



Cisco Catalyst SD-WAN ルーティング コンフィギュレーション ガイド、Cisco IOS XE Catalyst SD-WAN リリース 17.x

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/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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)

© 2019–2024 Cisco Systems, Inc. All rights reserved.



目次

第 1 章	最初にお読みください	1
第 2 章	Cisco IOS XE (SD-WAN) の新機能	3
第 3 章	ユニキャストオーバーレイ ルーティング	5
	サポートされているプロトコル	5
	OMP ルーティングプロトコル	6
	OMP ルートアドバタイズメント	6
	Cisco Catalyst SD-WAN コントローラの OMP ルートアドバタイズメント	11
	OMP ルートの再配布	12
	アドミニストレーティブ ディスタンス	15
	OMP ベストパスアルゴリズム	16
	OMP グレースフルリスタート	20
	BGP および OSPF ルーティングプロトコル	21
	OSPFv3	23
	EIGRP	23
	ルーティング情報プロトコル (RIP)	24
	Routing Information Protocol のサポートについて	25
	Routing Information Protocol の使用の前提条件	28
	Routing Information Protocol の使用に関する制約事項	28
	ユニキャストオーバーレイ ルーティングの設定	28
	BGP を設定する	29
	CLI を使用した BGP の設定	40
	OSPF の設定	45

CLI を使用した OSPF の設定	53
OMP の設定	54
CLI を使用した OMP の設定	59
OSPFv3 の設定	65
CLI を使用した OSPFv3 の設定	72
EIGRP の設定	73
CLI を使用した EIGRP の設定	77
CLI を使用した EIGRP 設定の確認	78
CLI を使用した Routing Information Protocol (RIPv2) の設定	79
CLI を使用した RIPv2 設定の確認	82
CLI を使用した RIPv2 の設定	83
RIPv2 の設定例	86
CLI を使用した RIPv2 設定の確認	86

第 4 章

マルチキャスト オーバーレイ ルーティング	89
マルチキャスト オーバーレイ ルーティング	89
サポートされているプロトコル	91
PIM	91
IGMP	93
MSDP	93
マルチキャスト オーバーレイ ルーティングのトラフィックフロー	94
マルチキャスト オーバーレイ ルーティングの設定	95
マルチキャストの設定	96
設定グループを使用したマルチキャストの設定	97
CLI を使用したマルチキャストの設定	102
CLI アドオンテンプレートを使用したマルチキャスト用の ACL の設定	102
PIM の設定	103
PIM BSR によるランデブーポイント選択プロセス	107
PIM BSR による RP 選択のサンプルトポロジ	109
PIM BSR の設定	109
PIM BSR 選択の CLI 設定	113

CLI を使用した VRRP 対応 PIM の確認	115
IGMP の設定	115
CLI を使用した PIM および IGMP の設定	118
CLI テンプレートを使用した MSDP の設定	119
Cisco SD-WAN と非 SD-WAN を相互接続するための MSDP のサポート	120
Cisco SD-WAN と非 SD-WAN を相互接続するための MSDP のサポートについて	120
Cisco SD-WAN と非 SD-WAN を相互接続するための MSDP のサポートの利点	122
Cisco SD-WAN と非 SD-WAN を相互接続するための MSDP のサポートの前提条件	123
Cisco SD-WAN と非 SD-WAN を相互接続するための MSDP のサポートに関する制約事項	123
Cisco SD-WAN と非 SD-WAN を相互接続するための MSDP の設定	123
CLI テンプレートを使用した Cisco SD-WAN と非 SD-WAN を相互接続するための MSDP の設定	124
Cisco SD-WAN と非 SD-WAN を相互接続するための MSDP の設定の確認	124
Cisco SD-WAN と非 SD-WAN を相互接続するための MSDP の設定のモニター	125
トラブルシューティング	126
MSDP SA キャッシュが入力されない	126
OMP SA ルートがアドバタイズされない	126

第 5 章

無線対応ルーティング	127
RAR のサポートされるデバイス	128
RAR の前提条件	128
RAR の利点	128
RAR に関する制約事項	129
RAR について	129
RAR の概要	129
RAR のシステムコンポーネント	131
RAR の設定	132
バイパスモードでの RAR 機能の設定	134
集約モードでの RAR 機能の設定	135

第 6 章	VPN 間のルートリーク 137
	サポートされているプロトコル 138
	ルートリークと再配布の制約事項 139
	ルートリークに関する情報 140
	ルートリークのユースケース 142
	ルートプリファレンスの特定方法 143
	Cisco SD-WAN Manager を使用したルートリーク設定のワークフロー 143
	ローカライズされたルートポリシーの設定 143
	グローバル VRF とサービス VPN 間のルートリークの設定および有効化 145
	サービス VPN 間のルートリークの設定 148
	サービス側の VPN 機能テンプレートのデバイステンプレートへの添付 149
	CLI を使用したルートリークの設定と確認 150
	CLI を使用したグローバル VRF とサービス VPN 間のルート再配布の設定 156
	ルートの再配布の確認 158
	CLI テンプレートを使用したサービス VPN 間のルートリークの設定 160
	CLI を使用したサービス VPN 間ルートリーク設定の確認 161
	CLI を使用したリークされたサービス VPN を追跡するための VRRP トラッカーの設定 162
	VRRP トラッキングの確認 164
	ルートリークの設定例 165

第 7 章	Cisco Catalyst SD-WAN のルーティングプロトコルの BFD 169
	ルーティングプロトコルの BFD に関する情報 170
	BFD の概要 170
	Cisco Catalyst SD-WAN での BFD の仕組み 170
	サポートされているプロトコルとインターフェイス 172
	制限事項と制約事項 173
	ルーティングプロトコルの BFD の設定 173
	ルーティングプロトコルの BFD の有効化 174
	サービス側 BGP の BFD の設定 174
	トランスポート側 BGP の BFD の設定 175

サービス側 EIGRP の BFD の設定	176
サービス側 OSPF および OSPFv3 の BFD の設定	177
デバイステンプレートへの機能テンプレートの添付	179
CLI を使用したルーティングプロトコルの BFD の設定	179
BFD 設定のモニタと確認	182
一般的な BFD エラーのトラブルシューティング	183

第 8 章

Cisco Catalyst SD-WAN BFD 185

Cisco Catalyst SD-WAN BFD について	186
BFD セッションの自動一時停止について	187
BFD セッションの自動一時停止の利点	188
BFD セッションの自動一時停止の仕組み	188
BFD セッションの自動一時停止に関する制約事項	190
CLI テンプレートを使用した BFD セッションの自動一時停止の設定	190
BFD セッションの自動一時停止の確認	192

第 9 章

TLOC カラーによる Cisco Catalyst SD-WAN コントローラ のルートフィルタリング 193

TLOC カラーによる Cisco SD-WAN コントローラ のルートフィルタリングについて	194
TLOC カラーによる Cisco SD-WAN コントローラ のルートフィルタリングのサポートされる デバイス	197
TLOC カラーによる Cisco SD-WAN コントローラ のルートフィルタリングの前提条件	197
TLOC カラーによる Cisco SD-WAN コントローラ のルートフィルタリングに関する制約事項	197
CLI テンプレートを使用した TLOC カラーによる Cisco SD-WAN コントローラ のルートフィ ルタリングの設定	197
CLI テンプレートを使用したルートフィルタリングの有効化	198
CLI テンプレートを使用した TLOC カラーによるルートフィルタリングの更新間隔の設定	198
CLI テンプレートを使用した TLOC カラーによる Cisco SD-WAN コントローラ のルート フィルタリングのデフォルト TLOC カラー互換性のオーバーライド	199
TLOC カラーによる Cisco SD-WAN コントローラ のルートフィルタリングのモニター	200
デバイスの TLOC カラーの表示	201

TLOC カラーの互換性の確認 201

第 10 章

トランスポートゲートウェイ (Transport Gateway) 203

- トランスポートゲートウェイ (Transport Gateway) 204
- トランスポートゲートウェイに関する情報 204
 - サイトタイプ 206
 - OMP ベストパスロジックとトランスポートゲートウェイパス優先順位 207
 - コンフィギュレーションの概要 208
- トランスポートゲートウェイの制約事項 211
- トランスポートゲートウェイのユースケース 212
- Cisco SD-WAN Manager を使用したトランスポートゲートウェイとしてのルータの設定 214
- CLI テンプレートを使用したトランスポートゲートウェイとしてのルータの設定 215
- トランスポートゲートウェイパス優先順位の設定 215
 - Cisco SD-WAN Manager を使用したトランスポートゲートウェイパス優先順位の設定 216
 - CLI テンプレートを使用したトランスポートゲートウェイパス優先順位の設定 217
- Cisco SD-WAN Manager を使用したルータのサイトタイプの設定 218
- CLI テンプレートを使用したルータのサイトタイプの設定 218
- CLI を使用したルータのサイトタイプの確認 219
- CLI を使用したトランスポートゲートウェイ設定の確認 219

第 11 章

ハブアンドスポーク 221

- ハブアンドスポーク 222
- ハブアンドスポークについて 222
 - 例：ハブアンドスポーク接続 224
 - Device0 (ハブ) の設定前と設定後 226
 - Device1 (Spoke1) の設定前と設定後 229
 - Device2 (Spoke2) の設定前と設定後 231
- ハブアンドスポークの利点 233
- ハブアンドスポークに関する制約事項 234
- ハブアンドスポークのユースケース 234
- ハブアンドスポークトポロジの設定 235

Cisco SD-WAN Manager を使用したハブアンドスポークを有効にするための Cisco Catalyst SD-WAN コントローラ の設定	235
CLI テンプレートを使用してハブアンドスポークを有効にするための Cisco SD-WAN コントローラ の設定	236
トランスポートゲートウェイとしてのルータの設定 (ハブアンドスポークの場合)	236
ルータのサイトタイプの設定 (ハブアンドスポークの場合)	237
ハブアンドスポーク設定の確認	237
Cisco Catalyst SD-WAN コントローラ でハブアンドスポーク設定が有効になっていることの確認	237

 第 12 章

対称ルーティング	239
対称ルーティング	240
対称ルーティングについて	240
対称ルーティング設定の利点	241
対称ルーティングを保証するメカニズム	241
オーバーレイネットワーク外のデバイスの OMP メトリクスの変換	245
OMP メトリックの BGP 属性への変換	246
OMP メトリックの OSPF メトリックへの変換	249
コンフィギュレーションの概要	250
対称ルーティングの設定例とそのメカニズム	253
サポートされているシナリオ	259
シナリオ: ハブアンドスポークトポロジ、データセンターにサービスを提供する複数のハブ、アクティブ/アクティブ	260
シナリオ: ハブアンドスポークトポロジ、データセンターにサービスを提供する複数のハブ、アクティブ/パッシブ	261
シナリオ: ハブアンドスポークトポロジ、データセンターにサービスを提供する複数のハブ、VRF によるアクティブ/アクティブ	261
シナリオ: マルチリージョンファブリック環境	262
シナリオ: マルチリージョンファブリック、サブリージョンにサービスを提供するトランスポートゲートウェイ	262
シナリオ: ルートリクのあるマルチリージョンファブリック	263
対称ルーティングの前提条件	267

対称ルーティングに関する制約事項	268
対称ルーティングの設定	268
Cisco SD-WAN Manager を使用した自動アフィニティグループ優先順位を使用するルータの設定	268
ルータアフィニティグループまたはアフィニティグループ優先順位の設定	269
Cisco SD-WAN Manager を使用した特定 VRF のルータアフィニティグループの設定	269
CLI テンプレートを使用した特定 VRF のルータアフィニティグループの設定	270
CLI テンプレートを使用した自動アフィニティグループ優先順位を使用するルータの設定	271
CLI テンプレートを使用した OMP メトリックを BGP または OSPF に変換するルータの設定	271
対称ルーティングの確認	273
ルータでの特定プレフィックスのネクストホップの確認	273
接続先ルータへのパスの確認	273
ルータでの VRF 固有アフィニティグループ設定の確認	274
ルートリークの制御ポリシーの確認	274
ルートの導出アフィニティグループの確認	275
RIB メトリック変換のモニター	276
OMP メトリック	276
BGP メトリック	277
OSPF メトリック	277

第 13 章	Cisco Catalyst SD-WAN ルーティングのトラブルシューティング	279
	概要	279
	サポート記事	280
	フィードバックのリクエスト	281
	免責事項と注意事項	281



第 1 章

最初にお読みください



- (注) 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

参考資料

- [Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations](#) [英語]
- [Cisco Catalyst SD-WAN Device Compatibility](#) [英語]

ユーザーマニュアル

- [User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17](#) [英語]

通信、サービス、およびその他の情報

- **Cisco Profile Manager** で、シスコの E メールニュースレターおよびその他の情報にサインアップしてください。
- ネットワーク運用の信頼性を高めるための最新のテクニカルサービス、アドバンスドサービス、リモートサービスについては、[シスコサービス](#) にアクセスしてください。
- 安全かつ検証されたエンタープライズクラスのアプリ、製品、ソリューション、サービスをお求めの場合は、[CiscoDevnet](#) にアクセスしてください。

- Cisco Press 出版社による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。
- リリースで未解決および解決済みのバグをご覧になる場合は、[Cisco Bug Search Tool](#) 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、[シスコ サポート](#) にアクセスしてください。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。



第 2 章

Cisco IOS XE (SD-WAN) の新機能

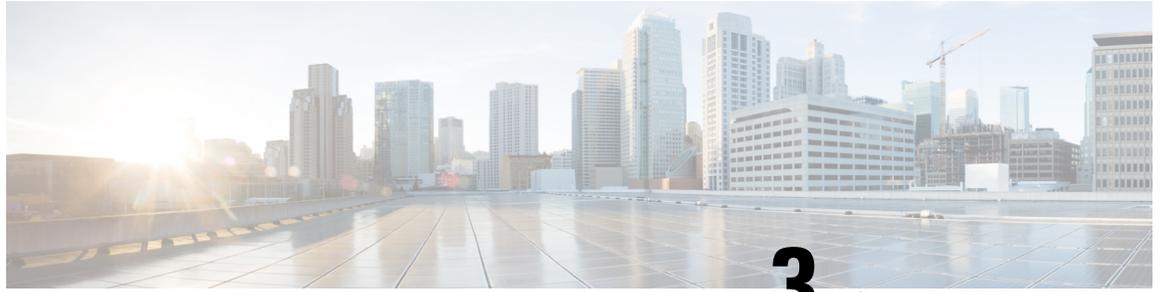


- (注) 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。



- (注) シスコでは、リリースごとに Cisco Catalyst SD-WAN ソリューションを継続的に強化しています。また、コンテンツも最新の強化に合致したものとなるように努めています。次の表に、コンフィギュレーションガイド、コマンドリファレンスガイド、およびハードウェア設置ガイドに記載されている新機能と変更された機能を示します。Cisco Catalyst SD-WAN ソリューションに関する追加機能と修正については、リリースノートの「解決されたバグおよび未解決のバグ」セクションを参照してください。

[What's New in Cisco IOS XE Catalyst SD-WAN Release 17.x \[英語\]](#)



第 3 章

ユニキャスト オーバーレイ ルーティング



- (注) 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

オーバーレイネットワークは、Cisco Catalyst SD-WAN オーバーレイルーティングの中心である Cisco Catalyst SD-WAN オーバーレイ管理プロトコル (OMP) によって制御されます。このソリューションでは、スケーラブルで、動的かつオンデマンドでセキュアな VPN を構築できます。Cisco Catalyst SD-WAN ソリューションでは、オーケストレーションが容易な一元化されたコントローラを使用して、きめ細かいアクセス制御と、すべてのエッジノード間のスケーラブルでセキュアなデータプレーンを含む完全なポリシー制御を行います。

Cisco Catalyst SD-WAN ソリューションにより、エッジノードは、パブリック WAN、インターネット、メトロイーサネット、MPLS など、あらゆるタイプのトランスポートネットワークを介して直接通信できます。

- [サポートされているプロトコル \(5 ページ\)](#)
- [ユニキャスト オーバーレイ ルーティングの設定 \(28 ページ\)](#)

サポートされているプロトコル

ここでは、ユニキャストルーティングでサポートされるプロトコルについて説明します。

OMP ルーティングプロトコル

Cisco Catalyst SD-WAN オーバーレイ管理プロトコル (OMP) は、Cisco Catalyst SD-WAN コントロールプレーンの確立と維持を行うプロトコルです。次のサービスを提供します。

- ネットワークサイト間の接続、サービスチェーン、VPNまたはVRF トポロジを含む、オーバーレイネットワーク通信のオーケストレーション
- サービスレベルルーティング情報および関連するロケーションマッピングの配布
- データプレーン セキュリティ パラメータの配布
- ルーティングポリシーの一元管理と配布

OMP は、オーバーレイネットワーク内の Cisco Catalyst SD-WAN コントローラと Cisco IOS XE Catalyst SD-WAN デバイスとの間でルーティング、ポリシー、および管理情報を交換するために使用される制御プロトコルです。これらのデバイスは自動的にデバイス間の OMP ピアリングセッションを開始し、OMP セッションの 2 つの IP エンドポイントは 2 つのデバイスのシステム IP アドレスです。

OMP は、サービスをトランスポートから分離することでオーバーレイネットワークを実現する、包括的な情報管理および配信プロトコルです。一般的な VPN 設定で提供されるサービスは、通常、VRF ドメイン内にあり、VRF の外部から見えないように保護されています。このような従来のアーキテクチャでは、VRF ドメインとサービス接続を拡張することが課題です。

OMP は、論理トランスポート エンドポイントの場所に基づいてサービストラフィックを効率的に管理する方法を提供することで、これらの拡張性の課題に対処します。この方法は、データプレーンとコントロールプレーンの分離の概念をルータ内からネットワーク全体に拡張します。OMP は、関連するポリシーとともにコントロールプレーン情報を配布します。中央の Cisco Catalyst SD-WAN コントローラは、オーバーレイ ルーティング ドメインのルーティングおよびアクセスポリシーに関するすべての決定を行います。OMP は、データプレーンの接続と転送のためにエッジデバイスによって使用されるルーティング、セキュリティ、サービス、およびポリシーを伝達するために使用されます。

OMP ルートアドバタイズメント

Cisco Catalyst SD-WAN コントローラおよび Cisco IOS XE Catalyst SD-WAN デバイスでは、OMP はローカルサイトから学習したルートとサービスを、対応するトランスポート ロケーションマッピング (TLOC と呼ばれる) とともにピアにアドバタイズします。これらのルートは、標準の IP ルートと区別するために OMP ルートまたは vRoute と呼ばれます。アドバタイズされるルートは、実際にはルートとそのルートに関連付けられた TLOC で構成されるタプルです。Cisco Catalyst SD-WAN コントローラは、オーバーレイネットワークのトポロジとネットワークで使用可能なサービスを OMP ルートを介して学習します。

OMP は、オーバーレイネットワークのローカルサイトで従来のルーティングと情報を交換します。OMP は OSPF や BGP などの従来のルーティングプロトコルから情報をインポートします。このルーティング情報によってローカルサイト内の到達可能性が提供されます。従来のルーティングプロトコルからのルーティング情報のインポートは、ユーザー定義のポリシーに依存します。

OMPはオーバーレイネットワーク環境で動作するため、ルーティングピアの概念は従来のネットワーク環境とは異なります。論理的な観点から見ると、オーバーレイ環境は中央集中型コントローラと複数のエッジデバイスで構成されます。各エッジデバイスは、インポートされたルートを中央集中型コントローラにアドバタイズします。このコントローラは、ポリシーの決定に基づいて、オーバーレイルーティング情報をネットワーク内の他のエッジデバイスに配布します。エッジデバイスがOMPやその他の方法を使用して、ルーティング情報を相互にアドバタイズすることはありません。中央集中型コントローラとエッジデバイス間のOMPピアリングセッションは、コントロールプレーントラフィックの交換にのみ使用されます。どのような状況においても、データトラフィックに使用されることはありません。

登録されたエッジデバイスは、直接接続されたネットワークからのルート、およびIGPプロトコルから学習したスタティックルートを自動的に収集します。エッジデバイスは、BGPから学習したルートを収集するようにも設定できます。

ルートマップASパスおよびコミュニティ設定（ASパスプリペンドなど）は、ルートマップがプロトコル再配布用に設定されている場合はサポートされません。再配布されたOMPルートのASパスは、BGPネイバーアウトバウンドポリシーのルートマップを使用して設定および適用できます。

OMPは、各ローカルデバイスでパス選択、ループ回避、およびポリシー実装を実行し、任意のエッジデバイスのローカルルーティングテーブルにインストールされるルートを決定します。



- (注) OMPへのルートアドバタイズメントは、グローバルレベルまたは特定のVPNレベルで設定を適用することによって行われます。OMPへのルートアドバタイズメントをグローバルレベルで設定するには、OMP機能テンプレートを使用します。一方、OMPへのルートアドバタイズメントを特定のVPNレベルで設定するには、VPN機能テンプレートを使用します。OMPへのルートアドバタイズメントの設定の詳細については、[OMPの設定 \(54ページ\)](#)を参照してください。



- (注) Cisco Catalyst SD-WANでは、OMPプロトコルを介したサービス側ルートの再帰ルックアップはサポートされていません。Cisco IOS XE SD-WAN リリース 17.12.1a以降では、Cisco IOS XE Catalyst SD-WANでのOMPプロトコルを介したサービス側ルートの再帰ルックアップがサポートされています。

OMPは、次のタイプのルートをアドバタイズします。

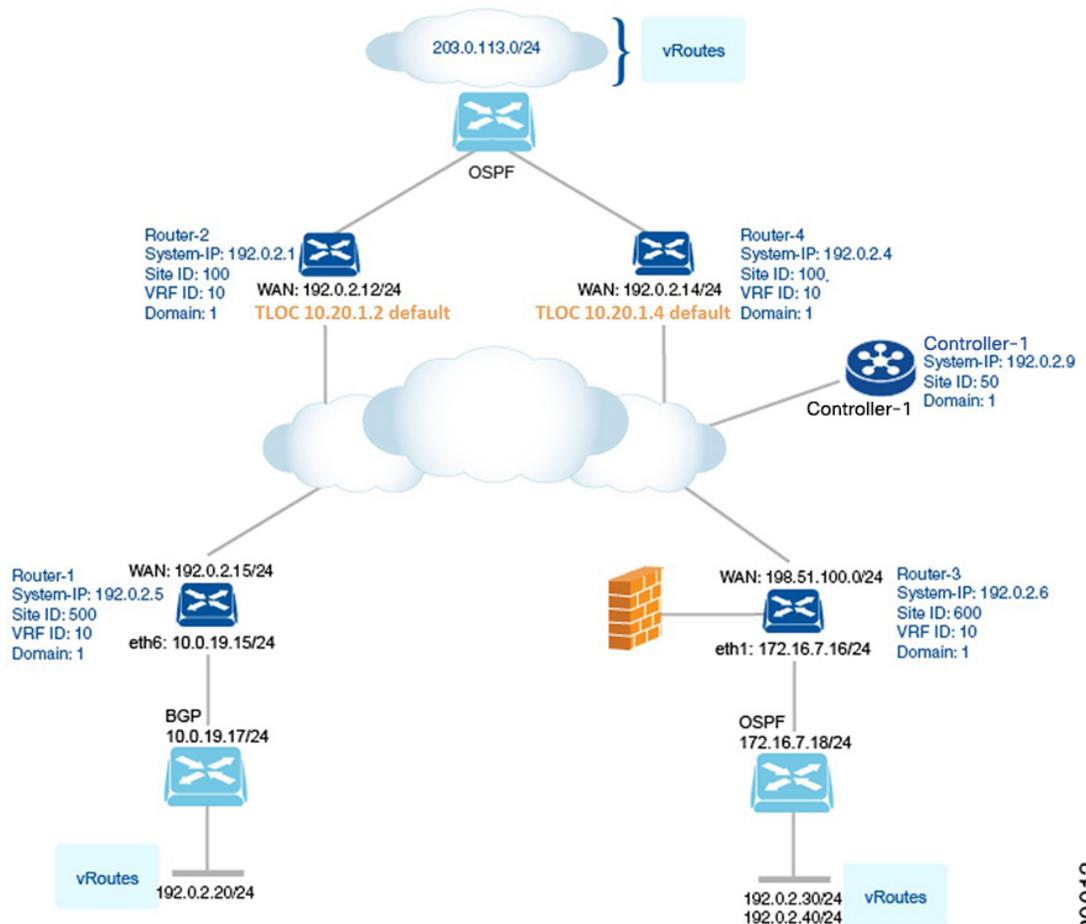
- OMPルート（vRouteとも呼ばれる）：OMP編成のトランスポートネットワークを使用するエンドポイント間の到達可能性を確立するプレフィックス。OMPルートは、中央データセンターのサービス、ブランチオフィスのサービス、またはオーバーレイネットワークの任意の場所にあるホストやその他のエンドポイントの集合を表すことができます。OMPルートは、機能転送のためにTLOCを必要とし、TLOCに解決されます。BGPと比較すると、OMPルートは、BGP AFI/SAFI NLRI フィールド（Address Family Indicator（AFI））、

Subsequent Address Family Identifier (SAFI)、Network Layer Reachability Information (NLRI)) のいずれかのフィールドで伝送されるプレフィックスと同等です)。

- トランスポートロケーション (TLOC) : OMP ルートを物理ロケーションに関連付ける識別子。TLOC は、基盤となるネットワークから認識できる OMP ルーティングドメインの唯一のエンティティであり、基盤となるネットワークのルーティングを介して到達する必要があります。TLOC は、物理ネットワークのルーティングテーブル内のエントリを介して直接到達できるか、または NAT デバイスの外部に存在するプレフィックスによって表され、ルーティングテーブルに含まれている必要があります。BGP と比較すると、TLOC は OMP ルートのネクストホップとして機能します。

次の図は、2 種類の OMP ルートを示しています。

図 1: さまざまな種類の OMP ルート



520013

OMP ルート

ブランチまたはローカルサイトの各デバイスは、ドメイン内の Cisco Catalyst SD-WAN コントローラに OMP ルートをアドバタイズします。これらのルートには、デバイスがそのサイトのローカルネットワークから学習したルーティング情報が含まれています。

Cisco Catalyst SD-WAN デバイスは、次のタイプのサイトローカルルートのいずれかをアドバタイズできます。

- 接続済み（別名、直接接続）
- スタティック
- BGP
- EIGRP
- LISP
- OSPF（エリア間、エリア内、および外部）
- OSPFv3（エリア間、エリア内、および外部）
- IS-IS

OMP ルートは次の属性をアドバタイズします。

- **TLOC** : vRoute のネクストホップのトランスポートロケーション ID。これは、BGP NEXT_HOP 属性に似ています。TLOC は次の 3 つの要素で構成されます。
 - OMP ルートを発信する OMP スピーカーのシステム IP アドレス
 - リンクタイプを識別する色
 - トランスポートトンネルのカプセル化タイプ
- **[Origin]** : ルートの送信元（BGP、OSPF、接続、スタティックなど）、および元のルートに関連付けられたメトリック。
- **[Originator]** : ルートの起点の OMP 識別子（ルートの学習元の IP アドレス）。
- **[Preference]** : OMP ルートの優先度。プリファレンス値が高いほど優先されます。
- **[Site ID]** : OMP ルートが属する Cisco Catalyst SD-WAN オーバーレイ ネットワーク ドメイン内のサイトの識別子。
- **[Tag]** : OMP スピーカーが受け入れ、優先、または再配布するルーティング情報を制御するために使用できるオプションの移行パス属性。
- **[VRF]** : OMP ルートが属する VRF またはネットワークセグメント。

システム IP、色、カプセル化タイプ、キャリア、プリファレンス、サービス、サイト ID、VPN VRF など、一部の OMP ルート属性値を設定します。Cisco Catalyst SD-WAN コントローラで制御ポリシーをプロビジョニングすることで、一部の OMP ルート属性を変更できます。

TLOC ルート

TLOC ルートはトランスポートロケーションを識別します。これらは、WAN インターフェイスがキャリアに接続するポイントなど、物理トランスポートに接続するオーバーレイネットワーク内の場所です。TLOC は、OMP スピーカーのシステム IP アドレス、色、およびカプセル化タイプで構成される 3 タプルで表されます。OMP は各 TLOC を個別にアドバタイズします。

TLOC ルートは次の属性をアドバタイズします。

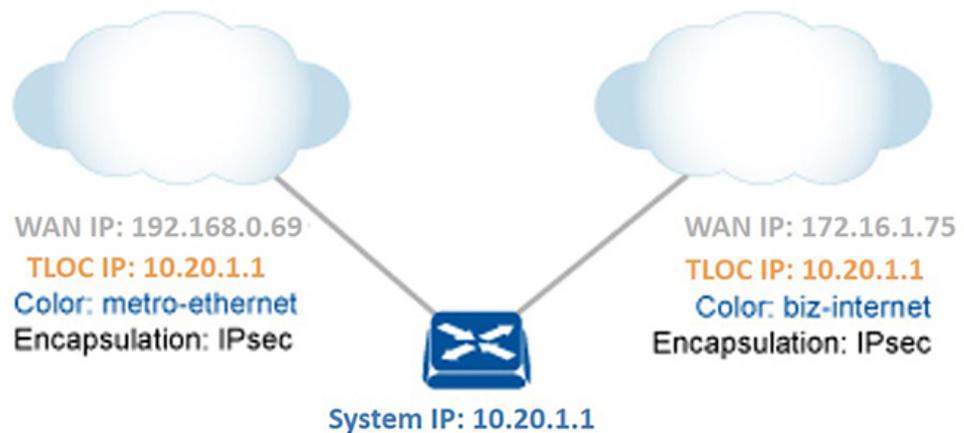
- [TLOC private address] : TLOC に関連付けられたインターフェイスのプライベート IP アドレス。
- [TLOC public address] : TLOC の NAT 変換されたアドレス。
- [Carrier] : キャリアタイプの識別子。一般に、トランスポートがパブリックかプライベートかを示すために使用されます。
- [Color] : リンクタイプを示します。
- [Encapsulation type] : トンネルカプセル化タイプ。
- [Preference] : 同じ OMP ルートをアドバタイズする TLOC を区別するために使用される優先度。
- [Site ID] : TLOC が属する Cisco Catalyst SD-WAN オーバーレイ ネットワーク ドメイン内のサイトの識別子。
- [Tag] : OMP スピーカーが TLOC へのルーティング情報のフローを制御するために使用できるオプションの移行パス属性。OMP ルートがその TLOC とともにアドバタイズされると、両方またはいずれかがコミュニティ TAG で配布され、TLOC のグループとの間におけるトラフィックの送受信方法を決定するために使用されます。
- [Weight] : OMP ルートが 2 つ以上の TLOC を介して到達可能な場合に、複数のエントリポイントを区別するために使用される値。

TLOC で使用される IP アドレスは、デバイス自体の固定システムアドレスです。TLOC を示すために IP アドレスまたはインターフェイス IP アドレスを使用しない理由は、IP アドレスは移動や変更が可能なためです。たとえば、DHCP によって割り当てられることも、インターフェイスカードを交換することもできます。システム IP アドレスを使用して TLOC を識別することにより、IP アドレッシングに関係なく常にトランスポート エンドポイントを識別できます。

リンクの色は、デバイス上の WAN インターフェイスのタイプを表します。Cisco Catalyst SD-WAN ソリューションでは、デバイスの設定で割り当てられた定義済みの色が提供されます。色は次のデフォルト色のいずれかになります。3g、biz-internet、blue、bronze、custom1、custom2、custom3、gold、green、lte、metro-ethernet、mpls、private1、private2、public-internet、red、または silver。

カプセル化はトンネルインターフェイスで使用され、IPSec か GRE のいずれかです。

図 2: ルータ属性



368487

右側の図は、2つの WAN 接続と 2つの TLOC を持つデバイスを示しています。ルータのシステム IP アドレスは 10.20.1.1 です。左側の TLOC は、システム IP アドレス : 10.20.1.1、色 : metro-ethernet、およびカプセル化 : IPSec によって一意に識別され、IP アドレスが 192.168.0.69 の物理 WAN インターフェイスにマッピングされます。右側の TLOC は、システム IP アドレス : 10.20.1.1、色 : biz-internet、およびカプセル化 : IPSec によって一意に識別され、WAN IP アドレス 172.16.1.75 にマッピングされます。

システム IP アドレス、色、カプセル化など、一部の TLOC 属性を設定します。属性の一部は、Cisco Catalyst SD-WAN コントローラで制御ポリシーをプロビジョニングすることで変更できます。「Centralized Control Policy」を参照してください。

Cisco Catalyst SD-WAN コントローラの OMP ルートアドバタイズメント

表 1: 機能の履歴

機能名	リリース情報	説明
Cisco Catalyst SD-WAN コントローラの OMP パス制限の増加	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a	この機能により、Cisco Catalyst SD-WAN コントローラの間で交換できる OMP ルート数の制限が 128 に拡張されます。このリリース以前は、制限は 16 でした。

概要

トランスポートロケーション (TLOC) 情報は、Cisco Catalyst SD-WAN コントローラおよびそのローカルサイトブランチを含む OMP ピアにアドバタイズされます。Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降、プレフィックスごとの VPN ごとに Cisco Catalyst SD-WAN コントローラの間で交換できる OMP パス数の制限は、最大 128 に拡張されます。

制限事項

- マルチテナント Cisco Catalyst SD-WAN コントローラは、グローバル OMP 設定のみをサポートします。
- 共有されるパスの数は、メモリや内部データ構造の構成などの要因によって異なります。

パス制限の設定

次に、Cisco Catalyst SD-WAN コントローラが別の Cisco Catalyst SD-WAN コントローラに送信できるパスの数を設定する例を示します。

```
Device(config)# omp
Device(config-omp)# controller-send-path-limit 100
```

Cisco Catalyst SD-WAN コントローラの間で交換される最大 128 の送信パス制限を設定するには、**controller-send-path-limit** コマンドを使用します。送信パス制限をデフォルトに戻すには、このコマンドの **no** 形式を使用します。デフォルト設定では、コントローラは最大 128 までの使用可能なすべてのパスの情報を送信できます。



(注) デフォルト設定を使用することを推奨します。デフォルト設定では、使用可能なすべてのパスに関する情報が送信されますが、パス数は 128 に制限されます。これにより、コントローラ間でネットワークの可視性を得られます。

パス制限は頻繁に変更しないことを推奨します。ピアにおけるすべての変更について、Cisco Catalyst SD-WAN コントローラは完全なルートデータベースの更新を実行するため、ネットワークが完全に更新されます。

パス制限の設定の詳細については、[controller-send-path-limit](#) コマンドページを参照してください。

OMP ルートの再配布

OMP は、ローカルに学習、またはルーティングピアから学習した次のタイプのルートを自動的に再配布します。

- 接続されている状態
- スタティック
- OSPF エリア内ルート
- OSPF エリア間ルート
- OSPFv3 エリア内ルート (アドレスファミリー IPv6)
- OSPFv3 エリア間ルート (アドレスファミリー IPv6)

ルーティンググループと最適でないルーティングを回避するには、次のタイプのルートの再配布には明示的な設定が必要です。

- BGP
- EIGRP
- LISP
- IS-IS
- OSPF 外部ルート
- OSPFv3 外部ルート (アドレスファミリ IPv6)
- OSPFv3 全ルート (アドレスファミリ IPv4)

advertise network<ipv4-prefix> コマンドを使用すると、特定のプレフィックスに対応する非 OMP ルートが VRF IPv4 ルーティングテーブルに存在する場合に、そのプレフィックスをアドバタイズできます。このコマンドは **address-family ipv4** でのみサポートされることに注意してください。

次に、ネットワーク設定をアドバタイズする例を示します。

```
omp
no shutdown
graceful-restart
address-family ipv4 vrf 1
  advertise connected
  advertise static
  advertise network X.X.X.X/X
!
```

エッジからネットワークのアクセス部分への過剰なルーティング情報の伝達を回避するために、OMP を介してデバイスが受信するルートは、ルータで実行されている他のルーティングプロトコルに自動的に再配布されません。OMP を介して受信したルートを再配布する場合は、各デバイスでローカルに再配布を有効にする必要があります。

OMP は、各 OMP ルートの起点とサブ起点タイプを設定して、ルートの起点を示します (次の表を参照)。ルートを選択する場合、Cisco Catalyst SD-WAN コントローラ とルータは起点タイプとサブタイプを考慮します。

VRF1 の OMP への OSPF ルートの再配布を設定するには、**advertise ospf route-map <route-map-name> external** を設定する必要があります。OSPF 内部ルートは、明示的な設定がない場合、デフォルトで OMP に再配布されます。

次に、すべての VRF での OSPF 外部ルート再配布の例を示します。

```
omp
no shutdown
ecmp-limit 6
graceful-restart
no as-dot-notation
timers
  holdtime 15
  graceful-restart-timer 120
exit
address-family ipv4
  advertise ospf external <-- This configuration implies OSPF Inter-Area/Intra-Area
  routes & External routes are redistributed into OMP
  advertise connected
```

```
advertise static
!
```

次に、特定の VRF での OSPF 外部ルート再配布の例を示します。

```
omp
no shutdown
ecmp-limit      6
graceful-restart
no as-dot-notation
timers
  holdtime      15
  graceful-restart-timer 120
exit
address-family ipv4 vrf 1
advertise ospf external
advertise ospf route-map RLB
!
```

external キーワードを使用すると、指定したルートマップが外部と内部の両方の OSPF ルート（エリア内/エリア間）に適用されます。

次に、OSPFv3 外部ルート再配布の例を示します。

```
omp
no shutdown
ecmp-limit      6
graceful-restart
no as-dot-notation
timers
  holdtime      15
  graceful-restart-timer 120
exit
address-family ipv6
advertise ospfv3
advertise ospf external
!
```



(注) Cisco IOS XE Catalyst SD-WAN リリース 17.7.2 以降では、過度の CPU の使用を回避するために、Cisco SD-WAN Manager で受信およびアドバタイズされる OMP ルートのリアルタイム表示が 4001 ルートのみに制限されます。

表 2:

OMP ルートの起点タイプ	OMP ルートの起点サブタイプ
BGP	External Internal
接続されている状態	—
OSPF	Intra-area、Inter-area、External-1、External-2、NSSA-External-1、および NSSA-External-2
OSPFv3	Intra-area、Inter-area、External-1、External-2、NSSA-External-1、および NSSA-External-2

OMP ルートの起点タイプ	OMP ルートの起点サブタイプ
スタティック	—
EIGRP	<ul style="list-style-type: none"> • EIGRP サマリー • EIGRP 内部 • EIGRP 外部
LISP	—
IS-IS	レベル 1 とレベル 2

OMP は、元のルートのメトリックも伝送します。メトリック 0 は、接続ルートを示します。

アドミニストレーティブ ディスタンス

アドミニストレーティブ ディスタンスは、複数のルーティングプロトコルから同じ宛先に向かう 2 つ以上の異なるルートが存在する場合に、ベストパスを選択するために使用されるメトリックです。Cisco Catalyst SD-WAN コントローラまたはルータが宛先への OMP ルートを選択する際には、アドミニストレーティブ ディスタンスの値が最も小さいルートが優先されます。

次の表に、Cisco Catalyst SD-WAN デバイスで使用されるデフォルトのアドミニストレーティブ ディスタンスを示します。

表 3:

Protocol	アドミニストレーティブ ディスタンス
接続されている状態	0
スタティック	1
NAT (NAT とスタティックルートは同じ VPN に共存できず、NAT によりスタティックルートが上書きされます)。	1
DHCP から学習	1
EIGRP サマリー	5
EBGP	20
EIGRP	内部 : 90、外部 : 170
OSPF	110
OSPFv3	110
IS-IS	115

Protocol	アドミニストレーティブ ディスタ ンス
IBGP	200
OMP	251

OMP ベストパスアルゴリズム

Cisco Catalyst SD-WAN デバイスは、OMP を使用してローカルパスを Cisco Catalyst SD-WAN コントローラにアドバタイズします。ネットワークトポロジによっては、複数のデバイスから一部のパスがアドバタイズされる場合があります。Cisco Catalyst SD-WAN デバイスは、次のアルゴリズムを使用してベストパスを選択します。

表 4: ベストパスアルゴリズム

ステップ	適用対象	説明
1	エッジデバイス Cisco Catalyst SD-WAN コントローラ	パスの有効性 OMP パスが有効かどうかを確認します。有効でない場合は無視します。
2	エッジデバイス Cisco Catalyst SD-WAN コントローラ	アクティブパスと古いパス 古いパスよりもアクティブパスを優先します。 アクティブパスは、OMP セッションが稼働状態であるピアからのパスです。古いパスは、OMPセッションがグレースフルリスタートモードであるピアからのパスです。 (注) 古いパスは、古いバージョンがルート情報ベース (RIB) バージョンと類似している場合にのみアドバタイズされます。それ以外の場合、古いパスはドロップされます。
3	エッジデバイス	Administrative distance アドミニストレーティブディスタンスがより小さいOMPパスを選択します。 例: デバイスがBGPを介してローカルに学習するパスは、OMPを介してCisco SD-WAN コントローラから学習するパスよりも優先されます。アドミニストレーティブディスタンスについては、 アドミニストレーティブディスタンス (15 ページ) を参照してください。

ステップ	適用対象	説明
4	エッジデバイス Cisco Catalyst SD-WAN コントローラ	OMP パス優先順位 OMP パス優先順位値がより高いOMP パスを選択します。
5	Cisco Catalyst SD-WAN コントローラ	アクセスリージョン Cisco SD-WAN コントローラは、境界ルータ (BR) から同じリージョン内のBR へのアドバタイズメントをドロップします。
6	エッジデバイス	コアリージョン Cisco SD-WAN コントローラは同じアクセスリージョン内の BR 間のアドバタイズメントを許可しますが、BR を受信するとアドバタイズメントがドロップされます。
7	マルチリージョン ファブリック シナリオのみ エッジデバイス	リージョンパスの長さ リージョンパスの長さを比較します。短い方を優先します。 region-path-length-ignore が設定されている場合は、この手順をスキップします (これは、マルチリージョン ファブリックのセカンダリリージョンに対応します)。
8	マルチリージョン ファブリック シナリオのみ 境界ルータ	アクセスリージョンとコアリージョン コアリージョンパスよりもアクセスリージョンパスを優先します。
9	エッジデバイス	ダイレクトパスとトランスポートゲートウェイパス トランスポートゲートウェイパスよりもダイレクトパスを優先します。 この手順は、トランスポートゲートウェイパス優先順位オプションによって変更される可能性があります。これにより、(a)トランスポートゲートウェイパスが優先されるか、(b)パスが同等と見なされるようになります。『Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN) Configuration Guide』の「 Configure the Transport Gateway Path Preference 」を参照してください。

ステップ	適用対象	説明
10	マルチリージョンファブリックシナリオのみ エッジデバイス	マルチリージョンファブリックのサブリージョンの比較 <ul style="list-style-type: none"> ルータ自身のサブリージョンからのパスを優先します。 ルータのサブリージョンからではない2つのパスを比較する場合は、サブリージョンの一部ではないパスを優先します。
11	マルチリージョンファブリックシナリオのみ エッジデバイス	境界ルータ優先順位 境界ルータ優先順位値がより高いパスを優先します。
12	エッジデバイス	導出アフィニティ 導出アフィニティ値がより低いパスを優先します。
13	アフィニティ優先順位が設定されたエッジデバイス	アフィニティ優先順位 デバイスに設定されているアフィニティ優先順位に基づき、アフィニティが優先順位リストでより上にある（優先順位がより高い）パスを優先します。デバイスが affinity-preference-auto を使用している場合は、アフィニティグループの数値がより小さいパスを優先します。 (注) 再発信タイプが類似している2つのパス（アフィニティ値を持つパスと持たないパス）を比較する場合は、アフィニティ値を持つパスを優先します。
14	エッジデバイス	TLOC 設定 TLOC 優先順位値がより高い OMP パスを選択します。

ステップ	適用対象	説明
15	エッジデバイス Cisco Catalyst SD-WAN コントローラ	<p>発信元タイプとサブタイプ</p> <p>発信元タイプとサブタイプを比較し、次のリストで最初に一致するものを選択します。</p> <ul style="list-style-type: none"> • 接続されている状態 • スタティック • EIGRP サマリー • BGP 外部 • EIGRP 内部 • OSPF/OSPFv3 エリア内 • OSPF/OSPFv3 エリア間 • IS-IS レベル 1 • EIGRP 外部 • OSPF/OSPFv3 外部（外部 OSPF タイプ 1 は外部 OSPF タイプ 2 よりも優先されます） • IS-IS レベル 2 • BGP 内部 • 不明
16	エッジデバイス Cisco Catalyst SD-WAN コントローラ	<p>発信元メトリック</p> <p>発信元メトリックがより低い OMP パスを選択します。</p>
17	Cisco Catalyst SD-WAN コントローラ	<p>パス送信元</p> <p>エッジルータから送信されるパスを、Cisco Catalyst SD-WAN コントローラからの同じパスよりも優先します。</p>
18	エッジデバイス Cisco Catalyst SD-WAN コントローラ	<p>プライベート IP アドレス</p> <p>ルータ ID が等しい場合、Cisco IOS XE Catalyst SD-WAN デバイスは、プライベート IP アドレスがより小さい OMP パスを選択します。Cisco Catalyst SD-WAN コントローラが2つの異なるサイトから同じプレフィックスを受信し、すべての属性が等しい場合、両方が選択されます。</p>



- (注) ベストパスとして選択され、ポリシーによって受け入れられた特定のプレフィックスに対するすべての等コストマルチパスから、`send-path-limit` で指定されたパス数より少ないパスをアドバタイズします。

次に、ベストパスを選択する例を示します。

- Cisco Catalyst SD-WAN コントローラは、OSPF の発信元コードを持つ Cisco IOS XE Catalyst SD-WAN デバイスから OMP を介して 10.10.10.0/24 への OMP パスを受信し、また OSPF の発信元コードを持つ別の Cisco Catalyst SD-WAN コントローラから同じパスを受信します。他の条件がすべて等しい場合、ベストパスアルゴリズムでは Cisco IOS XE Catalyst SD-WAN デバイスからのパスが選択されます。
- Cisco Catalyst SD-WAN コントローラは、同じサイトにある 2 つの Cisco IOS XE Catalyst SD-WAN デバイスから同じ OMP パス 10.10.10.0/24 を学習します。他のパラメータがすべて同じ場合、両方のパスが選択され、他の OMP ピアにアドバタイズされます。デフォルトでは、最大 4 つの等コストパスが選択され、アドバタイズされます。

Cisco IOS XE Catalyst SD-WAN デバイスは、向かう先の TLOC がアクティブな場合にのみ、その転送テーブル (FIB) に OMP パスをインストールします。TLOC をアクティブにするには、アクティブな BFD セッションをその TLOC に関連付ける必要があります。BFD セッションは、各リモート TLOC との個別の BFD セッションを作成する各デバイスによって確立されます。BFD セッションが非アクティブになると、Cisco Catalyst SD-WAN コントローラはその TLOC を指すすべての OMP パスを転送テーブルから削除します。

OMP グレースフルリスタート

OMP のグレースフルリスタートにより、コントロールプレーンの機能が停止した場合や使用できなくなった場合でも、Cisco Catalyst SD-WAN オーバーレイネットワークのデータプレーンが引き続き機能できます。グレースフルリスタートでは、ネットワーク内の Cisco SD-WAN コントローラがダウンした場合、または複数の Cisco SD-WAN コントローラが同時にダウンした場合に、Cisco IOS XE Catalyst SD-WAN デバイスでデータトラフィックの転送を続行できます。転送は、Cisco SD-WAN コントローラから受信した最後の既知の良好な情報を使用して行われます。Cisco SD-WAN コントローラが再び使用可能になると、デバイスへの DTLS 接続が再確立されます。そのデバイスは更新された最新のネットワーク情報を Cisco SD-WAN コントローラから受信します。

OMP グレースフルリスタートが有効になっている場合、Cisco IOS XE Catalyst SD-WAN デバイスと Cisco SD-WAN コントローラ (2 つの OMP ピア) は、それぞれのピアから学習した OMP 情報をキャッシュします。この情報には、OMP ルート、TLOC ルート、サービスルート、IPSec SA パラメータ、および一元化されたデータポリシーが含まれます。OMP ピアの 1 つが使用できなくなった場合、他のピアはキャッシュされた情報を使用してネットワークでの動作を継続します。したがって、たとえば、デバイスが Cisco SD-WAN コントローラへの OMP 接続の存在を検出しなくなった場合、そのデバイスはキャッシュされた OMP 情報を使用してデータトラフィックの転送を続行します。そのデバイスは、Cisco SD-WAN コントローラが再び使用可能になったかどうかも定期的に確認します。コントローラが使用可能になり、デバイスがその

コントローラへの接続を再確立すると、そのデバイスはローカルキャッシュをフラッシュし、Cisco SD-WAN コントローラからの新しい OMP 情報のみが有効で信頼できる情報と見なします。同じシナリオは、Cisco SD-WAN コントローラが Cisco IOS XE Catalyst SD-WAN デバイスの存在を検出しなくなった場合にも発生します。



- (注) OMP グレースフルリスタート設定が変更されると、Cisco SD-WAN コントローラ とデバイス間の OMP セッションがフラップされます。これにより、TLOC、IPv4 または IPv6 ユニキャスト、IPv4 マルチキャスト、およびその他のファミリーなど、異なるアドレスファミリーに属するすべての OMP ルートがローカルで撤回され、Cisco SD-WAN コントローラとの OMP セッションが再開された数秒後に再学習されます。TLOC ルートが一時的に削除され、再び追加されると、Bidirectional Forwarding Detection (BFD) セッションも瞬間的にフラップします。これは予期されている動作です。

BGP および OSPF ルーティングプロトコル

Cisco Catalyst SD-WAN オーバーレイネットワークは、BGP および OSPF ユニキャストルーティングプロトコルをサポートします。これらのプロトコルは、トランスポートおよび管理 VRF を除くすべての VRF の Cisco IOS XE Catalyst SD-WAN デバイス で設定して、ローカルサイトのネットワークへの到達可能性を提供できます。Cisco IOS XE Catalyst SD-WAN デバイスは、OMP がオーバーレイネットワーク内のパスをより適切に選択できるように、BGP および OSPF から学習したルート情報を OMP に再配布できます。

ローカルサイトがレイヤ 3 VPN MPLS WAN クラウドに接続すると、デバイスは MPLS CE デバイスとして機能し、L3VPN MPLS クラウド内の PE ルータに接続するための BGP ピアリングセッションを確立します。

ローカルサイトのデバイスが WAN クラウドに直接接続していないが、WAN からは 1 つ以上のホップの位置にあり、非 Cisco SD-WAN デバイスを介して間接的に接続する場合、WAN クラウドに到達できるように、デバイスの DTLS 接続で標準ルーティングを有効にする必要があります。OSPF または BGP をルーティングプロトコルにできます。

どちらのタイプのトポロジでも、BGP または OSPF セッションは、VRF 0 のループバック インターフェイスで作成された DTLS 接続を介して実行されます。VRF 0 は、オーバーレイネットワークで制御トラフィックを伝送するトランスポート VRF です。Cisco Catalyst SD-WAN Validator は、ループバック インターフェイスを介してこの DTLS 接続について学習し、TLOC 関連情報を追跡できるようにこの情報を Cisco Catalyst SD-WAN コントローラに伝えます。VRF 0 では、Cisco IOS XE Catalyst SD-WAN デバイスをネイバー (MPLS の場合は PE ルータ、あるいはローカルサイトの場合はハブまたはネクストホップルータ) に接続する物理インターフェイスも設定しますが、その物理インターフェイスでは DTLS トンネル接続を確立しません。

BGP コミュニティの伝達

表 5: 機能の履歴

機能名	リリース情報	説明
BGP から OMP への再配布中にコミュニティを照合および設定する機能	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco vManage リリース 20.4.1	この機能は、Cisco IOS XE Catalyst SD-WAN デバイスで BGP から OMP へ、またはその逆にルートを再配布するための <code>match</code> および <code>set</code> 句の実装を強化します。BGP から OMP ルーティングにルートを再配布して、ルートトラフィックによりネットワーク内のアクセシビリティを向上させることができます。 <code>route-maps</code> は、各デバイスでローカルに定義され、送信元ルーティングプロトコルからのルートをフィルタリングします。OMP コミュニティを操作して、BGP ルートを伝達できます。次のコマンドが更新されました。 <pre>route-map advertise bgp route-map bgp-to-omp redistribute omp route-map omp-to-bgp</pre>
BGP コミュニティの伝達	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a Cisco vManage リリース 20.3.1	この機能により、ルートの再配布中にルーティングプロトコル間で BGP コミュニティを伝達できます。一方のノードでは OMP が BGP からのルートを再配布し、もう一方のノードでは BGP が OMP からのルートを再配布します。設定可能な AS パス属性の伝達に加えて、BGP コミュニティを伝達するオプションがあります。BGP コミュニティの伝達は、OMP 再配布を使用して VPN を介して Cisco Catalyst SD-WAN サイト間で BGP コミュニティを伝達するのに役立ちます。OMP からのルートの再配布中に BGP コミュニティを伝達するには、 propagate-community コマンドを使用します。

コミュニティ伝達機能は、Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a 以降サポートされています。このオプションを使用しない場合、BGP コミュニティは、接続されている場合でも BGP ネイバーに送信されません。この機能により、Cisco IOS XE Catalyst SD-WAN デバイスは BGP エントリに接続されたコミュニティのネイバーへの伝達を開始できます。BGP オーバーレイは Cisco Catalyst SD-WAN オーバーレイに移行され、VPN を介して Cisco Catalyst SD-WAN サイト間で BGP ルート属性が伝達されます。**propagate-community** コマンドの詳細については、「[propagate-community](#)」を参照してください。

Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以降、BGP から OMP にコミュニティを伝達するときにコミュニティを操作し、`route-map` コマンドを使用して OMP から BGP に戻すことができます。このコマンドでは、あるルーティングプロトコルから別のルーティングプロトコルにルートを再配布するための条件を定義します。`route-map` コマンドごとに、それに関連し

た `match` および `set` コマンドのリストがあります。 `match` コマンドでは、 `match communities`（再配布が許可される条件）を指定します。 `set` コマンドでは、 `set communities`（`match` コマンドによって強制される基準を満たした場合に実行される特定の再配布アクション）を指定します。コマンドの詳細については、[コマンドリファレンスガイド \[英語\]](#) を参照してください。

OSPFv3

表 6: 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE Catalyst SD-WAN デバイスでの OSPFv3 サポート	Cisco IOS XE Catalyst SD-WAN リリース 17.3.2 Cisco vManage リリース 20.3.1	Open Shortest Path First バージョン 3 (OSPFv3) は、IPv6 と IPv4 ユニキャストアドレスファミリーをサポートする IPv4 および IPv6 リンクステートルーティングプロトコルです。

OSPFv3 は、IPv4 および IPv6 アドレスファミリーのルーティングプロトコルです。リンクステートプロトコルは、送信元マシンと宛先マシンを接続するリンクステートに基づいて、ルーティングの決定を行います。リンクステートは、インターフェイスと、その隣接ネットワークデバイスとの関係を説明するものです。インターフェイス情報には、インターフェイスの IPv6 プレフィックス、ネットワークマスク、接続先のネットワークのタイプ、そのネットワークに接続されているデバイスなどが含まれます。この情報は、さまざまなタイプのリンクステートアドバタイズメント (LSA) で伝播されます。

OSPFv3 の大部分は、OSPF バージョン 2 と同じです。RFC 5340 に説明されているように、OSPFv3 では、OSPF バージョン 2 が拡張され、IPv6 ルーティングプレフィックスと、より大きなサイズの IPv6 アドレスに対するサポートが提供されています。

アドレスファミリー IPv6 の場合、OSPFv3 ルートは OSPF ルートを参照し、OSPFv3 内部ルート（エリア内およびエリア間）は OMP に暗黙的にアドバタイズされます。OSPFv3 外部ルート（AS-External と NSSA の両方）は、OSPF 外部設定のアドバタイズを使用して OMP で明示的にアドバタイズできます。これは、OSPF 内部ルートが暗黙的に OMP でアドバタイズされるアドレスファミリー IPv4 の OSPF ルートと一致します。同様に、OSPF 外部ルートは、OSPF 外部設定のアドバタイズを使用して OMP に明示的にアドバタイズできます。

アドレスファミリー IPv4 の場合、OSPFv3 ルートは OSPFv3 ルートとして参照され、OSPFv3 内部ルートは OMP で暗黙的にアドバタイズされません。すべての OSPFv3 IPv4 ルートは、OSPFv3 設定のアドバタイズを使用して OMP でアドバタイズできます。コントローラモードでの OSPFv3 統合はサポートされていません。

EIGRP

Cisco EIGRP (Enhanced Interior Gateway Routing Protocol) は、シスコ独自のルーティングプロトコルです。このプロトコルは、オープンスタンダードの内部ゲートウェイプロトコル (IGP) です。EIGRP は、シスコによって開発された元の Interior Gateway Routing Protocol (IGRP) の

拡張バージョンです。ネットワークに変更がない場合、EIGRPは完全には更新されません。そのため、他のIGPでのフラッディングアクティビティが減少します。また、IGP間で一意の等コストパスと不等コストパスの両方を使用できます。

EIGRPはCisco IOS XE Catalyst SD-WANデバイスでのみサポートされます。

EIGRPの詳細については、「[Introduction to EIGRP](#)」を参照してください。

EIGRPの利点

- ネットワーク幅を15ホップから100ホップに増加
- 高速コンバージェンス
- 増分更新、帯域幅の最小化
- プロトコルに依存しないネイバー探索
- 容易なスケーリング

制限事項と制約事項

- EIGRPはCisco IOS XE Catalyst SD-WANデバイスのトランスポート側ネットワークではサポートされていません。
- EIGRPルート一致は、Cisco SD-WANコントローラ集中管理ポリシーではサポートされていません。

ルーティング情報プロトコル (RIP)

表 7: 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE Catalyst SD-WAN デバイスでのRIPv2サポート	Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a Cisco vManage リリース 20.7.1 Cisco SD-WAN リリース 20.7.1	この機能を使用すると、Cisco IOS XE Catalyst SD-WAN デバイスでRIPv2を設定できます。ルータは、Cisco Catalyst SD-WAN オーバーレイでアダプタイズするためにOverlay Management Protocol (OMP) にRIPv2ルートを再配布し、サービス側ルーティングのためにOpen Shortest Path Firstバージョン3 (OSPFv3) に再配布します。

機能名	リリース情報	説明
Cisco IOS XE Catalyst SD-WAN デバイスでの RIPng (IPv6) サポート	Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a Cisco vManage リリース 20.8.1 Cisco SD-WAN リリース 20.8.1	この機能により、Cisco IOS XE Catalyst SD-WAN デバイスでの IPv6 アドレスとプレフィックスのサポートが追加されます。また、次世代 Routing Information Protocol (RIPng) への接続、スタティック、Overlay Management Protocol (OMP)、および Open Shortest Path First (OSPF) ルートの再配布もサポートします。

Routing Information Protocol のサポートについて

Routing Information Protocol (RIP) は、ブロードキャストまたはマルチキャスト User Datagram Protocol (UDP) データパケットを使用してルーティング情報を交換します。RIPは、小規模から中規模の TCP/IP ネットワークで一般的に使用されるルーティングプロトコルです。RIP はディスタンスベクター アルゴリズムを使用してルートを計算します。Cisco IOS ソフトウェアからは、ルーティング情報の更新が 30 秒ごとに送信されます。この処理はアドバタイジングと呼ばれます。RIP は、ルーティングアップデート メッセージを定期的送信するだけでなく、ネットワークトポロジが変更された場合にも送信します。

RIPv2 (RIP for IPv4)

RIP バージョン 2 (RIPv2) の Cisco IOS ソフトウェア実装では、RIP プロセスごとにローカルデータベースが維持されます。RIP ローカルデータベースには、RIP 対応ルータに隣接するすべてのネットワークデバイスから学習した最良コストの RIP ルートセットが格納されます。ルート再配布では、ルートマップとプレフィックスリストを使用して、プレフィックスでルートを指定できます。

RIPv2 のシスコの実装では、プレーンテキスト認証、メッセージダイジェスト アルゴリズム 5 (MD5) 認証、ルート集約、Classless Inter-Domain Routing (CIDR)、および可変長サブネットマスク (VLSM) をサポートしています。RIPv2 パケットを送受信する場合は、RIPv1 が認証をサポートしていないため、インターフェイスで RIP 認証を有効にすることをお勧めします。各 RIPv2 パケットのデフォルト認証は、プレーンテキスト認証です。

デフォルトでは、ソフトウェアは RIP バージョン 1 (RIPv1) および RIPv2 パケットを受信しますが、送信するのは RIPv1 パケットのみです。RIPv1 パケットのみを送受信するようにソフトウェアを設定できます。または、RIPv2 パケットのみを送受信するようにソフトウェアを設定できます。デフォルトの動作を上書きするには、インターフェイスから送信する RIP バージョンを設定します。同様に、インターフェイスから受信したパケットを処理する方法も制御できます。RIPv2 は、サービス側とトランスポート側の両方でサポートされます。



- (注) ネットワーク設定では、クラスフル IP ネットワーク ID アドレッシングを使用することをお勧めします。

CLI を使用した設定の詳細については、「[CLI を使用した Routing Information Protocol の設定](#)」を参照してください。

RIPng (RIP for IPv6)

次世代 Routing Information Protocol (RIPng) は、IPv6 ネットワークを介したルートの計算に使用されるルーティング情報を通信するための UDP ベースのプロトコルです。RFC 2080 で詳述されている IPv6 用の RIP 拡張には、IPv6 アドレスとプレフィックスのサポートが含まれています。

内部ゲートウェイプロトコル (IGP) としての RIPng は、次の再配布をサポートしています。

- RIP への OMP ルートの再配布
- OMP への RIP ルートの再配布
- OSPFv3 への RIP ルートの再配布
- RIP への OSPFv3 ルートの再配布
- RIP へのスタティックルートの再配布
- スタティックへの RIP ルートの再配布
- RIP への接続ルートの再配布
- 接続への RIP ルートの再配布

RIPng を実装する各ルータには、次のフィールドを含むルーティングテーブルが必要です。

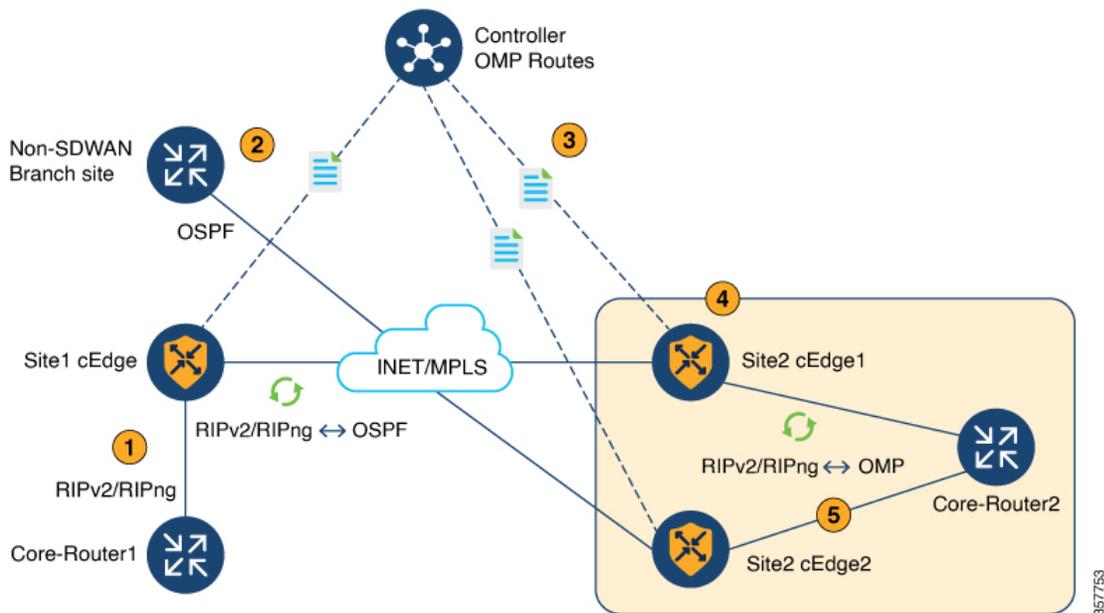
- 接続先の IPv6 プレフィックス。
- メトリック：アドレスに関してアドバタイズされたメトリックの合計コスト。
- ルートタグ：ルートとともにアドバタイズおよび再配布する必要があるルート属性。
- 接続先のネクストホップ IPv6 アドレス。
- ルートに関連付けられたさまざまなタイマー。

Virtual Routing and Forwarding (VRF) モード以外では、IPv6 RIPng プロセスおよびそれに関連付けられた設定ごとに、同じルーティングテーブル内のすべてのルートが保持されます。IPv6 RIPng VRF 対応サポートは、単一のルーティングテーブルに保存されるルートの数を減らすことによって、分離やモジュール性を有効にし、潜在的なパフォーマンスを改善します。さらにこれにより、ネットワーク管理者は異なるいくつかの RIP ルーティングテーブルを作成し、単一の RIP プロトコル コンフィギュレーション ブロックに格納されている同じプロトコル設定を共有することもできます。

大規模なネットワークの RIPng ではルーティンググループが発生しやすく、それによりトラフィックのパスが長くなります。ルートループを回避するために、RIP および RIPng ルートは、ウェルノウン OMP RIP タグを使用して識別されます。

次の図は、RIPv2 および RIPng OMP ルートタギングプロセスを示しています。

図 3: RIPv2 および RIPng トポロジ



1. Core-Router1 が、RIPv2 および RIPng ルートを Site1 にアドバタイズします。
一般的なルールとして、RIPv2 および RIPng ルートのデフォルトのアドミニストレーティブディスタンスは 120 です。OMP ルートのデフォルトのアドミニストレーティブディスタンスは 251 です。
2. RIPv2 および RIPng ルートが OMP で再配布され、アドバタイズされます。
3. Cisco Catalyst SD-WAN コントローラが、OMP ルートを他のブランチにアドバタイズします。
4. Site-2 Edge1 ルータが、一意の値である 44270 の OMP ルートタグを追加し、「OMP が学習したルート」を RIPv2 および RIPng に再配布します。
5. タグ 44270 を持つこのルートを Site-2 Edge2 ルータが受信すると、OMP を介してルート（アドミニストレーティブディスタンス 251）をすでに学習しているため、このルートはインストール「されません」。

OMP ルートが取り消されると、Site-2 Edge2 ルータは、サービス側 VPN を介して RIPv2 および RIPng プロトコルによって学習したルート（タグ 44270）を、アドミニストレーティブディスタンス 252（OMP ルートより 1 つ大きい値）でルーティングテーブルにインストールします。

さらに、Cisco Catalyst SD-WAN のタグ付きルートは、RIPv2 および RIPng ルートが OMP に再配布される場合、OMP で再アダプタイズされません。

CLI を使用した RIPng の設定の詳細については、「[CLI を使用した RIPng の設定](#)」を参照してください。

Routing Information Protocol の使用の前提条件

- バージョン 2 は、RIPv2 パケットのみを送受信するように設定する必要があります。デフォルトでは、RIP バージョン 1 (RIPv1) および RIP バージョン 2 (RIPv2) パケットを受信しますが、送信するのは RIPv1 パケットのみです。

Routing Information Protocol の使用に関する制約事項

RIPv2 (IPv4)

RIP は、異なるルートの値を評価するためのメトリックとしてホップカウントを使用します。ホップカウントは、ルート内で経由されるデバイス数です。直接接続しているネットワークのメトリックはゼロです。到達不能のネットワークのメトリックは16です。このようにメトリックの範囲は狭いため、RIP は大規模なネットワークには適しません。

RIPng (IPv6)

- sdwan** キーワードのみを使用して、コンフィギュレーションコマンドで IPv6 RIP ルーティングプロセス名 (*ripng-instance*) を設定できます。
- IPv6 RIP での VRF 対応サポートでは、一度に 1 つの RIP インスタンスのみが許可されます。複数の RIP インスタンスは許可されません。
- RIPng は、GigabitEthernet、TenGigabitEthernet、および VLAN インターフェイスでのみ設定できます。

ユニキャストオーバーレイルーティングの設定

このトピックでは、ユニキャストオーバーレイルーティングをプロビジョニングする方法について説明します。

トランスポート側ルーティング

Cisco SD-WAN デバイス間の通信を有効にするには、VPN 0 のループバック インターフェイスで OSPF または BGP を設定します。ループバック インターフェイスは、Cisco IOS XE Catalyst SD-WAN デバイスがオーバーレイネットワークに参加するために必要な DTLS および IPSec トンネル接続の終端となる仮想トランスポート インターフェイスです。

Cisco SD-WAN Manager を使用してトランスポート側の BGP を設定するには、「BGP の設定」を参照してください。CLI を使用してトランスポート側の BGP を設定するには、「CLI を使用した BGP の設定」のトピックを参照してください。

BGP を設定する

ボーダー ゲートウェイ プロトコル (BGP) は、ローカルサイトのネットワークへの到達可能性を提供するサービス側ルーティングに使用できます。また、デバイスが WAN クラウドに直接接続されていない場合に Cisco Catalyst SD-WAN デバイス間の通信を可能にするトランスポート側ルーティングに使用できます。2 つの BGP ルーティングタイプに個別の BGP テンプレートを作成します。



