自動ルートの確認

IGP の ISIS 自動ルートを確認するには、次の 2 つのコマンドを使用します。

```

ASR903-R1#show ip cef 10.12.12.12 -----□IGP ROUTE
10.12.12.12/32
nexthop 10.12.12.12 Tunnel65536 -----□Tunnel pushed for IGP ROUTE

ASR903-R1# show ip cef 10.12.12.12 internal
10.12.12.12/32, epoch 3, RIB[I], refcnt 6, per-destination sharing
sources: RIB
feature space:
  IPRM: 0x00028000
  Broker: linked, distributed at 1st priority
  LFD: 10.12.12.12/32 0 local labels
  contains path extension list
ifnums:
  Tunnel65536(64)
path list 3C97B678, 3 locks, per-destination, flags 0x49 [shble, rif, hwc]
path 3E393010, share 1/1, type attached nexthop, for IPv4
  MPLS short path extensions: [rib | lblmrg | srlbl] MOI flags = 0x1 label
implicit-null
  nexthop 10.12.12.12 Tunnel65536, IP midchain out of Tunnel65536 2FFE3D00
output chain:
  IP midchain out of Tunnel65536 2FFE3D00
  label [16012|16012]
  FRR Primary (0x3D9D4CE0)
    <primary: TAG adj out of Port-channell, addr 10.100.0.2 3C9559C0>
    <repair: TAG adj out of BDI1110, addr 10.111.0.2 3C954FC0>

```

SR ポリシーのトンネル ID の確認

```

ASR903-R1# show segment-routing traffic-eng policy name margin detail
Name: Margin (Color: 1000 End-point: 10.12.12.12)
Owners : CLI
Status:
  Admin: up, Operational: up for 00:50:52 (since 09-16 11:00:06.697)
Candidate-paths:
  Preference 10 (CLI):
    Dynamic (pce 10.13.13.13) (active)
    Metric Type: TE, Path Accumulated Metric: 5
    16012 [Prefix-SID, 10.12.12.12]
Attributes:
  Binding SID: 15900
  Allocation mode: explicit
  State: Programmed
IPv6 caps enabled
Tunnel ID: 65536 (Interface Handle: 0x15B)
Per owner configs:
  CLI
  Binding SID: 15900
Stats:
  Packets: 535473 Bytes: 805338440
Event history:
  Timestamp          Client          Event type      Context: Value
  -----          -
  09-16 11:00:06.377  CLI            Policy created  Name: CLI
  09-16 11:00:06.418  CLI            Set colour     Colour: 1000

```

```
09-16 11:00:06.418 CLI Set end point End-point: 10.12.12.12
09-16 11:00:06.446 CLI Set binding SID BSID: Binding SID set
09-16 11:00:06.577 CLI Set dynamic Path option: dynamic
09-16 11:00:06.620 CLI BSID allocated FWD: label 15900
09-16 11:00:06.637 FH Resolution Policy state UP Status: PATH RESOLVED
09-16 11:00:06.697 FH Resolution Policy state DOWN Status: PATH NOT RESOLVED

09-16 11:00:06.706 CLI Set dynamic pce Path option: dynamic pce
09-16 11:00:07.240 FH Resolution Policy state UP Status: PATH RESOLVED
09-16 11:00:09.520 FH Resolution REOPT triggered Status: REOPTIMIZED
```




第 38 章

Cisco ACI から SR-MPLS ハンドオフにおける DC-PE ルータ

SR-MPLS ハンドオフは、セグメントルーティング (SR) MPLS アンダーレイを使用して Cisco ACI から WAN への相互接続を可能にする相互接続オプションです。

Cisco IOS XE 17.14.1a 以降、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータおよび Cisco Catalyst 8500 シリーズ エッジプラットフォームは、ACI から SR-MPLS ハンドオフ相互接続の中間 DC-PE デバイスとして使用できます。

- [前提条件 \(391 ページ\)](#)
- [機能制限 \(391 ページ\)](#)
- [ACI から SR-MPLS ハンドオフにおける DC-PE ルータに関する情報 \(392 ページ\)](#)
- [サポートされるプラットフォーム \(393 ページ\)](#)
- [DC-PE ルータの設定方法 \(393 ページ\)](#)
- [DC-PE ルータ設定の確認 \(401 ページ\)](#)
- [トラブルシューティングとデバッグ \(404 ページ\)](#)
- [Cisco ACI から SR-MPLS ハンドオフにおける DC-PE ルータの機能情報 \(405 ページ\)](#)

前提条件

ACI から SR-MPLS ハンドオフにおける DC-PE ルータに関する特定の前提条件はありません。

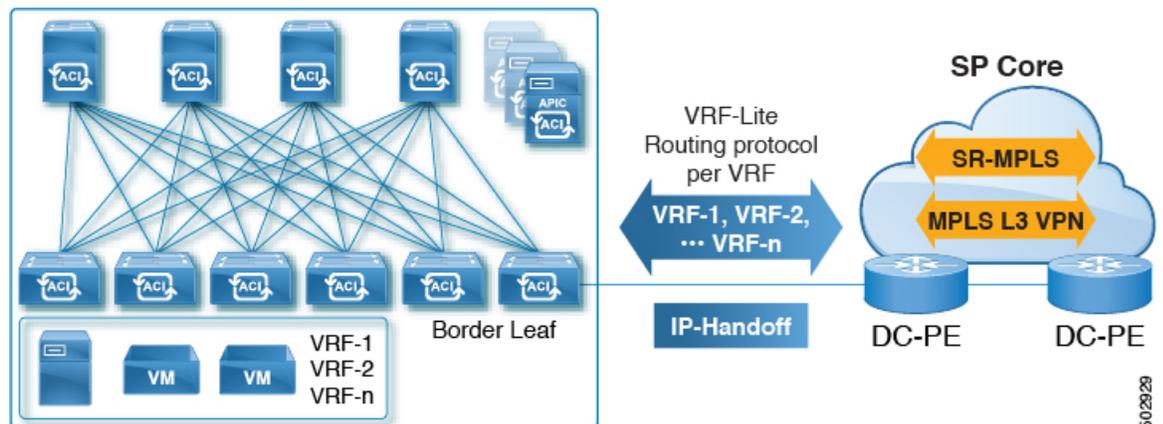
機能制限

- iBGP は、DC-PE とボーダー/リモートリーフ間ではサポートされていません。
- ルータ ID は、すべての境界リーフスイッチと DC-PE で一意である必要があります。

ACI から SR-MPLS ハンドオフにおける DC-PE ルータに関する情報

SR/MPLS ハンドオフは、セグメントルーティング（SR）MPLS アンダーレイを使用して Cisco ACI ファブリックから WAN への相互接続を可能にする相互接続オプションです。SR/MPLS は、SP コアでははるかに一般的であるため、他の既知のソリューションよりも優れたソリューションです。このソリューションには、次の利点があります。

- DC と SP 間の統合トランスポートとポリシー
- 複数の VRF の単一コントロールプレーンセッション
- DC から制御される SP コアのトラフィック エンジニアリング



Cisco ACI ファブリックおよび基盤となる ACI から SR-MPLS ハンドオフ相互接続の詳細については、次の資料を参照してください。

- [ACI SRMPLS ハンドオフホワイトペーパー](#)
- ACI SRMPLS アーキテクチャ：
 1. [Cisco ACI から SR-MPLS ハンドオフの検証済み設計：概要](#)
 2. [Cisco ACI から SR-MPLS ハンドオフの検証済み設計：テナント設定](#)
 3. [ACI ファブリック L3Out ホワイトペーパー](#)
- [ACI SRMPLS アーキテクチャ/サンプルユースケース](#)

サポートされるプラットフォーム

Cisco IOS XE 17.14.1a 以降、次のルータは、ACI から SR-MPLS ハンドオフ相互接続の DC-PE デバイスとして設定できます。

- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ
- Cisco Catalyst 8500 シリーズ エッジプラットフォーム

DC-PE ルータの設定方法

DC-PE ルータで VRF と BGP を設定するには、次の手順を実行します。

DC-PE ルータでの VRF の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *vpn-route-distinguisher*
5. **address-family ipv4** [**multicast** | **unicast**]
6. **route-target** {**export** | **import** | **both**} *route-target-ext-community*
7. **route-target** {**export** | **import** | **both**} *route-target-ext-community* **stitching**
8. **exit-address-family**
9. **address-family ipv6** [**multicast** | **unicast**]
10. **route-target** {**export** | **import** | **both**} *route-target-ext-community*
11. **route-target** {**export** | **import** | **both**} *route-target-ext-community* **stitching**
12. **exit-address-family**
13. **end**

手順の詳細

手順

	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 モードを開始します。パスワードの入力を求められたら、入力します。

	コマンドまたはアクション	目的
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	vrf definition vrf-name 例： Device(config)# vrf definition test	指定した VRF インスタンスの VRF コンフィギュレーション モードを開始します。
ステップ 4	rd vpn-route-distinguisher 例： Device(config-vrf)# rd 65000:1	VRF インスタンスのルート識別子を指定します。
ステップ 5	address-family ipv4 [multicast unicast] 例： Device(config-vrf)# address-family ipv4	IPv4 アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 6	route-target {export import both} route-target-ext-community 例： Device(config-vrf-af)# route-target import 1:1 例： Device(config-vrf-af)# route-target export 2:2	指定した VRF のインポートまたはエクスポート、あるいはインポートとエクスポートの両方のルートターゲットコミュニティのリストを作成します。 自律システム番号および任意の数 (xxx:y)、または IP アドレスおよび任意の数 (A.B.C.D:y) のいずれかを入力します。
ステップ 7	route-target {export import both} route-target-ext-community stitching 例： Device(config-vrf-af)# route-target import 3:3 stitching 例： Device(config-vrf-af)# route-target export 4:4 stitching	VRF の EVPN ルートターゲットコミュニティのインポートまたはエクスポート、あるいはインポートとエクスポートの両方を設定します。
ステップ 8	exit-address-family 例： Device(config-vrf-af)# exit-address-family	VRF アドレス ファミリ コンフィギュレーション モードを終了し、VRF 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	address-family ipv6 [multicast unicast] 例： Device(config-vrf)# address-family ipv6	IPv6 アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 10	route-target {export import both} route-target-ext-community 例：	指定した VRF のインポートまたはエクスポート、あるいはインポートとエクスポートの両方のルートターゲットコミュニティのリストを作成します。

	コマンドまたはアクション	目的
	Device(config-vrf-af)# route-target import 1:1 例 : Device(config-vrf-af)# route-target export 2:2	自律システム番号および任意の数 (xxx:y) 、または IP アドレスおよび任意の数 (A.B.C.D:y) のいずれかを入力します。
ステップ 11	route-target {export import both} route-target-ext-community stitching 例 : Device(config-vrf-af)# route-target import 3:3 stitching 例 : Device(config-vrf-af)# route-target export 4:4 stitching	VRF の EVPN ルートターゲットコミュニティのインポートまたはエクスポート、あるいはインポートとエクスポートの両方を設定します。
ステップ 12	exit-address-family 例 : Device(config-vrf-af)# exit-address-family	VRF アドレス ファミリ コンフィギュレーション モードを終了し、VRF コンフィギュレーションモードを開始します。
ステップ 13	end 例 : Device(config-vrf)# end	特権 EXEC モードに戻ります。

例

次に、DC-PE ルータに必要な VRF 設定の例を示します。

```
vrf definition test
 rd 65000:1
  address-family ipv4
    route-target import 1:1
    route-target export 2:2
    route-target import 3:3 stitching
    route-target export 4:4 stitching
  exit
  address-family ipv6
    route-target import 1:1
    route-target export 2:2
    route-target import 3:3 stitching
    route-target export 4:4 stitching
  exit
```

DC-PE ルータでの BGP の設定

手順の概要

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

3. **routerbgpas-number**
4. **neighbor dc-border-leaf-address remote-as number**
5. **neighbor wan-router-address remote-as number**
6. **address-family l2vpn evpn**
7. **import vpv4 unicast [re-originate]**
8. **import vpv6 unicast [re-originate]**
9. **neighbor ip-address activate**
10. **neighbor ip-address send-community [both | extended | standard]**
11. **exit-address-family**
12. **address-family vpv4**
13. **import l2vpn evpn [re-originate]**
14. **neighbor ip-address activate**
15. **neighbor ip-address send-community [both | extended | standard]**
16. **neighbor {ip-address | peer-group-name} next-hop-self [all]**
17. **exit-address-family**
18. **address-family vpv6**
19. **import l2vpn evpn [re-originate]**
20. **neighbor ip-address activate**
21. **neighbor ip-address send-community [both | extended | standard]**
22. **neighbor {ip-address | peer-group-name} next-hop-self [all]**
23. **exit-address-family**
24. **address-family ipv4 vrf vrf-name**
25. **maximum-paths eibgp number**
26. **exit-address-family**
27. **address-family ipv6 vrf vrf-name**
28. **maximum-paths eibgp number**
29. **exit-address-family**
30. **end**

手順の詳細

手順

	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。パスワードを入力します（要求された場合）。
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	routerbgpas-number 例：	BGP ルーティングプロセスを設定し、ルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	Device(config)# router bgp 1	
ステップ 4	neighbor dc-border-leaf-address remote-as number 例： Device(config-router)# neighbor 1.1.1.1 remote-as 2	EVPN ネットワーク内のマルチプロトコル BGP ネイバーを定義します。 スパインスイッチの IP アドレスをネイバー IP アドレスとして使用します。これにより、スパインスイッチが BGP ネイバーとして設定されます。
ステップ 5	neighbor wan-router-address remote-as number 例： Device(config-router)# neighbor 2.2.2.2 remote-as 1	外部 MPLS ネットワークのマルチプロトコル BGP ネイバーを定義します。 外部 MPLS ネットワークピアの IP アドレスをネイバー IP アドレスとして使用します。これにより、外部 MPLS ネットワークピアが BGP ネイバーとして設定されます。
ステップ 6	address-family l2vpn evpn 例： Device(config-router)# address-family l2vpn evpn	L2VPN アドレスファミリを指定し、アドレスファミリ コンフィギュレーションモードを開始します。
ステップ 7	import vpnv4 unicast [re-originate] 例： Device(config-router-af)# import vpnv4 unicast re-originate	外部ピアから EVPN アドレスファミリにインポートされた VPNv4 ルートを EVPN ルートとして再生成し、EVPN ファブリック内で配布します。
ステップ 8	import vpnv6 unicast [re-originate] 例： Device(config-router-af)# import vpnv6 unicast re-originate	外部ピアから EVPN アドレスファミリにインポートされた VPNv6 ルートを EVPN ルートとして再生成し、EVPN ファブリック内で配布します。
ステップ 9	neighbor ip-address activate 例： Device(config-router-af)# neighbor 1.1.1.1 activate	BGP ネイバーからの情報交換を有効にします。 スパインスイッチの IP アドレスをネイバー IP アドレスとして使用します。
ステップ 10	neighbor ip-address send-community [both extended standard] 例： Device(config-router-af)# neighbor 1.1.1.1 send-community both	BGP ネイバーに送信したコミュニティ属性を指定します。 スパインスイッチの IP アドレスをネイバー IP アドレスとして使用します。 (注) extended キーワードまたは both キーワードを使用します。 standard キーワードを使用すると、外部接続を確立できません。

	コマンドまたはアクション	目的
ステップ 11	exit-address-family 例： Device(config-router-af)# exit-address-family	アドレスファミリー コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻ります。
ステップ 12	address-family vpnv4 例： Device(config-router)# address-family vpnv4	VPNv4 アドレス ファミリーを指定し、アドレスファミリー コンフィギュレーションモードを開始します。
ステップ 13	import l2vpn evpn [re-originate] 例： Device(config-router-af)# import l2vpn evpn re-originate stitching-rt	EVPN ファブリックから VPNv4 アドレスファミリーにインポートされた EVPN ルートを VPNv4 ルートとして再生成し、それらを外部ネットワークに配布します。
ステップ 14	neighbor ip-address activate 例： Device(config-router-af)# neighbor 2.2.2.2 activate	BGP ネイバーからの情報交換を有効にします。 外部 MPLS ネットワークルータの IP アドレスをネイバー IP アドレスとして使用します。
ステップ 15	neighbor ip-address send-community [both extended standard] 例： Device(config-router-af)# neighbor 2.2.2.2 send-community both	BGP ネイバーに送信したコミュニティ属性を指定します。 外部 MPLS ネットワークルータの IP アドレスをネイバー IP アドレスとして使用します。 (注) extended キーワードまたは both キーワードを使用します。standard キーワードを使用すると、外部接続を確立できません。
ステップ 16	neighbor {ip-address peer-group-name} next-hop-self [all] 例： Device(config-router-af)# neighbor 2.2.2.2 next-hop-self all	ルータを BGP スピーキングネイバーまたはピアグループのネクストホップとして設定します。 all キーワードは、EVPN ファブリックと MPLS ネットワークが同じ BGP 自律システム番号にある、iBGP を介した外部接続を実装する場合に必須です。 EVPN ファブリックと MPLS ネットワークが異なる BGP 自律システム番号にある、eBGP を介した外部接続を実装する場合は、all キーワードは任意です。
ステップ 17	exit-address-family 例： Device(config-router-af)# exit-address-family	アドレスファミリー コンフィギュレーションモードを終了し、ルータ コンフィギュレーション モードに戻ります。
ステップ 18	address-family vpnv6 例： Device(config-router)# address-family vpnv6	VPNv6 アドレス ファミリーを指定し、アドレスファミリー コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 19	import l2vpn evpn [re-originate] 例： Device(config-router-af)# import l2vpn evpn re-originate stitching-rt	EVPN ファブリックから VPNv6 アドレスファミリにインポートされた EVPN ルートを VPNv6 ルートとして再生成し、それらを外部ネットワークに配布します。
ステップ 20	neighbor ip-address activate 例： Device(config-router-af)# neighbor 2.2.2.2 activate	BGP ネイバーからの情報交換を有効にします。 スパインスイッチの IP アドレスをネイバー IP アドレスとして使用します。
ステップ 21	neighbor ip-address send-community [both extended standard] 例： Device(config-router-af)# neighbor 2.2.2.2 send-community both	BGP ネイバーに送信したコミュニティ属性を指定します。 スパインスイッチの IP アドレスをネイバー IP アドレスとして使用します。 (注) extended キーワードまたは both キーワードを使用します。 standard キーワードを使用すると、外部接続を確立できません。
ステップ 22	neighbor {ip-address peer-group-name} next-hop-self [all] 例： Device(config-router-af)# neighbor 2.2.2.2 next-hop-self all	ルータを BGP スピーキングネイバーまたはピアグループのネクストホップとして設定します。 all キーワードは、EVPN ファブリックと MPLS ネットワークが同じ BGP 自律システム番号にある、iBGP を介した外部接続を実装する場合に必須です。 EVPN ファブリックと MPLS ネットワークが異なる BGP 自律システム番号にある、eBGP を介した外部接続を実装する場合は、 all キーワードは任意です。
ステップ 23	exit-address-family 例： Device(config-router-af)# exit-address-family	アドレスファミリ コンフィギュレーションモードを終了し、ルータ コンフィギュレーションモードに戻ります。
ステップ 24	address-family ipv4 vrf vrf-name 例： Device(config-router)# address-family ipv4 vrf test	ルータをアドレスファミリ コンフィギュレーションモードにします。 別々の VRF マルチパス設定は、固有ルート識別子によって分離されます。
ステップ 25	maximum-paths eibgp number 例： Device(config-router-af)# maximum-paths eibgp 16	ルーティングテーブルにインストールできるパラレルの iBGP ルートおよび eBGP ルートの数を設定します。 (注) maximum-paths eibgp コマンドは、IPv4 VRF アドレスファミリ コンフィギュレーションモードでのみ設定できます。

