



Cisco APIC レイヤ 3 ネットワーク設定ガイド、リリース 6.0(x)

初版：2022 年 6 月 17 日

最終更新：2022 年 8 月 18 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/>



Trademarks

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at:

<http://www.cisco.com/go/softwareterms>. Cisco product warranty information is available at

<http://www.cisco.com/go/warranty>. US Federal Communications Commission Notices are found here

<http://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

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 products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and-if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

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.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

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



目次

はじめに :	Trademarks iii
--------	-----------------------

第 1 章	新規および変更情報 1
	新規および変更情報 1

第 1 部 :	レイヤ 3 の設定 3
---------	--------------------

第 2 章	Cisco ACI 転送 5
	ファブリック内での転送 5
	ACI ファブリックは現代のデータ センター トラフィック フローを最適化する 5
	ACI で VXLAN 6
	サブネット間のテナント トラフィックの転送を促進するレイヤ 3 VNID 8

第 3 章	レイヤ 3 ネットワーク設定の前提条件 11
	レイヤ 3 前提条件 11
	ブリッジ ドメインの設定 12

第 4 章	共通パーベイスブ ゲートウェイ 13
	概要 13
	GUI を使用した共通パーベイスブ ゲートウェイの設定 14

第 5 章	IP エージング 17
	概要 17
	GUI を使用した IP エージングポリシーの設定 17

第 6 章	スタティック ルートブリッジ ドメイン	19
	スタティック ルートブリッジ ドメインについて	19
	GUI を使用してブリッジ ドメインでのスタティック ルートを設定する	20

第 7 章	データプレーン IP アドレス学習	21
	データプレーン IP アドレス ラーニングの概要	21
	データプレーン IP アドレス ラーニングのガイドラインと制限事項	22
	無効にするデータプレーン IP アドレス ラーニングの機能相互作用	23
	GUI を使用した VRF インスタンスごとのデータプレーン IP アドレス ラーニングの設定	24
	GUI を使用したエンドポイントごとのデータ プレーン IP アドレス ラーニングの設定	25
	GUI を使用したサブネットごとのデータ プレーン IP アドレス ラーニングの設定	26

第 8 章	IPv6 ネイバー探索	29
	ネイバー探索	29
	ブリッジ ドメインでの IPv6 ネイバー探索の設定	30
	GUI を使用して、ブリッジ ドメイン上に IPv6 ネイバー探索対応のテナント、VRF、およびブリッジ ドメインを作成する	30
	レイヤ 3 インターフェイス上での IPv6 ネイバー探索の設定	32
	注意事項と制約事項	32
	GUI を使用して、レイヤ 3 インターフェイス上の RA の IPv6 ネイバー探索インターフェイス ポリシーの設定	32
	IPv6 ネイバー探索重複アドレス検出の設定	33
	ネイバー探索重複アドレス検出について	33
	GUI を使用したネイバー探索重複アドレス検出の設定	34

第 9 章	Microsoft NLB	37
	Microsoft NLB について	37
	ユニキャスト モードについて	38
	マルチキャスト モードについて	40
	IGMP モードについて	40

Cisco ACI Microsoft NLB サーバの設定	41
Microsoft Network Load Balancing の注意事項と制限事項	45
GUI を使用したユニキャスト モードでの Microsoft NLB の設定	46
GUI を使用したマルチキャスト モードでの Microsoft NLB の設定	47
GUI を使用した IGMP モードでの Microsoft NLB の設定	48