- (注) Cisco IOS XE Catalyst SD-WAN デバイスは、VPN の代わりに VRF を使用します。ただし、Cisco SD-WAN Manager を介した Cisco IOS XE Catalyst SD-WAN デバイスの設定には引き続き次の手順が適用されます。設定を完了すると、VPN 設定が VRF 設定に自動的にマッピングされます。

Cisco SD-WAN Manager テンプレートを使用して BGP ルーティングプロトコルを設定するには、次の手順を実行します。

1. BGP 機能テンプレートを作成して、BGP パラメータを設定します。
2. VPN 機能テンプレートを作成して、サービス側 BGP ルーティング (VPN 0 または VPN 512 以外の VPN) またはトランスポート側 BGP ルーティング (VPN 0) のいずれかに VPN パラメータを設定します。

BGP テンプレートの作成

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** の順に選択します。
2. **[Device Template]** をクリックします。



- (注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Device Template]** のタイトルは **[Device]** です。

3. **[Create Template]** をクリックします。
4. **[Create Template]** ドロップダウンリストから、**[From Feature Template]** を選択します。
5. **[Device Model]** ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
6. VPN 0 または VPN 512 のテンプレートを作成するには、次の手順を実行します。

1. [Description] フィールドのすぐ下にある [Transport & Management VPN] をクリックするか、[Transport & Management VPN] セクションまでスクロールします。
 2. [Additional VPN 0 Templates] で、[BGP] をクリックします。
 3. [BGP] ドロップダウンリストから、[Create Template] をクリックします。[BGP] テンプレートフォームが表示されます。フォームの上部にはテンプレートに名前を付けるためのフィールドがあり、下部にはBGPパラメータを定義するためのフィールドがあります。
7. VPN 1 ～ 511 および 513 ～ 65530 のテンプレートを作成するには、次の手順を実行します。
1. [Description] フィールドのすぐ下にある [Service VPN] をクリックするか、[Service VPN] セクションまでスクロールします。
 2. [Service VPN] ドロップダウンリストをクリックします。
 3. [Additional VPN Templates] で、[BGP] をクリックします。
 4. [BGP] ドロップダウンリストから、[Create Template] をクリックします。[BGP] テンプレートフォームが表示されます。フォームの上部にはテンプレートに名前を付けるためのフィールドがあり、下部にはBGPパラメータを定義するためのフィールドがあります。
8. [テンプレート名 (Template Name)] フィールドに、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。
9. [Template Description] フィールドに、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。

基本的な BGP パラメータの設定

ボーダー ゲートウェイ プロトコル (BGP) を設定するには、[Basic Configuration] をクリックし、次のパラメータを設定します。BGPを設定する場合、アスタリスクの付いたパラメータは必須です。

パラメータ名	説明
Shutdown*	[No] をクリックして、VPN の BGP を有効にします。
[AS number] *	ローカル AS 番号を入力します。
Router ID	10 進数の 4 つの部分からなるドット付き表記で BGP ルータ ID を入力します。
[Propagate AS Path]	BGP AS パス情報を OMP に伝送するには、[On] をクリックします。

パラメータ名	説明
Internal Routes Distance	ある AS から別の AS に到達するルートの BGP ルート アドミニストレーティブ ディスタンスとして適用する値を入力します。 範囲：0 ～ 255 デフォルト：200
[Local Routes Distance]	ローカル AS 内のルートの BGP ルート アドミニストレーティブ ディスタンスを指定します。デフォルトでは、BGP からローカルに受信したルートが OMP から受信したルートよりも優先されます。 範囲：0 ～ 255 デフォルト：200
External Routes Distance	オーバーレイネットワーク内の他のサイトから学習したルートの BGP ルート アドミニストレーティブ ディスタンスを指定します。 範囲：0 ～ 255 デフォルト：20

サービス側 BGP では、デバイスが学習する Cisco Catalyst SD-WAN コントローラの任意の BGP ルートにアダプタイズするようにオーバーレイ管理プロトコル (OMP) を設定できます。デフォルトでは、Cisco SD-WAN デバイスはデバイスの接続ルートとデバイスに設定されているスタティックルートの両方を OMP にアダプタイズしますが、デバイスが学習した BGP 外部ルートはアダプタイズしません。このルートアダプタイズメントは、デバイスまたは Cisco SD-WAN ソフトウェアの OMP テンプレートで設定します。

トランスポート側 BGP では、VPN 0 の物理インターフェイスとループバック インターフェイスも設定する必要があります。また、ループバック インターフェイス アドレスをネイバーにアダプタイズする BGP のポリシーを作成し、BGP インスタンスまたは特定のネイバーにポリシーを適用する必要があります。

機能テンプレートを保存するには、[Save] をクリックします。

ユニキャストアドレスファミリの設定

グローバル BGP アドレスファミリ情報を設定するには、[Unicast Address Family] をクリックし、次のパラメータを設定します。

パラメータ	オプション	サブオプション	説明
IPv4 / IPv6			IPv4 ユニキャストアドレスファミリを設定するには、[IPv4] をクリックします。IPv6 ユニキャストアドレスファミリを設定するには、[IPv6] をクリックします。

パラメータ	オプション	サブオプション	説明
Maximum Paths			IBGP マルチパス ロードシェアリングを有効にするために、ルートテーブルにインストールできるパラレル IBGP パスの最大数を指定します。 範囲：0 ～ 32
Mark as Optional Row			この設定をデバイス固有としてマークするには、[Mark as Optional Row] をクリックします。デバイスにこの設定を含めるには、デバイステンプレートをデバイスに添付するときに要求された変数値を入力するか、テンプレート変数スプレッドシートを作成して変数を適用します。

パラメータ	オプション	サブオプション	説明	
Redistribute	[Redistribute] > [New Redistribute] をクリックします。			
	Mark as Optional Row	この設定をデバイス固有としてマークするには、[Mark as Optional Row] をクリックします。デバイスにこの設定を含めるには、デバイステンプレートをデバイスに添付するときに要求された変数値を入力するか、テンプレート変数スプレッドシートを作成して変数を適用します。		
	Protocol	すべての BGP セッションに対して、ルートを BGP に再配布するプロトコルを選択します。次のオプションがあります。		
		static	スタティックルートを BGP に再配布します。	
		connected	接続ルートを BGP に再配布します。	
		ospf	Open Shortest Path First ルートを BGP に再配布します。	
		omp	オーバーレイ管理プロトコルルートを BGP に再配布します。	
		nat	ネットワークアドレス変換ルートを BGP に再配布します。	
		[natpool-outside]	外部 NAT ルートを BGP に再配布します	
少なくとも、次の項目を選択します。				
<ul style="list-style-type: none"> サービス側 BGP ルーティングの場合は、[OMP] を選択します。デフォルトでは、OMP ルートは BGP に再配布されません。 トランスポート側 BGP ルーティングの場合は、[Connected] を選択し、[Route Policy] で、BGP がループバック インターフェイスアドレスをネイバーにアドバタイズするルートポリシーを指定します。 				
Route Policy	再配布されるルートに適用するルートポリシーの名前を入力します。			
[Add] をクリックして再配布情報を保存します。				

パラメータ	オプション	サブオプション	説明
ネットワーク	[Network] > [New Network] をクリックします。		
	Mark as Optional Row		この設定をデバイス固有としてマークするには、[Mark as Optional Row] をクリックします。デバイスにこの設定を含めるには、デバイステンプレートをデバイスに添付するときに要求された変数値を入力するか、テンプレート変数スプレッドシートを作成して変数を適用します。
	[Network Prefix]		BGP によってアドバタイズされるネットワークプレフィックスをプレフィックス/長さの形式で入力します。
	[Add] をクリックして、ネットワークプレフィックスを保存します。		
[Aggregate Address]	[Aggregate Address] > [New Aggregate Address] をクリックします。		
	Mark as Optional Row		この設定をデバイス固有としてマークするには、[Mark as Optional Row] をクリックします。デバイスにこの設定を含めるには、デバイスにデバイステンプレートを添付するときに変数値を入力するか、テンプレート変数スプレッドシートを作成して変数を適用します。
	[Aggregate Prefix] [IPv6 Aggregate Prefix]		すべての BGP セッションに対して集約するアドレスのプレフィックスをプレフィックス/長さの形式で入力します。
	[AS Set Path]		集約されたプレフィックスの設定パス情報を生成するには、[On] をクリックします。
	[Summary Only]		BGP アップデートから特定のルートを除外するには、[On] をクリックします。
	[Add] をクリックして、集約アドレスを保存します。		

機能テンプレートを保存するには、[Save] をクリックします。

AS 番号を変更するには、次の手順を実行します。

1. BGP 設定を削除します。数秒間待ちます。
2. 変更した global-as および local-as 設定を使用して BGP を再度設定します。

BGP ネイバーの設定

ネイバーを設定するには、[Neighbor] > [New Neighbor] をクリックし、次のパラメータを設定します。



(注) BGP を機能させるには、少なくとも 1 つのネイバーを設定する必要があります。

パラメータ名	オプション	サブオプション	説明
IPv4 / IPv6	IPv4 ネイバーを設定するには、[IPv4] をクリックします。IPv6 ネイバーを設定するには、[IPv6] をクリックします。		
Address/IPv6 Address	BGP ネイバーの IP アドレスを指定します。		
Description	BGP ネイバーの説明を入力します。		
Remote AS	リモート BGP ピアの AS 番号を入力します。		
アドレスファミリ (Address Family)	[On] をクリックし、アドレスファミリを選択します。アドレスファミリ情報を入力します。ソフトウェアは、BGP IPv4 ユニキャストアドレスファミリのみをサポートします。		
	アドレスファミリ (Address Family)	アドレスファミリを選択します。ソフトウェアは、BGP IPv4 ユニキャストアドレスファミリのみをサポートします。	
	[Maximum Number of Prefixes]	ネイバーから受信可能なプレフィックスの最大数を指定します。 範囲：1 ~ 4294967295 デフォルト：0	
	Threshold	警告メッセージを生成するしきい値、または BGP 接続を再起動するしきい値を指定します。しきい値はプレフィックスの最大数の割合です。再起動間隔または警告のみを指定できます。	
	[Restart Interval]	BGP 接続の再起動を待機する時間を指定します。範囲：1 ~ 65535 分	
	[Warning Only]	BGP 接続を再起動せずに警告メッセージを表示するには、[On] をクリックします。	
	[Route Policy In]	[On] をクリックして、ネイバーから送信されるプレフィックスを持つルートポリシーの名前を指定します。	
[Route Policy Out]	[On] をクリックして、ネイバーに送信するプレフィックスを持つルートポリシーの名前を指定します。		
Shutdown	BGP ネイバーへの接続を有効にするには、[On] をクリックします。		

MPLS インターフェイスの設定

表 8: 機能の履歴

機能名	リリース 情報	説明
サービス側の MPLS-BGP サ ポート	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	この機能を使用すると、マルチプロトコルラベルスイッ チング (MPLS) をサポートできます。複数のサービス VPN は、相互自律システム (AS) BGP ラベル付きパス を使用してトラフィックを転送するため、より少ないコン トロールプレーンシグナリングでサービス側 VPN を 拡張できます。 特定のデバイスにおける特定の VPN ルーティングおよ び転送 (VRF) インスタンスのラベル配布は、ボーダー ゲートウェイプロトコル (BGP) で処理できます。

Cisco IOS XE Catalyst SD-WAN デバイスは、マルチプロトコルラベルスイッチング (MPLS) をサポートして、マルチプロトコル環境を実現します。MPLS は、非常にスケーラブルでプロトコルに依存しない、データ伝送メカニズムを提供します。このメカニズムでは、割り当てられたラベルを持つデータパケットが、仮想リンクを介してネットワーク全体に転送されます。BGP プロトコルの拡張を使用して、MPLS パスを管理できます。Cisco IOS XE Catalyst SD-WAN デバイスには、BGP MPLS VPN オプション B の機能もあります。

複数のサービス VPN は、相互自律システム (AS) BGP ラベル付きパスを使用してトラフィックを転送するため、より少ないコントロールプレーンシグナリングでサービス側 VPN を拡張できます。MPLS インターフェイスは、グローバル VRF でのみサポートされます。

MPLS インターフェイスを設定するには、次の手順を実行します。

- [MPLS Interface] をクリックします。
- [Interface Name] フィールドにインターフェイス名を入力します。
- [+] をクリックしてインターフェイスを追加し、設定を保存できます。

ラベル範囲の設定

Cisco SD-WAN Manager では、BGP MPLS のラベルスペースが自動的にプログラムされます。ラベルは VPN ごとに割り当てられます。設定を表示するには、**show sdwan running-config** コマンドを使用します。

設定例

```
show sdwan running-config
mpls label range 100000 1048575 static 16 999
mpls label mode all-vrfs protocol bgp-ipv4 per-vrf
mpls label mode all-vrfs protocol bgp-ipv6 per-vrf
```

ルートターゲットの設定

Cisco IOS XE Catalyst SD-WAN デバイスにルートターゲットを設定できます。ルートターゲットの設定は、eBGP および IPv4 ピアデバイスでのみサポートされます。サポートされているすべてのプロトコルを BGP に再配布できます。

ルートターゲットを設定するには、[Route Targets] をクリックし、次のパラメータを設定します。

パラメータ	オプション	サブオプション	説明
IPv4 / IPv6			IPv4 インターフェイスのルートターゲットを設定するには、[IPv4] をクリックします。IPv6 インターフェイスのルートターゲットを設定するには、[IPv6] をクリックします。
[Add VPN]			[Add VPN] をクリックして、VPN を追加します。
[VPN ID for IPv4]			IPv4 インターフェイスの VPN ID を指定します。
[インポート (Import)]			ターゲット VPN 拡張コミュニティからルーティング情報をインポートします。
[エクスポート (Export)]			ターゲット VPN 拡張コミュニティにルーティング情報をエクスポートします。

機能テンプレートを保存するには、[Save] をクリックします。

最初からデバイスにデフォルトのルートターゲットが設定されている場合は、必要に応じてエントリを追加できます。

詳細なネイバーパラメータの設定

ネイバーの詳細なパラメータを設定するには、[Neighbor] > [Advanced Options] をクリックします。

パラメータ名	説明
[Next-Hop Self]	BGP ネイバーにアドバタイズされるルートのネクストホップとしてルータを設定するには、[On] をクリックします。
[Send Community]	ローカルルータの BGP コミュニティ属性を BGP ネイバーに送信するには、[On] をクリックします。
[Send Extended Community]	ローカルルータの BGP 拡張コミュニティ属性を BGP ネイバーに送信するには、[On] をクリックします。
[Negotiate Capability]	ネイバーによってサポートされている BGP 拡張機能について BGP セッションが学習できるようにするには、[On] をクリックします。
[Source Interface Address]	BGP がネイバーへの TCP 接続に使用するネイバーにおける特定のインターフェイスの IP アドレスを入力します。

パラメータ名	説明
[Source Interface Name]	BGP がネイバーへの TCP 接続に使用するネイバーにおける特定のインターフェイスの名前を、ge port/slot の形式で入力します。
[EBGP Multihop]	外部ピアへの BGP 接続の存続可能時間 (TTL) を設定します。 範囲：0 ～ 255 デフォルトは 1 です。
Password	MD5 メッセージダイジェストの生成に使用するパスワードを入力します。パスワードを設定すると、BGP ピアとの TCP 接続で MD5 認証が有効になります。パスワードは、大文字と小文字が区別され最大 25 文字です。パスワードには、すべての英数字 (スペースを含む) を使用できます。最初の文字を数値にはできません。
Keepalive Time	キープアライブメッセージが BGP ピアにアダバタイズされる頻度を指定します。キープアライブメッセージは、ローカルルータがまだアクティブであり、使用可能だと見なされることをピアに示します。グローバルキープアライブ時間をオーバーライドするネイバーのキープアライブ時間を指定します。 範囲：0 ～ 65535 秒 デフォルト：60 秒 (ホールド時間値の 3 分の 1)
Hold Time	ローカル BGP セッションでそのピアが使用可能でないと見なされるキープアライブメッセージを受信しない間隔を指定します。ローカルルータは、そのピアへの BGP セッションを終了します。グローバルホールド時間をオーバーライドするネイバーのホールド時間を指定します。 範囲：0 ～ 65535 秒 デフォルト：180 秒 (キープアライブタイマーの 3 倍)
[Connection Retry Time]	ダウンした設定済みの BGP ネイバーピアへの接続確立を再試行する間隔の秒数を指定します。 範囲：0 ～ 65535 秒 デフォルト：30 秒
Advertisement Interval	BGP ネイバーの場合、BGP ルーティングアップデートパケットがそのネイバーに送信される最小ルートアダバタイズメントインターバル (MRAI) を設定します。 範囲：0 ～ 600 秒。 デフォルト：IBGP ルートアダバタイズメントの場合は 5 秒。EBGP ルートアダバタイズメントの場合は 30 秒

機能テンプレートを保存するには、[Save] をクリックします。

パラメータ値の範囲の変更

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が [Default] (👍) に設定され、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、パラメータフィールドの左側にある [Scope] ドロップダウンリストをクリックし、次のいずれかを選択します。

パラメータ名	説明
 [Device Specific]	<p>デバイス固有の値がパラメータに使用されます。デバイス固有のパラメータの場合、機能テンプレートに値を入力できません。デバイスをデバイステンプレートに添付するときに、値を入力します。</p> <p>[Device Specific] をクリックすると、[Enter Key] ボックスが表示されます。このボックスには、作成する CSV ファイル内のパラメータを識別する一意の文字列であるキーが表示されます。このファイルは、キーごとに1つの列を含む Excel スプレッドシートです。ヘッダー行にはキー名（行ごとに1つのキー）が含まれます。その後の各行は、デバイスに対応し、そのデバイスのキーの値を定義します。デバイスをデバイステンプレートに添付するときに、この CSV ファイルをアップロードします。</p> <p>デフォルトキーを変更するには、新しい文字列を入力し、[Enter Key] ボックスの外にカーソルを移動します。</p> <p>デバイス固有のパラメータの例としては、システム IP アドレス、ホスト名、GPS ロケーション、サイト ID があります。</p>
 グローバル	<p>パラメータの値を入力し、その値をすべてのデバイスに適用します。</p> <p>デバイスのグループにグローバルに適用できるパラメータの例としては、DNS サーバー、Syslog サーバー、インターフェイス MTU があります。</p>

詳細な BGP パラメータの設定

BGP の詳細パラメータを設定するには、[Advanced] をクリックし、次のパラメータを設定します。

パラメータ名	説明
Hold Time	ローカル BGP セッションでそのピアが使用可能でないと見なされるキープアライブメッセージを受信しない間隔を指定します。ローカルデバイスはその後、そのピアへの BGP セッションを終了します。このホールド時間は、グローバルホールド時間です。 範囲：0 ～ 65535 秒 デフォルト：180 秒（キープアライブタイマーの 3 倍）
キープアライブ	キープアライブメッセージが BGP ピアにアダバタイズされる頻度を指定します。キープアライブメッセージは、ローカルデバイスがまだアクティブであり、使用可能だと見なされることをピアに示します。このキープアライブ時間は、グローバルキープアライブ時間です。 範囲：0 ～ 65535 秒 デフォルト：60 秒（ホールド時間値の 3 分の 1）
[Compare MED]	比較されるルートのピア AS が同じであるかどうかに関係なく、MED を常に比較するには、[On] をクリックします。
[Deterministic MED]	ルートの受信タイミングに関係なく、同じ AS から受信したすべてのルートの Multi-Exit 識別子 (MED) を比較するには、[On] をクリックします。
[Missing MED as Worst]	パスに MED 属性がない場合、パスを最下位のパスと見なすには、[On] をクリックします。
[Compare Router ID]	BGP パス間でデバイス ID を比較し、アクティブパスを決定するには、[On] をクリックします。
[Multipath Relax]	BGP ベストパスプロセスに AS 内の異なるルートから選択させるには、[On] をクリックします。デフォルトでは、BGP マルチパスを使用している場合、BGP ベストパスプロセスは同じ AS 内のルートから選択し、複数のパス間でロードバランシングを行います。

機能を保存するには、[Save] をクリックします。

CLI を使用した BGP の設定

これは、Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以前のリリースの Cisco IOS XE Catalyst SD-WAN デバイスにおける BGP 設定の例です。

```
router bgp 100
  bgp log-neighbor-changes
  distance bgp 20 200 20
  !
  address-family ipv4 vrf 100
    bgp router-id 10.0.0.0
    redistribute omp
    neighbor 10.0.0.1 remote-as 200
```

```

neighbor 10.0.0.1 activate
neighbor 10.0.0.1 send-community both
neighbor 10.0.0.1 route-map OMP_BGP-POLICY in
neighbor 10.0.0.1 maximum-prefix 2147483647 100

route-map OMP_BGP-POLICY permit 1
match ip address prefix-list OMP-BGP-TEST-PREFIX-LIST
set omp-tag 10000
route-map OMP_BGP-POLICY permit 65535

ip prefix-list OMP-BGP-TEST-PREFIX-LIST seq 5 permit 10.0.0.0/8

```



(注) Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以降、非 VRF アドレスファミリの BGP 設定に次の変更が適用されます。

- **remote-as** キーワードは、非 VRF **address-family** コマンドではサポートされていません。非 VRF アドレスファミリの場合、**remote-as ASN** はルータ BGP モードで設定する必要があります。
- BGP 距離設定は、ルータ BGP モードではサポートされていません。BGP 距離は、指定された非 VRF アドレスファミリで設定する必要があります。

導入された変更を反映するように設定を変更するには、デバイス CLI テンプレートまたは CLI アドオン機能テンプレートを手動で更新する必要があります。

次に、Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以降の BGP 設定の例を示します。

```

router bgp 100
neighbor 10.10.10.10 remote-as
address-family ipv4
distance bgp 20 200 200
neighbor 10.10.10.10 activate
address-family ipv4 unicast vrf RED
distance bgp 30 300 300
neighbor 10.11.11.11 remote-as
neighbor 10.11.11.11 activate

```

OMP での BGP 再配布ルートの確認

```

デバイス#show sdwan omp routes 10.0.0.0/8
-----
omp route entries for vpn 100 route 10.0.0.0/8
-----
RECEIVED FROM:
peer          172.16.0.0
path-id       470777
label         1002
status        C,I,R
loss-reason   not set
lost-to-peer  not set
lost-to-path-id not set
Attributes:
originator    10.0.0.1

```

```

type                installed
tloc                172.16.0.1, mpls, ipsec
ultimate-tloc      not set
domain-id           not set
overlay-id          1
site-id             1
preference          not set
tag                 10000 <=====
origin-PROTO        eBGP
as-path             not set
unknown-attr-len   not set

```

次に、Cisco IOS XE Catalyst SD-WAN デバイスでの BGP コミュニティの伝達の例を示します。

```

vm5# show sdwan omp routes 192.168.0.0/16 detail
-----
omp route entries for vpn 1 route
192.168.0.0/16-----
                RECEIVED FROM:
peer           10.0.0.0
path-id        70
label          1007
status         C,Red,R
loss-reason    not set
lost-to-peer   not set
lost-to-path-id not set
Attributes:
  originator   192.168.0.0
  type         installed
  tloc         192.168.0.1, lte, ipsec
  ultimate-tloc not set
  domain-id    not set
  overlay-id   1
  site-id      500
  preference   not set
  tag          not set
  origin-PROTO iBGP
  origin-metric 0
  as-path      not set
  community    100:1 100:2 100:3
  unknown-attr-len not set
                ADVERTISED TO:
peer           192.168.0.1

```

ここでは、ユニキャストオーバーレイルーティングのサービス側とトランスポート側に BGP を設定する方法について説明します。

サービス側ルーティングの設定

Cisco IOS XE Catalyst SD-WAN デバイスでルーティングを設定するには、1 つまたは複数の VPN をプロビジョニングします（セグメンテーションが必要な場合）。各 VPN 内で、その VPN に参加するインターフェイスと、その VPN で動作するルーティングプロトコルを設定します。

1. VPN を設定します。

```

Device(config)# vrf definition vpn-id
Device(config-vrf)# address-family ipv4
Device(config-ipv4)# exit
Device(config-vrf)# address-family ipv6
Device(config-ipv6)# exit
Device(config-vrf)# exit
Device(config)#

```

vpn-id には、VPN 0 および VPN 512 以外の VPN である任意のサービス側 VPN を指定できます。VPN 0 はトランスポート VPN であり、制御トラフィックのみを伝送し、VPN 512 は管理 VPN です。

2. VPN で実行するように BGP を設定します。

1. ローカル AS 番号を設定します。

```
Device(config)# router bgp local-as-number
Device(config-router)# address-family ipv4 unicast vrf vpn-id
```

AS 番号は、2 バイトの ASDOT 表記（1 - 65535）または 4 バイトの ASDOT 表記（1.0 - 65535.65535）で指定できます。

2. アドレスと AS 番号（リモート AS 番号）を指定して BGP ピアを設定し、ピアへの接続を有効にします。

```
Device(config-router-af)# neighbor neighbor-ip-address remote-as remote-as-number
```

3. Cisco IOS XE Catalyst SD-WAN デバイスのシステム IP アドレスを設定します。

```
Device(config)# system system-ipaddress
```

SD-WAN IOS XE ルータでの BGP 設定の例

```
Device# show running-config system
system
  system-ip 10.1.2.3
!
Device# show running-config vpn 1
router bgp 2
  bgp log-neighbor-changes
  timers bgp 1 111
  neighbor 10.20.25.16 remote-as 1
!
  address-family ipv4 unicast
  neighbor 10.20.25.16 activate
  exit-address-family
!
  address-family vpnv4 unicast
  neighbor 10.20.25.16 activate
  neighbor 10.20.25.16 send-community extended
  exit-address-family
!
  address-family vpnv6 unicast
  neighbor 10.20.25.16 activate
  neighbor 10.20.25.16 send-community extended
  exit-address-family
!
  address-family ipv4 unicast vrf 1
  redistribute connected
  redistribute static
  exit-address-family
!
  address-family ipv6 unicast vrf 1
  redistribute connected
  redistribute omp
!
exit-address-family
!
```

```

address-family ipv4 unicast vrf 2
redistribute connected

exit-address-family

```

ルートターゲットの設定例：

```

vrf config

vrf definition 1
rd 1:1

!
address-family ipv4

route-target export 200:1

route-target import 100:1

exit-address-family
!
address-family ipv6
route-target export 101:1
route-target import 201:1
exit-address-family

```

BGP ルートと AS パス情報の再配布

デフォルトでは、他のルーティングプロトコルからのルートは BGP に再配布されません。このことは、OMP はオーバーレイネットワーク全体の宛先へのルートを学習するため、BGP が OMP ルートを学習するのに役立ちます。Cisco Catalyst SD-WAN デバイスの BGP は、ネットワークのサービス側にあるすべての BGP ルータに OMP ルートをアドバタイズします。

```

config-transaction
router bgp 2
  address-family ipv4 unicast
    redistribute omp route-map route_map

```

OMP ルートを BGP に再配布して、それらのルートがネットワークのサービス側にあるすべての BGP ルータにアドバタイズされるようにするには、トランスポート VRF や管理 VRF を除くすべての VRF で再配布を設定します。

Cisco IOS XE Catalyst SD-WAN デバイスの場合、ルータ BGP 設定では、`redistribute omp metric` がすべてのブランチで無効になっているため、`redistribute omp metric 0` 設定の代わりに `redistribute omp route-map set/match` が使用されます。

```

デバイス(config)# router bgp 100
デバイス(config-router)# address-family ipv4 vrf 100
デバイス(config-router-af)# redistribute omp [route-map policy-name]

```

```

config-transaction
router bgp 100
  address-family ipv4 vrf 100
    redistribute omp route_map route_map

```

上記の例に示すように、OSPF などの他のプロトコルから学習したルートを再配布し、BGP にリッピングし、ポリシーを適用することもできます。

ルートの再配布はネイバー単位で制御できます。

```
config-transaction
router bgp 100
  address-family ipv4
    neighbor 10.0.100.1 route-map route_map (in | out)
```

Cisco Catalyst SD-WAN コントローラから OMP を介してから学習した BGP ルートをアドバタイズするように Cisco IOS XE Catalyst SD-WAN デバイスを設定できます。設定することで、Cisco Catalyst SD-WAN コントローラはオーバーレイネットワーク内の他の Cisco IOS XE Catalyst SD-WAN デバイスにそれらのルートをアドバタイズできます。BGP ルートをグローバルに、または特定の VRF に対してアドバタイズできます。

```
config-transaction
sdwan
  omp
    address-family ipv4 vrf 100
      advertise bgp
    exit
```

OSPF の設定

すべての Cisco Catalyst SD-WAN デバイスに OSPF テンプレートを使用します。



- (注) Cisco IOS XE SD-WAN デバイスは、VPN の代わりに VRF を使用します。ただし、Cisco SD-WAN Manager を介した Cisco IOS XE Catalyst SD-WAN デバイスの設定には引き続き次の手順が適用されます。設定を完了すると、VPN 設定が VRF 設定に自動的にマッピングされます。

Cisco SD-WAN Manager テンプレートを使用してデバイスで OSPF を設定するには、次の手順を実行します。

1. OSPF 機能テンプレートを作成して、OSPF パラメータを設定します。OSPF は、ローカルサイトのネットワークへの到達可能性を提供するサービス側ルーティングに使用できます。また、ルータが WAN クラウドに直接接続されていない場合に Cisco Catalyst SD-WAN デバイス間の通信を可能にするトランスポート側ルーティングに使用できます。2つの OSPF ルーティングタイプに個別の OSPF テンプレートを作成します。
2. VPN 機能テンプレートを作成して、サービス側 OSPF ルーティング (VPN 0 または VPN 512 以外) またはトランスポート側 OSPF ルーティング (VPN 0) の VPN パラメータを設定します。詳細については、VPN のヘルプトピックを参照してください。

OSPF テンプレートの作成

1. Cisco SD-WAN Manager メニューから、[Configuration] > [Templates] の順に選択します。
2. [Device Template] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. [テンプレートの作成 (Create Template)] をクリックします。
4. [Create Template] ドロップダウンリストから、[From Feature Template] を選択します。
5. [Device Model] ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。VPN 0 または VPN 512 のテンプレートを作成するには、次の手順を実行します。
 1. [Description] フィールドのすぐ下にある [Transport & Management VPN] をクリックするか、[Transport & Management VPN] セクションまでスクロールします。
 2. [Additional VPN 0 Templates] で、[OSPF] をクリックします。
 3. [OSPF] ドロップダウンリストから、[Create Template] をクリックします。[OSPF] テンプレートフォームが表示されます。フォームの上部にはテンプレートに名前を付けるためのフィールドがあり、下部には OSPF パラメータを定義するためのフィールドがあります。
6. VPN 1 ~ 511 および 513 ~ 65530 のテンプレートを作成するには、次の手順を実行します。
 1. [Description] フィールドのすぐ下にある [Service VPN] をクリックするか、[Service VPN] セクションまでスクロールします。
 2. [Service VPN] ドロップダウンリストをクリックします。
 3. [Additional VPN Templates] で、[OSPF] をクリックします。
 4. [OSPF] ドロップダウンリストから、[Create Template] をクリックします。[OSPF] テンプレートフォームが表示されます。フォームの上部にはテンプレートに名前を付けるためのフィールドがあり、下部には OSPF パラメータを定義するためのフィールドがあります。
7. [テンプレート名 (Template Name)] フィールドに、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。
8. [Template Description] フィールドに、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が [Default] に設定され (チェックマークで示される)、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、パラメータフィールドの左側にある [Scope] ドロップダウンリストをクリックし、次のいずれかを選択します。

表 9:

パラメータの範囲	範囲の説明
デバイス固有 (ホストのアイコンで示される)	<p>デバイス固有の値がパラメータに使用されます。デバイス固有のパラメータの場合、機能テンプレートに値を入力できません。Cisco SD-WAN デバイスをデバイステンプレートに添付するときに、値を入力します。</p> <p>[Device Specific] をクリックすると、[Enter Key] ボックスが表示されます。このボックスには、作成する CSV ファイル内のパラメータを識別する一意の文字列であるキーが表示されます。このファイルは、キーごとに 1 つの列を含む Excel スプレッドシートです。ヘッダー行にはキー名 (行ごとに 1 つのキー) が含まれます。その後の各行は、デバイスに対応し、そのデバイスのキーの値を定義します。Cisco SD-WAN デバイスをデバイステンプレートに添付するときに、この CSV ファイルをアップロードします。詳細については、「Create a Template Variables Spreadsheet」を参照してください。</p> <p>デフォルトキーを変更するには、新しい文字列を入力し、[Enter Key] ボックスの外にカーソルを移動します。</p> <p>デバイス固有のパラメータの例としては、システム IP アドレス、ホスト名、GPS ロケーション、サイト ID があります。</p>
グローバル (地球のアイコンで示される)	<p>パラメータの値を入力し、その値をすべてのデバイスに適用します。</p> <p>デバイスのグループにグローバルに適用できるパラメータの例としては、DNS サーバー、Syslog サーバー、インターフェイス MTU があります。</p>

基本的な OSPF の設定

基本的な OSPF を設定するには、[Basic Configuration] を選択し、次のパラメータを設定します。パラメータはすべてオプションです。OSPF を機能させるには、次に説明するようにエリア 0 を設定する必要があります。

表 10:

パラメータ名	説明
Router ID	10 進数の 4 つの部分からなるドット表記で OSPF ルータ ID を入力します。これは、リンクステートアドバタイズメント (LSA) および隣接関係にある OSPF ルータに関連付けられた一意の 32 ビット識別子です。
Distance for External Routes	<p>他のドメインから学習したルートの OSPF ルート アドミニストレーティブ ディスタンスを指定します。</p> <p>範囲 : 0 - 255、デフォルト : 110</p>

パラメータ名	説明
Distance for Inter-Area Routes	あるエリアから別のエリアに到達するルートの OSPF ルートアドミニストレーティブ ディスタンスを指定します。 範囲：0 ～ 255、デフォルト：110
Distance for Intra-Area Routes	エリア内のルートの OSPF ルートアドミニストレーティブ ディスタンスを指定します。 範囲：0 ～ 255、デフォルト：110

機能テンプレートを保存するには、[Save] をクリックします。

OSPF へのルートの再配布

他のプロトコルから学習したルートを Cisco SD-WAN デバイス上の OSPF に再配布するには、**[Redistribute] > [Add New Redistribute]** を選択し、次のパラメータを設定します。

表 11:

パラメータ名	説明
Protocol	OSPF にルートを再配布するプロトコルを選択します。[BGP]、[Connected]、[NAT]、[OMP]、[EIGRP]、および [Static] から選択します。
Route Policy	OSPF に再配布される前にルートに適用するローカライズされた制御ポリシーの名前を入力します。

別の OSPF ルート再配布ポリシーを追加するには、プラス記号 (+) をクリックします。

テンプレートコンフィギュレーションから OSPF ルート再配布ポリシーを削除するには、エントリの右側にあるゴミ箱アイコンをクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

最大メトリックをアダバタイズする OSPF の設定

他のデバイスが Cisco IOS XE Catalyst SD-WAN デバイスを最短パス優先 (SPF) 計算で中間ホップとして優先しないように、OSPF が最大メトリックをアダバタイズするように設定するには、**[Maximum Metric (Router LSA)] > [Add New Router LSA]** を選択し、次のパラメータを設定します。

表 12:

パラメータ名	説明
Type	<p>タイプを選択します。</p> <ul style="list-style-type: none"> • [Administrative] : オペレータの介入によって最大メトリックがただちに有効になるようにします。 • [On-Startup] : 指定した時間の最大メトリックをアドバタイズします。
Advertisement Time	<p>[On-Startup] を選択した場合は、ルータの起動後に最大メトリックをアドバタイズする秒数を指定します。</p> <p>範囲 : 0、5 – 86400 秒、デフォルト : 0 秒 (ルータが起動するとすぐに最大メトリックがアドバタイズされます)</p>

機能テンプレートを保存するには、[Save] をクリックします。

OSPF エリアの設定

Cisco SD-WAN デバイスの VPN 内の OSPF エリアを設定するには、[Area] > [Add New Area] を選択します。OSPF を機能させるには、エリア 0 を設定する必要があります。

表 13:

パラメータ名	説明
Area Number	<p>OSPF エリアの番号を入力します。</p> <p>範囲 : 32 ビットの数値</p>
Set the Area Type	OSPF エリアのタイプ ([Stub] または [NSSA]) を選択します。
No Summary	エリアに OSPF サマリールートを挿入しない場合は、[On] をクリックします。
Translate	<p>エリアタイプを NSSA として設定した場合は、ABR (エリア境界ルータ) である Cisco Catalyst SD-WAN デバイスがタイプ 7 LSA をタイプ 5 LSA に変換できるタイミングを選択します。</p> <ul style="list-style-type: none"> • [Always] : ルータは常にタイプ 7 LSA のトランスレータとして機能します。つまり、ABR であっても、他のルータがトランスレータになることはありません。2 つの ABR が常にトランスレータになるように設定されている場合、実際に変換されるのは 1 つの ABR だけです。 • [Candidate] : ルータは変換サービスを提供しますが、トランスレータになることを要求しません。 • [Never] : タイプ 7 LSA を変換しません。

新しいエリアを保存するには、[Add] をクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

OSPF エリアでのインターフェイスの設定

OSPF エリアのインターフェイスのプロパティを設定するには、[Area]>[Add New Area]>[Add Interface] の順に選択します。[Add Interface] ポップアップで、次のパラメータを設定します。

表 14:

パラメータ名	説明
Interface Name	インターフェイスの名前を ge slot/port または loopback number の形式で入力します。
Hello Interval	ルータが OSPF hello パケットを送信する頻度を指定します。 範囲：1 ～ 65535 秒、デフォルト：10 秒
Dead Interval	Cisco IOS XE Catalyst SD-WAN デバイスがネイバーから OSPF hello パケットを受信する頻度を指定します。パケットを受信しない場合、Cisco IOS XE Catalyst SD-WAN デバイスはネイバーがダウンしているから見なします。 範囲：1 ～ 65535 秒、デフォルト：40 秒（デフォルトの hello 間隔の 4 倍）
LSA Retransmission Interval	OSPF プロトコルが LSA をネイバーに再送信する頻度を指定します。 範囲：1 ～ 65535 秒、デフォルト：5 秒
Interface Cost	OSPF インターフェイスのコストを指定します。 範囲：1 ～ 65535

OSPF エリアでインターフェイスの詳細オプションを設定するには、[Add Interface] ポップアップで [Advanced Options] をクリックし、次のパラメータを設定します。

表 15:

パラメータ名	説明
Designated Router Priority	ルータが代表ルータ（DR）として選択される優先順位を設定します。最大の優先順位を持つルータが DR になります。優先順位が等しい場合、ルータ ID が最も高いノードが DR またはバックアップ DR になります。 範囲：0 ～ 255、デフォルト：1

パラメータ名	説明
OSPF Network Type	<p>インターフェイスを接続する OSPF ネットワークタイプを選択します。</p> <ul style="list-style-type: none"> • ブロードキャストネットワーク：WAN または同様のネットワーク。 • ポイントツーポイント ネットワーク：インターフェイスは単一のリモート OSPF ルータに接続します。 • 非ブロードキャスト：ポイントツーマルチポイント。 <p>デフォルト：ブロードキャスト</p>
Passive Interface	<p>[On] または [Off] をクリックして、OSPF インターフェイスをパッシブに設定するかどうかを指定します。パッシブインターフェイスはアドレスをアドバタイズしますが、OSPF プロトコルをアクティブに実行しません。デフォルト：[Off]</p>
Authentication	<p>インターフェイスで認証および認証キーを指定して、OSPF がルーティングアップデート情報を安全に交換できるようにします。</p>
• Authentication Type	<p>認証タイプを選択します。</p> <ul style="list-style-type: none"> • 簡易認証：パスワードはクリアテキストで送信されます。 • メッセージダイジェスト認証：MD5 アルゴリズムによりパスワードが生成されます。
• Authentication Key	<p>認証キーを入力します。プレーンテキスト認証は、エリア内のデバイスがより安全度が高い MD5 認証をサポートできない場合に使用されます。1 ～ 32 文字のキーを使用できます。</p>
• Message Digest	<p>Message Digest (MD5) を使用している場合は、キー ID と認証キーを指定します。</p>
• Message Digest Key ID	<p>メッセージダイジェスト (MD5 認証) のキー ID を入力します。1 ～ 32 文字の ID を使用できます。</p>
• Message Digest Key	<p>クリアテキストで、または AES 暗号化キーとして、MD5 認証キーを入力します。1 ～ 255 文字のキーを使用できます。</p>

インターフェイス設定を保存するには、[Save] をクリックします。

新しいエリアを保存するには、[Add] をクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

サマリー LSA のインターフェイス範囲の設定

OSPF エリアのインターフェイスのプロパティを設定するには、[Area]>[Add New Area]>[Add Range] の順に選択します。[Area Range] ポップアップで [Add Area Range] をクリックし、次のパラメータを設定します。

表 16:

パラメータ名	説明
Address	統合およびアドバタイズする IP アドレスの IP アドレスとサブネットマスクをプレフィックス/長さの形式で入力します。
Cost	タイプ 3 サマリー LSA の番号を指定します。OSPF は、SPF 計算時にこのメトリックを使用して、宛先への最短パスを決定します。 範囲 : 0 ~ 16777215
No Advertise	タイプ 3 サマリー LSA をアドバタイズしない場合は [On] を、アドバタイズする場合は [Off] をクリックします。

エリア範囲を保存するには、[Save] をクリックします。

新しいエリアを保存するには、[Add] をクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

他の OSPF プロパティの設定

他の OSPF プロパティを設定するには、[Advanced] をクリックし、次のプロパティを設定します。

表 17:

パラメータ名	説明
Reference Bandwidth	インターフェイスの OSPF 自動コスト計算の基準帯域幅を指定します。 範囲 : 1 ~ 4294967 Mbps、デフォルト : 100 Mbps
RFC 1538 Compatible	デフォルトでは、OSPF 計算は RFC 1583 に従って行われます。RFC 2328 に基づいてサマリールートのコストを計算するには、[Off] をクリックします。

パラメータ名	説明
Originate	<p>デフォルトの外部ルートを OSPF ルーティングドメインに生成するには、[On] をクリックします。</p> <ul style="list-style-type: none"> • [Always] : OSPF ルーティングドメインでデフォルトルートを常にアドバタイズするには、[On] をクリックします。 • [Default metric] : デフォルトルートの生成に使用されるメトリックを設定します。 範囲 : 0 - 16777214、デフォルト : 10 • [Metric type] : デフォルトルートを OSPF タイプ 1 外部ルートまたは OSPF タイプ 2 外部ルートとしてアドバタイズする場合に選択します。
SPF Calculation Delay	<p>トポロジに対する最初の変更を受信してから SPF 計算を実行するまでの時間を指定します。 範囲 : 0 - 600000 ミリ秒 (60 秒)、デフォルト : 200 ミリ秒</p>
Initial Hold Time	<p>連続する SPF 計算間の時間を指定します。 範囲 : 0 - 600000 ミリ秒 (60 秒)、デフォルト : 1000 ミリ秒</p>
Maximum Hold Time	<p>連続する SPF 計算間の最長時間を指定します。 範囲 : 0 - 600000、デフォルト : 10000 ミリ秒 (60 秒)</p>
Policy Name	<p>OSPF ネイバーからのルートに適用するローカライズされた制御ポリシーの名前を入力します。</p>

機能テンプレートを保存するには、[Save] をクリックします。

CLI を使用した OSPF の設定

ここでは、ユニキャストオーバーレイルーティングの基本的なサービス側 OSPF の設定方法について説明します。

基本的なサービス側 OSPF の設定

Cisco IOS XE Catalyst SD-WAN デバイスでルーティングを設定するには、VRF をプロビジョニングします (セグメンテーションが必要な場合)。各 VRF 内で、その VRF に参加するインターフェイスと、その VRF で動作するルーティングプロトコルを設定します。



- (注) CLI から OSPF を設定する場合は、OSPF プロセス ID (PID) と VRF ID が一致することを確認して、OSPF の OMP 再配布が指定された VRF で機能するようにします。プロセス ID は、インターフェイスが属する OSPF プロセスの ID です。プロセス ID はルータに対してローカルであり、ローカル OSPF プロセスの識別子として使用されます。

次に、Cisco IOS XE Catalyst SD-WAN デバイスでサービス側 OSPF を設定する例を示します。

```
config-transaction
router ospf 1 vrf1
  auto-cost reference-bandwidth 100
  max-metric router-lsa
  timers throttle spf 200 1000 10000
  router-id 172.16.255.15
  default-information originate
  distance ospf external 110
  distance ospf inter-area 110
  distance ospf intra-area 110
  redistribute connected subnets route-map route_map
exit
interface GigabitEthernet0/0/1
  no shutdown
  arp timeout 1200
  vrf forwarding 1
  ip address 10.1.100.14 255.255.255.0
  ip redirects
  ip mtu 1500
  ip ospf 1 area 0
  ip ospf network broadcast
  mtu 1500
  negotiation auto
exit
```

OMP の設定

OMP テンプレートを使用して、すべての Cisco IOS XE Catalyst SD-WAN デバイス、および Cisco Catalyst SD-WAN コントローラの OMP パラメータを設定します。

OMP はすべての Cisco IOS XE Catalyst SD-WAN デバイス、Cisco SD-WAN Manager NMS、および Cisco Catalyst SD-WAN コントローラではデフォルトで有効になっているため、OMP を明示的に有効にする必要はありません。Cisco SD-WAN オーバーレイネットワークが機能するには、OMP が動作可能である必要があります。OMP を無効にすると、オーバーレイネットワークが無効になります。



- (注)
- OMP のルートアドバタイズメントは、グローバルレベルまたは特定の VRF レベルで設定を適用することによって行われます。OMP のルートアドバタイズメントの詳細については、このトピックの「OMP アドバタイズメントの設定」セクションを参照してください。
 - Cisco IOS XE Catalyst SD-WAN デバイスは、VPN の代わりに VRF を使用します。ただし、Cisco SD-WAN Manager を介した Cisco IOS XE Catalyst SD-WAN デバイスの設定には引き続き次の手順が適用されます。設定を完了すると、VPN 設定が VRF 設定に自動的にマッピングされます。

OMP テンプレートの作成

1. Cisco SD-WAN Manager メニューから、[**Configuration**] > [**Templates**] の順に選択します。
2. [Device Template] をクリックします。



- (注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. [テンプレートの作成 (Create Template)] をクリックします。
4. [Create Template] ドロップダウンリストから、[From Feature Template] を選択します。
5. [Device Model] ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
6. OMP のカスタムテンプレートを作成するには、[Factory_Default_OMP_Template] を選択し、[Create Template] をクリックします。[OMP] テンプレートフォームが表示されます。フォームの上部にはテンプレートに名前を付けるためのフィールドがあり、下部には OMP パラメータを定義するためのフィールドがあります。さらにフィールドを表示するには、[Operation] またはプラス記号 (+) をクリックする必要がある場合があります。
7. [テンプレート名 (Template Name)] フィールドに、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。
8. [Template Description] フィールドに、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が [Default] に設定され (チェックマークで示される)、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、パラメータフィールドの左側にある [Scope] ドロップダウンリストをクリックし、次のいずれかを選択します。

表 18:

パラメータの範囲	範囲の説明
デバイス固有 (ホストのアイコンで示される)	<p>デバイス固有の値がパラメータに使用されます。デバイス固有のパラメータの場合、機能テンプレートに値を入力できません。Cisco SD-WAN デバイスをデバイステンプレートに添付するときに、値を入力します。</p> <p>[Device Specific] をクリックすると、[Enter Key] ボックスが表示されます。このボックスには、作成する CSV ファイル内のパラメータを識別する一意の文字列であるキーが表示されます。このファイルは、キーごとに 1 つの列を含む Excel スプレッドシートです。ヘッダ行にはキー名 (行ごとに 1 つのキー) が含まれます。その後の各行は、デバイスに対応し、そのデバイスのキーの値を定義します。Cisco SD-WAN デバイスをデバイステンプレートに添付するときに、この CSV ファイルをアップロードします。</p> <p>デフォルトキーを変更するには、新しい文字列を入力し、[Enter Key] ボックスの外にカーソルを移動します。</p> <p>デバイス固有のパラメータの例としては、システム IP アドレス、ホスト名、GPS ロケーション、サイト ID があります。</p>
グローバル (地球のアイコンで示される)	<p>パラメータの値を入力し、その値をすべてのデバイスに適用します。</p> <p>デバイスのグループにグローバルに適用できるパラメータの例としては、DNS サーバー、Syslog サーバー、インターフェイス MTU があります。</p>

基本的な OMP オプションの設定

基本的な OMP オプションを設定するには、[Basic Configuration] をクリックし、次のパラメータを設定します。パラメータはすべてオプションです。

表 19:

パラメータ名	説明
Graceful Restart for OMP	グレースフルリスタートを有効にするには、[Yes] が選択されていることを確認します。デフォルトでは、OMP のグレースフルリスタートは有効になっています。
Overlay AS Number	OMP がルータの BGP ネイバーにアドバタイズする BGP AS 番号を指定します。

パラメータ名	説明
Graceful Restart Timer	OMP 情報キャッシュをフラッシュして更新する頻度を指定します。タイマー値を 0 にすると、OMP グレースフルリスタートが無効になります。 範囲：0 ～ 604800 秒（168 時間、7 日）、デフォルト：43200 秒（12 時間）
Number of Paths Advertised Per Prefix	プレフィックスごとにアドバタイズされる等コストルートの最大数を指定します。がルートを Cisco Catalyst SD-WAN コントローラにアドバタイズし、コントローラが学習したルートを再配布し、各ルート TLOC タプルをアドバタイズします。Cisco IOS XE Catalyst SD-WAN デバイスは最大 4 つの TLOC を持つことができ、デフォルトでは各ルート TLOC タプルを Cisco Catalyst SD-WAN コントローラにアドバタイズします。ローカルサイトに Cisco IOS XE Catalyst SD-WAN デバイスが 2 つある場合、Cisco Catalyst SD-WAN コントローラは同じルートに対して 8 つのルート TLOC タプルを学習する可能性があります。設定された制限がルート TLOC タプルの数よりも小さい場合は、最適なルートがアドバタイズされます。 範囲：1 ～ 16、デフォルト：4
ECMP Limit	Cisco IOS XE Catalyst SD-WAN デバイスのローカルルートテーブルにインストールできる Cisco Catalyst SD-WAN コントローラから受信する OMP パスの最大数を指定します。デフォルトでは、Cisco IOS XE Catalyst SD-WAN デバイスはルートテーブルに最大 4 つの一意の OMP パスをインストールします。 範囲：1 ～ 16、デフォルト：4
Send Backup Paths (Cisco Catalyst SD-WAN コントローラのみ)	OMP が Cisco IOS XE Catalyst SD-WAN デバイスにバックアップルートをアドバタイズするようにするには、[On] をクリックします。デフォルトでは、OMP は最適なルートのみをアドバタイズします。バックアップパスを送信するように設定すると、OMP は最適なルートに加えて、最初の最適ではないルートもアドバタイズします。
Shutdown	Cisco SD-WAN オーバーレイネットワークを有効にするために [No] が選択されていることを確認します。[Yes] をクリックして OMP を無効にし、Cisco SD-WAN オーバーレイネットワークを無効にします。OMP はデフォルトで有効になっています。
Discard Rejected (Cisco Catalyst SD-WAN コントローラのみ)	ポリシーに基づいて拒否されたルートを OMP で破棄するには、[Yes] をクリックします。デフォルトでは、拒否されたルートは破棄されません。

機能テンプレートを保存するには、[Save] をクリックします。

OMP タイマーの設定

OMP タイマーを設定するには、[Timers] をクリックし、次のパラメータを設定します。

表 20:

パラメータ名	説明
Advertisement Interval	OMP 更新パケット間の時間を設定します。 範囲：0 ～ 65535 秒、デフォルト：1 秒
Hold Time	ピアへの OMP 接続を閉じるまでの待機時間を指定します。ピアがホールド時間内に3回連続してキープアライブメッセージを受信しない場合、ピアへの OMP 接続は閉じられます。 範囲：0 ～ 65535 秒、デフォルト：60 秒 Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、デフォルトの保留時間は 300 秒です。
EOR Timer	OMPセッションがダウンしてから復帰し、End-of-RIB (EOR) マーカーを送信するまでの待機時間を指定します。このマーカーが送信された後、OMPセッションの復帰後に更新されなかったルートは、古いルートと見なされ、ルートテーブルから削除されます。 範囲：1 ～ 3600 秒 (1 時間) 、デフォルト：300 秒 (5 分)

機能テンプレートを保存するには、[Save] をクリックします。

OMP アドバタイズメントの設定



- (注) OMP のルートアドバタイズメントは、グローバルレベルまたは特定の VRF レベルで設定を適用することによって行われます。

Cisco IOS XE Catalyst SD-WAN デバイスによってローカルに学習されたルートを OMP にアドバタイズするには、[Advertise] をクリックし、次のパラメータを設定します。

表 21:

パラメータ名	説明
Advertise	<p>ローカルで学習したルートを Cisco IOS XE Catalyst SD-WAN デバイスが OMP にアドバタイズするのを有効にする場合は [On] をクリックし、無効にする場合は [Off] をクリックします。</p> <ul style="list-style-type: none"> • [BGP] : BGP ルートを OMP にアドバタイズするには、[On] をクリックします。デフォルトでは、BGP ルートは OMP にアドバタイズされません。 • [Connected] : OMP への接続ルートのアドバタイズを無効にするには、[Off] をクリックします。デフォルトでは、接続ルートは OMP にアドバタイズされます。 • [OSPF] : [On] をクリックし、OMP に外部 OSPF ルートをアドバタイズするために表示される [External] フィールドでもう一度 [On] をクリックします。エリア間およびエリア内の OSPF ルートは常に OMP にアドバタイズされます。デフォルトでは、外部 OSPF ルートは OMP にアドバタイズされません。 • [Static] : OMP へのスタティックルートのアドバタイズを無効にするには、[Off] をクリックします。デフォルトでは、スタティックルートは OMP にアドバタイズされます。 <p>OMP への VPN ごとのルートアドバタイズメントを設定するには、VPN 機能テンプレートを使用します。</p>

[Save] をクリックします。

CLI を使用した OMP の設定

デフォルトでは、OMP はすべての Cisco IOS XE Catalyst SD-WAN デバイスおよび Cisco Catalyst SD-WAN コントローラで有効になっています。Cisco SD-WAN オーバーレイネットワークが機能するには、OMP が動作している必要があります。OMP を無効にすると、オーバーレイネットワークが無効になります。

Cisco SD-WAN の OMP サポートには、次のものが含まれます。

- IPv6 サービスルート
- IPv4 および IPv6 プロトコル。デフォルトでは両方ともオン
- BGP、EIGRP、OSPF、接続ルート、スタティックルートなどへの OMP ルートアドバタイズメント

OMP グレースフルリスタートの設定

OMP グレースフルリスタートは、Cisco Catalyst SD-WAN コントローラおよび Cisco SD-WAN デバイスで、デフォルトで有効になっています。OMP グレースフルリスタートには、キャッシュされ、アドバタイズされたルートを保持する期間を OMP ピアに伝えるタイマーがあります。このタイマーが期限切れになると、キャッシュされたルートは無効と見なされ、OMP ピアはルートテーブルからそれらのルートをフラッシュします。

デフォルトのタイマーは 43,200 秒（12 時間）で、タイマーの範囲は 1 ～ 604,800 秒（7 日）です。デフォルトのタイマー値を変更するには、次の手順を実行します。

```
Device# config-transaction
Device(config)# sdwan
Device(config-omp)# timers graceful-restart-timer seconds
```

OMP グレースフルリスタートを無効にするには、次の手順を実行します。

```
Device(config-omp)# no graceful-restart
```

グレースフルリスタートタイマーは、各 OMP ピアで個別に設定されます。つまり、Cisco IOS XE Catalyst SD-WAN デバイスと Cisco Catalyst SD-WAN コントローラで個別に設定されます。この点を説明するために、300 秒（5 分）のグレースフルリスタート時間を使用する Cisco SD-WAN コントローラ、および 600 秒（10 分）のタイマーが設定された Cisco IOS XE Catalyst SD-WAN デバイスを考えてみましょう。Cisco Catalyst SD-WAN コントローラは、そのデバイスから学習した OMP ルートを 10 分間保持します。この時間は、デバイスに設定され、OMP セッションのセットアップ中にデバイスから Cisco Catalyst SD-WAN コントローラに送信されたグレースフルリスタートタイマー値です。Cisco IOS XE Catalyst SD-WAN デバイスは、Cisco SD-WAN コントローラから学習したルートを 5 分間保持します。この時間は、Cisco Catalyst SD-WAN コントローラで使用されるデフォルトのグレースフルリスタート時間値であり、OMP セッションのセットアップ中にコントローラからデバイスに送信された値でもあります。

Cisco Catalyst SD-WAN コントローラがダウンしており、Cisco IOS XE Catalyst SD-WAN デバイスがキャッシュされた OMP 情報を使用している場合、デバイスをリブートすると、キャッシュされた情報が失われるため、Cisco Catalyst SD-WAN コントローラへのコントロールプレーン接続を確立できるまでデータトラフィックを転送できません。

OMP へのルートのアドバタイズ

表 22: 機能の履歴

機能名	リリース情報	説明
OMP ルート集約	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a Cisco vManage リリース 20.3.1	これは、ブラックホールルーティングを回避するためにルート再配布用に設定されたルートに対してのみ OMP ルート集約が実行される拡張機能です。この拡張機能は、再配布が要求された場合にのみ、OSPF プロトコル、接続プロトコル、静的プロトコル、BGP プロトコル、およびその他のプロトコルに適用されます。

デフォルトでは、Cisco IOS XE Catalyst SD-WAN デバイスは接続ルート、スタティックルート、OSPF エリア間ルート、OSPF エリア内ルート、OSPFv3 IPv6 エリア内ルートをアドバタイズし、OSPF IPv6 エリア間ルートがデバイスのドメインを担当する Cisco Catalyst SD-WAN コントローラの OMP にアドバタイズされます。

デバイスにこれらのルートを OMP にアドバタイズさせ、Cisco Catalyst SD-WAN コントローラにデバイスのドメインを担当させるには、`advertise` コマンドを使用します。



- (注) OMP でのルートアドバタイズメントの設定は、グローバルレベルまたは特定の VRF レベルで設定を適用することによって行われます。

次の例では、すべての VRF の BGP ルートの OMP アドバタイズメントを有効にします。すべての VRF に対する OMP プロトコルのプロトコルルートアドバタイズメントを有効にするには、グローバルレベルで設定を追加します。

```
Device(config)# sdwan
Device(config-sdwan)# omp
Device(config-omp)# address-family ipv4
Device(config-ipv4)# advertise bgp
```

少数の VRF のプロトコルルートアドバタイズメントを有効にするには、`no advertise bgp` コマンドを使用してグローバルレベルの設定を削除し、VRF レベルごとの設定を追加します。

```
Device(config)# sdwan
Device(config-sdwan)# omp
Device(config-omp)# address-family ipv4
Device(config-ipv4)# no advertise bgp
Device(config-ipv4)# address-family ipv4 vrf 2
Device(config-vrf-2)# advertise bgp
Device(config-vrf-2)# address-family ipv4 vrf 4
Device(config-vrf-4)# advertise bgp
Device(config-vrf-4)# commit
```



- (注) すべてまたは少数の VRF に対して特定のプロトコルルートアドバタイズメントを無効にするには、その設定がグローバルレベルにも、VRF レベルにも存在しないことを確認します。

デバイスに設定されているすべての VRF に対して、そのデバイスが OMP にアドバタイズするルートを設定するには、次の手順を実行します。

```
config-transaction
sdwan
  omp
  address-family ipv4
  advertise ospf external
  advertise bgp
  advertise eigrp
  advertise connected
  advertise static
  exit
address-family ipv6
  advertise ospf external
  advertise bgp
```

```

advertise eigrp
advertise connected
advertise static
exit

```

OSPF の場合、ルートタイプは `external` にできます。

`bgp`、`connected`、`ospf`、および `static` オプションは、そのタイプのすべての学習済みルートまたは設定済みルートを OMP にアドバタイズします。プロトコルのすべてのルートをアドバタイズする代わりに、特定のルートをアドバタイズするには、`network` オプションを使用して、アドバタイズするルートのプレフィックスを指定します。

デバイスの特定の VRF に対して、そのデバイスが OMP にアドバタイズするルートを設定するには、次の手順を実行します。

```

config-transaction
sdwan
omp
  address-family ipv4 vrf 1
  advertise aggregate prefix 10.0.0.0/8
  advertise ospf external
  advertise bgp
  advertise eigrp
  advertise connected
  advertise static
  exit
  address-family ipv6 vrf 1
  advertise aggregate 2001:DB8::/32
  advertise ospf external
  advertise bgp
  advertise eigrp
  advertise connected
  advertise static
  exit

```

個々の VRF の場合、指定したプレフィックスからのルートは、`advertise protocol config` コマンドを使用して OMP にアドバタイズした後に集約できます。デフォルトでは、集約されたプレフィックスとすべての個々のプレフィックスがアドバタイズされます。集約されたプレフィックスだけをアドバタイズするには、次に示すように、`aggregate-only` オプションを含めます。

```

config-transaction
sdwan
omp
  address-family ipv4 vrf 1
  advertise aggregate 10.0.0.0/8 aggregate-only
  exit

```



(注) OMP のルートアドバタイズメントは、グローバルレベルで設定を適用するか、特定の VRF に設定を適用することによって行われます。特定の VRF 設定が、OMP のグローバル VRF 設定をオーバーライドすることはありません。

BGP は、ルートを OMP にアドバタイズするときに、各プレフィックスのメトリックをアドバタイズします。BGP は、プレフィックスの AS パスもアドバタイズできます。

```
config-transaction
router bgp 200
address-family ipv4 vrf 11
neighbor 10.20.1.0 remote-as 200
propagate-aspath
exit
```

AS パス情報を伝達するように BGP を設定すると、デバイスは BGP を実行している Cisco IOS XE Catalyst SD-WAN デバイス（サービス側ネットワーク内）の背後にあるデバイスに AS パス情報を送信し、それらのルータから AS パス情報を受信します。BGP ルートを OMP に再配布する場合、AS パス情報はアドバタイズされた BGP ルートに含まれます。オーバーレイネットワーク内のすべてのデバイスではなく、一部のデバイスで BGP AS パスの伝達を設定した場合、設定されていないデバイスは AS パス情報を受信しますが、ローカルサービス側ネットワークの BGP ルータには転送しません。AS パス情報を伝達することで、BGP ルーティングループを回避できます。

オーバーレイ接続とアンダーレイ接続の両方があるネットワークでは（たとえば、デバイスが Cisco SD-WAN オーバーレイネットワークと MPLS アンダーレイネットワークの両方で相互接続されている場合）、AS 番号として OMP 自体に割り当てることができます。BGP を実行しているデバイスの場合、このオーバーレイ AS 番号は BGP ルートアップデートの AS パスに含まれます。オーバーレイ AS を設定するには、次の手順を実行します。

```
config-transaction
sdwan
omp
overlay-as 55
exit
```

AS 番号は、2 バイトの ASDOT 表記（1 ～ 65535）または 4 バイトの ASDOT 表記（1.0 ～ 65535.65535）で指定できます。ベストプラクティスとして、オーバーレイ AS 番号は、オーバーレイネットワークとアンダーレイネットワークの両方で一意の AS 番号にすることを推奨します。その場合は、ネットワークの他の場所で使用されていない AS 番号を選択します。

オーバーレイネットワーク内の複数のデバイスに同じオーバーレイ AS 番号を設定すると、これらのデバイスはすべて同じ AS の一部と見なされるため、オーバーレイ AS 番号を含むルートは転送されません。このメカニズムは、ネットワーク内の BGP ルーティングループを防止するための追加技術です。

アドバタイズされるルートの数の設定

Cisco IOS XE Catalyst SD-WAN デバイスには最大 8 つの WAN インターフェイスを設定でき、各 WAN インターフェイスには異なる TLOC があります（WAN インターフェイスは、トンネルインターフェイスとして設定されている VPN0（またはトランスポート VRF）内の任意のインターフェイスです。物理インターフェイスとループバックインターフェイスの両方をトンネルインターフェイスとして設定できます）。つまり、各ルータに最大 8 つの TLOC を設定できます。デバイスは各ルート TLOC タプルを Cisco Catalyst SD-WAN コントローラにアドバタイズします。

Cisco Catalyst SD-WAN コントローラは、Cisco IOS XE Catalyst SD-WAN デバイスから学習したルートを再配布し、各ルート TLOC タプルをアドバタイズします。たとえば、ローカルサイト

に2つのデバイスがある場合、Cisco Catalyst SD-WAN コントローラは同じルートの8つのルート TLOC タプルを学習する可能性があります。

デフォルトでは、Cisco IOS XE Catalyst SD-WAN デバイスと Cisco Catalyst SD-WAN コントローラは同じルートに対して最大4つの等コストルート TLOC タプルをアドバタイズします。同じルートについて1～16のルート TLOC タプルをアドバタイズするようにデバイスを設定できます。

```
Device(config-omp)# send-path-limit 14
```

Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.8.x 以降では、階層型 SD-WAN 環境で動作する Cisco SD-WAN コントローラを設定して、同じルートについて1～32のルート TLOC タプルをエッジデバイスにアドバタイズできます。

Cisco SD-WAN コントローラリリース 20.9.x 以降では、任意の Cisco SD-WAN 環境の Cisco SD-WAN コントローラを設定して、同じルートについて1～32のルート TLOC タプルをエッジデバイスにアドバタイズできます。

制限がルート TLOC タプルの数よりも小さい場合、Cisco IOS XE Catalyst SD-WAN デバイスまたは Cisco Catalyst SD-WAN コントローラは最適なルートをアドバタイズします。

インストール済み OMP パスの数の設定

Cisco IOS XE Catalyst SD-WAN デバイスは、Cisco Catalyst SD-WAN コントローラから受信した OMP パスをローカルルートテーブルにインストールします。デフォルトでは、Cisco IOS XE Catalyst SD-WAN デバイスはルートテーブルに最大4つの一意の OMP パスをインストールします。次の番号を変更できます。

```
Device(config-omp)# ecmp-limit 2
```

インストールされる OMP パスの最大数は1～16です。

OMP ホールド時間の設定

OMP ホールド時間により、ピアへの OMP 接続を閉じるまでの待機時間が決まります。ピアがホールド時間内に3回連続してキープアライブメッセージを受信しない場合、ピアへの OMP 接続は閉じられます。デフォルトの OMP ホールド時間は60秒ですが、最大65,535秒に設定できます。

Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、デフォルトの保留時間は300秒です。

OMP ホールド時間間隔を変更するには、次の手順を実行します。

```
Device(config-omp)# timers holdtime 75
```

ホールド時間は0～65535秒の範囲で指定できます。

キープアライブタイマーはホールド時間の3分の1であり、設定できません。

ローカルデバイスとピアのホールド時間間隔が異なる場合は、大きい方の値が使用されます。

ホールド時間を0に設定すると、ローカルデバイスとピアのキープアライブタイマーとホールドタイマーは0に設定されます。

ホールド時間は、トランスポート VRF の WAN トンネルインターフェイスで設定された `hello tolerance` 間隔の2倍以上である必要があります。hello tolerance インターフェイスを設定するには、`hello-tolerance` コマンドを使用します。

OMP 更新アドバタイズメント間隔の設定

デフォルトでは、OMP は更新パケットを 1 秒に 1 回送信します。この間隔を変更するには、次の手順を実行します。

```
Device(config-omp)# timers advertisement-interval 5000
```

間隔は 0 ～ 65535 秒の範囲で指定できます。

End-of-RIB タイマーの設定

OMP セッションがダウンし再びアップした後、300 秒（5 分）後に End-of-RIB（EOR）マーカが送信されます。このマーカが送信された後、OMP セッションの復帰後に更新されなかったルートは、古いルートと見なされ、ルートテーブルから削除されます。EOR タイマーを変更するには、次の手順を実行します。

```
Device(config-omp)# timers eor-timer 300
```

時間の範囲は 1 ～ 3600 秒（1 時間）です。

複数の BGP コミュニティの OMP タグへのマッピング

表 23: 機能の履歴

機能名	リリース 情報	説明
複数の BGP コミュニティの OMP タグへのマッピング	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	この機能を使用すると、Cisco Catalyst SD-WAN コントローラおよび Cisco IOS XE Catalyst SD-WAN デバイスの OMP ルートに関する情報を表示できます。OMP ルートは、デバイスがローカルネットワーク上で実行されているルーティングプロトコルから学習した情報を伝送します。情報には、BGP および OSPF から学習したルート、直接ルート、接続ルート、およびスタティックルートが含まれます。

`show sdwan omp routes` コマンドの詳細については、[show sdwan mp routes](#) を参照してください。

OSPFv3 の設定

Cisco SD-WAN Manager テンプレートを使用して OSPFv3 ルーティングプロトコルを設定するには、次の手順を実行します。

1. OSPFv3 機能テンプレートを作成して、OSPFv3 パラメータを設定します。

- VPN 機能テンプレートを作成して、サービス側ルーティング（VPN 0 または VPN 512 以外の VPN）の VPN パラメータを設定します。
- デバイステンプレートを作成し、正しいデバイスにテンプレートを適用します。

OSPFv3 テンプレートの作成

- Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
- [Feature Templates]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Feature Templates]** のタイトルは **[Feature]** です。

- [Add Template]** をクリックし、リストからデバイスを選択します。
- [Other Templates]** セクションで、**[OSPFv3]** を選択し、テンプレートの名前と説明を入力します。
- [IPv4]** または **[IPv6]** を選択します。