	コマンドまたはアクション	目的
ステップ 26	exit-address-family 例： Device(config-router-af)# exit-address-family	アドレスファミリー コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻ります。
ステップ 27	address-family ipv6 vrf vrf-name 例： Device(config-router)# address-family ipv6 vrf test	ルータをアドレスファミリー コンフィギュレーション モードにします。 別々の VRF マルチパス設定は、固有ルート識別子によって分離されます。
ステップ 28	maximum-paths eibgp number 例： Device(config-router-af)# maximum-paths eibgp 16	ルーティング テーブルにインストールできるパラレルの iBGP ルートおよび eBGP ルートの数を設定します。 (注) maximum-paths eibgp コマンドは、IPv6 VRF アドレスファミリー コンフィギュレーション モードでのみ設定できます。
ステップ 29	exit-address-family 例： Device(config-vrf-af)# exit-address-family	VRF アドレスファミリー コンフィギュレーション モードを終了し、VRF コンフィギュレーション モードに戻ります。
ステップ 30	end 例： Device(config-vrf)# end	特権 EXEC モードに戻ります。

例

次に、DC-PE ルータに必要な VRF 設定の例を示します。

```
router bgp 1
  neighbor 1.1.1.1 remote-as 2
  neighbor 2.2.2.2 remote-as 1
  address-family l2vpn evpn
    import vpv4 unicast re-originate
    import vpv6 unicast re-originate
    neighbor 1.1.1.1 active
    neighbor 1.1.1.1 send-community both
  exit
  address-family vpv4
    import l2vpn evpn re-originate stitching-rt
    neighbor 2.2.2.2 active
    neighbor 2.2.2.2 send-community both
    neighbor 2.2.2.2 next-hop-self all
  exit
  address-family vpv6
    import l2vpn evpn re-originate stitching-rt
    neighbor 2.2.2.2 active
    neighbor 2.2.2.2 send-community both
```

```
neighbor 2.2.2.2 next-hop-self all
exit
address-family ipv4 vrf test
  maximum-paths eibgp 16
exit
address-family ipv6 vrf test
  maximum-paths eibgp 16
exit
```

DC-PE ルータ設定の確認

ここでは、DC-PE ルータの設定を確認するために使用できる show コマンドについて説明します。

ACI からの IPv4 および IPv6 ルートの確認

次のコマンドを使用して、ACI からの IPv4 ルートを確認します。

```
Router#show bgp l2vpn evpn route-type 5 0 99.1.2.0 24
BGP routing table entry for [5][2:2][0][24][99.1.2.0]/17, version 2
Paths: (1 available, best #1, table EVPN-BGP-Table)
  Not advertised to any peer
  Refresh Epoch 1
  65000 65001
    2.2.2.2 (via default) from 5.5.5.5 (5.5.5.5)
      Origin incomplete, localpref 100, valid, external, best
      EVPN ESI: 00000000000000000000, Gateway Address: 0.0.0.0, VNI Label 0, MPLS VPN
      Label 19
      Extended Community: RT:2:2 Color:10
      rx pathid: 0, tx pathid: 0x0
      Updated on Feb 27 2024 15:46:31 PST
```

```
Router#show bgp vpnv4 uni all 99.1.2.0
BGP routing table entry for 6:6:99.1.2.0/24, version 2
Paths: (1 available, best #1, table red)
  Advertised to update-groups:
    1
  Refresh Epoch 1
  65000 65001, imported path from [5][2:2][0][24][99.1.2.0]/17 (global)
    2.2.2.2 (via default) from 5.5.5.5 (5.5.5.5)
      Origin incomplete, localpref 100, valid, external, best
      Extended Community: RT:2:2 Color:10
      mpls labels in/out IPv4 VRF Aggr:19/19
      rx pathid: 0, tx pathid: 0x0
      Updated on Feb 27 2024 15:46:31 PST
```

```
Router#show ip route vrf red 99.1.2.0
Routing Table: red
Routing entry for 99.1.2.0/24
Known via "bgp 65100", distance 20, metric 0
Tag 65000, type external
Last update from 2.2.2.2 00:07:23 ago
Routing Descriptor Blocks:
* 2.2.2.2 (default), from 5.5.5.5, 00:07:23 ago
opaque_ptr 0x7F055237F160
Route metric is 0, traffic share count is 1
```

```
AS Hops 2
Route tag 65000
MPLS label: 19
```

次のコマンドを使用して、ACI からの IPv6 ルートを確認します。

```
Router#show bgp l2vpn evpn route-type 5 0 2001::99:1:2:0 112
BGP routing table entry for [5][2:2][0][112][2001::99:1:2:0]/29, version 4
Paths: (1 available, best #1, table EVPN-BGP-Table)
  Not advertised to any peer
  Refresh Epoch 1
  65000 65001
    2.2.2.2 (via default) from 5.5.5.5 (5.5.5.5)
      Origin incomplete, localpref 100, valid, external, best
      EVPN ESI: 00000000000000000000, Gateway Address:::,VNI Label 0,MPLS VPN Label 21
      Extended Community: RT:2:2 Color:10
      rx pathid: 0, tx pathid: 0x0
      Updated on Feb 27 2024 15:46:31 PST
```

```
Router#show bgp vpnv6 uni all 2001::99:1:2:0/112
BGP routing table entry for [6:6]2001::99:1:2:0/112, version 2
Paths: (1 available, best #1, table red)
  Advertised to update-groups:
    1
  Refresh Epoch 1
  65000 65001, imported path from [5][2:2][0][112][2001::99:1:2:0]/29 (global)
    ::FFFF:2.2.2.2 (via default) from 5.5.5.5 (5.5.5.5)
      Origin incomplete, localpref 100, valid, external, best
      Extended Community: RT:2:2 Color:10
      mpls labels in/out IPv6 VRF Aggr:20/21
      rx pathid: 0, tx pathid: 0x0
      Updated on Feb 27 2024 15:46:31 PST
```

```
Router#show ipv6 route vrf red 2001::99:1:2:0/112
Routing entry for 2001::99:1:2:0/112
Known via "bgp 65100", distance 20, metric 0
Tag 65000, type external
Route count is 1/1, share count 0
Routing paths:
  2.2.2.2%default indirectly connected
  Route metric is 0, traffic share count is 1
  MPLS label: 21
  From ::FFFF:5.5.5.5
  opaque_ptr 0x7F05523C42C8
  Last updated 00:10:33 ago
```

WAN からの IPv4 および IPv6 ルートの確認

次のコマンドを使用して、WAN からの IPv4 ルートを確認します。

```
Router#show bgp vpnv4 uni vrf red 13.13.13.13
BGP routing table entry for 6:6:13.13.13.13/32, version 19
Paths: (1 available, best #1, table red)
Flag: 0x100
  Not advertised to any peer
  Refresh Epoch 1
  65013, imported path from 12:12:13.13.13.13/32 (global)
    12.12.12.12 (metric 30) (via default) from 7.7.7.7 (7.7.7.7)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
```

```
Extended Community: RT:12:12 Color:10
Originator: 12.12.12.12, Cluster list: 7.7.7.7
mpls labels in/out nolabel/18
binding SID: 22 (color - 10) (state - UP)
rx pathid: 0, tx pathid: 0x0
Updated on Feb 27 2024 15:46:32 PST
```

```
Router#show bgp l2vpn evpn route-type 5 0 13.13.13.13 32
BGP routing table entry for [5][6:6][0][32][13.13.13.13]/17, version 18
Paths: (1 available, best #1, table EVPN-BGP-Table)
Advertised to update-groups:
 1
  Refresh Epoch 1
  65013, imported path from base
    12.12.12.12 (metric 30) (via default) from 7.7.7.7 (7.7.7.7)
    Origin incomplete, metric 0, localpref 100, valid, internal, best
    EVPN ESI: 00000000000000000000, Gateway Address: 0.0.0.0, local vtep: 0.0.0.0, VNI
    Label 0, MPLS VPN Label 18, MPLS VPN Local Label 19
    Extended Community: RT:2:2 RT:4:4 Color:10
    Originator: 12.12.12.12, Cluster list: 7.7.7.7
    rx pathid: 0, tx pathid: 0x0
    Updated on Feb 27 2024 15:46:32 PST
```

```
Router#show ip route vrf red 13.13.13.13
Routing Table: red
Routing entry for 13.13.13.13/32
Known via "bgp 65100", distance 200, metric 0
Tag 65013, type internal
Routing Descriptor Blocks:
* Binding Label: 22, from 7.7.7.7, 00:07:48 ago
opaque_ptr 0x7F055237ED70
Route metric is 0, traffic share count is 1
AS Hops 1
Route tag 65013
MPLS label: 18
MPLS Flags: MPLS Required
```

次のコマンドを使用して、WAN からの IPv6 ルートを確認します。

```
Router#show bgp vpnv6 uni vrf red 2001::13:13:13:13/128
BGP routing table entry for [6:6]2001::13:13:13:13/128, version 19
Paths: (1 available, best #1, table red)
Flag: 0x100
Not advertised to any peer
Refresh Epoch 1
65013, imported path from [12:12]2001::13:13:13:13/128 (global)
::FFFF:12.12.12.12 (metric 30) (via default) from 7.7.7.7 (7.7.7.7)
Origin incomplete, metric 0, localpref 100, valid, internal, best
Extended Community: RT:12:12 Color:10
Originator: 12.12.12.12, Cluster list: 7.7.7.7
mpls labels in/out nolabel/20
binding SID: 22 (color - 10) (state - UP)
rx pathid: 0, tx pathid: 0x0
Updated on Feb 27 2024 15:46:32 PST
```

```
Router#show bgp l2vpn evpn route-type 5 0 2001::13:13:13:13 128
BGP routing table entry for [5][6:6][0][128][2001::13:13:13:13]/29, version 12
Paths: (1 available, best #1, table EVPN-BGP-Table)
Advertised to update-groups:
 1
  Refresh Epoch 1
  65013, imported path from base
```

```

::FFFF:12.12.12.12 (metric 30) (via default) from 7.7.7.7 (7.7.7.7)
  Origin incomplete, metric 0, localpref 100, valid, internal, best
  EVPN ESI: 00000000000000000000, Gateway Address: ::, local vtep: 0.0.0.0, VNI Label
  0, MPLS VPN Label 20, MPLS VPN Local Label 20
  Extended Community: RT:2:2 RT:4:4 Color:10
  Originator: 12.12.12.12, Cluster list: 7.7.7.7
  rx pathid: 0, tx pathid: 0x0
  Updated on Feb 27 2024 15:46:32 PST

```

```

Router#show ipv6 route vrf red 2001::13:13:13:13/128
Routing entry for 2001::13:13:13:13/128
Known via "bgp 65100", distance 200, metric 0
Tag 65013, type internal
Route count is 1/1, share count 0
Routing paths:
Bind Label: 22 indirectly connected
Route metric is 0, traffic share count is 1
MPLS label: 20
From ::FFFF:7.7.7.7
opaque_ptr 0x7F05523C3ED8
Last updated 00:10:03 ago

```

トラブルシューティングとデバッグ

次のデバッグコマンドを使用すると、BGP ラベルマネージャのデバッグに必要なデバッグを有効にできます。

```

debug bgp lmm address-family vpnv4
debug bgp lmm address-family vpnv6

```

次に、**debug bgp lmm address-family vpnv4/6** コマンドの出力例を示します。

```

*Jul 18 21:32:09.835: BGP_LMM (VPNv4): Add update info for 1:1:3.3.3.0/24, neighbor
1.1.1.3, NH unchanged (no), topology neighbor labeled (yes)
*Jul 18 21:34:48.577: BGP_LMM (VPNv6): Add update info for [1:1]3333::/120, neighbor
1.1.1.3, NH unchanged (no), topology neighbor labeled (yes)
*Jul 18 21:32:09.835: BGP_LMM (VPNv4): Allocated and installed a per VRF aggregate label
  10 for vrf red, address family ipv4"
*Jul 18 21:32:09.835: BGP_LMM (VPNv4): Allocated and installed a per VRF aggregate label
  11 for vrf red, address family ipv6"

```

次の **debug** コマンドを使用して、BGP EVPN から L3VPN へのインポート/再発信をデバッグできます。

```

debug bgp all import updates
debug bgp all import events

```

次に、**debug bp all import** コマンドの出力例を示します。

```

*Jul 21 14:31:22.693: BGP VPN-IMP: red:VPNv4 Unicast:base 1:1:3.3.3.0/24 Exporting doing
PATHS.
*Jul 21 14:31:22.693: BGP VPN-IMP: VPNv4 Unicast:base Building ETL from VPN
*Jul 21 14:31:22.693: BGP VPN-IMP: VPNv4 Unicast:base GBL Building ETL.
*Jul 21 14:31:22.693: BGP VPN-IMP: VPNv4 Unicast:base -> global:IPv4 Unicast:base Creating
Import Topo.

```

```
*Jul 21 14:31:22.693: BGP VPN-IMP: VPNv4 Unicast:base -> global:IPv4 Unicast:base GBL
Adding topology IPv4 Unicast to ETL.
*Jul 21 14:31:22.693: BGP VPN-IMP: VPNv4 Unicast:base -> global:IPv4 Multicast:base
Creating Import Topo.
*Jul 21 14:31:22.693: BGP VPN-IMP: VPNv4 Unicast:base -> global:IPv4 Multicast:base GBL
Adding to ETL.
*Jul 21 14:31:22.693: BGP VPN-IMP: VPNv4 Unicast:base Building GBL ETL done.
*Jul 21 14:31:22.693: BGP VPN-IMP: VPNv4 Unicast:base L2VPN E-VPN AF_PRIV Building ETL.
```

Cisco ACI から SR-MPLS ハンドオフにおける DC-PE ルータの機能情報

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 48: Cisco ACI から SR-MPLS ハンドオフにおける DC-PE ルータの機能情報

機能名	リリース	機能情報
Cisco ACI から SR-MPLS ハンドオフにおける DC-PE ルータ	Cisco IOS XE 17.14.1a	Cisco IOS XE 17.14.1a 以降、Cisco ASR 1000 シリーズ アグリゲーションサービス ルータ および Cisco Catalyst 8500 シリーズ エッジプラットフォームは、Cisco ACI から SR-MPLS ハンドオフ相互接続の中間 DC-PE デバイスとして使用できます。SR-MPLS ハンドオフは、セグメントルーティング (SR) MPLS アンダーレイを使用して Cisco ACI から WAN への相互接続を可能にする相互接続オプションです。



第 39 章

IPv6 を介したセグメントルーティング

セグメントルーティング (SR) は、MPLS データプレーンおよび IPv6 データプレーンの両方に適用できます。Cisco IOS XE 17.12.1a 以降、Segment Routing over IPv6 (SRv6) は IPv6 データプレーンを介してセグメントルーティングのサポートを拡張します。

- [IPv6 を介したセグメントルーティング \(408 ページ\)](#)
- [SRv6 の設定 \(413 ページ\)](#)
- [IS-IS での SRv6 \(417 ページ\)](#)
- [SRv6 BGP ベースのサービス \(419 ページ\)](#)
- [BGP SRv6 L3VPN オンデマンドネクストホップ \(429 ページ\)](#)
- [SRv6 トラフィック エンジニアリング ポリシー \(441 ページ\)](#)
- [SRv6 のパフォーマンス測定 \(447 ページ\)](#)
- [SRv6 OAM \(453 ページ\)](#)

IPv6 を介したセグメントルーティング

機能情報

表 49: SRv6 の機能情報テーブル

機能名	リリース	説明
IPv6 データプレーンを介したセグメントルーティング	Cisco IOS XE リリース 17.12.1a	<p>セグメントルーティング (SR) は現在、マルチプロトコルラベルスイッチング (MPLS) データプレーンに適用できます。Cisco IOS XE 17.12.1a 以降、SR は次のプロトコルの IPv6 データプレーンを介してサポートされています。</p> <ul style="list-style-type: none"> • 内部ゲートウェイプロトコル (IS-IS のみ) • Border Gateway Protocol (BGP) <p>さらに、IPv6 データプレーンを介したセグメントルーティングでは、次の機能を使用できます。</p> <ul style="list-style-type: none"> • セグメントルーティングトラフィックエンジニアリングポリシー • スタティックルート • パフォーマンス管理 • 運用、管理、およびメンテナンス (OAM)
BGP SRv6L3VPN オンデマンドネクストホップ	Cisco IOS XE リリース 17.13.1a	この機能が導入されました。