第 10 章

IGMP スヌーピング 51

Cisco APIC および IGMP スヌーピングについて	51
ACI ファブリックに IGMP スヌーピングを実装するには	51
仮想化のサポート	53
APIC IGMP スヌーピング機能、IGMPv1、IGMPv2、および高速リーブ機能	53
APIC IGMP スヌーピング ファンクション キーと IGMPv3	53
Cisco APIC および IGMP スヌーピング クエリア関数	54
APIC IGMP スヌーピング機能の注意事項と制約事項	55
IGMP スヌーピング ポリシーの設定と割り当て	55
拡張 GUI のブリッジ ドメインへの IGMP スヌーピング ポリシーの設定と割り当て	55
GUI を使用した IGMP スヌーピング ポリシーの設定	55
GUI を使用した IGMP スヌーピング ポリシーのブリッジ ドメインへの割り当て	57
IGMP スヌーピングの静的ポート グループの有効化	57
静的ポート グループの IGMP スヌーピングを有効にする	57
前提条件: 静的ポートに EPG を導入する	58
GUI を使用した、スタティック ポートでの IGMP スヌーピングとマルチキャストの有効化	58
IGMP スヌープ アクセス グループの有効化	59
IGMP スヌープ アクセス グループの有効化	59
GUI を使用して、IGMP スヌーピングとマルチキャストへのグループアクセスを有効にする	60

第 11 章

MLD スヌーピング 63

Cisco APIC および MLD スヌーピングについて	63
注意事項と制約事項	65

GUIを使用した MLD スヌーピング ポリシーの設定とブリッジ ドメインへの割り当て	65
GUIを使用した MLD スヌーピング ポリシーの設定	65
GUIを使用した MLD スヌーピング ポリシーのブリッジ ドメインへの割り当て	67

第 12 章

IP Multicast : IP マルチキャスト	69
レイヤ 3 マルチキャスト	70
リモート リーフ スイッチでのレイヤ 3 マルチキャストのサポート	71
ファブリック インターフェイスについて	73
IPv4/IPv6 マルチキャスト ルーティングの有効化	74
VRF GIPo の割り当て	74
指定フォワーダーとしての複数のボーダー リーフ スイッチ	75
PIM/PIM6 指定ルータの選定	76
非境界リーフ スイッチの動作	77
アクティブな境界リーフ スイッチ リスト	77
ブート時のオーバーロード動作	77
ファーストホップ機能	78
ラストホップ	78
高速コンバージェンス モード	78
ランデブー ポイントについて	79
Inter-VRF マルチキャストについて	80
Inter-VRF マルチキャストの要件	81
ACI マルチキャスト機能のリスト	81
レイヤ 3 IPv4/IPv6 マルチキャストの設定のガイドライン、制約事項、および予想される動作	89
GUIを使用したレイヤ 3 IPv4 マルチキャストの設定	92
GUIを使用したレイヤ 3 IPv6 マルチキャストの設定	95
BGP IPv4/IPv6 マルチキャスト アドレス ファミリーについて	96
BGP IPv4/IPv6 マルチキャスト アドレス ファミリーのガイドラインと制約事項	97
GUIを使用した BGP IPv4/IPv6 マルチキャストの設定	98
マルチキャスト フィルタリングについて	101
マルチキャスト フィルタリングのガイドラインと制約事項	103

GUIを使用したマルチキャスト フィルタリングの設定	104
SVI L3Out のレイヤ 3 マルチキャストについて	108
GUIを使用した SVI L3Out 上のレイヤ 3 マルチキャストの設定	113

第 13 章
マルチポッド 115

マルチポッドについて	115
マルチポッドのプロビジョニング	116
マルチポッド ファブリックの設定に関するガイドライン	118
マルチポッド ファブリックの設定	121
IPN 接続のためのポッドの準備	121
マルチポッド ファブリックを作成するポッドの追加	123
Cisco Nexus 9000 シリーズ スイッチでのマルチポッド IPN 設定の例	125
APIC を 1 つのポッドから別のポッドに移動する	127
OSPF IPN アンダーレイから BGP IPN アンダーレイへの移行	128
マルチポッド スパインバックツーマックについて	130