基本設定

[Basic Configuration] をクリックして、テンプレートの基本的な詳細を設定します。

パラメータ名	説明
Router ID	ルータの IP アドレスを入力します。例： 10.20.1.1
Distance	ルータを設置するアドミニストレーティブディスタンスを入力します。
External Routes	他のドメインから学習したルートの OSPFv3 ルートアドミニストレーティブディスタンスを指定します。 範囲：0 - 255 デフォルト：110
Inter-Area Routes	あるエリアから別のエリアに到達するルートの OSPFv3 ルートアドミニストレーティブディスタンスとして適用する値を入力します。 範囲：0 - 255 デフォルト：110

パラメータ名	説明
Intra-Area Routes	直接接続されたエリアからのルートの OSPF ルートアドミニストレーティブディスタンスとして適用する値を入力します。 範囲：0 ～ 255 デフォルト：110
Timers Throttle SPF	スロットリングの最短パス優先（SPF）タイマーを指定します。
Table Map	ルートマップを指定して、ルート属性を変更するか、または OSPFv3 がグローバルまたは VRF ルーティングテーブルにインストールするルートをフィルタリングします。
Filter	テーブルマップに指定されたルートマップで受け入れられないルートをフィルタリングするには、[On] をクリックします。

OSPFv3 に対するルートの再配布の設定

他のプロトコルから学習したルートを Cisco IOS XE Catalyst SD-WAN デバイス上の OSPF に再配布するには、[Redistribute] > [Add New Redistribute] を選択し、次のパラメータを設定します。

表 24 : Redistribution Parameters

パラメータ名	値	説明
Mark as Optional Row		この設定をデバイス固有としてマークするには、[Optional] をクリックします。デバイスにこの設定を含めるには、デバイステンプレートをデバイスに添付するときに要求された変数値を入力するか、テンプレート変数スプレッドシートを作成して変数を適用します。

パラメータ名	値	説明
Protocol *		すべての OSPFv3 セッションについて、OSPFv3 にルートを再配布するプロトコルを選択します。
	bgp	BGP ルートを OSPFv3 に再配布します。
	connected	接続ルートを OSPFv3 に再配布します。
	nat-route	NAT ルートを OSPFv3 に再配布します。
	omp	OMP ルートを OSPFv3 に再配布します。
	eigrp	EIGRP ルートを OSPFv3 に再配布します。
	lisp	LISP ルートを OSPFv3 に再配布します。
	isis	IS-IS ルートを OSPFv3 に再配布します。
	ospf	OSPF ルートを OSPFv3 に再配布します。 (注) OSPF の再配布は、IPv4 アドレスファミリーでのみサポートされます。
	static	スタティックルートを OSPFv3 に再配布します。
Route Policy *		再配布されるルートに適用するルートポリシーの名前を入力します。

[Save] をクリックします。

最大メトリックをアドバタイズする OSPFv3 の設定

他のデバイスが Cisco IOS XE Catalyst SD-WAN デバイスを最短パス優先 (SPF) 計算で中間ホップとして優先しないように、OSPFv3 が最大メトリックをアドバタイズするように設定するには、[Maximum Metric (Router LSA)] > [Add New Router LSA] を選択し、次のパラメータを設定します。

表 25:

パラメータ名	説明
Type	タイプを選択します。 <ul style="list-style-type: none"> • [Administrative] : オペレータの介入によって最大メトリックがただちに有効になるようにします。 • [On-Startup] : 起動後に、指定した時間の最大メトリックをアドバタイズします。

パラメータ名	説明
Advertisement Time	[On-Startup] を選択した場合は、ルータの起動後に最大メトリックをアドバタイズする秒数を指定します。 範囲：0、5 ～ 86400 秒、デフォルト：0 秒（ルータが起動するとすぐに最大メトリックがアドバタイズされます）

[Save] をクリックします。

OSPFv3 エリアの設定

Cisco IOS XE Catalyst SD-WAN デバイスの VPN 内の OSPFv3 エリアを設定するには、[Area] > [Add New Area] を選択します。OSPFv3 を機能させるには、エリア 0 を設定する必要があります。

表 26:

パラメータ名	説明
Area Number	OSPFv3 エリアの番号を入力します。 範囲：32 ビットの数値
Set the Area Type	OSPFv3 エリアのタイプを選択します。次のオプションがあります。 <ul style="list-style-type: none"> • normal • [stub]：外部ルートなし • [nssa]：not-so-stubby area（外部ルートを許可）
No Summary	エリアタイプを stub または NSSA として設定した場合は、[On] をクリックして、OSPFv3 サマリールートがエリアに挿入されないようにします。
Translate	エリアタイプを NSSA として設定した場合は、エリア境界ルータ（ABR）である デバイスがタイプ 7 LSA をタイプ 5 LSA に変換できるタイミンングを選択します。 <ul style="list-style-type: none"> • [Always]：ルータは常にタイプ 7 LSA のトランスレータとして機能します。つまり、ABR であっても、他のルータがトランスレータになることはありません。2つの ABR が常にトランスレータになるように設定されている場合、実際に変換されるのは 1つの ABR だけです。 • [Candidate]：ルータは変換サービスを提供しますが、トランスレータになることを要求しません。 • [Never]：ルータはタイプ 7 LSA の NSSA トランスレータにはなりません。

OSPFv3 エリアのインターフェイスのプロパティを設定するには、[Area]>[Add New Area]>[Add Interface] の順に選択します。[Add Interface] ポップアップで、次のパラメータを設定します。

パラメータ名	説明
Interface Name	インターフェイスの名前を ge slot/port または loopback number の形式で入力します。
Hello Interval	ルータが OSPF hello パケットを送信する頻度を指定します。 範囲：1 ～ 65535 秒、デフォルト：10 秒
Dead Interval	Cisco IOS XE Catalyst SD-WAN デバイスがネイバーから OSPF hello パケットを受信する時間間隔を指定します。パケットを受信しない場合、Cisco IOS XE Catalyst SD-WAN デバイスはネイバーがダウンしていると見なします。 範囲：1 ～ 65535 秒、デフォルト：40 秒（デフォルトの hello 間隔の 4 倍）
LSA Retransmission Interval	OSPF プロトコルが LSA をネイバーに再送信する頻度を指定します。 範囲：1 ～ 65535 秒、デフォルト：5 秒
Interface Cost	OSPF インターフェイスのコストを指定します。 範囲：1 ～ 65535

OSPF エリアのインターフェイスのプロパティを設定するには、[Area]>[Add New Area]>[Add Range] の順に選択します。[Area Range] ポップアップで [Add Area Range] をクリックし、次のパラメータを設定します。

パラメータ名	説明
Address	統合およびアドバタイズする IP または IPv6 アドレスの IP アドレスとプレフィックス長をプレフィックス/長さの形式で 2 回入力します。アドレスタイプは、アドレスファミリーによって異なります。
Cost	タイプ 3 サマリー LSA の番号を指定します。OSPFv3 は、SPF 計算時にこのメトリックを使用して、宛先への最短パスを決定します。 範囲：0 ～ 16777215
No Advertise	タイプ 3 サマリー LSA をアドバタイズしない場合は [On] を、アドバタイズする場合は [Off] をクリックします。

インターフェイス設定を保存するには、[Save] をクリックします。

新しいエリアを保存するには、[Add] をクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

OSPFv3 詳細プロパティの設定

他の OSPFv3 プロパティを設定するには、[Advanced] をクリックします。

表 27:

パラメータ名	説明
Reference Bandwidth (Mbps)	インターフェイスの OSPFv3 自動コスト計算の基準帯域幅を指定します。 範囲：1 ～ 4294967 Mbps、デフォルト：100 Mbps
Originate	デフォルトの外部ルートを OSPF ルーティングドメインに生成するには、[On] をクリックします。 <ul style="list-style-type: none"> • [Always]：OSPF ルーティングドメインでデフォルトルートを作成するには、[On] をクリックします。 • [Default metric]：デフォルトルートの生成に使用されるメトリックを設定します。 範囲：0 ～ 16777214、デフォルト：10 • [Metric type]：デフォルトルートをアドバタイズするメトリックタイプ、OSPF タイプ 1 外部ルートまたは OSPF タイプ 2 外部ルートを選択します。
SPF Calculation Delay (ミリ秒)	トポロジに対する最初の変更を受信してから SPF 計算を実行するまでの時間を指定します。 範囲：0 ～ 600000 ミリ秒 (60 秒)、デフォルト：200 ミリ秒
Initial Hold Time (ミリ秒)	連続する SPF 計算間の時間を指定します。 範囲：0 ～ 600000 ミリ秒 (60 秒)、デフォルト：1000 ミリ秒
Maximum Hold Time (ミリ秒)	連続する SPF 計算間の最長時間を指定します。 範囲：0 ～ 600000、デフォルト：10000 ミリ秒 (60 秒)
Policy Name	OSPFv3 によってグローバルルート情報ベース (RIB) にインストールされたルートに適用するローカライズされた制御ポリシーの名前を入力します。
Filter	ポリシーに一致しない OSPFv3 ルートがグローバル RIB にインストールされないようにフィルタリングします。

機能テンプレートを保存するには、[Save] をクリックします。

CLI を使用した OSPFv3 の設定

IPv4 および IPv6 アドレスファミリの Cisco IOS XE SD-WAN デバイスで OSPFv3 を設定するには、次の手順を実行します。

```

config-transaction
router ospfv3 <vpn-id>
!
address-family ipv4 unicast vrf <vpn-id>
router-id <ipv4-address-format>
auto-cost reference-bandwidth <1-4294967>
default-information originate [always] [route-map <route-map-name>] [metric <1-16777214>]
                                     [metric-type {1|2}]
distance <1-254>
distance ospf {external <1-254> | intra-area <1-254> | inter-area <1-254>}
timers throttle spf <1-600000> <1-600000> <1-600000>
redistribute {bgp <1-4294967295>| connected | eigrp <vpn-id>| isis <vpn-id>| lisp |
nat-route | omp |
                                     ospf <vpn-id> | static}
                                     [route-map <route-map-name>]
max-metric router-lsa [on-startup <5-86400>]
table-map <route-map-name> [filter]
area <1-4294967295> stub [no-summary]
area <1-4294967295> nssa [no-summary] [translate type7 always]
area <1-4294967295> range <ipv4-prefix-address> <ipv4-prefix-mask> ! 192.168.0.1
255.255.255.0
                                     [not-advertise | advertise] [cost
<1-16777214>]16777214
exit-address-family

address-family ipv6 unicast vrf <vpn-id>
router-id <ipv4-address-format>
auto-cost reference-bandwidth <1-4294967>
default-information originate [always] [route-map <route-map-name>] [metric <1-16777214>]
                                     [metric-type {1|2}]
distance <1-254>
distance ospf {external <1-254> | intra-area <1-254> | inter-area <1-254>}
timers throttle spf <1-600000> <1-600000> <1-600000>
redistribute {bgp <1-4294967295> | connected | eigrp <vpn-id>| isis <vpn-id>| lisp |
omp |
                                     static}
                                     [route-map <route-map-name>]
max-metric router-lsa [on-startup <5-86400>]
table-map <route-map-name> [filter]
area <1-4294967295> stub [no-summary]
area <1-4294967295> nssa [no-summary] [translate type7 always]
area <1-4294967295> range <ipv6-prefix>
                                     ! 2001:DB8::/48
                                     [not-advertise | advertise] [cost
<1-16777214>]
exit-address-family

```

OSPFv3 テーブルマップの設定

```

router ospfv3 1
!
address-family ipv4 unicast vrf 1
redistribute omp route-map match-omp-tag

```

```
    table-map set-omp-tag
  exit-address-family
  !
  address-family ipv6 unicast vrf 1
    table-map set-omp-tag
    redistribute omp route-map match-omp-tag
  exit-address-family
  !
  route-map set-omp-tag permit 20
    set omp-tag 2000
  route-map match-omp-tag permit 10
    match omp-tag 1000
    set metric 20
  route-map match-omp-tag permit 20
    match omp-tag 2000
    set metric 30
  route-map match-omp-tag deny 30
```

EIGRP の設定

Cisco SD-WAN Manager テンプレートを使用して EIGRP ルーティングプロトコルを設定するには、次の手順を実行します。

1. EIGRP 機能テンプレートを作成して、EIGRP パラメータを設定します。
2. VPN 機能テンプレートを作成して、サービス側ルーティング (VPN 0 または VPN 512 以外の VPN) の VPN パラメータを設定します。
3. デバイステンプレートを作成し、正しいデバイスにテンプレートを適用します。

EIGRP テンプレートの作成

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. **[Feature Templates]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Feature Templates]** のタイトルは **[Feature]** です。

3. **[Add Template]** をクリックし、リストからデバイスを選択します。
4. **[Other Templates]** セクションで、**[EIGRP]** を選択し、テンプレートの名前と説明を入力します。

基本設定

[Basic Configuration] をクリックして、テンプレートのローカル自律システム (AS) 番号を設定します。

パラメータ名	説明
Autonomous System ID *	ローカル AS 番号を入力します。 <ul style="list-style-type: none"> • 範囲：1 ~ 65,535 • デフォルト：なし

IPv4 ユニキャストアドレスファミリの設定

1つのプロトコル（ルーティングドメイン）から EIGRP ルーティングドメインにルートを再配布するには、[New Redistribute] をクリックし、次のパラメータ値を入力します。

表 28: *Redistribution Parameters*

パラメータ名	値	説明
Mark as Optional Row		この設定をデバイス固有としてマークするには、[Optional] をクリックします。デバイスにこの設定を含めるには、デバイステンプレートをデバイスに添付するときに要求された変数値を入力するか、テンプレート変数スプレッドシートを作成して変数を適用します。
Protocol *		すべての EIGRP セッションに対して、EIGRP にルートを再配布するプロトコルを選択します。
	bgp	ボーダーゲートウェイプロトコル (BGP) ルートを EIGRP に再配布します。
	connected	接続ルートを EIGRP に再配布します。
	nat-route	ネットワークアドレス変換 (NAT) ルートを EIGRP に再配布します。
	omp	オーバーレイ管理プロトコル (OMP) ルートを EIGRP に再配布します。
	ospf	Open Shortest Path First (OSPF) ルートを EIGRP に再配布します。 (注) Cisco IOS XE Catalyst SD-WAN リリース 16.12.1b 以降の CLI アドオン機能テンプレートを使用して、再配布のメトリック値を設定できます。次のコマンドを使用します。 <code>redistribute ospf 1 metric 1000000 1 1 1 1500</code> 詳細については、「 CLI Add-on Feature Templates 」を参照してください。
	static	スタティックルートを EIGRP に再配布します。

パラメータ名	値	説明
Route Policy *		再配布されるルートに適用するルートポリシーの名前を入力します。
[Add] をクリックして再配布情報を保存します。		

プレフィックスを EIGRP ルーティングドメインにアダタイズするには、[Network] をクリックし、[New Network] をクリックして、次のパラメータ値を入力します。

表 29: *Configure Network*

パラメータ名	説明
Mark as Optional Row	この設定をデバイス固有としてマークするには、[Optional] をクリックします。デバイスにこの設定を含めるには、デバイステンプレートをデバイスに添付するときに要求された変数値を入力するか、テンプレート変数スプレッドシートを作成して変数を適用します。「Create a Template Variables Spreadsheet」を参照してください。
Network Prefix *	EIGRP がアダタイズするネットワークプレフィックスを、プレフィックス/マスクの形式で入力します。
[Add] をクリックして、ネットワークプレフィックスを保存します。	

詳細なパラメータの設定

EIGRP の詳細なパラメータを設定するには、[Advanced] をクリックし、次のパラメータ値を設定します。

表 30: *Advanced Parameters*

パラメータ名	説明
Hold Time seconds	EIGRP がネイバーをダウンしていると見なす間隔を設定します。ローカルルータは、そのピアへの EIGRP セッションを終了します。この時間はグローバルホールド時間として機能します。 <ul style="list-style-type: none"> • 範囲 : 0 ~ 65,535 • デフォルト : 15 秒

パラメータ名	説明
[Hello Interval] (秒)	ルータがEIGRP hello パケットを送信する間隔を設定します。 <ul style="list-style-type: none"> • 範囲：0 ～ 65,535 • デフォルト：5 秒
Route Policy Name	EIGRP ルートポリシーの名前を入力します。

ルート認証パラメータの設定

IP Enhanced IGRP のルート認証機能は、EIGRP ルーティングプロトコルからのルーティングアップデートに対する MD5 または HMAC-SHA-256 認証をサポートします。EIGRP ルートの認証を設定するには、次の手順を実行します。

1. [Authentication] をクリックします。
2. [Authentication] をクリックして、[Authentication Type] フィールドを開きます。
3. [global] パラメータ範囲を選択します。
4. ドロップダウンリストから、[md5] または [hmac-sha-256] を選択します。

パラメータ	オプション	説明
MD5	MD5 Key ID	MD5 キー ID を入力し、その値を使用して EIGRP パケットの内容に対する MD5 ハッシュを計算します。
	MD5 Authentication Key	送信パケットでエンコードされた MD5 チェックサムを使用するには、MD5 認証キーを入力します。
	Authentication Key	HMAC の計算に使用され、メッセージの送信側と受信側の両方で認識される 256 バイトの一意の情報。
[Add] をクリックして、認証パラメータを保存します。		



(注) 優先ルートマップを使用するには、MD5 キー (ID または認証キー) とルートマップの両方を指定します。

インターフェイスパラメータの設定

EIGRP ルートのインターフェイスパラメータを設定するには、[Interface] をクリックし、次のパラメータ値を入力します。

表 31: インターフェイスのパラメータ

パラメータ名	説明
Mark as Optional Row	この設定をデバイス固有としてマークするには、[Optional] をクリックします。デバイスにこの設定を含めるには、デバイステンプレートをデバイスに添付するときに要求された変数値を入力するか、テンプレート変数スプレッドシートを作成して変数を適用します。
Interface name	EIGRP を実行するインターフェイス名を入力します。
Shutdown	[No] (デフォルト) : インターフェイスで EIGRP を実行できません。 [Yes] : インターフェイスを無効にします。
[Add] をクリックして、インターフェイスを保存します。	

CLI を使用した EIGRP の設定

Cisco IOS XE Catalyst SD-WAN デバイスでの EIGRP の設定

次に、CLI を使用して Cisco IOS XE Catalyst SD-WAN デバイスで EIGRP を設定する例を示します。

```
config-transaction
router eigrp vpn
!
address-family ipv4 unicast vrf 1 autonomous-system 100
!
topology base
table-map foo filter
redistribute omp
exit-af-topology
network 10.1.44.0 255.0.0.0
exit-address-family
!
address-family ipv6 unicast vrf 1 autonomous-system 200
!
topology base
table-map bar
redistribute omp
exit-af-topology
exit-address-family
!
```

例 : OMP への EIGRP ルートのアドバタイズ

```
config-transaction
sdwan
omp
no shutdown
graceful-restart
address-family ipv4 vrf 1
advertise eigrp
```

```

!
address-family ipv6 vrf 1
advertise eigrp
!
address-family ipv4
advertise connected
advertise static
!
!

```

CLI を使用した EIGRP 設定の確認

Cisco IOS XE Catalyst SD-WAN デバイスの設定

次の show コマンドの出力は、Cisco IOS XE Catalyst SD-WAN デバイスの EIGRP 設定を示しています。

Cisco IOS XE Catalyst SD-WAN デバイスの IPv4 EIGRP ルートを表示します。

```

デバイス# show ip route vrf 1
m      192.168.22.22 [251/0] via 192.168.11.12, 00:28:00
       192.168.55.0/32 is subnetted, 1 subnets
D EX   192.168.55.55 [170/1] via 10.1.44.2, 00:33:58, GigabitEthernet3.2
       192.168.66.0/32 is subnetted, 1 subnets
B      192.168.66.66 [20/0] via 192.168.1.3, 00:33:57
       192.168.1.0/32 is subnetted, 3 subnets
D EX   192.168.1.3 [170/1] via 10.1.44.2, 00:33:58, GigabitEthernet3.2
m      192.168.1.33 [251/0] via 192.168.11.14 (3), 00:28:01

```

Cisco IOS XE Catalyst SD-WAN デバイスの IPv6 EIGRP ルートを表示します。

```

デバイス# show ipv6 route vrf 1
C      300:4::/64 [0/0]
       via GigabitEthernet3.2, directly connected
L      300:4::1/128 [0/0]
       via GigabitEthernet3.2, receive
D      2000:1:3::1/128 [90/1]
       via FE80::20C:29FF:FEF5:C767, GigabitEthernet3.2
L      FF00::/8 [0/0]
       via Null0, receive
cEdge4-Naiming#show ipv6 route vrf 1 2000:1:3::1/128
Routing entry for 2000:1:3::1/128
  Known via "eigrp 200", distance 90, metric 1
  OMP Tag 888, type internal
  Redistributing via omp
  Route count is 1/1, share count 0
  Routing paths:
    FE80::20C:29FF:FEF5:C767, GigabitEthernet3.2
      From FE80::20C:29FF:FEF5:C767
      Last updated 00:22:06 ago

```

Cisco IOS XE Catalyst SD-WAN デバイスの EIGRP の OMP ルートを表示します。

```

デバイス# show eigrp address-family ipv4 vrf 1 topology 192.168.44.4/24
EIGRP-IPv4 VR(vpn) Topology Entry for AS(100)/ID(192.168.1.44)
  Topology(base) TID(0) VRF(1)
EIGRP-IPv4(100): Topology base(0) entry for 192.168.44.4/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 1
  Descriptor Blocks:
    192.168.1.5, from Redistributed, Send flag is 0x0
      Composite metric is (1/0), route is External

```

```
Vector metric:
  Minimum bandwidth is 0 Kbit
  Total delay is 0 picoseconds
  Reliability is 0/255
  Load is 0/255
  Minimum MTU is 0
  Hop count is 0
  Originating router is 192.168.1.44
External data:
  AS number of route is 0
  External protocol is OMP-Agent, external metric is 4294967294
  Administrator tag is 0 (0x00000000)
```

CLIを使用した Routing Information Protocol (RIPv2) の設定

CLI デバイステンプレートおよび CLI アドオン機能テンプレートを使用して、RIPng を設定できます。

ここでは、Cisco IOS XE Catalyst SD-WAN デバイスでの RIP 設定に関する情報を示します。



- (注)
- **show ip protocols** コマンドを使用して RIP の設定を確認するには、VRF ルーティングテーブルとアドレスファミリサブモードの初期設定が必要です。
 - これらのコマンドは、任意の順序で実行できます。

- RIP ルーティングプロセスを設定します。

RIP ルーティングプロセスを有効にして、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-transaction
Device (config)# router rip
Device (config-router)#
```

- RIP VRF 対応サポートを設定します。

VRF 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、IPv4 アドレスプレフィックスを有効にします。

```
Device (config)# router rip
Device (config-router)# address-family ipv4 vrf vrf-name
```

- RIP バージョンを指定します。

デバイスが RIP バージョン 2 (RIPv2) パケットのみを送信できるようにするには、RIP バージョンを 2 に指定します。

```
Device (config)# router rip
Device (config-router)# version {1|2}
```

- RIP ルート集約を設定します。

サブネットルートを、ルータ コンフィギュレーション モードで使用するネットワークレベルルートに自動集約するデフォルトの動作を無効にするか、復元します。

```
Device(config)# router rip
Device(config-router)# auto-summary
```

- 送信元 IP アドレスを検証します。

ルータが着信 RIP アップデートの送信元 IP アドレスで検証チェックを実行できるようにします。

```
Device(config)# router rip
Device(config-router)# network ip-address
Device(config-router)# validate-update-source
```

- パケット間遅延を設定します。

発信 RIP アップデートの packets 間遅延（ミリ秒単位）を設定します。

```
Device(config)# router rip
Device(config-router)# output-delay delay-value
```

- RIP ルーティングプロセスにルートを再配布します。

指定したルートを IPv4 RIP ルーティングプロセスに再配布します。プロトコル設定の再配布は送信元ルータプロトコルの設定後にのみ行うことをお勧めします。protocol 引数は、**bgp**、**connected**、**isis**、**eigrp**、**omp**、**ospf**、**ospfv3**、または **static** キーワードのいずれかにすることができます。Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a では、Cisco IOS XE Catalyst SD-WAN デバイスの RIP バージョン 2 設定は、再配布されるプロトコルとして OMP をサポートしています。

```
Device(config)# router rip
Device(config-router)# redistribute protocol [metric metric-value] [route-map map-name]
```

- RIP ルーティングアップデートをフィルタ処理します。

インターフェイスを介して送受信される RIP ルーティングアップデートに、プレフィックスリストを適用します。

```
Device(config)# router rip
Device(config-router)# distribute-list prefix-list listname {in | out} [interface-type interface-number]
```

- RIP パラメータを設定します。

network コマンドは、RIP (v2) のインターフェイスを有効にし、ネットワークを RIP ルーティングプロセスに関連付けるために必要です。ルータで使用できる network コマンドの数に制限はありません。ネットワーク設定では、クラスフル（クラス A、クラス B、クラス C）の IP ネットワーク ID アドレッシングを使用することをお勧めします。

```
Device(config)# router rip
Device(config-router)# network ip-address
```

ルーティング情報を交換するネイバーデバイスを定義します。

```
Device(config)# router rip
Device(config-router)# network ip-address
Device(config-router)# neighbor ip-address bfd
```

ルーティングメトリックにオフセットリストを適用します。

```
Device(config)# router rip
Device(config-router)# offset-list acl-number in offset[ interface-type
|interface-name]
```

ルーティング プロトコル タイマーを調整します。

```
Device(config)# router rip
Device(config-router)# timers basic update invalid holddown flush
```

- RIP をカスタマイズします。

IPv4 RIP でサポートできる等コストルートの最大数を定義します。

```
Device(config)# router rip
Device(config-router)# maximum-paths number-paths
```

- ルートタグを設定します。

デフォルトでは、再配布された OMP ルートに対して自動 RIPv2 ルートタグが有効になっています。ルータが別の Cisco IOS XE Catalyst SD-WAN デバイスによってインストールされる場合、アドミニストレーティブ ディスタンスは 252 に設定されるため、OMP ルートは再配布された OMP ルートよりも優先されます。

```
Device(config)# router rip
Device(config-router)# omp-route-tag
```

- トラフィックを設定します。

最小コストパスを使用するようにトラフィックを設定し、等コストパスを持つマルチインターフェイスで負荷を分割します。

```
Device(config)# router rip
Device(config-router)# traffic-share min across-interfaces
```

設定例

次に、CLI を使用した Cisco IOS XE Catalyst SD-WAN デバイスの RIP の完全な設定例を示します。

```
config-transaction
!
    vrf definition 172
    address-family ipv4
    exit-address-family
!
    router rip
    address-family ipv4 vrf 172
    distance 70
    omp-route-tag /* Default is enabled */
    default-information originate route-map RIP-MED
    version 2
    network 10.0.0.20 /* Only classful A, B, or C network. */
    distribute-list prefix v4KANYU-RIP in TenGigabitEthernet0/1/3.791
    redistribute rip v6kanyu metric 1 metric-type 1 route-map v6RED-RIP-OSPF1
    distribute-list prefix v4KANYU-RIP in TenGigabitEthernet0/1/3.792
    no auto-summary
!
```

CLI を使用した RIPv2 設定の確認

CLI または Cisco SD-WAN Manager の [IP Routes] ウィンドウを使用して、RIP 設定を確認できます。次に、ルータの RIP 設定を表示する **show sdwan running | sec rip** コマンドの出力例を示します。

```
Device# show sdwan running | sec rip
router rip
  version 2
  redistribute connected
  output-delay 20
  input-queue 20
!
address-family ipv4 vrf 200
  redistribute connected
  redistribute omp metric 2
  network 56.0.0.0
  no auto-summary
  version 2
  exit-address-family
```

次に、デフォルトのルーティングテーブルに含まれる RIP ルートを表示する **show ip route rip** コマンドの出力例を示します。

```
Device# show ip route rip
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, m - OMP
        n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
        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
        H - NHRP, G - NHRP registered, g - NHRP registration summary
        o - ODR, P - periodic downloaded static route, l - LISP
        a - application route
        + - replicated route, % - next hop override, p - overrides from PfR
        & - replicated local route overrides by connected

Gateway of last resort is 10.0.5.13 to network 10.10.10.10

R      10.11.0.0/16 [120/1] via 172.16.1.2, 00:00:02, GigabitEthernet1
```

次に、VRF テーブルの RIP ルートを表示する **show ip route vrf vrf-id rip** コマンドの出力例を示します。

```
Device# show ip route vrf 1 rip
Routing Table: 1
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, m - OMP
        n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
        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
        H - NHRP, G - NHRP registered, g - NHRP registration summary
        o - ODR, P - periodic downloaded static route, l - LISP
        a - application route
        + - replicated route, % - next hop override, p - overrides from PfR
        & - replicated local route overrides by connected

Gateway of last resort is not set
```

```
10.0.0.14/32 is subnetted, 1 subnets
R 10.14.14.14 [120/1] via 10.20.25.18, 00:00:18, GigabitEthernet5
```

次に、RIP プライベートデータベースの内容を表示する **show ip rip database** コマンドの出力例を示します。

```
Device# show ip rip database
10.11.0.0/16 auto-summary
10.11.0.0/16
[1] via 172.16.1.2, 00:00:00, GigabitEthernet1
```

次に、RIP Bidirectional Forwarding Detection (BFD) ネイバーを表示する **show ip rip neighbors** コマンドの出力例を示します。

```
Device# show ip rip neighbors
BFD sessions created for the RIP neighbors
Neighbor Interface SessionHandle
10.10.10.2 GigabitEthernet1 1
```

次に、セクション RIP を使用してデバイスでの RIP プロトコル設定のみを表示する **show ip protocols** コマンドの出力例を示します。

```
Device# show ip protocols | sec rip
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 19 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Neighbor(s):
    10.1.1.2
  Default version control: send version 2, receive version 2
  Interface Send Recv Triggered RIP Key-chain
  GigabitEthernet1 2 2 No none
  Loopback10 2 2 No none
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.11.0.1
  Routing Information Sources:
    Gateway Distance Last Update
    10.1.1.2 120 00:00:15
  Distance: (default is 120)
```

CLI を使用した RIPng の設定

CLI デバイステンプレートおよび CLI アドオン機能テンプレートをを使用して、RIPng を設定できます。

ここでは、Cisco IOS XE Catalyst SD-WAN デバイスでの RIPng 設定について説明します。



(注) **show ipv6 route vrf** コマンドを使用して RIP の設定を確認するには、VRF ルーティングテーブルとアドレスファミリーサブモードの初期設定が必要です。

1. IPv6 RIPng VRF-Aware サポートを設定します。

1. IPv6 RIPng ルーティングの VRF-Aware サポートを有効にします。サービス VPN 内で RIPng を設定する必要があります。

```
Device(config)# ipv6 rip vrf-mode enable
```

2. IPv6 ユニキャストデータグラムの転送を有効にします。

```
Device(config)# ipv6 unicast-routing
```

2. IPv6 RIPng ルーティングプロセスを設定し、IPv6 RIPng ルーティングプロセスのルータ コンフィギュレーション モードを有効にします。



- (注) *ripng-instance* の場合は、*sdwan* を使用します。

```
Device(config)# ipv6 router rip ripng-instance  
Device(config-rtr)#
```

3. VRF 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、IPv6 アドレスプレフィックスを有効にします。

```
Device(config)# ipv6 router rip ripng-instance  
Device(config-rtr)# address-family ipv6 vrf vrf-name  
Device(config-ipv6-router-af)#
```

4. ルーティングテーブルに挿入されたルートのアドミニストレーティブディスタンスを定義します。

```
Device(config)# ipv6 router rip ripng-instance  
Device(config-rtr)# address-family ipv6 vrf vrf-name  
Device(config-ipv6-router-af)# distance distance
```

5. ルートタグを設定します。

デフォルトでは、再配布された OMP ルートに対して自動 RIPng ルートタグが有効になっています。一意の SD-WAN タグ (44270) を持つ RIPv2 および RIPng ルートを Cisco IOS XE Catalyst SD-WAN デバイスが学習すると、ルータは、OMP ディスタンス (251) よりも大きいアドミニストレーティブディスタンス (252) のルートをインストールします。それにより、その OMP ルートが、再配布された OMP ルートよりも優先されます。

```
Device(config)# ipv6 router rip ripng-instance  
Device(config-rtr)# omp-route-tag
```

6. IPv6 プレフィックスリストのエントリを作成します。

```
Device(config)# ipv6 prefix-list list-name [seq seq-number] permit IPv6 prefix (IP/length)
```

7. インターフェイス上で受信または送信される IPv6 RIPng ルーティングアップデートに、プレフィックスリストを適用します。

```
Device(config)# ipv6 router rip ripng-instance  
Device(config-rtr)# distribute-list prefix-list prefix-list-name {in | out} [interface-type | interface-number]
```

8. 指定したルートを IPv6 RIPng ルーティングプロセスに再配布します。rip キーワードと *ripng-instance* は、IPv6 RIPng ルーティングプロセスを指定します。

```
Device(config)# ipv6 router rip ripng-instance
Device(config-rtr)# redistribute protocol [metric default-metric] [route-map
map-tag]
```

9. インターフェイスを設定します。

1. 指定された IPv6 RIPng ルーティングプロセスをインターフェイス上で有効にします。



(注) *ripng-instance* の場合は、sdwan を使用します。

```
Device(config)# interface type number
Device(config-if)# ipv6 rip ripng-instance enable
```

2. (任意) IPv6 デフォルトルート (::/0) が配布され、指定したインターフェイスから送信される指定した RIPng ルーティングプロセスのアップデートに格納されます。



(注) *ripng-instance* の場合は、sdwan を使用します。

```
Device(config)# interface type number
Device(config-if)# ipv6 rip ripng-instance default-information {only |
originate} [metric metric-value]
```

3. インターフェイスの IPv6 RIPng メトリックオフセットを設定します。



(注) *ripng-instance* の場合は、sdwan を使用します。

```
Device(config)# interface type number
Device(config-if)# ipv6 rip ripng-instance metric-offset metric-value
```

4. インターフェイスで集約された IPv6 アドレスをアドバタイズし、集約するルートを識別する IPv6 プレフィックスを指定するように IPv6 RIPng を設定します。



(注) *ripng-instance* の場合は、sdwan を使用します。

```
Device(config)# interface type number
Device(config-if)# ipv6 address {ipv6-prefix/prefix-length | prefix-name |
sub-bits/prefix-length}
Device(config-if)# ipv6 rip ripng-instance summary-address
{ipv6-prefix/prefix-length}
```

RIPng の設定例

次の例は、CLI を使用した Cisco IOS XE Catalyst SD-WAN デバイスの完全な RIPng 設定を示しています。

```
config-transaction
!
  vrf definition 1
    address-family ipv6
    exit-address-family
!
  ipv6 rip vrf-mode enable
  ipv6 unicast-routing
!
  ipv6 prefix-list cisco seq 10 permit 2000:1::/64
!
  ipv6 router rip sdwan
    address-family ipv6 vrf 1
      distance 130
      omp-route-tag
      distribute-list prefix-list cisco in GigabitEthernet0/0/0
      redistribute omp metric 10
      exit-address-family
!
  interface GigabitEthernet0/0/0
    ipv6 address 2001:DB8::/64
    ipv6 rip sdwan enable
    ipv6 rip sdwan default-information originate
    ipv6 rip sdwan metric-offset 10
    ipv6 rip sdwan summary-address 2001:90::1/32
!
```

CLI を使用した RIPng 設定の確認

次に、ルータの RIPng 設定を表示する **show ipv6 route vrf** コマンドの出力例を示します。

```
Device# show ipv6 route vrf 1
IPv6 Routing Table - 1 - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, ls - LISP destinations-summary, a - Application
       m - OMP
R 1100::/64 [120/2]
   via FE80::20C:29FF:FE2E:13FF, GigabitEthernet2
R 2000::/64 [120/2]
   via FE80::20C:29FF:FE51:762F, GigabitEthernet2
R 2001:10::/64 [120/2]
   via FE80::20C:29FF:FE82:D659, GigabitEthernet2
R 2500::/64 [252/11], tag 44270
   via FE80::20C:29FF:FEE1:5237, GigabitEthernet2
C 2750::/64 [0/0]
   via GigabitEthernet2, directly connected
L 2750::1/128 [0/0]
   via GigabitEthernet2, receive
```

```
R 2777::/64 [252/11], tag 44270
   via FE80::20C:29FF:FEE1:5237, GigabitEthernet2
m 2900::/64 [251/0]
   via 192.168.1.5%default
R 3000::/64 [120/2]
   via FE80::20C:29FF:FE2E:13FF, GigabitEthernet2
R 3400::/64 [252/11], tag 44270
   via FE80::20C:29FF:FE51:762F, GigabitEthernet2
L FF00::/8 [0/0]
   via Null0, receive
```




第 4 章

マルチキャスト オーバーレイ ルーティング

- [マルチキャスト オーバーレイ ルーティング \(89 ページ\)](#)
- [サポートされているプロトコル \(91 ページ\)](#)
- [マルチキャスト オーバーレイ ルーティングのトラフィックフロー \(94 ページ\)](#)
- [マルチキャスト オーバーレイ ルーティングの設定 \(95 ページ\)](#)
- [Cisco SD-WAN と非 SD-WAN を相互接続するための MSDP のサポート \(120 ページ\)](#)

マルチキャスト オーバーレイ ルーティング



(注) 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

表 32: 機能の履歴

機能名	リリース情報	説明
L3 TLOC 拡張経由のマルチキャスト	Cisco IOS XE リリース 17.3.2 Cisco vManage リリース 20.3.1	この機能は、トランスポートロケーション (TLOC) のサポートを有効にします。これにより、追加 IP のコストを回避するためにピアトランスポートを追加でき、複数のトランスポート間でダイナミックロードバランスを使用できます。
マルチキャストオーバーレイルーティングプロトコルのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	この機能により、1対多のトラフィックを効率的に分散できます。IPv4 マルチキャスト、IGMPv3、PIM SSM、PIM ASM、Auto-RP、スタティック RP などのマルチキャストルーティングプロトコルは、複数の受信者にデータ (オーディオ/ビデオストリーミングブロードキャストなど) を配信します。マルチキャストオーバーレイプロトコルを使用すると、送信元は単一のデータパケットを単一のマルチキャストアドレスに送信し、受信者のグループ全体に配信できます。

Cisco IOS XE Catalyst SD-WAN マルチキャストオーバーレイソフトウェアは、オーバーレイ管理プロトコル (OMP) を使用して、Protocol Independent Multicast Source-Specific Multicast (PIM-SSM) を Cisco Catalyst SD-WANオーバーレイ上に拡張します。Protocol Independent Multicast Sparse-Mode (PIM-SM) がカスタマー VPN に導入され、Cisco IOS XE MVPN がカスタマー VPN の PIM とオーバーレイの OMP の統合に使用されます。OMP レプリケータはオーバーレイマルチキャストで使用され、オーバーレイトポロジ全体でマルチキャスト配信ツリーを最適化します。Cisco IOS XE Catalyst SD-WAN ルータは、IGMPv2 および IGMPv3 レポートをサポートし、OMP を使用して受信者のマルチキャスト対象をリモート Cisco Catalyst SD-WAN ルータにアドバタイズします。必要な最適化のレベルに応じて、Cisco Catalyst SD-WAN ルータはレプリケータとの間で参加またはプルーニングを行い、レプリケータは OMP を使用して Cisco Catalyst SD-WAN ルータに参加またはプルーニングをリレーし、PIM-RP または送信元へのオーバーレイ接続を提供します。

Cisco IOS XE Catalyst SD-WAN マルチキャストオーバーレイ実装は、オーバーレイネットワーク上で動作するセキュアな最適化マルチキャストツリーを作成することにより、ネイティブマルチキャストを拡張します。

サポートされるマルチキャストオーバーレイ機能

- IPv4 オーバーレイマルチキャスト (PIM SSM)
- IPv4 オーバーレイマルチキャスト (PIM ASM)
- IOS XE VPN 上の PIM-RP
- 地理位置情報 (GPS) を使用したレプリケータ
- スタティック RP および Auto-RP

- サービス側の IGMPv2、IGMPv3、および PIM
- IPSec および GRE カプセル化
- vEdge および IOS XE Catalyst SD-WAN 相互運用
- OMP を使用したオーバーレイ マルチキャスト シグナリング

Cisco IOS XE Catalyst SD-WAN リリース 17.3.2 以降では、マルチキャストおよびマルチキャスト アプリケーション認識ルートポリシー機能を備えた TLOC 拡張がサポートされています。

マルチキャスト設定の制限事項

マルチキャスト オーバーレイ ルーティングは、次の機能をサポートしていません。

- Cisco Catalyst SD-WAN ルータ上の MSDP/Anycast-RP
- IPv6 オーバーレイと IPv6 アンダーレイ
- マルチキャストのダイナミック BFD トンネル
- 非対称ユニキャストルーティングによるマルチキャスト
- マルチキャストオーバーレイは、データポリシーをサポートしていません。データポリシーが設定されている場合、必要なトラフィックのみが一致し、マルチキャストトラフィックは一致しません。
- Cisco SD-WAN デバイスは、ラストホップルータ (LHR) としてのみ使用できます。

サポートされているプロトコル

Cisco IOS XE Catalyst SD-WAN オーバーレイ マルチキャスト ネットワークは、すべてのプラットフォームで Protocol Independent Multicast (PIM)、Internet Group Management Protocol (IGMP)、およびマルチキャストテンプレート設定をサポートします。

PIM

Cisco IOS XE Catalyst SD-WAN オーバーレイマルチキャストでは、PIM バージョン 2 (RFC 4601 で定義) がサポートされますが、いくつかの制限があります。

サービス側では、Cisco IOS XE Catalyst SD-WAN ソフトウェアはネイティブマルチキャストをサポートします。ルータはネイティブ PIM ルータとして表示され、ローカルサイトの他の PIM ルータとの PIM ネイバーシップを確立します。Cisco IOS XE SD-WAN ルータは、直接接続されたローカル送信元 (ファーストホップルータ (FHR)) をサポートします。ルータのダウンストリームにある受信者は、IGMP メンバーシップレポートをデバイスと直接交換することでマルチキャストストリームに参加できます。他のルータは必要ありません。さらに、Cisco Catalyst SD-WAN ルータはローカルサイトの PIM-RP として機能できます。

トランスポート側では、PIM 対応 Cisco IOS XE Catalyst SD-WAN ルータがマルチキャストサービスイニシエーションルート（マルチキャスト自動検出ルート）を発信し、OMP を使用して Cisco Catalyst SD-WAN コントローラに送信します。マルチキャスト自動検出ルートは、ルータがレプリケータであるかどうか、およびローカルしきい値を示します。また、各 PIM ルータは、ローカルサイトマルチキャスト対応ルータから送信された PIM Join メッセージから学習した情報（マルチキャストグループの状態、送信元情報、RP など）も伝送します。これらのルートは、既存のマルチキャスト送信元に参加するときに、Cisco IOS XE Catalyst SD-WAN ルータがオーバーレイ全体で最適化された結合を実行できるようにします。

Cisco IOS XE Catalyst SD-WAN ルータは、PIM Source-Specific Mode (SSM) と ASM (Any Source Multicast) モードの両方をサポートします。

ランデブーポイント

PIM マルチキャスト共有ツリーのルートは、ランデブーポイント (RP) として設定されたルータ上にあります。Cisco Catalyst SD-WAN ソリューションでは、RP はローカルサイトに存在する Cisco Catalyst SD-WAN ルータまたは非 Cisco Catalyst SD-WAN ルータになります。

Cisco IOS XE Catalyst SD-WAN は、次の RP ディスカバリモードをサポートしています。

- スタティック RP
- Auto-RP
- Auto-RP プロキシ

ダイナミック RP グループマッピングは、Auto-RP を使用して Cisco IOS XE Catalyst SD-WAN ソリューションに伝達されます。ACL を使用して、特定のグループ範囲を制御したり、特定の RP にマッピングしたりできます。この情報を使用して、各 PIM ルータは、ダウンストリーム IGMP クライアントが参加しようとしているグループの正しい RP に参加情報を転送できます。Auto-RP アップデートは、ダウンストリーム PIM ルータがローカルサイトに存在し、オーバーレイを介して同じ VPN に属するリモートサイトに到達する場合、ダウンストリーム PIM ルータに伝達されます。Auto-RP を使用する場合は、レプリケータノードを Auto-RP マッピングエージェントとして設定する必要があります。

PIM-SM バージョン 2 では、Auto-RP に続いてブートストラップルータ (BSP) と呼ばれるもう 1 つの RP 選択モデルが導入されました。Auto-RP はシスコ独自のプロトコルですが、PIM BSR は PIM バージョン 2 仕様の一部です。BSR は、RP 機能およびグループの RP 情報のリレーに候補ルータを使用するという点において Auto-RP と同様に動作します。

レプリケータ

WAN 帯域幅を効率的に使用するために、必須の Cisco IOS XE Catalyst SD-WAN ルータをオーバーレイネットワーク全体に配置し、レプリケータとして設定できます。レプリケータにより、ローカル送信元または PIM-RP を使用する Cisco Catalyst SD-WAN ルータが、各受信者に対してマルチキャストストリームを 1 回複製するという要件が緩和されます。前述のように、レプリケータは、OMP マルチキャスト自動検出ルートを使用して、オーバーレイネットワーク内の Cisco Catalyst SD-WAN コントローラにレプリケータ自体をアドバタイズします。次に、

コントローラは、レプリケータと同じ VPN 内にある PIM 対応 Cisco IOS XE Catalyst SD-WAN ルータにレプリケータのロケーション情報を転送します。

レプリケータ Cisco IOS XE Catalyst SD-WAN ルータは、マルチキャスト送信元からストリームを受信してストリームを複製し、同じ VPN 内のマルチキャスト受信者を持つ他の Cisco Catalyst SD-WAN ルータに転送します。複製プロセスの詳細については、「Multicast Traffic Flow through the Overlay Network」を参照してください。通常、レプリケータは、WAN トランスポートネットワークへの高速接続を備えた共同のサイトまたは別のサイトにある Cisco IOS XE Catalyst SD-WAN ルータです。

マルチキャスト サービス ルート

Cisco IOS XE Catalyst SD-WAN ルータは、OMP を使用して Cisco Catalyst SD-WAN コントローラにマルチキャスト サービス ルートを送信します。コントローラは、これらのルートから、要求されたマルチキャストグループの参加を処理し、元の PIM Join メッセージで指定されている送信元アドレスまたは PIM-RP に向けて転送します。その結果、Cisco Catalyst SD-WAN ルータは OMP マルチキャスト サービス ルートをアダプタイズします。送信元アドレスは、発信元ルータが PIM 共有ツリーに参加しようとしている場合は RP の IP アドレス、発信元ルータが送信元ツリーに参加しようとしている場合はマルチキャストストリームにおける実際の送信元の IP アドレスになります。

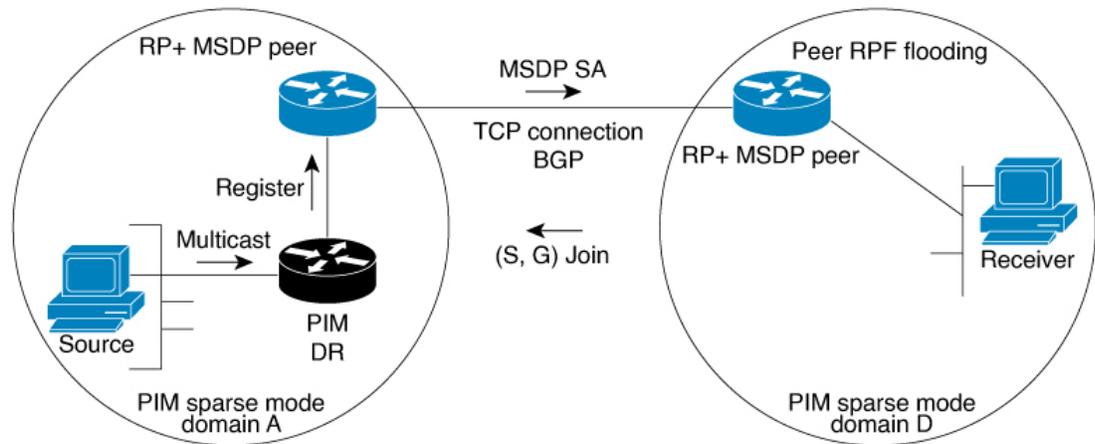
IGMP

Cisco IOS XE Catalyst SD-WAN ルータは、Internet Group Management Protocol (IGMP) V2 および V3 プロトコルをサポートします。IGMP は、IPv4 ホストおよびルータが、特定のマルチキャストグループのマルチキャストトラフィックの受信に関心があることを示すために使用されます。IGMPv3 レポートは、特定の送信元から特定のマルチキャストグループトラフィックへの関心を示すために使用されます。これらのメンバーシップレポートから、Cisco IOS XE Catalyst SD-WAN ルータは対応する PIM Join または OMP サービス ルートアダプタイズメントを発信します。

MSDP

Multicast Source Discovery Protocol (MSDP) は、複数の PIM-SM ドメインを接続する手段であり、他の PIM ドメインのマルチキャスト送信元を検出するために使用されます。ネットワークで MSDP が設定されている場合、ランデブーポイント (RP) は、他のドメインの MSDP 対応ルータとの MSDP ピア関係を維持することで、他のドメインの RP と送信元情報を交換します。このピアリング関係は、TCP 接続を通じて発生します。Cisco IOS XE Catalyst SD-WAN デバイスは、RP として設定することで、ドメイン外のアクティブな送信元を検出できます。

図 4: MSDP



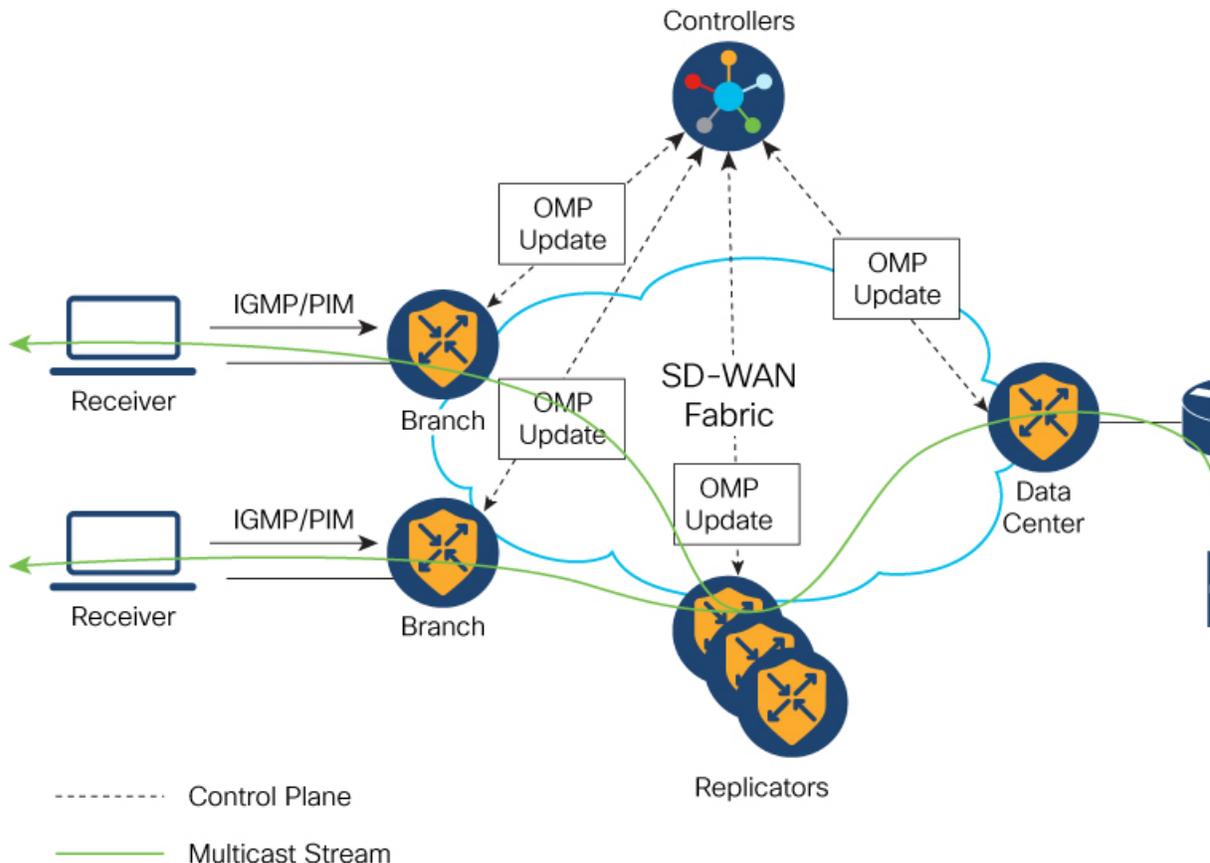
この図は、MSDP が実装されている場合に発生する一連のイベントを示しています。

1. ドメイン A の PIM 指定ルータ (DR) が送信元をドメイン A の RP に登録すると、その RP が送信元アクティブ (SA) メッセージをすべての RP MSDP ピアに送信します。SA メッセージでは、ソースアドレス、ソースの送信先グループ、および RP のアドレスまたは発行者 ID が識別されます (設定されている場合)。
2. ドメイン B の RP MSDP ピアは、SA メッセージを受信すると、ダウンストリームのすべてのピアに SA メッセージを送信します。
3. ドメイン B の RP MSDP ピアは、アドバタイズされたグループの受信者がそのドメイン内に存在するかどうかを確認します。グループの受信者が存在する場合、ドメイン B の RP MSDP ピアは、(S,G) 加入要求を送信元に送信します。その結果、ドメイン A とドメイン B の間に接続が確立されます。マルチキャストパケットが RP に到着すると、RP のドメイン内の受信者に転送されます。マルチキャストトラフィックを受信する受信者は、PIM-SM ドメイン外の送信元を認識 (送信元からのマルチキャストパケットの到着によって) すると、その送信元に PIM 加入要求を送信して、送信元のドメインに参加し、マルチキャストトラフィックを受信することができます。

マルチキャストオーバーレイルーティングのトラフィックフロー

次の図は、Cisco IOS XE Catalyst SD-WAN デバイス上のマルチキャストオーバーレイルーティングのトポロジの例を示しています。

図 5: マルチキャストオーバーレイルーティングのトポロジ



マルチキャストオーバーレイルーティングの設定

Cisco IOS XE SD-WAN ルータをマルチキャストオーバーレイネットワークに参加させるには、ルータで PIM を設定する必要があります。

前提条件

1. ランデブーポイント (RP) 選択を制限する場合は、CLI アドオンテンプレートを使用して IPv4 ACL を設定します。PIM を有効にする前に、標準または拡張アクセスリストを使用して IPv4 ACL を設定し、デバイスに接続します。マルチキャスト設定で ACL を使用する前に、有効な標準または拡張 ACL を作成しておく必要があります。



(注) Cisco SD-WAN Manager を使用して PIM 機能テンプレートの ACL を設定することはできません。CLI アドオンテンプレートを使用して ACL を設定する必要があります。Cisco IOS XE Catalyst SD-WAN マルチキャストオーバーレイの実装では、IOS XE 標準または拡張アクセスリストがサポートされています。

2. オーバーレイマルチキャスト設定には、少なくとも1つのレプリケータが必要です。
3. オプションで、サービス側にある個々のホストが特定のVPN内にあるマルチキャストグループに参加できるようにIGMPを設定できます。

マルチキャストの設定

Cisco IOS XE Catalyst SD-WAN ルータをレプリケータとして使用する場合は、次の手順を使用してマルチキャストを設定します。

1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Templates]** の順に選択します。
2. **[Device Template]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Device Templates]** のタイトルは **[Device]** です。

3. **[テンプレートの作成 (Create Template)]** をクリックします。
4. **[Create Template]** ドロップダウンリストから、**[From Feature Template]** を選択します。
5. **[Device Model]** ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
6. **[Service VPN]** セクションの **[Service VPN]** をクリックします。
7. **[Service VPN]** ドロップダウンリストをクリックします。
8. **[Additional VPN Templates]** で、**[Multicast]** をクリックします。
9. デバイスで **[Local Replicator]** を有効にするには、**[On]** を選択します（有効にしない場合は **[Off]** のままにします）。
10. レプリケータを設定するには、**[Threshold]** を選択します（オプション、レプリケータを設定しない場合はデフォルトのままにします）。
11. 機能テンプレートを保存します。
12. 機能テンプレートをデバイステンプレートに添付します。
13. **[Template Description]** フィールドに、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が **[Default]** に設定され（チェックマークで示される）、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、パラメータフィールドの左側にある **[Scope]** ドロップダウンリストをクリックし、値を選択します。

設定グループを使用したマルチキャストの設定

Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a 以降では、設定グループを使用してマルチキャストを設定するオプションがあります。

1. Cisco SD-WAN Manager のメニューから、[Configuration] > [Templates] > [Configuration Groups] を選択します。
2. 設定グループ名の横にある [...] をクリックし、[Edit] を選択します。
3. [Service Profile] をクリックします。
4. [Add Feature] をクリックします。
5. 機能ドロップダウンリストから、[Multicast] を選択します。

Cisco IOS XE Catalyst SD-WAN オーバーレイ マルチキャスト ネットワークは、次のプロトコルをサポートしています。

- プロトコルに依存しないマルチキャスト (PIM)
- インターネット グループ管理プロトコル (IGMP)
- MSDP

次の表では、マルチキャスト機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
Feature Name*	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。

表 33: 基本設定

フィールド	説明
SPT Only	最短パスツリーを使用してランデブーポイント (RP) が相互に通信できるようにするには、このオプションを有効にします。
Local Replicator	Cisco IOS XE Catalyst SD-WAN デバイスをマルチキャストレプリケータとして設定するには、このオプションを有効にします。
Threshold	値を指定します。 オプションで、レプリケータを設定しない場合はデフォルト値に設定されたままにします。

表 34: PIM

フィールド	説明
Source Specific Multicast (SSM)	SSM を設定するには、このオプションを有効にします。
ACL	<p>アクセス制御リストの値を指定します。アクセス制御リストにより、グループ（場合によっては送信元 IPv4 または IPv6 アドレス）を使用して、マルチキャストトラフィックストリームをフィルタ処理できます。</p> <p>PIM を有効にする前に、標準または拡張アクセスリストを使用して IPv4 アクセス制御リストを設定し、デバイスに接続します。マルチキャスト設定で ACL を使用する前に、有効な標準または拡張 ACL を作成しておく必要があります。</p> <p>(注) Cisco SD-WAN Manager を使用して PIM 機能テンプレートの ACL を設定することはできません。CLI アドオンテンプレートを使用して ACL を設定する必要があります。CLI アドオンテンプレートを使用した ACL の設定については、『Cisco SD-WAN Routing Configuration Guide』の「Multicast Overlay Routing」の章にある「Configure an ACL for Multicast Using a CLI Add-On Template」セクションを参照してください。</p>
SPT Threshold	共有ツリーから最短パスツリー (SPT) に切り替えるトラフィックレートを kbps 単位で指定します。この値を設定すると、トラフィックは強制的に共有ツリーに残り、SPT ではなく RP 経由で送信されます。
Add Interface	
Interface Name	PIM ドメインに参加するインターフェイスの名前を ge slot /port の形式で入力します。
Query Interval(sec)	インターフェイスが PIM クエリメッセージを送信する頻度を指定します。クエリメッセージは、ルータで PIM が有効になっていることをアドバタイズします。
Join/Prune Interval(sec)	PIM マルチキャストトラフィックがランデブーポイントツリー (RPT) または最短パスツリー (SPT) に参加する、または各ツリーから削除される頻度を指定します。Cisco IOS XE Catalyst SD-WAN デバイスは join および prune メッセージをアップストリーム RPF ネイバーに送信します。
<p>How do you want to configure your Rendezvous Point (RP)</p> <p>Cisco IOS XE SD-WAN は、次のモードをサポートしています。</p>	

フィールド	説明
Static	ランデブーポイント (RP) のスタティック IP アドレスを指定するには、このチェックボックスをクリックします。
Add Static RP	
IP Address	ランデブーポイント (RP) のスタティック IP アドレスを指定します。
ACL	ACL の値を指定します。
Override	<p>ダイナミックグループから RP へのマッピングとスタティックグループから RP へのマッピングが同時に使用されており、RP アドレスの競合がある場合は、このオプションを有効にします。この場合、スタティックグループから RP へのマッピングに関して設定された RP アドレスが優先されます。</p> <p>このオプションが有効になっておらず、RP アドレスの競合がある場合、ダイナミックグループから RP へのマッピングがスタティックグループから RP へのマッピングよりも優先されます。</p>
Auto RP	PIM グループから RP へのマッピングの更新を受信できるようにするには、このチェックボックスをクリックします。これにより、Auto-RP マルチキャストグループ 224.0.1.39 および 224.0.1.40 で受信できるようになります。
RP Announce	Auto-RP マルチキャストメッセージを送信できるようにするには、このチェックボックスをクリックします。
RP Discovery	PIM ネットワーク内のランデブーポイント (RP) の Auto-RP 自動検出を有効にして、ルータが Auto-RP マッピングエージェントとして機能できるようにするには、このチェックボックスをクリックします。Auto-RP マッピングは、すべての RP と RP のマルチキャストグループを受信し、グループから RP へのマッピングの一貫した更新をアドバタイズします。
Interface	Auto-RP RP アナウンスまたは RP ディスカバリメッセージの送信元インターフェイスを指定します。
Scope	Auto-RP RP アナウンスメントまたは RP ディスカバリメッセージの IP ヘッダー存続可能時間 (TTL) を指定します。
PIM-BSR	PIM BSR を設定します。
RP Candidate	
Interface Name	PIM 機能テンプレートの設定に使用したインターフェイスを選択します。

フィールド	説明
Access List	値を使用してアクセスリストを設定した場合は、アクセスリストの値を追加します。
Interval	値を使用して間隔を設定した場合は、間隔値を追加します。
Priority	Cisco IOS XE SD-WAN デバイスでは、サービス側デバイスよりも高い優先順位を指定します。
BSR Candidate (Maximum: 1)	
Interface Name	PIM機能テンプレートの設定に使用したものと同一インターフェイスをドロップダウンリストから選択します。
Hash Mask Length	ハッシュマスク長を指定します。ハッシュマスク長の有効な値は0～32です。
Priority	Cisco IOS XE Catalyst SD-WAN デバイスでは、サービス側デバイスよりも高い優先順位を指定します。
RP Candidate Access List	値を使用してRP候補アクセスリストを設定した場合は、値を追加します。 RP 候補は、アクセスリストの名前を入力できる標準の ACL を使用します。

表 35: IGMP

フィールド	説明
Add IGMP	
Interface	IGMPに使用するインターフェイスの名前を入力します。別のインターフェイスを追加するには、[Add] をクリックします。
Version	バージョン番号を指定します。 オプションで、デフォルトのバージョン番号に設定したままにします。
Group Address	マルチキャストグループに参加するためのグループアドレスを入力します。
Source Address	マルチキャストグループに参加するための送信元アドレスを入力します。
Add	[Add] をクリックしてグループの IGMP を追加します。

表 36 : MSDP

フィールド	説明
Originator-ID	発信元デバイスの ID を指定します。この ID は、RP アドレスとして使用されるインターフェイスの IP アドレスです。
Connection Retry Interval	ピアリングセッションがリセットされてからピアリングセッションの再確立が試行されるまで MSDP ピアが待機する間隔を設定します。
Mesh Group	
Mesh Group Name	メッシュグループ名を入力します。これにより、MSDP メッシュグループが設定され、MSDP ピアがそのメッシュグループに属することが指定されます。 (注) メッシュグループに参加しているデバイス上に存在するすべての MSDP ピアは、フルメッシュ内に存在し、他のすべての MSDP ピアがそのグループに含まれている必要があります。各デバイスの各 MSDP ピアは、 ip msdp peer コマンドを使用してピアとして設定する必要があります。また、 ip msdp mesh-group コマンドを使用して、そのメッシュグループのメンバーとして設定する必要があります。
Peer-IP	IP アドレスによって指定された MSDP ピアを設定します。
詳細設定	
Connect-Source Interface	TCP 接続の送信元 IP アドレスとして使用される、指定されたローカルインターフェイスのプライマリアドレスを入力します。
Peer Authentication Password	2 つの MSDP ピア間の TCP 接続の MD5 パスワード暗号化をイネーブルにします。 (注) どちらの MSDP ピアでも同じパスワードを使用して MD5 認証を設定する必要があります。そうしない場合は、これらの間の接続を確立できません。
Keep Alive	MSDP ピアがキープアライブメッセージを送信する間隔を設定します。
Hold-Time	MSDP ピアが、他のピアがダウンとしたと宣言するまでに他のピアからのキープアライブメッセージを待機する間隔を設定します。
Remote AS	MSDP ピアの自律システム番号を指定します。このキーワードおよび引数は、表示目的でのみ使用されます。

フィールド	説明
SA Limit	SA キャッシュ内で許可される特定の MSDP ピアからの SA メッセージの数を制限します。
Default Peer	すべての MSDP SA メッセージの受信元となるデフォルトピアを設定します。

CLI を使用したマルチキャストの設定

マルチキャストを設定するには、次の手順を実行します。

```
sdwan multicast address-family ipv4 vrf 1
replicator [threshold <num>]
```

マルチキャスト設定の例：

```
Device(config)# sdwan
Device(config)# multicast
  Device(config)# address-family ipv4 vrf 1
  Device(config)# replicator threshold 7500
Device(config)# !
!
```

CLI アドオンテンプレートを使用したマルチキャスト用の ACL の設定

CLI アドオンテンプレートを使用して、RP およびブートストラップルータ (BSR) の選択を制限するように ACL を設定できます。ACL により、グループ（場合によっては送信元 IPv4 または IPv6 アドレス）を使用して、マルチキャストトラフィックストリームをフィルタ処理できます。

CLI アドオンテンプレートを作成したら、デバイスに添付します。

(任意) Cisco SD-WAN Manager で同じ標準および拡張 ACL 値を設定できます。これにより、次の設定例が生成されます。

```
ip pim vrf 1 bsr-candidate Loopback0 32 100 accept-rp-candidate 101
ip pim vrf 1 rp-candidate Loopback0 group-list 27 interval 30 priority 0
```



(注) この設定例は、手順に示されている CLI アドオン設定例に基づいています。

1. マルチキャスト用の ACL を設定するには、[CLI アドオン機能テンプレート](#)を作成し、[デバイステンプレート](#)に添付します。

ここでは、設定例を示します。

```
ip access-list standard 27
1 permit 225.0.0.0 0.255.255.255
2 permit 226.0.0.0 0.255.255.255
3 permit 227.0.0.0 0.255.255.255
4 permit 228.0.0.0 0.255.255.255
5 deny 229.0.0.0 0.255.255.255
```