(注) 各機能およびリリースでサポートされるプラットフォームの詳細については、[サポートされるプラットフォーム \(412 ページ\)](#) を参照してください。

SRv6 に関する制約事項

- Cisco IOS XE は、32 ビット uSID ブロックと 16 ビット uSID ID (3216) を持つ uSID をサポートしています。この形式は、SRv6 uSID ドメインの uSID ロケータに使用する必要があります。
- Cisco IOS XE は、最大 10 個の uSID ロケータをサポートします。
- Cisco IOS XE は、次の SRv6 uSID の動作とバリエーションをサポートしています。
 - PSP/USD を備えた uN
 - PSP/USD を備えた uA
 - uDT4
 - uDT6
 - uDT46
- Cisco IOS XE は、**H.Encaps.Red SRv6** ポリシーヘッドエンドの動作をサポートしていません。

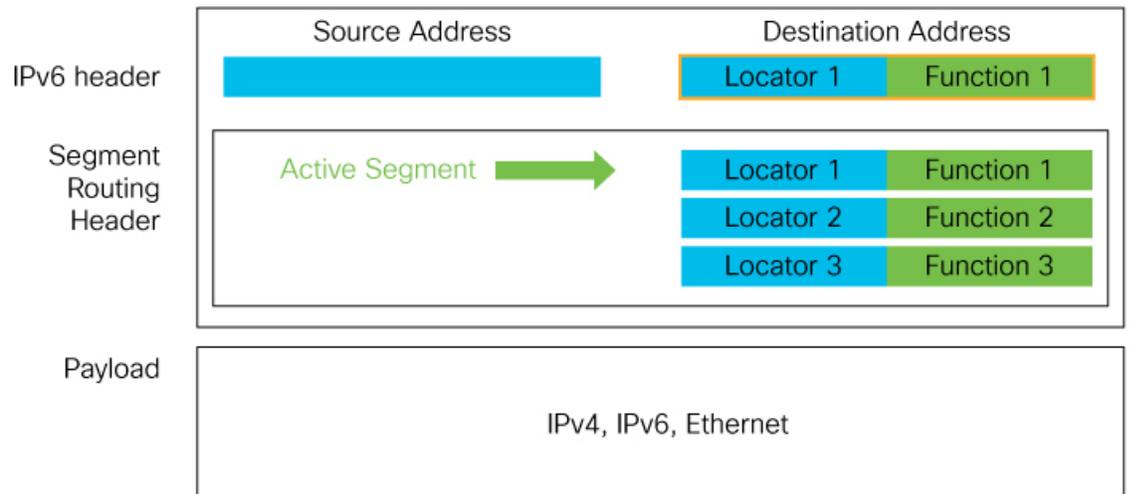
SRv6 に関する情報

SR-MPLS 対応ネットワークでは、MPLS ラベルは命令を表します。送信元ノードでは、パケットヘッダーの宛先へのパスがラベルのスタックとしてプログラムされます。

SRv6 にはネットワークプログラミングフレームワークが導入されており、IPv6 パケットヘッダー内の一連の命令をエンコードすることで、ネットワークオペレータまたはアプリケーションがパケット処理プログラムを指定できます。各命令は、ネットワーク内の 1 つまたは複数のノードに実装され、パケット内の SRv6 セグメント識別子 (SID) によって識別されます。SRv6 ネットワークプログラミングフレームワークは、[IETF RFC 8986 SRv6 ネットワークプログラミング](#) で定義されます。

SRv6 では、IPv6 アドレスは命令を表します。SRv6 では、命令の順序付きリストをエンコードするために、セグメントルーティングヘッダー (SRH) と呼ばれる新しいタイプの IPv6 ルーティング拡張ヘッダーが使用されます。アクティブセグメントはパケットの宛先アドレスによって示され、次のセグメントは SRH のポインタによって示されます。

図 40: パケットヘッダーのネットワークプログラム



521485

SRv6 SRH は、[IETF RFC 8754 IPv6 セグメントルーティング ヘッダー \(SRH\)](#) に記載されています。

SRv6 ノードロール

SRv6 ノードロールは、[IETF RFC 8754 IPv6 セグメントルーティング ヘッダー \(SRH\)](#) に記載されています。

SRv6 ヘッドエンドの動作

カプセル化を使用した SRv6 ヘッドエンドの動作は、[IETF RFC 8986 SRv6 ネットワークプログラミング](#)に記載されています。

SRv6 エンドポイントの動作

SRv6 エンドポイントの動作は、[IETF RFC 8986 SRv6 ネットワークプログラミング](#)に記載されています。

SRv6 エンドポイントの動作のバリエーション

SRv6 エンドポイントの動作のバリエーションは、[IETF RFC 8986 SRv6 ネットワークプログラミング](#)に記載されています。

SRv6 マイクロセグメント (uSID)

複数の SRv6 uSID は、uSID キャリアと呼ばれる単一の 128 ビット SID 内でエンコードされる場合があります。

SRv6 uSID は、IETF ドラフトの「[Network Programming extension: SRv6 uSID instruction](#)」および「[Compressed SRv6 Segment List Encoding in SRH](#)」に記載されています。

この章では、SRv6 マイクロセグメントを **uSID** と呼びます。

SRv6 uSID の用語

SRv6 uSID の用語は、「[Network Programming extension: SRv6 uSID instruction](#)」に記載されています。

uSID ブロック内の SRv6 uSID の割り当て

SRv6 uSID の割り当ては、「[Network Programming extension: SRv6 uSID instruction](#)」に記載されています。

uSID に関連付けられた SRv6 エンドポイントの挙動

SRv6 uSID エンドポイントの挙動は、「[Network Programming extension: SRv6 uSID instruction](#)」に記載されています。

SRv6 の導入

SRv6 設定を有効にするために、Cisco IOS XE 17.12.1a では新しいコマンド **segment-routing srv6** が導入されました。

```
segment-routing srv6
  encapsulation
    source-address {ipv6-addr}
    hop-limit [propagate | <value>]
    traffic-class [propagate | <value>]
  locators
    locator <name>
    format usid-f3216
    prefix <locator-ipv6-prefix/prefix-len>
  sid holdtime <value>
  explicit-sids
    sid <SRv6-SID> behavior {end-dt46 | end-dt4 | end-dt6}
    forwarding
      path <1>
      decap-and-lookup [vrf-name <vrf>]
```

このコマンドのパラメータは次のとおりです。

SRv6 ロケータ名、プレフィックス、および uSID 関連パラメータ

このセクションでは、**segment-routing SRv6** コマンドの設定可能なキーワードについて説明します。

locator name	SRv6 ロケータを設定します。
locator name prefix locator	ロケータプレフィックス値を設定します。
locator name format usid-f3216	ロケータをマイクロセグメント (uSID) として指定します。

SRv6 カプセル化パラメータ

このセクションでは、設定可能な SRv6 カプセル化パラメータについて説明します。これらのオプションのパラメータには、次のものが含まれます。

encapsulation source-address ipv6-addr	外部カプセル化 IPv6 ヘッダーの送信元アドレス。カプセル化のデフォルトの送信元アドレスは、最下位のループバック インターフェイスの最下位のグローバルユニキャスト IPv6 アドレスです。ループバックアドレスと静的カプセル化送信元アドレスが設定されていない場合、送信元アドレスは未割り当て (0::0) のままです。
encapsulation hop-limit {count <propagate>}	外部カプセル化 IPv6 ヘッダーのホップ制限。count の範囲は 1 ~ 255 で、ホップ制限のデフォルト値は 64 です。(着信パケット/フレームからの) 伝播によるホップ制限値を設定するには、 propagate を使用します。
encapsulation traffic-class {value <propagate>}	IPv6 ヘッダーのトラフィッククラスフィールドの設定。トラフィッククラスの値 (2 つの 16 進数ニブル) を指定します。有効な値は 0x0 ~ 0xff です。デフォルト値は 0 です (着信パケット/フレームからの) 伝播によってトラフィッククラス値を設定するには、 propagate を使用します。

SRv6 SID パラメータ

このセクションでは、設定可能な SRv6 SID パラメータについて説明します。

sid holdtime minutes	古いまたは解放された SID のホールド時間。minutes の範囲は 0 (無効) ~ 60 分です。
sid <SRv6-SID> behavior {end-dt46 end-dt4 end-dt6}	SID アドレスと動作コンテキストを指定して、静的 SID を設定します。

サポートされるプラットフォーム

Cisco IOS XE 17.12.1a リリース以降、複数の SRv6 機能は以下のプラットフォームでサポートされています。

- Cisco ASR1000 RP3 + ESP100-X、ASR1001-HX、ASR1002-HX
- Cisco Catalyst 8000V Edge ソフトウェア
- Cisco Catalyst 8200 シリーズ エッジプラットフォーム

- Cisco Catalyst 8300 シリーズ エッジプラットフォーム
- Cisco Catalyst 8500 および 8500L シリーズ エッジプラットフォーム

サポートされる機能については、[機能情報 \(408 ページ\)](#) を参照してください。

Cisco IOS XE 17.13.1a リリース以降、BGP SRv6 L3VPN ODN は以下のプラットフォームでサポートされています。

- Cisco ASR1000 RP3 + ESP100-X、ASR1001-HX、ASR1002-HX
- Cisco Catalyst 8000V Edge ソフトウェア
- Cisco Catalyst 8200 シリーズ エッジプラットフォーム
- Cisco Catalyst 8300 シリーズ エッジプラットフォーム
- Cisco Catalyst 8500 および 8500L シリーズ エッジプラットフォーム

SRv6 の設定

SRv6 の設定

SRv6 を有効にするには、次の高度な設定手順を実行します。

- ロケータを使用したグローバル SRv6 の設定
- オプションの SRv6 パラメータの設定

ロケータを使用したグローバル SRv6 の設定

次の例で、SRv6 をグローバルに有効化し、ロケータを設定する方法を示します。

```
Router(config)# segment-routing srv6
Router(config-srv6)# locators
Router(config-srv6-locator)# locator myLoc1
Router(config-srv6-locator)# format usid-f3216
Router(config-srv6-locator)# prefix 2001:0:8::/48
```

オプションの SRv6 パラメータの設定

次の例で、オプションの SRv6 パラメータを設定する方法を示します。

```
Router(config)# segment-routing srv6
Router(config-srv6)# encapsulation
Router(config-srv6-encap)# source-address 1::1
Router(config-srv6-encap)# hop-limit 60
Router(config-srv6-encap)# traffic-class propagate
Router(config-srv6-encap)# exit
Router(config-srv6)# sid holdtime 10
```

SPv6 の設定の確認

次の例を使用して、SRv6 の設定を確認します。

例 1 : この例では、ロケータの設定とその動作ステータスを確認する方法を示します。

```
router# show segment-routing srv6 locator
Name           Algo      Prefix           Format           Status
----           -
loc1           0        FC01:101:2::/48 usid-f3216      Up
```

例 2 : 次の例では、プラットフォームの機能とパラメータを表示する方法を示します。

```
router# show segment-routing srv6 capabilities-parameters
```

```
Platform Capabilities:
SRv6:Yes
PFP:Yes
TILFA:No
Endpoint behaviors:
uN (PSP/USD)
uA (PSP/USD)
uDT6
uDT4
uDT46
Transit.ENCAP.RED
Encap Parameters:
Max-SL :16
Encap :Collapsed
Hop-limit propagate :Yes
Traffic-class propagate :Yes
Parameters in-use:
Encap Parameters:
Source Address: 2001::1:1:1:2, Loopback1 (Default)
Hop-Limit: 64 (Default)
Traffic-class: 0 (Default)
```

```
router# show srv6 capabilities-parameters
```

```
Platform Capabilities:
SRv6:Yes
PFP:Yes
TILFA:No
Endpoint behaviors:
uN (PSP/USD)
uA (PSP/USD)
uDT6
uDT4
uDT46
Transit.ENCAP.RED
Encap Parameters:
Max-SL :16
Encap :Collapsed
Hop-limit propagate :Yes
Traffic-class propagate :Yes
Parameters in-use:
Encap Parameters:
Source Address: A001::1, Loopback0 (Default)
Hop-Limit: 64 (Default)
Traffic-class: 0 (Default)
```

例 3 : 次の例では、SID の概要と詳細を表示する方法を示します。

```

router# show segment-routing srv6 sid
SID          Locator      Behavior      Context      Owner
----          -
FC01:101:2::  loc1        uN (PSP/USD)
SID-MGR
FC01:101:2:E000::  loc1        uDT4          ce1
router bgp
FC01:101:2:E001::  loc1        uDT6          ce1
router bgp
FC01:101:2:E002::  loc1        uA (PSP/USD)  Ethernet2/0 2001::99:2:3:3
router isis sr
FC01:101:2:E003::  loc1        uA (PSP/USD)  Ethernet2/1 2001::100:2:3:3
router isis sr
FC01:101:2:E004::  loc1        uA (PSP/USD)  Ethernet3/0 2001::99:2:4:4
router isis sr
FC01:101:2:E005::  loc1        uA (PSP/USD)  Ethernet3/1 2001::100:2:4:4
router isis sr
FC01:101:2:E006::  loc1        uA (PSP/USD)  Ethernet4/0 2001::99:2:5:5
router isis sr
FC01:101:2:E007::  loc1        uA (PSP/USD)  Ethernet4/1 2001::100:2:5:5
router isis sr

```

```

router# show segment-routing srv6 sid FC01:101:2:: detail

```

```

SID: FC01:101:2::  Type: DYNAMIC
Behavior: uN (PSP/USD) (48)
Context:
  interface: (not-set)
  vrf: (not-set), v4-topo-id: 0xFFFF, v6-topo-id: 0xFFFF
  next-hop: (not-set)
  policy: (not-set)
  distinguisher: (not-set)
Stats:
  Packets: 0 Bytes: 0
User list:
  User:Refcount      Locator:Refcount
  -----
  SID-MGR(2):1      loc1:1
Event history:
  Timestamp          Client          Event type
  -----
  04-15 05:44:43.992  SID-MGR(2)     ALLOC

```

例 4 : 次の例では、古い SID を表示する方法を示します。

```

router# show segment-routing srv6 sid stale
SID          Owner          Locator      Behavior      Context
----          -
FC01:101:2:E002::  loc1        uA (PSP/USD)  Ethernet2/0 2001::99:2:3:3

```

```

router# show segment-routing srv6 sid stale detail

```

```

SID: FC01:101:2:E002::
Behavior: uA (PSP/USD) (57)
Context:
  interface: Ethernet2/0
  vrf: (not-set), v4-topo-id: 0xFFFF, v6-topo-id: 0xFFFF
  next-hop: 2001::99:2:3:3
  policy: (not-set)
  distinguisher: (not-set)
Event history:
  Timestamp          Client          Event type
  -----

```

```
04-15 06:58:13.961  router isis sr(3 ALLOC
04-15 07:24:49.831  router isis sr(3 DEALLOC
```

例 5 : 次の例では、設定済みの IPv6 ルートとルータプレフィックスを表示する方法を示します。

```
router# show ipv6 route
(snip)
C   FC01:101:2::/48 [0/0]
   via SR0, directly connected
L   FC01:101:2::/128 [0/0]
   via SR0, receive
I2  FC01:101:3::/48 [115/10]
   via FE80::A8BB:CCFF:FE02:8F02, Ethernet2/0
   via FE80::A8BB:CCFF:FE02:8F12, Ethernet2/1
I2  FC01:101:4::/48 [115/10]
   via FE80::A8BB:CCFF:FE01:C901, Ethernet3/0
   via FE80::A8BB:CCFF:FE01:C911, Ethernet3/1
I2  FC01:101:5::/48 [115/10]
   via FE80::A8BB:CCFF:FE03:A404, Ethernet4/0
   via FE80::A8BB:CCFF:FE03:A414, Ethernet4/1

router# show ipv6 route FC01:101:2::/48
Routing entry for FC01:101:2::/48
  Known via "connected", distance 0, metric 0, type connected
  Route count is 1/1, share count 0
  Routing paths:
    directly connected via SR0
      Route metric is 0, traffic share count is 1
      Last updated 00:37:54 ago
```

例 6 : この例では、設定済みエクスプレス転送パス (CEF) を表示する方法を示します。

```
router# show ipv6 cef FC01:101:2::/48 internal
FC01:101:2::/48, epoch 0, flags [att, cnn, srsid], RIB[C], refcnt 5, per-destination
sharing
  sources: SRv6-SID, RIB
  feature space:
    IPRM: 0x00038004
    Broker: linked, distributed at 2nd priority
  subblocks:
    SRv6 SID: FC01:101:2::/48
    Block-len:32 Node-len:16 Func-len:0 Arg-len:0
    END Flags:0x1 OCE:
      End OCE stats:
        packet count: 0
        byte count: 0
        punt packet count: 0
        punt byte count: 0
        error count: 0
    SRv6 end 0x80007FF32CFA6F38, 4 locks [Flags: clean]
    Lookup in input interface's IPv6 table
  ifnums: (none)
  path list 7FF32C863280, 21 locks, per-destination, flags 0x65 [shble, hvsh, rcrsv,
hwc]
  path 7FF32C85D978, share 1/1, type recursive, for IPv6
    recursive via ::[IPv6:Default], fib 7FF32C87D000, 1 terminal fib, v6:Default:::/127

    path list 7FF32C8631D0, 2 locks, per-destination, flags 0x61 [shble, rcrsv, hwc]
      path 7FF32C85D8A8, share 1/1, type recursive, for IPv6, flags [dsnt-src-via,
cef-intnl]
```

```

recursive via ::/127<nh::>[IPv6:Default], fib 7FF32C3592D8, 1 terminal fib,
v6:Default:::/127
  path list 7FF32C2F5860, 5 locks, per-destination, flags 0x41 [shble, hwcn]
  path 7FF32BF8ED50, share 1/1, type special prefix, for IPv6
  discard
output chain:
  SRv6 end 0x80007FF32CFA6F38, 5 locks [Flags: clean]
  Lookup in input interface's IPv6 table