```

6 permit any
ip access-list extended 101
1 permit pim 172.16.10.0 0.0.0.255 any
2 permit pim 10.1.1.0 0.0.0.255 any

```

2. **[Configuration]** > **[Templates]** ウィンドウから、**[Feature]** を選択します。
3. [...] をクリックし、**[Edit]** をクリックすることにより、RP または BSR 候補に設定した **Cisco PIM** 機能テンプレートを編集します。
詳細については、「[PIM BSR の設定](#)」を参照してください。
4. (任意) 設定された RP 候補の **[Access List]** フィールドに、CLI アドオンテンプレートで設定したのと同じ ACL 値を入力します。
5. (任意) 設定された BSR 候補の **[RP Candidate Access List]** フィールドに、CLI アドオンテンプレートで設定したのと同じ ACL 値を入力します。
6. 機能テンプレートを更新し、機能テンプレートをデバイステンプレートに添付します。

PIM の設定

すべての Cisco IOS XE Catalyst SD-WAN デバイスに PIM テンプレートを使用します。

ルータが Cisco IOS XE Catalyst SD-WAN マルチキャストオーバーレイ ネットワークに参加できるように、Cisco SD-WAN Manager テンプレートを使用して PIM スパースモード (PIM-SM) プロトコルを設定します。

1. PIM 機能テンプレートを作成して、PIM パラメータを設定します。
2. オプションで、IGMP 機能テンプレートを作成して、サービス側の個々のホストが特定の VPN 内のマルチキャストグループに参加できるようにします。詳細については、「[Configure IGMP Using Cisco SD-WAN Manager Templates](#)」を参照してください。[IGMP の設定 \(115 ページ\)](#)
3. 必要に応じて、マルチキャスト機能テンプレートを作成し、Cisco IOS XE Catalyst SD-WAN をマルチキャストレプリケータとして設定します。
4. VPN 機能テンプレートを作成して、PIM を実行している VPN のパラメータを設定します。

PIM 機能テンプレートの作成

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** の順に選択します。
2. **[Device Template]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Device Templates]** のタイトルは **[Device]** です。

3. **[テンプレートの作成 (Create Template)]** をクリックします。

4. [Create Template] ドロップダウンリストから、[From Feature Template] を選択します。
5. [Device Model] ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
6. [Description] フィールドのすぐ下にある [Service VPN] をクリックするか、[Service VPN] セクションまでスクロールします。
7. [Service VPN] ドロップダウンリストをクリックします。
8. [Additional VPN Templates] で、[PIM] をクリックします。
9. [PIM] ドロップダウンリストから、[Create Template] をクリックします。[PIM] テンプレートフォームが表示されます。フォームの上部にはテンプレートに名前を付けるためのフィールドがあり、下部には PIM パラメータを定義するためのフィールドがあります。
10. [テンプレート名 (Template Name)] フィールドに、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。
11. [Template Description] フィールドに、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。
12. [Basic Configuration] をクリックし、[SSM – On/Off] を設定します。
13. アクセスリストを設定します (定義済みの場合)。
14. RP オプション (Auto-RP またはスタティック RP) を設定します。
15. RP アナウンス設定を設定します。
16. サービス側でインターフェイス名を設定します。
17. 機能テンプレートを保存し、機能テンプレートをデバイステンプレートに添付します。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が [Default] に設定され (チェックマークで示される)、デフォルト設定またはデフォルト値が表示されません。デフォルト値を変更するか、値を入力するには、パラメータフィールドの左側にある [Scope] ドロップダウンリストをクリックし、値を選択します。

表 37:

パラメータの範囲	範囲の説明
デバイス固有 (ホストのアイコンで示される)	<p>デバイス固有の値がパラメータに使用されます。デバイス固有のパラメータの場合、機能テンプレートに値を入力できません。Cisco IOS XE Catalyst SD-WAN デバイスをデバイステンプレートに添付するときに、値を入力します。</p> <p>[Device Specific] をクリックすると、[Enter Key] ボックスが表示されます。このボックスには、作成する CSV ファイル内のパラメータを識別する一意の文字列であるキーが表示されます。このファイルは、キーごとに 1 つの列を含む Excel スプレッドシートです。Cisco IOS XE Catalyst SD-WAN デバイスをデバイステンプレートに添付するときに、この CSV ファイルをアップロードします。</p> <p>デフォルトキーを変更するには、新しい文字列を入力し、[Enter Key] ボックスの外にカーソルを移動します。</p> <p>デバイス固有のパラメータの例としては、システム IP アドレス、ホスト名、GPS ロケーション、サイト ID があります。</p>
Global	<p>パラメータの値を入力し、その値をすべてのデバイスに適用します。</p> <p>デバイスのグループにグローバルに適用できるパラメータの例としては、DNS サーバー、Syslog サーバー、インターフェイス MTU があります。</p>

基本的な PIM の設定

PIM を設定するには、[Basic Configuration] をクリックし、次のパラメータを設定します。PIM を設定する場合、アスタリスクの付いたパラメータは必須です。

表 38:

パラメータ名	説明
Auto-RP	[On] をクリックして Auto-RP を有効にし、PIM グループから RP へのマッピングの更新を受信できるようにします。これにより、Auto-RP マルチキャストグループ 224.0.1.39 および 224.0.1.40 で受信できるようになります。デフォルトでは、Auto-RP は無効になっています。
Auto-RP RP Announce	Auto-RP マルチキャストメッセージの送信を有効にするには、[On] をクリックします。デフォルトでは、RP アナウンスは無効になっています。

パラメータ名	説明
Auto-RP RP Discovery	[On] をクリックして、PIM ネットワーク内のランデブーポイント (RP) の Auto-RP 自動検出を有効にし、ルータが Auto-RP マッピングエージェントとして機能できるようにします。Auto-RP マッピングは、すべての RP と RP のマルチキャストグループを受信し、グループから RP へのマッピングの一貫した更新をアドバタイズします。デフォルトでは、RP ディスカバリは無効になっています。
Static-RP	ランデブーポイント (RP) の IP アドレスを指定します。
SPT Threshold	共有ツリーから最短パスツリー (SPT) に切り替えるトラフィックレートを kbps 単位で指定します。この値を設定すると、トラフィックは強制的に共有ツリーに残り、SPT ではなく RP 経由で送信されます。
Interface	Auto-RP RP アナウンスまたは RP ディスカバリメッセージの送信元インターフェイスを指定します。
Scope	Auto-RP RP アナウンスメントまたは RP ディスカバリメッセージの IP ヘッダー存続可能時間 (TTL) を指定します。

機能テンプレートを保存するには、[Save] をクリックします。

PIM インターフェイスの設定

ルータが単なるマルチキャストレプリケータであり、マルチキャスト送信元または受信者を含むローカルネットワークの一部ではない場合、PIM インターフェイスを設定する必要はありません。レプリケータは、Cisco Catalyst SD-WAN コントローラと交換する OMP メッセージからマルチキャスト送信元と受信者の場所を学習します。これらのコントロールプレーンメッセージは、トランスポート VPN (VPN 0) で交換されます。同様に、他の Cisco IOS XE Catalyst SD-WAN デバイスは、Cisco Catalyst SD-WAN コントローラからの OMP メッセージを使用して、レプリケータを動的に検出します。

PIM インターフェイスを設定するには、[Interface] をクリックします。次に、[Add New Interface] をクリックして、次のパラメータを設定します。

表 39:

パラメータ名	説明
Name	PIM ドメインに参加するインターフェイスの名前を ge slot /port の形式で入力します。
Hello Interval	インターフェイスが PIM hello メッセージを送信する頻度を指定します。Hello メッセージは、ルータで PIM が有効になっていることをアドバタイズします。 範囲：1 ~ 3600 秒 デフォルト：30 秒

パラメータ名	説明
Join/Prune Interval	PIMマルチキャストトラフィックがランデブーポイントツリー（RPT）または最短パスツリー（SPT）に参加する、または各ツリーから削除される頻度を指定します。Cisco IOS XE Catalyst SD-WANはjoinおよびpruneメッセージをアップストリーム RPF ネイバーに送信します。 範囲：0～600秒。 デフォルト：60秒

インターフェイスを編集するには、エントリの右側にある鉛筆アイコンをクリックします。
インターフェイスを削除するには、エントリの右側にあるゴミ箱アイコンをクリックします。
機能テンプレートを保存するには、[Save] をクリックします。

PIM BSR によるランデブーポイント選択プロセス

表 40: 機能の履歴

機能名	リリース情報	説明
PIM BSR によるダイナミックランデブーポイント（RP）の選択	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能により、IPv4 マルチキャストオーバーレイで PIM BSR を使用した RP 候補の自動選択のサポートが追加されます。すべてのサイトにローカル RP があるため、シングルポイント障害はありません。 Cisco IOS XE Catalyst SD-WAN デバイスは RP として選択されるデバイスで、サービス側デバイスではありません。

PIM は BSR を使用して各グループプレフィックスの RP 設定情報を検出し、PIM ドメイン内のすべてのルータにアナウンスします。これは、Auto-RP によって行われるのと同じ機能ですが、BSR は PIM バージョン 2 仕様の一部です。



- (注) Cisco Auto-RP は PIM BSR と共存できません。Cisco Auto-RP モードは、SPT Only モードで無効にする必要があります。

シングルポイント障害を回避するために、1つの PIM ドメインに複数の候補 BSR を設定できます。BSR は候補 BSR の中から自動的に選択されます。BSR はブートストラップメッセージを使用して最も優先順位の高い BSR を検出します。その後、このルータが BSR であると PIM ドメイン内のすべての PIM ルータに通知します。ネットワーク内の任意のルータを BSR の候補にできます。

選定された BSR は、ドメイン内のすべての候補 RP から候補 RP メッセージを受信します。BSR から送信されるブートストラップメッセージには、すべての候補 RP に関する情報が含まれています。

RP は、マルチキャストデータのソースとレシーバの接点として機能します。PIM SIM ネットワークでは、ソースが RP にトラフィックを送信する必要があります。このトラフィックは、それから共有配信ツリーを下ってレシーバに転送されます。デフォルトでは、レシーバのファーストホップルータは、ソースを認識すると、ソースに加入メッセージを直接送信し、ソースからレシーバへのソースベースの配信ツリーを作成します。ソースとレシーバ間の最短パス内に RP が配置されていない限り、このソースツリーに RP は含まれません。



(注) BSR が複数の Cisco Catalyst SD-WAN サイトにまたがるマルチキャストストリームで機能するためには、SPT Only モードである必要があります。Cisco Catalyst SD-WAN サイト内のローカルサイトマルチキャストストリーム内の BSR では、SPT Only モードを有効にする必要はありません。



(注) 同じサイトに 2 つの Cisco IOS XE Catalyst SD-WAN デバイスが存在する場合、すべての Cisco IOS XE Catalyst SD-WAN デバイスをトラフィックフローのレプリケータとして設定する必要があります。

機能と利点

- IPv4 サポート。
- RP は静的ではなく動的に選択。
- 1 つの RP が使用できない場合の自動フェールオーバー。
- RP ディスカバリは BSR によって処理。
- 同じグループ範囲に対する複数の RP 候補の設定。
- RP としての Cisco IOS XE Catalyst SD-WAN デバイスの選択。

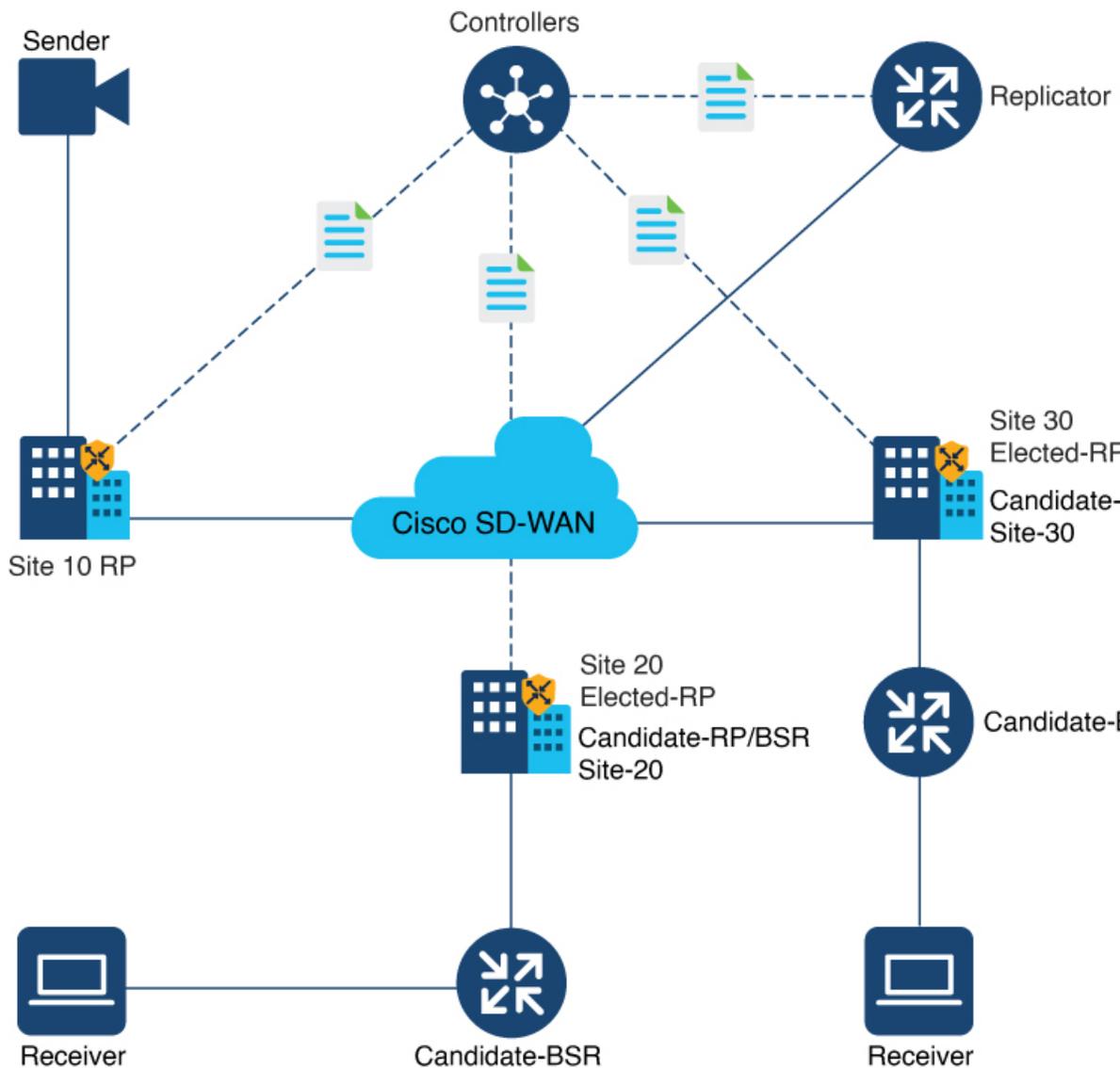
PIM BSR の制約事項

- IPv6 はサポートされていません。
- IPv4 の双方向 PIM はサポートされていません。
- BSR は、Cisco IOS XE Catalyst SD-WAN デバイスのハブアンドスポークトポロジではサポートされていません。

PIM BSR による RP 選択のサンプルトポロジ

次に、Cisco IOS XE Catalyst SD-WAN デバイス上の PIM BSR による RP 選択のサンプルトポロジを示します。

図 6: PIM BSR 選択のトポロジ



PIM BSR の設定

BSR 候補を設定するための前提条件

- すべての Cisco Catalyst SD-WAN サイトに独自の RP が必要です。

- すべての Cisco Catalyst SD-WAN サイトで SPT Only モードを有効にする必要があります。



(注) BSR が複数の Cisco Catalyst SD-WAN サイトにまたがるマルチキャストストリームで機能するためには、SPT Only モードである必要があります。Cisco Catalyst SD-WAN サイト内のローカルサイトマルチキャストストリーム内の BSR では、SPT Only モードを有効にする必要はありません。

ワークフロー

PIM BSR で RP を選択するには、Cisco SD-WAN Manager で次の項目を設定します。

1. 選択した Cisco IOS XE Catalyst SD-WAN デバイスの [SPT Only] が [On] に設定されているマルチキャスト機能テンプレート。
2. インターフェイスを含む PIM 機能テンプレート。
3. RP 候補。
4. BSR 候補。

マルチキャスト機能テンプレートの最短パスツリー (SPT Only) モードの設定

Cisco SD-WAN Manager で、[SPT Only] モードを設定して、最短パスツリーを使用して RP が相互に通信できるようにします。



(注) BSR を設定する場合、[SPT Only] モードの設定は必須です。

1. Cisco SD-WAN Manager メニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Add template] をクリックします。
4. [Select Devices] ドロップダウンリストから、Cisco IOS XE Catalyst SD-WAN デバイスを選択します。
5. [Other Templates] で、[Cisco Multicast] を選択します。
6. [テンプレート名 (Template Name)] フィールドに、テンプレートの名前を入力します。

7. [Description] フィールドに、テンプレートの説明を入力します。
説明の最大長は 2048 文字で、英数字のみを使用できます。
8. [Basic Configuration] セクションの [SPT Only] で、[On] を選択します。
9. デバイスで [Local Replicator] を有効にするには、[On] を選択します（有効にしない場合は [Off] に設定したままにします）。
10. レプリケータを設定するには、[Threshold] を選択し、値を指定します（オプションで、レプリケータを設定しない場合はデフォルト値に設定します）。
11. [Save] をクリックします。

PIM 機能テンプレートの設定とインターフェイスの追加

PIM 機能テンプレートを設定し、RP および BSR 候補のインターフェイスを追加します。

1. Cisco SD-WAN Manager メニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Add template] をクリックします。
4. [Select Devices] ドロップダウンリストから、Cisco IOS XE Catalyst SD-WAN デバイスを選択します。
5. [Other Templates] で、[Cisco PIM] を選択します。
6. [テンプレート名 (Template Name)] フィールドに、テンプレートの名前を入力します。
名前の最大長は 128 文字で、英数字のみを使用できます。
7. [Description] フィールドに、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。
8. [Interface] をクリックします。
PIM インターフェイスの設定方法については、「[PIM の設定](#)」を参照してください。
9. [New Interface] をクリックします。
10. [Interface Name] フィールドで、値を持つインターフェイスを指定します。
11. [Query Interval (seconds)] フィールドに、フィールドが自動入力されます。
12. [Join/Prune Interval (seconds)] フィールドに、フィールドが自動入力されます。
13. [Add] をクリックします。

14. [Save] をクリックします。

RP 候補の設定

すべてのマルチキャストグループまたは選択グループの候補 RP と同じ Cisco IOS XE Catalyst SD-WAN デバイスを設定します。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. **[Feature Templates]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Feature Templates]** のタイトルは **[Feature]** です。

3. [...] をクリックし、**[Edit]** をクリックして、作成した PIM 機能テンプレートを編集します。
4. **[Basic Configuration]** をクリックします。
5. **[RP Candidate]** をクリックします。
6. **[New RP Candidate]** をクリックします。
7. **[Interface]** ドロップダウンリストから、PIM 機能テンプレートの設定に使用したインターフェイスを選択します。
8. (任意) 値を設定してアクセスリストを設定した場合は、**[Access List]** フィールドに同じ値を追加します。
9. (任意) **[Interval]** フィールドで、値を設定して間隔を設定した場合は、同じ間隔値を追加します。
10. **[Priority]** フィールドで、サービス側デバイスよりも高い優先順位を Cisco IOS XE Catalyst SD-WAN デバイ스에指定します。
11. **[Add]** をクリックします。
12. **[Update]** をクリックして設定の変更を保存します。

BSR 候補の設定

1. 「RP 候補の設定」のステップ 1～4 を繰り返します。
2. **[BSR Candidate]** をクリックします。
3. **[BSR Candidate]** フィールドで、PIM 機能テンプレートの設定に使用したものと同一インターフェイスをドロップダウンリストから選択します。
4. (任意) **[Hash Mask Length]** フィールドで、ハッシュマスク長を指定します。
ハッシュマスク長の有効な値は 0～32 です。

5. [Priority] フィールドで、サービス側デバイスよりも高い優先順位を Cisco IOS XE Catalyst SD-WAN デバイスに指定します。
6. (任意) [RP Candidate Access List] フィールドで、RP 候補アクセスリストに値を設定している場合は、同じ値を追加します。
RP 候補は、アクセスリストの名前を入力できる標準のアクセスコントロールリスト (ACL) を使用します。
7. [Update] をクリックして設定の変更を保存します。

PIM BSR 選択の CLI 設定

BSR 候補の設定

1. 候補 BSR としての Cisco IOS XE Catalyst SD-WAN デバイスの設定

```
Device(config)# ip pim vrf 1 bsr-candidate Loopback 99
```



- (注) ループバック インターフェイスは、ここでは例としてのみ使用されます。ループバックは、RP 候補の設定に使用できる数あるインターフェイスタイプの 1 つです。

2. BSR に関する情報を表示するには、**show ip pim vrf bsr-router** コマンドを使用します。

```
Device# show ip pim vrf 1 bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
BSR address: 10.1.10.2 (?)
Uptime:      15:46:38, BSR Priority: 100, Hash mask length: 32
Next bootstrap message in 00:00:52
Candidate RP: 10.1.10.2 (Loopback0)
  Holdtime 75 seconds
  Advertisement interval 30 seconds
  Next advertisement in 00:00:18
  Group acl: 27
```

RP 候補の設定

1. すべてのマルチキャストグループまたは選択グループの候補 RP として Cisco IOS XE Catalyst SD-WAN デバイスを設定します。

```
Device(config)# ip pim vrf 1 rp-candidate Loopback 1 priority 0
```

または

```
Device(config)# ip pim vrf 1 rp-candidate Loopback 1 group-list acl1 priority 0
Device(config)# ip pim vrf 1 rp-candidate Loopback 2 group-list acl2 priority 0
```

2. **show ip pim vrf 1 rp mapping** コマンドを使用して、RP マッピングの割り当てを確認します。

```
Device# show ip pim vrf 1 rp mapping
PIM Group-to-RP Mappings
This system is a candidate RP (v2)
```

```

This system is the Bootstrap Router (v2)

Group(s) 224.0.0.0/4
  RP 10.1.10.2 (?), v2
    Info source: 10.1.10.2 (?), via bootstrap, priority 0, holdtime 75
    Uptime: 15:46:47, expires: 00:00:57
Group(s) 225.0.0.0/8
  RP 10.1.10.2 (?), v2
    Info source: 10.1.10.2 (?), via bootstrap, priority 0, holdtime 75
    Uptime: 15:46:47, expires: 00:00:57
  RP 10.1.10.1 (?), v2
    Info source: 10.1.10.1 (?), via bootstrap, priority 10, holdtime 75
    Uptime: 15:45:45, expires: 00:00:59
Group(s) 226.0.0.0/8
  RP 10.1.10.2 (?), v2
    Info source: 10.1.10.2 (?), via bootstrap, priority 0, holdtime 75
    Uptime: 15:46:55, expires: 00:00:49
  RP 10.1.10.1 (?), v2
    Info source: 10.1.10.1 (?), via bootstrap, priority 10, holdtime 75
    Uptime: 15:46:02, expires: 00:01:09
Group(s) 227.0.0.0/8
  RP 10.1.10.2 (?), v2
    Info source: 10.1.10.2 (?), via bootstrap, priority 0, holdtime 75
    Uptime: 15:47:13, expires: 00:00:59
  RP 10.1.10.1 (?), v2
    Info source: 10.1.10.1 (?), via bootstrap, priority 10, holdtime 75
    Uptime: 15:46:20, expires: 00:00:53
Group(s) 228.0.0.0/8
  RP 10.1.10.2 (?), v2
    Info source: 10.1.10.2 (?), via bootstrap, priority 0, holdtime 75
    Uptime: 15:47:31, expires: 00:01:13

```

Cisco IOS XE Catalyst SD-WAN デバイスを SPT-Only として設定

1. Cisco IOS XE Catalyst SD-WAN デバイスを SPT-Only として設定します。

```

Device(config)# sdwan multicast address-family ipv4 vrf 1
spt-only

```

2. システム IP アドレスが SPT-Only モードで設定されていることを確認するには、**show platform software sdwan multicast remote-nodes vrf** コマンドを使用します。

```

Device# show platform software sdwan multicast remote-nodes vrf 1

```

```

Multicast SDWAN Overlay Remote Nodes (* - Replicator):

```

System IP	SPT-Only Mode	Label	Received		Sent	
			(X,G) Join/Prune	(S,G) Join/Prune	(X,G) Join/Prune	(S,G) Join/Prune
172.16.255.11	Yes	1003	0/0	0/0	0/0	0/0
172.16.255.14	Yes	1003	0/0	0/0	1/0	10/10
172.16.255.16	Yes	1003	0/0	0/0	0/0	0/0
172.16.255.21	Yes	1003	0/0	0/0	0/0	0/0

SPT-Only のマルチキャスト設定の例

```

Device(config)# sdwan
Device(config)# multicast
Device(config)# address-family ipv4 vrf 1
Device(config)# spt-only
!
```

CLI を使用した VRRP 対応 PIM の確認

ルータ 1 での VRRP 対応 PIM 設定の例：

```
interface Vlan13
no shutdown
arp timeout 1200
vrf forwarding 1
ip address 10.0.0.1 255.255.255.0
ip pim sparse-mode
ip pim redundancy 1 vrrp dr-priority 200
ip tcp adjust-mss 1350
ip mtu 1500
ip igmp version 3
vrrp 1 address-family ipv4
vrrpv2
address 10.0.0.3
priority 200
timers advertise 100
track omp shutdown
vrrs leader 1
exit
```

ルータ 2 での VRRP 対応 PIM 設定の例：

```
interface Vlan13
no shutdown
arp timeout 1200
vrf forwarding 1
ip address 10.0.0.2 255.255.255.0
ip pim sparse-mode
ip pim redundancy 1 vrrp dr-priority 200
ip tcp adjust-mss 1350
ip mtu 1500
ip igmp version 3
vrrp 1 address-family ipv4
vrrpv2
address 10.0.0.3
priority 200
timers advertise 100
track omp shutdown
vrrs leader 1
exit
```

IGMP の設定

すべての Cisco IOS XE Catalyst SD-WAN デバイスに IGMP テンプレートを使用します。Internet Group Management Protocol (IGMP) を使用すると、ルータは特定の VPN 内のマルチキャストグループに参加できます。

Cisco SD-WAN Manager テンプレートを使用して IGMP を設定するには、次の手順を実行します。

1. IGMP 機能テンプレートを作成して、IGMP パラメータを設定します。
2. IGMP に使用するインターフェイスを VPN に作成します。VPN-Interface-Ethernet のヘルプトピックを参照してください。

- VPN 機能テンプレートを作成して、VPN パラメータを設定します。VPN のヘルプトピックを参照してください。

[Template] ウィンドウに移動し、テンプレートに命名する

- Cisco SD-WAN Manager メニューから、[Configuration] > [Templates] の順に選択します。
- [Device Template] をクリックします。



(注) Cisco vManage リリース 20.x.7 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

- [テンプレートの作成 (Create Template)] をクリックします。
- [Create Template] ドロップダウンリストから、[From Feature Template] を選択します。
- [Device Model] ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
- [Description] フィールドのすぐ下にある [Service VPN] をクリックするか、[Service VPN] セクションまでスクロールします。
- [Service VPN] ドロップダウンリストをクリックします。
- [Additional VPN Templates] で、[IGMP] をクリックします。
- [IGMP] ドロップダウンリストから、[Create Template] をクリックします。[IGMP] テンプレートフォームが表示されます。フォームの上部にはテンプレートに名前を付けるためのフィールドがあり、下部には IGMP パラメータを定義するためのフィールドがあります。
- サービス側でインターフェイス名を追加して、IGMP を有効にします。
- (任意) [Join Group And Source Address] フィールドで、[Add Join Group and Source Address] をクリックします。[Join Group and Source Address] ウィンドウが表示されます。
- (任意) 参加するグループアドレスと送信元アドレスを入力します。
- [テンプレート名 (Template Name)] フィールドに、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。
- [Template Description] フィールドに、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が [Default] に設定され (チェックマークで示される)、デフォルト設定またはデフォルト値が表示されません。デフォルト値を変更するか、値を入力するには、パラメータフィールドの左側にある [Scope] ドロップダウンをクリックし、値を選択します。

表 41:

パラメータの範囲	範囲の説明
デバイス固有 (ホストのアイコンで示される)	<p>デバイス固有の値がパラメータに使用されます。デバイス固有のパラメータの場合、機能テンプレートに値を入力できません。Cisco IOS XE Catalyst SD-WAN デバイスをデバイステンプレートに添付するときに、値を入力します。</p> <p>[Device Specific] をクリックすると、[Enter Key] ボックスが表示されます。このボックスには、作成する CSV ファイル内のパラメータを識別する一意の文字列であるキーが表示されます。このファイルは、キーごとに 1 つの列を含む Excel スプレッドシートです。Cisco IOS XE Catalyst SD-WAN デバイスをデバイステンプレートに添付するときに、この CSV ファイルをアップロードします。</p> <p>デフォルトキーを変更するには、新しい文字列を入力し、[Enter Key] ボックスの外にカーソルを移動します。</p> <p>デバイス固有のパラメータの例としては、システム IP アドレス、ホスト名、GPS ロケーション、サイト ID があります。</p>
グローバル	<p>パラメータの値を入力し、その値をすべてのデバイスに適用します。</p> <p>デバイスのグループにグローバルに適用できるパラメータの例としては、DNS サーバー、Syslog サーバー、インターフェイス MTU があります。</p>

基本的な IGMP パラメータの設定

IGMP を設定するには、[Basic Configuration] をクリックして IGMP を有効にします。次に、[Interface] をクリックし、[Add New Interface] をクリックして IGMP インターフェイスを設定します。IGMP を設定するには、次に示すすべてのパラメータが必要です。

表 42:

パラメータ名	説明
Interface Name	<p>IGMP に使用するインターフェイスの名前を入力します。</p> <p>別のインターフェイスを追加するには、プラス記号 (+) をクリックします。</p>
Join Group Address	<p>必要に応じて、[Add Join Group Address] をクリックしてマルチキャストグループを入力します。</p> <p>[Add] をクリックしてグループの IGMP を追加します。</p>

機能テンプレートを保存するには、[Save] をクリックします。

CLI を使用した PIM および IGMP の設定

1 つ以上のマルチキャスト送信元を含むサイトにある Cisco IOS XE Catalyst SD-WAN ルータの場合は、サービス側インターフェイスで PIM を有効にします。これらは、サービス側ネットワークに接続するインターフェイスです。VPN ごとに PIM または IGMP を有効にするには、マルチキャストサービスをサポートするすべての VPN に対して PIM または IGMP とそれぞれのインターフェイスを設定する必要があります。PIM 設定は、VPN 0（オーバーレイネットワークに面するトランスポート VPN）または VPN 512（管理 VPN）では必要ありません。

送信元インターフェイスが **send-rp-discovery** コンテナで指定されている場合は、そのインターフェイスにすでに IP アドレスと PIM が設定されていることを確認します。

設定例

```
vrf definition 1
  rd 1:1
  address-family ipv4
    exit-address-family
  !
  !
  ip pim vrf 1 autorp listener
  ip pim vrf 1 send-rp-announce Loopback1 scope 12 group-list 10
  ip pim vrf 1 send-rp-discovery Loopback1 scope 12
  ip pim vrf 1 ssm default
  ip access-list standard 10
    10 permit 10.0.0.1 0.255.255.255
  !
  ip multicast-routing vrf 1 distributed
  interface GigabitEthernet0/0/0.1
    no shutdown
    encapsulation dot1Q 1
    vrf forwarding 1
    ip address 172.16.0.0 255.255.255.0
    ip pim sparse-mode
    ip igmp version 3
    ip ospf 1 area 0
  exit
  interface GigabitEthernet0/0/2
    no shutdown
    vrf forwarding 1
    ip address 172.16.0.1 255.255.255.0
    ip pim sparse-mode
    ip ospf 1 area 0
  exit
  interface Loopback1
    no shutdown
    vrf forwarding 1
    ip address 192.0.2.255 255.255.255.255
    ip pim sparse-mode
    ip ospf 1 area 0
  exit
sdwan
multicast
  address-family ipv4 vrf 1
    replicator threshold 7500
  exit
```

CLI テンプレートをを使用した MSDP の設定

はじめる前に



(注) MSDP ピアをイネーブルにすることで、MSDP は暗黙的にイネーブルになります。

- IPマルチキャストルーティングをイネーブルにし、PIM-SMを設定する必要があります。詳細については、「[PIM の設定 \(103 ページ\)](#)」を参照してください。

CLI テンプレートをを使用した MSDP の設定

CLI テンプレートの使用の詳細については、[CLI アドオン機能テンプレート](#)および [CLI テンプレート](#)を参照してください。



(注) デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

ここでは、MSDP を設定するための CLI 設定の例を示します。

1. MSDP を有効にして、DNS 名または IP アドレスで指定される MSDP ピアを設定します。

```
ip msdp peer peer ip address connect-source
```

connect-source キーワードを指定した場合、指定されたローカルインターフェイスの **type** と **number** の値で示されるプライマリアドレスは TCP 接続の送信元 IP アドレスとして使用されます。リモートドメイン内のデバイスとのピアを確立している境界上の MSDP ピアの場合は特に、**connect-source** キーワードを推奨します。

2. 発信元アドレスを設定します。

SA メッセージを発信する MSDP スピーカーがそのインターフェイスの IP アドレスを SA メッセージ内の RP アドレスとして使用できるようにするには、次の任意の作業を実行します。

また、次のいずれかの理由により、発信元 ID を変更できます。

- Anycast RP の MSDP メッシュ グループに複数のデバイスを設定する場合。
- デバイスが PIM-SM ドメインと PIM-DM ドメインの境界にある場合。デバイスが PIM-SM ドメインと PIM-DM ドメインの境界にあり、PIM-DM ドメイン内のアクティブなソースをアドバタイズする場合は、SA メッセージ内の RP アドレスが発信元デバイスのインターフェイスのアドレスになるように設定します。

```
ip msdp originator-id type number
```

3. MSDP メッシュグループを設定します。

MSDP メッシュグループを設定し、MSDP ピアがそのメッシュグループに属することを指定します。



(注) デバイスごとに複数のメッシュグループを設定できます。

```
ip msdp mesh-group mesh name{peer-ip address | peer name}
```



(注) メッシュグループに参加しているデバイス上のすべての MSDP ピアは、そのグループ内の他のすべての MSDP ピアと完全にメッシュ構造になっている必要があります。各デバイスの各 MSDP ピアは、**ip msdp peer** コマンドを使用して、ピアとして設定する必要があります。また、**ip msdp mesh-group** コマンドを使用して、そのメッシュグループのメンバーとしても設定する必要があります。

Cisco SD-WAN と非 SD-WAN を相互接続するための MSDP のサポート

表 43:機能の履歴

機能名	リリース情報	機能説明
Cisco SD-WAN ドメインと非 SD-WAN ドメインを相互接続するための MSDP のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a Cisco vManage リリース 20.11.1	この機能により、Cisco Catalyst SD-WAN に含まれる Cisco IOS XE Catalyst SD-WAN デバイス と非 SD-WAN セットアップに含まれるデバイスの間の Multicast Source Discovery Protocol (MSDP) 相互運用性が有効になります。 (注) この機能は、オーバーレイネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイス間に形成された MSDP ピアに関するサポートを提供しません。

Cisco SD-WAN と非 SD-WAN を相互接続するための MSDP のサポートについて

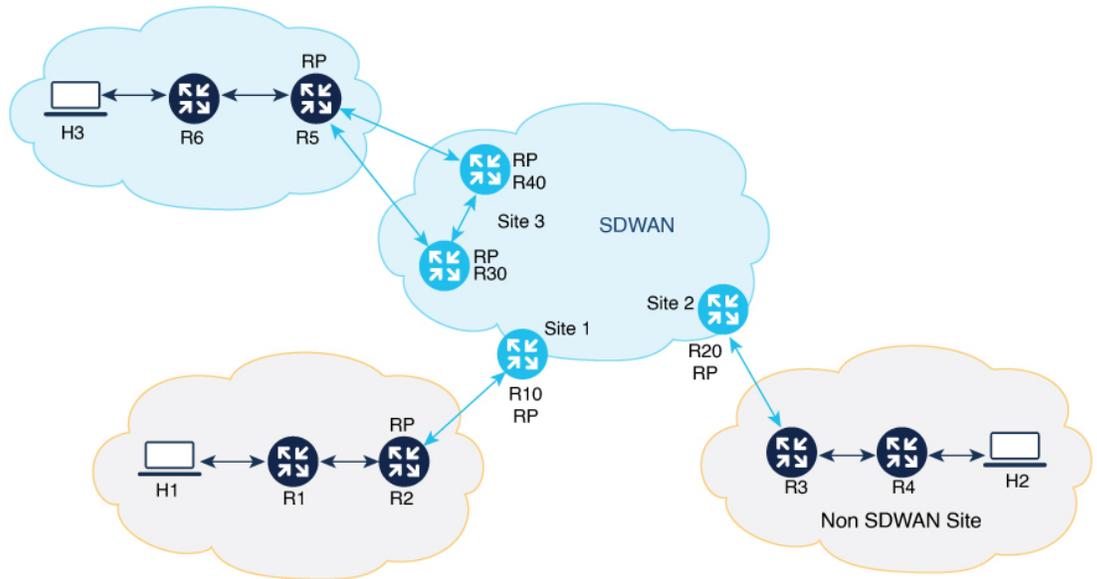
MSDP によって、複数の Protocol Independent Multicast Sparse-Mode (PIM-SM) ドメインの相互接続が容易になります。Cisco IOS XE Catalyst SD-WAN デバイスで MSDP が有効になっている場合、PIM-SM ドメインのランデブーポイント (RP) は、他のドメインの MSDP 対応ルータと

の MSDP ピアリング関係を維持します。MSDP の詳細については、[MSDP \(93 ページ\)](#) を参照してください。

Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a 以降では、他のデバイスとの MSDP 相互運用性のために Cisco IOS XE Catalyst SD-WAN デバイスを設定できます。MSDP 相互運用性のために Cisco IOS XE Catalyst SD-WAN デバイスが設定されている場合、MSDP ピアから受信した送信元アクティブ (SA) メッセージを OMP ルートに、またはその逆に変換します。

次の図は、Cisco Catalyst SD-WAN 内の Cisco IOS XE Catalyst SD-WAN デバイス と非 SD-WAN セットアップのデバイス間の MSDP 相互運用性を示しています。

図 7: MSDP 相互運用性



シングルホームネットワーク

このトポロジの例では、サイト 2 の Cisco IOS XE Catalyst SD-WAN デバイス (R20) で MSDP 相互運用性が有効になっています。R3 は、非 SD-WAN サイトで PIM ドメインの RP として設定されます。MSDP ピアリングは、非 SD-WAN サイトの R3 とサイト 2 の R20 の間で確立されます。送信元 H2 が R4 にトラフィックを送信すると、R4 が R3 へのデータ登録を開始し、その後、R3 が R20 に MSDP SA メッセージを送信します。R20 では MSDP 相互運用性が有効になっているため、R20 は、受信した MSDP SA メッセージを OMP SA ルートに変換し、それらを、Cisco IOS XE Catalyst SD-WAN デバイスにサービスを提供する Cisco SD-WAN コントローラを介して他のサイトにあるすべての Cisco IOS XE Catalyst SD-WAN デバイスにアドバタイズします。サイト 1 の Cisco IOS XE Catalyst SD-WAN デバイス (R10) は、この OMP SA ルートを受信すると、OMP SA ルートを MSDP SA メッセージに変換し、その MSDP SA メッセージを非 SD-WAN サイトの MSDP ピア (R2) にアドバタイズします。R2 は、MSDP SA メッセージでアドバタイズされたグループを対象の受信者を持つ場合、(S,G) 加入要求を送信元に送信します。その結果、ドメイン間送信元ツリーが Cisco Catalyst SD-WAN 全体に確立されます。マルチキャストパケットは、R2 (RP) に着信すると、その共有ツリーを経由して

RP のドメイン内のグループメンバーに転送されます。R20 は、MSDP SA メッセージが期限切れになった場合にのみ、アドバタイズされた OMP SA ルートを撤回します。

デュアルホームネットワーク

デュアルホームネットワークでは、MSDP 相互運用性のために 2 つの Cisco IOS XE Catalyst SD-WAN デバイスが設定されています。デュアルホーム Cisco Catalyst SD-WAN サイト 3 では、Cisco IOS XE Catalyst SD-WAN デバイス R30、R40、および非 SDWAN デバイス R5 の間で MSDP ピアリングを確立する必要があります。送信元が RP R5 にトラフィックを登録すると、R5 は、R30 と R40 の両方に MSDP SA メッセージを送信します。R30 は、MSDP SA メッセージを受信すると、その MSDP SA メッセージを OMP SA ルートに変換して、他のサイトにあるすべての Cisco IOS XE Catalyst SD-WAN デバイスにアドバタイズし、同じサイト 3 内の R40 にアドバタイズします。Overlay Management Protocol (OMP) を介して他の Cisco IOS XE Catalyst SD-WAN デバイスおよびサイトから受信した SA メッセージをドロップするために、R30 と R40 の間で MSDP SA フィルタを設定する必要があります。サイト 1 の Cisco IOS XE Catalyst SD-WAN デバイス R10 は、同じ送信元グループ (S、G) の 2 つの OMP SA ルートを受信し、両方をキャッシュします。その後、R10 は、OMP SA ルートを MSDP SA メッセージに変換し、非 SD-WAN サイトの MSDP ピア R2 にアドバタイズします。R2 は、MSDP SA メッセージでアドバタイズされたグループを対象の受信者を持つ場合、(S,G) 加入要求を送信元に送信します。その結果、ドメイン間送信元ツリーが Cisco Catalyst SD-WAN 全体に確立されます。

MSDP は、Cisco Catalyst SD-WAN サイトの Cisco IOS XE Catalyst SD-WAN デバイスが非 SD-WAN サイトにある他のデバイスとの MSDP 相互運用性のために設定されている次のシナリオをサポートします。

- Cisco Catalyst SD-WAN サイトにある送信元デバイスと、Cisco Catalyst SD-WAN サイトおよび非 SD-WAN サイトにある受信者。
- 非 SD-WAN サイトにある送信元デバイスと、Cisco Catalyst SD-WAN サイトおよび非 SD-WAN サイトにある受信者。
- Cisco Catalyst SD-WAN での MSDP 相互運用性のために 2 つのデバイスが設定され、送信元と受信者が Cisco Catalyst SD-WAN サイトに配置されている、デュアルボーダーサイト内。
- 非 SD-WAN での MSDP 相互運用性のために 2 つのデバイスが設定され、送信元と受信者が非 SD-WAN サイトに配置されている、デュアルボーダーサイト内。
- Cisco Catalyst SD-WAN サイトに存在する任意の Cisco IOS XE Catalyst SD-WAN デバイスをレプリケータにできます。レプリケータの詳細については、[PIM \(91 ページ\)](#) の「レプリケータ」セクションを参照してください。

Cisco SD-WAN と非 SD-WAN を相互接続するための MSDP のサポートの利点

Cisco SD-WAN サイトにあるデバイスと非 SD-WAN サイトにあるデバイス間の MSDP 相互運用性を容易に実現できます。

Cisco SD-WAN と非 SD-WAN を相互接続するための MSDP のサポートの前提条件

- MSDP の相互運用性を機能させるには、Cisco IOS XE Catalyst SD-WAN デバイス で最短パストリー (SPT) の SPT Only モードを有効にするとともに、デバイスを RP として選択する必要があります。詳細については、[設定グループを使用したマルチキャストの設定 \(97 ページ\)](#) の「基本設定」を参照してください。
- MSDP の相互運用性を実現するには、メッシュグループでピアデバイスをセットアップする必要があります。
- デュアルホームセットアップでは、他の Cisco IOS XE Catalyst SD-WAN デバイスからの MSDP SA メッセージをドロップするように Cisco IOS XE Catalyst SD-WAN デバイスで MSDP SA フィルタを設定します。

Cisco SD-WAN と非 SD-WAN を相互接続するための MSDP のサポートに関する制約事項

- Cisco Catalyst SD-WAN では、サイトごとに1つの MSDPメッシュグループのみがサポートされます。
- MSDP ピアデバイスは、同じサイトに配置する必要があり、複数のサイトに分散させることはできません。

Cisco SD-WAN と非 SD-WAN を相互接続するための MSDP の設定



- (注) Cisco SD-WAN Manager の機能テンプレートまたは設定グループを使用して MSDP 相互運用性を設定することはできません。

Cisco IOS XE Catalyst SD-WAN デバイスで MSDP 相互運用性を設定するには、次のタスクを実行します。

1. Cisco IOS XE Catalyst SD-WAN デバイスで MSDP を有効にします。詳細については、「[CLI テンプレートを使用した MSDP の設定 \(119 ページ\)](#)」を参照してください。
2. CLI テンプレートを使用して MSDP インターワーキングを設定します。詳細については、[CLI テンプレートを使用した Cisco SD-WAN と非 SD-WAN を相互接続するための MSDP の設定 \(124 ページ\)](#) を参照してください。

CLI テンプレートを使用した Cisco SD-WAN と非 SD-WAN を相互接続するための MSDP の設定

Cisco Catalyst SD-WAN で MSDP 相互運用性機能を設定するには、CLI テンプレートを使用します。CLI テンプレートの使用の詳細については、[CLI アドオン機能テンプレート](#)および[CLI テンプレート](#)を参照してください。



(注) デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

1. Cisco IOS XE Catalyst SD-WAN デバイス で MSDP を有効にします。詳細については、[CLI テンプレートを使用した MSDP の設定 \(119 ページ\)](#) を参照してください。
2. Cisco IOS XE Catalyst SD-WAN デバイス を設定して、非 SD-WAN サイトの他のデバイスとの MSDP 相互運用性を実現します。

```
multicast address-family ipv4 vrf vrf-name
spt-only
msdp-interworking
```

次に、Cisco Catalyst SD-WAN で MSDP 相互運用性を設定する完全な設定例を示します。

```
sdwan

multicast address-family ipv4 vrf 1

spt-only

msdp-interworking
```

Cisco SD-WAN と非 SD-WAN を相互接続するための MSDP の設定の確認

次に、MSDP 相互運用性が有効かどうかを示す **show platform software sdwan multicast remote-nodes vrf/** コマンドの出力例を示します。

```
Device# show platform software sdwan multicast remote-nodes vrf 1
Multicast SDWAN Overlay Remote Nodes (* - Replicator, ^ - Delete Pending):
```

System IP	SPT-Only Mode	MSDP I-Work	Label	Received (X,G)		Sent (X,G)	
				Join/Prune	Join/Prune	Join/Prune	Join/Prune
10.16.255.11	No	No	1003	0/0	0/0	0/0	1/0
10.16.255.15	No	No	1003	1/0	1/0	0/0	0/0
10.16.255.16	Yes	No	1003	1/0	1/0	0/0	0/0
10.16.255.21	Yes	Yes	1003	0/0	0/0	0/0	0/0

Cisco SD-WAN と非 SD-WAN を相互接続するための MSDP の設定のモニター

Cisco IOS XE Catalyst SD-WAN デバイスで MSDP 相互運用性をモニターするには、次の show コマンドを使用します。

```
Device# show ip msdp vrf 1 sa-cache
MSDP Source-Active Cache - 1 entries
(10.169.1.1, 12.169.1.1), RP 41.41.41.41, AS ?,6d20h/00:05:55, Peer 12.168.3.11
```

```
Device# show ip msdp vrf 1 count
SA State per Peer Counters, <Peer>: <# SA learned>
 12.168.3.11: 1
 12.168.11.15: 0
 12.168.12.12: 0
 12.168.14.14: 0
 12.168.5.24: 0
SA State per ASN Counters, <asn>: <# sources>/<# groups>
Total entries: 1
?: 1/1
```

```
Device# show ip msdp vrf 1 summary
MSDP Peer Status Summary
Peer Address      AS      State   Uptime/  Reset SA   Peer Name
                  AS      State   Downtime Count Count
12.168.3.11      ?      Up      17w6d   0      1      ?
12.168.11.15     ?      Up      17w6d   0      0      ?
12.168.12.12     ?      Up      17w6d   0      0      ?
12.168.14.14     ?      Up      17w6d   0      0      ?
12.168.5.24      ?      Up      17w6d   1      0      ?
```

```
Device# show ip msdp vrf 1 peer 12.168.15.19 advertised-SAs
MSDP SA advertised to peer 12.168.15.19 (?) from mroute table

MSDP SA advertised to peer 12.168.15.19 (?) from SA cache

MSDP SA advertised to peer 12.168.15.19 (?) from mvpn sact table

20.169.1.1      13.169.1.1 RP 41.41.41.41 (?) 6d20h ref: 2
```

上記の出力では、**mvpn sact table** からの **MSDP SA advertised to peer 12.168.15.19 (?)** エントリが、受信した OMP SA ルートに基づいてピアにアドバタイズされた SA キャッシュメッセージに関する情報を提供します。

```
Device# show ip msdp vrf 1 peer 12.168.21.29
MSDP Peer 12.168.21.29 (?), AS ?
Connection status:
  State: Up, Resets: 0, Connection source: GigabitEthernet5 (12.168.21.28)
  Uptime(Downtime): 16w4d, Messages sent/received: 169100/169106
  Output messages discarded: 82
  Connection and counters cleared 16w4d ago
  Peer is member of mesh-group site3
SA Filtering:
  Input (S,G) filter: sa-filter, route-map: none
  Input RP filter: none, route-map: none
  Output (S,G) filter: none, route-map: none
  Output RP filter: none, route-map: none
SA-Requests:
  Input filter: none
Peer ttl threshold: 0
SAs learned from this peer: 0
Number of connection transitions to Established state: 1
```

```
Input queue size: 0, Output queue size: 0
MD5 signature protection on MSDP TCP connection: not enabled
Message counters:
  RPF Failure count: 0
  SA Messages in/out: 10700/10827
  SA Requests in: 0
  SA Responses out: 0
  Data Packets in/out: 0/10
```

トラブルシューティング

MSDP SA キャッシュが入力されない

問題 サイト内の送信元がトラフィックを送信するときに MSDP SA キャッシュが Cisco IOS XE Catalyst SD-WAN デバイスに入力されません。

考えられる原因 MSDP ピア間に接続または設定の問題があるかどうかを確認します。

解決法 問題を解決するには、次の手順を実行します。

解決法 Cisco IOS XE Catalyst SD-WAN デバイス と非 SD-WAN 内のデバイス間の MSDP ピアリングステータスを確認します。

解決法 Cisco IOS XE Catalyst SD-WAN デバイスで **msdp-interworking** コマンドと **spt-only** コマンドが設定されていることを確認します。

OMP SA ルートがアドバタイズされない

問題 Cisco IOS XE Catalyst SD-WAN デバイスが、MSDP ピアから MSDP SA メッセージを受信したときに、OMP SA ルートをアドバタイズしません。

考えられる原因 **msdp-interworking** 設定が失われている可能性があります。

解決法 適切な VRF で **msdp-interworking** コマンドを設定します。



第 5 章

無線対応ルーティング



- (注) 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

表 44: 機能の履歴

機能名	リリース情報	説明
無線対応ルーティングのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能により、Cisco IOS XE Catalyst SD-WAN デバイスでの無線対応ルーティング (RAR) のサポートが有効になります。RAR は、無線信号を使用してルーティングプロトコル OSPFv3 と情報を交換し、1 ホップルーティングネイバーのアピアランス、ディスプレイアランス、およびリンク状態について信号で伝えるメカニズムです。大規模なモバイルネットワークでは、ルーティングネイバーへの接続が距離と無線障害により中断されます。RAR は、モバイルネットワークで IP ルーティングと無線通信を統合する際に直面する課題に対処します。

- [RAR のサポートされるデバイス \(128 ページ\)](#)
- [RAR の前提条件 \(128 ページ\)](#)

- [RAR の利点 \(128 ページ\)](#)
- [RAR に関する制約事項 \(129 ページ\)](#)
- [RAR について \(129 ページ\)](#)
- [RAR の設定 \(132 ページ\)](#)

RAR のサポートされるデバイス

RAR をサポートするプラットフォームは次のとおりです。

- Cisco 4000 シリーズ サービス統合型ルータ
- Cisco 1000 シリーズ サービス統合型ルータ
- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ
- Cisco CSR 1000 シリーズ クラウド サービス ルータ
- Cisco CSR 8000 シリーズ クラウド サービス ルータ

RAR の前提条件

RAR 設定には、モバイルアドホック ネットワーク (MANET) のサポートが必要です。RAR に PPP over Ethernet (PPPoE) および仮想マルチポイント インターフェイス (VMI) 機能を使用するには、ルーティングプロトコル (OSPFv3 または EIGRP) に対する MANET の統一された表現が必要です。

RAR の利点

無線対応ルーティング機能には次のようなメリットがあります。

- 変更を即座に認識することで、ネットワーク コンバージェンスを高速化します。
- 障害の発生している、または減衰している無線リンクのルーティングを有効にします。
- ラインオブサイトパスと非ラインオブサイトパス間のルーティングを容易にします。
- 高速コンバージェンスと最適なルート選択が可能になるため、音声やビデオなど遅延の影響を受けやすいトラフィックが中断されません。
- 無線リソースと帯域幅の効率的な使用が可能になります。
- ルータで輻輳制御を実行することにより、無線リンクへの影響を軽減します。
- 無線電力の節減に基づくルート選択が可能になります。
- ルーティング機能と無線機能の分離を有効にします。

- RFC 5578、R2CP、および DLEP に準拠した無線へのシンプルなイーサネット接続を実現します。

RAR に関する制約事項

無線対応ルーティング機能には次の制約事項があります。

- Dynamic Link Exchange Protocol (DLEP) プロトコルと Router to Radio Control Protocol (R2CP) プロトコルはサポートされていません。
- マルチキャストトラフィックは、集約モードではサポートされていません。
- 高可用性 (HA) はサポートされていません。

RAR について

無線対応ルーティング (RAR) は、無線インターフェイスを使用して Open Shortest Path First (OSPFv3) プロトコルと情報を交換し、1 ホップルーティングネイバーのアピアランスおよびリンク状態について信号で伝えるメカニズムです。

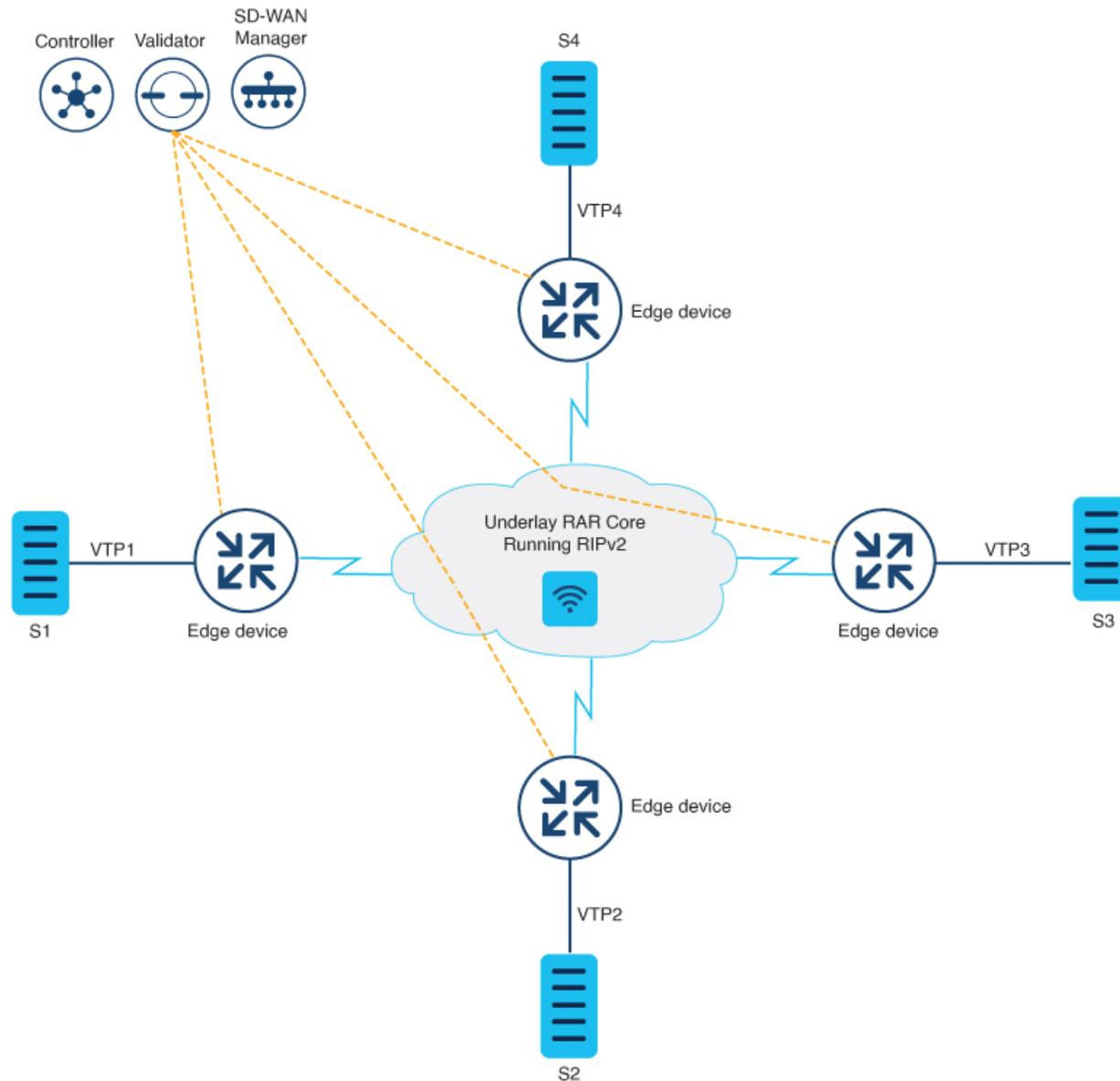
大規模なモバイルネットワークでは、距離と無線障害によりルーティングネイバーへの接続が中断されることがよくあります。該当する信号がルーティングプロトコルに到達しない場合、プロトコルタイマーを使用してネイバーのステータスが更新されます。ルーティングプロトコルには期間の長いタイマーがありますが、モバイルネットワークでは推奨されません。

2 つの Cisco IOS XE Catalyst SD-WAN デバイス間の接続は、可変帯域幅と制限付きバッファリングを使用する PPPoE 接続を介して行われます。OSPFv3 および EIGRP は、サポートされているルーティングプロトコルです。

RAR の概要

次のトポロジは、Cisco IOS XE Catalyst SD-WAN デバイス での RAR 展開を示しています。

図 8: RAR アーキテクチャ



- 4 つの Cisco IOS XE Catalyst SD-WAN デバイスは、デバイスの物理インターフェイスに接続された無線を介して相互に接続されます。
- PPPoE-RAR の設定は 3 つのルータのすべてで行われ、アンダーレイ RAR ネットワークが確立されると、ネットワークで Cisco Catalyst SD-WAN トンネルが形成されます。
- ループバック インターフェイスは、WAN インターフェイスとして機能し、仮想マルチポイント インターフェイス (VMI) にバインドします。その後、VMI インターフェイスが物理インターフェイスにバインドします。
- 任意の 2 つのデバイス間の PPP 接続は、アンダーレイネットワークとして機能します。

- Cisco Catalyst SD-WAN トンネルは、PPPoE-RAR アンダーレイネットワークを介して確立されます。
- Cisco SD-WAN Manager、Cisco SD-WAN コントローラ、および Cisco SD-WAN Validator は、展開シナリオで無線接続を介して接続されます。

モバイルアドホック ネットワーク (MANET)

デバイスから無線への通信に使用される MANET は、アドホック ネットワーキングアプリケーションで IP ルーティングとモバイル無線通信を統合する際に直面する課題に対処します。MANET ルーティングプロトコルは、MANET ルータ間のシグナリングを提供します。これには、ネットワーク内の MANET ルーティングプロトコルシグナリングの範囲限定フラッドイングやポイントツーポイント配信が含まれます。

RAR のシステムコンポーネント

無線対応ルーティング (RAR) 機能は、PPPoE、仮想マルチポイント インターフェイス (VMI)、QoS、ルーティングプロトコル インターフェイス、RAR プロトコルなどのさまざまなコンポーネントで構成される MANET (モバイルアドホック ネットワーク) インフラストラクチャを使用して導入されます。

Point-to-Point Protocol over Ethernet (PPPoE)

PPPoE は、クライアントとサーバーの間の明確に定義された通信メカニズムです。RAR の導入では、無線が PPPoE クライアントの役割を果たし、ルータが PPPoE サーバーの役割を果たします。その結果、明確に定義された予測可能な通信メカニズムを提供しながら、無線とルータを疎結合することが可能になります。

PPPoE はセッションまたは接続指向プロトコルであるため、外部無線から IOS ルータへのポイントツーポイント無線周波数 (RF) リンクを拡張します。

PPPoE 拡張

PPPoE 拡張は、ルータが無線と通信するときに使用されます。PPPoE の Cisco IOS 導入では、個々のセッションは仮想アクセスインターフェイス (無線ネイバーへの接続) で表され、これらの PPPoE 拡張を使用して QoS を適用できます。

RFC5578 は、信頼ベースのフロー制御とセッションベースのリアルタイムリンクメトリックをサポートするための PPPoE の拡張を実現します。この拡張は、可変帯域幅および制限付きバッファリング機能 (無線リンクなど) を使用した接続に非常に役立ちます。

仮想マルチポイント インターフェイス (VMI)

PPPoE 拡張によってルータと無線間で通信するためのセットアップの大部分が実現しますが、VMI は、上位レイヤ (ルーティングプロトコルなど) が消費するイベントを管理および変換する必要に対処します。また、VMI はバイパスモードで動作します。

バイパスモードでは、無線ネイバーを表すすべての仮想アクセスインターフェイス（VAI）がルーティングプロトコル OSPFv3 および EIGRP に明示されるため、ルーティングプロトコルは、ユニキャストとマルチキャスト両方のルーティングプロトコルトラフィックに関してそれぞれの VAI と直接通信します。

集約モードでは、VMI がルーティングプロトコル（OSPF）に明示されるため、ルーティングプロトコルは VMI を活用して効率を最適化できます。ネットワークネイバーが、VMI でのブロードキャストおよびマルチキャスト機能を備えたポイントツーマルチポイントリンク上のネットワークの集合と見なされる場合、VMI は、PPPoE から作成された複数の仮想アクセスインターフェイスの集約に役立ちます。VMI は、単一のマルチアクセスレイヤ2ブロードキャスト対応インターフェイスを提供します。VMI レイヤは、ユニキャストルーティングプロトコルトラフィックを適切な P2P リンク（仮想アクセスインターフェイス）にリダイレクトし、フローする必要があるすべてのマルチキャスト/ブロードキャストトラフィックを複製します。ルーティングプロトコルは単一のインターフェイスと通信するため、ネットワークの完全性に影響を与えることなく、トポロジデータベースのサイズが縮小されます。

RAR の設定

Cisco SD-WAN Manager を使用して RAR を設定するには、[CLI アドオン機能テンプレートを作成し、デバイステンプレートに添付します。](#)

ここでは、CLI アドオンテンプレートに追加できる RAR の設定例を示します。

RAR のサービスの設定

```
policy-map type service rar-lab
  pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
  !
```

OSPF ルーティングの設定

```
router ospfv3 1
  router-id 10.0.0.1
  !
  address-family ipv4 unicast
    redistribute connected metric 1 metric-type 1
    log-adjacency-changes
  exit-address-family
  !
  address-family ipv6 unicast
    redistribute connected metric-type 1
    log-adjacency-changes
  exit-address-family
  !
ip local pool PPPoEpool2 192.0.2.0 192.0.2.1
```

RAR の設定

```
interface GigabitEthernet0/0/0
```

```
no shutdown
no mop enabled
no mop sysid
negotiation auto
pppoe enable group PPPOE_RAR

interface vmil
ip address 10.0.0.0 255.255.255.0
ipv6 enable
physical-interface GigabitEthernet0/0/0
mode bypass
exit
interface Virtual-Template1
no shutdown
ip unnumbered vmil
ipv6 enable
ospfv3 1 network manet
ospfv3 1 ipv4 area 0
ospfv3 1 ipv6 area 0
exit

interface Tunnell100
no shutdown
ip unnumbered Loopback100
tunnel source Loopback100
tunnel mode sdwan
exit

interface Loopback100
tunnel-interface
encapsulation ipsec
color mpls
no allow-service bgp
allow-service dhcp
exit

router ospfv3 1
router-id 10.0.0.1
address-family ipv4 unicast
log-adjacency-changes
redistribute connected
redistribute connected metric 1 metric-type 1
exit-address-family
!
address-family ipv6 unicast
log-adjacency-changes
redistribute connected
redistribute connected metric-type 1
exit-address-family
```

次の例では、PPPoE 拡張セッションでの QoS プロビジョニングについて説明します。

```
policy-map rar_policer
class class-default
police 10000 2000 1000 conform-action transmit exceed-action drop violate-action
drop
policy-map rar_shaper
class class-default
shape average percent 1
```

```
interface Virtual-Template2
 ip address 192.0.2.255 255.255.255.0
 no peer default ip address
 no keepalive
 service-policy input rar_policer
end
```

バイパスモードでの RAR 機能の設定

次に、バイパスモードにおける RAR のエンドツーエンド設定の例を示します。



- (注) RAR の設定を開始する前に、まず **subscriber authorization enable** コマンドを設定して RAR セッションを起動する必要があります。許可を有効にしないと、ポイントツーポイント プロトコルはこれを RAR セッションとして認識せず、PPPoE プロトコルで *manet_radio* がタグ付けされない場合があります。デフォルトでは、設定にバイパスモードが表示されません。モードがバイパスとして設定されている場合にのみ表示されます。

RAR のサービスの設定

```
policy-map type service rar-lab
 pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

ブロードバンドの設定

```
interface pppoe VMI2
 virtual-template 2
 service profile rar-lab
!
interface GigabitEthernet0/0/0
 description Connected to Client1
 negotiation auto
 pppoe enable group VMI2
!
```

RAR のサービスの設定

```
policy-map type service rar-lab
 pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

バイパスモードの設定

- 仮想テンプレートで明示的に設定された IP アドレス

```
interface Virtual-Template2
 ip address 192.0.2.255 255.255.255.0
```

```

no ip redirects
peer default ip address pool PPPoEpool2
ipv6 enable
ospfv3 1 network manet
ospfv3 1 ipv4 area 0
ospfv3 1 ipv6 area 0
no keepalive
service-policy input rar_policer Or/And
service-policy output rar_shaper

```

- 仮想テンプレートで設定された番号なしの VMI

```

interface Virtual-Template2
ip unnumbered vmi2
no ip redirects
peer default ip address pool PPPoEpool2
ipv6 enable
ospfv3 1 network manet
ospfv3 1 ipv4 area 0
ospfv3 1 ipv6 area 0
no keepalive
service-policy input rar_policer Or/And
service-policy output rar_shaper

```

バイパスモードでの仮想マルチポイント インターフェイスの設定

```

interface vmi2 //configure the virtual multi interface
ip address 192.0.2.255 255.255.255.0
physical-interface GigabitEthernet0/0/0
mode bypass

interface vmi3//configure the virtual multi interface
ip address 192.0.2.255 255.255.255.0
physical-interface GigabitEthernet0/0/1
mode bypass

```

集約モードでの RAR 機能の設定

次に、集約モードにおける RAR のエンドツーエンド設定の例を示します。



- (注) RAR を設定する前に、まず **subscriber authorization enable** コマンドを設定して RAR セッションを起動する必要があります。許可を有効にしないと、ポイントツーポイント プロトコルはこれを RAR セッションとして認識せず、PPPoE で manet_radio がタグ付けされない場合があります。

RAR のサービスの設定

```

policy-map type service rar-lab
pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

ブロードバンドの設定

```
bba-group pppoe VMI2
  virtual-template 2
  service profile rar-lab

!
interface GigabitEthernet0/0/0
  description Connected to Client1
  negotiation auto
  pppoe enable group VMI2

!
```

RAR のサービスの設定

```
policy-map type service rar-lab
  pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

集約モードでの設定

```
interface Virtual-Template2
  ip unnumbered vmi2
  no ip redirects
  no peer default ip address
  ipv6 enable
  no keepalive
  service-policy input rar_policer Or/And
  service-policy output rar_shaper
```



第 6 章

VPN 間のルートリーク



- (注) 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

表 45: 機能の履歴

機能名	リリース情報	説明
グローバル VRF とサービス VPN 間のルートリーク	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a Cisco vManage リリース 20.3.1	この機能を使用すると、グローバル VRF とサービス VPN の間でルートを双方向にリークできます。ルートリークにより、ハブのパイパスが可能になり、移行されたブランチが移行されていないブランチに直接アクセスできるため、サービスの共有が可能になり、移行のユースケースで役立ちます。
OSPF、EIGRP プロトコルへの複製された BGP ルートの再配布	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能を使用すると、グローバル VRF とサービス VPN の間で BGP ルートをリーク（または複製）し、リークした BGP ルートを再配布できます。EIGRP および OSPF プロトコルにリークされたルートの再配布は、対応する VRF に BGP ルートを複製した後に行われます。

機能名	リリース情報	説明
BGP、OSPF、および EIGRP プロトコルへの複製ルートの再配布	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能を使用すると、次の項目を設定できます。 Cisco IOS XE Catalyst SD-WAN デバイス上の BGP、OSPF、および EIGRP プロトコルのグローバル VRF とサービス VPN 間のリークまたは複製ルートの再配布 MPLS ルートよりも OMP ルートを優先する OMP アドミニストレーティブ ディスタンス オプション リークされたルートが到達可能かどうかを追跡する VRRP トラッキング。
サービス VPN 間のルートリーク	Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能を使用すると、同じエッジデバイスのサービス VPN 間でルートをリークできます。 ルートリーク機能により、Cisco IOS XE Catalyst SD-WAN デバイスでの接続、スタティック、BGP、OSPF、および EIGRP について、サービス VPN 間で複製されたルートを再配布できます。

- [サポートされているプロトコル \(138 ページ\)](#)
- [ルートリークと再配布の制約事項 \(139 ページ\)](#)
- [ルートリークに関する情報 \(140 ページ\)](#)
- [Cisco SD-WAN Manager を使用したルートリーク設定のワークフロー \(143 ページ\)](#)
- [CLI を使用したルートリークの設定と確認 \(150 ページ\)](#)
- [CLI を使用したグローバル VRF とサービス VPN 間のルート再配布の設定 \(156 ページ\)](#)
- [ルートの再配布の確認 \(158 ページ\)](#)
- [CLI テンプレートを使用したサービス VPN 間のルートリークの設定 \(160 ページ\)](#)
- [CLI を使用したサービス VPN 間ルートリーク設定の確認 \(161 ページ\)](#)
- [CLI を使用したリークされたサービス VPN を追跡するための VRRP トラッカーの設定 \(162 ページ\)](#)
- [VRRP トラッキングの確認 \(164 ページ\)](#)
- [ルートリークの設定例 \(165 ページ\)](#)

サポートされているプロトコル

グローバル VRF とサービス VPN 間のルートリークに対して、次のプロトコルがサポートされています。

- 接続されている状態
- スタティック
- BGP
- OSPF
- EIGRP

次のプロトコルは、サービス VPN とグローバル VRF 間のルートの再配布でサポートされる宛先および送信元プロトコルです。

送信元プロトコル

- 接続されている状態
- スタティック
- BGP
- OSPF
- EIGRP

宛先プロトコル

- BGP
- OSPF
- EIGRP



(注) EIGRP プロトコルは、サービス VPN でのみ使用でき、グローバル VRF では使用できません。したがって、ルートリークは、サービス VPN からグローバル VRF へのルートに対してのみサポートされます。

ルートリークと再配布の制約事項

- EIGRP プロトコルは、サービス VRF でのみ使用でき、グローバル VRF では使用できません。したがって、グローバル VRF からサービス VRF へのルート、および EIGRP プロトコルのサービス VRF 間のルートでは、ルートリークはサポートされません。
- サービス側 NAT は、グローバル VRF とサービス VRF の間のルートリークではサポートされません。
- NAT は、トランスポート VRF ルートリークではサポートされません。
- IPv6 アドレスファミリーはサポートされません。

- 各サービス VRF は、最大 1000 ルートをリーク（インポートおよびエクスポート）できません。
- リークされたルートのフィルタリングに使用されるルートマップでは、プレフィックスリスト、タグ、およびメトリックのみを照合できます。
- マルチテナント機能を備えた Cisco IOS XE Catalyst SD-WAN デバイスでのサービス VRF 間ルートルークはサポートされません。
- オーバーレイループを防止するために、Overlay Management Protocol (OMP) ルートは VRF ルートルークに参加しません。
- Cisco SD-WAN のエクスポートポリシーを使用したさまざまなデバイスまたはサイト間のルートルークはサポートされません。
- EIGRP での再配布では、ベストパスを選択するために帯域幅、負荷、信頼性、遅延、および MTU の設定が必要です。
- **all** キーワードを使用したルート複製は推奨されません。
- 集中型ポリシーを使用したルートルークはサポートされません。
- VRF のルートルークを設定する際には、ルートループを防止するために、**global-address-family ipv4** コマンドの下の **route-replicate** コマンドで、unicast オプションの protocol としてキーワード **all** を指定しないでください。