```

IS-IS での SRv6

IS-IS での SRv6

Intermediate System-to-Intermediate System (IS-IS) プロトコルは、MPLS データプレーン (SR-MPLS) によるセグメントルーティングをすでにサポートしています。Cisco IOS XE 17.12.1a以降、IS-ISは、IPv6 データプレーン (SRv6) によるセグメントルーティングをサポートするように拡張されています。拡張機能には、ノード、ノードセグメント、および隣接セグメントの SRv6 機能を SRv6 SID としてアダプタイズすることが含まれています。

IS-IS での SRv6 に関する情報

IS-IS の SRv6 は、次の機能を実行します。

- ローカルのロケータプレフィックスを学習するための SID マネージャとの対話と、IGP ドメイン内のロケータプレフィックスの通知。
- 他の IS-IS ネイバルータからのリモートのロケータプレフィックスの学習と、学習したリモートのロケータ IPv6 プレフィックスの RIB へのインストール。
- プレフィックス SID および隣接関係 (アジャセンシー) SID の割り当てまたは学習、ローカル SID エントリの作成、および IGP ドメインでのそれらのアダプタイズ。

IS-IS での SRv6 の設定

次の例に示すように、**segment-routing srv6** コマンドを **router isis** コマンドの下で使用して、IS-IS IPv6 アドレスファミリで SRv6 を有効にします。**level {1|2}** キーワードを使用して、指定した IS-IS レベルでのみロケータをアダプタイズします。

基本的な SRv6 の設定については、[SRv6 の設定](#) セクションを参照してください。

次の例で、IS-IS で SRv6 を設定する方法を示します。

```

Router(config)# router isis core
Router(config-isis)# address-family ipv6 unicast
Router(config-isis-af)# router-id Loopback0
Router(config-isis-af)# segment-routing srv6
Router(config-isis-af-srv6)# locator loc5
Router(config-isis-af-srv6-locator)# level 1
Router(config-isis-srv6-locator)# exit

```

次の例で、IS-IS で複数の SRv6 ロケータを割り当てる方法を示します。

```
Router(config)# router isis core
Router(config-isis)# address-family ipv6 unicast
Router(config-isis-af)# segment-routing srv6
Router(config-isis-srv6)# locator myLocBestEffort
Router(config-isis-srv6-loc)# exit
Router(config-isis-srv6)# locator myLocLowLat
Router(config-isis-srv6-loc)# exit
```

IS-IS の設定の詳細については、『Cisco IP Routing Configuration Guide』の「[IS-IS Overview and Basic Configuration](#)」の章を参照してください。



(注) **router-id** キーワードによって、SRv6 ポリシーが使用できるようになります。

SRv6 IS-IS の設定の確認

例 1 : show segment-routing srv6 locator コマンドを使用して、IS-IS 設定で SRv6 を確認します。

```
Router# show segment-routing srv6 locator
```

Name	ID	Algo	Prefix	Status	Flags
myLoc1	3	0	2001:0:8::/48	Up	U
myLocBestEffort	5	0	2001:0:1::/48	Up	U

例 2 : show isis srv6 locators コマンドを使用して、SID ロケータを表示します。

```
router# show isis srv6 locators
ISIS SRv6 Locators:
Tag sr:
Name          Prefix          Level
----          -
loc1          FC01:101:2::/48  2

router# show isis srv6 locators detail
ISIS SRv6 Locators:
Tag sr:
Name          Prefix          Level
----          -
loc1          FC01:101:2::/48  2

Level-1 metric: 0
Level-2 metric: 0
End-SIDs:
FC01:101:2::
```

SRv6 BGP ベースのサービス

SRv6 BGP ベースのサービス

機能名	リリース	説明
デュアルスタック L3VPN サービス (IPv4、IPv6) (SRv6 マイクロ SID)	Cisco IOS XE リリース 17.12.1a	この機能により、VPNv4 および VPNv6 VRF のサポート SRv6 が導入されます。同じインターフェイス、サブインターフェイス、または VRF 上の uDT4 および uDT6 ベースの SRv6 サービスがサポートされます。

IETF ドラフトの [BGP/MPLSIP 仮想プライベートネットワーク \(VPN\)](#) で定義されているメッセージと手順に基づいて構築された BGP は、SRv6 ネットワークを介して次のサービスを提供するように拡張されています。

- IPv4 レイヤ 3 VPN
- IPv6 レイヤ 3 VPN

IETF ドラフトの [SRv6 BGP ベースのオーバーレイサービス](#) で定義されているメッセージと手順に基づいて、BGP は対応する BGP アップデートのプレフィックス SID 属性で SRv6 サービス SID をエンコードし、それを IPv6 BGP ピアにアダプタイズします。

BGP の詳細については、『*Cisco IP Routing Configuration Guide, Cisco IOS XE 17.x*』の「[Cisco BGP の概要](#)」の章を参照してください。

SRv6 BGP ベースのサービスに関する制約事項

- 次の SRv6 BGP ベースのサービスがサポートされています。
 - IPv4 L3VPN
 - IPv6 L3VPN
- L3VPN の uDT4、uDT6、および uDT46 がサポートされています。
- BGP は、uDT46 の割り当てとアダプタイズメントをサポートしていません。

SRv6 BGP ベースのサービスに関する情報

SRv6 ロケータの継承ルール

SRv6 ロケータは、BGP ルーティングプロセス内のさまざまなレベルで割り当てることができます。BGP は、次の継承ルールにしたがって、設定したロケータスペースから SRv6 サービス SID を割り当てます。

1. サービスで定義されているロケータを使用する。特定のサービスで定義されていない場合は、次のようにする。
2. 対応するアドレスファミリで定義されているロケータを使用する。対応するアドレスファミリで定義されていない場合は、次のようする。
3. BGP でグローバルに定義されているロケータを使用する。

BGP の下には、ロケータが指定されている場所が複数あります。

- グローバル（最も汎用）
- VPN AF
- VRF AF（最も限定的）

特定のロケータが設定されていない場合は、上位レベルのロケータ設定が次の順序で継承されます。

グローバル -> VPN-AF -> VRF-AF



-
- (注) デフォルトの SRv6 SID 割り当てモードはなく、SRv6 SID 割り当てモードなしでロケータモードを設定することはできません。ロケータが設定または継承されていない場合、BGP は SID を割り当てません。
-

SID マネージャロケータの変更の BGP 処理

BGP で設定したロケータが SID マネージャに存在しない場合、

- BGP 設定は受け入れられますが、アクティブにはなりません。
- BGP は syslog を生成します。
- BGP は、SID マネージャからのロケータ設定通知をリッスンします。

BGP で設定したロケータが SID マネージャで作成された場合、

- SID マネージャが BGP に作成を通知します。
- BGP は、一致するロケータ設定があればそれをアクティブにします。
- BGP は該当するプレフィックスの SID を割り当て、それらをアドバタイズします。

BGP で設定したロケータが SID マネージャから削除された場合、

- SID マネージャが BGP に削除を通知します。
- BGP は、一致するロケータ設定があればそれを非アクティブにします。
- BGP は該当するプレフィックスの SID の割り当てを解除し、それらを取り消します。

BGP で設定したロケータが SID マネージャで変更された（つまりロケータプレフィックスが変更された）場合、

- SID マネージャは BGP に変更を通知します。
- BGP は、以前のロケータプレフィックスに関連付けられているすべての SID を解放します。
- BGP は、新しいロケータプレフィックスに新しい SID を割り当て、更新されたプレフィックスをアドバタイズします。

SRv6 ロケータの設定方法の詳細については、[SRv6 の設定](#) セクションを参照してください。

SRv6 ベースの L3VPN

このセクションでは、SRv6 ネットワーク上の L3VPN（VPNv4 および VPNv6）について説明します。

SRv6 ネットワーク上の L3VPN には、次の制約が適用されます。

- VRF 単位の割り当てモードのみがサポートされる（uDT4 および uDT6 の動作）。
- 等コストマルチパス（ECMP）はサポートされ、不等コストマルチパス（UCMP）はサポートされない。
- MPLSL3VPN および SRv6 L3VPN インターワーキングゲートウェイはサポートされない。

SRv6 ベースの L3VPN の設定

SRv6 ベースの L3VPN を有効にするには、BGP で SRv6 を有効にし、ロケータを指定し、SID 割り当てモードを設定する必要があります。ロケータの割り当ては、[ルータ bgp](#) 設定のさまざまな場所で実行できます。[SRv6 ロケータの継承ルール](#) セクションを参照してください。

BGP での SRv6 のグローバルな有効化

BGP ルーティングプロセスで SRv6 をグローバルに有効にするには、`router bgp as-number` コマンドの下で `segment-routing srv6` コマンドを使用します。`as-number` の範囲は 1 ~ 65535 です。

```
router bgp 65000
  segment-routing srv6
  locator loc1
  exit-srv6
!
```

SRv6 IPv4 L3VPN の設定

この例は、SRv6 ベースの IPv4 L3VPN の完全な設定を示しています。

```
router bgp 65000
!
bgp router-id interface Loopback1
no bgp default ipv4-unicast
neighbor 2001::1:1:1:4 remote-as 65000
neighbor 2001::1:1:1:4 update-source Loopback1
address-family vpnv4
!
segment-routing srv6
locator loc1
alloc-mode per-vrf
exit-srv6
!
neighbor 2001::1:1:1:4 activate
neighbor 2001::1:1:1:4 send-community both
```

SRv6 IPv6 L3VPN の設定

この例は、SRv6 ベースの IPv6 L3VPN の完全な設定を示しています。

```
router bgp 65000
!
bgp router-id interface Loopback1
no bgp default ipv4-unicast
neighbor 2001::1:1:1:4 remote-as 65000
neighbor 2001::1:1:1:4 update-source Loopback1
address-family vpnv6
!
segment-routing srv6
locator loc1
alloc-mode per-vrf
exit-srv6
!
neighbor 2001::1:1:1:4 activate
neighbor 2001::1:1:1:4 send-community both
```

SRv6 IPvx VRF L3VPN の設定

この例は、アドレスファミリ IPvx VRF の SRv6 ベースの L3VPN の完全な設定を示しています。

```
router bgp 65000
!
bgp router-id interface Loopback1
no bgp default ipv4-unicast
neighbor 2001::1:1:1:4 remote-as 65000
neighbor 2001::1:1:1:4 update-source Loopback1
address-family ipv4 vrf cel
!
segment-routing srv6
locator loc1
alloc-mode per-vrf
exit-srv6
!
neighbor 99.1.2.1 remote-as 65001
neighbor 99.1.2.1 activate
neighbor 99.1.2.1 send-community both
```

```

address-family ipv6 vrf ce1
!
segment-routing srv6
  locator loc1
  alloc-mode per-vrf
exit-srv6
!
neighbor 1002::1 remote-as 65002
neighbor 1002::1 activate
neighbor 1002::1 send-community both

```

BGP MPLS と SRv6 の共存

MPLS ネイバーと SRv6 ネイバーの両方を持つデュアル接続 PE は、送信元/CE ルートのローカル MPLS ラベルと SRv6 SID を同時に割り当てます。

制約事項

- SRV6 が BGP AFI VRF に対して有効になっている場合、MPLS ラベル割り当ては無効になります。
- **mpls alloc enable** コマンドは、MPLS ラベル割り当てを有効にする、デフォルトの割り当てモードです。SRV6 と MPLS の両方の割り当てが有効で、MPLS がデフォルトの割り当てモードになっています。
- MPLS と SRv6 の共存設定では、MPLS ラベルはデフォルトでネイバーにアダプタイズされます。
- SRv6 SID をネイバーにアダプタイズするには、**neighbor <> encap srv6** コマンドが必要です。

L3VPN の MPLS と SRv6 の共存設定

次に、L3VPN の MPLS と SRv6 の共存を有効にする設定の例を示します。

```

router bgp <instance>
  address-family [ipv4 | ipv6] unicast vrf <vrf-name>
    segment-routing srv6
      mpls alloc enable          >>>> required for MPLS/SRV6 coexistence
  address-family vpnv4/vpnv6
    neighbor <A>                >>>> can send any kind of update
    neighbor <B> encap srv6     >>>> SRv6 only neighbor

```



(注) MPLS と SRv6 の共存が有効になっている VRF からの送信元プレフィックスまたは CE プレフィックスは、MPLS ラベルとともに送信されます。

SRv6 の状態の確認

SRv6 BGP の設定を確認するには、次の show コマンドを使用します。

例 1 : show segment-routing srv6 sid

```

device# show segment-routing srv6 sid
SID                Locator    Behavior    Context
Owner
----
-----
FC01:101:2::      loc1      uN (PSP/USD)
SID-MGR
FC01:101:2:E000:: loc1      uDT4        cel
router bgp
FC01:101:2:E001:: loc1      uDT6        cel
router bgp
FC01:101:2:E002:: loc1      uA (PSP/USD) Ethernet2/0 2001::99:2:3:3
router isis sr
FC01:101:2:E003:: loc1      uA (PSP/USD) Ethernet2/1 2001::100:2:3:3
router isis sr
FC01:101:2:E004:: loc1      uA (PSP/USD) Ethernet3/0 2001::99:2:4:4
router isis sr
FC01:101:2:E005:: loc1      uA (PSP/USD) Ethernet3/1 2001::100:2:4:4
router isis sr
FC01:101:2:E006:: loc1      uA (PSP/USD) Ethernet4/0 2001::99:2:5:5
router isis sr
FC01:101:2:E007:: loc1      uA (PSP/USD) Ethernet4/1 2001::100:2:5:5
router isis sr

```

例 2 : show segment-routing srv6 sid <SID> detail

```

device# show segment-routing srv6 sid FC01:101:2:E000:: detail
SID: FC01:101:2:E000:: Type: DYNAMIC
Behavior: uDT4 (63)
Context:
  interface: (not-set)
  vrf: cel, v4-topo-id: 0x1, v6-topo-id: 0xFFFF
  next-hop: (not-set)
  policy: (not-set)
  distinguisher: (not-set)
Stats:
  Packets: 0 Bytes: 0
User list:
  User:Refcount      Locator:Refcount
  -----
  router bgp(5):1    loc1:1
Event history:
  Timestamp          Client          Event type
  -----
  04-15 07:24:08.165 router bgp(5)  ALLOC

```

例 3 : show ip bgp srv6 locator

```

device# show ip bgp srv6 locator
Locator-1
  Name: loc1
  Active: Yes
  Refcount: 3

```

例 4 : show ip bgp srv6 sid

```

device# show ip bgp srv6 sid
SID-1

```

```

locator : loc1
alloc-mode : 0
status : ALLOCATED
state : 1
ref_count : 5
topoid : 0x1E000001
sid_value : FC01:101:2:E001::
prefix_length : 64
block_length : 32
node_length : 16
function_length : 16
arg_length : 0
behaviour : 62
SID-2
locator : loc1
alloc-mode : 0
status : ALLOCATED
state : 1
ref_count : 5
topoid : 0x1
sid_value : FC01:101:2:E000::
prefix_length : 64
block_length : 32
node_length : 16
function_length : 16
arg_length : 0
behaviour : 63

```

例 5 : show ipv6 cef <prefix> internal

```

device# show ipv6 cef FC01:101:8:E006:: internal
FC01:101:8:E006::/128, epoch 0, flags [att, srsid], refcnt 4, per-destination sharing
sources: SRv6-SID
subblocks:
  SRv6 SID: FC01:101:8:E006::/128
  Block-len:32 Node-len:16 Func-len:16 Arg-len:0
  END-DT4 Flags:0x5 OCE:
  End OCE stats:
    packet count: 20
    byte count: 2280
    punt packet count: 0
    punt byte count: 0
    error count: 0
  SRv6 end 0x80007FD05D9BC970, 4 locks [Flags: clean decap]
  Lookup in table IPv4:ce2
ifnums: (none)
path list 7FD05BD3F530, 21 locks, per-destination, flags 0x65 [shble, hvsh, rcrsv,
hwc]
  path 7FD05BD2D578, share 1/1, type recursive, for IPv6
  recursive via ::[IPv6:Default], fib 7FD05BD43C60, 1 terminal fib, v6:Default:::/127

  path list 7FD05BD3F480, 2 locks, per-destination, flags 0x61 [shble, rcrsv, hwc]
  path 7FD05BD2D4A8, share 1/1, type recursive, for IPv6, flags [dsnt-src-via,
cef-intnl]
  recursive via ::/127<nh::>[IPv6:Default], fib 7FD056DAB760, 1 terminal fib,
v6:Default:::/127
  path list 7FD054328EF8, 5 locks, per-destination, flags 0x41 [shble, hwc]
  path 7FD05AF52578, share 1/1, type special prefix, for IPv6
  discard
output chain:
  SRv6 end 0x80007FD05D9BC970, 5 locks [Flags: clean decap]
  Lookup in table IPv4:ce2

```

例 6 : show isis database verbose

```

device# show isis database verbose
pe3.00-00          0x00000025  0xEF58          742/1198      0/0/0
  Area Address: 49
  NLPID:         0xCC 0x8E
  Topology:      IPv4 (0x0)
                 IPv6 (0x2)
  Router ID:     1.1.1.8
  Router CAP:    1.1.1.8, D:0, S:0
  SRv6 Oflag:0
  Segment Routing: I:1 V:0, SRGB Base: 16000 Range: 8000
  Segment Routing Algorithms: SPF, Strict-SPF
  Segment Routing Local Block: SRLB Base: 30000 Range: 10000
  Node-MSD
  MSD: 16
  Hostname: iolpe3
(snip)
SRv6 Locator: (MT-IPv6) FC01:101:8::/48 Metric:0 Algorithm:0
  End SID: FC01:101:8:: uN (PSP/USD)
  SID Structure:
    Block Length: 32, Node-ID Length: 16, Func-Length: 0, Args-Length: 0

```

例 7 : show ipv6 route <prefix>

```

device# show ipv6 route FC01:101:8::/48
Routing entry for FC01:101:8::/48
  Known via "isis sr", distance 115, metric 30, type level-2
  Route count is 4/4, share count 0
  Routing paths:
    FE80::A8BB:CCFF:FE01:E411, Ethernet3/1
      Route metric is 30, traffic share count is 1
      From FE80::A8BB:CCFF:FE01:E411
      Last updated 01:03:27 ago
    FE80::A8BB:CCFF:FE03:F504, Ethernet4/0
      Route metric is 30, traffic share count is 1
      From FE80::A8BB:CCFF:FE03:F504
      Last updated 01:03:27 ago
    FE80::A8BB:CCFF:FE03:F514, Ethernet4/1
      Route metric is 30, traffic share count is 1
      From FE80::A8BB:CCFF:FE03:F514
      Last updated 01:03:27 ago
    FE80::A8BB:CCFF:FE01:E401, Ethernet3/0
      Route metric is 30, traffic share count is 1
      From FE80::A8BB:CCFF:FE01:E401
      Last updated 01:03:27 ago

```

例 8 : show bgp [vpngv4|vpngv6] rd <rd> <prefix>

VPNv4 の出力例 :

```

device# show bgp vpngv4 uni rd 1:1 22.22.22.22

BGP routing table entry for 1:1:22.22.22.22/32, version 13
Paths: (1 available, best #1, table red)
Not advertised to any peer
Refresh Epoch 1
3, imported path from 2:2:22.22.22.22/32 (global)
2023:1:1 (via default) from 1.1.1.3 (1.1.1.3)
Origin incomplete, metric 0, localpref 100, valid, internal, best
Extended Community: RT:1:1 RT:2:2

```

```

Originator: 11.1.1.1, Cluster list: 1.1.1.3
srv6 out-sid: FCCC:CCC1:AA88:E000::
rx pathid: 0, tx pathid: 0x0
Updated on Jun 28 2023 11:29:52 PST

```

VPNv6 の出力例 :

```

device# show bgp vpnv6 uni rd 1:1 2222::1/128

BGP routing table entry for [1:1]2222::1/128, version 11
Paths: (1 available, best #1, table red)
Not advertised to any peer
Refresh Epoch 1
3, imported path from [2:2]2222::1/128 (global)
2023:1::1 (via default) from 1.1.1.3 (1.1.1.3)
Origin incomplete, metric 0, localpref 100, valid, internal, best
Extended Community: RT:2:2
Originator: 11.1.1.1, Cluster list: 1.1.1.3
srv6 out-sid: FCCC:CCC1:AA88:E001::
rx pathid: 0, tx pathid: 0x0
Updated on Jun 28 2023 11:29:52 PST

```

例 9 : `show ip route vrf <vrf> <prefix>`

```

device# show ip route vrf cel 1.1.1.10
Routing Table: cel
Routing entry for 1.1.1.10/32
  Known via "bgp 65000", distance 200, metric 0
  Tag 65010, type internal
  Last update from FC01:101:8:E006:: 08:51:34 ago
  Routing Descriptor Blocks:
  * FC01:101:8:E006:: (default:ipv6), from 1.1.1.4, 08:51:34 ago
    opaque_ptr 0x7FF32E0B9640
    Route metric is 0, traffic share count is 1
    AS Hops 1
    Route tag 65010
    MPLS label: none

```

例 10 : `show ipv6 route vrf <vrf> <prefix>`

```

device# show ipv6 route vrf red 2222::1/128

Routing entry for 2222::1/128
Known via "bgp 1", distance 200, metric 0
Tag 3, type internal
Route count is 1/1, share count 0
Routing paths:
FCCC:CCC1:AA88:E001::%default
Route metric is 0, traffic share count is 1
From ::FFFF:1.1.1.3
opaque_ptr 0x7FF38CDB6848
Last updated 00:03:16 ago

```

例 11 : `show ip cef vrf <vrf> <prefix> internal`

```

device# show ip cef vrf red 22.22.22.22 internal

22.22.22.22/32, epoch 0, flags [rnolbl, rlbls], RIB[B], refcnt 5, per-destination sharing

sources: RIB
feature space:

```

```

IPRM: 0x00018000
VPN-SID(s) on: 1/0:v4-rcrsv-FCCC:CCC1:AA88:E000::
Path: v4-rcrsv-FCCC:CCC1:AA88:E000:: (VPN-SID: FCCC:CCC1:AA88:E000::)
Flags: 00000004 [vpn-sid]
IPv6 TC: 0 Hop Limit: 64
  Src: C02:1::7
  Dst: FCCC:CCC1:AA88:E000::
  Via: FCCC:CCC1:AA88:E000::
Segment List (1)
  FCCC:CCC1:AA88:E000::
Flow-based Encap Chains: 1
  IPv6 adj out of Ethernet0/0, addr FE80::A8BB:CCFF:FE00:3300 from FCCC:CCC1:AA88::/48
<= SRv6 SID List OCE 0x7FF38D329078 (5) 1 Segments
ifnums:
  Ethernet0/0(2): FE80::A8BB:CCFF:FE00:3300
  path list 7FF38CDE0D8, 7 locks, per-destination, flags 0x8269 [shble, rif, rcrsv,
hwc, bgp, sb-oce]
  path 7FF38CCDB128, share 1/1, type recursive, for IPv4, flags [vpn-sid],
vpn-sid:FCCC:CCC1:AA88:E000::
  recursive via FCCC:CCC1:AA88:E000::[IPv6:Default], fib 7FF38CDA31B0, 1 terminal
fib, v6:Default:FCCC:CCC1:AA88::/48
  path list 7FF38CCDE18, 2 locks, per-destination, flags 0x69 [shble, rif, rcrsv,
hwc]
  path 7FF38CCDAE8, share 1/1, type recursive, for IPv6, flags [dsnt-src-via,
cef-intnl]
  recursive via FCCC:CCC1:AA88::/48<nh:FCCC:CCC1:AA88:E000::>[IPv6:Default],
fib 7FF38CDA3D78, 1 terminal fib, v6:Default:FCCC:CCC1:AA88::/48
  path list 7FF38CCDE658, 5 locks, per-destination, flags 0x49 [shble, rif,
hwc]
  path 7FF38CCDB7A8, share 1/1, type attached nexthop, for IPv6
  nexthop FE80::A8BB:CCFF:FE00:3300 Ethernet0/0, IPv6 adj out of
Ethernet0/0, addr FE80::A8BB:CCFF:FE00:3300 7FF38CDE1848
output chain:
  SRv6 SID List OCE 0x7FF38D329078 (8) 1 Segments
  Segment List (1)
  FCCC:CCC1:AA88:E000::
  PushCounter(SRv6 Encap) 7FF386CF0E58
  SRv6 Encap OCE 0x7FF38D328BE8 (4) fwd-id:0 FCCC:CCC1:AA88:E000::
  Flags: 00000004 [vpn-sid]
  IPv6 TC: 0 Hop Limit: 64
  Src: C02:1::7
  Dst: FCCC:CCC1:AA88:E000::
  IPv6 adj out of Ethernet0/0, addr FE80::A8BB:CCFF:FE00:3300 7FF38CDE1848

```

例 12 : show ipv6 cef vrf <vrf> <prefix> internal

```

device# show ipv6 cef vrf red 2222::1/128 internal

2222::1/128, epoch 0, RIB[B], refcnt 4, per-destination sharing
sources: RIB
feature space:
  IPRM: 0x00018000
  VPN-SID(s) on: 1/0:v6-rcrsv-FCCC:CCC1:AA88:E001::
  Path: v6-rcrsv-FCCC:CCC1:AA88:E001:: (VPN-SID: FCCC:CCC1:AA88:E001::)
  Flags: 00000004 [vpn-sid]
  IPv6 TC: 0 Hop Limit: 64
  Src: C02:1::7
  Dst: FCCC:CCC1:AA88:E001::
  Via: FCCC:CCC1:AA88:E001::
  Segment List (1)
  FCCC:CCC1:AA88:E001::
  Flow-based Encap Chains: 1
  IPv6 adj out of Ethernet0/0, addr FE80::A8BB:CCFF:FE00:3300 from FCCC:CCC1:AA88::/48

```

```

<= SRv6 SID List OCE 0x7FF38D329018 (6) 1 Segments
ifnums:
  Ethernet0/0(2): FE80::A8BB:CCFF:FE00:3300
  path list 7FF38CCDDDD68, 9 locks, per-destination, flags 0x8269 [shble, rif, rcrsv,
hwn, bgp, sb-oce]
  path 7FF38CCDAD18, share 1/1, type recursive, for IPv6, flags [vpn-sid],
vpn-sid:FCCC:CC1:AA88:E01::
  recursive via FCCC:CC1:AA88:E01::[IPv6:Default], fib 7FF38CDA2E10, 1 terminal
fib, v6:Default:FCCC:CC1:AA88::/48
  path list 7FF38CCDDCB8, 2 locks, per-destination, flags 0x69 [shble, rif, rcrsv,
hwn]
  path 7FF38CCDAC48, share 1/1, type recursive, for IPv6, flags [dsnt-src-via,
cef-intnl]
  recursive via FCCC:CC1:AA88::/48<nh:FCCC:CC1:AA88:E01::>[IPv6:Default],
fib 7FF38CDA3D78, 1 terminal fib, v6:Default:FCCC:CC1:AA88::/48
  path list 7FF38CCDE658, 5 locks, per-destination, flags 0x49 [shble, rif,
hwn]
  path 7FF38CCDB7A8, share 1/1, type attached nexthop, for IPv6
  nexthop FE80::A8BB:CCFF:FE00:3300 Ethernet0/0, IPV6 adj out of
Ethernet0/0, addr FE80::A8BB:CCFF:FE00:3300 7FF38CDE1848
output chain:
  SRv6 SID List OCE 0x7FF38D329018 (9) 1 Segments
  Segment List (1)
  FCCC:CC1:AA88:E01::
  PushCounter(SRv6 Encap) 7FF386CF0DC8
  SRv6 Encap OCE 0x7FF38D328B48 (4) fwd-id:0 FCCC:CC1:AA88:E01::
  Flags: 00000004 [vpn-sid]
  IPv6 TC: 0 Hop Limit: 64
  Src: C02:1::7
  Dst: FCCC:CC1:AA88:E01::
  IPV6 adj out of Ethernet0/0, addr FE80::A8BB:CCFF:FE00:3300 7FF38CDE1848
device#

```

SRv6 BGP のトラブルシューティングとデバッグ

次の BGP コマンドを使用して、BGP アップデートをデバッグできます。

- **debug bgp <> updates**
- **debug bgp <> addpath**

SRv6 に関連するイベントをデバッグするために、次の新しいコマンドが導入されました。

- **debug ip bgp srv6**

BGP SRv6 L3VPN オンデマンドネクストホップ

BGP SRv6L3VPN オンデマンドネクストホップ

ドメイン全体にルーティング情報を再配布すると、マルチドメインサービス (L3VPN) のプロビジョニングにそれ自体の複雑性と拡張性の問題が発生します。オンデマンドネクストホップ (ODN) 設定により、BGP は拡張カラーコミュニティ属性を使用してルートを学習した結果

としてSRポリシーを動的に作成できます。次に、サービスがForwarding Information Base (FIB) へ移行する間に応答されたマルチドメインLSPをインストールします。

ここでは、SRv6 トラフィック エンジニアリング (SRv6-TE) がオンデマンドネクストホップ (ODN) メカニズムと連携する仕組みについて説明します。

BGP SRv6 L3VPN ODN の前提条件

BGP SRv6L3VPN オンデマンドネクストホップを設定する前に、「IS-IS での SRv6」セクションを参照してください。

BGP SRv6L3VPN ODN に関する情報

セグメントルーティングトラフィックエンジニアリング (SR-TE) オンデマンドネクストホップ (ODN) は、パケットの属性に基づくセグメントルーティングポリシーでのトラフィックのステアリングを可能にするメカニズムです。パケットはシスコの拡張ポリシーベースルーティング (ePBR) を使用して分類され、転送クラス (FC) と呼ばれる内部タグを使用してマークされます。PFP または PDP は、FC とそれに対応するパス間のマッピングに基づく、マークされたパケットのルーティングに使用されます。これは、トラフィックがその ePBR マーキングに基づいてステアリングされ、パケットの FC に基づいて適切なパスにスイッチされることを意味します。

BGP カラー拡張コミュニティと VRF プレフィックスのカラーリング

SR-TE メカニズムでは、SR-TE ルーティングパスを必要とするプレフィックスは、カラー拡張コミュニティ (プレフィックスにカラーを割り当てる属性) に関連付けられます。BGP には現在、neighbor コマンドのルートマップアウトバウンド設定のみに基づいてカラー拡張コミュニティをアタッチする機能があります。送信元 VRF、宛先 VRF、CE ネイバー、送信元プロトコルなどの属性に基づいてプレフィックスをカラーリングするために、カラーをアタッチする次のような方法が導入されています。

- VRF エクスポートのカラーリング
- VRF インポートのカラーリング
- BGP へのルート再配布カラーリング
- ネイバー インバウンド カラーリング

ルートマップ追加カラー拡張コミュニティ

新しいカラーがリストにない場合、ルートマップからの新しいカラー拡張コミュニティを、プレフィックス属性に存在する既存のカラー拡張コミュニティリストに追加できます。プレフィックスの既存のカラー拡張コミュニティを置き換えるのではなく、カラー拡張コミュニティの既存のリストに新しいカラー拡張コミュニティを追加するには、**route-map set extcommunity color** コマンドでキーワード **additive** を使用します。

```
route-map SRTE-color-map permit
  set extcommunity color < 1-4294967295> [additive]
```



- (注)
- **route-map set extcommunity color** コマンドが **additive** キーワードなしで設定されている場合、ルートマップからの新しいカラー拡張コミュニティによって、プレフィックス属性に存在する既存のカラーコミュニティが置き換えられます。
 - プレフィックスに追加できるカラー拡張コミュニティの数は、BGP アップデートメッセージに追加できる拡張コミュニティの数によって制限されます。

複数のカラーを受信する BGP

BGP は、複数のカラー拡張コミュニティを含むアップデートを受信した場合、[draft-ietf-spring-segment-routing-policy-08](#) で定義されているように、最も高いカラー値に対してのみ SR ポリシーを作成し、他のカラー値に対しては SR ポリシーを作成しません。

最も高いカラーの SR ポリシーがダウンしているか使用できない場合、BGP パスは引き続きベストパスとなりますが、最適パスをルーティングパスとして使用します（たとえば、SRv6 SID をルーティングパスとして）。

SR ポリシーは最も高いカラーの値に対してのみ作成されるため、**show ip bgp <prefix>** コマンドには、最も高いカラーの SR ポリシー情報が含まれます。最も高いカラーの SR ポリシーの状態によって、SR ポリシーと最適パスのどちらがルーティングパスとして使用されるかが決まります。



- (注) 最新のドラフト ([draft-ietf-spring-segment-routing-policy-09](#)、[RFC 9256](#)) で定義されている、より高いカラー値の SR ポリシーがダウンまたは使用できない場合に、より低いカラー値の SR ポリシーを使用するための複数カラーの処理は、サポートされていません。

SRv6 L3VPN ODN の設定

次に、SRv6 L3VPN ODN を設定する例を示します。

PE1 (出力) 設定

```
route-map test permit 10
  set extcommunity color 10
!

segment-routing srv6
  locators
    locator foo
      prefix FCCC:CCC2:C3::/48
      format usid-f3216
  !
!

router bgp 1
  neighbor 2023:1::3 remote-as 1
  !
address-family vpnv4
```

```

segment-routing srv6
  locator foo
  alloc-mode per-vrf
  exit-srv6
  !
  neighbor 2023:1::3 activate
  neighbor 2023:1::3 send-community both
  neighbor 2023:1::3 route-map test out
  exit-address-family
  !