```
global-address-family ipv4
  route-replicate from vrf <vrf> unicast all
```

- この例に示されているように、キーワード **all** を特定の protocol 名に置き換える必要があります。

```
global-address-family ipv4
  route-replicate from vrf <vrf> unicast connected
```

ルートルークに関する情報

グローバル VRF とサービス VPN 間のルートルーク

Cisco Catalyst SD-WAN ソリューションを使用すると、VPN を使用してネットワークをセグメント化できます。グローバルまたはデフォルト VRF（トランスポート VPN）とサービス VPN 間のルートルークにより、複数の VPN がアクセスする必要がある共通サービスを共有できます。この機能を使用すると、グローバル VRF（別名、トランスポート VPN）とサービス VPN の間で双方向のルートルークを介してルートが複製されます。VRF 間のルートルークは、ルーティング情報ベース（RIB）を使用して行われます。



- (注) Cisco Catalyst SD-WAN のコンテキストでは、VRF と VPN という用語は同じ意味で使用されません。Cisco IOS XE Catalyst SD-WAN デバイスは、セグメンテーションとネットワーク分離に VRF を使用しますが、VPN 機能テンプレートは、Cisco SD-WAN Manager を使用してこれらを設定するために使用されます。Cisco SD-WAN Manager を使用して Cisco IOS XE Catalyst SD-WAN デバイスの VPN を設定すると、Cisco SD-WAN Manager は自動的に VPN 設定を VRF 設定に変換します。

ルーティングネイバーにルートをリークするには、グローバル VRF とサービス VPN の間でリークされたルートを再配布します。

リークされたルートの OMP アドミニストレーティブ ディスタンス

Cisco SD-WAN オーバーレイ管理プロトコル (OMP) アドミニストレーティブ ディスタンスを低い値に設定すると、ブランチ間ルーティングシナリオでリークされたルートよりも優先して、OMP ルートを優先ルートおよびプライマリルートとして設定できます。

次の点に基づいて、Cisco IOS XE Catalyst SD-WAN デバイスの OMP アドミニストレーティブ ディスタンスを設定します。

- グローバル VRF レベルとサービス VRF レベルの両方で OMP アドミニストレーティブ ディスタンスを設定すると、VRF レベルの設定でグローバル VRF レベルの設定がオーバーライドされます。
- サービス VRF をグローバル VRF よりも低いアドミニストレーティブ ディスタンスで設定すると、サービス VRF を除き、残りすべての VRF でグローバル VRF からのアドミニストレーティブ ディスタンスの値が使用されます。

Cisco SD-WAN Manager を使用して OMP アドミニストレーティブ ディスタンスを設定するには、「[Configure Basic VPN Parameters](#)」および「[Configure OMP Using SD-WAN Manager Templates](#)」を参照してください。

CLI を使用して OMP アドミニストレーティブ ディスタンスを設定するには、「[CLI を使用した OMP の設定](#)」の「OMP アドミニストレーティブ ディスタンスの設定」を参照してください。

サービス VRF 間ルートリーク

サポート対象の最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a、Cisco vManage リリース 20.9.1。

サービス VRF 間ルートリーク機能は、サービス VRF 間の選択的ルートを同じサイト上の発信元デバイスにリークする機能を提供します。

Cisco SD-WAN コントローラを使用するときに発生するルーティング拡張性の課題を解決するために、エッジデバイスで VRF 間のルートをリークできます。

Cisco SD-WAN Manager を使用してサービス VRF 間ルートリーク機能を設定するには、「[サービス VRF 間のルートリークの設定](#)」を参照してください。

CLIを使用してサービス VRF 間ルートルーク機能を設定するには、「[CLIを使用したサービス VRF 間のルートルークの設定](#)」を参照してください。

リークされたサービス VPN に VRRP トラッカーを使用する

Virtual Router Redundancy Protocol (VRRP) は、リークされたルートが到達可能かどうかをトラックできます。トラック対象ルートに到達できない場合、VRRP は、VRRP グループの優先順位を変更します。VRRP は新しいプライマリルータの選択をトリガーできます。VRRP トラッカーは、VRRP 設定に含まれるルーティングインスタンスのルーティングテーブル内のルートの存在に基づいて、ルートが到達可能かどうかを判断します。

Cisco SD-WAN Manager を使用してリークされたサービス VPN を追跡するように VRRP トラッカーを設定するには、「[Configure VRRP for Cisco VPN Interface Ethernet template](#)」を参照してください。

CLIを使用してリークされたサービス VPN を追跡するように VRRP トラッカーを設定するには、「[CLIを使用したリークされたサービス VPN を追跡するための VRRP トラッカーの設定](#)」を参照してください。

ルートルークの機能

- グローバル VRF とサービス VPN 間のルートを直接リークできます。
- 複数のサービス VPN がグローバル VRF にリークされる可能性があります。
- 複数のサービス VRF の同じサービス VRF へのリークがサポートされています。
- グローバル VRF とサービス VPN の間でルートがリークまたは複製される場合、メトリック、送信元 VPN 情報、タグ、アドミニストレーティブ ディスタンス、ルートの起点などのルートプロパティは保持されます。
- ルートマップを使用して、リークされたルートを制御できます。
- ルートマップでは、照合操作を使用して、ルートをリークする前にルートをフィルタリングできます。
- この機能は、Cisco SD-WAN Manager と CLI の両方で設定できます。

ルートルークのユースケース

- **サービスプロバイダーのセントラルサービス**：MPLS の SP セントラルサービスは、VPN ごとに複製することなく直接アクセスできます。これにより、セントラルサービスへのアクセスがより簡単かつ効率的になります。
- **移行**：ルートルークにより、Cisco SD-WAN に移行したブランチは、ハブをバイパスして移行されていないブランチに直接アクセスできるため、アプリケーションの SLA が向上します。
- **集中型ネットワーク管理**：コントロールプレーンとサービス側の機器をアンダーレイで管理できます。

- **PCI 準拠に関する小売業者の要件**：サービス VRF のルートリークは、VRF トラフィックが、PCIに準拠しながら、同じブランチルータ上のゾーンベースファイアウォールを通過する場合に使用されます。

ルートプリファレンスの特定方法

グローバル VRF とサービス VPN の間でルートが複製またはリークされた場合、次のルールによってルートプリファレンスが決まります。

あるデバイスが 2 つの送信元からルートを受信し、両方のルートで同じ送信元 VRF が使用されていて一方のルートが複製される場合、複製されないルートが優先されます。

前述のルールが適用されない場合、次のルールに従い、以下の順番でルートプリファレンスが決まります。

1. アドミントレーティブ ディスタンスが小さいルートが優先されます。
2. デフォルトのアドミントレーティブ ディスタンスが小さいルートが優先されます。
3. レプリケートされたルートよりもレプリケートされていないルートが優先されます。
4. 元の VRF 名を比較します。辞書の観点から VRF 名が小さいルートが優先されます。
5. 元のサブアドレスファミリを比較します。マルチキャストルーティングよりもユニキャストルーティングが優先されます。
6. 最も古いルートが優先されます。

Cisco SD-WAN Manager を使用したルートリーク設定のワークフロー

1. ローカライズ型ポリシーを設定し、有効にして、ルートポリシーを添付します。
2. グローバル VPN とサービス VPN 間のルートリーク機能を設定して有効にします。
3. サービス VPN 間のルートリーク機能を設定して有効にします。
4. サービス側の VPN 機能テンプレートをデバイステンプレートに添付します。

ローカライズされたルートポリシーの設定

ルートポリシーの設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。
2. **[ローカライズ側ポリシー (Localized Policy)]** を選択します。

3. [Custom Options] ドロップダウンの [Localized Policy] で [Route Policy] を選択します。
4. [Add Route Policy] をクリックし、[Create New] を選択します。
5. ルートポリシーの名前と説明を入力します。
6. 左側のペインで、[シーケンスタイプの追加 (Add Sequence Type)] をクリックします。
7. 右側のペインで、[シーケンスルールの追加 (Add Sequence Rule)] をクリックして、ポリシーに単一のシーケンスを作成します。デフォルトでは [マッチ (Match)] が選択されています。
8. [Protocol] ドロップダウンリストから目的のプロトコルを選択します。オプションは、[IPv4]、[IPv6]、またはその両方です。
9. マッチ条件をクリックします。
10. 左側に、マッチ条件の値を入力します。
11. 右側に、ポリシーが一致した場合に実行するアクションを入力します。
12. [マッチとアクションの保存 (Save Match and Actions)] をクリックして、シーケンスルールを保存します。
13. どのルート ポリシー シーケンスルールにも一致するパケットがない場合、デフォルトのアクションはパケットをドロップすることです。デフォルトのアクションを変更するには、次の手順を実行します。
 1. 左側のペインで [Default Action] をクリックします。
 2. [鉛筆 (Pencil)] アイコンをクリックします。
 3. デフォルトのアクションを [Accept] に変更します。
 4. [Save Match and Actions] をクリックします。
14. [Save Route Policy] をクリックします。

ルートポリシーの追加

1. Cisco SD-WAN Manager メニューから、[Configuration] > [Policies] の順に選択します。
2. [Localized Policy] を選択します。
3. [Add Policy] をクリックします。
4. ローカルポリシーウィザードで、[Configure Route Policy] オプションが表示されるまで [Next] をクリックします。
5. [Add Route Policy] をクリックし、[Import Existing] を選択します。
6. [Policy] ドロップダウンから、作成されたルートポリシーを選択します。[Import] をクリックします。

7. [Next] をクリックします。
8. [Policy Name] にポリシー名を入力し、[Description] に説明を入力します。
9. [Preview] をクリックして、CLI 形式でポリシー設定を表示します。
10. [Save Policy] をクリックします。

デバイステンプレートへのローカライズ型ポリシーの関連付け



(注) 以前に作成したローカライズ型ポリシーを利用するための最初の手順は、デバイステンプレートに関連付けることです。

1. Cisco SD-WAN Manager メニューから、[Configuration] > [Templates] を選択します。
2. [Device Templates] をクリックし、目的のテンプレートを選択します。
3. [...] をクリックして、[Edit] をクリックします。
4. [Additional Templates] をクリックします。
5. [Policy] ドロップダウンから、作成されたローカライズ型ポリシーを選択します。
6. [Update] をクリックします。



(注) ローカライズ型ポリシーがデバイステンプレートに追加されると、[Update] オプションを選択することにより、このデバイステンプレートに関連付けられているすべてのデバイスに設定変更がすぐにプッシュされます。複数のデバイスがデバイステンプレートに関連付けられている場合は、複数のデバイスが変更されていることを示す警告メッセージが表示されます。

7. [Next] をクリックし、[Configure Devices] をクリックします。
8. 検証プロセスが完了するまで待って、Cisco SD-WAN Manager からデバイスに設定をプッシュします。

グローバル VRF とサービス VPN 間のルートリークの設定および有効化

1. Cisco SD-WAN Manager メニューから、[Configuration] > [Templates] を選択します。
2. ルートリークを設定するには、[Feature Templates] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] は [Feature] と呼ばれます。

次のいずれかを実行します。

- 機能テンプレートを作成するには、次の手順を実行します。
 1. [Add template] をクリックします。デバイスのリストからデバイスを選択します。選択したデバイスで使用可能なテンプレートが右側のペインに表示されます。
 2. 右側のペインから [Cisco VPN] テンプレートを選択します。



(注) ルートリークはサービス VPN にのみ設定できますしたがって、[Basic Configuration] の下の [VPN] フィールドに入力する番号は、1 ~ 511 または 513 ~ 65527 のいずれかです。

基本設定、DNS、Virtual Router Redundancy Protocol (VRRP) トラッキングなどのさまざまな VPN パラメータの設定の詳細については、「[Configure a VPN Template](#)」を参照してください。ルートリーク機能に固有の詳細については、ステップ c に進みます。

3. [Template Name] と [Description] に機能テンプレートの名前と説明をそれぞれ入力します。
4. [Description] フィールドの下にある [Global Route Leak] をクリックします。
5. グローバル VRF からルートを一リークするには、[Add New Route Leak from Global VPN to Service VPN] をクリックします。
 1. [Route Protocol Leak from Global to Service] ドロップダウンリストで、[Global] を選択してプロトコルを選択します。それ以外の場合は、[Device-Specific] を選択してデバイス固有の値を使用します。
 2. [Route Policy Leak from Global to Service] ドロップダウンリストで、[Global] を選択します。次に、ドロップダウンリストから使用可能なルートポリシーのいずれかを選択します。
 3. [Redistribute to protocol (in Service VPN)] フィールドで、[Add Protocol] をクリックします。
[Protocol] ドロップダウンリストで、[Global] を選択してプロトコルを選択します。それ以外の場合は、[Device-Specific] を選択してデバイス固有の値を使用します。
[Redistribution Policy] ドロップダウンリストで、[Global] を選択します。次に、ドロップダウンリストから使用可能な再配布ポリシーのいずれかを選択します。
 4. [Add] をクリックします。
6. サービス VPN からグローバル VRF にルートを一リークするには、[Add New Route Leak from Service VPN to Global VPN] をクリックします。

1. [Route Protocol Leak from Service to Global] ドロップダウンリストで、[Global] を選択してプロトコルを選択します。それ以外の場合は、[Device-Specific] を選択してデバイス固有の値を使用します。
2. [Route Policy Leak from Service to Global] ドロップダウンリストで、[Global] を選択します。次に、ドロップダウンリストから使用可能なルートポリシーのいずれかを選択します。
3. [Redistribute to protocol (in Global VPN)] フィールドで、[Add Protocol] をクリックします。
[Protocol] ドロップダウンリストで、[Global] を選択してプロトコルを選択します。それ以外の場合は、[Device-Specific] を選択してデバイス固有の値を使用します。
[Redistribution Policy] ドロップダウンリストで、[Global] を選択します。次に、ドロップダウンリストから使用可能な再配布ポリシーのいずれかを選択します。
4. [Add] をクリックします。
7. [Save/Update] をクリックします。設定は、機能テンプレートがデバイステンプレートに添付されるまで有効になりません。
8. リークされたルートを、Cisco SD-WAN Manager を使用して再配布するには、[CLI アドオン機能テンプレート](#)を使用して、使用環境に適した設定を入力します。次に例を示します。

```
Device (config)# router ospf 65535
Device (config-router)# redistribute vrf 1 ospf 103

Device (config)# router eigrp vpn
Device (config-router)# address-family ipv4 vrf 1 autonomous-system 50
Device (config-router-af)# topology base
Device (config-router-af-topology)# redistribute vrf global ospf 65535

metric 1 2 3 4 5
```

CLI アドオンテンプレートを作成したら、ルートを再配布するプロトコルテンプレートに添付する必要があります。この例では、EIGRP テンプレートに添付します。

- 既存の機能テンプレートを変更するには、次の手順を実行します。
 1. 変更する機能テンプレートを選択します。
 2. テーブルの行の横にある [...] をクリックし、[Edit] をクリックします。
 3. [Global Route Leak] をクリックします。

4. 情報を編集するには、[Add New Route Leak from Global VPN to Service VPN] または [Add New Route Leak from Service VPN to Global VPN] の下にあるテーブルで、[Edit] をクリックします。

[Update Route Leak] ダイアログボックスが表示されます。

5. 機能テンプレートを作成するステップ d のすべての操作を実行します。
機能テンプレートを作成するステップ c のすべての操作を実行します。
6. [Save Changes] をクリックします。
7. [更新 (Update)] をクリックします。



- (注) ・設定は、サービス VPN 機能テンプレートがデバイステンプレートに添付されるまで有効になりません。

サービス VPN 間のルートルークの設定

サポート対象の最小リリース : Cisco vManage リリース 20.9.1

1. Cisco SD-WAN Manager メニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックします。
3. デバイスの **Cisco VPN** テンプレートに移動します。



- (注) **VPN** テンプレートを作成するには、「[VPN テンプレートの作成](#)」を参照してください。

4. [Route Leak] をクリックします。
5. [Route Leak between Service VPN] をクリックします。
6. [Add New Inter Service VPN Route Leak] をクリックします。
7. [Source VPN] ドロップダウンリストから、[Global] を選択して、ルートをリークするサービス VPN を設定します。それ以外の場合は、[Device-Specific] を選択してデバイス固有の値を使用します。

Cisco IOS XE Catalyst SD-WAN デバイスのサービス側データトラフィック用に、VPN 1 ~ 511 および 513 ~ 65530 の範囲内でサービス VPN を設定できます (VPN 512 は、ネットワーク管理トラフィック用に予約済みです。VPN 0 は、設定された WAN トランスポート インターフェイスを使用した制御トラフィック用に予約済みです)。

8. [Route Protocol Leak to Current VPN] ドロップダウンリストから、[Global] を選択して、現在の VPN へのルートリークを有効にするルートプロトコルを選択します。それ以外の場合は、[Device-Specific] を選択してデバイス固有の値を使用します。
ルートリークについては、[Connected]、[Static]、[OSPF]、[BGP]、および [EIGRP] プロトコルを選択できます。
9. [Route Policy Leak to Current VPN] ドロップダウンリストから、[Global] を選択して、現在の VPN へのルートリークを有効にするルートポリシーを選択します。それ以外の場合は、[Device-Specific] を選択してデバイス固有の値を使用します。
利用可能なルートポリシーがない場合、このフィールドは無効になります。
10. [Redistribute to protocol (in Service VPN)] を設定するには、[Add Protocol] をクリックします。
[Protocol] ドロップダウンリストから、[Global] を選択して、プロトコルを選択します。それ以外の場合は、[Device-Specific] を選択してデバイス固有の値を使用します。
再配布については、[Connected]、[Static]、[OSPF]、[BGP]、および [EIGRP] プロトコルを選択できます。
(任意) [Redistribution Policy] ドロップダウンリストから、[Global] を選択します。次に、ドロップダウンリストから使用可能な再配布ポリシーのいずれかを選択します。
利用可能なルートポリシーがない場合、このフィールドは無効になります。
11. [Add] をクリックします。
12. [Save] をクリックします。

サービス側のVPN機能テンプレートのデバイステンプレートへの添付

1. Cisco SD-WAN Manager メニューから、[Configuration] > [Templates] を選択します。
2. [Device Templates] をクリックし、目的のテンプレートを選択します。
3. [...] をクリックして、[Edit] をクリックします。
4. [Service VPN] をクリックします。
5. [Add VPN] をクリックします。[Available VPN Templates] ペインに示されているサービス VPN 機能テンプレートを選択します。右矢印をクリックしてテンプレートを [Selected VPN Templates] リストに追加します。
6. テンプレートが左側 ([Available VPN Templates]) から右側 ([Selected VPN Templates]) に移動したら、[Next] をクリックします。
7. [Add] をクリックします。
8. [更新 (Update)] をクリックします。
9. [Next] をクリックし、[Configure Devices] をクリックします。

- 最後に、検証プロセスが完了するのを待って、Cisco SD-WAN Manager からデバイスに設定をプッシュします。

CLI を使用したルートリークの設定と確認

例：グローバル VRF とサービス VPN 間のルートリーク

次に、グローバル VRF とサービス VPN 間のルートリークを設定する例を示します。この例では、VRF 103 がサービス VPN です。次に、接続ルートがグローバル VRF から VRF 103 にリークされる例を示します。同様に、同じ接続ルートが VRF 103 からグローバル VRF にリークされます。

```
vrf definition 103
!
  address-family ipv4
    route-replicate from vrf global unicast connected
!
global-address-family ipv4
  route-replicate from vrf 103 unicast connected
  exit-address-family
```

設定の確認



- (注) 出力では、リークされたルートは、リークされたルートの横にある+記号で表されます。例：C+ は、接続ルートがリークされたことを示します。

```
Device#show ip route
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, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
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
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from Pfr
& - replicated local route overrides by connected

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
O 10.1.14.0/24 [110/11] via 10.1.15.13, 00:02:22, GigabitEthernet1
C 10.1.15.0/24 is directly connected, GigabitEthernet1
L 10.1.15.15/32 is directly connected, GigabitEthernet1
O 10.1.16.0/24 [110/11] via 10.1.15.13, 00:02:22, GigabitEthernet1
C 10.1.17.0/24 is directly connected, GigabitEthernet2
L 10.1.17.15/32 is directly connected, GigabitEthernet2
172.16.0.0/12 is subnetted, 1 subnets
[170/10880] via 192.168.24.17(103), 01:04:13, GigabitEthernet5.103
192.168.0.0/16 is variably subnetted, 2 subnets, 2 masks
C + 192.0.2.0/24 is directly connected, GigabitEthernet5.103
```

```

L & 192.168.24.15/16 is directly connected, GigabitEthernet5.103
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 203.0.113.0/24 is directly connected, GigabitEthernet6
L 203.0.113.15/32 is directly connected, GigabitEthernet6
10.20.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 198.51.100.0/24 is directly connected, GigabitEthernet7
L 198.51.100.15/24 is directly connected, GigabitEthernet7
192.0.2.0/32 is subnetted, 1 subnets
O E2 100.100.100.100 [110/20] via 10.1.15.13, 00:02:22, GigabitEthernet1
172.16.0.0/32 is subnetted, 1 subnets
O E2 172.16.255.14 [110/20] via 10.1.15.13, 00:02:22, GigabitEthernet1

```

グローバル VRF からサービス VRF テーブルにリークされたルートの表示

show ip route vrf <vrfid> コマンドを使用して、グローバル VRF からサービス VRF テーブルにリークされたルートを表示します。



- (注) 出力では、リークされたルートは、リークされたルートの横にある+記号で示されます。例：C+ は、接続ルートがリークされたことを示します。

```

Device#show ip route vrf 103
Routing Table: 103
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, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
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
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
C + 10.0.1.0/24 is directly connected, GigabitEthernet9
L & 10.0.1.15/32 is directly connected, GigabitEthernet9
C + 10.0.20.0/24 is directly connected, GigabitEthernet4
L & 10.0.20.15/32 is directly connected, GigabitEthernet4
C + 10.0.100.0/24 is directly connected, GigabitEthernet8
L & 10.0.100.15/32 is directly connected, GigabitEthernet8
C + 10.1.15.0/24 is directly connected, GigabitEthernet1
L & 10.1.15.15/32 is directly connected, GigabitEthernet1
C + 10.1.17.0/24 is directly connected, GigabitEthernet2
L & 10.1.17.15/32 is directly connected, GigabitEthernet2
172.16.0.0/12 is subnetted, 1 subnets
D EX 172.16.20.20
[170/10880] via 192.168.24.17, 01:04:07, GigabitEthernet5.103
192.168.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 192.0.2.0/24 is directly connected, GigabitEthernet5.103
L 192.168.24.15/16 is directly connected, GigabitEthernet5.103
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C + 203.0.113.0/24 is directly connected, GigabitEthernet6
L & 203.0.113.15/32 is directly connected, GigabitEthernet6
10.20.0.0/8 is variably subnetted, 2 subnets, 2 masks
C + 198.51.100.0/24 is directly connected, GigabitEthernet7

```

```
L & 198.51.100.15/24 is directly connected, GigabitEthernet7
192.0.2.0/32 is subnetted, 1 subnets
```

例：リーク前のルートのフィルタリング

グローバル VRF とサービス VRF の間でリークされたルートをさらにフィルタリングするには、次の例に示すようにルートマップを適用できます。

```
vrf definition 103
!
 address-family ipv4
   route-replicate from vrf global unicast connected route-map myRouteMap permit 10
   match ip address prefix-list pList seq 5 permit 10.1.17.0/24
!
```

設定の確認



(注) 出力では、リークされたルートは、リークされたルートの横にある+記号で示されます。例：C+ は、接続ルートがリークされたことを示します。

```
Device#show ip route vrf 103

Routing Table: 1
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, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
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
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PFR
& - replicated local route overrides by connected

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C + 10.1.17.0/24 is directly connected, GigabitEthernet2
L & 10.1.17.15/32 is directly connected, GigabitEthernet2
m 10.1.18.0/24 [251/0] via 172.16.255.14, 19:01:28, Sdwan-system-intf
m 10.2.2.0/24 [251/0] via 172.16.255.11, 17:28:44, Sdwan-system-intf
m 10.2.3.0/24 [251/0] via 172.16.255.11, 17:26:50, Sdwan-system-intf
C 10.20.24.0/24 is directly connected, GigabitEthernet5
L 10.20.24.15/32 is directly connected, GigabitEthernet5
m 10.20.25.0/24 [251/0] via 172.16.255.11, 16:14:18, Sdwan-system-intf
172.16.0.0/32 is subnetted, 3 subnets
m 172.16.255.112 [251/0] via 172.16.255.11, 17:28:44, Sdwan-system-intf
O E2 172.16.255.117 [110/20] via 10.20.24.17, 1d11h, GigabitEthernet5
m 172.16.255.118 [251/0] via 172.16.255.11, 16:14:18, Sdwan-system-intf
```

リークされたルートをモニタするには、**show ip cef** コマンドを使用します。出力には、複製またはリークされたルートが表示されます。

```
Device#show ip cef 10.1.17.0 internal
10.1.17.0/24, epoch 2, flags [rcv], refcnt 6, per-destination sharing
[connected cover 10.1.17.0/24 replicated from 1]
```

```

sources: I/F
feature space:
Broker: linked, distributed at 4th priority
sublocks:
gsb Connected receive chain(0): 0x7F6B4315DB80
Interface source: GigabitEthernet5 flags: none flags3: none
Dependent covered prefix type cover need deagg, cover 10.20.24.0/24
ifnums: (none)
path list 7F6B47831168, 9 locks, per-destination, flags 0x41 [shble, hwcn]
path 7F6B3D9E7B70, share 1/1, type receive, for IPv4
receive for GigabitEthernet5
output chain:
receive

```

例：OSPF および EIGRP プロトコルへの BGP ルートの再配布

次に、BGP ルートをグローバル VRF からサービス VRF に複製する例を示します。

```

Device#config-transaction
Device(config)# vrf definition 2
Device(config-vrf)# address-family ipv4
Device(config-ipv4)# route-replicate from vrf global unicast bgp 1
Router(config-ipv4)# commit

```

グローバル VRF の BGP ルートをサービス VRF の EIGRP に再配布するための設定



- (注) 他のプロトコルへの BGP ルートの再配布は、bgp redistribute-internal 設定が BGP ルートに存在する場合にのみサポートされます。

```

Device#config-transaction
Device(config)# router eigrp test
Device(config-router)# address-family ipv4 unicast vrf 2 autonomous-system 100
Device(config-router-af)# topology base
Device(config-router-af-topology)# redistribute vrf global bgp 1 metric 10000 100 200 1
1500
Device(config-ipv4)# commit

```

```

* Here we are redistributing BGP routes in global VRF to EIGRP in VRF 2.
* Routes replication must be done before doing inter VRF redistribution.
-----

```

設定の確認

設定前にグローバル VRF に存在する BGP ルートの表示

```

Device#show ip route bgp
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, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
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
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

```

```
Gateway of last resort is not set

10.0.0.0/9 is subnetted, 1 subnets
B 172.16.255.1 [200/20] via 10.1.15.14, 00:00:25
Device#
```

* We have a BGP route in the global VRF.

設定前にサービス VRF に存在しない BGP ルートの表示

show ip route vrf <vrf id> [protocol] コマンドを使用して、サービス VRF テーブルの BGP ルートを表示します。

```
Device#show ip route vrf 2 bgp

Routing Table: 2
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, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
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
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PFR
& - replicated local route overrides by connected

Gateway of last resort is not set

Device#
```

* We do not have any BGP route in VRF 2.

設定後の BGP ルートの表示

show running config [configuration-hierarchy] | details コマンドを使用して、レプリケーションコンフィギュレーションが存在するかどうかを確認します。

```
Device#show running-config | section vrf definition 2
vrf definition 2
  rd 1:1
  route-target export 1:1
  route-target import 1:1
  !
  address-family ipv4
    route-replicate from vrf global unicast bgp 1
  exit-address-family
Device#
```

* We have successfully applied the route-replicate configuration.

* In our example we are replicating bgp 1 routes from global VRF to VRF 2.

設定後にグローバル VRF からサービス VRF に複製される BGP ルートの表示

show ip route vrf <vrf id> [protocol] コマンドを使用して、サービス VRF テーブルの BGP ルートを表示します。

```
Device#show ip route vrf 2 bgp
```

```

Routing Table: 2
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, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
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
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

```

```
Gateway of last resort is not set
```

```

      10.0.0.0/9 is subnetted, 1 subnets
B    +   172.16.255.1 [200/20] via 10.1.15.14, 00:04:01
Device#

```

```

* After route replication, we can see that the BGP route in the global VRF has been
replicated into VRF 2.
* + sign indicates replicated routes.
-----

```

BGP 再配布情報のない EIGRP 設定の表示

```

Device#show running-config | section router eigrp
router eigrp test
!
address-family ipv4 unicast vrf 2 autonomous-system 100
!
topology base
exit-af-topology
network 10.0.0.0
exit-address-family
Router#

```

EIGRP トポロジテーブルの表示

show eigrp address-family ipv4 vrf<vrf-num>topology コマンドを使用して、サービス VRF テーブルの BGP ルートを表示します。

```

Device#show eigrp address-family ipv4 vrf 2 topology
EIGRP-IPv4 VR(test) Topology Table for AS(100)/ID(10.10.10.2)
Topology(base) TID(0) VRF(2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.0.0.0/8, 1 successors, FD is 1310720
   via Connected, GigabitEthernet2

Device#

* EIGRP 100 is running on VRF 2.
-----

```

BGP 再配布後の EIGRP ルートの表示

show eigrp address-family ipv4 vrf<vrf-num>topology コマンドを使用して、EIGRP プロトコルに再配布される BGP ルートを表示します。

```

Device#show eigrp address-family ipv4 vrf 2 topology
EIGRP-IPv4 VR(test) Topology Table for AS(100)/ID(10.10.10.2)
  Topology(base) TID(0) VRF(2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.10.10.0/8, 1 successors, FD is 1310720
   via Connected, GigabitEthernet2
P 172.16.0.0/12, 1 successors, FD is 131072000
   via +Redistributed (131072000/0)

-Device#

* BGP route has been redistributed into EIGRP.

```

CLI を使用したグローバル VRF とサービス VPN 間のルート再配布の設定

1. グローバル コンフィギュレーション モードを開始して、BGP ルーティングプロセスを作成します。



- (注) **router eigrp** または **router ospf** を使用して、特定のルーティングプロトコルのルーティングプロセスを設定できます。次に、BGP ルーティングプロトコルの構文の例を示します。さまざまなプロトコルのコマンド構文については、[Cisco IOS XE SD-WAN 認定コマンドリファレンスガイド \[英語\]](#) を参照してください。

```

Device# config-transaction
Device(config)# router bgp autonomous-system-number

```

2. サービス VPN の IPv4 アドレスファミリを設定します。次に、BGP および EIGRP プロトコルのコマンド構文の例を示します。

- BGP プロトコル :

```

Device(config-router-af)# address-family ipv4 [unicast] [vrf vrf-name]

```

- EIGRP プロトコル :

```

Device(config-router-af)# address-family ipv4 vrf vrf-number

```

3. グローバル VRF とサービス VPN 間のルートを再配布します。ここでは、BGP、OSPF、および EIGRP プロトコルの構文を示します。

- サービス VPN からグローバル VRF にルートを再配布します。

- BGP プロトコル :

```

Device(config-router-af)# redistribute vrf vrf-name src_protocol
[src_protocol_id] [route-map route-map-name]

```

- OSPF プロトコル :

```
Device(config-router-af)# redistribute vrf vrf-name src_protocol
[src_protocol_id] [match {internal|external 1|external 2}] [metric
{metric-value}] [subnets] [route-map route-map-name]
```

- EIGRP プロトコル :

```
Device(config-router-af)# redistribute vrf vrf-name src_protocol
[src_protocol_id] [metric bandwidth-metric delay-metric reliability-metric
effective-bandwidth-metric mtu-bytes] [route-map route-map-name]
```

- グローバル VRF からサービス VPN へのルートを再配布します。

- BGP プロトコル :

```
Device(config-router-af)# redistribute vrf global src_protocol
[src_protocol_id] [route-map route-map-name]
```

- OSPF プロトコル :

```
Device(config-router-af)# redistribute vrf global src_protocol
[src_protocol_id] [match {internal|external 1|external 2}]
[subnets] [route-map route-map-name]
```

- EIGRP プロトコル :

```
Device(config-router-af)# redistribute vrf global src_protocol
[src_protocol_id] [metric bandwidth-metric delay-metric reliability-metric
effective-bandwidth-metric mtu-bytes]
```

次に、グローバル VRF とサービス VPN 間のルート再配布の設定例を示します。この例では、VRF 103 と VRF 104 がサービス VPN です。次に、BGP ルートがグローバル VRF から VRF 103、VRF 104 に再配布される例を示します。

```
config-transaction
router bgp 100

address-family ipv4 vrf 103
redistribute vrf global bgp 100 route-map test2
!
address-family ipv4 vrf 104
redistribute vrf global bgp 100 route-map test2
!
```

次に、グローバル VRF 65535 からサービス VRF に再配布される OSPF 内部ルートおよび外部ルートの設定例を示します。

この場合、**internal** および **external** キーワードの両方を使用して、すべての OSPF ルートがサービス VRF に再配布されます。

```
config-transaction
router ospf 1
redistribute vrf global ospf 65535 match internal external 1 external 2 subnets route-map
ospf-route-map
```

次に、サービス VPN からグローバル VRF に再配布される OSPF 内部ルートおよび外部ルートの設定例を示します。

```

config-transaction
router ospf 101
redistribute vrf 101 ospf 101 match internal external 1 external 2 metric 1 subnets
route-map ospf-route-map

```

次に、サービス VPN からグローバル VRF に再配布される BGP ルートの設定例を示します。

```

config-transaction
router bgp 50000
address-family ipv4 unicast
redistribute vrf 102 bgp 50000 route-map BGP-route-map

```

次に、グローバル VRF からサービス VPN に再配布される BGP ルートの設定例を示します。

```

config-transaction
router bgp 50000
address-family ipv4 vrf 102
redistribute vrf global bgp 50000

```

次に、EIGRP ルーティングプロセスでの設定時に、グローバル VRF から VRF 1 への BGP プロトコル、接続プロトコル、OSPF プロトコル、および静的プロトコルのルート再配布の設定例を示します。

```

config-transaction
router eigrp 101
address-family ipv4 vrf 1
redistribute vrf global bgp 50000 metric 1000000 10 255 1 1500
redistribute vrf global connected metric 1000000 10 255 1 1500
redistribute vrf global ospf 65535 match internal external 1 external 2 metric 1000000
10 255 1 1500
redistribute vrf global static metric 1000000 10 255 1 1500

```

ルートの再配布の確認

例 1:

次に、**show ip bgp** コマンドで **internal** キーワードを使用した場合の出力例を示します。次に、VRF 102 からのルートが複製された後、グローバル VRF に正常に再配布される例を示します。

```
Device# show ip bgp 10.10.10.10 internal
```

```

BGP routing table entry for 10.10.10.10/8, version 515
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
700000 70707
10.10.14.17 from 0.0.0.0 (172.16.255.15)
Origin IGP, aigp-metric 77775522, metric 7777, localpref 100, weight 32768, valid,
sourced, replicated, best
Community: 0:7227 65535:65535
Extended Community: SoO:721:75 RT:50000:102
rx pathid: 0, tx pathid: 0x0
net: 0x7FB320235DC0, path: 0x7FB320245DF8, pathext: 0x7FB3203A4660
flags: net: 0x0, path: 0x808040003, pathext: 0x81
attribute: 0x7FB38E5B6258, ref: 14
Updated on Jul 1 2021 01:16:36 UTC
vm5#

```

この出力では、ルートは VRF 102 からグローバル VRF に再配布されます。

次に、再配布のために複製されたルートを示す **show ip route** コマンドの出力例を示します。

```
Device# show ip route 10.10.10.10

Routing entry for 10.10.10.10/8
Known via "bgp 50000", distance 60, metric 7777
Tag 700000, type external,
replicated from topology(102)
Redistributing via ospf 65535, bgp 50000
Advertised by ospf 65535
bgp 50000 (self originated)
Last update from 10.10.14.17 5d15h ago
Routing Descriptor Blocks:
* 10.10.14.17 (102), from 10.10.14.17, 5d15h ago
opaque_ptr 0x7FB3202563A8
Route metric is 7777, traffic share count is 1
AS Hops 2
Route tag 700000
MPLS label: none
```

例 2 :

次に、**show ip bgp vpnv4 vrf** コマンドで **internal** キーワードを使用した場合の出力例を示します。

```
Device# show ip bgp vpnv4 vrf 102 209.165.201.0 internal

BGP routing table entry for 1:102:10.10.10.10/8, version 679
BGP routing table entry for 1:209.165.201.0/27, version 679
Paths: (1 available, best #1, table 102)
Advertised to update-groups:
4
Refresh Epoch 1
7111 300000
10.1.15.13 (via default) from 0.0.0.0 (172.16.255.15)
Origin IGP, aigp-metric 5755, metric 900, localpref 300, weight 32768, valid, sourced,
replicated, best
Community: 555:666
Large Community: 1:2:3 5:6:7 412789:412780:755
Extended Community: SoO:533:53 RT:50000:102
rx pathid: 0, tx pathid: 0x0
net: 0x7FB38E5C5718, path: 0x7FB3202668D8, pathext: 0x7FB38E69E960
flags: net: 0x0, path: 0x808040007, pathext: 0x181
attribute: 0x7FB320256798, ref: 7
Updated on Jul 6 2021 16:43:04 UTC
```

この出力では、ルートはグローバル VRF から VRF 102 に再配布されます。

次に、VRF 102 の再配布用に複製されたルートを示す **show ip route vrf** コマンドの出力例を示します。

```
Device# show ip route vrf 102 209.165.201.0

Routing Table: 102
Routing entry for 209.165.201.0/27
Known via "bgp 50000", distance 20, metric 900
Tag 7111, type external,
replicated from topology(default)
Redistributing via bgp 50000
Advertised by bgp 50000 (self originated)
Last update from 10.1.15.13 00:04:57 ago
Routing Descriptor Blocks:
* 10.1.15.13 (default), from 10.1.15.13, 00:04:57 ago
```

```
opaque_ptr 0x7FB38E5B5E98
Route metric is 900, traffic share count is 1
AS Hops 2
Route tag 7111
MPLS label: none
```

CLI テンプレートを使用したサービス VPN 間のルートリークの設定

サポート対象の最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a

CLI テンプレートの使用の詳細については、「[CLI Add-on Feature Templates](#)」および「[CLI Templates](#)」を参照してください。



- (注) デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

ここでは、Cisco IOS XE Catalyst SD-WAN デバイスでサービス VPN 間ルートリークを設定する CLI 設定例を示します。

- 同じデバイス上のサービス VRF 間でルートを複製します。

```
vrf definition vrf-number
address-family ipv4
route-replicate from vrf source-vrf-name unicast protocol [route-map
map-tag]
```

- サービス VPN 間で複製されたルートを再配布します。

サブネットは、bgp、nhrp、ospf、ospfv3、および static プロトコルタイプについてのみ設定できます。

```
router ospf process-id vrf vrf-number
redistribute vrf vrf-name protocol subnets [route-map map-tag]
```

次に、サービス VRF 間のルート複製および再配布の完全な設定例を示します。

```
vrf definition 2
rd 1:2
!
address-family ipv4
route-replicate from vrf 1 unicast static route-map VRF1_TO_VRF2
exit-address-family
!
!
ip prefix-list VRF1_TO_VRF2 seq 5 permit 10.10.10.97/32
!
route-map VRF1_TO_VRF2 permit 1
match ip address prefix-list VRF1_TO_VRF2
!
```

```
router ospf 2 vrf 2
 redistribute vrf 1 static route-map VRF1_TO_VRF2
```

CLI を使用したサービス VPN 間ルートトリーク設定の確認

サポート対象の最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a

次に、VRF 2 への再配布のために複製されたルートを示す **show ip route vrf** コマンドの出力例を示します。

```
Device# show ip route vrf 2
Routing Table: 2
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, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       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
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PFR
       & - replicated local route overrides by connected
```

Gateway of last resort is not set

```
          10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
S   +   10.10.10.97/32 [1/0] via 10.20.1.2 (1)
C     10.20.2.0/24 is directly connected, GigabitEthernet5
L     10.20.2.1/32 is directly connected, GigabitEthernet5
```

次に、VRF 1 から複製されたルートを示す **show ip cef vrf** コマンドの出力例を示します。

```
Device# show ip cef vrf 2 10.10.10.97 internal
10.10.10.97/32, epoch 0, RIB[S], refcnt 6, per-destination sharing
sources: RIB
feature space:
  IPRM: 0x00048000
  Broker: linked, distributed at 3rd priority
subblocks:
  Replicated from VRF 1
ifnums:
  GigabitEthernet3(9): 10.20.1.2
path list 7F890C8E2F20, 7 locks, per-destination, flags 0x69 [shble, rif, rcrsv, hwcn]

  path 7F890FB18F08, share 1/1, type recursive, for IPv4
    recursive via 10.20.1.2[IPv4:1], fib 7F890B609578, 1 terminal fib, v4:1:10.20.1.2/32

  path list 7F890C8E3148, 2 locks, per-destination, flags 0x49 [shble, rif, hwcn]
    path 7F890FB19178, share 1/1, type adjacency prefix, for IPv4
      attached to GigabitEthernet3, IP adj out of GigabitEthernet3, addr 10.20.1.2
7F890FAE4CD8
output chain:
  IP adj out of GigabitEthernet3, addr 10.20.1.2 7F890FAE4CD8
```

CLI を使用したリークされたサービス VPN を追跡するための VRRP トラッカーの設定

トラックを設定します。

1. グローバル コンフィギュレーション モードを開始し、IP ルートの状態を追跡し、トラッキング コンフィギュレーション モードを開始します。

```
Device# config-transaction  
Device(config)# track object-number {ip} route address|prefix-length {  
reachability | metric threshold}
```

2. VPN ルーティングおよび転送 (VRF) テーブルを設定します。

```
Device(config-track)# ip vrf vrf-name
```

3. 特権 EXEC モードに戻ります。

```
Device(config-track)# end
```

VRRP バージョン 2 (VRRPv2) を設定します。

1. ギガビットイーサネットなどのインターフェイスタイプを設定します。

```
Device(config)# interface type number [name-tag]
```

2. VRF インスタンスをギガビットイーサネットインターフェイスに関連付けます。

```
Device(config-if)# vrf forwarding vrf-name
```

3. ギガビットイーサネットインターフェイスのプライマリ IP アドレスを設定します。

```
Device(config-if)# ip address ip-address [mask]
```

4. ギガビットイーサネットインターフェイスの速度、デュプレックスモード、およびフロー制御を自動ネゴシエーションプロトコルで設定できるようにします。

```
Device(config-if)# negotiation auto
```

5. VRRP グループを作成し、VRRP コンフィギュレーション モードを開始します。

```
Device(config-if)# vrrp group address-family ipv4
```

6. VRRP バージョン 3 と同時に VRRP バージョン 2 のサポートを有効にします。

```
Device(config-if-vrrp)# vrrpv2
```

7. VRRP の優先順位レベルを設定します。

```
Device(config-if-vrrp)# priority level
```

8. インターフェイス リスト トラッキングを単一のエンティティとして設定します。

```
Device(config-if-vrrp)# track track-list-name [decrement priority]
```

9. 優先順位の高いデバイスが引き継ぐ前に最低限の期間待機するように、プリエンプション遅延を設定します。

```
Device(config-if-vrrp)# preempt delay minimum seconds
```

10. VRRP のプライマリ IP アドレスを指定します。

```
Device(config-if-vrrp)# address ip-address primary
```

VRF を設定します。

1. VRF ルーティング テーブル インスタンスを設定し、VRF コンフィギュレーション モードを開始します。

```
Device(config)# vrf definition vrf-number
```

2. VRF コンフィギュレーション モードで、アドレスファミリ IPv4 を設定します。

```
Device(config-vrf)# address-family ipv4
```

3. アドレスファミリ コンフィギュレーション モードを終了します。

```
Device(config-ipv4)# exit-address-family
```

次に、VRRP トラッキングの設定例を示します。

VRF red にトラックを追加するには、次の設定を使用します。

```
config-transaction
track 1 ip route 10.1.15.13 255.255.255.0 reachability
ip vrf red
```

インターフェイストラッキングを設定し、デバイスの優先順位を下げるには、次の設定を使用します。

```
interface GigabitEthernet 1.101
vrf forwarding 100
ip address 10.1.15.13 255.255.255.0
negotiation auto
vrrp 2 address-family ipv4
vrrpv2
priority 220
track 1 decrement 25
preempt delay minimum 30
address 10.1.15.100 primary
exit
```

設定された VRF の VRF ルーティング テーブル インスタンスを設定するには、次の設定を使用します。

```
vrf definition 100
!
address-family ipv4
exit-address-family
```

VRRP トラッキングの確認

例 1:

次に、Cisco IOS XE Catalyst SD-WAN デバイスに設定された VRRP グループのステータスを表示する **show vrrp details** コマンドの出力例を示します。

```
Device# show vrrp details
GigabitEthernet1/0/1 - Group 1 - Address-Family IPv4
  State is BACKUP <----- check states
  State duration 2 mins 13.778 secs
  Virtual IP address is 10.0.0.1
  Virtual MAC address is 0000.5E00.0101
  Advertisement interval is 1000 msec
  Preemption enabled
  Priority is 1 (Configured 100) <----- shows current and configured priority
  Track object 121 state DOWN decrement 220 Master Router is 10.1.1.3, priority is
200 <---- track object state
  Master Advertisement interval is 1000 msec (learned)
  Master Down interval is 3609 msec (expires in 2737 msec)
  FLAGS: 0/1
  VRRPv3 Advertisements: sent 27 (errors 0) - rcvd 149
  VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0
  Group Discarded Packets: 0
    VRRPv2 incompatibility: 0
    IP Address Owner conflicts: 0
    Invalid address count: 0
    IP address configuration mismatch : 0
    Invalid Advert Interval: 0
    Advert received in Init state: 0
    Invalid group other reason: 0
  Group State transition:
    Init to master: 0
    Init to backup: 1 (Last change Wed Feb 17 23:02:04.259)
    Backup to master: 1 (Last change Wed Feb 17 23:02:07.869) <----- check this for
flaps
    Master to backup: 1 (Last change Wed Feb 17 23:02:32.008)
    Master to init: 0
    Backup to init: 0
```

例 2:

次に、VRRP トラッキングプロセスによって追跡されるオブジェクトに関する情報を表示する **show track** コマンドの出力例を示します。

```
Device# show track 1
Track 1
  IP route 209.165.200.225 209.165.200.236 reachability
  Reachability is Down (no ip route)
  1 change, last change 1w1d
  VPN Routing/Forwarding table "vrrp"
  First-hop interface is unknown
rtr3#
```

例 3 :

次に、VRRP トラッキングプロセスによって追跡されるギガビットイーサネットインターフェイスの設定を表示する **show running-config interface** コマンドの出力例を示します。

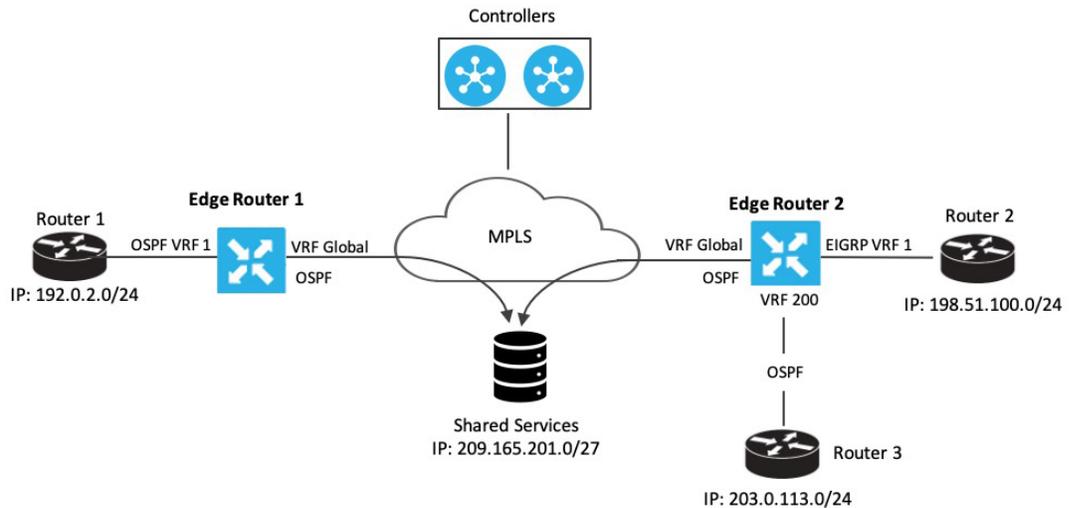
```
Device# show running-config interface GigabitEthernet 4
Building configuration...
Current configuration : 234 bytes
!
interface GigabitEthernet4
ip address 172.16.0.1 255.255.255.0
negotiation auto
vrrp 7 address-family ipv4
    priority 200
    vrrpv2
    track 5 decrement 5β-----priority decrement
    address 172.16.0.0 primary
    exit-vrrp
no mop enabled
no mop sysid
end
```

ルートリークの設定例

ルートリークは通常、共有サービスを使用する必要があるシナリオで使用されます。ルートレプリケーションを設定すると、VRF または VPN 間の相互再配布が可能になります。ルートレプリケーションにより、ルートがグローバル VPF およびサービス VPN 間で複製またはリークされ、ある VPN に存在するクライアントが別の VPN に存在する一致するプレフィックスに到達できるため、共有サービスが可能になります。

トポロジの例

このセクションでは、ルートリーク設定を示すトポロジの例を使用します。ここでは、エッジルータ 1 と 2 がオーバーレイネットワークの 2 つの異なるサイトにあり、MPLS を介して相互に接続されています。両方のエッジルータで、アンダーレイネットワークのサービスにアクセスできるようにルートリークが設定されています。ルータ 1 は、サービス側のエッジルータ 1 の背後にあります。このサイトのローカルネットワークは OSPF を実行します。ルータ 2 は、VPN 1 に EIGRP があるネットワーク上のエッジルータ 2 の背後にあります。ルータ 3 もエッジルータ 2 の背後にあり、VRF 200 で OSPF を実行しています。



エッジルータ 1 は、ルータ 1 の送信元 IP アドレス 192.0.2.0/24 をエッジルータ 1 のグローバル VRF にインポートします。したがって、192.0.2.0/24 はグローバル VRF にリークされたルートです。エッジルータ 2 は、ルータ 2 の送信元 IP アドレス 198.51.100.0/24 とエッジルータ 3 の送信元 IP アドレス 203.0.113.0/24 をエッジルータ 2 のグローバル VRF にインポートします。

アンダーレイ MPLS ネットワークの共有サービスは、ループバックアドレス 209.21.25.18/27 を介してアクセスされます。共有サービスの IP アドレスは、OSPF を介してエッジルータ 1 および 2 のグローバル VRF にアドバタイズされます。この共有サービスの IP アドレスは、エッジルータ 1 の VRF 1 と、エッジルータ 2 の VRF 1 および VRF 200 にリークされます。ルートリークに関しては、リークされたルートは両方のエッジルータのサービス VRF にインポートされます。



(注) OMP はルートループを防止するために、リークされたルートをサービス VPN からオーバーレイネットワークにアドバタイズしません。

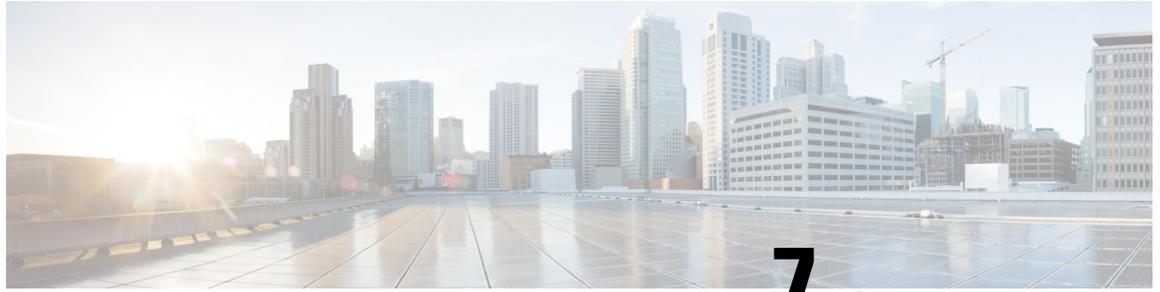
設定例

次に、エッジルータ 2 のグローバル VRF と VPN 1 の間で BGP および OSPF ルートリークが発生する設定の例を示します。

```
vrf definition 1
 rd 1:1
 !
 address-family ipv4
  route-replicate from vrf global unicast ospf 65535
 !
 global-address-family ipv4
  route-replicate from vrf 1 unicast eigrp
 exit-address-family
```

次に、エッジルータ 2 のグローバル VRF と VPN 200 の間で BGP および OSPF ルートリークが発生する設定の例を示します。

```
vrf definition 200
  rd 1:200
  !
  address-family ipv4
    route-replicate from vrf global unicast ospf 65535
  !
global-address-family ipv4
  route-replicate from vrf 200 unicast eigrp
  exit-address-family
```

第 7 章

Cisco Catalyst SD-WAN のルーティングプロトコルの BFD



(注) 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

表 46: 機能の履歴

機能名	リリース情報	説明
Cisco Catalyst SD-WAN のルーティングプロトコルの BFD	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a Cisco vManage リリース 20.3.1	この機能により、Cisco Catalyst SD-WAN ソリューション内の BGP、OSPF、および EIGRP プロトコルに BFD のサポートが拡張されます。BFD では、一定のレートで転送パス障害を検出する一貫した障害検出方法が提供されるため、再コンバージェンス時間を短縮できます。

- [ルーティングプロトコルの BFD に関する情報 \(170 ページ\)](#)
- [ルーティングプロトコルの BFD の設定 \(173 ページ\)](#)
- [CLI を使用したルーティングプロトコルの BFD の設定 \(179 ページ\)](#)

- [BFD 設定のモニタと確認 \(182 ページ\)](#)
- [一般的な BFD エラーのトラブルシューティング \(183 ページ\)](#)

ルーティングプロトコルの BFD に関する情報

BFD の概要

エンタープライズ ネットワークでは、ビジネスに不可欠なアプリケーションを共通の IP インフラストラクチャに統合することが一般的になっています。データの重要性を考えると、エンタープライズ ネットワークは通常、高度な冗長性を持つ構成になっています。高度な冗長性は望ましいものですが、その有効性は個々のネットワークデバイスの障害を迅速に検出し、トラフィックを代替パスに再ルーティングする能力によって決まります。既存のプロトコルの検出時間は通常 1 秒より長く、さらに長いこともあります。一部のアプリケーションでは、検出時間が長すぎると意味がありません。このような場合、Bidirectional Forwarding Detection (BFD) が使用されます。

BFD は、オーバーヘッドを小さく保ちながら、転送エンジン間で迅速に障害検知を行います。また、すべてのプロトコル層であらゆるメディアを通じて、リンク、デバイス、またはプロトコルの障害を検出する単一の標準化された方式を実現し、ビジネスに不可欠なアプリケーションの迅速な再コンバージェンスを可能にします。

ルーティングプロトコル用の BFD を設定する利点

- あらゆるメディアタイプ、カプセル化、トポロジ、およびルーティングプロトコルの障害検出時間の短縮
- アプリケーションの再コンバージェンスの高速化
- 一貫した障害検出方法

Cisco Catalyst SD-WAN での BFD の仕組み

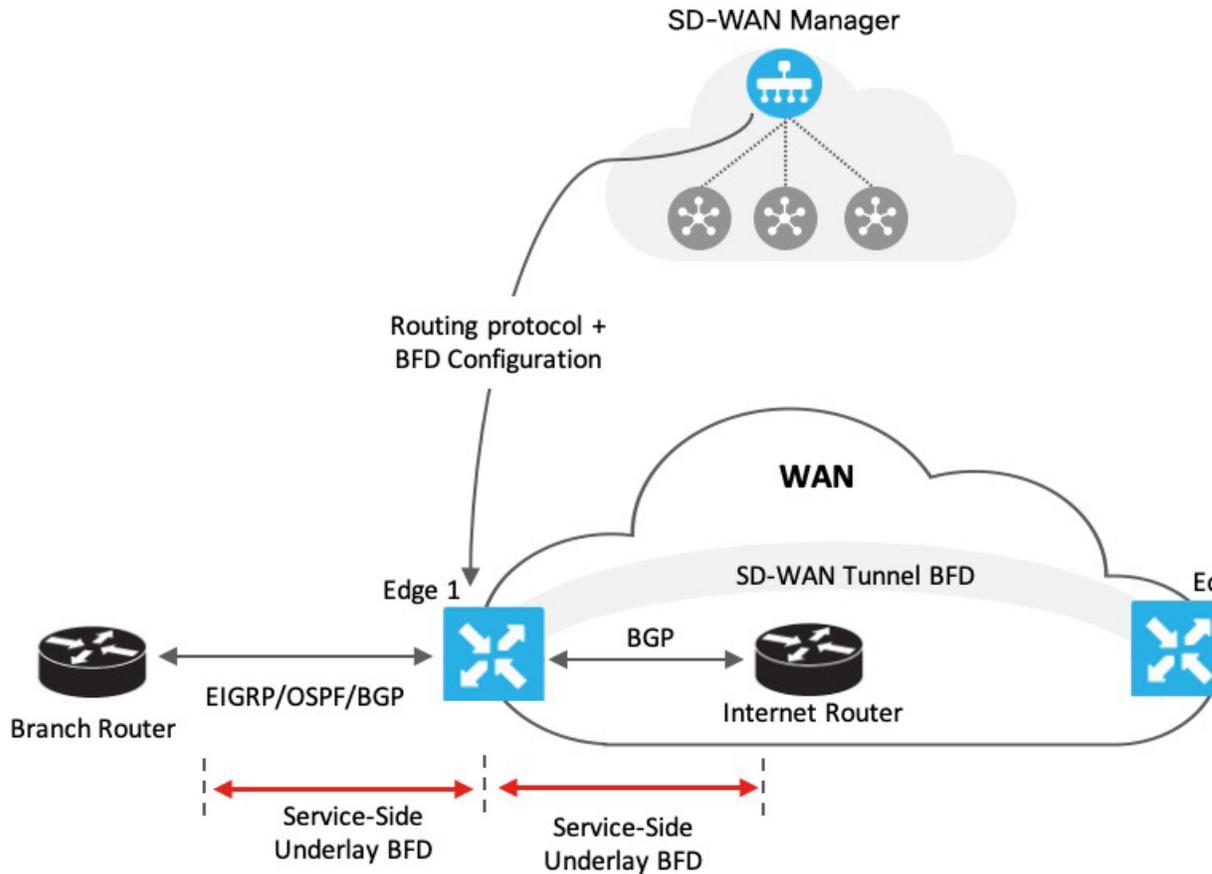
この機能の導入により、Cisco Catalyst SD-WAN ソリューションには、競合することなく独立して機能する、異なる機能がある 2 つのタイプの BFD があります。

- **Cisco Catalyst SD-WAN ルーティングプロトコルの BFD サポート (レガシー BFD)** : この機能は、Cisco IOS XE ですでに使用可能であり、Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a 以降の Cisco Catalyst SD-WAN ソリューションにまで拡張されているため、レガシー BFD と呼ばれます。
- **Cisco Catalyst SD-WAN BFD** : この機能はオーバーレイ BFD に固有の Cisco Catalyst SD-WAN の既存機能です。

Cisco Catalyst SD-WAN BFD の詳細については、「[Cisco Catalyst SD-WAN BFD](#)」を参照してください。

表 47:相違点 : Cisco Catalyst SD-WAN ルーティングプロトコルの BFD と Cisco Catalyst SD-WAN BFD

Cisco Catalyst SD-WAN ルーティングプロトコルの BFD	Cisco Catalyst SD-WAN BFD
<ul style="list-style-type: none"> • トランスポート側とサービス側の両方のインターフェイスで実行 • 次のプロトコルを登録できます。BGP、OSPF、および EIGRP <ul style="list-style-type: none"> • BGP (トランスポートおよびサービス側) • EIGRP (サービス側) • OSPF および OSPFv3 (サービス側) • ピアのアップまたはダウンの観点から、ピアのリンク障害を検出 	<ul style="list-style-type: none"> • オーバーレイトンネルの障害を検出するために Cisco Catalyst SD-WAN トンネルで実行 • これはデフォルトで有効になっており、無効化できない • 通常は OMP に対して有効になっている • リンク障害に加えて、遅延、損失、およびアプリケーション対応ルーティングで使用されるその他のリンク統計情報も測定



図に示すように、BFDはCisco SD-WAN Managerを介してルーティングプロトコル用に設定されています。Cisco SD-WAN Managerは、この設定をエッジルータにプッシュします。この例では、BFDから転送パス検出障害メッセージを受信するようにOSPFが設定されているとします。物理リンクに障害が発生した場合、OSPFはネイバーをシャットダウンし、リモートネイバーとの間でアドバタイズまたは受信したルーティング情報を復元するように求められます。

同様に、ルータEdge1は、そのトランスポートインターフェイスを介してインターネットルータに接続されます。BFDは、Edge1のトランスポート側とインターネットルータ間のBGP用に設定されます。ここで、BFDは接続の正常性を検出し、障害を報告します。

サポートされているプロトコルとインターフェイス

サポートされているプロトコル

Cisco Catalyst SD-WANでは、次のルーティングプロトコルを、BFDから転送パス検出障害メッセージを受信するように設定できます。

- BGP

- EIGRP
- OSPF および OSPFv3

サポートされるインターフェイス

- GigabitEthernet
- TenGigabitEthernet
- FiveGigabitEthernet
- FortyGigabitEthernet
- HundredGigabitEthernet
- SVI
- サブインターフェイス

制限事項と制約事項

次の制約事項がコントローラモードの Cisco IOS XE Catalyst SD-WAN デバイスに適用されません。

- シングルホップ BFD のみがサポートされます。
- BFD はスタティックルートではサポートされていません。
- BFD セッションモードをソフトウェアモードとハードウェアモードの間で変更するには、既存の BFD 設定をすべて削除して再設定する必要があります。
- BFD は、BGP、EIGRP、OSPF、および OSPFv3 でのみサポートされます。
- Cisco Catalyst SD-WAN のルーティングプロトコルの BFD は、Cisco SD-WAN Manager からモニターできません。Cisco Catalyst SD-WAN ルーティングプロトコルの BFD をモニターするには、CLI の show コマンドを使用します。
- BFD セッションが確立されると、BFD セッションモード（エコーとエコーなし、またはその逆、あるいはソフトウェアとハードウェア、またはその逆）は、Cisco SD-WAN Manager の BFD テンプレートパラメータの変更直後には更新されません。BFD モードの変更は、セッションが少なくとも 1 回フラップした後にのみ有効になります。

ルーティングプロトコルの BFD の設定

Cisco SD-WAN Manager には、ルーティングプロトコルの BFD を設定するための独立したテンプレートはありません。ただし、サポートされているプロトコルは、Cisco SD-WAN Manager の CLI アドオンテンプレートを使用して設定を追加することで、受信した BFD パケットに登録したり、登録解除したりできます。CLI アドオンテンプレートを使用して、以下を設定します。

- タイマー、乗数、セッションモードなどのパラメータを含むシングルホップ BFD テンプレートを追加します。
- インターフェイスで BFD テンプレートを有効にします。インターフェイスごとに追加できる BFD テンプレートは 1 つだけです。
- サポートされるルーティングプロトコルの BFD を有効または無効にします。BFD を有効または無効にする設定は、サポートされるルーティングプロトコル (BGP、EIGRP、OSPF、および OSPFv3) ごとに異なります。

ルーティングプロトコルの BFD の有効化

サービス側 BGP の BFD の設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. **[Feature Templates]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Feature Templates]** のタイトルは **[Feature]** です。

3. **[Add template]** をクリックします。
4. デバイスリストからデバイスを選択します。
5. **[Other Templates]** で **[CLI Add-on Template]** を選択します。
6. 次の例に示すように、シングルホップ BFD テンプレートを追加し、サービス BGP の BFD を有効にする CLI 設定を入力します。

```
bfd-template single-hop t1
  interval min-tx 500 min-rx 500 multiplier 3
  !
interface GigabitEthernet1
  bfd template t1

router bgp 10005
address-family ipv4 vrf 1
  neighbor 10.20.24.17 fall-over bfd
  !
address-family ipv6 vrf 1
  neighbor 2001::7 fall-over bfd
```

CLI 設定について

この例では、最小および最大間隔と乗数を指定するシングルホップ BFD テンプレートが作成されます。これらのパラメータの指定は必須です。さらに、エコーモード (デフォルトで有効) や BFD ダンプニング (デフォルトではオフ) など、他の BFD パラメータも指定できます。作成された BFD テンプレートは、インターフェイス (この例では GigabitEthernet1) で有効になります。



- (注) インターフェイスで有効になっている BFD テンプレートを変更するには、まず既存のテンプレートを削除して変更してから、再度インターフェイスで有効にする必要があります。



- (注) すでに BGP 機能テンプレートが添付されているデバイステンプレートに BFD 設定を加える場合は、CLI アドオンテンプレートの BGP 設定を更新して、**no neighbor ip-address ebgp-multihop** コマンドを含めるようにしてください。デフォルトでは、BGP 機能テンプレートで **neighbor ip-address ebgp-multihop** コマンドがアクティブになっているため、この変更は必須です。

7. [Save] をクリックします。
8. [デバイステンプレートへの機能テンプレートの添付](#)



- (注) 設定を有効にするには、デバイステンプレートに BGP 機能テンプレートが添付されている必要があります。

9. [デバイステンプレートをデバイスに添付します。](#)

トランスポート側 BGP の BFD の設定

1. Cisco SD-WAN Manager メニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックします。



- (注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Add template] をクリックします。
4. デバイスリストからデバイスを選択します。
5. [Other Templates] で [CLI Add-on Template] を選択します。
6. 次の例に示すように、CLI 設定を入力して、シングルホップ BFD テンプレートを追加し、トランスポート BGP の BFD を有効にします。

```
bfd-template single-hop t1
interval min-tx 500 min-rx 500 multiplier 3
!
interface GigabitEthernet1
bfd template t1
!
router bgp 10005
```

```
neighbor 10.1.15.13 fall-over bfd
!
sdwan
interface GigabitEthernet1
 tunnel-interface
 allow-service bfd
 allow-service bgp
```

CLI 設定について

この例では、最小および最大間隔と乗数を指定するシングルホップ BFD テンプレートが作成されます。これらのパラメータの指定は必須です。さらに、エコーモード（デフォルトで有効）や BFD ダンプニング（デフォルトではオフ）など、他の BFD パラメータも指定できます。作成された BFD テンプレートは、インターフェイス（この例では GigabitEthernet1）で有効になります。この例では、GigabitEthernet1 が SD-WAN トンネルの送信元でもあります。GigabitEthernet1 のトンネルインターフェイスでサービスを許可すると、BGP および BFD パケットがトンネルを通過することが保証されます。



- (注) インターフェイスで有効になっている BFD テンプレートを変更するには、まず既存のテンプレートを削除して変更してから、再度インターフェイスで有効にする必要があります。



- (注) すでに BGP 機能テンプレートが添付されているデバイステンプレートに BFD 設定を加える場合は、CLI アドオンテンプレートの BGP 設定を更新して、**no neighbor ip-address ebgp-multihop** コマンドを含めるようにしてください。デフォルトでは、BGP 機能テンプレートで **neighbor ip-address ebgp-multihop** コマンドがアクティブになっているため、この変更は必須です。

7. [Save] をクリックします。
8. [デバイステンプレートへの機能テンプレートの添付](#)



- (注) 設定を有効にするには、デバイステンプレートに BGP 機能テンプレートが添付されている必要があります。

9. [デバイステンプレートをデバイスに添付します。](#)

サービス側 EIGRP の BFD の設定

1. Cisco SD-WAN Manager メニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Add template] をクリックします。
4. デバイスリストからデバイスを選択します。
5. [Other Templates] で [CLI Add-on Template] を選択します。
6. 次の例に示されているように、CLI 設定を入力し、シングルホップ BFD テンプレートを追加して、EIGRP の BFD を有効にします。