```

PE2（入力）設定

```

segment-routing traffic-eng
  on-demand color 10
  authorize
  candidate-paths
  preference 1
  constraints
  segments
  dataplane srv6
  !
  !
  dynamic

router bgp 1
  neighbor 2023:1::3 remote-as 1
  !
  address-family vpnv4
  neighbor 2023:1::3 activate
  neighbor 2023:1::3 send-community both
  exit-address-family

  address-family vpnv6
  neighbor 2023:1::3 activate
  neighbor 2023:1::3 send-community both
  exit-address-family

```

SRv6 ODN カラーテンプレートの設定

BGP が SR-TE SRv6 ポリシーを動的にインスタンス化してトラフィックを誘導するには、オンデマンドネクストホップ（ODN）カラーテンプレートを使用してポリシーの属性を定義します。これらのテンプレートはすでに存在し、次の設定例に示すように SRv6 用に拡張されています。

```

ipv6 prefix-list From-PE6 seq 5 permit A006::1/128
!
segment-routing traffic-eng
  on-demand color 1000
  authorize restrict
  ipv6 prefix-list From-PE6
  candidate-paths
  preference 100
  per-flow
  forward-class 0 color 10000
  forward-class 1 color 10001
  forward-class 2 color 10002
  forward-class 3 color 10003
  forward-class 4 color 10004
  !
  on-demand color 10000
  authorize restrict

```

```
ipv6 prefix-list From-PE6
candidate-paths
preference 100
constraints
  segments
    dataplane srv6
  !
  affinity
    include-all
    name non-voice
  !
  !
  !
dynamic
metric
  type delay
  !
  !
preference 50
constraints
  segments
    dataplane srv6
  !
  affinity
    include-all
    name voice
  !
  !
  !
dynamic
  !
  !
  !
performance-measurement
delay-measurement
liveness-detection
invalidation-action down
!
on-demand color 10001
authorize restrict
  ipv6 prefix-list From-PE6
candidate-paths
preference 100
constraints
  segments
    dataplane srv6
  !
  affinity
    include-all
    name non-voice
  !
  !
  !
dynamic
metric
  type delay
  !
  !
preference 50
constraints
  segments
    dataplane srv6
  !
  affinity
```

```

        include-all
        name voice
        !
        !
        dynamic
        !
        !
    !
performance-measurement
delay-measurement
liveness-detection
invalidation-action down

```

BGP ネイバー アウトバウンド プレフィックスのカラーリング

カラー拡張コミュニティをアウトバウンド BGP プレフィックスアップデートにアタッチするには、次の設定を使用します。

```

route-map SRTE-color-map permit
    set extcommunity color <1-4294967295> [additive]

router bgp <ASnum>
    address-family <AF>
        neighbor <address> route-map SRTE-color-map out
    exit-address-family
    !
    address-family <AF> vrf <vrfname>
        neighbor <address> route-map SRTE-color-map out
    exit-address-family

```

BGP ネイバー インバウンド プレフィックスのカラーリング

カラー拡張コミュニティをインバウンド BGP プレフィックスアップデートにアタッチするには、次の設定を使用します。

```

route-map SRTE-color-map permit
    set extcommunity color <1-4294967295> [additive]

router bgp <ASnum>
    address-family <AF>
        neighbor <address> route-map SRTE-color-map in
    exit-address-family
    !
    address-family <AF> vrf <vrfname>
        neighbor <address> route-map SRTE-color-map in
    exit-address-family

```

BGP VRF エクスポートプレフィックスのカラーリング

この設定を使用して、VRFに関連付けられたエクスポートルートマップのカラー拡張コミュニティにしたがって、カラー拡張コミュニティを VPN プレフィックスにアタッチします。

```

route-map SRTE-color-map permit
    set extcommunity color <1-4294967295> [additive]

vrf def SRTE-VRF
    rd 1:1
    !
    address-family ipv4
        export map SRTE-color-map

```

```

exit-address-family
!
address-family ipv6
    export map SRTE-color-map
exit-address-family

```

BGP VRF インポートプレフィックスのカラーリング

この設定を使用して、VRF に関連付けられたインポートルートマップのカラー拡張コミュニティにしたがって、カラー拡張コミュニティを VPN プレフィックスにアタッチします。

```

route-map SRTE-color-map permit
    set extcommunity color <1-4294967295> [additive]

vrf def SRTE-VRF
    rd 1:1
    !
    address-family ipv4
        import map SRTE-color-map
    exit-address-family
    !
    address-family ipv6
        import map SRTE-color-map
    exit-address-family

```

BGP ルート再配布プレフィックスのカラーリング

BGP に再配布される BGP プレフィックスにカラー拡張コミュニティをアタッチするには、次の設定を使用します。

```

route-map SRTE-color-map permit
    set extcommunity color <1-4294967295> [additive]

router bgp <ASnum>
    address-family ipv4 vrf <vrf-name>
        redistribute <source-protocol> route-map SRTE-color-map
    or
        network <address> mask <network-mask> route-map SRTE-color-map
    exit-address-family
    !
    address-family ipv6 vrf <vrf-name>
        redistribute <source-protocol=> route-map SRTE-color-map
    or
        network <address>/masklen route-map SRTE-color-map
    exit-address-family

```

SRv6 L3VPN ODN 設定の確認

BGP の出力例

show prefix コマンドは、BGP プレフィックスパスに関連付けられたカラーとバインディング SID を表示します。

- show bgp vpnv4 unicast vrf <vrfname> <prefix>
- show bgp vpnv6 unicast vrf <vrfname> <prefix>

```

PE# show bgp vpnv4 unicast vrf red 22.22.22.22
BGP routing table entry for 1:1:22.22.22.22/32, version 44

```

```

Paths: (1 available, best #1, table red)
  Advertised to update-groups:
    1
  Refresh Epoch 2
  3, imported path from 2:2:22.22.22.22/32 (global)
    2023:1::1 (via default) from 1.1.1.3 (1.1.1.3)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:1:1 RT:2:2 Color:10
      Originator: 11.1.1.1, Cluster list: 1.1.1.3
      binding SID: 16777218 (color - 10) (state - UP)
      srv6 out-sid: FCCC:CC1:AA88:E000::
      rx pathid: 0, tx pathid: 0x0
      Updated on Mar 29 2023 12:38:45 PST

PE2#show bgp vpnv6 unicast vrf red 2222::1/128
BGP routing table entry for [1:1]2222::1/128, version 45
Paths: (1 available, best #1, table red)
  Advertised to update-groups:
    1
  Refresh Epoch 2
  3, imported path from [2:2]2222::1/128 (global)
    2023:1::1 (via default) from 1.1.1.3 (1.1.1.3)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:2:2 Color:11
      Originator: 11.1.1.1, Cluster list: 1.1.1.3
      binding SID: 16777220 (color - 11) (state - UP)
      srv6 out-sid: FCCC:CC1:AA88:E001::
      rx pathid: 0, tx pathid: 0x0
      Updated on Mar 30 2023 15:58:52 PST

```

SRv6 ODN ポリシーの出力例

show segment-routing traffic-eng policy name <name> コマンドは、SRv6 ODN SR ポリシー情報を表示します。

```

device#show segment-routing traffic-eng policy name *A006::1|1000

Name: *A006::1|1000 (Color: 1000 End-point: A006::1)
Owners : BGP
Status:
  Admin: up, Operational: up for 00:01:16 (since 11-23 09:57:11.624)
Candidate-paths:
  Preference 100 (BGP):
  Per-flow Information (active):
    Forward      PDP      PDP      BSID RW
    Class        Color    Status   Status
    -----
    0             10000    up       Pending
    1             10001    up       Pending
    2             10002    up       Pending
    3             10003    up       Pending
    4             10004    up       Pending
  Default Forward Class: 0
Attributes:
  IPv6 caps enabled

device#show segment-routing traffic-eng policy name *A006::1|10000

Name: *A006::1|10000 (Color: 10000 End-point: A006::1)
Owners : BGP-PFP-AUTO
Status:
  Admin: up, Operational: up for 00:02:23 (since 11-23 09:56:34.669)
Candidate-paths:
  Preference 100 (BGP-PFP-AUTO):

```

```

PM State: Up
Constraints:
  Affinity:
    include-all:
      non-voice
Dynamic (active)
  Metric Type: DELAY, Path Accumulated Metric: 120
  F:1:1:E002:: [Adjacency-SID]
  F:1:2:E002:: [Adjacency-SID]
  F:1:3:E002:: [Adjacency-SID]
Preference 50 (BGP-PFP-AUTO):
PM State: Up
Constraints:
  Affinity:
    include-all:
      voice
Dynamic (inactive)
  Metric Type: TE, Path Accumulated Metric: 30
  F:1:4:: [Node-SID]
  F:1:5:: [Node-SID]
  F:1:6:: [Node-SID]
Attributes:

```

show segment-routing traffic-eng policy name <name> detail コマンドは、SRv6 ODN ポリシーの詳細を表示します。

```
device#show segment-routing traffic-eng policy name *A006::1|1000 detail
```

```

Name: *A006::1|1000 (Color: 1000 End-point: A006::1)
Owners : BGP
Status:
  Admin: up, Operational: up for 00:01:20 (since 11-23 09:57:11.624)
Candidate-paths:
  Preference 100 (BGP):
  Per-flow Information (active):
    Forward      PDP      PDP      BSID RW
    Class        Color    Status   Status
    -----
    0            10000   up       Pending
    1            10001   up       Pending
    2            10002   up       Pending
    3            10003   up       Pending
    4            10004   up       Pending
  Default Forward Class: 0
Attributes:
  IPv6 caps enabled
  Forwarding-ID: 16778667
Per owner configs:
  BGP
  Binding SID: not configured
Stats:
  Packets: 0 Bytes: 0

Event history:
  Timestamp          Client      Event type      Context: Value
  -----
  11-23 09:56:34.668 BGP        Policy created  Name: BGP
  11-23 09:56:34.668 BGP        Set colour     Colour: 1000
  11-23 09:56:34.668 BGP        Set end point  End-point: A006::1
  11-23 09:56:34.669 BGP        Set dynamic pce Path option: per flow
  11-23 09:57:11.624 FH Resolution Policy state UP  Status: PFP RESOLVED CP:
100
  11-23 09:57:11.706 FH Resolution REOPT triggered Status: REOPTIMIZED CP: 100

```

```

11-23 09:57:11.711    FH Resolution    REOPT triggered    Status: REOPTIMIZED CP: 100
11-23 09:57:12.208    FH Resolution    REOPT triggered    Status: REOPTIMIZED CP: 100

```

```
device#show segment-routing traffic-eng policy name *A006::1|10000 detail
```

```

Name: *A006::1|10000 (Color: 10000 End-point: A006::1)
Owners : BGP-PFP-AUTO
Status:
  Admin: up, Operational: up for 00:02:28 (since 11-23 09:56:34.669)
Candidate-paths:
  Preference 100 (BGP-PFP-AUTO):
    PM State: Up
    Constraints:
      Affinity:
        include-all:
          non-voice
    Dynamic (active)
      Metric Type: DELAY, Path Accumulated Metric: 120
      F:1:1:E002:: [Adjacency-SID]
      F:1:2:E002:: [Adjacency-SID]
      F:1:3:E002:: [Adjacency-SID]
  Preference 50 (BGP-PFP-AUTO):
    PM State: Up
    Constraints:
      Affinity:
        include-all:
          voice
    Dynamic (inactive)
      Metric Type: TE, Path Accumulated Metric: 30
      F:1:4:: [Node-SID]
      F:1:5:: [Node-SID]
      F:1:6:: [Node-SID]
Attributes:
Forwarding-ID: 16778668
Per owner configs:
  BGP-PFP-AUTO
    Binding SID: not configured
    Performance-measurement:
      liveness-detection
      invalidation-action down
Stats:
  Packets: 0 Bytes: 0
PM profile: Not configured

Event history:
  Timestamp          Client          Event type          Context: Value
  -----          -
  11-23 09:56:34.669 BGP-PFP-AUTO    Policy created      Name: BGP-PFP-AUTO
  11-23 09:56:34.669 BGP-PFP-AUTO    Set colour          Colour: 10000
  11-23 09:56:34.670 BGP-PFP-AUTO    Set end point       End-point: A006::1
  11-23 09:56:34.670 BGP-PFP-AUTO    Set dynamic         Path option: dynamic
  11-23 09:56:34.672 BGP-PFP-AUTO    Set dynamic         Path option: dynamic
  11-23 09:56:34.673 BGP-PFP-AUTO    Set delay measure   status: Enabled
  11-23 09:56:34.673 BGP-PFP-AUTO    Set Live Detection  status: Enabled
  11-23 09:56:34.673 BGP-PFP-AUTO    Set Live Invalidation: down
  11-23 09:57:07.662 FH Resolution    Liveness            CP: 100, SL2153 is Waiting

  11-23 09:57:07.663 FH Resolution    Liveness            CP: 50, SL2154 is Waiting
  11-23 09:57:11.609 PM              Liveness            CP: 50, SL2154 is Up
  11-23 09:57:11.623 FH Resolution    Policy state UP     Status: PATH RESOLVED CP:
50
  11-23 09:57:12.740 PM              Liveness            CP: 100, SL2153 is Up
  11-23 09:57:12.766 FH Resolution    REOPT triggered     Status: REOPTIMIZED CP:

```

```

100      11-23 09:57:18.334    FH Resolution    REOPT triggered    Status: REOPTIMIZED CP:
100      11-23 09:57:18.382    PM                Liveness           CP: 50, SL2154 is Unknown
          11-23 09:57:19.922    FH Resolution    REOPT triggered    Status: REOPTIMIZED CP:
100      11-23 09:57:28.707    FH Resolution    REOPT triggered    Status: REOPTIMIZED CP:
100      11-23 09:57:28.708    FH Resolution    Liveness           CP: 50, SL2154 is Waiting
          11-23 09:57:28.709    FH Resolution    REOPT triggered    Status: REOPTIMIZED CP:
100      11-23 09:57:32.000    PM                Liveness           CP: 50, SL2154 is Up
          11-23 09:57:32.003    FH Resolution    REOPT triggered    Status: REOPTIMIZED CP:
100

```

SRv6-TE 設定の確認の詳細については、「[Verifying SRv6-TE Configuration](#)」の項を参照してください。

SRv6 L3VPN ODN 設定のデバッグ

SR ODN に関連するイベントを追跡するには、次の debug コマンドを使用します。

- **debug ip bgp sr-policy**

```

*Apr 10 17:35:48.773: BGP(4): 2023:1::3 rcvd UPDATE w/ attr: nexthop 2023:1::1, origin
?, localpref 100, metric 0, originator 11.1.1.1, clusterlist 1.1.1.3, merged path 3,
AS_PATH , extended community RT:1:1 RT:2:2 Color:10, PrefixSid attribute: SRV6 SID
FCCC:CCC1:AA88::
*Apr 10 17:35:48.773: BGP(4): 2023:1::3 rcvd 2:2:22.22.22.22/32, label 2162163712
(0x80E00000)
*Apr 10 17:35:48.773: BGP SRv6 SID ATTR: blk 32 node 16 fun 16 arg 0 pos 16 off 48
*Apr 10 17:35:48.774: BGP-SR Policy (7F7911708510): Binding SID 10/2023:1::1/ request
*Apr 10 17:35:48.774: BGP(4): Revise route installing 1 of 1 routes for 22.22.22.22/32
-> 0.0.0.0(red) to red IP table

PE2#show bgp vpnv4 uni vrf red 22.22.22.22
BGP routing table entry for 1:1:22.22.22.22/32, version 33
Paths: (1 available, best #1, table red)
  Advertised to update-groups:
    3
  Refresh Epoch 1
  3, imported path from 2:2:22.22.22.22/32 (global)
    2023:1::1 (via default) from 1.1.1.3 (1.1.1.3)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:1:1 RT:2:2 Color:10
      Originator: 11.1.1.1, Cluster list: 1.1.1.3
      binding SID: 16777219 (color - 10) (state - UP)
      srv6 out-sid: FCCC:CCC1:AA88:E000::
      rx pathid: 0, tx pathid: 0x0
      Updated on Apr 10 2023 09:35:48 PST

PE2(config)#segment-routing traffic-eng
PE2(config-srte-on-demand-color)#on-demand color 10

PE2(config-srte-on-demand-color)#no authorize
*Apr 10 17:37:25.964: BGP SR: color change notification callback for color 10, auth_type
3
*Apr 10 17:37:25.964: BGP SR: color change state handler for color 10, color_state 2
*Apr 10 17:37:25.964: BGP SR: deletion of policy *2023:1::1|10 is successful
*Apr 10 17:37:25.964: BGP SR: sr_policymgr color 10, delete: timer started
*Apr 10 17:37:26.678: BGP SR: Policy change timer expired.: bgp_sr_policy_service_change
started
*Apr 10 17:37:26.679: BGP(4): Revise route installing 1 of 1 routes for 5.5.6.8/32 ->

```

```

0.0.0.0(red) to red IP table
*Apr 10 17:37:26.680: BGP(4): Revise route installing 1 of 1 routes for 10.1.1.0/24 ->
0.0.0.0(red) to red IP table
*Apr 10 17:37:26.680: BGP(4): Revise route installing 1 of 1 routes for 22.22.22.22/32
-> 0.0.0.0(red) to red IP table
PE2(config-srte-on-demand-color)#do sh bgp vpnv4 uni vrf red 22.22.22.22
BGP routing table entry for 1:1:22.22.22.22/32, version 30
Paths: (1 available, best #1, table red)
  Advertised to update-groups:
    3
  Refresh Epoch 1
  3, imported path from 2:2:22.22.22.22/32 (global)
  2023:1::1 (via default) from 1.1.1.3 (1.1.1.3)
    Origin incomplete, metric 0, localpref 100, valid, internal, best
    Extended Community: RT:1:1 RT:2:2 Color:10
    Originator: 11.1.1.1, Cluster list: 1.1.1.3
    binding SID: none (color-10)
    srv6 out-sid: FCCC:CCCL:AA88:E000::
    rx pathid: 0, tx pathid: 0x0
    Updated on Apr 10 2023 09:35:48 PST

PE2(config-srte-on-demand-color)#authorize
*Apr 10 17:37:41.096: BGP SR: color change notification callback for color 10, auth_type
  2
*Apr 10 17:37:41.096: BGP SR: color change state handler for color 10, color_state 1
*Apr 10 17:37:41.096: BGP SR POLICY: policy *2023:1::1|10 create request
*Apr 10 17:37:41.097: BGP SR: sr_policymgr color 10, add
*Apr 10 17:37:41.097: BGP SR: Policy change for *2023:1::1|10, type 5, bsid 0
*Apr 10 17:37:41.097: BGP SR Policy Change notification: color: 10, nexthop: 2023:1::1:
  timer started
*Apr 10 17:37:41.097: BGP_SR_POLICY: policy *2023:1::1|10 registered for policy
notification
*Apr 10 17:37:41.097: BGP SR: Policy change for *2023:1::1|10, type 3, bsid 1000003
*Apr 10 17:37:41.097: BGP SR Policy Change notification: color: 10, nexthop: 2023:1::1
*Apr 10 17:37:41.097: BGP SR Policy Found: color: 10, nexthop: 2023:1::1: timer already
  running
*Apr 10 17:37:41.097: BGP SR: Policy change for *2023:1::1|10, type 4, bsid 1000003
*Apr 10 17:37:41.097: BGP SR Policy Change notification: color: 10, nexthop: 2023:1::1
*Apr 10 17:37:41.097: BGP SR Policy Found: color: 10, nexthop: 2023:1::1: timer already
  running
*Apr 10 17:37:42.039: BGP SR: Policy change timer expired.: bgp_sr_policy_service_change
  started
*Apr 10 17:37:42.040: BGP(4): Revise route installing 1 of 1 routes for 5.5.6.8/32 ->
0.0.0.0(red) to red IP table
*Apr 10 17:37:42.040: BGP(4): Revise route installing 1 of 1 routes for 10.1.1.0/24 ->
0.0.0.0(red) to red IP table
*Apr 10 17:37:42.040: BGP(4): Revise route installing 1 of 1 routes for 22.22.22.22/32
-> 0.0.0.0(red) to red IP table
PE2(config-srte-on-demand-color)#do sh bgp vpnv4 uni vrf red 22.22.22.22
BGP routing table entry for 1:1:22.22.22.22/32, version 33
Paths: (1 available, best #1, table red)
  Advertised to update-groups:
    3
  Refresh Epoch 1
  3, imported path from 2:2:22.22.22.22/32 (global)
  2023:1::1 (via default) from 1.1.1.3 (1.1.1.3)
    Origin incomplete, metric 0, localpref 100, valid, internal, best
    Extended Community: RT:1:1 RT:2:2 Color:10
    Originator: 11.1.1.1, Cluster list: 1.1.1.3
    binding SID: 16777219 (color - 10) (state - UP)
    srv6 out-sid: FCCC:CCCL:AA88:E000::
    rx pathid: 0, tx pathid: 0x0
    Updated on Apr 10 2023 09:35:48 PST

```

SRv6-TE のトラブルシューティングとデバッグの詳細については、「[Troubleshooting and Debugging SRv6-TE](#)」の項を参照してください。

SRv6 トラフィック エンジニアリング ポリシー

SRv6 トラフィック エンジニアリング ポリシー

Cisco IOS XE 17.12.1a以降、セグメントルーティングトラフィックエンジニアリング (SR-TE) メカニズムが Segment Routing over IPv6 (SRv6) に拡張されています。

SRv6-TE ポリシーに関する制約事項

- ローカルパスのみがサポートされます。パス計算の PCE 委任はサポートされません。
- ダイナミック セグメント リストのみがサポートされます。明示的なセグメントリストはサポートされません。
- SRv6 バインディング SID はサポートされません。
- オンデマンドネクストホップ (ODN) はサポートされません。
- SR-TE を介した L2VPN はサポートされません。
- PFP または PDP を介した自動ルート通知はサポートされません。
- 複数の SID を使用してポリシーを作成すると、出力 PE に到達する最後の SID はノード SID であり、SID リストから削除されます。
- VPN SID には、SID の一部として常にロケータ情報が含まれている必要があります。

SRv6-TE ポリシーに関する情報

SRv6 トラフィック エンジニアリング (SRv6-TE) では、ネットワークを介してトラフィックをステアリングする SRv6 ポリシーを使用します。SRv6 ポリシーにはフロー別ポリシー (PFP) と宛先別ポリシー (PDP) が含まれており、どちらもサポートされています。

ePBR ポリシーは、トラフィックを分類して転送クラス (FC) に関連付ける方法を定義するために、入力インターフェイスに適用されます。PFP は、最大 8 エントリのフロー別転送クラステーブルで設定されます。各エントリは FC によってインデックス化され、PDP を指し示します。

PFP では、パケットは入力インターフェイスで分類され、ePBR による分類に基づいて同じ宛先に転送するためにさまざまな PDP パスを選択します。

SRv6-TE の設定

次の例は、SRv6-TE の設定方法を示しています。

PDP の設定

```

segment-routing traffic-eng
  policy SRV6PM
    color 1 end-point C02:1::1
    candidate-paths
      preference 1
      constraints
        segments
          dataplane srv6
      !
      !
      dynamic
      !
      !
    !
    preference 2
    constraints
      segments
        dataplane srv6
      !
      affinity
        exclude-any
          name blue
      !
      !
      dynamic
        metric
          type delay
      !
      !
    performance-measurement
      delay-measurement
        liveness-detection
          invalidation-action down
      !
      !
      !

```

PFP の設定

```

segment-routing traffic-eng
  policy PFP
    color 100 end-point C02:1::1
    candidate-paths
      preference 1
      per-flow
        forward-class 0 color 1
        forward-class 1 color 2
        forward-class 2 color 3
        forward-class 3 color 4
        forward-class 4 color 5

```

ePBR の設定

```

policy-map type epbr PFP
  class FC1
    set forward-class 1
  class FC2
    set forward-class 2
  class FC3
    set forward-class 3

```

```

class FC4
  set forward-class 4
class class-default
  set forward-class 0

interface TenGigabitEthernet2/2/0.1000
  encapsulation dot1Q 1000
  vrf forwarding vpn-1000
  ip address 17.0.0.1 255.255.255.0
  ipv6 address 1700::1/64
  service-policy type epbr input PFP

```

スタティック ルートの設定

1. プレフィックスの IPv6 静的ルート、NO SR ポリシー、およびオプションの VPN SID

```

ipv6 route vrf blue 1002:1::/64 2001:1::2 nexthop-vrf default sid-list h-encaps-red
  FCCC:CC1:C3:E005::

```

2. オプションの SR ポリシーと VPN SID を介してステアリングされるトラフィックを持つプレフィックスの IPv6 静的ルート

```

ipv6 route vrf blue 1002:1::/64 segment-routing srv6 via policy PFP sid-list
  h-encaps-red FCCC:CC1:C3:E005::

```

3. オプションの SR ポリシーと VPN SID を介してステアリングされるトラフィックを持つプレフィックスの IPv4 静的ルート

```

ip route vrf blue 2.2.2.2 255.255.255.255 segment-routing srv6 via policy PFP sid-list
  h-encaps-red FCCC:CC1:C3:E004::

```



(注) プレフィックスの IPv4 静的ルート、NO SR ポリシー、およびオプションの VPN SID はサポートされていません。

SRv6-TE の設定の確認

例 1 : `show segment-routing traffic-eng policy name` コマンドを使用して、PDP および PFP を使用した SRv6-TE の設定を確認します。

```

router# show segment-routing traffic-eng policy name SRV6PM detail

Name: SRV6PM (Color: 1 End-point: C02:1:1)
Owners : CLI
Status:
  Admin: up, Operational: up for 70:55:04 (since 04-11 12:10:05.054)
Candidate-paths:
  Preference 2 (CLI):
    PM State: Up
    Constraints:
      Affinity:
        exclude-any:
          blue
    Dynamic (active)
      Metric Type: DELAY, Path Accumulated Metric: 40
      FCCC:CC1:AA22:: [Node-SID]
      FCCC:CC1:AA33:: [Node-SID]

```

```

        FCCC:CC1:AA11:: [Node-SID]
        FCCC:CC1:AA11:E001:: [Adjacency-SID]
Preference 1 (CLI):
  PM State: Unknown
  Dynamic (inactive)
    Inactive Reason: Perf Measure State Change to Pending
  Metric Type: TE, Path Accumulated Metric: 10
  FCCC:CC1:C3:: [Node-SID]
Attributes:
Forwarding-ID: 16777217
Per owner configs:
  CLI
    Binding SID: not configured
    Performance-measurement:
      liveness-detection
      invalidation-action down
Stats:
  Packets: 0 Bytes: 0
  PM profile: Not configured

router# show segment-routing traffic-eng policy name PFP

Name: PFP (Color: 100 End-point: C02:1::1)
Owners : CLI
Status:
  Admin: up, Operational: up for 00:03:00 (since 04-17 10:46:06.552)
Candidate-paths:
Preference 1 (CLI):
  Per-flow Information (active):
    Forward      PDP      PDP  BSID RW
    Class        Color    Status Status
    -----
           0          1      up  Pending
           1          2      up  Pending
  Default Forward Class: 0
Attributes:

```

例 2 : `show ip cef label-table <label> internal` コマンドを使用して、PFP ラベルの詳細を表示します。

```

router# show ip cef label-table 16777218 internal
Label-FIB is Enabled
VRF Default
  3 prefixes (3/0 fwd/non-fwd)
  Table id 0x30000000
  Database epoch:      0 (3 entries at this epoch)

16777218 , epoch 0, refcnt 8, per-destination sharing
sources: RR, Bnd-Lbl-SRv6-Pol
subblocks:
  1 RR source [no flags]
  Binding Label SRv6 Policy: 16777218
  Policy-Name: PFP (16777218) è PFP Policy Name
  Path: 0
    Flags: 00000000
    IPv6 Header Parameters
      TC: 0 Flow: 0 Hop Limit: 0
      Src: C01:1::1
      Dst: 16777217
    Segment List (0)
  Path: 1
    Flags: 00000000
    IPv6 Header Parameters

```

```

TC: 0   Flow: 0           Hop Limit: 0
Src: C01:1::1
Dst: 16777217
Segment List (0)
Path: 2
Flags: 00000000
IPv6 Header Parameters
TC: 0   Flow: 0           Hop Limit: 0
Src: C01:1::1
Dst: 16777217
Segment List (0)
Path: 3
Flags: 00000000
IPv6 Header Parameters
TC: 0   Flow: 0           Hop Limit: 0
Src: C01:1::1
Dst: 16777217
Segment List (0)
Path: 4
Flags: 00000000
IPv6 Header Parameters
TC: 0   Flow: 0           Hop Limit: 0
Src: C01:1::1
Dst: 16777217
Segment List (0)
Path: 5
Flags: 00000000
IPv6 Header Parameters
TC: 0   Flow: 0           Hop Limit: 0
Src: C01:1::1
Dst: 16777217
Segment List (0)
Path: 6
Flags: 00000000
IPv6 Header Parameters
TC: 0   Flow: 0           Hop Limit: 0
Src: C01:1::1
Dst: 16777217
Segment List (0)
Path: 7
Flags: 00000000
IPv6 Header Parameters
TC: 0   Flow: 0           Hop Limit: 0
Src: C01:1::1
Dst: 16777217
Segment List (0)

```

例 3 : `show segment-routing traffic-eng cspf` コマンドを使用して、CSPF の詳細を表示します。

```
router# show segment-routing traffic-eng cspf ipv6 source A001::1 destination A006::1
metric-type delay
```

```
Path:
HOP0: SRv6 NODE SID=F:1:6::
Path Cost = 10

CSPF result: Shortest Path Success (rc=8)
```

例 4 : `show prefix` コマンドを使用して、BGP プレフィックスパスに関連付けられたカラーとバインディング SID を表示します。

```

router# show bgp vpnv4 unicast vrf red 22.22.22.22
BGP routing table entry for 1:1:22.22.22.22/32, version 14
Paths: (1 available, best #1, table red)
Advertised to update-groups:
3
Refresh Epoch 1
3, imported path from 2:2:22.22.22.22/32 (global)
2023:1::1 (via default) from 1.1.1.3 (1.1.1.3)
Origin incomplete, metric 0, localpref 100, valid, internal, best
Extended Community: RT:1:1 RT:2:2 Color:10
Originator: 11.1.1.1, Cluster list: 1.1.1.3
binding SID: 16777217 (color - 10) (state - UP)
srv6 out-sid: FCCC:CC1:AA88:E000::
rx pathid: 0, tx pathid: 0x0
Updated on Jun 12 2023 15:33:20 PST

router# show bgp vpnv6 unicast vrf red 2222::1/128
BGP routing table entry for [1:1]2222::1/128, version 13
Paths: (1 available, best #1, table red)
Advertised to update-groups:
3
Refresh Epoch 1
3, imported path from [2:2]2222::1/128 (global)
2023:1::1 (via default) from 1.1.1.3 (1.1.1.3)
Origin incomplete, metric 0, localpref 100, valid, internal, best
Extended Community: RT:2:2 Color:10
Originator: 11.1.1.1, Cluster list: 1.1.1.3
binding SID: 16777217 (color - 10) (state - UP)
srv6 out-sid: FCCC:CC1:AA88:E001::
rx pathid: 0, tx pathid: 0x0
Updated on Jun 12 2023 15:33:20 PST

```

SRv6-TE のトラブルシューティングとデバッグ

SRv6TE をトラブルシューティングするには、次のコマンドを使用します。

- **debug ip bgp sr-policy**
- **debug segment-routing traffic-eng**
 - **forwarding** : SR 転送のデバッグ
 - **ha** : SR ハイアベイラビリティ デバッグ
 - **path** : SR パスのデバッグ
 - **pcalc** : SR pcalc のデバッグ
 - **policy** : SR ポリシーのデバッグ
 - **topology** : SR トポロジーのデバッグ

```

router# debug ip bgp sr-policy
*Apr 10 17:35:48.773: BGP(4): 2023:1::3 rcvd UPDATE w/ attr: nexthop 2023:1::1, origin
?, localpref 100, metric 0, originator 11.1.1.1, clusterlist 1.1.1.3, merged path 3,
AS_PATH , extended community RT:1:1 RT:2:2 Color:10, PrefixSid attribute: SRV6 SID
FCCC:CC1:AA88::
*Apr 10 17:35:48.773: BGP(4): 2023:1::3 rcvd 2:2:22.22.22.22/32, label 2162163712
(0x80E00000)
*Apr 10 17:35:48.773: BGP SRv6 SID ATTR: blk 32 node 16 fun 16 arg 0 pos 16 off 48
*Apr 10 17:35:48.774: BGP-SR Policy (7F7911708510): Binding SID 10/2023:1::1/ request

```

```
*Apr 10 17:35:48.774: BGP(4): Revise route installing 1 of 1 routes for 22.22.22.22/32
-> 0.0.0.0(red) to red IP table
```

SRv6 のパフォーマンス測定

SRv6 のパフォーマンス測定

機能名	リリース情報	説明
IPv6 を介したセグメントルーティングのパフォーマンス測定	Cisco IOS XE Dublin 17.12.1a	この機能は、IPv6 データプレーンを介したセグメントルーティング設定にパフォーマンス測定の活性を拡張します。

SRv6 のパフォーマンス測定の活性

Cisco IOS XE 17.12.1a 以降、パフォーマンス測定の活性は、IPv6 データプレーンを介したセグメントルーティングに拡張されます。

この機能により、PM プローブを使用して、転送テーブルに存在するすべての候補パスのすべてのセグメントリストで SR ポリシーのパフォーマンス測定 (PM) の活性を検出できるようになります。トラフィックパスをモニターし、ケーブルやハードウェアの不具合または設定ミスによるトラフィックのドロップを効率的に検出できます。

前提条件

- SRv6 の PM を設定する前に、すべてのノードで SRV6 を有効にする必要があります。

制約事項

- デフォルトでは、プローブは 3 秒ごとに送信されます。バースト間隔パラメータ (*) を使用してインターバルを延ばすことができます。プローブ間隔を 3 秒未満に短縮することは推奨されません。

SRv6 の PM 活性の設定

SRv6 の PM 活性を設定するには、次の例を使用します。

- SRV6 ポリシーで **liveness-detection** 設定を使用して、SRV6 パスの状態を継続的にモニターします。このオプションはモニタリングのみを行います。ポリシーマネージャによるアクションは実行されません。
- invalidation-action down** 設定を使用して、ポリシーマネージャを次のように設定します。
 - PM プローブで検証された後にも、HW でパスをプログラムする。

- パスを継続的にモニターする。
- PM プローブが機能しなくなった場合は、別の CP に再最適化する、または他のパスが使用できない場合は、ポリシーを停止する。

ポリシーでの SRv6-TE PM 活性の設定

```
policy SRV6PM
  performance-measurement
  delay-measurement
  liveness-detection
  invalidation-action down
```

活性のデフォルト遅延プロファイルの設定

```
performance-measurement
  delay-profile sr-policy
  probe
  liveness-detection
  multiplier 3
```

次のセクションでは、スケーリング展開の推奨設定について説明します。

すべての PE ノードの PM パントポリサーの設定

```
platform punt-policer sr-twamp-probe 3000
platform punt-policer sr-twamp-probe 3000 high
performance-measurement
  max-pps 3000
```

ヘッドエンドおよびエンドポイントノードでの WAN インターフェイスのインターフェイスキューの設定

```
interface Tunnel121
  hold-queue 10000 in
```

または

```
interface GigabitEthernet0/0/1
  hold-queue 10000 in
```



(注) WAN インターフェイスには、物理インターフェイスと GRE-TP トンネルが含まれます。

SRv6 のパフォーマンス測定の確認

SRv6 の PM 設定を確認するには、次の show コマンドを使用します。

例 1 : `show performance-measurement sr-policy name <name>`

```
device# show performance-measurement sr-policy name SRV6PM
SR Policy name: SRV6PM
Color                               : 1
```

```

Endpoint                : C02:1::1
Source                  : C01:1::1
Profile name            : Not configured
Policy Update Timestamp : 04-11 12:12:51.658
Number of candidate-paths : 2
Candidate-Path:
  Preference            : 1
  Protocol-origin       : CLI
  Discriminator         : 0
  Number of segment-lists : 1
  Number of atomic paths : 1
  Number of live UP atomic paths: 0
  Number of live Unknown atomic : 0
  Max Pkts per Burst    : 1500
  Max Pkts per Probe    : 15000
  AP Min Run per Probe  : 3
  Round-robin bursts    : 1
  Round-robin probes    : 1
  Last advertisement:
    Advertised at: 12:12:06 04-11 2023 (516007 seconds ago)
Atomic path:
  Hops                  : C2:1::1, C3:1::1, C1:1::1
                        : 2021:2::1
  Labels                : FCCC:CC1:AA22:AA33:AA11:E004::
  Outgoing Interface    : Ethernet0/2
  Max IP MTU            : 1500
  Next Hop              : FE80::A8BB:CCFF:FE00:FA10
  Destination           : C02:1::1
  Session ID            : 8
  Last advertisement:
    No advertisements have occurred
  Next advertisement:
    Aggregated delays (uSec): avg: 2744, min: 1480, max: 21676, variance: 1172
    Rolling average (uSec): 2744
  Last probe:
    Packets Sent: 10, received: 10
    Measured delays (uSec): avg: 1666, min: 1480, max: 1853, variance: 186
  Current probe:
    Packets Sent: 2, received: 2
    Measured delays (uSec): avg: 6192, min: 1619, max: 10765, variance: 4573
  Probe samples:
    Packet Rx Timestamp      Measured Delay (nsec)
    11:37:29 04-17 2023      1619000
    11:37:26 04-17 2023      10765000