```
bfd-template single-hop t1
  interval min-tx 500 min-rx 500 multiplier 3
  !
interface GigabitEthernet5
  bfd template t1

router eigrp myeigrp
address-family ipv4 vrf 1 autonomous-system 1
  af-interface GigabitEthernet5
    bfd
```

CLI 設定について

この例では、最小および最大間隔と乗数を指定するシングルホップ BFD テンプレートが作成されます。各項目の指定は必須です。さらに、エコーモード（デフォルトで有効）や BFD ダンプニング（デフォルトではオフ）など、他の BFD パラメータも指定できます。

作成された BFD テンプレートは、インターフェイス（この例では GigabitEthernet5）で有効になります。



(注) インターフェイスで有効になっている BFD テンプレートを変更するには、まず既存のテンプレートを削除して変更し、インターフェイスで再度有効にする必要があります。

7. [Save] をクリックします。
8. [デバイステンプレートへの機能テンプレートの添付](#)



(注) 設定を有効にするには、デバイステンプレートに EIGRP 機能テンプレートが添付されている必要があります。

9. [デバイステンプレートをデバイスに添付します](#)。

サービス側 OSPF および OSPFv3 の BFD の設定

1. Cisco SD-WAN Manager メニューから、[Configuration] > [Templates] を選択します。

- [Feature Templates] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

- [Add template] をクリックします。
- デバイスリストからデバイスを選択します。
- [Other Templates] で [CLI Add-on Template] を選択します。
- 次の例に示されているように、CLI 設定を入力して、シングルホップ BFD テンプレートを追加し、OSPF および OSPFv3 の BFD を有効にします。

OSPF

```
bfd-template single-hop t1
interval min-tx 500 min-rx 500 multiplier 3
!
interface GigabitEthernet5
bfd template t1
!
interface GigabitEthernet1
bfd template t1
!
router ospf 1 vrf 1
  bfd all-interfaces
!
```

OSPFv3

```
bfd-template single-hop t1
  interval min-tx 500 min-rx 500 multiplier 3

interface GigabitEthernet5
  bfd template t1
router ospfv3 1
  address-family ipv4 vrf 1
    bfd all-interfaces
```

CLI 設定について

各例では、最小および最大間隔と乗数を指定するシングルホップ BFD テンプレートが作成されます。各項目の指定は必須です。さらに、エコーモード（デフォルトで有効）や BFD ダンプニング（デフォルトではオフ）など、他の BFD パラメータも指定できます。

作成された BFD テンプレートは、インターフェイス（この例では GigabitEthernet5）で有効になります。



(注) インターフェイスで有効になっている BFD テンプレートを変更するには、まず既存のテンプレートを削除して変更し、インターフェイスで再度有効にする必要があります。

- [Save] をクリックします。

- この設定の CLI アドオンテンプレートをデバイステンプレートに添付します。



(注) 設定を有効にするには、デバイステンプレートに OSPF 機能テンプレートが添付されている必要があります。

- デバイステンプレートをデバイスに添付します。

デバイステンプレートへの機能テンプレートの添付

CLI アドオンテンプレートを作成して BFD を有効にした後、設定を有効にするためにテンプレートをデバイステンプレートに添付します。デバイステンプレートに設定を添付するには、次の手順に従います。機能テンプレートを添付するデバイステンプレートに、関連する機能テンプレート (BGP、OSPF、EIGRP) がすでに添付されていることを確認します。

- Cisco SD-WAN Manager メニューから、**[Configuration] > [Templates]** の順に選択します。
- [Device Template]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Device Templates]** のタイトルは **[Device]** です。

- [Create Template]** をクリックし、ドロップダウンオプションから **[From Feature Template]** を選択します。
- [Device Model]** ドロップダウンオプションから、デバイスを選択します。テンプレートの名前と説明を入力します。
- [作成 (Create)]** をクリックします。
- [Additional Templates]** をクリックします。
- [CLI Add-on Template]** フィールドで、ルーティングプロトコルの BFD を有効にするために設定した CLI アドオンテンプレートを選択します。
- [作成 (Create)]** をクリックします。

次の手順：「[Attach device template to device](#)」

CLI を使用したルーティングプロトコルの BFD の設定

デバイス CLI を使用して BGP、EIGRP、OSPF、および OSPF3 の BFD を設定するには、このトピックの手順に従います。

BFD テンプレートの作成

次の例に示すように、シングルホップ BFD テンプレートを作成します。

```
bfd-template single-hop t1
  interval min-tx 500 min-rx 500 multiplier 3
```



(注) BFD テンプレートを作成するための CLI 設定は、設定するプロトコルに関係なく同じです。

サービス側 BGP の BFD の有効化

次に、BGP が設定され、VRF 1 の下のインターフェイスで BFD が有効になり、その後サービス側の BGP で有効になる例を示します。

```
interface GigabitEthernet5
bfd template t1
!
router bgp 10005
  bgp log-neighbor-changes
  distance bgp 20 200 20
  !
  address-family ipv4 vrf 1
  bgp router-id 10.20.24.15
  redistribute connected
  neighbor 10.20.24.17 remote-as 10007
  neighbor 10.20.24.17 activate
  neighbor 10.20.24.17 send-community both
  neighbor 10.20.24.17 maximum-prefix 2147483647 100
  neighbor 10.20.24.17 fall-over bfd
  exit-address-family
  !
  address-family ipv6 vrf 1
  bgp router-id 10.20.24.15
  neighbor 2001::7 remote-as 10007
  neighbor 2001::7 activate
  neighbor 2001::7 send-community both
  neighbor 2001::7 maximum-prefix 2147483647 100
  neighbor 2001::7 fall-over bfd
  exit-address-family
```

トランスポート側 BGP の BFD の有効化

```
interface GigabitEthernet1
bfd template t1
!
router bgp 10005
  bgp router-id 10.1.15.15
  bgp log-neighbor-changes
  distance bgp 20 200 20
  neighbor 10.1.15.13 remote-as 10003
  neighbor 10.1.15.13 fall-over bfd
  address-family ipv4 unicast
  neighbor 10.1.15.13 remote-as 10003
  neighbor 10.1.15.13 activate
  neighbor 10.1.15.13 maximum-prefix 2147483647 100
  neighbor 10.1.15.13 send-community both
  redistribute connected
  exit-address-family
```

```
!  
timers bgp 60 180  
  
sdwan  
interface GigabitEthernet1  
tunnel-interface  
allow-service bgp  
allow-service bfd
```

EIGRP の BFD の有効化

次に、EIGRP が設定され、VRF 1 の下のインターフェイスで BFD が有効になり、その後サービ側 EIGRP で有効になる例を示します。

```
interface GigabitEthernet5  
bfd template t1  
!  
router eigrp myeigrp  
address-family ipv4 vrf 1 autonomous-system 1  
  af-interface GigabitEthernet5  
  no dampening-change  
  no dampening-interval  
  hello-interval 5  
  hold-time 15  
  split-horizon  
  bfd  
  exit-af-interface  
  !  
  network 10.20.24.0 0.0.0.255  
  topology base  
  redistribute connected  
  redistribute omp  
  exit-af-topology  
  !  
  exit-address-family  
  !
```

OSPFv3 の BFD の有効化

次に、OSPFv3 が設定され、VRF 1 の下のインターフェイスで BFD が有効になり、その後サービ側 EIGRP で有効になる例を示します。

```
interface GigabitEthernet5  
  bfd template t1  
  ospfv3 1 ipv4 area 0  
  ospfv3 1 ipv4 dead-interval 40  
  ospfv3 1 ipv4 hello-interval 10  
  ospfv3 1 ipv4 network broadcast  
  ospfv3 1 ipv4 priority 1  
  ospfv3 1 ipv4 retransmit-interval 5  
  ospfv3 1 ipv6 area 0  
  ospfv3 1 ipv6 dead-interval 40  
  ospfv3 1 ipv6 hello-interval 10  
  ospfv3 1 ipv6 network broadcast  
  ospfv3 1 ipv6 priority 1  
  ospfv3 1 ipv6 retransmit-interval 5  
  
router ospfv3 1  
  address-family ipv4 vrf 1  
  area 0 normal  
  bfd all-interfaces  
  router-id 10.20.24.15
```

```

distance 110
exit-address-family
!
address-family ipv6 vrf 1
area 0 normal
bfd all-interfaces
router-id 10.20.24.15
distance 110
exit-address-family
!
!
exit

```

BFD 設定のモニタと確認

ここでは、BFD 設定を確認するために実行できるコマンドのリストを示します。

インターフェイスで BFD テンプレートを確認するには、**show bfd interface** コマンドを実行します。

```

Device# show bfd interface
Interface Name: GigabitEthernet5
Interface Number: 11
Configured bfd interval using bfd template: 12383_4T1
Min Tx Interval: 50000, Min Rx Interval: 50000, Multiplier: 3

```

BGP の BFD 設定の確認

show bfd neighbors client bgp ipv4 コマンドを実行して、BFD セッションのステータスを確認します。

```

Device# show bfd neighbors client bgp ipv4

IPv4 Sessions
NeighAddr                LD/RD          RH/RS          State          Int
10.20.24.17              1/1            Up             Up             Gi5

```

EIGRP の BFD 設定の確認

show bfd neighbors client eigrp コマンドを実行して、BFD セッションのステータスを確認します。

```

Device# show bfd neighbors client eigrp

IPv4 Sessions
NeighAddr                LD/RD          RH/RS          State          Int
10.20.24.17              1/1            Up             Up             Gi5

```

OSPF の BFD 設定の確認

show bfd neighbors client ospf コマンドを実行して、BFD セッションのステータスを確認します。

```

Device# show bfd neighbors client ospf

```

```
IPv4 Sessions
NeighAddr      LD/RD      RH/RS      State      Int
10.20.24.17    1/1        Up          Up          Gi5
```

一般的な BFD エラーのトラブルシューティング

制御接続の確認

BFD で問題が発生した場合は、まず **show sdwan control connections** コマンドを実行して、Cisco SD-WAN Manager とエッジルータ間の制御接続を確認します。

```
Device#show sdwan control connections
```

```
PEER                                PEER
  CONTROLLER
PEER  PEER PEER                      SITE      DOMAIN PEER
PRIV  PEER
  GROUP
TYPE  PROT SYSTEM IP                    ID        ID        PRIVATE IP
PORT  PUBLIC IP
      ID
-----
vsmart dtls 172.16.255.19  100      1        10.0.5.19
12355 10.0.5.19
0
vsmart dtls 172.16.255.20  200      1        10.0.12.20
12356 10.0.12.20
0
vmanage dtls 172.16.255.22  200      0        10.0.12.22
12346 10.0.12.22
0 < ---- up
                                lte          No    up    0:12:45:44
                                lte          No    up    0:15:59:45
                                lte          No    up    0:15:59:45
```

デバイスへのデバイステンプレートのプッシュに関する問題

デバイステンプレートをデバイスにプッシュする際に問題が見つかった場合は、次に示すように、エッジデバイスでデバッグログを収集します。

```
debug netconf all
request platform soft system shell
tail -f /var/log/confd/cia-netconf-trace.log
```

Cisco SD-WAN Manager が設定をデバイスに正常にプッシュしても問題が解決しない場合は、**show sdwan running-config** コマンドを実行して BFD に関連するすべての詳細を表示します。

トランスポート側 BFD の問題

トランスポート側 BFD セッションがダウンしている場合は、Cisco Catalyst SD-WAN トンネルインターフェイスの下のパケットフィルタデータを調べて、トランスポート側で BFD パケットの通過が許可されていることを確認します。出力で **allow-service bgp** および **allow-service bfd** を探します。

```
Device#show sdwan running-config | sec sdwan
 tunnel mode sdwan
sdwan
 interface GigabitEthernet1
  tunnel-interface
  encapsulation ipsec
```

```
color lte
allow-service bgp
allow-service bfd
.....
```



第 8 章

Cisco Catalyst SD-WAN BFD



- (注) 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

表 48: 機能の履歴

機能名	リリース情報	説明
不安定な Cisco Catalyst SD-WAN BFD セッションの自動一時停止	Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.10.1	この機能を使用すると、フラップサイクルパラメータまたはサービスレベル契約 (SLA) パラメータに基づいて、不安定な Cisco Catalyst SD-WAN Bidirectional Forwarding Detection (BFD) セッションを自動的に一時停止できます。 また、一時停止された BFD セッションをモニターしたり、一時停止された BFD セッションを手動でリセットすることもできます。 この機能を使用すると、フラップサイクルパラメータまたはサービスレベル契約 (SLA) パラメータに基づいて、不安定な Cisco Catalyst SD-WAN Bidirectional Forwarding Detection (BFD) セッションを自動的に一時停止できます。

- [Cisco Catalyst SD-WAN BFD について \(186 ページ\)](#)
- [BFD セッションの自動一時停止について \(187 ページ\)](#)
- [BFD セッションの自動一時停止に関する制約事項 \(190 ページ\)](#)
- [CLI テンプレートを使用した BFD セッションの自動一時停止の設定 \(190 ページ\)](#)
- [BFD セッションの自動一時停止の確認 \(192 ページ\)](#)

Cisco Catalyst SD-WAN BFD について

Cisco Catalyst SD-WAN 内には、次のタイプの BFD があります。

• Cisco Catalyst SD-WAN BFD

このタイプの BFD は、オーバーレイトンネルにおける障害を検出し、次の特性を備えています。

- これはデフォルトで有効になっており、無効化できない

- 通常、Cisco Catalyst SD-WAN Overlay Management Protocol (OMP) に対して有効になっている
- Cisco Catalyst SD-WAN BFD は、リンク障害に加えて、遅延、損失、ジッター、およびアプリケーション認識型ルーティングで使用されるその他のリンク統計も測定
アプリケーション認識型ルーティングで使用される遅延、損失、およびジッターを測定するための Cisco Catalyst SD-WAN BFD の詳細については、「[Application-Aware Routing](#)」を参照してください。
- Cisco Catalyst SD-WAN のルーティングプロトコルに対する BFD サポート
このタイプの BFD は、Cisco Catalyst SD-WAN の BGP、OSFP、および EIGRP ルーティングプロトコルをサポートします。
ルーティングプロトコルの BFD の詳細については、「[BFD for Routing Protocols in Cisco Catalyst SD-WAN](#)」を参照してください。

BFD セッションの自動一時停止について

サポートされている最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a、Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.10.1

BFD セッションでフラッピングが発生することがあります。つまり、BFD セッションがダウン状態になり、その後稼働状態に戻ります。これは、BFD セッションに含まれるデバイスの 1 つが使用できなくなり、その後使用可能に戻ると、発生する可能性があります。BFD セッションがフラップすると、そのトンネルで実行されているアプリケーションが中断されます。不安定な BFD セッションが起動することがありますが、不安定な接続により、BFD セッションがすぐに再び中断される可能性があります。この機能を使用すると、不安定な BFD セッションが原因でアプリケーショントラフィックが 1 つのオーバーレイパスから別のパスに不必要に誘導されるという影響を回避できます。

BFD セッションフラップのサイクルを回避するために、Cisco Catalyst SD-WAN は、次のパラメータに基づいて BFD セッションを一時停止するための自動一時停止メカニズムを提供します。

• フラップサイクル

フラップサイクルは、次のようにのみ定義されます。

- BFD セッションは稼働状態
- BFD セッションはダウン状態
- BFD セッションは復旧中

• SLA しきい値

SLA しきい値は、BFD セッションが一時停止リストに追加されるしきい値です。SLA しきい値は、損失、遅延、ジッターなどのトラフィックメトリックのしきい値です。これら

のメトリックのいずれかが、トラフィックパフォーマンスがしきい値で定義されたポイントまで低下したことを示す場合、BFDセッションの状態が一時停止に変更されます。これらのしきい値は、SLAで指定されたトラフィックパフォーマンスのレベルを反映します。



- (注) SLA しきい値はオプションの設定です。SLA しきい値を設定する場合は、損失、遅延、およびジッターのメトリックを高く設定して、SLA しきい値が SLA クラスで定義されている SLA パラメータと競合しないようにしてください。SLA クラスの詳細については、『[Cisco Catalyst SD-WAN Policies Configuration Guide](#)』を参照してください。

BFD セッションの自動一時停止の利点

- BFD一時停止リストからの影響を受ける回路またはトンネルインターフェイスの手動削除をサポートします。
- 一時停止されたトンネルのモニタリングを提供します。

BFD セッションの自動一時停止の仕組み

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a、Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.10.1

Cisco SD-WAN Manager デバイス CLI テンプレートまたは CLI アドオンテンプレートを使用して、次の BFD セッションパラメータを設定します。

表 49: BFDセッションフラップサイクルおよび SLA パラメータ

フィールド	説明
enable-lr	BFD 一時停止時のラストリゾートの有効にします。 トンネルインターフェイスでラストリゾートを有効にする方法の詳細については、「 last-resort-circuit 」を参照してください。
duration	BFD セッションの一時停止状態が維持される時間。
flapping-window	BFD セッションフラップを検出するタイムフレームまたはウィンドウ。

フィールド	説明
flap-count	BFDセッションが一時停止されるまでのBFDセッションフラップの回数。 flap-count の推奨設定は3です。
thresholds	BFDセッションの一時停止をトリガーするSLA しきい値。

BFD セッション一時停止ワークフロー

設定されたフラッピングウィンドウ間隔内でBFDセッションが **flap-count** の値を超えると、BFDセッションは、設定された期間間隔まで一時停止状態が維持される必要があります。

一時停止状態のBFDセッションでは、次のようになります。

1. セッションが再フラップするか、定義されたしきい値パラメータを超えると、セッションは一時停止状態に戻り、期間は再びリセットされます。
2. セッションがフラップせず、しきい値の範囲内にある場合、期間間隔が経過すると、セッションの一時停止状態は自動的に解除されます。
3. **request platform software sdwan auto-suspend reset** コマンドを使用して、一時停止されたBFDセッションを手動で削除することもできます。詳細については、『[Cisco IOS XE SD-WAN Qualified Command Reference Guide](#)』を参照してください。

通常のSLA測定およびエコー応答またはパス最大伝送ユニット（PMTU）制御トラフィックのみが、一時停止されたBFDセッションを介して送信されます。



- (注) BFDセッションが一時停止状態の場合、データトラフィックはオーバーレイネットワークを介して送信されません。



- (注) この機能は、BFDセッションの状態を操作しません。



- (注) BFD一時停止機能はフォワードデータトラフィック用であるため、データトラフィックのドロップを回避するために、リモートエンドノードでBFD一時停止を有効にしてリバースデータトラフィックをブロックする必要があります。

BFD セッションの自動一時停止に関する制約事項

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a、Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.10.1

- 単一の TLOC を持つ Cisco IOS XE Catalyst SD-WAN デバイスの場合、BFD セッションの自動一時停止により、BFD セッションがドロップされる可能性があります。
- トンネルインターフェイスですべての BFD セッションがダウンしていない限り、ラストリゾート回線は単一のサイトでは機能しない可能性があります。ラストリゾート回線は、非ラストリゾート回線上のすべての BFD セッションが一時停止またはダウンしている場合にのみ有効になります。
- Cisco SD-WAN Manager 機能テンプレートは、BFD セッションの自動一時停止の設定をサポートしていません。

サポートは、デバイス CLI または CLI アドオンテンプレートを使用して BFD 自動一時停止を設定する場合にのみ提供されます。

- 重複したトラフィックが別の BFD セッションで送信された場合、その重複したトラフィックは、BFD 一時停止セッションを介してルーティングされる可能性があります。

CLI テンプレートを使用した BFD セッションの自動一時停止の設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a、Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.10.1

CLI テンプレートの使用の詳細については、[CLI アドオン機能テンプレート](#)および[CLI テンプレート](#)を参照してください。



(注) デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

1. ラストリゾートの有無にかかわらず、BFD の自動一時停止を有効にします。

```
auto-suspend
  enable-lr
```

```
auto-suspend
  no enable-lr
```



- (注) BFD 自動一時停止機能のラストリゾートを有効にする前に、トンネルインターフェイスでラストリゾート回線を有効にする必要があります。

ラストリゾートの詳細については、「[last-resort-circuit](#)」を参照してください。

2. 次のフラップパラメータを設定します。

```
duration sec
  flapping-window sec
  flap-count flap-count
```



- (注) SLA ベースの BFD 自動一時停止を使用する場合、**duration** は **bfd multiplier x bfd poll interval** の数よりも大きくする必要があります。BFD 自動一時停止期間は 30 分以上に設定することをお勧めします。

3. (任意) SLA パラメータを設定します。

```
thresholds
  color
  all
  jitter jitter-value
  latency latency-value
  loss loss-value
  !
```

SLA しきい値を有効にする前に、BFD セッションフラッピングのパラメータと期間を設定します。

次に、ラストリゾートを有効にして BFD 自動一時停止を設定する完全な設定例を示します。

```
auto-suspend
  enable-lr
  duration 3600
  flapping-window 300
  flap-count 1
  thresholds
  color
  all
  latency 10
  loss 10
  jitter 10
```



- (注) **color all** と特定の **color** を有効にすると、特定のカラーが **color all** パラメータよりも優先されます。BFD カラーの詳細については、「[bfd color](#)」を参照してください。

BFD セッションの自動一時停止の確認

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a、Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.10.1

次の `show sdwan bfd sessions suspend` コマンドの出力例は、合計一時停止回数（BFD セッションが一時停止された回数）を示しています。

```
Device# show sdwan bfd sessions suspend
SYSTEM IP          STATE  SOURCE TLOC  REMOTE TLOC  SOURCE IP  DST PUBLIC  DST PUBLIC  ENCAP  RE-SUSPEND  SUSPEND  TOTAL  SUSPEND
          COLOR    COLOR                IP          IP          PORT        ENCAP  COUNT  TIME LEFT  COUNT  DURATION
-----
172.16.255.14    up     lte          lte          10.1.15.15 10.1.14.14 12426      ipsec  0           0:00:19:52  18     0:00:00:07
```

BFD セッション一時停止メトリックを分析するために、RE-SUSPEND COUNT、SUSPEND TIME LEFT、TOTAL COUNT、および SUSPEND DURATION の列が追加されました。

次の `show sdwan bfd sessions alt` コマンドの出力例は、一時停止フラグが BFD セッションおよびその他の BFD セッションメトリックに追加されている場合に表示されます。

```
Device# show sdwan bfd sessions alt
*Sus = Suspend
*NA = Flag Not Set
SYSTEM IP          SITE ID  STATE  SOURCE TLOC  REMOTE TLOC  SOURCE IP  DST PUBLIC  DST PUBLIC  ENCAP  BFD-LD  FLAGS  UPTIME
          COLOR    COLOR                IP          IP          PORT        ENCAP  BFD-LD  FLAGS  UPTIME
-----
172.16.255.14    400     up     3g          lte          10.0.20.15 10.1.14.14 12426      ipsec  20004  NA     0:19:30:40
172.16.255.14    400     up     lte          lte          10.1.15.15 10.1.14.14 12426      ipsec  20003  Sus    0:00:02:46
172.16.255.16    600     up     3g          lte          10.0.20.15 10.0.106.1 12366      ipsec  20002  NA     0:19:30:40
172.16.255.16    600     up     lte          lte          10.1.15.15 10.0.106.1 12366      ipsec  20001  NA     0:19:20:14
```

BFD の一時停止用に、BFD-LD および FLAGS の列が追加されました。

ローカル識別子 (LD) は、すべての BFD セッションに関する一意の識別子です。LD の値はゼロ以外である必要があります。LD は、Cisco Technical Assistance Center (TAC) が BFD セッションのトラブルシューティングに使用する内部値です。

一時停止された BFD セッションを識別するために、BFD セッションフラグ `Sus` が追加されます。

次の出力例は、`Sus` フラグが追加された BFD セッションを示しています。

```
Device# show sdwan bfd history
SYSTEM IP          SITE ID  COLOR  STATE  DST PUBLIC  DST PUBLIC  ENCAP  TIME  RX  TX  DEL  FLAGS
          IP          PORT        IP          IP          PORT        ENCAP  TIME  PKTS PKTS DEL  FLAGS
-----
172.16.255.16    600     lte    up     10.0.106.1 12366      ipsec  06/03/22 02:51:06  0  0  0  [ ]
172.16.255.16    600     lte    up     10.0.106.1 12366      ipsec  06/03/22 02:52:04 153 154 0  [Sus]
172.16.255.16    600     lte    down   10.0.106.1 12366      ipsec  06/03/22 03:00:50 1085 1085 0  [Sus]
```

次の出力例は、BFD セッションの概要を示しています。これには、どの BFD セッションが稼働状態であり、ダウン状態であり、フラップされており、一時停止されているかが含まれます。

```
Device# show sdwan bfd summary
sessions-total      4
sessions-up        4
sessions-max       4
sessions-flap      4
poll-interval      60000
sessions-up-suspended  1
sessions-down-suspended  0
```

BFD セッションの一時停止用に、`sessions-flap`、`sessions-up-suspended`、および `sessions-down-suspended` フィールドが追加されます。



第 9 章

TLOC カラーによる Cisco Catalyst SD-WAN コントローラのルートフィルタリング



- (注) 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

表 50: 機能の履歴

機能名	リリース情報	説明
TLOC カラーによる Cisco SD-WAN コントローラのルートフィルタリング	Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.11.1	Cisco SD-WAN コントローラは、特定デバイスに関連しないルートを除外するために、ネットワーク内のルータにアダプタイズするルートの数を減らすことができます。ルートの数を減らすためのフィルタリングは、各デバイスの TLOC カラーに基づきます。たとえば、パブリック TLOC へのルートは、プライベート TLOC のみを持つルータには関係しません。アダプタイズするルートを減らすことは、ネットワーク内のルータの送信パス制限に達することを回避するために役立ちます。

- [TLOC カラーによる Cisco SD-WAN コントローラのルートフィルタリングについて \(194 ページ\)](#)

- TLOC カラーによる Cisco SD-WAN コントローラ のルートフィルタリングのサポートされるデバイス (197 ページ)
- TLOC カラーによる Cisco SD-WAN コントローラ のルートフィルタリングの前提条件 (197 ページ)
- TLOC カラーによる Cisco SD-WAN コントローラ のルートフィルタリングに関する制約事項 (197 ページ)
- CLI テンプレートを使用した TLOC カラーによる Cisco SD-WAN コントローラ のルートフィルタリングの設定 (197 ページ)
- TLOC カラーによる Cisco SD-WAN コントローラ のルートフィルタリングのモニター (200 ページ)

TLOC カラーによる Cisco SD-WAN コントローラ のルートフィルタリングについて

最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a、Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.11.1

ルートフィルタリングを使用することで、Cisco SD-WAN コントローラは、特定デバイスに関連しないルートを除外するために、ネットワーク内のルータにアダプタイズするルート数を減らすことができます。フィルタリングは、各デバイスの TLOC の色に基づきます。個々のルータごとに、Cisco SD-WAN コントローラ は、1 つ以上のルータの TLOC と互換性があるルートのみをアダプタイズします。

利点

より少ないルートをアダプタイズすることには、次の利点があります。

- 送信パス制限に達することを回避します。

TLOC カラーによる Cisco SD-WAN コントローラ のルートフィルタリングは、ネットワーク内のルータの送信パス制限に達することを回避するために役立ちます。たとえば、送信パス制限が 32 に設定されているものの、Cisco SD-WAN コントローラ で、デバイスにアダプタイズする特定プレフィックスのルートが 32 を超える場合があります。無関係なルートをフィルタリングすると、制限に達することを回避するために役立ちます。

- 関連するルートに優先順位を付けます。

送信パス制限が低い値 X に設定されており、アダプタイズするルートが多数ある場合、Cisco SD-WAN コントローラ は、X の無関係なルートをデバイスにアダプタイズし、関連するルートをアダプタイズする前に送信パス制限に達する可能性があります。これにより、ルーティングが失敗する可能性があります。関連するルートのみをアダプタイズすることで、このような失敗を防ぐことができます。

デフォルトの動作

TLOC カラーによる Cisco SD-WAN コントローラのルートフィルタリングは、デフォルトでは無効になっています。

ロジック

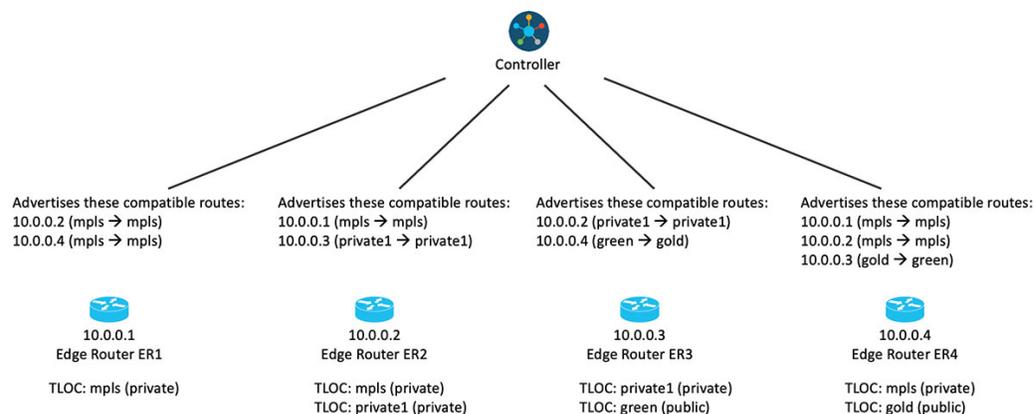
Cisco SD-WAN コントローラは、ルートに互換性があるかどうかを判断するときに、次のロジックを適用します。

- パブリックカラーを使用した TLOC は、ピアデバイス上のパブリックカラーを使用した TLOC のルートへのパスを解決できます。
- 特定のカラーの TLOC は、ピアデバイス上の同じカラーの TLOC のルートへのパスを解決できます。
- パブリックカラーを使用した TLOC は、プライベートカラーセットの TLOC を使用したパスを解決できません。

パブリックカラーには、default、biz-internet、public-internet、lte、3g、red、green、blue、gold、silver、bronze、custom1、custom2 などがあります。プライベートカラーには、mpls、metro-ethernet、private1、private2 などがあります。プライベートおよびパブリック TLOC カラーの詳細については、『*Cisco SD-WAN Routing Configuration Guide, Cisco IOS XE Release 17.x*』の「[Unicast Overlay Routing](#)」を参照してください。

たとえば、ルータにプライベートカラーを使用した TLOC のみがある場合、Cisco SD-WAN コントローラは、パブリックルートをデバイスにアダプタイズしません。同様に、ルータにパブリックカラーを使用した TLOC のみがある場合、Cisco SD-WAN コントローラは、プライベートルートをデバイスにアダプタイズしません。次の図に、より詳細な例を示します。

図 9:機能が有効になっている場合の TLOC カラーによる Cisco Catalyst SD-WAN コントローラのルートフィルタリング



TLOC のカラー割り当てを変更すると、デバイスは Cisco SD-WAN コントローラを更新します。これにより、それらが、変更に応じて TLOC カラーによる Cisco SD-WAN コントローラのルートフィルタリングを調整することが可能になります。

Override

必要に応じてデフォルトのロジックをオーバーライドし、次のいずれかを実行することができます。

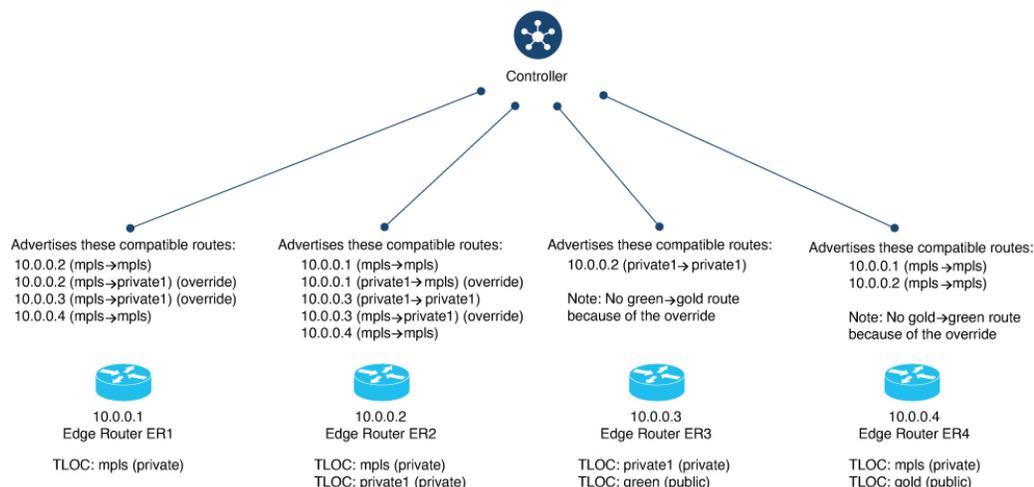
- デフォルトでは互換性がない場合でも、2つの TLOC カラーを互換性があるように設定します。
- デフォルトでは互換性がある場合でも、2つの TLOC カラーを互換性がないように設定します。

これは、特定の非標準的なシナリオで役立つ場合があります。CLI テンプレートを使用した [TLOC カラーによる Cisco SD-WAN コントローラのルートフィルタリングのデフォルト TLOC カラー互換性のオーバーライド \(199 ページ\)](#) の `tloc-color-compatibility` コマンドを参照してください。

次の図は、2つのオーバーライドを適用した、TLOC カラーによるルートフィルタリングの例を示しています。

- green と gold を互換性がないように設定します。
- mpls と private1 を互換性があるように設定します。

図 10: 機能が有効になっており、オーバーライドを適用した場合の TLOC カラーによる Cisco Catalyst SD-WAN コントローラのルートフィルタリング



変更による Cisco SD-WAN コントローラの更新

ネットワーク内のルータは、TLOC のステータスが変更されると、Cisco SD-WAN コントローラを更新します。これには、TLOC の別のカラーへの再設定が含まれる場合があります。

フラッピングによって TLOC が一時的に使用不能になることを考慮するために、TLOC ステータスの変更の報告を遅延させる減衰間隔が設けられています。デフォルトでは 60 秒ですが、60～1200 秒の値に設定できます。詳細については、[CLI テンプレートを使用した TLOC カラーによるルートフィルタリングの更新間隔の設定 \(198 ページ\)](#) を参照してください。

TLOC カラーによる Cisco SD-WAN コントローラのルートフィルタリングのサポートされるデバイス

最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a、Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.11.1

Cisco IOS XE Catalyst SD-WAN デバイスについて

TLOC カラーによる Cisco SD-WAN コントローラのルートフィルタリングの前提条件

最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a、Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.11.1

Cisco SD-WAN コントローラがパスの互換性を判断するには、TLOC のカラーを規則に従って設定する必要があります。たとえば、MPLS 接続を処理する TLOC には、カラー `mpls` が必要です。

TLOC カラーによる Cisco SD-WAN コントローラのルートフィルタリングに関する制約事項

最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a、Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.11.1

ネットワークで TLOC カラーによる Cisco SD-WAN コントローラのルートフィルタリングを有効にする場合は、必ず、ネットワーク内のすべての Cisco SD-WAN コントローラで有効にしてください。同じネットワーク内の一部の Cisco SD-WAN コントローラで TLOC カラーによるルートフィルタリングが有効になっており、他のコントローラでは無効になっているシナリオは、サポートされていません。

CLI テンプレートを使用した TLOC カラーによる Cisco SD-WAN コントローラのルートフィルタリングの設定

ここでは、TLOC カラーによる Cisco SD-WAN コントローラのルートフィルタリングを設定する方法について説明します。

CLI テンプレートを使用したルートフィルタリングの有効化

最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a、Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.11.1

CLI テンプレートの使用の詳細については、[CLI アドオン機能テンプレート](#)および[CLI テンプレート](#)を参照してください。デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

次の設定は、Cisco SD-WAN コントローラに適用されます。

1. OMP モードを開始します。

```
omp
```

2. フィルタルート コンフィギュレーション モードを開始します。

```
filter-route
```

3. ルートフィルタリングを有効にします。

```
outbound tloc-color
```

例

```
omp
  filter-route
    outbound tloc-color
!
```

CLI テンプレートを使用した TLOC カラーによるルートフィルタリングの更新間隔の設定

最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a、Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.11.1

CLI テンプレートの使用の詳細については、[CLI アドオン機能テンプレート](#)および[CLI テンプレート](#)を参照してください。デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

次の設定は、Cisco IOS XE Catalyst SD-WAN デバイスに適用されます。

1. OMP コンフィギュレーション モードを開始します。

```
omp
```

2. 更新間隔（秒単位）を 60 ~ 1200 の範囲で設定します。

```
timers
```

```
tloc-color-cap-update-interval interval
```

例

```
omp
no shutdown
ecmp-limit      6
graceful-restart
no as-dot-notation
timers
  holdtime              15
  tloc-color-cap-update-interval 120
  graceful-restart-timer 120
exit
address-family ipv4
  advertise ospf external
  advertise connected
  advertise static
!
address-family ipv6
  advertise ospf external
  advertise connected
  advertise static
!
!
```

CLI テンプレートを使用した TLOC カラーによる Cisco SD-WAN コントローラのルートフィルタリングのデフォルト TLOC カラー互換性のオーバーライド

最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a、Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.11.1

CLI テンプレートの使用の詳細については、[CLI アドオン機能テンプレート](#)および [CLI テンプレート](#)を参照してください。デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

はじめる前に

必要に応じてデフォルトのロジックをオーバーライドし、次のいずれかを実行することができます。

- デフォルトでは互換性がない場合でも、2つの TLOC カラーを互換性があるように設定します。
- デフォルトでは互換性がある場合でも、2つの TLOC カラーを互換性がないように設定します。

これは、特定の非標準的なシナリオで役立つ場合があります。

Cisco SD-WAN コントローラのルートフィルタリングのデフォルト TLOC カラー互換性のオーバーライド

次の設定は、Cisco SD-WAN コントローラに適用されます。

1. システムモードを開始します。

```
system
```

2. TLOC カラー互換性モードを開始します。

```
tloc-color-compatibility
```

3. 次の1つ以上を入力します。

- 互換性を持つように2つの TLOC カラーを設定するには、次の手順を実行します。

```
compatible first-color second-color
```

- 互換性を持たないように2つの TLOC カラーを設定するには、次の手順を実行します。

```
incompatible first-color second-color
```

例

この例では、次の操作を実行します。

- 互換性を持つように lte および private1 TLOC カラーを設定します。
- 互換性を持つように private1 および private2 TLOC カラーを設定します。
- 互換性を持たないように lte および default TLOC カラーを設定します。
- 互換性を持たないように lte および 3g TLOC カラーを設定します。

```
system
host-name vm1
system-ip 10.0.10.1
site-id 100
tloc-color-compatibility
compatible lte private1
!
compatible private1 private2
!
incompatible lte default
!
incompatible lte 3g
!
!
```

TLOC カラーによる Cisco SD-WAN コントローラ のルートフィルタリングのモニター

ここでは、TLOC カラーによる Cisco SD-WAN コントローラ のルートフィルタリングをモニターする方法について説明します。

デバイスの TLOC カラーの表示

最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a、Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.11.1

デバイスが Cisco SD-WAN コントローラにアドバタイズする TLOC カラーのリストを表示するには、Cisco SD-WAN コントローラで **show support omp peer peer-ip** コマンドを使用します。ルートフィルタリングを適用する場合、コントローラは、この TLOC カラー情報を使用して、デバイスに関連するルートを決めます。

次の例は、ピアデバイス 10.0.0.15 がアドバタイズしている TLOC カラー（この例では lte および 3g）を示しています。

```
vsmart#show support omp peer peer-ip 10.0.0.15 | inc color
ed bitmap: 0xc0, TLOC color supported list: lte 3g
```

TLOC カラーの互換性の確認

最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a、Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.11.1

TLOC カラーの互換性を確認するには、**request support omp tloc-color-compat** コマンドを使用します。

次の例では、3g と lte のカラーに互換性があるかどうかに関する情報を要求します。これらは両方ともパブリック TLOC カラーであるため、互換性があります。

```
vsmart# request support omp tloc-color-compat 3g lte
Checking compatibility for colors:3g and lte
TLOC colors: 3g and lte are compatible
```

次の例では、3g と mpls の TLOC カラーに互換性があるかどうかに関する情報を要求します。これらには、互換性はありません。

```
vsmart# request support omp tloc-color-compat 3g mpls
Checking compatibility for colors:3g and mpls
TLOC colors: 3g and mpls are incompatible
```




第 10 章

トランスポートゲートウェイ (Transport Gateway)



(注) 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

- [トランスポートゲートウェイ \(Transport Gateway\) \(204 ページ\)](#)
- [トランスポートゲートウェイに関する情報 \(204 ページ\)](#)
- [トランスポートゲートウェイの制約事項 \(211 ページ\)](#)
- [トランスポートゲートウェイのユースケース \(212 ページ\)](#)
- [Cisco SD-WAN Manager を使用したトランスポートゲートウェイとしてのルータの設定 \(214 ページ\)](#)
- [CLI テンプレートを使用したトランスポートゲートウェイとしてのルータの設定 \(215 ページ\)](#)
- [トランスポートゲートウェイ パス優先順位の設定 \(215 ページ\)](#)
- [Cisco SD-WAN Manager を使用したルータのサイトタイプの設定 \(218 ページ\)](#)
- [CLI テンプレートを使用したルータのサイトタイプの設定 \(218 ページ\)](#)
- [CLI を使用したルータのサイトタイプの確認 \(219 ページ\)](#)
- [CLI を使用したトランスポートゲートウェイ設定の確認 \(219 ページ\)](#)

トランスポートゲートウェイ (Transport Gateway)

表 51: 機能の履歴

機能名	リリース情報	説明
トランスポートゲートウェイ (Transport Gateway)	Cisco Catalyst SD-WAN Manager リリース 20.12.1 Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a	<p>トランスポートゲートウェイは、ハブアンドスポークルーティングトポロジのハブとして動作します。複雑なルーティングポリシー設定を必要とせずに、このトポロジを実現できるという利点があります。次は、トランスポートゲートウェイの使用例です。</p> <ul style="list-style-type: none"> • 分離されたアンダーレイネットワーク内のルータへの接続を提供する • 1つの個別ネットワークにおけるすべてのトラフィックが別の個別ネットワークに到達するためのゲートウェイ (ハブ) として機能する (すべてのローカルネットワークトラフィックをクラウドゲートウェイに転送するなど)

トランスポートゲートウェイに関する情報

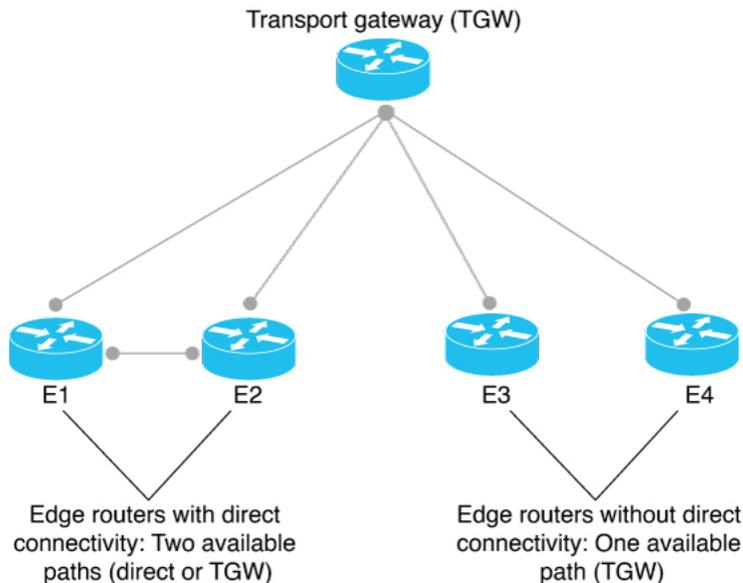
トランスポートゲートウェイは、直接接続の有無にかかわらずにルータを接続します。トランスポートゲートウェイの一般的なユースケースは、物理 LAN とクラウドベースネットワークの間など、分離されたネットワーク内のルータ間の接続を提供することです。

トランスポートゲートウェイがない場合、これらのルータの間接接続を設定する 1 つの方法は、両方のネットワークへの接続を持つ中間デバイスを介したルートを設定する制御ポリシーを作成することです。これにより、分離されたルータ間の間接接続が提供されます。このアプローチには、次の問題があります。

- 複雑さ：プレフィックスをアドバタイズするための制御ポリシーの構成は複雑です。
- 潜在的な使用不可トラフィックエンドポイント：制御ポリシーは、デバイスまたは設定されたルートが使用できないかどうかを検出できません。これにより、ルートが使用できなくなった場合にパケット損失が発生する可能性があります。

トランスポートゲートウェイとして動作するようにルータを設定すると、この問題が解決されるだけでなく、設定プロセスがより簡単になります。

図 11: トランスポートゲートウェイ (Transport Gateway)



ハブアンドスポーク トポロジ

Cisco Catalyst SD-WAN のコンテキストでは、トランスポートゲートウェイをハブとして使用することで、ハブアンドスポーク ルーティング トポロジを効率的に設定できます。これにより、複雑なルーティングポリシー設定を必要とせずに、ハブアンドスポーク トポロジを作成できます。詳細については、[ハブアンドスポーク \(222 ページ\)](#) を参照してください。

ルートの再発信

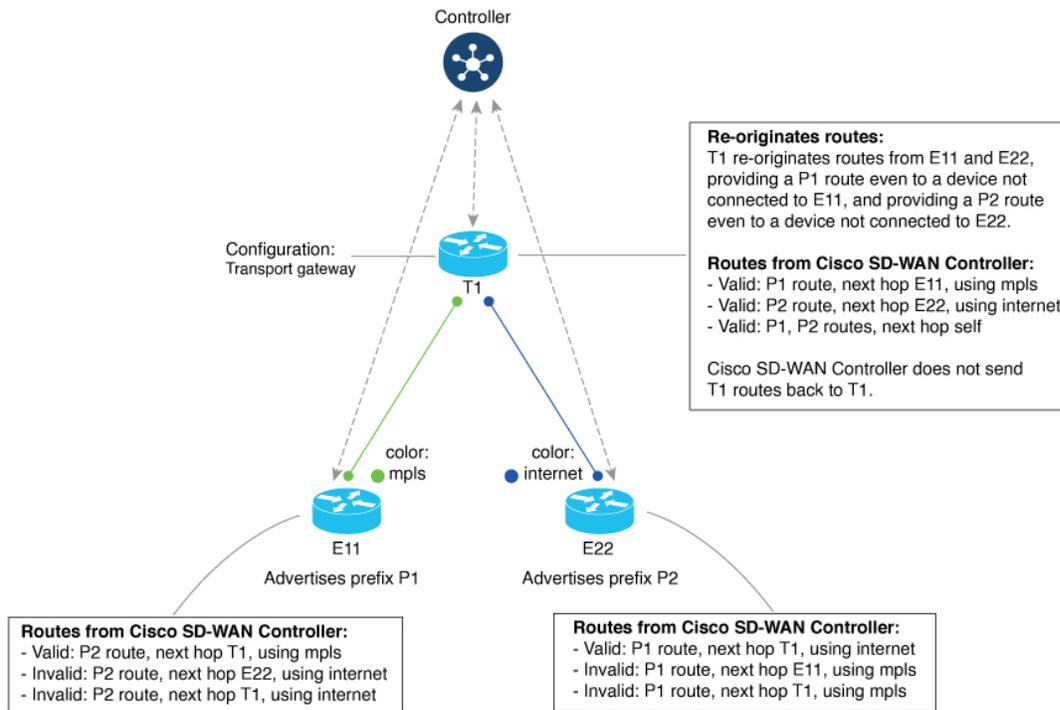
ルータは、トランスポートゲートウェイとして機能するように設定されている場合、Cisco SD-WAN コントローラから学習した各ルートに対して次のことを行います。

1. トランスポートゲートウェイは、ルートのネクストホップとして独自の TLOC を置き換え、各ルートを再発信します。これは、TLOC を各ルートのネクストホップとして置き換えることを意味します。
2. トランスポートゲートウェイは、再発信されたルートを Cisco SD-WAN コントローラにアドバタイズします。
3. トランスポートゲートウェイは、再発信するルートに独自のアフィニティ属性を付加します。ネットワーク内のルータが複数のトランスポートゲートウェイから使用可能なルートを再発信したシナリオでは、ルータは、アフィニティグループ優先順位ロジックを適用してルートを選択します。

次の図では、E11 がプレフィックス P1 をアドバタイズし、E22 がプレフィックス P2 をアドバタイズしています。E11 と E22 は分離されており、直接接続されていません。トランスポート

ゲートウェイは、E11 および E22 からのルート情報を再発信し、E22 への P1 ルートと E11 への P2 ルートを提供します。

図 12: ルートを再発信するトランスポートゲートウェイ



サイトタイプ

トランスポートゲートウェイを使用するようにネットワークを設定する手順の1つは、ネットワーク内のルータにサイトタイプパラメータを割り当てることです。サイトタイプは、ルータの意図された機能を分類し、トポロジ内のルータの位置を定義するために役立ちます。サイトタイプの値には、br、branch、cloud、spoke、type-1、type-2、および type-3 があります。

サイトタイプを割り当てたら、特定サイトタイプ宛てのトラフィックに対してのみトランスポートゲートウェイパスを優先するようにルータを設定できます。これにより、トランスポートゲートウェイパスの優先順位をよりきめ細かく設定できます。

サイトタイプは任意であり、br と spoke を除き、特定の意味を持ちません。br (境界ルータ) と spoke にはそれぞれ、マルチリージョンファブリックまたはハブアンドスポークトポロジに関する固有の用途があります。

サイトタイプの継承

ルータから発信される OMP vRoute および TLOC はすべて、ルータのサイトタイプ属性を継承します。

ルータのサイトタイプの設定については、[Cisco SD-WAN Manager](#) を使用したルータのサイトタイプの設定 (218 ページ) を参照してください。

OMP ベストパスロジックとトランスポート ゲートウェイ パス優先順位

一般に、2つのルータ間で複数のパスを使用できる場合、Overlay Management Protocol (OMP) は、ベストパス選択ロジックを適用してベストパスを選択します。ベストパス選択ロジックでは、ホップ数の少ないパスが優先されます。

トランスポートゲートウェイを設定済みの場合、トランスポートゲートウェイ再発信パス (使用可能な場合) に特定の優先順位を適用するようにルータを設定できます。これにより、以下で説明するように、設定の詳細に従って、トランスポートゲートウェイを含めるように OMP ベストパス計算が変更されます。

トランスポートゲートウェイ再発信パスの優先順位の設定については、[トランスポートゲートウェイ パス優先順位の設定 \(215 ページ\)](#) を参照してください。

ベストパスロジック

ルータ設定		結果として得られるベストパス動作
トランスポートゲートウェイ パスの動作	サイトタイプの指定	
設定なし	非対応	(デフォルトの動作)。ダイレクトパスを優先します。
Prefer Transport Gateway Path	非対応	ダイレクトパスよりもトランスポートゲートウェイ パスを優先します。
Prefer Transport Gateway Path	あり	指定されたサイトタイプに一致するトランスポートゲートウェイパスの場合、ダイレクトパスよりもトランスポートゲートウェイパスを優先します。 指定されたサイトタイプに一致しないトランスポートゲートウェイパスの場合、トランスポートゲートウェイパスよりもダイレクトパスを優先します。
Do ECMP Between Direct and Transport Gateway Paths	非対応	ダイレクトパスとトランスポートゲートウェイパスを同等に扱います。

ルータ設定		結果として得られるベストパス動作
トランスポートゲートウェイパスの動作	サイトタイプの指定	
Do ECMP Between Direct and Transport Gateway Paths	あり	指定されたサイトタイプに一致するトランスポートゲートウェイパスの場合、ダイレクトパスとトランスポートゲートウェイパスを同等に扱います。 指定されたサイトタイプに一致しないトランスポートゲートウェイパスの場合、トランスポートゲートウェイパスよりもダイレクトパスを優先します。

複数トランスポートゲートウェイオプション

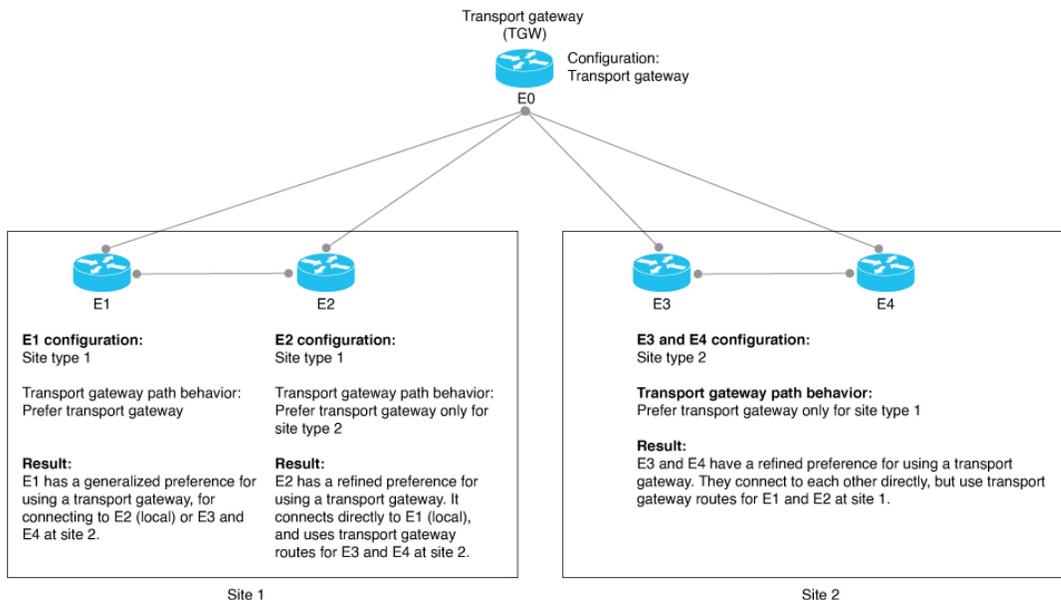
前述のように、トランスポートゲートウェイは、再発信するパスに独自のアフィニティ属性を付加します。ネットワーク内のルータが複数のトランスポートゲートウェイから使用可能なパスを再発信したシナリオでは、ルータは、アフィニティグループ優先順位ロジックを適用してパスを選択します。

コンフィギュレーションの概要

1. トランスポートゲートウェイとして機能するようにルータを設定するには、システム機能テンプレートまたは CLI アドオンテンプレートを使用します。[Cisco SD-WAN Manager を使用したトランスポートゲートウェイとしてのルータの設定 \(214 ページ\)](#) を参照してください。
2. トランスポートゲートウェイパスを使用するようにルータを設定するには、OMP 機能テンプレートまたは CLI アドオンテンプレートを使用します。[Cisco SD-WAN Manager を使用したトランスポートゲートウェイパス優先順位の設定 \(216 ページ\)](#) を参照してください。次のように OMP ロジックを構成できます。
 - ダイレクトパスよりもトランスポートゲートウェイパスを優先します。
 - サイトタイプ属性に応じて、特定トラフィックについてのみトランスポートゲートウェイパスを優先します。[Cisco SD-WAN Manager を使用したルータのサイトタイプの設定 \(218 ページ\)](#) を参照してください。
 - ダイレクトパスとトランスポートゲートウェイパスは同等であるとみなします。

次の図は、ネットワーク内のルータがトランスポートゲートウェイを使用して動作し、すべてのトラフィックまたは特定トラフィックをトランスポートゲートウェイルートを通じて優先的に転送する方法を示しています。

図 13: エッジルータとトランスポートゲートウェイパス優先順位



図のデバイスは、次のように設定されています。

デバイス	設定
E0	<p>1. トランスポートゲートウェイとして設定します。</p> <ul style="list-style-type: none"> • 機能テンプレートを 使用 : Cisco システムテンプレートで、[Transport Gateway] フィールドを使用します。 • CLI アドオンテンプレートを 使用 : system transport-gateway enable

デバイス	設定
E1	<p>1. サイトタイプを <code>type-1</code> として設定します。</p> <ul style="list-style-type: none"> • 機能テンプレートを使用 : Cisco システムテンプレートで、[Site Type] フィールドを使用します。 • CLI アドオンテンプレートを使用 : system site-type type-1 <p>2. ベストパスについて、トランスポート ゲートウェイ ルートの優先順位を設定します。</p> <ul style="list-style-type: none"> • 機能テンプレートを使用 : OMP テンプレートで、[Transport Gateway Path Behavior] フィールドを使用します。[Prefer Transport Gateway Path] オプションを選択します。 • CLI アドオンテンプレートを使用 : omp best-path transport-gateway prefer
E2	<p>1. サイトタイプを <code>type-1</code> として設定します。</p> <ul style="list-style-type: none"> • 機能テンプレートを使用 : Cisco システムテンプレートで、[Site Type] フィールドを使用します。 • CLI アドオンテンプレートを使用 : system site-type type-1 <p>2. ベストパスについて、<code>type-2</code> デバイスへのトラフィックに関するトランスポート ゲートウェイ ルートの優先順位を設定します。</p> <ul style="list-style-type: none"> • 機能テンプレートを使用 : OMP テンプレートで、[Transport Gateway Path Behavior] フィールドを使用します。[Prefer Transport Gateway Path] オプションを選択します。[Site Types] フィールドで、[type-2] を選択します。 • CLI アドオンテンプレートを使用 : omp best-path transport-gateway prefer transport-gateway-settings type-2

デバイス	設定
E3 および E4	<p>1. サイトタイプを <code>type-2</code> として設定します。</p> <ul style="list-style-type: none"> 機能テンプレートを使用 : Cisco システムテンプレートで、[Site Type] フィールドを使用します。 CLI アドオンテンプレートを使用 : system site-type type-2 <p>2. ベストパスについて、<code>type-1</code> デバイスへのトラフィックに関するトランスポートゲートウェイ ルートの優先順位を設定します。</p> <ul style="list-style-type: none"> 機能テンプレートを使用 : OMP テンプレートで、[Transport Gateway Path Behavior] フィールドを使用します。[Prefer Transport Gateway Path] オプションを選択します。[Site Types] フィールドで、[type-1] を選択します。 CLI アドオンテンプレートを使用 : omp best-path transport-gateway prefer transport-gateway-settings type-1

トランスポートゲートウェイの制約事項

制約事項	説明
トランスポートゲートウェイ機能のリソース要求	トランスポートゲートウェイ機能のリソース要求のため、追加の負荷を処理する CPU とメモリリソースを備えた高性能デバイスでのみこれを有効にすることをお勧めします。特定のリソース要件は、ネットワーク環境によって異なります。
複数のトランスポートゲートウェイ : ベストパス	複数のデバイスでトランスポートゲートウェイ機能を有効にすると、エッジルータは、ベストパス選択ロジックを適用してベストパスを決定します。これには、複数のトランスポートゲートウェイパスが含まれる場合があります。

制約事項	説明
複数のトランスポートゲートウェイ：ルーティンググループの防止	ネットワーク内の複数のデバイスでトランスポートゲートウェイ機能を有効にすると、ルーティンググループを回避するために、ネットワークのCisco SD-WAN コントローラは、次のように動作します：Cisco SD-WAN コントローラは、あるトランスポートゲートウェイによって再発信されたルートを受信すると、そのルートを別のトランスポートゲートウェイにアドバタイズしません。別のトランスポートゲートウェイへのトランスポートゲートウェイルートへのアドバタイズを防止することにより、ルーティンググループが回避されます。
オンデマンドトンネル	トランスポートゲートウェイとして構成されたデバイスに動的オンデマンドトンネルを構成することはできません。ただし、トランスポートゲートウェイとして動作していないエッジルータは、オンデマンドトンネルを使用できます。動的オンデマンドトンネルの詳細については、『Cisco SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.x』の「 Dynamic On-Demand Tunnels 」を参照してください。

トランスポートゲートウェイのユースケース

このユースケースでは、組織は、ローカルネットワークとクラウドサービス ネットワーク (AzureやAWSなど) をブリッジする必要があります。ローカルネットワークとクラウドネットワークのエッジルータには直接接続がありません。

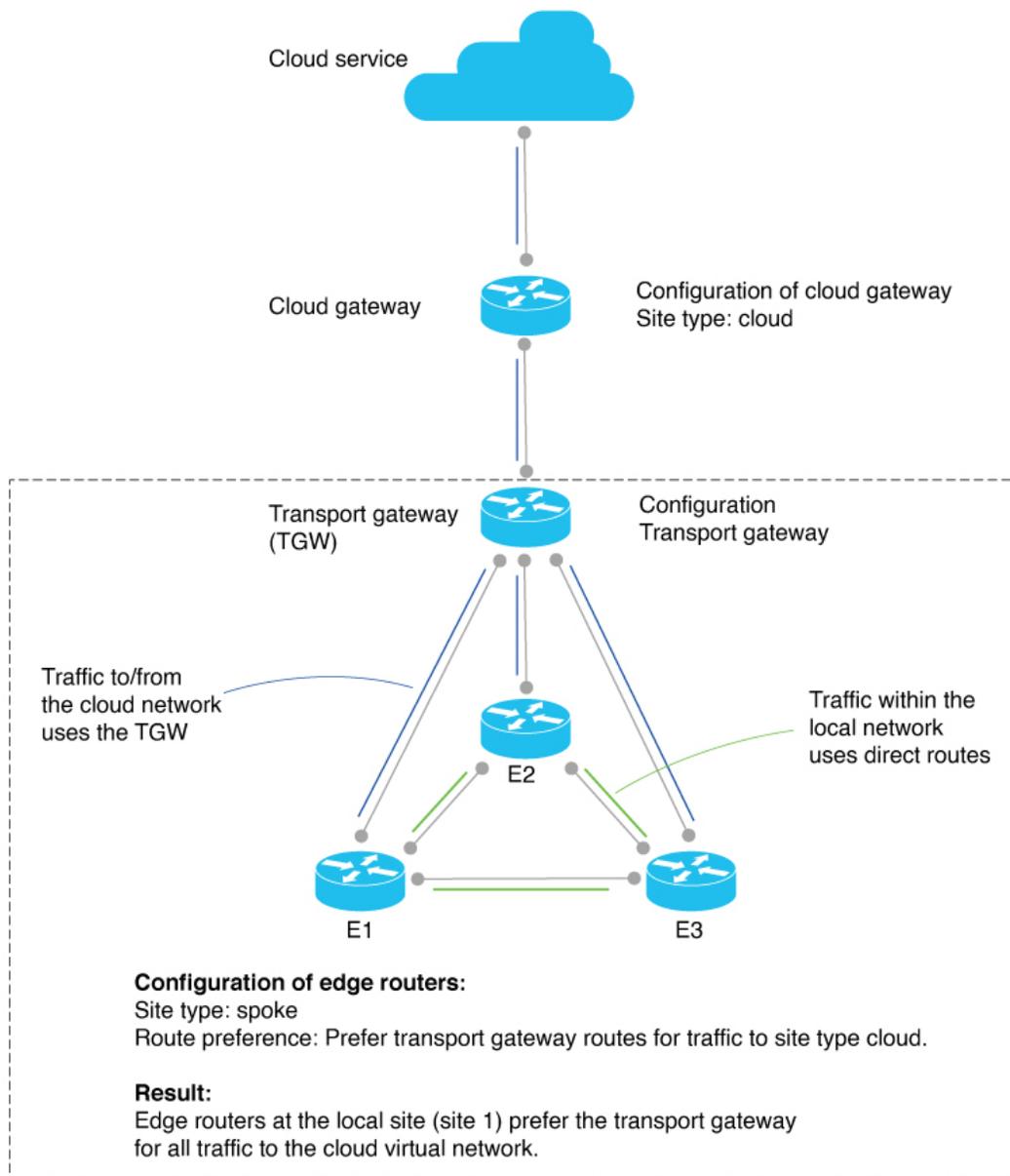
ローカルネットワークとクラウドネットワークをブリッジするトランスポートゲートウェイを作成するには、ネットワーク管理者が、次のようにデバイスを設定します。

Intent	設定するデバイス	設定
クラウドゲートウェイルータをサイトタイプ cloud で設定します。	クラウドゲートウェイルータ	<ol style="list-style-type: none"> 1. サイトタイプを cloud に設定します。 <ul style="list-style-type: none"> • 機能テンプレートを使用：Cisco システムテンプレートで、[Site Type] フィールドを使用します。 • CLI テンプレートを使用： <code>system site-type cloud</code>

Intent	設定するデバイス	設定
<p>ローカルネットワーク内のデバイスからのクラウド宛てトラフィックのハブとして動作するトランスポートゲートウェイを展開します。トランスポートゲートウェイは、クラウド宛てトラフィックを取り込み、クラウドベースネットワークのクラウドゲートウェイにルーティングします。</p>	<p>トランスポートゲートウェイルータ</p>	<p>1. トランスポートゲートウェイとして有効にします。</p> <ul style="list-style-type: none"> • 機能テンプレートを使用：Cisco システムテンプレートで、[Transport Gateway] フィールドを使用します。 • CLI テンプレートを使用： system transport-gateway enable
<p>ローカルネットワーク内のトラフィックは、トランスポートゲートウェイルートではなく、直接ルートを使用します。ローカルネットワークからクラウドへのトラフィックは、トランスポートゲートウェイルートを使用します。</p>	<p>ローカルネットワークのエッジルータ</p>	<p>1. すべてのクラウド宛てトラフィックについて、トランスポートゲートウェイルートを使用します。</p> <ul style="list-style-type: none"> • 機能テンプレートを使用：OMP テンプレートで、[Transport Gateway Path Behavior] フィールドを使用します。[Prefer Transport Gateway Path] オプションを選択します。 • CLI テンプレートを使用： omp best-path transport-gateway prefer transport-gateway-settings cloud <p>2. サイトタイプを spoke として設定します。</p> <ul style="list-style-type: none"> • 機能テンプレートを使用：Cisco システムテンプレートで、[Site Type] フィールドを使用します。 • CLI テンプレートを使用： system site-type spoke

次の図は、このトポロジと設定を示します。

図 14: トランスポートゲートウェイのトポロジと設定



Cisco SD-WAN Manager を使用したトランスポートゲートウェイとしてのルータの設定

1. Cisco SD-WAN Manager メニューから、[Configuration] > [Templates] を選択します。

2. [Feature Templates] をクリックします。
3. 次のいずれかを実行します。
 - 新しいシステムテンプレートを作成するには、[Add Template] をクリックし、デバイスタイプを選択して、[Cisco System] をクリックします。
 - 既存のシステムテンプレートを編集するには、既存の機能テンプレートのテーブルでシステムテンプレートを見つけ、テンプレートの横にある [...] をクリックして、[Edit] を選択します。
4. [Basic Configuration] の [Transport Gateway] フィールドで、[On] を選択します。
5. [Save] (新しいテンプレートを作成する場合) または [Update] (既存のテンプレートを編集する場合) をクリックします。

CLI テンプレートを使用したトランスポートゲートウェイとしてのルータの設定

CLI テンプレートの使用の詳細については、[CLI アドオン機能テンプレート](#)および [CLI テンプレート](#)を参照してください。デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

1. システム コンフィギュレーション モードを開始します。

```
system
```

2. トランスポートゲートウェイ機能を有効にします。

```
transport-gateway enable
```



(注) トランスポートゲートウェイ機能を無効にするには、このコマンドの **no** 形式を使用します。

例

```
system
transport-gateway enable
```

トランスポート ゲートウェイ パス優先順位の設定

ここでは、トランスポートゲートウェイ再発信パスを処理するようにルータのベストパス決定を設定する方法について説明します。

Cisco SD-WAN Manager を使用したトランスポートゲートウェイパス優先順位の設定

1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Templates]** を選択します。
2. **[Feature Templates]** をクリックします。
3. 次のいずれかを実行します。
 - 新しいOMPテンプレートを作成するには、**[Add Template]** をクリックし、デバイスタイプを選択して、**[Cisco OMP]** をクリックします。
 - 既存のOMPテンプレートを編集するには、既存の機能テンプレートのテーブルでOMPテンプレートを見つけ、テンプレートの横にある **[...]** をクリックして、**[Edit]** を選択します。
4. **[Best Path]** セクションの **[Transport Gateway Path Behavior]** フィールドで、**[Global]** モードを選択し、次のオプションのいずれかを選択します。

オプション	説明
Do ECMP Between Direct and Transport Gateway Paths	トランスポートゲートウェイとダイレクトパスを介して接続できるデバイスの場合、使用可能なすべてのパスに等コストマルチパス (ECMP) を適用します。
Prefer Transport Gateway Path	トランスポートゲートウェイを介して接続できるデバイスの場合、他のパスが使用可能な場合でも、トランスポートゲートウェイパスのみを使用します。



(注) このフィールドを設定しない場合、デフォルトでは、ルータは、ダイレクトパスをベストパスとして優先します。

5. (任意) **[Site Types]** フィールドをクリックし、トランスポートゲートウェイの動作を適用する1つ以上のサイトタイプを選択します。**[Site Types]** のパラメータが **[Transport Gateway Path Behavior]** のパラメータとどのように連動するのかについては、[OMP ベストパスロジックとトランスポートゲートウェイパス優先順位 \(207 ページ\)](#) を参照してください。
6. **[Save]** (新しいテンプレートを作成する場合) または **[Update]** (既存のテンプレートを編集する場合) をクリックします。

CLI テンプレートを使用したトランスポート ゲートウェイ パス優先順位の設定

トランスポートゲートウェイを使用するようにデバイスを設定するには、そのデバイスで次の手順を実行します。

1. SD-WAN コンフィギュレーション モードを開始します。

```
sdwan
```

2. システム OMP コンフィギュレーション モードを開始します。

```
omp
```

3. 次のいずれかのオプションを使用して、トランスポート ゲートウェイ パスの設定を構成します。

```
best-path transport-gateway {prefer | ecmp-with-direct-path}
```

オプション	説明
ecmp-with-direct path	トランスポートゲートウェイとダイレクトパスを介して接続できるデバイスの場合、使用可能なすべてのパスに等コストマルチパス (ECMP) を適用します。
prefer	トランスポートゲートウェイを介して接続できるデバイスの場合、他のパスが使用可能な場合でも、トランスポートゲートウェイ パスのみを使用します。

4. (任意) トランスポートゲートウェイの動作を適用する 1 つ以上のサイトタイプを指定します。[Site Types] のパラメータが [Transport Gateway Path Behavior] のパラメータとどのように連動するのかについては、[OMP ベストパスロジックとトランスポート ゲートウェイ パス優先順位 \(207 ページ\)](#) を参照してください。

```
omp best-path transport-gateway-settings site-types site-types
```

オプション	説明
site-types	1 つ以上のサイトタイプ (cloud 、 branch 、 br 、 type-1 、 type-2 、 type-3) をスペースで区切って含めます。



(注) このコマンドを使用するには、必ず、前の手順で **omp best-path transport-gateway prefer** を使用してください。

例

次の例では、トランスポート ゲートウェイ ルートを優先するようにデバイスを設定しています。

```
sdwan
omp
omp best-path transport-gateway prefer
```

次の例では、サイトタイプが **cloud** のサイト宛てのトラフィックについてのみトランスポートゲートウェイ ルートを優先するようにデバイスを設定しています。

```
sdwan
omp
omp best-path transport-gateway prefer
omp best-path transport-gateway-settings site-types cloud
```

Cisco SD-WAN Manager を使用したルータのサイトタイプの設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. **[Feature Templates]** をクリックします。
3. 次のいずれかを実行します。
 - 新しいシステムテンプレートを作成するには、**[Add Template]** をクリックし、デバイスタイプを選択して、**[Cisco System]** をクリックします。
 - 既存のシステムテンプレートを編集するには、既存の機能テンプレートのテーブルでシステムテンプレートを見つけ、テンプレートの横にある **[...]** をクリックして、**[Edit]** を選択します。
4. **[Basic Configuration]** で、**[Site Type]** をクリックし、ドロップダウンリストからタイプを選択します。
5. **[Save]** (新しいテンプレートを作成する場合) または **[Update]** (既存のテンプレートを編集する場合) をクリックします。

CLI テンプレートを使用したルータのサイトタイプの設定

CLI テンプレートの使用の詳細については、[CLI アドオン機能テンプレート](#) および [CLI テンプレート](#) を参照してください。デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

1. システム コンフィギュレーション モードを開始します。

```
system
```

2. ルータのサイトタイプを最大 4 つ設定します。有効な値は、br、branch、cloud、spoke、type-1、type-2、および type-3 です。

```
site-type site-type
```



(注) トランスポートゲートウェイ機能を無効にするには、このコマンドの **no** 形式を使用します。

例

次に、ルータのサイトタイプを **cloud** として設定する例を示します。

```
system
  site-type cloud
```

例

次に、ルータをサイトタイプ **cloud** および **branch** で設定する例を示します。

```
system
  site-type cloud branch
```

CLI を使用したルータのサイトタイプの確認

ルータのサイトタイプ設定を確認するには、デバイスに関して **show sdwan omp summary** コマンドを使用します。出力には、**site-type** フィールドと設定されている値が含まれます。

この例では、ルータはサイトタイプ **spoke** で設定されています。

```
Device#show sdwan omp summary
...
site-type      SPOKE
...
```

CLI を使用したトランスポートゲートウェイ設定の確認

デバイスで **show sdwan running-config system** コマンドを使用して、デバイスがトランスポートゲートウェイとして設定されているかどうかを確認します。出力では、**[transport-gateway enable]** は、設定されていることを示しています。

```
Device#show sdwan running-config system
system
system-ip          192.168.1.1
domain-id         1
site-id           11100
region 1
!
role               border-router
transport-gateway enable
...
```

デバイスで **show sdwan omp summary** コマンドを使用して、デバイスがトランスポートゲートウェイとして設定されているかどうかを確認することもできます。出力では、**[transport-gateway enabled]** は、トランスポートゲートウェイ機能が有効になっていることを示しています。



第 11 章

ハブアンドスポーク



(注) 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

- [ハブアンドスポーク \(222 ページ\)](#)
- [ハブアンドスポークについて \(222 ページ\)](#)
- [ハブアンドスポークに関する制約事項 \(234 ページ\)](#)
- [ハブアンドスポークのユースケース \(234 ページ\)](#)
- [ハブアンドスポークトポロジの設定 \(235 ページ\)](#)
- [ハブアンドスポーク設定の確認 \(237 ページ\)](#)

ハブアンドスポーク

表 52: 機能の履歴

機能名	リリース情報	説明
ハブアンドスポーク 設定	Cisco Catalyst SD-WAN Manager リ リース 20.12.1 Cisco IOS XE Catalyst SD-WAN リ リース 17.12.1a	ハブアンドスポーク設定により、ハブアンドスポークトポロジの設定プロセスが簡素化され、複雑な集中管理ポリシーが不要になります。代わりに、いくつかの簡単な設定手順のみで設定できます。つまり、(a) ネットワークにサービスを提供する Cisco SD-WAN コントローラ、(b) ハブとして機能するルータ、および (c) スポークとして動作するルータのそれぞれで1つのコマンドを実行するだけです。

ハブアンドスポークについて

ハブアンドスポークトポロジはネットワーキングの基礎となりますが、このトポロジの設定は複雑で、専門知識が必要になる場合があります。Cisco Catalyst SD-WAN 環境では、集中管理ポリシーの設定手順が長時間になる可能性があります。

Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a 以降では、新しい設定メソッドにより、複雑な制御ポリシーを必要とせず、迅速なハブアンドスポーク設定が実現されます。簡単に言えば、このメソッドでは、ネットワークにサービスを提供する Cisco SD-WAN コントローラを設定してハブアンドスポークを有効にし、ハブとして機能するルータでトランスポートゲートウェイ機能を設定します。



(注) 結果として得られるハブアンドスポークトポロジは、すべての VRF に適用されます。

コンフィギュレーションの概要

Cisco Catalyst SD-WAN のハブアンドスポーク設定には、次の表に示す3つの部分があります。

Intent	設定するデバイスまたはコントローラ	設定
1. ネットワークでハブアンドスポークトポロジを有効にします。	ネットワークにサービスを提供する Cisco SD-WAN コントローラ	<p>ネットワークでハブアンドスポーク設定を有効にします。</p> <p>次を参照してください。</p> <ul style="list-style-type: none"> • Cisco SD-WAN Manager を使用したハブアンドスポークを有効にするための Cisco Catalyst SD-WAN コントローラ の設定 (235 ページ) • CLI テンプレートをを使用してハブアンドスポークを有効にするための Cisco SD-WAN コントローラ の設定 (236 ページ) <p>CLI テンプレートメソッドでは、topology hub-and-spoke enable コマンドを使用します。</p>
2. ルータを、ハブとして機能するトランスポートゲートウェイとして設定します。	ハブとして指定されたルータ	<p>ルータでトランスポートゲートウェイ機能を有効にします。</p> <p>トランスポートゲートウェイとしてのルータの設定 (ハブアンドスポークの場合) (236 ページ) を参照してください。</p> <p>CLI テンプレートメソッドでは、transport-gateway enable コマンドを使用します。</p>
3. ルータをスポークとして機能するように設定します。	スポークとして指定されたルータ	<p>デバイスサイトタイプを spoke として設定します。</p> <p>ルータのサイトタイプの設定 (ハブアンドスポークの場合) (237 ページ) を参照してください。</p> <p>CLI テンプレートメソッドでは、site-type コマンドを使用します。</p>

結果

この設定により、次のようになります。

- ネットワーク内の Cisco SD-WAN コントローラは、ネットワーク内の各ルータにアドバタイズする TLOC およびルート情報をフィルタ処理します。

- ハブ（トランスポートゲートウェイ）として動作するルータは、すべてのTLOCおよびルート情報を受信します。
- スポークとして動作するルータは、ネットワーク内のハブ（トランスポートゲートウェイ）に関するTLOCおよびルート情報を受信します。他のスポークに関するTLOCまたはルートは受信しません。その結果、スポークデバイス間にBidirectional Forwarding Detection (BFD) セッションは存在しません。
- すべてのスポーク間トラフィックはトランスポートゲートウェイを通過し、各スポークのルートが再発信されます。

これらを組み合わせると、ハブアンドスポークトポロジが実現します。

例：ハブアンドスポーク接続

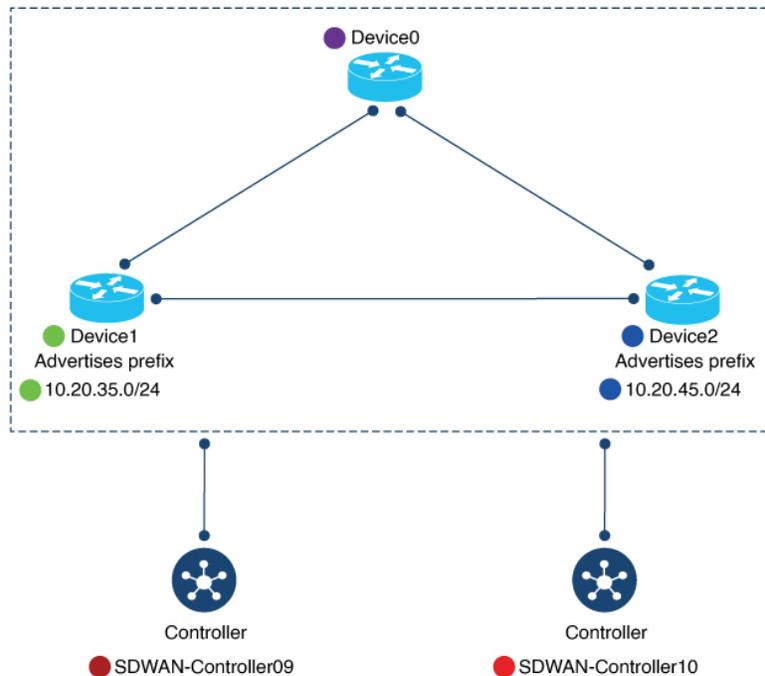
このセクションの詳細な例では、フルメッシュネットワークをハブアンドスポークトポロジに変換したときにネットワーク内のデバイス間の接続がどのように変更されるかが示されます。次の表に、この例のデバイスに関する情報と、この例のセクションで後に続く多数の図で使用されている色分けを示します。

表 53: デバイス、IPアドレス、ロール、インターフェイス、およびプレフィックス

デバイス	目的のロール	インターフェイス	Prefixes
Device0 172.16.255.15 図の色：紫色	ハブ	10.0.20.15 (3g) 10.1.15.15 (LTE)	なし
Device1 172.16.255.35 図の色：緑色	Spoke1	10.5.1.35 (LTE)	10.20.35.0/24 図の色：緑色でハイライト
Device2 172.16.255.45 図の色：青色	Spoke2	10.0.6.45 (LTE)	10.20.45.0/24 図の色：青色でハイライト
SDWAN-Controller09 172.16.255.19 図の色：暗い赤色	Cisco SD-WAN コントローラ	N/A	N/A
SDWAN-Controller10 172.16.255.20 図の色：赤色	Cisco SD-WAN コントローラ	N/A	N/A

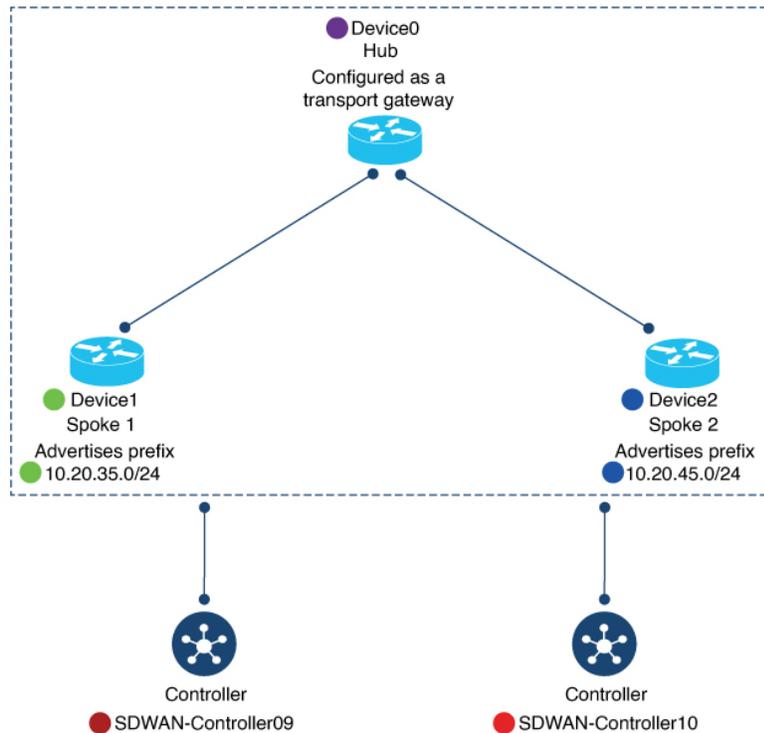
次の図は、ハブアンドスポークを設定する前のフルメッシュ接続によるネットワークの初期状態を示しています。

図 15:変更前：フルメッシュ接続



次の図は、ハブアンドスポークを設定した後のネットワーク接続を示しています。

図 16: 変更後 : ハブアンドスポーク接続



Device0 (ハブ) の設定前と設定後

ここでは、ハブアンドスポーク設定前後の Device0 (ハブ) の接続を示します。これには、次の情報が含まれます。

- BFD セッション
- OMP ルート
- IP ルート

BFD セッション

ハブアンドスポークを設定する前に、Device0 (将来のハブ) で `show sdwan bfd sessions` コマンドを実行すると、Device1 (Spoke1) と Device2 (Spoke1) の両方との BFD セッションがあることが示されます。

ハブアンドスポークの設定後、Device0 (ハブ) は、Device1 (Spoke1) と Device2 (Spoke2) の両方との同じ BFD セッションを保持します。

図 17: ハブ : 設定前と設定後の BFD セッション

Before

```
Device0-future-hub#show sdwan bfd sessions
```

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP	DST PUBLIC	IP
172.16.255.45	2500	up	3g	lte	10.0.20.15		10.0.6.45
172.16.255.35	1500	up	3g	lte	10.0.20.15		10.5.1.35
172.16.255.45	2500	up	lte	lte	10.1.15.15		10.0.6.45
172.16.255.35	1500	up	lte	lte	10.1.15.15		10.5.1.35

BFD sessions with Device1 (green) and Device2 (blue)

After

```
Device0-Hub#show sdwan bfd sessions
```

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP	DST PUBLIC	IP
172.16.255.45	2500	up	3g	lte	10.0.20.15		10.0.6.45
172.16.255.35	1500	up	3g	lte	10.0.20.15		10.5.1.35
172.16.255.45	2500	up	lte	lte	10.1.15.15		10.0.6.45
172.16.255.35	1500	up	lte	lte	10.1.15.15		10.5.1.35

BFD sessions with Device1 (green) and Device2 (blue)

OMP ルート

ハブアンドスポークを設定する前に、Device0 (将来のハブ) で `show sdwan omp route vpn 1` コマンドを実行すると、Device1 (Spoke1) および Device2 (Spoke2) によってアドバタイズされるプレフィックスがそれぞれ Device1 (Spoke1) および Device2 (Spoke2) を介してのみ到達可能であることが示されます。

Device0 (ハブ) でハブアンドスポークを設定すると、Device1 (Spoke1) プレフィックスと Device2 (Spoke2) プレフィックスがハブ自体を介して到達可能になります (**FROM PEER** 列には **0.0.0.0** と表示されます)。

図 18: ハブ: 設定前と設定後の OMP ルート

Before

```
Device0-future-hub#show sdwan omp route vpn 1
```

TENANT	VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP	COLOR
Device1 prefix	0	10.20.35.0/24	172.16.255.19	13	1003	C,I,R	installed	172.16.255.35	lte
			172.16.255.20	21	1003	C,R	installed	172.16.255.35	lte
	0	10.20.45.0/24	172.16.255.19	46	1003	C,I,R	installed	172.16.255.45	lte
			172.16.255.20	17	1003	C,R	installed	172.16.255.45	lte

After

```
Device0-hub#show sdwan omp route vpn 1
```

TENANT	VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP	COLOR
Device1 prefix	0	10.20.35.0/24	0.0.0.0	10737	1003	C,Red,R,	installed	172.16.255.15	lte
			0.0.0.0	41894	1003	TGW-R			
			0.0.0.0	10737	1003	C,Red,R,	installed	172.16.255.15	3g
	0	10.20.45.0/24	172.16.255.19	8	1003	C,I,R	installed	172.16.255.35	lte
			172.16.255.20	8	1003	C,R	installed	172.16.255.35	lte
			0.0.0.0	10737	1003	C,Red,R,	installed	172.16.255.15	lte
Device2 prefix	0	0.0.0.0	0.0.0.0	41894	1003	TGW-R			
			0.0.0.0	10737	1003	C,Red,R,	installed	172.16.255.15	3g
			0.0.0.0	41895	1003	TGW-R			
Device2 prefix	0	0.0.0.0	172.16.255.19	9	1003	C,I,R	installed	172.16.255.45	lte
			172.16.255.20	9	1003	C,R	installed	172.16.255.45	lte

IP ルート

ハブアンドスポークを設定する前に、Device0 (将来のハブ) で `show ip route vrf 1` コマンドを実行すると、Device1 (Spoke1) および Device2 (Spoke2) によってアドバタイズされるプレフィックスがそれぞれ Device1 (Spoke1) および Device2 (Spoke2) を介して到達可能であることが示されます。

ハブアンドスポークを設定した後、Device0 (ハブ) については、これは同じままです。

図 19:ハブ：設定前と設定後の IP ルート

```

Before
Device0-hub#show ip route vrf 1

m    10.20.35.0/24 [251/0] via 172.16.255.35, 09:20:11, Sdwan-system-intf
m    10.20.45.0/24 [251/0] via 172.16.255.45, 09:20:11, Sdwan-system-intf
    \
    /
    Device1 prefix (green) via Device1 (green)
    Device2 prefix (blue) via Device 2 (blue)

```

```

After
Device0-hub#show ip route vrf 1

m    10.20.35.0/24 [251/0] via 172.16.255.35, 10:14:26, Sdwan-system-intf
m    10.20.45.0/24 [251/0] via 172.16.255.45, 10:14:26, Sdwan-system-intf
    \
    /
    Device1 prefix (green) via Device1 (green)
    Device2 prefix (blue) via Device 2 (blue)

```

Device1 (Spoke1) の設定前と設定後

ここでは、ハブアンドスポーク設定前後の Device1 (Spoke1) の接続を示します。これには、次の情報が含まれます。

- BFD セッション
- OMP ルート
- IP ルート

BFD セッション

ハブアンドスポークを設定する前に、Device1 (将来の Spoke1) で `show sdwan bfd sessions` コマンドを実行すると、Device0 (将来のハブ) と Device2 (将来の Spoke2) の両方との BFD セッションが示されます。

ハブアンドスポークを設定すると、Device1 (Spoke1) では、他のスポークではなくハブとの BFD セッションのみが示されます (この例では、Spoke2 との BFD セッションは示されません)。

図 20: Spoke1: 設定前と設定後の BFD セッション

Before

```
Device1-future-spoke1#show sdwan bfd sessions
```

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP	DST PUBLIC IP
172.16.255.45	2500	up	lte	lte	10.5.1.35	10.0.6.45
172.16.255.15	500	up	lte	3g	10.5.1.35	10.0.20.15
172.16.255.15	500	up	lte	lte	10.5.1.35	10.1.15.15

BFD sessions with Device2 (blue) and Hub (purple)

After

```
Device1-spoke1#show sdwan bfd sessions
```

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP	DST PUBLIC IP
172.16.255.15	500	up	lte	3g	10.5.1.35	10.0.20.15
172.16.255.15	500	up	lte	lte	10.5.1.35	10.1.15.15

BFD sessions only with Hub (purple)

OMP ルート

ハブアンドスポークを設定する前に、Device1 (将来の Spoke1) で `show sdwan omp route vpn 1` コマンドを実行すると、Device2 を介して Device2 (Spoke2) プレフィックスに直接到達できることが示されます。これは、**TLOC IP** 列に Device2 のシステム IP が表示されることから明らかです。

ハブアンドスポークを設定すると、Device1 (Spoke1) はハブを介してのみ Device2 (Spoke2) プレフィックスに到達できます。

図 21: Spoke1 : 設定前と設定後の OMP ルート

Before
Device1-future-spoke1#show sdwan omp route vpn 1

TENANT	VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP	COLOR
0	1	10.20.45.0/24	172.16.255.19	43	1003	C,I,R	installed	172.16.255.45	lte
			172.16.255.20	21	1003	C,R	installed	172.16.255.45	lte

Device2 prefix (points to PREFIX)
via Device2 (points to TLOC IP)

After
Device1-spoke1#show sdwan omp route vpn 1

TENANT	VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP	COLOR
0	1	10.20.45.0/24	172.16.255.19	10	1003	C,I,R	installed	172.16.255.15	lte
			172.16.255.19	11	1003	C,I,R	installed	172.16.255.15	3g
			172.16.255.20	10	1003	C,R	installed	172.16.255.15	lte
			172.16.255.20	11	1003	C,R	installed	172.16.255.15	3g

Device2 prefix (points to PREFIX)
via Hub (points to TLOC IP)

IP ルート

ハブアンドスポークを設定する前に、Device1 (将来の Spoke1) で `show ip route vrf 1` コマンドを実行すると、Device2 を介して Device2 プレフィックスに直接到達できることが示されます。ハブアンドスポークを設定すると、Device1 (Spoke1) はハブを介してのみ Device2 (Spoke2) プレフィックスに到達できます。

図 22: Spoke1 : 設定前と設定後の IP ルート

Before
Device1-future-spoke1#show ip route vrf 1

```
m 10.20.45.0/24 [251/0] via 172.16.255.45, 06:03:36, Sdwan-system-intf
```

Device2 prefix (blue) via Device2 (blue)

After
Device1-spoke1#show ip route vrf 1

```
m 10.20.45.0/24 [251/0] via 172.16.255.15, 10:14:58, Sdwan-system-intf
```

Device2 prefix (blue) via Hub (purple)

Device2 (Spoke2) の設定前と設定後

ここでは、ハブアンドスポーク設定前後の Device2 (Spoke2) の接続を示します。これには、次の情報が含まれます。

- BFD セッション

- OMP ルート
- IP ルート

ハブアンドスポークを設定する前と後の Device2 の変化は、Device1 の変化とほとんど同じです。

BFD セッション

ハブアンドスポークを設定する前に、Device2 (将来の Spoke2) で `show sdwan bfd sessions` コマンドを実行すると、Device0 (将来のハブ) と Device1 (将来の Spoke1) の両方との BFD セッションが示されます。

ハブアンドスポークを設定すると、Device2 (Spoke2) では、他のスポークではなくハブとの BFD セッションのみが示されます (この例では、Spoke1 との BFD セッションは示されません)。

図 23: Spoke2: 設定前と設定後の BFD セッション

Before

```
Device2-future-spoke2#show sdwan bfd sessions
```

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP	DST PUBLIC	IP
172.16.255.35	1500	up	lte	lte	10.0.6.45		10.5.1.35
172.16.255.15	500	up	lte	3g	10.0.6.45		10.0.20.15
172.16.255.15	500	up	lte	lte	10.0.6.45		10.1.15.15

BFD sessions with Device1 (green) and Hub (purple)

After

```
Device2-spoke2#show sdwan bfd sessions
```

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP	DST PUBLIC	IP
172.16.255.15	500	up	lte	3g	10.0.6.45		10.0.20.15
172.16.255.15	500	up	lte	lte	10.0.6.45		10.1.15.15

BFD sessions only with Hub (purple)

OMP ルート

ハブアンドスポークを設定する前に、Device2 (将来の Spoke2) で `show sdwan omp route vpn 1` コマンドを実行すると、Device1 を介して Device1 (Spoke1) プレフィックスに直接到達できることが示されます。これは、TLOC IP 列に Device1 のシステム IP が表示されることから明らかです。

ハブアンドスポークを設定すると、Device2 (Spoke2) はハブを介してのみ Device1 (Spoke1) プレフィックスに到達できます。

図 24: Spoke2 : 設定前と設定後の OMP ルート

Before
Device2-future-spoke2#show sdwan omp route vpn 1

TENANT	VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP	COLOR
0	1	10.20.35.0/24	172.16.255.19	17	1003	C,I,R	installed	172.16.255.35	lte
			172.16.255.20	23	1003	C,R	installed	172.16.255.35	lte

Device1 prefix (green) via Device1

After
Device2-spoke2#show sdwan omp route vpn 1

TENANT	VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP	COLOR
0	1	10.20.35.0/24	172.16.255.19	11	1003	C,I,R	installed	172.16.255.15	lte
			172.16.255.19	12	1003	C,I,R	installed	172.16.255.15	3g
			172.16.255.20	11	1003	C,R	installed	172.16.255.15	lte
			172.16.255.20	12	1003	C,R	installed	172.16.255.15	3g

Device1 prefix (green) via Hub (purple)

IP ルート

ハブアンドスポークを設定する前に、Device2（将来の Spoke2）で `show ip route vrf 1` コマンドを実行すると、Device1 を介して Device1 プレフィックスに直接到達できることが示されます。

ハブアンドスポークを設定すると、Device2（Spoke2）はハブを介してのみ Device1（Spoke1）プレフィックスに到達できます。

図 25: Spoke2 : 設定前と設定後の IP ルート

Before
Device2-future-spoke2#show ip route vrf 1

```
m 10.20.35.0/24 [251/0] via 172.16.255.35, 06:05:43, Sdwan-system-intf
```

Device1 prefix (green) via Device1 (green)

After
Device2-spoke2#show ip route vrf 1

```
m 10.20.35.0/24 [251/0] via 172.16.255.15, 10:21:41, Sdwan-system-intf
```

Device1 prefix (green) via Hub (purple)

ハブアンドスポークの利点

ハブアンドスポークトポロジには、次のような多くの用途と利点があります。

- 各スポークネットワークをある程度分離して運用することで、個別のスポークごとに異なるポリシーやトランスポートメカニズムなどを適用できます。
- 各スポークにサービスを提供するエッジルータのピア数を減らすと、これらのエッジルータのリソース需要が減少します。
- ハブを介してすべてのスポーク間トラフィックをルーティングすると、ファイアウォールポリシーなどのネットワークサービスをすべてのスポーク間トラフィックに適用できます。

ここで説明するプロセスを使用してハブアンドスポークトポロジを設定すると、設定プロセスが簡素化され、複雑な集中管理ポリシーを回避できます。

ハブアンドスポークに関する制約事項

制約事項	説明
トランスポートゲートウェイのサイトタイプ	トランスポートゲートウェイをハブとして使用する場合は、そのサイトタイプを <code>spoke</code> に設定しないでください。
オンデマンドトンネル	ハブアンドスポークトポロジでは、オンデマンドトンネルはサポートされていません。これは、ハブアンドスポークトポロジでスポーク間直接トンネルがサポートされていないためです。
移行	制御ポリシーによって定義されたハブアンドスポークトポロジから、ここで説明するハブアンドスポーク設定メソッドに移行するための自動手順はありません。

ハブアンドスポークのユースケース

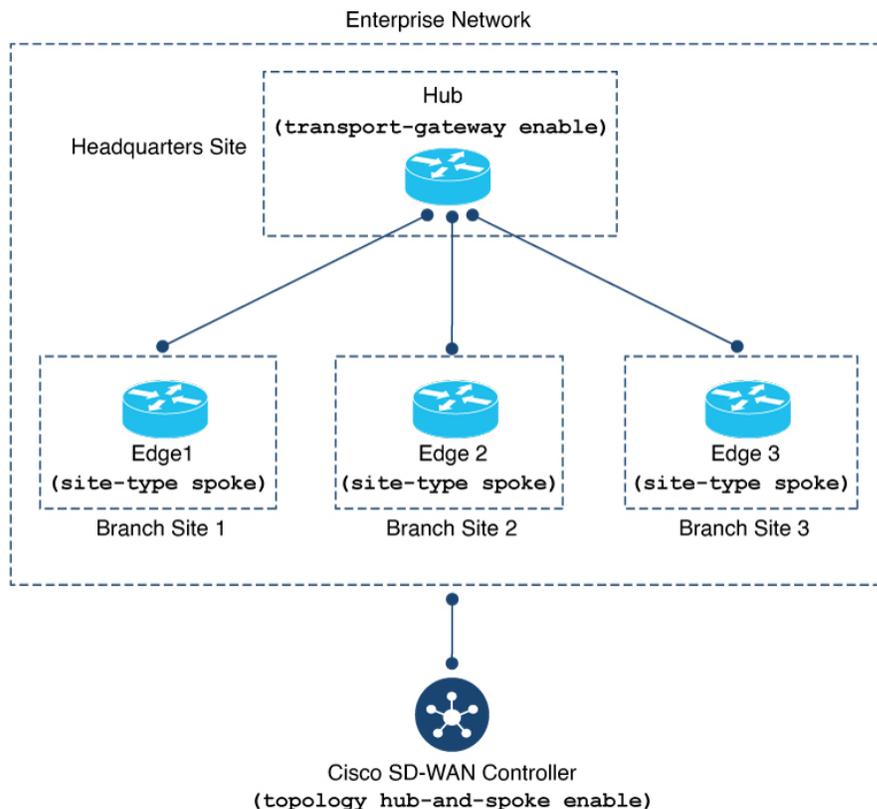
このユースケースでは、組織のネットワークに次の要素が含まれます。

- 多数のネットワークサービス（エンタープライズファイアウォールなど）を実行する、組織の本社サイトにある単一のデバイス。ネットワーク管理者は、これをハブデバイスとして指定することを選択しました。
- 3つのブランチサイト。各ブランチサイトには、サイトにサービスを提供するエッジルータがあります。

ネットワーク管理者は、ブランチサイト間のすべてのトラフィックフローを本社サイトのハブを介してルーティングするようにハブアンドスポークトポロジを設定することを選択しました。これにより、一元化されたネットワークサービスを、ブランチサイト間のすべてのトラフィックに適用できます。

次の図に示すように、ハブアンドスポークトポロジを設定します。

図 26:ハブアンドスポーク トポロジ



ハブアンドスポークトポロジの設定

ここでは、トランスポートゲートウェイを使用してハブアンドスポークトポロジを設定する手順について説明します。

Cisco SD-WAN Manager を使用したハブアンドスポークを有効にするための Cisco Catalyst SD-WAN コントローラ の設定

1. Cisco SD-WAN Manager メニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックします。
3. 次のいずれかを実行します。
 - Cisco SD-WAN コントローラの新しいシステムテンプレートを作成するには、[Add Template] をクリックし、[Controller] を選択して、[System] をクリックします。

- Cisco SD-WAN コントローラの既存のシステムテンプレートを編集するには、既存の機能テンプレートのテーブルで [Controller System] タイプのテンプレートを見つけ、テンプレートの横にある [...] をクリックして、[Edit] を選択します。

4. [Topology] フィールドで、[Hub and Spoke] を選択します。
5. [Save] (新しいテンプレートを作成する場合) または [Update] (既存のテンプレートを編集する場合) をクリックします。

CLI テンプレートを使用してハブアンドスポークを有効にするための Cisco SD-WAN コントローラの設定

CLI テンプレートの使用の詳細については、[CLI アドオン機能テンプレート](#) および [CLI テンプレート](#) を参照してください。デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

1. システム コンフィギュレーション モードを開始します。

```
system
```

2. ハブアンドスポーク トポロジを有効にします。

```
topology hub-and-spoke enable
```



(注) ハブアンドスポーク機能を無効にするには、このコマンドの **no** 形式を使用します。

例

```
system
 topology hub-and-spoke enable
```

トランスポートゲートウェイとしてのルータの設定 (ハブアンドスポークの場合)

ハブアンドスポーク設定では、トランスポートゲートウェイが使用されます。トランスポートゲートウェイのドキュメントで次の手順を参照してください。

- [Cisco SD-WAN Manager を使用したトランスポートゲートウェイとしてのルータの設定 \(214 ページ\)](#)
- [CLI テンプレートを使用したトランスポートゲートウェイとしてのルータの設定 \(215 ページ\)](#)

ルータのサイトタイプの設定（ハブアンドスポークの場合）

ハブアンドスポーク設定では、サイトタイプとトランスポートゲートウェイが使用されます。トランスポートゲートウェイのドキュメントで次の手順を参照してください。

- [Cisco SD-WAN Manager を使用したルータのサイトタイプの設定（218 ページ）](#)
- [CLI テンプレートを使用したルータのサイトタイプの設定（218 ページ）](#)

ハブアンドスポーク設定の確認

ハブアンドスポーク設定では、トランスポートゲートウェイとサイトタイプパラメータが使用されます。これらについては、[トランスポートゲートウェイ（Transport Gateway）](#)を参照してください。

- トランスポートゲートウェイ設定の確認については、[CLIを使用したトランスポートゲートウェイ設定の確認（219 ページ）](#)を参照してください。
- サイトタイプの確認については、[CLIを使用したルータのサイトタイプの確認（219 ページ）](#)を参照してください。
- ハブアンドスポーク設定後のネットワーク内のデバイスでの BFD セッション、OMP ルート、および IP ルートの確認については、次の場所にある、この機能の概要説明に含まれている例を参照してください：[例：ハブアンドスポーク接続（224 ページ）](#)

Cisco Catalyst SD-WAN コントローラ でハブアンドスポーク設定が有効になっていることの確認

Cisco SD-WAN コントローラ 設定に **topology hub-and-spoke enable** コマンドが含まれていることを確認するには、**show running-config** コマンドを使用します。

次の例では、Cisco SD-WAN コントローラ は、ハブアンドスポークトポロジを有効にするように設定されています。

```
sdwanController# show running-config
...
system
 topology hub-and-spoke
  enable
```

topology hub-and-spoke enable コマンドが有効になっていることを確認するには、**show omp summary** コマンドを使用します。出力にはトポロジが示されます。次の例では、トポロジはハブアンドスポークです。