```

例 2 : show performance-measurement sr-policy name <name> d p v | s Liveness

```

device# show performance-measurement sr-policy name SRV6PM d p v | s Liveness
Liveness Detection:
  Session Creation Timestamp: 04-11 12:10:49.981
  Session State: Down
  Last State Change Timestamp: 04-11 12:12:51.656
  Missed count [consecutive]: 84752
  Received count [consecutive]: 0
  Backoff      : 1
  Unique Path Name : Path-10
  Loss in Last Interval : 100 % [TX: 7 RX: 0]
Liveness Detection:
  Session Creation Timestamp: 04-11 12:12:36.636
  Session State: Up
  Last State Change Timestamp: 04-11 12:12:36.728
  Missed count [consecutive]: 0
  Received count [consecutive]: 84717

```

```

Backoff : 0
Unique Path Name : Path-12
Loss in Last Interval : 0 % [TX: 7 RX: 7]
Liveness Detection:
Session Creation Timestamp: 04-11 12:12:36.636
Session State: Up
Last State Change Timestamp: 04-11 12:12:36.728
Missed count [consecutive]: 0
Received count [consecutive]: 84717
Backoff : 0
Unique Path Name : Path-13
Loss in Last Interval : 0 % [TX: 7 RX: 7]

```

例 3 : show segment-routing traffic-eng policy all type per-destination

```

device# show segment-routing traffic-eng policy all type per-destination
Name: SRV6PM (Color: 1 End-point: C02:1::1)
Owners : CLI
Status:
  Admin: up, Operational: up for 70:55:04 (since 04-11 12:10:05.054)
Candidate-paths:
  Preference 2 (CLI):
    PM State: Up
    Constraints:
      Affinity:
        exclude-any:
          blue
    Dynamic (active)
      Metric Type: DELAY, Path Accumulated Metric: 40
      FCCC:CC1:AA22:: [Node-SID]
      FCCC:CC1:AA33:: [Node-SID]
      FCCC:CC1:AA11:: [Node-SID]
      FCCC:CC1:AA11:E001:: [Adjacency-SID]
  Preference 1 (CLI):
    PM State: Unknown
    Dynamic (inactive)
      Inactive Reason: Perf Measure State Change to Pending
      Metric Type: TE, Path Accumulated Metric: 10
      FCCC:CC1:C3:: [Node-SID]
Attributes:

```

例 4 : show performance-measurement history interfaces adv

```

device# show performance-measurement history interfaces adv
Interface Name: Ethernet0/0 (ifh: 0x2)
Delay-Measurement history (uSec):
  Session ID: 1
  Advertisement Timestamp   Average   Min      Max      Action
  12:10:05 04-11 2023       10       10       10       CFG
Interface Name: Ethernet0/1 (ifh: 0x3)
Delay-Measurement history (uSec):
  Session ID: 2
  Advertisement Timestamp   Average   Min      Max      Action
  12:10:05 04-11 2023       15       15       15       CFG
Interface Name: Tunnel100 (ifh: 0x15)
Delay-Measurement history (uSec):
  Session ID: 3
  Advertisement Timestamp   Average   Min      Max      Action
  13:10:55 04-13 2023       603      307      969      PER-MIN
  13:04:46 04-13 2023       8696     1384     18908    PER-MIN
  10:31:05 04-13 2023       6897     377     38335    PER-MIN
  10:26:56 04-13 2023       6792     1802     13778    PER-MIN

```

```

12:12:26 04-11 2023      3018      363      14081      FIRST
Interface Name: Tunnell101 (ifh: 0x16)
Delay-Measurement history (uSec):
Session ID: 4
Advertisement Timestamp   Average   Min       Max       Action
12:12:16 04-11 2023     1841     263      8400     FIRST

```

例 5 : show performance-measurement history sr-policy liveness-notification

```

device# show performance-measurement history sr-policy liveness-notification
SR Policy name: pdp-voice

```

```

Candidate-Path:
Preference           : 10
Protocol-origin      : CLI
Discriminator        : 0
Active               : No
Segment-list:
Name                 : SL13
Atomic path:
Hops                 : A006::1
Labels               : ::
Outgoing Interface   : Tunnell16
Next Hop             : 1634::6
Destination          : A006::1
Delay-Measurement:
Session ID           : 16
Liveness state change timestamp           New State
04:20:25 01-15 2023                               Up

```

```

Candidate-Path:
Preference           : 50
Protocol-origin      : CLI
Discriminator        : 0
Active               : No
Segment-list:
Name                 : SL12
Atomic path:
Hops                 : ::, ::, 5646::5
Labels               : F:1:2:5:E003::
Outgoing Interface   : Tunnell12
Next Hop             : 1211::2
Destination          : A006::1
Delay-Measurement:
Session ID           : 23
Liveness state change timestamp           New State
04:30:19 01-15 2023                               Up

```

```

Candidate-Path:
Preference           : 100
Protocol-origin      : CLI
Discriminator        : 0
Active               : Yes
Segment-list:
Name                 : SL11
Atomic path:
Hops                 : ::, ::, 5631::5
Labels               : F:1:4:5:E002::
Outgoing Interface   : GigabitEthernet2
Next Hop             : FE80::5054:FF:FE1A:DD62
Destination          : A006::1
Delay-Measurement:
Session ID           : 14

```

```

Liveness state change timestamp          New State
04:20:17 01-15 2023                    Up

```

例 6 : show isis teapp

```

device# show isis teapp
Tag null:
  ISIS TEAPP Information: Topology(ID:0x0) Type:SRTE, Enabled:1, Router ID:0.0.0.0 IPv6
Router ID:C01:1::1
Topology Id:0x0 Teapp_type:SRTE
  Interface(hdl:0x2): Ethernet0/0
    Affinity: set 1, affinity_bits 8
    TE Metric: set 1, te_metric 1000
    Extended Affinity: set 1, length 1, ext_affinity_bits: 8
Topology Id:0x0 Teapp_type:SRTE
  Interface(hdl:0x3): Ethernet0/1
    Affinity: set 1, affinity_bits 8
    TE Metric: set 1, te_metric 1000
    Extended Affinity: set 1, length 1, ext_affinity_bits: 8
ISIS TE Attr PM Information:
Et0/0: IDB num:2 Min:10 Max:10 Min-max-anomaly:0 Avg:10 Avg-anomaly:0 Var:0
      Is-Loss-set:0 Loss:0 Loss-anomaly:0
Et0/1: IDB num:3 Min:15 Max:15 Min-max-anomaly:0 Avg:15 Avg-anomaly:0 Var:0
      Is-Loss-set:0 Loss:0 Loss-anomaly:0
Tu100: IDB num:21 Min:307 Max:969 Min-max-anomaly:0 Avg:603 Avg-anomaly:0 Var:109
      Is-Loss-set:0 Loss:0 Loss-anomaly:0
Tu101: IDB num:22 Min:263 Max:8400 Min-max-anomaly:0 Avg:1841 Avg-anomaly:0 Var:1042
      Is-Loss-set:0 Loss:0 Loss-anomaly:0
device#

```

例 7 : show performance-measurement responder summary

```

device# show performance-measurement responder summary
Total interfaces                : 5
Total query packets received    : 509200
Total reply packets sent        : 509200
Total reply packets sent errors : 0
Total URO TLV not present errors : 0
Total invalid port number errors : 0
Total no source address errors  : 0
Total no return path errors     : 0
Total unsupported querier control code errors : 0
Total unsupported timestamp format errors : 0
Total timestamp not available errors : 0
Total unsupported mandatory TLV errors : 0
Total invalid packet errors     : 0
Total loss probe color errors   : 0
Current rate                    : 1 pkts/sec
Rate high water mark            : 3 pkts/sec

```

例 8 : show monitor event-trace perf_measure all

```

device# show monitor event-trace perf_measure all
Perf Measure error events:
Perf Measure event events:
*Apr 11 17:10:05.115: PM-TRACE-IGP-ADV :flood Ethernet0/0 10 10 10
*Apr 11 17:10:05.116: PM-TRACE-IGP-ADV :flood Ethernet0/1 15 15 15
*Apr 11 17:12:16.492: PM-TRACE-IGP-ADV :flood Tunnel101 263 8400 1841
*Apr 11 17:12:26.582: PM-TRACE-IGP-ADV :flood Tunnel100 363 14081 3018
*Apr 13 15:26:56.861: PM-TRACE-IGP-ADV :flood Tunnel100 1802 13778 6792

```

```
*Apr 13 15:31:05.510: PM-TRACE-IGP-ADV :flood Tunnel100 377 38335 6897
*Apr 13 18:04:46.608: PM-TRACE-IGP-ADV :flood Tunnel100 1384 18908 8696
*Apr 13 18:10:55.245: PM-TRACE-IGP-ADV :flood Tunnel100 307 969 603
interrupt context allocation count = 0
```

例 9 : show performance-measurement summary

```
device# show performance-measurement summary
Total interfaces                : 4
Total SR Policies               : 2
Total endpoints                 : 0
Maximum PPS                     : 2000 pkts/sec
Dual-color gre bit-position     : 9 - Failed, last success 0
Interface Delay-Measurement:
  Total sessions                : 4
  Counters:
    Packets:
      Total sent                 : 338865
      Total received             : 338861
    Errors:
      Total sent errors          : 14
      Total received errors      : 0
    Probes:
      Total started              : 33892
      Total completed            : 33884
      Total incomplete           : 4
      Total advertisements       : 8
SR Policy Delay-Measurement:
  Total sessions                : 4
  Counters:
    Packets:
      Total sent                 : 339076
      Total received             : 169602
    Errors:
      Total sent errors          : 0
      Total received errors      : 0
    Probes:
      Total started              : 33912
      Total completed            : 16964
      Total incomplete           : 16948
      Total advertisements       : 243
```

SRv6 OAM

SRv6 の運用、管理、およびメンテナンス

Cisco IOS XE 17.12.1a 以降、運用、管理、およびメンテナンス (OAM) 機能は、セグメントリストと SRv6 ポリシーを使用して SRv6 によってサポートされます。

SRv6 に関する制約事項

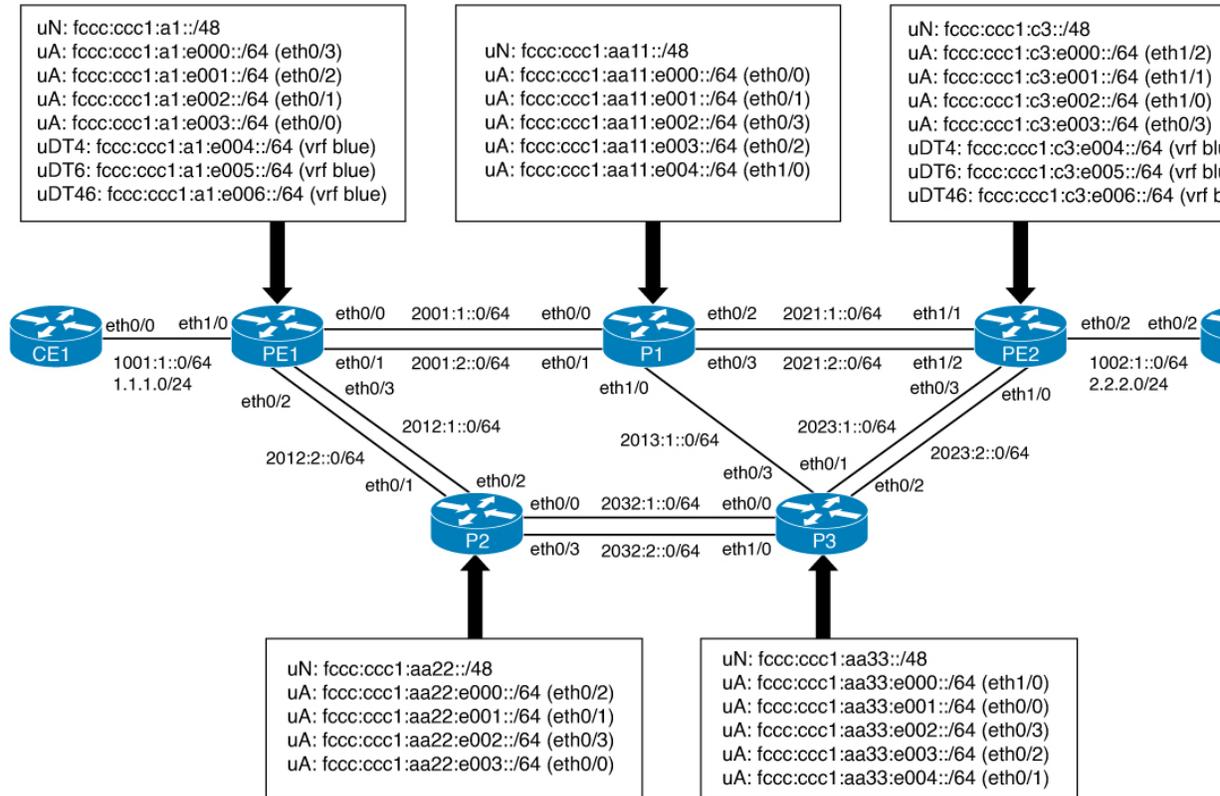
- IPv4 VRF へのトレースルートでは、コア PE ノードは表示されません。
- カスタム SID リストを使用した Ping または Traceroute IPv4 VRF はサポートされていません。

SRv6 OAM に関する情報

運用、管理、およびメンテナンス（OAM）により、サービスプロバイダーはSRv6パスをモニターして転送の問題を迅速に隔離し、ネットワークの異常検出とトラブルシューティングを支援できます。

次の図に、SRv6 OAM のトポロジの例を示します。

図 41: SRv6 OAM トポロジの例



SRv6 OAM の操作

SRv6 OAM には次の操作が含まれます。

- SRv6 コアを介した IPv6 Ping/Traceroute CE-CE
- SRv6 コアを介した IPv4 Ping/Traceroute CE-CE
- SRv6 コアを介した IPv6 Ping/Traceroute PE-CE
- SRv6 コアを介した IPv4 Ping/Traceroute PE-CE
- IPv6 SID Ping/Traceroute
- カスタム SID を使用した IPv6 VRF Ping/Traceroute

次の例は、図 x のトポロジを参照しています。

SRv6 コアを介した IPv6 Ping/Traceroute CE-CE の操作

Ping/Traceroute CE-CE 接続された IPv6 インターフェイス IP を操作するには、次の例を使用します。

```
CE1#ping 1002:1::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1002:1::2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/7 ms
CE1#
```

```
CE1#traceroute 1002:1::2 probe 1
Type escape sequence to abort.
Tracing the route to 1002:1::2
 1 1001:1::1 1 msec
 2 1002:1::2 1 msec
CE1#
```

SRv6 コアを介した IPv4 Ping/Traceroute CE-CE の操作

Ping/Traceroute CE-CE 接続された IPv4 インターフェイス IP を操作するには、次の例を使用します。

```
CE1#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
CE1#
```

```
CE1#traceroute 2.2.2.2 probe 1
Type escape sequence to abort.
Tracing the route to 2.2.2.2
VRF info: (vrf in name/id, vrf out name/id)
 1 1.1.1.1 1 msec
 2 2.2.2.2 1 msec
CE1#
```

SRv6 コアを介した IPv6 Ping/Traceroute PE-CE の操作

SRv6 コアを介して PE の VRF インターフェイスから Ping/Traceroute CE の IPv6 インターフェイスを操作するには、次の例を使用します。

```
PE1#ping vrf blue 1002:1::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1002:1::2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
PE1#
```

```
PE1#traceroute vrf blue 1002:1::2 probe 1
Type escape sequence to abort.
Tracing the route to 1002:1::2
 1 2001:1::2 1 msec
 2 2021:2::2 1 msec
 3 1002:1::2 1 msec
PE1#
```

SRv6 コアを介した IPv4 Ping/Traceroute PE-CE の操作

SRv6 コアを介して PE の VRF インターフェイスから Ping/Traceroute CE の IPv4 インターフェイスを操作するには、次の例を使用します。

```
PE1#ping vrf blue 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
PE1#

PE1#traceroute vrf blue 2.2.2.2 probe 1
Type escape sequence to abort.
Tracing the route to 2.2.2.2
VRF info: (vrf in name/id, vrf out name/id)
 1 *
 2 *
 3 2.2.2.2 1 msec
PE1#
```



(注) IPv4 ping は IPv6 ホップの代わりに「*」を表示します。

IPv6 SID Ping/Traceroute の操作

PE1 から Ping/Traceroute PE2 のノード SID SRv6 SID を操作するには、次の例を使用します。

```
PE1#ping FCCC:CCC1:C3::
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FCCC:CCC1:C3::, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
PE1#

PE1#traceroute FCCC:CCC1:C3:: probe 1
Type escape sequence to abort.
Tracing the route to FCCC:CCC1:C3::
 1 2001:1::2 0 msec
 2 2021:2::2 0 msec
PE1#
```

カスタム SID を使用した IPv6 VRF Ping/Traceroute の操作

カスタム SRv6 SID リストを使用して PE1 から Ping/Traceroute CE2 IPv6 インターフェイスを操作するには、次の例を使用します。

このトレースルートの SID は、PE1 から P1、P2、および P3 を介して PE2 に向かい、最後に CE2 に移動します。

- 最初の SID は PE1 から P1 です。
- P1 から P2 への次の SID は、P3 を介した ECMP パスです (P1 -> P3 -> P2)。
- VPN-SID PE2 に到達する次の SID は、P2 -> P3 -> PE2 です。
- 最後の SID は、PE2 から CE2 に到達することです (PE2 -> CE2)。

```
PE1#ping srv6 vrf blue 1002:1::2 via segment-list FCCC:CC1:AA11:AA22:C3:E005::
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1002:1::2 via [
  FCCC:CC1:AA11:AA22:C3:E005:], timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
PE1#

PE1# traceroute srv6 vrf blue 1002:1::2 via segment-list FCCC:CC1:AA11:AA22:C3:E005::
probe 1
Type escape sequence to abort.
Tracing the route to 1002:1::2 via [
  FCCC:CC1:AA11:AA22:C3:E005:]
  1 2001:1::2 1 msec
  2 2013:1::2 1 msec
  3 2032:2::1 1 msec
  4 2032:1::2 1 msec
  5 2023:1::1 1 msec
  6 1002:1::2 1 msec
PE1#
```


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。