```
sdwanController# show omp summary
per-state UP
admin-state UP
...
topology hub-and-spoke
```




第 12 章

対称ルーティング



(注) 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

- [対称ルーティング \(240 ページ\)](#)
- [対称ルーティングについて \(240 ページ\)](#)
- [コンフィギュレーションの概要 \(250 ページ\)](#)
- [サポートされているシナリオ \(259 ページ\)](#)
- [対称ルーティングの前提条件 \(267 ページ\)](#)
- [対称ルーティングに関する制約事項 \(268 ページ\)](#)
- [対称ルーティングの設定 \(268 ページ\)](#)
- [対称ルーティングの確認 \(273 ページ\)](#)
- [RIB メトリック変換のモニター \(276 ページ\)](#)

対称ルーティング

表 54: 機能の履歴

機能名	リリース情報	説明
対称ルーティング	<p>Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.12.1</p> <p>Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a</p>	<p>アフィニティグループ、アフィニティグループ優先順位、および RIB メトリックの変換を使用して、ネットワーク内のデバイス間でのトラフィックフローの対称ルーティングを確保できます。対称ルーティングは、マルチリージョン ファブリックを含むさまざまなネットワークトポロジに対応します。</p> <p>オーバーレイネットワークを超える対称ルーティングをサポートするために、トランスポートゲートウェイは、RIB メトリックを BGP や OSPF などのコントロールプレーンプロトコルに変換できます。これにより、パス優先順位設定が、オーバーレイネットワーク外のルータ（データセンター LAN 内のルータなど）に拡張されます。</p>

対称ルーティングについて

対称ルーティングとは、両方向のトラフィックに同じルートを使用する2つのエンドポイント間のトラフィックフローを指します。Cisco Network Based Application Recognition (NBAR2)、シスコのゾーンベース ファイアウォール (ZBF)、シスコの統合脅威防御 (UTD)、Cisco Application Quality of Experience (AppQoE)、ネットワークアドレス変換 (NAT) といった一部のネットワーク機能では、適切に動作するために対称ルーティングが必要です。

Cisco Catalyst SD-WAN ネットワーク内では、アフィニティグループ、アフィニティグループ優先順位、制御ポリシー、およびその他のメカニズムを使用して、2つのエンドポイント間の優先ルートが両方向のトラフィックで一致するようにネットワークを設定できます。これにより、それらのエンドポイント間のトラフィックフローの対称ルーティングが確保されます。一部のシナリオでは、Cisco Catalyst SD-WAN オーバーレイネットワークの外部にあるデバイスにおよぶトラフィックフローの対称ルーティングも確保できます。

ルータが動作しつづけるという前提

これらはすべて、トラフィックフロー中にルータが動作不能にならない状況に適用されます。トラフィックフローのパスに含まれるルータが動作不能になると、トラフィックはルートを変更する必要があり、その際、一時的にトラフィックフローの非対称ルーティングが発生する可能性があります。

対称ルーティング設定の利点

Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a 以前では、対称ルーティングの設定作業に次のことが含まれていました。

- オーバーレイネットワークにおいて：対称ルーティングを確保するために、双方向のトラフィックに関するホップバイホップルーティングをセットアップするための、複雑でエラーが発生しやすい制御ポリシー。
- サービス側ルーティングにおいて：双方向のトラフィックに関するパスの対称性をセットアップするための複雑なルートマップ。

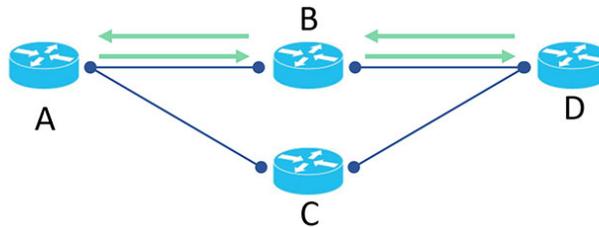
Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a 以降では、アフィニティグループおよび優先順位と、OMP メトリックの再配布を使用して、対称ルーティングを実現できます。ここでは、詳細とサポートされるシナリオについて説明します。

対称ルーティングを保証するメカニズム

Cisco Catalyst SD-WAN によって管理されるネットワークでは、Overlay Management Protocol (OMP) がコントロールプレーンタスクを維持します。これには、ベストパスアルゴリズムを適用して、2つのエンドポイント間のトラフィックの各ネクストホップを決定することが含まれます。OMP は、使用可能なさまざまなネクストホップを比較するときに、多数のパラメータを考慮します。詳細については、『Cisco Catalyst SD-WAN Routing Configuration Guide, Cisco IOS XE Release 17.x』の「Unicast Overlay Routing」を参照してください。

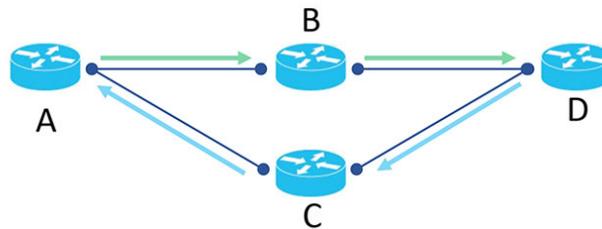
リターントラフィックが同じパスを選択するようにするには、各ホップについて、ベストパスの計算において両方向で同じルートが優先されるようにする必要があります。たとえば、次の図は、A から D へのフローを示しています。最初のホップは A から B であり、その後に B から D と続きます。特定のトラフィックフローについて、逆方向の最初のホップが D から B であり、その後に B から A と続くことを確認する必要があります。

図 27: 対称フロー



リバーストラフィック (D から A へ) で最初のホップとして D から C が使用される場合、次の図に示すように、トラフィックフローは非対称になります。

図 28: 非対称フロー



メカニズム

トランスポートゲートウェイをルーティングハブとして使用するトポロジ、またはマルチリージョンファブリックネットワークの場合、Cisco Catalyst SD-WAN は、次のメカニズムを使用して、デバイスが2つのエンドポイント間で両方向のトラフィックに同じパスを選択するようにします。

メカニズム	説明
アフィニティグループ	<p>アフィニティグループを使用すると、トラフィックフローの複数のネクストホップから選択する優先順位を指定できます。ルータアフィニティについては、『<i>Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN) Configuration Guide</i>』の「Router Affinity」を参照してください。</p> <p>関連する設定手順：</p> <ul style="list-style-type: none"> • Cisco SD-WAN Manager を使用したデバイスでのアフィニティグループまたはアフィニティグループ優先順位の設定 • CLI を使用したルータでのアフィニティグループの設定 <p>affinity-group group-id コマンドを使用します。</p>

メカニズム	説明
導出アフィニティグループ	<p>Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a 以降では、マルチリージョンファブリック トポロジの境界ルータ、またはマルチリージョンファブリック サブリージョンにサービスを提供するトランスポートゲートウェイがルートを再発信すると、導出アフィニティグループがルートに割り当てられます。これは、リターントラフィックがフォワードトラフィックと同じゲートウェイまたは境界ルータを使用することを保証する全体的なメカニズムの一部です。</p> <p>境界ルータは、アフィニティグループの代わりに導出アフィニティ属性を使用して、コアリージョン内の優先ルートを決定します。導出アフィニティ値が小さいほど、優先順位が高くなります。たとえば、境界ルータ BR1 にネクストホップとして使用可能な 2 つの境界ルータ (BR2 と BR3) がある場合、BR1 は、境界ルータによって計算された導出アフィニティグループ値が小さい方を選択します。</p> <p>(注) 対称ルーティングの前提条件 (267 ページ) で説明されているように、対称ルーティングを確保するには、境界ルータとトランスポートゲートウェイに、デバイスが処理するすべての VRF について (a) アフィニティグループ番号または (b) VRF ごとのアフィニティグループが必要です。</p>
特定の VRF 範囲のアフィニティグループ	<p>VRF 範囲ごとに異なるアフィニティグループを持つようにルータを設定できます。VRF ごとのアフィニティグループでは、VRF に従ってルートの優先順位をよりきめ細かく制御できます。</p> <p>関連する設定手順：</p> <ul style="list-style-type: none"> • Cisco SD-WAN Manager を使用した特定 VRF のルータアフィニティグループの設定 (269 ページ) • CLI テンプレートをを使用した特定 VRF のルータアフィニティグループの設定 (270 ページ) <p>affinity-per-vrf affinity-group vrf-range vrf-range コマンドを使用します。</p>

メカニズム	説明
アフィニティ優先順位	<p>これは、アフィニティグループとともに、ネクストホップのルート優先順位の制御を可能にします。アフィニティ優先順位を手動で設定すると、デバイスは、優先順位の高いアフィニティグループを持つルートを優先します。</p> <p>Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a 以降では、自動アフィニティ優先順位を設定できます。これを使用すると、デバイスは、アフィニティグループ番号が小さいルートを優先します。この場合、アフィニティグループ番号は、任意のタグとして扱われるのではなく、ルートの優先順位を示します（アフィニティグループ番号が小さいほど優先順位が高くなります）。</p> <p>(注) Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a 以降では、デバイスは、次のように、vRoute（Cisco Catalyst SD-WAN オーバーレイネットワーク内のルート）にアフィニティ優先順位属性でタグ付けします。</p> <ul style="list-style-type: none"> • デバイスのアフィニティ優先順位を手動で設定する場合、デバイスは、最大 8 つのアフィニティグループ（リストの最初の 8 つ）を使用して、設定した優先順位で vRoute にタグ付けします。 • 自動アフィニティ優先順位を設定すると、デバイスは、Cisco Catalyst SD-WAN によって内部的に使用される値（自動優先順位を示します）で vRoute をタグ付けします。 • デバイスのアフィニティ優先順位を手動で設定し、自動アフィニティ優先順位も設定した場合、デバイスは、前のオプションと同様に、Cisco Catalyst SD-WAN によって内部的に使用される値（自動優先順位を示します）で vRoute をタグ付けします（アフィニティ優先順位を手動で設定し、自動も同時に使用するユースケースについては、Cisco SD-WAN Manager を使用した自動アフィニティグループ優先順位を使用するルータの設定（268 ページ）を参照してください）。

メカニズム	説明
アフィニティ優先順位 (続き)	<p>関連する設定手順：</p> <ul style="list-style-type: none"> （手動設定） Cisco SD-WAN Manager を使用したデバイスでのアフィニティグループまたはアフィニティグループ優先順位の設定 （手動設定） CLI を使用したルータでのアフィニティグループ優先順位の設定 <p>affinity-group preference list コマンドを使用します。</p> <ul style="list-style-type: none"> （自動設定） Cisco SD-WAN Manager を使用した自動アフィニティグループ優先順位を使用するルータの設定 (268 ページ) （自動設定） CLI テンプレートをを使用した自動アフィニティグループ優先順位を使用するルータの設定 (271 ページ) <p>affinity-group preference-auto コマンドを使用します。</p>
サービス側ルーティングプロトコルへの OMP メトリックの再配布	<p>Cisco Catalyst SD-WAN によって管理されているルータと Cisco Catalyst SD-WAN によって管理されていないルータを含むネットワークトポロジでは、OMP からネットワークのサービス側部分にルーティング情報ベース (RIB) メトリックを伝達できます。ネットワークのサービス側部分では、ボーダー ゲートウェイ プロトコル (BGP) または Open Shortest Path First (OSPF) プロトコルを使用できます。これにより、サービス側ルータは、確実に、リターントラフィックに同じルートを優先させることができ、異なるコントロールプレーン間でもルーティングの対称性が実現されます。詳細については、オーバーレイネットワーク外のデバイスの OMP メトリクスの変換 (245 ページ) を参照してください。</p> <p>関連する設定手順：</p> <ul style="list-style-type: none"> CLI テンプレートをを使用した OMP メトリックを BGP または OSPF に変換するルータの設定 (271 ページ) <p>redistribute omp translate-rib-metric コマンドを使用します。</p>

オーバーレイネットワーク外のデバイスの OMP メトリクスの変換

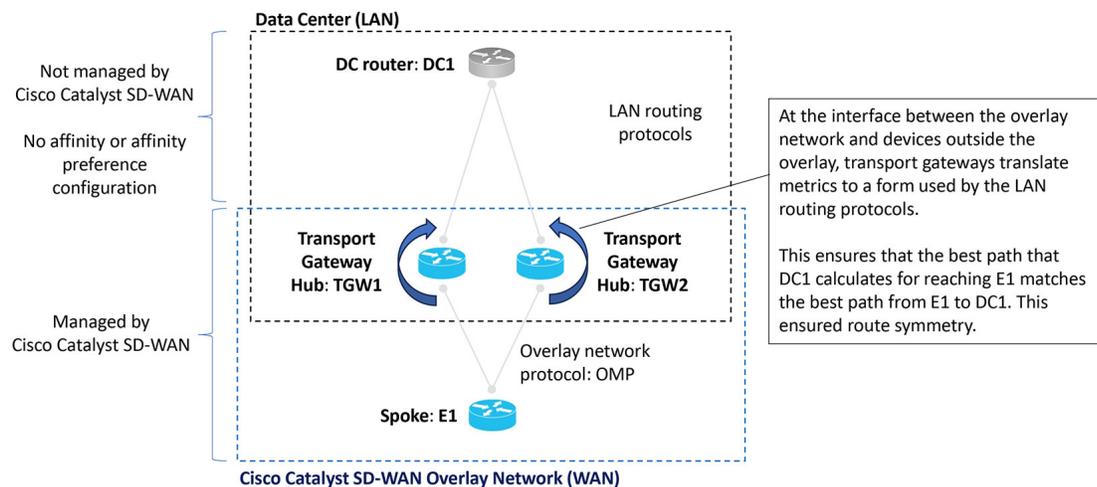
トランスポートゲートウェイとして設定され、ハブとして動作するルータ（次の図の TGW1）は、Cisco Catalyst SD-WAN オーバーレイネットワーク（WAN）内のデバイスとオーバーレイネットワーク（LAN）外のデバイス（次の図の DC1 など）の間でトラフィックを伝送できます。これは WAN から LAN へのトラフィックです。オーバーレイネットワーク外のデバイスは Cisco Catalyst SD-WAN によって管理されないことに注意してください。

トランスポートゲートウェイは、RIB メトリック情報を BGP または OSPF プロトコルで使用されるパラメータに変換します。トランスポートゲートウェイはこれらのパラメータを BGP ま

または OSPF ルーティングテーブルで使用し、BGP または OSPF ネイバーにルートをアドバタイズするときには、RIB から派生したパラメータをルートに含めます。

これらの RIB から派生したパラメータは、LAN 内のデバイスによるパス選択に影響します。これは、オーバーレイネットワークが WAN から LAN へのトラフィックに使用するのと同じパスを LAN が LAN から WAN へのトラフィックに確実に選択するために役立ちます。

図 29: OMP メトリックの変換



関連項目

[OMP メトリックの BGP 属性への変換 \(246 ページ\)](#)

[OMP メトリックの OSPF メトリックへの変換 \(249 ページ\)](#)

[CLI テンプレートをを使用した OMP メトリックを BGP または OSPF に変換するルータの設定 \(271 ページ\)](#)

[RIB メトリック変換のモニター \(276 ページ\)](#)

OMP メトリックの BGP 属性への変換

ルータが RIB メトリックを OMP から BGP に変換できるようにすると、そのルータは、次の OMP メトリックと属性を使用します。

- OMP ルートメトリック (用語に関する注: OMP メトリックの中には、特に「OMP」と呼ばれるものがあります)
- OMP AS-PATH

これにより、次の 3 つの BGP 属性を取得します。

- BGP MED
- BGP LOCAL_PREF
- BGP AS_PATH

ルートの OMP メトリックと結果として得られる BGP 属性の表示については、[RIB メトリック変換のモニター \(276 ページ\)](#) を参照してください。

OMP から BGP への変換は、次のとおりです。

表 55: OMP メトリックから BGP 属性への変換

BGP 属性	導出方法
BGP MED	OMP ルートメトリックと同じです。
BGP LOCAL_PREF	255 : (OMP ルートメトリック)
BGP AS_PATH	次の 2 つの可能性ががあります。 <ul style="list-style-type: none"> • propagate-aspath コマンドを使用する場合、次のようになります。 <ol style="list-style-type: none"> (a) OMP AS-PATH が空の場合、ルータは、独自のローカル AS 値を使用し、それを (OMP ルートメトリック) 回繰り返します (最大 13 回)。 (b) OMP AS-PATH が空でない場合、ルータは、OMP AS-PATH を使用し、その先頭に OMP AS-PATH の最初の AS を (OMP ルートメトリック) 回付加します (最大 13 回)。 • propagate-aspath コマンドを使用しない場合、次のようになります。ルータに設定され、(OMP ルートメトリック) 回繰り返され、先頭に値を付加する (最大 13 回)、独自のローカル AS 値のリスト。



- (注) ほとんどのシナリオでは、RIB メトリックの変換を有効にする場合 (**redistribute omp translate-rib-metric** コマンドを使用)、AS-PATH メトリックの伝達も有効にします (**propagate-aspath** コマンドを使用)。これを省略すると、ルータは、AS-PATH メトリックを空として扱います。

ルータは、これらの BGP 属性を、オーバーレイネットワーク外にあり、BGP を使用している LAN 内のデバイスに再発信するルートに含めます。

RIB メトリック変換なしの BGP 属性

次の表に、OMP メトリックの組み合わせと、RIB メトリック変換が有効になっていない場合にルータが取得する BGP 属性を示します。

表 56: RIB メトリック変換が有効になっていない場合の OMP から BGP への変換

	OMP メトリック : 組み合わせの例		BGP 属性への変換 : propagate-asmesh が有効 translate-rib-metric が有効ではない		
例	OMP ルートメ トリック	OMP AS-PATH	BGP MED	BGP LOCAL_PREF	BGP AS_PATH
1	0	100 101	1,000	50	100 101
2	1	100 101	1	50	100 101
3	2	100 101	2	50	100 101
4	10	(空)	10	50	(空)
5	14	100 101	14	50	100 101

RIB メトリック変換ありの BGP 属性

次の表に、OMP メトリックの組み合わせと、RIB メトリック変換が有効になっている場合にルータが取得する BGP 属性を示します。

表 57: RIB メトリック変換が有効になっている場合の OMP から BGP への変換

	OMP メトリック : 組み合わせの例		BGP 属性への変換 : propagate-asmesh が有効 および translate-rib-metric が有効		
例	OMP ルートメ トリック	OMP AS-PATH	BGP MED	BGP LOCAL_PREF	BGP AS_PATH
1	0	100 101	0	255	100 101 (OMP ルート メトリックが 0 であるため、何 も先頭に付加さ れない)
2	1	100 101	1	254	100 100 101 (リストの先頭 に付加される初 期値の 1 回の繰 り返し)

	OMP メトリック : 組み合わせの例		BGP 属性への変換 : propagate-aspath が有効 および translate-rib-metric が有効		
例	OMP ルートメ トリック	OMP AS-PATH	BGP MED	BGP LOCAL_PREF	BGP AS_PATH
3	2	100 101	2	253	100 100 100 101 (リストの先頭 に付加される初 期値の2回の繰 り返し)
4	10	(空) この例では、 ローカル AS 値 は 200 です。	10	245	200 200 200 200 200 200 200 200 200 200 (ルータ AS 値 の 10 回の繰り 返し)
5	14	100 101	14	241	100 100 100 100 100 100 100 100 100 100 100 100 100 100 101 (リストの先頭 に付加される初 期値の最大 13 回の繰り返し)

OMP メトリックの OSPF メトリックへの変換

RIB メトリックを変換するようにルータを設定しない場合、ルータは、Cisco Catalyst SD-WAN オーバーレイネットワーク外のデバイスにルートを再配布するときに、デフォルトの OSPF メトリックを使用します。デフォルトの OSPF メトリックは 16777214 (16 進数の FFFFFE) です。

ルータが RIB メトリックを変換できるようにすると、そのルータは、OMP ルートメトリック値を OSPF メトリックとして割り当てます。たとえば、OMP ルートメトリックが 10 の場合、OSPF メトリックも 10 になります。

ルートの OMP メトリックと結果として得られる BGP メトリックの表示については、[RIB メトリック変換のモニター \(276 ページ\)](#) を参照してください。

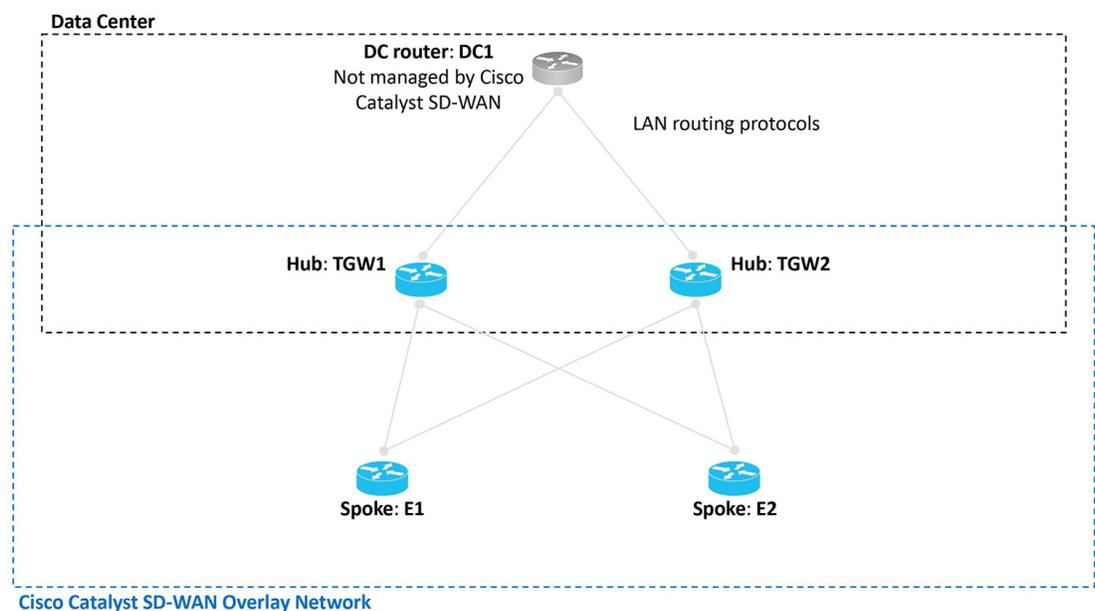
コンフィギュレーションの概要

設定ワークフローの概要は、Cisco Catalyst SD-WAN が対称ルーティングをサポートするシナリオを理解するために役立ちます。次の図は、トランスポートゲートウェイシナリオとマルチリージョンファブリックシナリオを示しています。

トランスポートゲートウェイシナリオ

トランスポートゲートウェイシナリオの目的は、スポークデバイス（図の E1 および E2）とデータセンタールータ（DC1）間の対称ルーティングを確保することです。

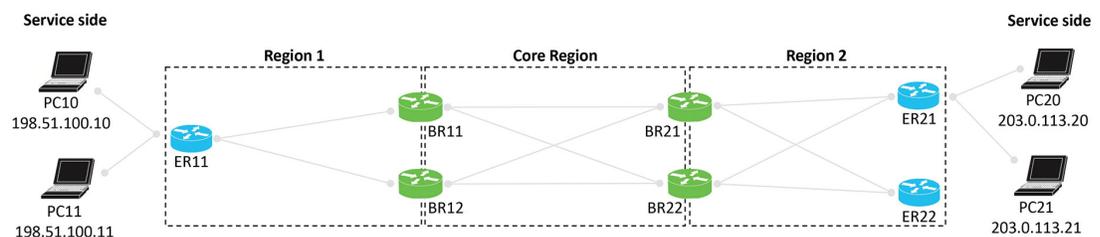
図 30: データセンター LAN を使用したトランスポートゲートウェイシナリオ



マルチリージョンファブリックシナリオ

マルチリージョンファブリックシナリオの目的は、リージョン1のエッジルータER11がサービスを提供するPCデバイスと、リージョン2のER21がサービスを提供するPCデバイス間の対称ルーティングを確保することです。

図 31: マルチリージョンファブリックシナリオ



コンフィギュレーションの概要

次の手順では、対称ルーティングに必要な設定の概要を示します。

設定手順	デバイス	説明
1. アフィニティグループ優先順位の設定	スポークルータ マルチリージョンファブリックシナリオのエッジルータ	<p>オーバーレイネットワーク内でトラフィックの対称性を確保するには、アフィニティグループ優先順位を使用してネットワーク内のスポークルータ（またはマルチリージョンファブリックシナリオのエッジルータ）を設定します。これには、手動で設定した優先順位または自動優先順位を使用できます。</p> <p>自動アフィニティ優先順位を使用すると、スポークデバイスまたはエッジルータは、より小さいアフィニティグループ番号でタグ付けされたパスを優先します。</p> <p>設定手順については、ルータアフィニティグループまたはアフィニティグループ優先順位の設定（269 ページ）を参照してください。</p>
2. アフィニティグループの設定	トランスポートゲートウェイ マルチリージョンファブリックシナリオの境界ルータ	<p>オーバーレイネットワーク内でトラフィックの対称性を確保するには、(a) アフィニティグループ番号、または (b) デバイスが処理する一部またはすべての VRF に関する VRF ごとのアフィニティグループを使用して、境界ルータとトランスポートゲートウェイを設定します。(a) と (b) の両方を同時に設定できます。</p> <p>たとえば、デバイスの VRF 範囲が 1 ～ 10 の場合、次のようにデバイスを設定できます。</p> <ul style="list-style-type: none"> システムレベルのアフィニティグループ 10 VRF ごとのアフィニティグループ : VRF6 ～ VRF10 のアフィニティグループ 20 <p>その結果、1 ～ 5 の範囲の vRoute はアフィニティグループ 10 でタグ付けされ（システムレベルのアフィニティグループから）、6 ～ 10 の範囲の vRoute はアフィニティグループ 20 でタグ付けされます。</p> <p>設定手順については、ルータアフィニティグループまたはアフィニティグループ優先順位の設定（269 ページ）を参照してください。</p>

設定手順	デバイス	説明
3. RIB メトリックの変換の有効化	トラnsポートゲートウェイ マルチリージョンファブリックシナリオの境界ルータ	<p>オーバーレイネットワークと LAN 間の対称ルーティングを有効にするには、LAN でトラフィックを伝送する境界ルータまたはトラnsポートゲートウェイで、OMP ルートを LAN ルーティングプロトコルに再配布するための RIB メトリックの変換を有効にします。</p> <p>詳細な説明については、オーバーレイネットワーク外のデバイスのOMPメトリックスの変換 (245 ページ) を参照してください。</p> <p>設定手順については、CLI テンプレートを使用した OMP メトリックを BGP または OSPF に変換するルータの設定 (271 ページ) を参照してください。</p>

次の図は、前述の2つのシナリオを、各ルータの設定例とともに示しています。ここで説明する手順により、対称ルーティングを確保できます。

図 32: 対称ルーティングの設定を示す、データセンター LAN を使用したトラnsポートゲートウェイシナリオ

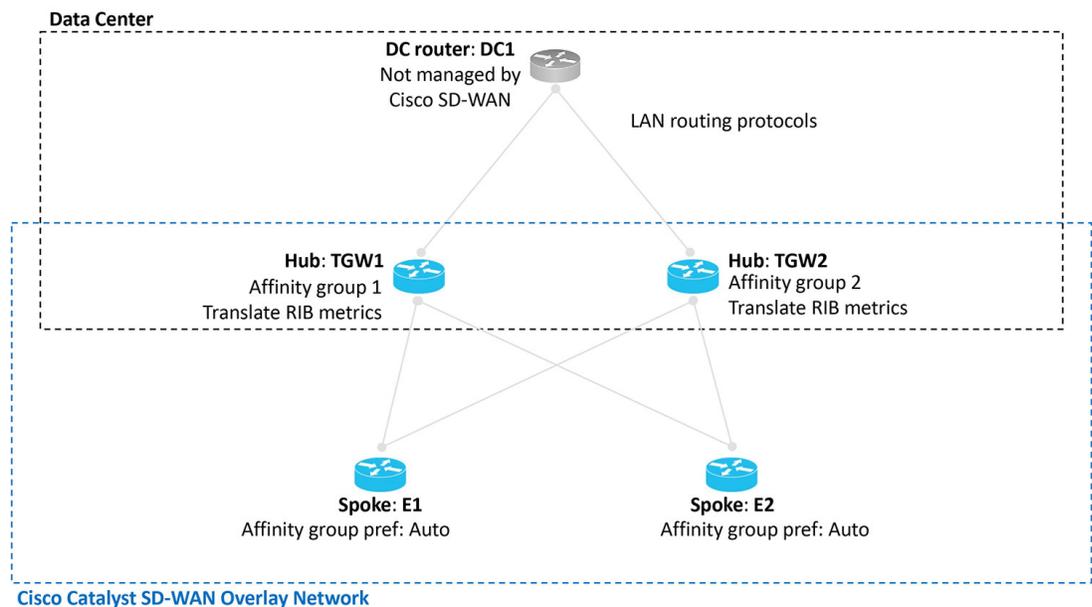
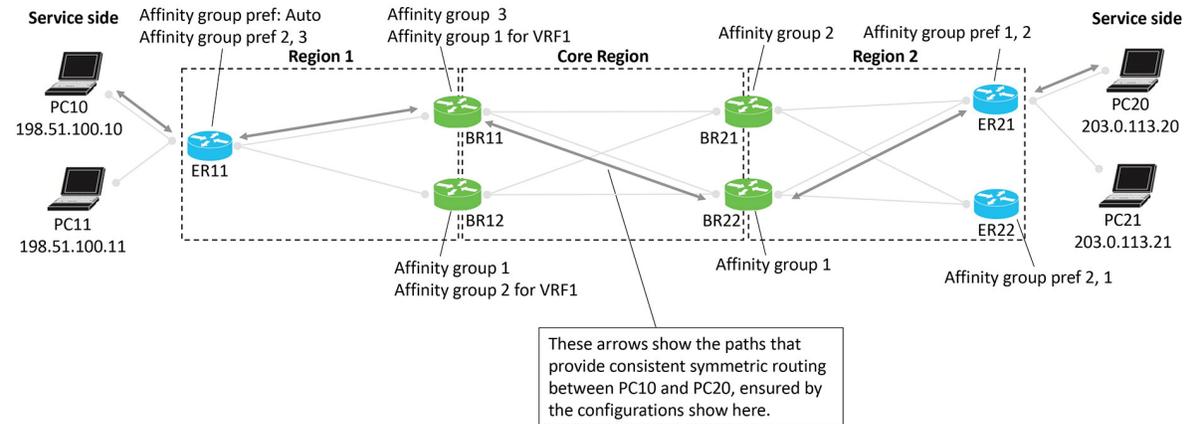


図 33: 対称ルーティングの設定を示す、マルチリージョン ファブリック シナリオ

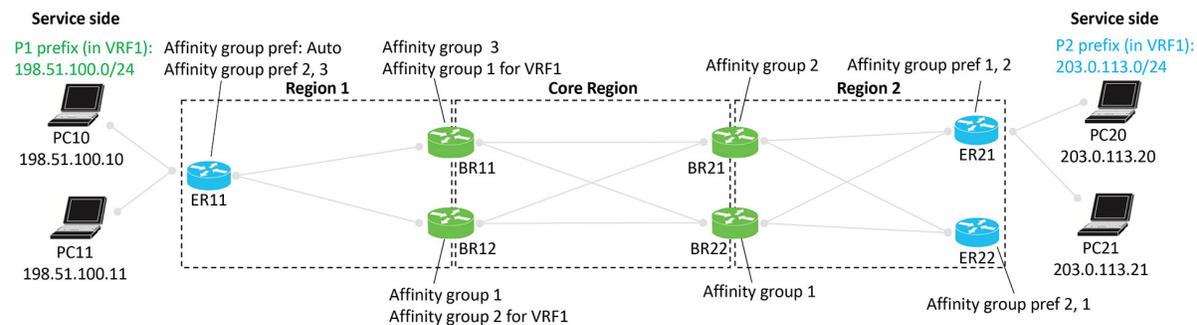


対称ルーティングの設定例とそのメカニズム

次の例は、リージョン 1 のエッジルータ ER11 がサービスを提供する PC デバイスとリージョン 2 の ER21 がサービスを提供する PC デバイスの間で対称ルーティングを提供するために、マルチリージョンファブリック環境で境界ルータとエッジルータを設定するアプローチを包括的に示しています。具体的には、この例は、PC10 と PC20 の間のトラフィックに焦点を当てています。

次のフローが順に示された図では、ルートの再発信とパスの優先順位により、両方向のトラフィックで複数のホップを経由する同じパスが優先される仕組みが示されています。

図 34: マルチリージョン ファブリックのシナリオ、対称ルーティングの設定



P1 ルートのアドバタイズ

エッジルータ ER11 は P1 ルートをアドバタイズします。これらのルートを境界ルータに再発信し、最終的に ER21 と ER22 に再発信するプロセスは、図の左から右へと進みます。このプ

ロセスでは、境界ルータが、ルート再発信するときアフィニティグループと導出アフィニティグループを割り当てます。

ネットワーク内のルータは、次のように優先ルートを選択します。

- コアリージョン外：アフィニティグループ優先順位に基づく
- コアリージョン内：導出アフィニティグループ (dag) の最小値に基づく

図 35: エッジルータ ER11 が P1 ルートをアドバタイズ

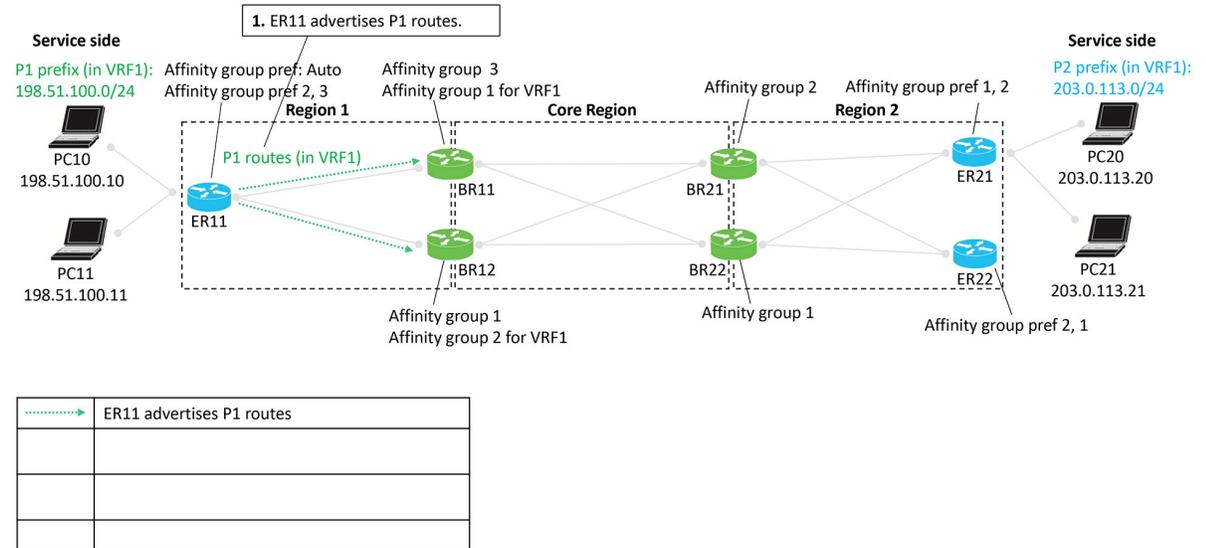


図 36: 境界ルータ BR11 および BR12 が P1 ルートを再発信

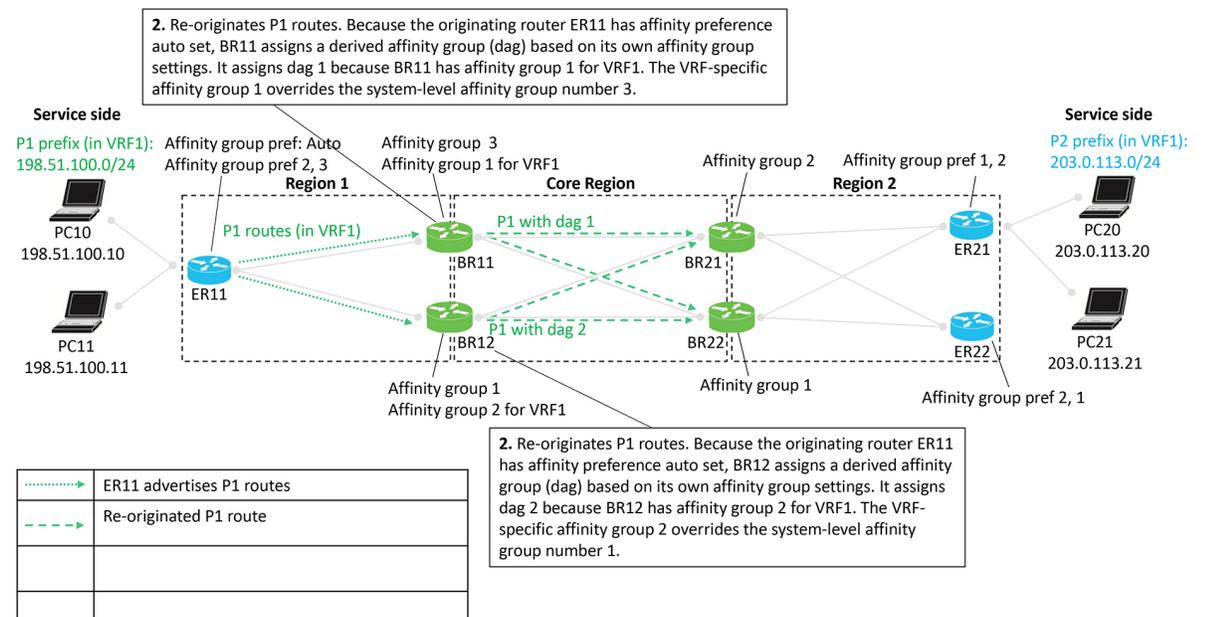


図 37: 境界ルータ BR21 および BR22 が P1 ルートを再発信

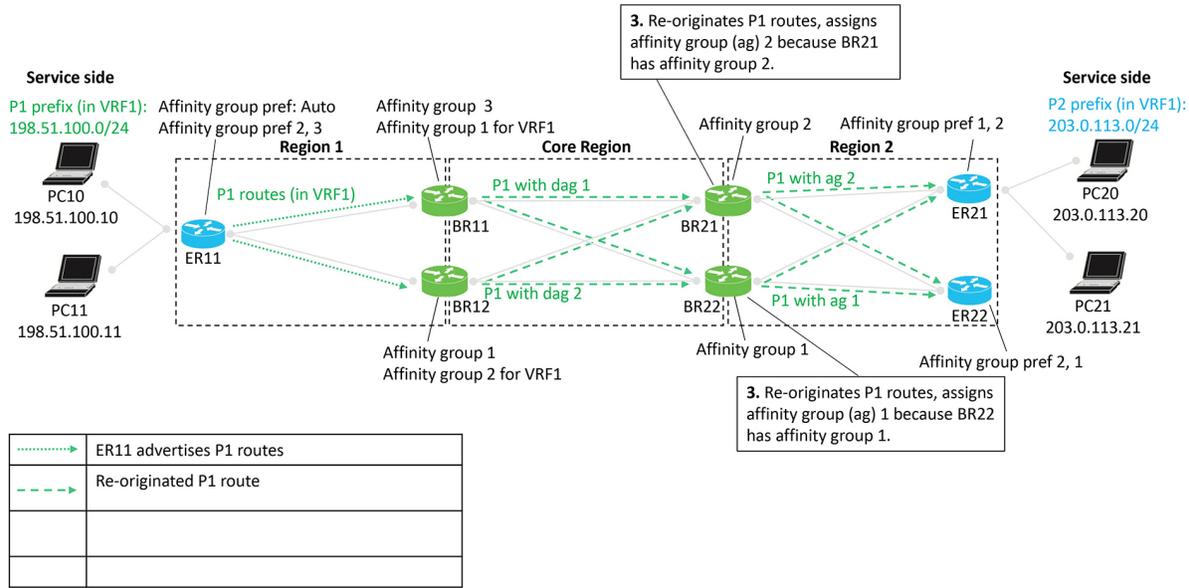


図 38: アフィニティグループと導出アフィニティグループに基づくルート優先順位

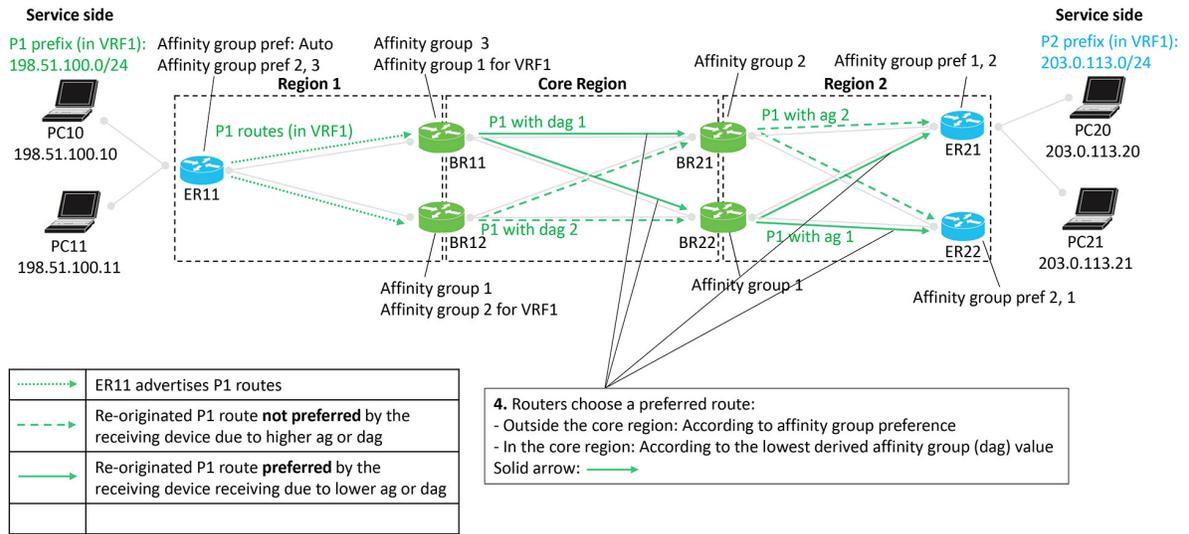
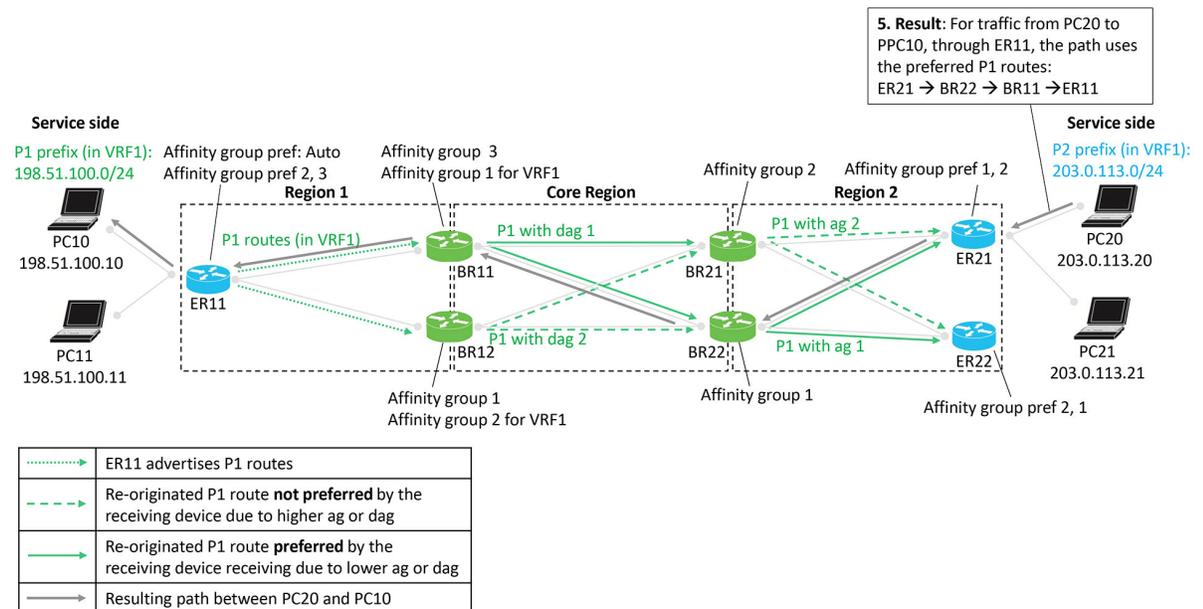


図 39: 結果として生じる P1 へのトラフィックパス



P2 ルートのアドバタイズ

エッジルータ ER21 および ER22 は P2 ルートをアドバタイズします。これらのルートを境界ルータに再発信し、最終的に ER11 に再発信するプロセスは、図の右から左へと進みます。このプロセスでは、境界ルータが、ルートを再発信するときにアフィニティグループと導出アフィニティグループを割り当てます。

ネットワーク内のルータは、次のように優先ルートを選択します。

- コアリージョン外：アフィニティグループ優先順位に基づく
- コアリージョン内：導出アフィニティグループ（dag）の最小値に基づく

図 40: エッジルータ ER21 が P2 ルートをアドバタイズ

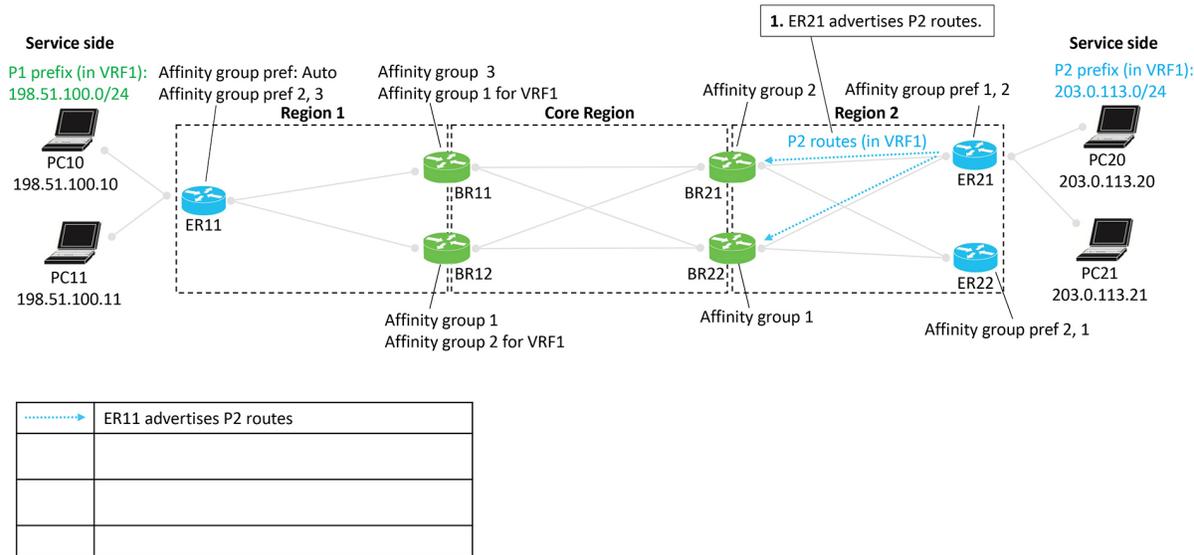


図 41: 境界ルータ BR21 および BR22 が P2 ルートを再発信

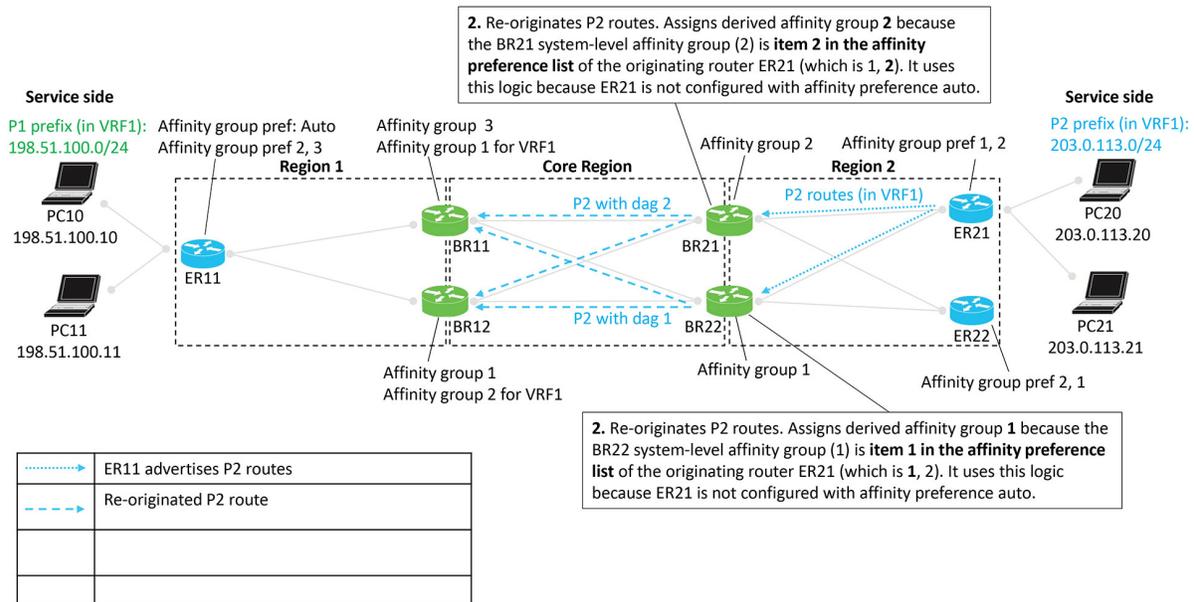


図 42: 境界ルータ BR11 および BR12 が P2 ルートを再発信

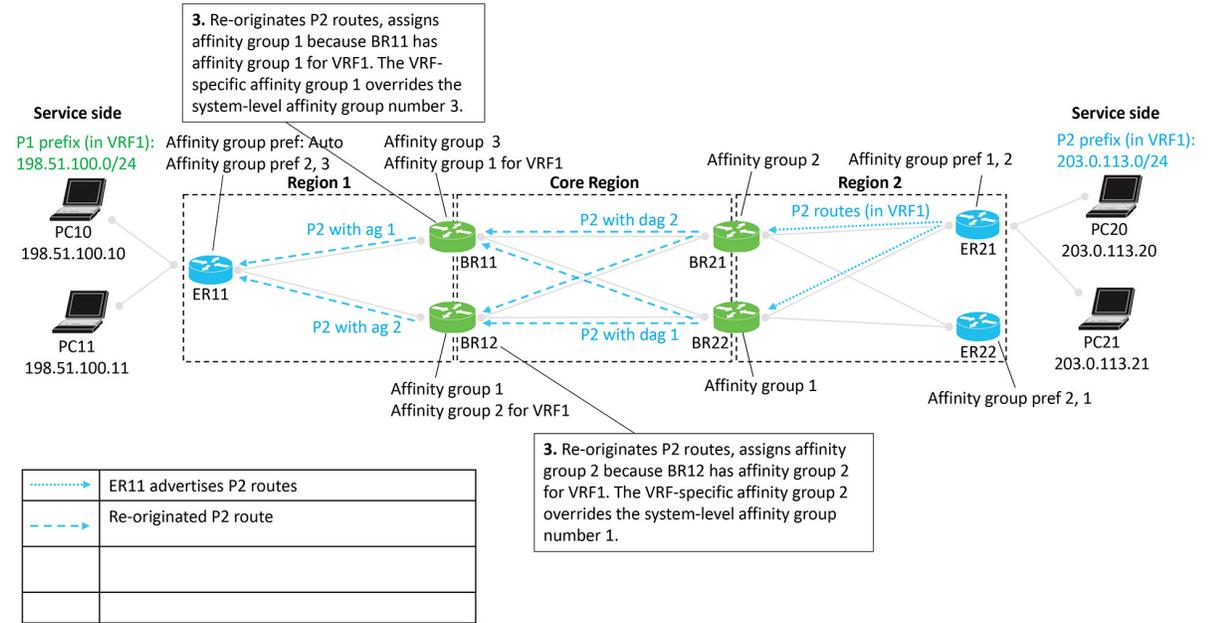


図 43: アフィニティグループと導出アフィニティグループに基づくルート優先順位

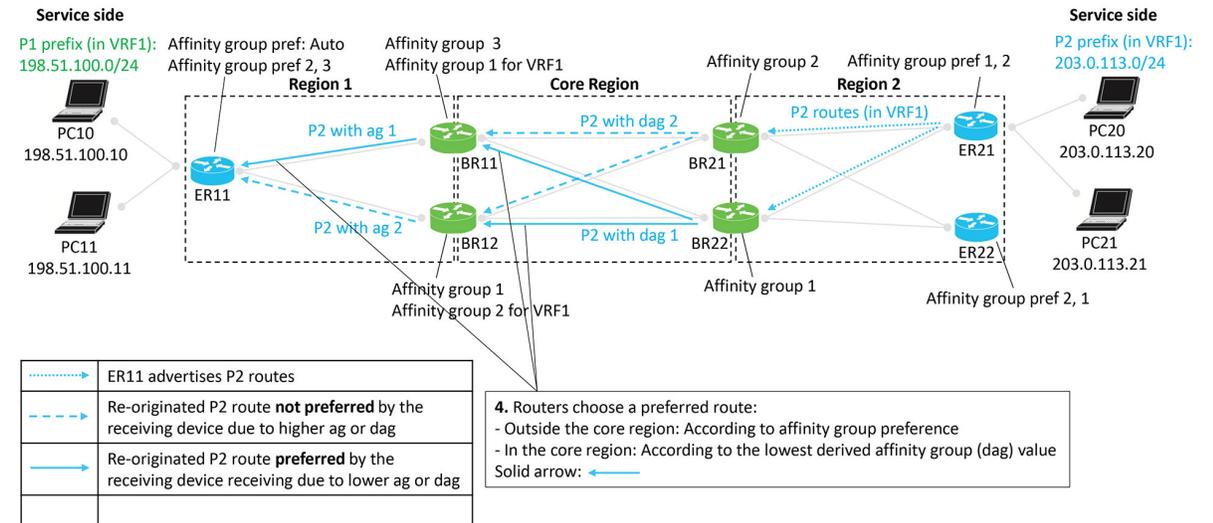
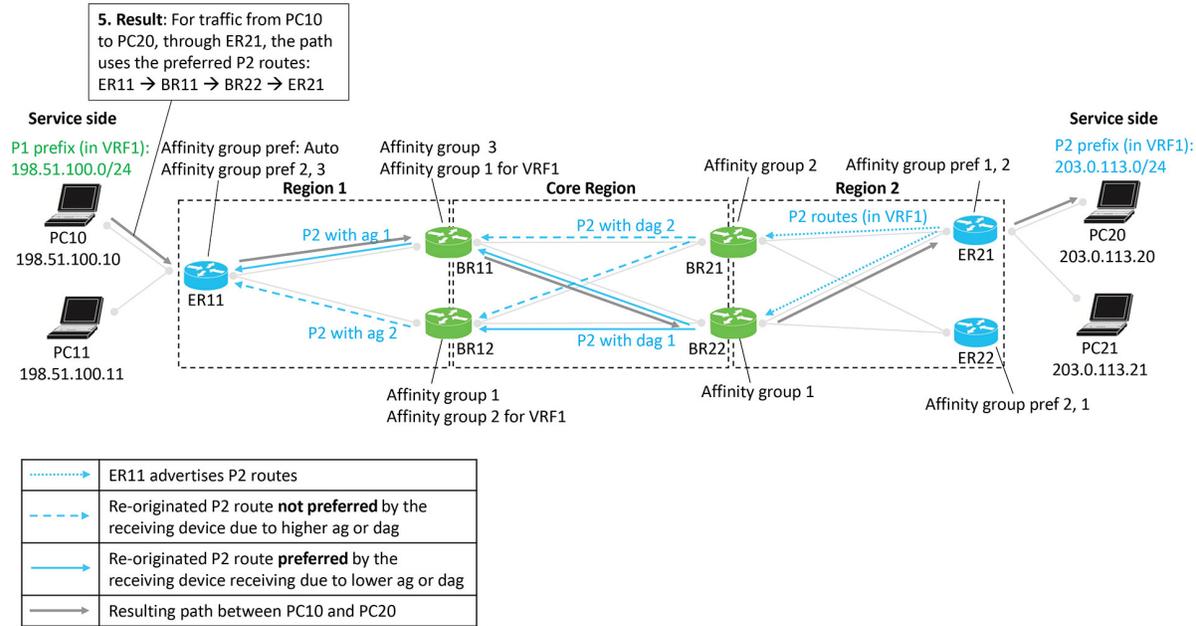


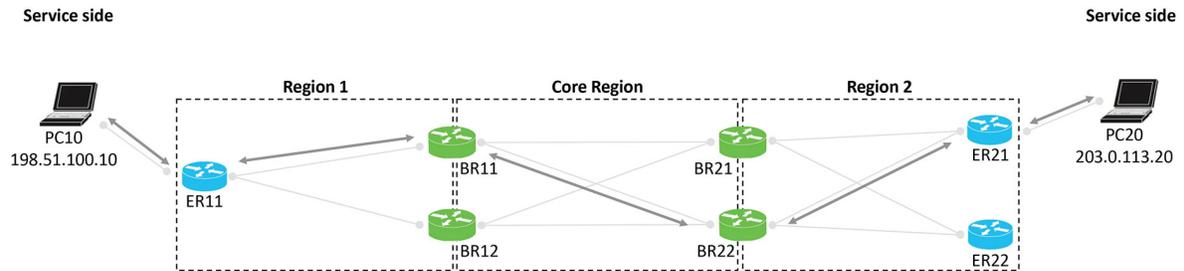
図 44: 結果として生じる P2 へのトラフィックパス



結果

次の図は、設定の結果が、フロー（この例では PC10 と PC20 の間）の対称ルーティングであることを示しています。

図 45: 結果は対称ルーティング



サポートされているシナリオ

ここで説明する対称ルーティングを設定するアプローチは、次のネットワークシナリオに適用されます。

- 複数のハブルータを使用したハブアンドスポークトポロジ

これには、ハブルータがマルチホームデータセンターにサービスを提供するシナリオが含まれます。

- 複数の境界ルータを使用したマルチリージョンファブリック

これには、マルチリージョンファブリックリージョンにマルチホームデータセンターが含まれるシナリオが含まれます。

- サブリージョンにサービスを提供するトランスポートゲートウェイを備えたマルチリージョンファブリック

ここでは、さまざまな特定シナリオについて簡単に説明し、シナリオで対称ルーティングをサポートする設定例を示します。

シナリオ：ハブアンドスポークトポロジ、データセンターにサービスを提供する複数のハブ、アクティブ/アクティブ

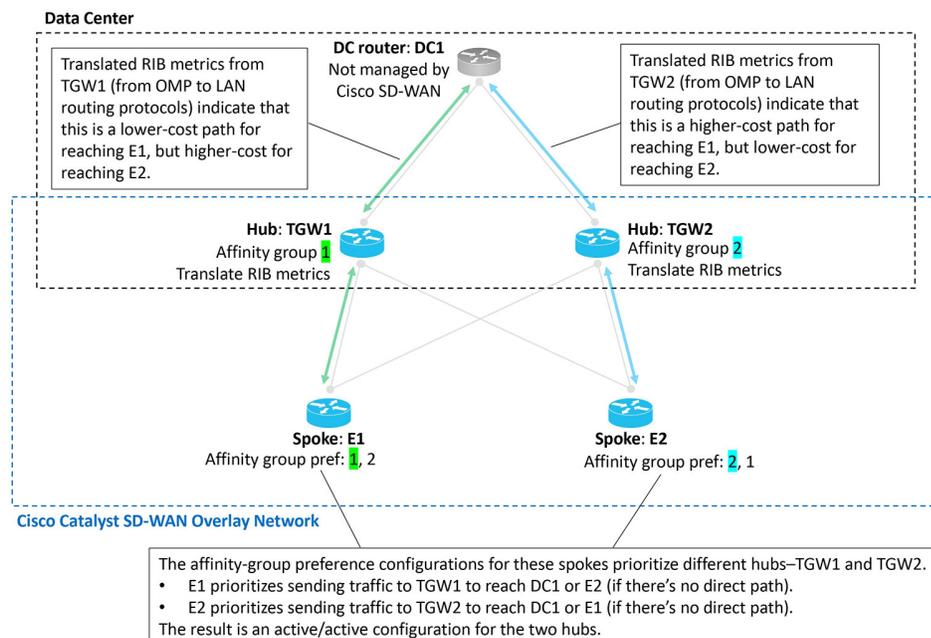
このシナリオでは、2つのハブがデータセンターにサービスを提供します。アクティブ/アクティブ配置の場合、2つのハブは両方ともアクティブです。

データセンターLANは、Cisco Catalyst SD-WAN オーバーレイネットワークの一部ではありません。



- (注) 図に示されている **redistribute omp translate-rib-metric** コマンドについては、[CLI テンプレートを使用した OMP メトリックを BGP または OSPF に変換するルータの設定 \(271 ページ\)](#) を参照してください。

図 46: データセンター、2つのハブ、アクティブ/アクティブ

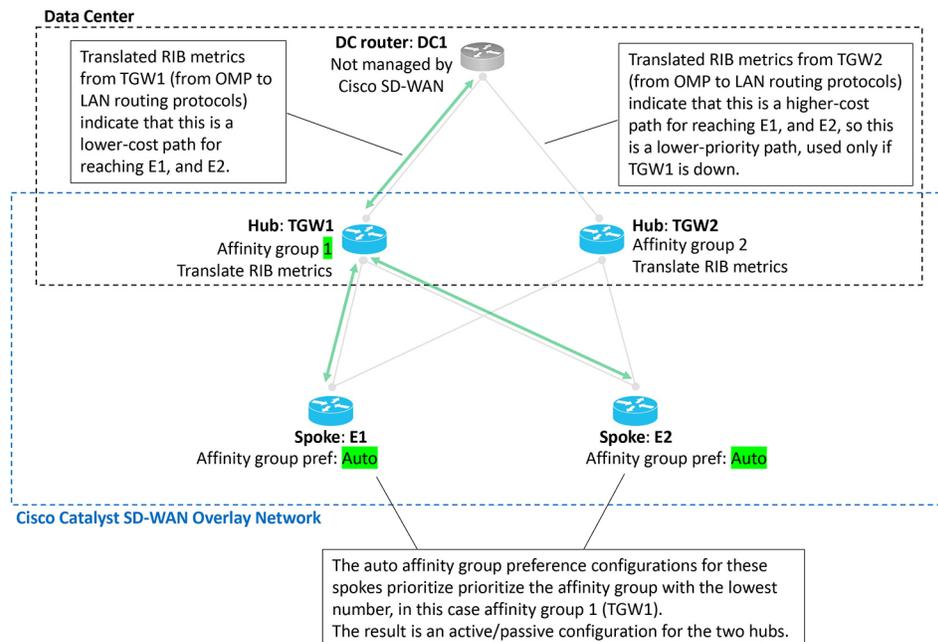


シナリオ：ハブアンドスポークトポロジ、データセンターにサービスを提供する複数のハブ、アクティブ/パッシブ

このシナリオでは、2つのハブがデータセンターにサービスを提供します。通常、1つのハブのみがアクティブになり、もう1つのハブは、アクティブハブが使用できなくなった場合に備えてスタンバイになります。これはアクティブ/パッシブ配置です。

データセンター LAN は、Cisco Catalyst SD-WAN オーバーレイネットワークの一部ではありません。

図 47: データセンター、2つのハブ、アクティブ/パッシブ

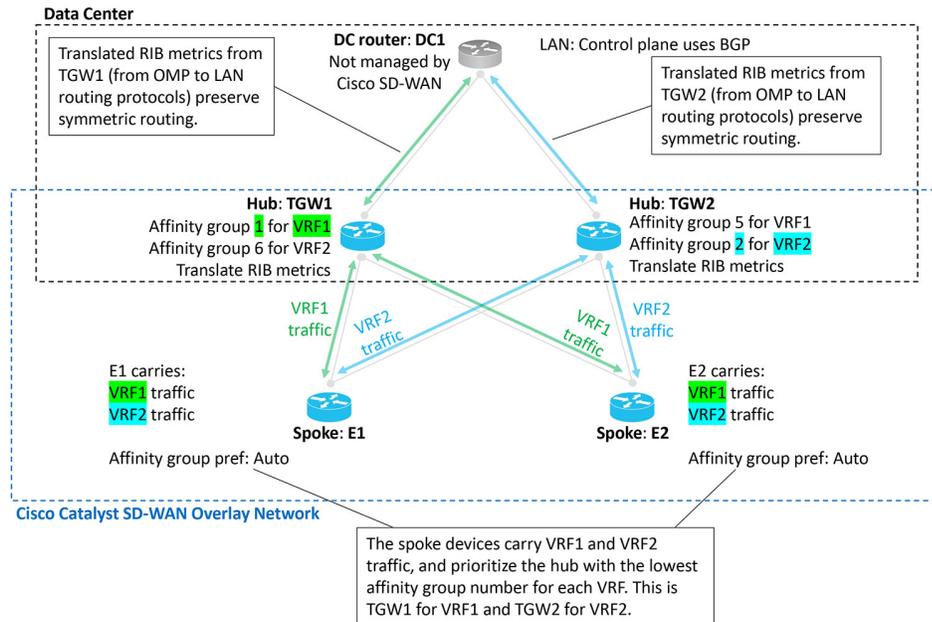


シナリオ：ハブアンドスポークトポロジ、データセンターにサービスを提供する複数のハブ、VRF によるアクティブ/アクティブ

このシナリオでは、2つのハブがデータセンターにサービスを提供します。2つの VRF のいずれかのトラフィックに対して、2つのハブは両方ともアクティブです。これは、VRF によって分離されたアクティブ/アクティブ配置です。ハブ TGW1 は VRF1 に対してアクティブであり、ハブ TGW2 は VRF2 に対してアクティブです。両方のハブは、他の VRF に対してスタンバイとして動作できます。

データセンター LAN は、Cisco Catalyst SD-WAN オーバーレイネットワークの一部ではありません。

図 48：データセンター、2つのハブ、アクティブ/アクティブ、VRFによって分離



シナリオ：マルチリージョン ファブリック環境

対称ルーティングの設定例とそのメカニズム (253 ページ) では、マルチリージョン ファブリックのシナリオについて詳しく説明します。

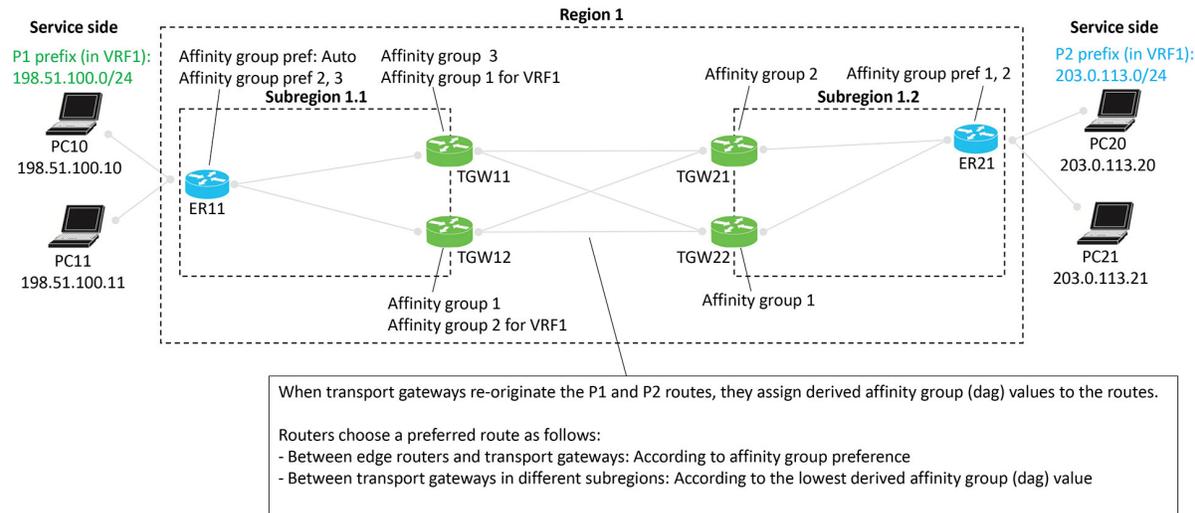
シナリオ：マルチリージョンファブリック、サブリージョンにサービスを提供するトランスポートゲートウェイ

トランスポートゲートウェイが2つのサブリージョンにサービスを提供するマルチリージョンファブリックのシナリオは、対称ルーティングの設定例とそのメカニズム (253 ページ) で説明されている包括的な例によく似ています。

包括的な例の境界ルータと同様に、トランスポートゲートウェイは、他のトランスポートゲートウェイに再発信するルートに導出アフィニティグループ (dag) を割り当てます。図に示されているように、次のようになります。

- トランスポートゲートウェイは、ルートを再発信するときに、導出アフィニティグループ (dag) 値をルートに割り当てます。
- ルータは、次のように優先ルートを選択します。
 - エッジルータとトランスポートゲートウェイ間：アフィニティグループ優先順位に基づく
 - 異なるサブリージョンのトランスポートゲートウェイ間：導出アフィニティグループの最小値に基づく

図 49: サブリージョンにサービスを提供するトランスポートゲートウェイを備えたマルチリージョン ファブリック



シナリオ：ルートリークのあるマルチリージョン ファブリック

トランスポートゲートウェイが2つのサブリージョンにサービスを提供し、ルートがリークされる、マルチリージョンファブリックのシナリオは、[対称ルーティングの設定例とそのメカニズム](#)（253 ページ）で説明されている包括的な例によく似ています。

包括的な例の境界ルータと同様に、トランスポートゲートウェイは、他のトランスポートゲートウェイに再発信するルートに導出アフィニティグループ（dag）を割り当てます。このシナリオは、[シナリオ：マルチリージョンファブリック](#)、[サブリージョンにサービスを提供するトランスポートゲートウェイ](#)（262 ページ）で説明されているシナリオに似ていますが、ルートがリークされます。図に示されているように、次のようになります。

- トランスポートゲートウェイは、ルートを再発信するときに、導出アフィニティグループ（dag）値をルートに割り当てます。
- ルータは、次のように優先ルートを選択します。
 - エッジルータとトランスポートゲートウェイ間：アフィニティグループ優先順位に基づく
 - 異なるサブリージョンのトランスポートゲートウェイ間：導出アフィニティグループの最小値に基づく
- この特定のシナリオでは、Cisco SD-WAN コントローラの制御ポリシーが、VRF1 から VRF2 へ、および VRF2 から VRF1 へのルートリークを提供します。ルートリークにより、異なる VRF 内のエンドポイント間の接続が可能になります。

このルートリークシナリオは、トランスポートゲートウェイ（または同様に、境界ルータ）が、ルートを再発信するときに導出アフィニティグループ（dag）を割り当てる方法を示しています。このロジックは少し分かりにくいですが、この例では明瞭に示されています。

デフォルトの動作

この例では、エッジルータとトランスポート ゲートウェイ ルータが次のように動作します。

- ER11：VRF1 にのみ登録し、VRF1 でプレフィックス P1 をアドバタイズします。
- ER21：VRF2 にのみ登録し、VRF2 でプレフィックス P2 をアドバタイズします。
- すべてのトランスポート ゲートウェイ ルータは、VRF1 と VRF2 の両方のトラフィックを処理するため、P1 (VRF1 内) ルートと P2 (VRF2 内) ルートの両方を再発信します。

デフォルトでは、ネットワークはVRF分離を提供します。つまり、デバイスがさまざまなVRFのルートを実バタイズする場合、Cisco SD-WAN コントローラは他のデバイスに提供する前にルートをフィルタ処理します。具体的には、Cisco SD-WAN コントローラは、VRF_xに登録しているデバイスにのみVRF_xルートをアドバタイズします。そのため、この例において、デフォルトでは、VRF1 にのみ登録している ER11 は、VRF2 でアドバタイズされる P2 ルートを受信しません。同様に、VRF2 にのみ登録している ER21 は、VRF1 でアドバタイズされる P1 ルートを受信しません。

その結果、VRF 分離により、異なる VRF に排他的に登録している ER11 と ER21 の間のトラフィックフローが妨げられます。

ルートリーク

ルートリークにより、デバイスは、ある VRF から別の VRF にルートをエクスポート（「リーク」）することにより、VRF 間でルートをアドバタイズできます。

- ルートの送信元 VRF：ルートの元の VRF
- ルートの現在の VRF：ルートがエクスポートされた VRF

エクスポートされたルートをアドバタイズする場合、ルータは、送信元 VRF と現在の VRF をトラックするため、各ルートのバックグラウンドが保持されます。この点は、以下で説明するロジックに組み込まれています。

この例では、次のルートリークが設定されています。

- ER11 のインバウンド制御ポリシーは、VRF1 ルートを受信し、それらのルートを VRF2 にエクスポートするように ER11 を設定します。結果：ER11 は、VRF1 と VRF2 の両方の P1 プレフィックスを、関連付けられたトランスポートゲートウェイである TGW11 と TGW12 にアドバタイズします。
- ER21 のインバウンド制御ポリシーは、VRF2 ルートを受信し、それらのルートを VRF1 にエクスポートするように ER21 を設定します。結果：ER21 は、VRF2 と VRF1 の両方の P2 プレフィックスを、関連付けられたトランスポートゲートウェイである TGW21 と TGW22 にアドバタイズします。

前述のように、ルートをリークした後、デバイスは、各ルートについて、送信元 VRF（ルートの送信元）と現在の VRF（リーク先の VRF）をトラックします。

導出アフィニティグループの計算

この例のようなトランスポート ゲートウェイ デバイス、または同様の例の境界ルータは、次のように、導出アフィニティグループ (dag) を、再発信するルートに割り当てます。

1. 発信元ルータがアフィニティグループ優先順位自動で設定されている場合 (例の ER11 を参照)、再発信元デバイス (TGW11 など) は、次のように、自身の (TGW11 の) アフィニティグループ設定に従って dag を決定します。

1. リークされるルートについては、その送信元 VRF と現在の VRF を考慮してください。2つの値のうち、数値的に小さい方を選択します。これを x とします。
2. 次のいずれかを実行します。
 - 再発信元デバイスにシステムレベルのアフィニティグループのみがあり、VRF 固有のアフィニティグループがない場合は、次を実行します。

システムレベルのアフィニティグループ番号を dag に使用します。ルートを再発信するときに、その番号の dag を割り当てます。
 - 再発信元デバイスに、手順 a で説明されている VRF x 用に設定された VRF 固有のアフィニティグループがある場合は、次を実行します。

この VRF 固有のアフィニティグループ番号を dag に使用します。ルートを再発信するときに、その番号の dag を割り当てます。

2. 発信元ルータがアフィニティグループ優先順位自動で設定されていない場合 (例の ER21 を参照)、再発信元デバイス (TGW21 など) は、次のように、再発信先ルータの dag を決定するときに、発信元デバイスで設定されたアフィニティ優先順位を考慮する必要があります。

1. リークされるルートについては、その送信元 VRF と現在の VRF を考慮してください。2つの値のうち、数値的に小さい方を選択します。これを x とします。
2. 次のいずれかを実行します。
 - 再発信元デバイスにシステムレベルのアフィニティグループのみがあり、VRF 固有のアフィニティグループがない場合は、次を実行します。

発信元デバイスのアフィニティグループ優先順位を確認します (ER21 を参照)。優先順位においてシステムレベルのアフィニティグループ番号が現れる場所の項目番号を特定します (優先順位リストの項目 1、2、3 など)。ルートを再発信するときに、その項目番号の dag を割り当てます。

TGW21 と ER21 の例で、ER21 の優先順位 (1、2) においてアフィニティグループ 2 が現れる場所を特定します。これは、リストの項目 2 です。そのため、ルートを再発信するときに、2 の dag を割り当てます。
 - 再発信元デバイスに、手順 a で説明されている VRF x 用に設定された VRF 固有のアフィニティグループがある場合は、次を実行します。

この VRF 固有のアフィニティグループを使用して、発信元デバイスのアフィニティグループ優先順位を確認します。優先順位において VRF 固有のアフィニティ

グループ番号が現れる場所の項目番号を特定します（優先順位リストの項目 1、2、3 など）。ルートを再発信するときに、その項目番号の **dag** を割り当てます。

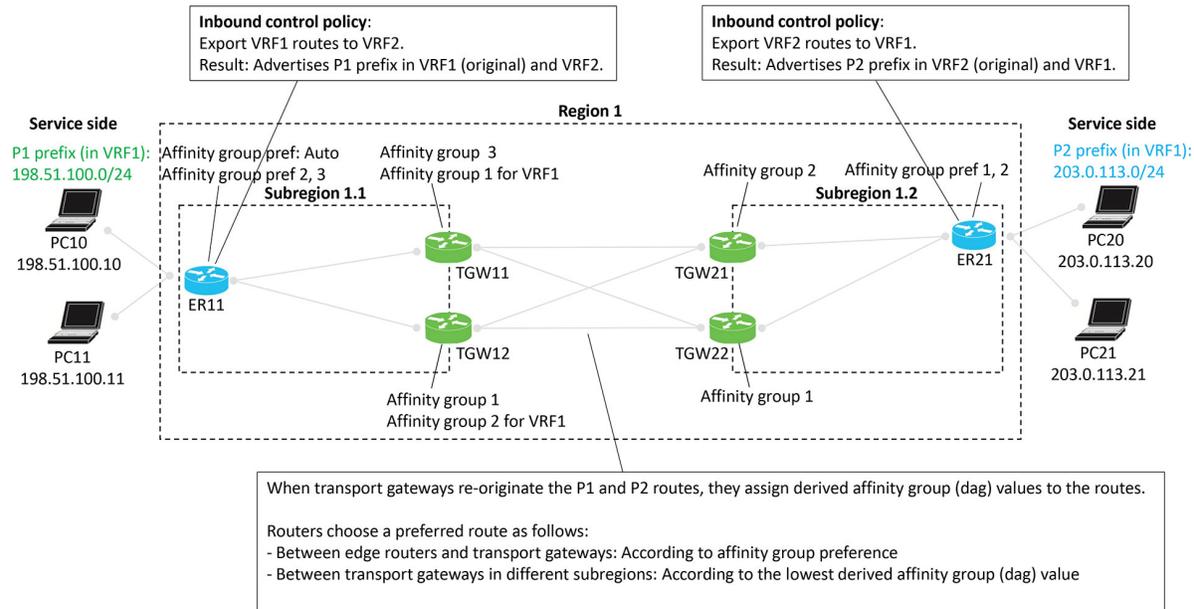
仮に、この例で TGW21 のシステムレベルのアフィニティグループが 2 であることに加えて、VRF1 に関する VRF 固有のアフィニティグループが 1 であった場合、TGW21 は、VRF1 にリークされた P2 ルートを ER21 から受信すると、発信元デバイス（ER21）の優先順位を考慮します。VRF 固有のアフィニティグループが 1 であるこの仮定の例では、ER21 から受信したルートについて、ER21 の優先順位（1、2）でアフィニティグループ 1 が現れる場所が確認されます。これは、リストの項目 1 です。そのため、TGW21 は、ルートを再発信するときに、1 の **dag** を割り当てます。

例

図で説明されているシナリオでは、VRF2 から VRF1 にリークされたルートの送信元 VRF 値は 2 で、現在の VRF 値は 1 です。トランスポートゲートウェイがこのルートを再発信する場合、2 つの VRF 番号のうち小さい方の番号である 1 に従って **dag** を割り当てます。たとえば、TGW12 が、送信元 VRF 値が 1 で現在の VRF 値が 2 のルートを再発信している場合、2 つの VRF 番号のうち小さい方の番号である 1 が選択されます。そのため、VRF1 に従って **dag** が計算されます。TGW12 は、システムレベルのアフィニティグループが 1 で、VRF1 に関する VRF 固有のアフィニティグループが 2 です。VRF1 に従って **dag** が計算されるため、VRF 固有のアフィニティグループから取得された **dag** 値 2 が、再発信されたルートに割り当てられます。

仮に、TGW12 のシステムレベルのアフィニティグループが 5 で、VRF1 固有のアフィニティグループが 7 であった場合、TGW12 は、送信元 VRF が 1 で現在の VRF が 2 のルートに、VRF1 に関する VRF 固有のアフィニティグループ 7 から取得された **dag** 値 7 を割り当てます。

図 50: サブリージョン、ルートリークのあるマルチリージョン ファブリック



対称ルーティングの前提条件

前提条件	説明
トランスポートゲートウェイが VRF にアクセスできる	トランスポートゲートウェイの「VRF ごとのアフィニティグループ」の設定を有効にするには、トランスポートゲートウェイが、アフィニティグループが設定されている VRF にアクセスする必要があります。
エッジルータにはアフィニティグループ優先順位が必要	詳細については、 コンフィギュレーションの概要 (250 ページ) を参照してください。
トランスポートゲートウェイと境界ルータにはアフィニティグループが必要	詳細については、 コンフィギュレーションの概要 (250 ページ) を参照してください。
LAN でトラフィックを伝送するトランスポートゲートウェイと境界ルータは OMP メトリックを LAN に再配布する必要があります	詳細については、 コンフィギュレーションの概要 (250 ページ) を参照してください。

対称ルーティングに関する制約事項

制約事項	説明
OMP メトリックの変換	同じデバイスで redistribute omp translate-rib-metric コマンドと redistribute omp metric コマンドの両方を同時に使用することはできません。 translate-rib-metric オプションでは OMP メトリックから BGP 属性と OSPF メトリックが生成されますが、 metric オプションではメトリックが明示的に設定されません。詳細については、 オーバーレイネットワーク外のデバイスの OMP メトリックの変換 (245 ページ) を参照してください。

対称ルーティングの設定

ここでは、対称ルーティングに必要な設定手順について説明します。

Cisco SD-WAN Manager を使用した自動アフィニティグループ優先順位を使用するルータの設定

はじめる前に

ルータのアフィニティ優先順位を手動で設定し、自動優先順位も設定した場合、ネクストホップの選択では自動優先順位が優先されます。

ただし、手動設定の優先順位リストは、**filter route outbound affinity-group preference** コマンドを使用したパスフィルタリングには引き続き有効です。デバイスのアフィニティリストにならないルータのパスをフィルタリングで除外する方法については、「[Information About Router Affinity Groups](#)」および『*Cisco IOS XE SD-WAN Qualified Command Reference*』の「[filter route outbound affinity-group preference](#)」コマンドリファレンスを参照してください。

自動アフィニティグループ優先順位を使用するルータの設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. **[Feature Templates]** をクリックします。
3. 次のいずれかを実行します。
 - デバイスのシステムテンプレートを作成するには、**[Add Template]** をクリックし、デバイスタイプを選択して、**[Cisco System]** をクリックします。

- 既存のシステムテンプレートを編集するには、既存の機能テンプレートのテーブルでシステムテンプレートを見つけ、テンプレートの横にある[...]をクリックして、[Edit]を選択します。
4. [Affinity Group Preference Auto] フィールドで、[On] を選択します。
 5. [Save] (新しいテンプレートを作成する場合) または [Update] (既存のテンプレートを編集する場合) をクリックします。

ルータアフィニティグループまたはアフィニティグループ優先順位の設定

ルータアフィニティグループとアフィニティグループ優先順位の設定については、次の手順を参照してください。

[Cisco SD-WAN Manager を使用したデバイスでのアフィニティグループまたはアフィニティグループ優先順位の設定](#)

[CLI を使用したルータでのアフィニティグループの設定](#)

[Cisco SD-WAN Manager を使用した特定 VRF のルータアフィニティグループの設定 \(269 ページ\)](#)

[CLI テンプレートを使用した特定 VRF のルータアフィニティグループの設定 \(270 ページ\)](#)

[CLI を使用したルータでのアフィニティグループ設定の構成](#)

[CLI テンプレートを使用した自動アフィニティグループ優先順位を使用するルータの設定 \(271 ページ\)](#)

Cisco SD-WAN Manager を使用した特定 VRF のルータアフィニティグループの設定

1. Cisco SD-WAN Manager メニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックします。
3. 次のいずれかを実行します。
 - デバイスのシステムテンプレートを作成するには、[Add Template] をクリックし、デバイスタイプを選択して、[Cisco System] をクリックします。
 - 既存のシステムテンプレートを編集するには、既存の機能テンプレートのテーブルでシステムテンプレートを見つけ、テンプレートの横にある[...]をクリックして、[Edit]を選択します。
4. [Affinity Group Number for VRFs] には2つのフィールドがあります。左側のフィールドに、アフィニティグループ番号を入力します。右側のフィールドに、VRF 番号または番号の範

囲 (2-4 など) を入力します。特定 VRF の追加グループ番号を設定するには、プラスボタンをクリックします。



- (注) Cisco SD-WAN Manager では、最大 4 つの範囲を設定できます。さらに設定する必要がある場合は、CLI テンプレートまたは CLI アドオンテンプレートを使用できます。[CLI テンプレートを使用した特定 VRF のルータアフィニティグループの設定 \(270 ページ\)](#) を参照してください。

5. [Save] (新しいテンプレートを作成する場合) または [Update] (既存のテンプレートを編集する場合) をクリックします。

CLI テンプレートを使用した特定 VRF のルータアフィニティグループの設定

CLI テンプレートの使用の詳細については、[CLI アドオン機能テンプレート](#) および [CLI テンプレート](#) を参照してください。デフォルトでは、CLI テンプレートはグローバル コンフィギュレーションモードでコマンドを実行します。

1. システム コンフィギュレーションモードを開始します。

```
system
```

2. 特定の VRF または VRF の範囲に適用するアフィニティグループを設定します。

```
affinity-per-vrf affinity-group vrf-range vrf-range
```

例

次に、VRF1 のアフィニティグループ 1 を設定する例を示します。

```
system
  affinity-per-vrf 1 vrf-range 1
```

次に、VRF 範囲 3 ~ 6 のアフィニティグループ 4 を設定する例を示します。

```
system
  affinity-per-vrf 4 vrf-range 3-6
```



- (注) VRF 固有アフィニティグループ設定の確認については、[ルータでの VRF 固有アフィニティグループ設定の確認 \(274 ページ\)](#) を参照してください。

CLI テンプレートをを使用した自動アフィニティグループ優先順位を使用するルータの設定

はじめる前に

CLI テンプレートの使用の詳細については、[CLI アドオン機能テンプレート](#)および[CLI テンプレート](#)を参照してください。デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

affinity-group preference-auto と **affinity-group preference list** の両方を使用してルータを設定する場合、ネクストホップの選択では **affinity-group preference-auto** コマンドが優先されます。

ただし、**affinity-group preference list** コマンドは、**filter route outbound affinity-group preference** コマンドを使用したパスフィルタリングには引き続き有効です。デバイスのアフィニティリストにないルータのパスをフィルタリングで除外する方法については、「[Information About Router Affinity Groups](#)」および『*Cisco IOS XE SD-WAN Qualified Command Reference*』の「**filter route outbound affinity-group preference**」コマンドリファレンスを参照してください。

自動アフィニティグループ優先順位を使用するルータの設定

1. システム コンフィギュレーション モードを開始します。

```
system
```

2. 自動アフィニティグループ優先順位を設定します。

```
affinity-group preference-auto
```

例

```
system
affinity-group preference-auto
```

CLI テンプレートをを使用した OMP メトリックを BGP または OSPF に変換するルータの設定

CLI テンプレートの使用の詳細については、[CLI アドオン機能テンプレート](#)および[CLI テンプレート](#)を参照してください。デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。



(注) この設定は、機能テンプレートでは使用できません。

1. 次のいずれかを実行します。
 - アンダーレイネットワークがボーダーゲートウェイプロトコル (BGP) を使用する場合は、ルータ コンフィギュレーション モードを開始し、BGP 自律システムを指定し

まず、BGP 自律システムパラメータについては、『[IP Routing Configuration Guide, Cisco IOS XE 17.x](#)』を参照してください。

```
router bgp bgp-AS
```

- アンダーレイネットワークが Open Shortest Path First (OSPF) プロトコルを使用する場合は、ルータ コンフィギュレーション モードを開始し、OSPF を指定します。

```
router ospf process-id [vrf vrf-name]
```

- アンダーレイネットワークが Open Shortest Path First バージョン 3 (OSPFv3) プロトコルを使用する場合は、ルータ コンフィギュレーション モードを開始し、OSPFv3 を指定します。

```
router ospfv3 process-id
```

2. 前の手順で BGP または OSPFv3 を指定した場合は、アドレスファミリモードを開始し、IPv4 または IPv6 を指定して、OMP メトリックを変換する VRF を指定します。

```
address-family {ipv4 | ipv6} vrf vrf-name
```

3. Cisco Catalyst SD-WAN オーバーレイネットワーク外のデバイスにルートを再配布する際の OMP ルートメトリックの BGP、OSPF、または OSPFv3 への変換を有効にします。



- (注) 同じデバイスで **redistribute omp translate-rib-metric** コマンドと **redistribute omp metric** コマンドの両方を同時に使用することはできません。 **translate-rib-metric** オプションでは OMP メトリックから BGP 属性と OSPF メトリックが生成されますが、**metric** オプションではメトリックが明示的に設定されます。

```
redistribute omp translate-rib-metric
```

4. アンダーレイネットワークが BGP を使用するシナリオでは、AS-PATH メトリックの伝達を有効にします。これを省略すると、ルータは AS-PATH メトリックを空として扱います。

```
propagate-aspath
```

例 1

この例は、アンダーレイネットワークが BGP を使用するシナリオに適用されます。

```
router bgp 1
  address-family ipv4 vrf 2
    redistribute omp translate-rib-metric
  propagate-aspath
```

例 2

この例は、アンダーレイネットワークが OSPF を使用するシナリオに適用されます。

```
router ospf 1 vrf 1
  redistribute omp translate-rib-metric
```

例 3

この例は、アンダーレイネットワークが OSPFv3 IPv4 を使用するシナリオに適用されます。

```
router ospfv3 1
  address-family ipv4 vrf 1
    redistribute omp translate-rib-metric
```

例 4

この例は、アンダーレイネットワークが OSPFv3 IPv6 を使用するシナリオに適用されます。

```
router ospfv3 1
  address-family ipv6 vrf 1
    redistribute omp translate-rib-metric
```

対称ルーティングの確認

ここでは、対称ルーティングに必要な設定の確認手順について説明します。

ルータでの特定プレフィックスのネクストホップの確認

特定プレフィックスのネクストホップを表示するには、ルータで **show sdwan omp routes prefix** を使用します。このコマンドについては、『Cisco IOS XE SD-WAN Qualified Command Reference』の「[show sdwan omp routes](#)」を参照してください。

例

```
Router#show sdwan omp routes 10.1.1.0/24
```

接続先ルータへのパスの確認

指定した VRF について、ネットワーク内の任意のデバイスから、指定した接続先デバイスまでのパスを表示するには、そのデバイスで **traceroute vrf vrf-number destination-ip-address numeric** を使用します。

出力には、接続先デバイスへのパスに含まれる各ホップのリストが表示されます。リストの最後の項目は、接続先デバイスです。

例

```
Device#traceroute vrf 1 10.1.1.1 numeric
Type escape sequence to abort.
Tracing the route to 10.1.1.1
VRF info: (vrf in name/id, vrf out name/id)
 1 209.165.200.225 3 msec 1 msec 1 msec
 2 209.165.200.226 2 msec 1 msec 1 msec
 3 10.1.1.1 4 msec * 4 msec
```

ルータでの VRF 固有アフィニティグループ設定の確認

ルータでの VRF 固有アフィニティグループ設定を表示するには、トランスポートゲートウェイ、またはマルチリージョンファブリックシナリオの境界ルータで、**show platform software sdwan rp active internal "omp daemon"** を使用します。出力には、設定された各 VRF 範囲のアフィニティグループが表示されます。

VRF 固有アフィニティグループの設定については、次の手順を参照してください。

- [Cisco SD-WAN Manager を使用した特定 VRF のルータアフィニティグループの設定 \(269 ページ\)](#) を使用した特定 VRF のルータアフィニティグループの設定 Cisco SD-WAN Manager
- [CLI テンプレートをを使用した特定 VRF のルータアフィニティグループの設定 \(270 ページ\)](#) CLI テンプレートをを使用した特定 VRF のルータアフィニティグループの設定



(注) ルータで VRF 固有アフィニティグループを定義できます。その特定 VRF が存在する必要はありません。

例

```
Device#show platform software sdwan rp active internal "omp daemon" |
include Affinity
...
Affinity per VRF:

Affinity Group Number: 1 for VRF Range: 1-1
Affinity Group Number: 5 for VRF Range: 2-8
```

ルートリークの制御ポリシーの確認

ある VRF から別の VRF へのルートリークを設定する制御ポリシーを表示するには（そのようなポリシーが存在する場合）、Cisco SD-WAN コントローラで **show running-config policy control-policy** を使用します。ある VRF から別の VRF にルートをエクスポートすることを「ルートのリーク」と呼びます。

VRF リストのルートを照合し、そのルートを特定の VRF にエクスポートする制御ポリシーの設定については、『*Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x*』の「[Configure Centralized Policies Using the CLI](#)」を参照してください。

制御ポリシーが適用されるサイトを表示するには、Cisco SD-WAN コントローラで **show running-config apply-policy** を使用します。

例 1

次の例は、VRF1 ルートを照合して VRF2 にエクスポートし、VRF2 ルートを照合して VRF1 にエクスポートする制御ポリシーを示しています。

```
sdwanController#show running-config policy control-policy
policy
```

```

control-policy LEAK_1_TO_2
sequence 1
match route
  vpn-list VRF1
!
action accept
  export-to
    vpn 2
!
!
!
default-action accept
!
control-policy LEAK_2_TO_1
sequence 1
match route
  vpn-list VRF2
!
action accept
  export-to
    vpn 1
!
!
!
default-action accept
!
!
!

```

例 2

次の例は、前の例で設定された 2 つのポリシーが適用されるサイトを示しています。

```

sdwanController#show running-config apply-policy
apply-policy
site-list SL1100
  control-policy LEAK_1_TO_2 in
!
site-list SL1300
  control-policy LEAK_2_TO_1 in
!
!
!

```

ルートの導出アフィニティグループの確認

プレフィックスに割り当てられた導出アフィニティグループを表示するには、トランスポートゲートウェイ、またはマルチリージョンファブリックシナリオの境界ルータで **show sdwan omp routes prefix detail** を使用します。この値は、出力の `derived-affinity-group` パラメータに示されます。

例

次の例では、導出アフィニティグループは 2 です。

```

Device#show sdwan omp routes 192.168.1.0/24 detail
...
preference          not set
affinity group      None
derived-affinity-group 2
affinity-preference-order  None

```

```

region-id      0
br-preference  not set

```

RIB メトリック変換のモニター

トランスポートゲートウェイがRIBメトリックを変換する方法の詳細については、[オーバーレイネットワーク外のデバイスのOMPメトリクスの変換 \(245 ページ\)](#) を参照してください。

OMP メトリック

ルートのOMP RIB メトリックを表示するには、OMP RIB メトリックを変換するトランスポートゲートウェイで **show ip route** コマンドを使用します。

次の例は、10.1.1.1 ルートのOMP RIB メトリックを示しています。出力では、次のメトリックが太字で示されています。

- OMP ルートメトリック : 3
- OMP AS-PATH : 100 101

```

Router#show ip route vrf 1 10.1.1.1 protocol-internal
Routing Table: 1
Routing entry for 10.1.1.1/32
  Known via "omp", distance 251, metric 3, type omp
  Redistributing via bgp 1
  Advertised by bgp 1
  Last update from 10.100.1.2 00:04:35 ago
  Routing Descriptor Blocks:
  * 10.100.1.2 (default), from 10.100.1.2, 00:04:35 ago
    opaque_ptr 0x7FC8D1470748
    pdb 0x111111111110, ndb 0x111111111120, rdb 0x111111111130
    OMP attribute 0x7FC8D1470748, ref 2
    aspath 0x7FC8D1474870, ref 2, length 10, value 100 101
    Total OMP attr count 1, aspath 1, community 0
    Route metric is 3, traffic share count is 1

```

IPv4 ルートの OMP ルートメトリック

トランスポートゲートウェイが再配布している各 IPv4 ルートプレフィックスのOMP ルートメトリックを表示するには、トランスポートゲートウェイで **show ip route** コマンドを使用します。出力ではOMP ルートメトリック (66) が太字で示されており、アドミニストレーティブディスタンスは 251 です。

```

Router#show ip route vrf 1 omp
Routing Table: 1

10.0.0.0/32 is subnetted, 1 subnets
m      10.10.10.10 [251/66] via 172.16.0.1, 00:09:15
...

```

IPv6 ルートの OMP ルートメトリック

トランスポートゲートウェイが再配布している各 IPv6 ルートプレフィックスの OMP ルートメトリックを表示するには、トランスポートゲートウェイで **show ipv6 route** コマンドを使用します。出力では OMP ルートメトリック (66) が太字で示されており、アドミニストレーティブ ディスタンスは 251 です。

```
Router#show ipv6 route vrf 1 omp
m 2001:DB8::/128 [251/66]
  via 172.16.0.1%default
...
```

BGP メトリック

ルートの派生 BGP メトリックを表示するには、OMP RIB メトリックを変換するトランスポートゲートウェイで **show ip bgp** コマンドを使用します。

次の例は、10.1.1.1 ルートの派生 BGP メトリックを示しています。この例では IPv4 ルートが示されていますが、IPv6 ルートもサポートされています。出力では、次のメトリックが太字で示されています。

- BGP MED : 3
- BGP LOCAL_PREF : 252
- BGP AS_PATH : 100 100 100 100 101 (これは 100 100 100 (3つのコピー) に OMP AS-PATH 値の元の 100 101 を加えた値です)

```
Router#show ip bgp vpv4 all 10.1.1.1
BGP routing table entry for 1:1:10.1.1.1/32, version 2
Paths: (1 available, best #1, table 1)
  Advertised to update-groups:
    1
  Refresh Epoch 1
  100 100 100 100 101
    10.100.1.2 (via default) from 0.0.0.0 (10.100.1.1)
      Origin incomplete, metric 3, localpref 252, valid, sourced, best
      Extended Community: SoO:0:0
      mpls labels in/out 16/nolabel
      rx pathid: 0, tx pathid: 0x0
      Updated on Apr 12 2023 19:08:17 EST
```

OSPF メトリック

ルータで **redistribute omp translation-rib-metric** コマンドがアクティブであることを表示するには、**show ip ospf** コマンドを使用します。出力に太字で表示されている結果は、ルータが RIB メトリックを変換するように設定されていることを示しています。

```
Router#show ip ospf
Routing Process "ospf 10" with ID 10.100.10.1
...
Redistributing External Routes from,
  omp, includes subnets in redistribution, translate rib metric
Maximum limit of redistributed prefixes 10240
Threshold for warning message 75%
```

IPv4 ルートの OSPF メトリック

トランスポートゲートウェイが IPv4 ルートを OSPF に配布するときに使用する OSPF メトリックを表示するには、トランスポートゲートウェイで **show ip ospf** コマンドを使用します。OMP ルートメトリックによって決定される OSPF メトリックは、この例では **66** であり、出力では太字で示されています。

```
Router#show ip ospf 1 rib redistribution
      OSPF Router with ID (192.168.0.1) (Process ID 1)

      Base Topology (MTID 0)

      OSPF Redistribution
      10.10.10.10/32, type 2, metric 66, tag 0, from OMP_AGENT Router
        via 172.16.0.1, unknown interface
      ...
```

IPv6 ルートの OSPF メトリック

トランスポートゲートウェイが IPv6 ルートを OSPF に配布するときに使用する OSPF メトリックを表示するには、トランスポートゲートウェイで **show ospfv3** コマンドを使用します。OMP ルートメトリックによって決定される OSPF メトリックは、この例では **66** であり、出力では太字で示されています。

```
Router#show ospfv3 vrf 1 ipv6 rib redistribution
      OSPFv3 10 address-family ipv6 vrf 1 (router-id 192.168.0.1)

      2001:DB8::/128, type 2, metric 66, tag 0, from omp
        via 172.16.0.1
      ...
```



第 13 章

Cisco Catalyst SD-WAN ルーティングのトラブルシューティング



(注) 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

- [概要 \(279 ページ\)](#)
- [サポート記事 \(280 ページ\)](#)
- [フィードバックのリクエスト \(281 ページ\)](#)
- [免責事項と注意事項 \(281 ページ\)](#)

概要

この章では、シスコの主題専門家 (SME) が作成したドキュメントへのリンクを提供します。サポートチケットを必要とせずに技術的な問題を解決できるようにすることを目的としています。これらのドキュメントで問題を解決できない場合は、該当する [シスココミュニティ](#) にアクセスすることをお勧めします。この問題をすでに経験し、解決策を提供している可能性のある他のシスコのお客様からは、豊富な情報とアドバイスを入手できます。コミュニティで解決策が見つからない場合は、[シスコサポート](#) でサポートチケットを提出するのが最善の方法です。サポートチケットを発行する必要がある場合、これらのドキュメントは、収集してサポートチケットに追加する必要があるデータに関するガイダンスを提供します。参照したサポートドキュメントを指定すると、TAC はドキュメントの所有者と改善要求を作成できます。

サポート記事

このセクションのドキュメントは、各記事の「使用するコンポーネント」セクションにリストされている特定のソフトウェアとハードウェアを使用して作成されています。ただし、これは、それらが使用されるコンポーネントにリストされているものに限定されるという意味ではなく、通常、ソフトウェアおよびハードウェアの新しいバージョンに関連し続けます。ソフトウェアまたはハードウェアに変更があり、コマンドが動作しなくなったり、構文が変更されたり、GUIやCLIがリリースごとに異なって見える可能性があることに注意してください。

このテクノロジーに関連するサポート記事は次のとおりです。

マニュアル	説明
Cisco IOS-XE Catalyst SD-WAN Installs OSPF External Route with DN-Bit	このドキュメントでは、Open Shortest Path First (OSPF) 外部ルートがルーティングテーブルにインストールされる場合の Cisco IOS [®] -XE SD-WAN ソフトウェアの予想される動作について説明します。
Collect an Admin-Tech in SDWAN Environment and Upload to TAC Case	このドキュメントでは、Cisco Catalyst SD-WAN 環境で admin-tech を開始する方法について説明します。
Exclude Routes from Redistributing into OMP	このドキュメントでは、不要なルートが Overlay Management Protocol (OMP) へ再配布されないようにする方法について説明します。
How to Avoid BGP-OMP Routing Loop in SD-WAN Overlay at Dual-Homed Sites with Two Routers	このドキュメントでは、ボーダー ゲートウェイ プロトコル (BGP) ルーティングと Site of Origin (SoO) が使用されている場合に SD-WAN ファブリックでルーティングループを回避する方法について説明します。
OMP Best Path Selection Peculiarities and Typical Confusions	このドキュメントでは、Overlay Management Protocol (OMP) のベストパス選択に関する一般的な誤解と、OMP ベストパス選択、イーグレスポリシー、および送信パス制限機能の動作順序について説明します。
クイックスタートガイド：さまざまな SD-WAN の問題に関するデータ収集	このドキュメントでは、トラブルシューティングや問題解決の速度を向上させるために、TAC ケースを開く前に事前に収集する必要がある関連データに沿って、いくつかの Cisco Catalyst SD-WAN の問題について説明します。
Troubleshoot OMP Route Instability in Failover Scenario	このドキュメントでは、Overlay Management Protocol (OMP) ルートのトラブルシューティングの方法と、Cisco SD-WAN コントローラ ルート選択の動作順序について説明します。

マニュアル	説明
Troubleshoot Inter-VPN Traffic Failing Between Sites in a Hub-and-Spoke Network	この記事では、ハブアンドスポークトポロジを使用するネットワーク内の2つのサイト間でVPN間トラフィック伝送が失敗した場合のトラブルシューティングについて説明します。

フィードバックのリクエスト

ユーザー入力役立ちます。これらのサポートドキュメントを改善するための重要な側面は、お客様からのフィードバックです。これらのドキュメントは、シスコ内の複数のチームによって所有および管理されていることに注意してください。ドキュメントに固有の問題（不明瞭、混乱、情報不足など）を見つけた場合：

- 対応する記事の右側のパネルにある [Feedback] ボタンを使用して、フィードバックを提供します。ドキュメントの所有者に通知され、記事が更新されるか、削除のフラグが付けられます。
- ドキュメントのセクション、領域、または問題に関する情報と、改善できる点を含めてください。できるだけ詳細に記述してください。

免責事項と注意事項

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このマニュアルで使用されるデバイスはすべて、初期設定（デフォルト）の状態から作業が開始されています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

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。