第 14 章
リモートリーフスイッチ 131

ACI ファブリックのリモートリーフスイッチについて	131
リモートリーフバックツーマック接続について	138
リモートリーフスイッチのハードウェアの要件	140
リモートリーフスイッチの制約事項と制限事項	141
WAN ルータとリモートリーフスイッチ設定の注意事項	144
GUIを使用してリモートリーフスイッチのポッドとファブリックメンバーシップを設定する	147
ウィザードを使用してリモートリーフスイッチのポッドとファブリックメンバーシップを設定する	147
GUIを使用してリモートリーフスイッチのポッドとファブリックメンバーシップを設定する (ウィザードは使用しない)	154
ダイレクトトラフィックフォワーディングについて	159
リモートリーフスイッチのアップグレードおよび直接トラフィック転送の有効化	160
直接トラフィック転送を無効化、およびリモートリーフスイッチのダウングレード	164
リモートリーフスイッチのフェールオーバー	165

リモートリーフフェールオーバーの要件	166
リモートリーフスイッチフェールオーバーの有効化	166
リモートのリーフスイッチのダウングレードする前に必要な前提条件	168

第 15 章

SR-MPLS ハンドオフ 169

ACI ハンドオフについて	169
リリース 5.0(1) 以前の ACI ハンドオフ : IP ハンドオフ	169
リリース 5.0(1) での ACI ハンドオフ : SR ハンドオフ	170
SR-MPLS ハンドオフの ACI 実装について	175
SR-MPLS インフラ L3Out	175
SR-MPLS VRF L3Out	180
SR-MPLS カスタム QoS ポリシー	182
SR-MPLS 設定モデルについて	184
注意事項と制約事項	189
GUI を使用した SR-MPLS インフラ L3Out の設定	196
GUI を使用した SR-MPLS VRF L3Out の設定	205
GUI を使用した SR-MPLS カスタム QoS ポリシーの作成	208
MPLS 統計情報の表示	210
インターフェイスの SR-MPLS 統計情報の表示	211
VRS 向け SR-MPLS 統計情報の表示	212
SR-MPLS グローバルブロック (GB) の設定	213
IP ハンドオフ設定から SR ハンドオフ設定への移行	215
SR-MPLS VRF L3Out での外部 EPG の設定	216
SR-MPLS L3Out へのトラフィックのリダイレクト	218
IP ベースの L3Out の切断	222
ループ防止のための BGP ドメインパス機能について	223
GUI を使用したループ防止のための BGP ドメインパス機能の設定	229

第 11 部 :

外部ルーティング (L3Out) の設定 233

第 16 章

WAN およびその他の外部ネットワーク フォワーディング 235

ネットワーク ドメイン	235
ルータ ピアリングおよびルート配布	236
ルートのインポートとエクスポート、ルート集約、ルート コミュニティの一致	237
ACI のルート再配布	242
ACI ファブリック内のルート配布	242
外部レイヤ 3 Outside 接続タイプ	243
レイヤ 3 外部接続の設定のモードについて	246
L3Out ネットワーク インスタンス プロファイルで設定されているサブネットで有効な制御	247
ACI レイヤ 3 Outside ネットワークのワークフロー	249

第 17 章

外部ネットワークへのルーテッド接続	251
外部ネットワークへルーテッドされた接続について	251
外部ネットワークへのルーテッド接続のためのレイヤ 3 Out	251
L3Out ウィザードの作成	253
L3Out の設定例	253
トポロジの例	254
前提条件	256
Create L3Out Wizard を使用した L3Out の作成例	256
確認 : Create L3Out Wizard を使用した L3Out の作成例	261
ルート マップによる BD サブネットのアドバタイズの設定	262
コントラクトの確認	265
OSPF インターフェイス レベル パラメータの変更 (任意)	266
アドバタイズ ホスト ルート	267
ルート リフレクタの設定	270
GUI を使用した MP-BGP ルート リフレクタの設定	270
MP-BGP ルート リフレクタ設定の確認	271

第 18 章

L3Out のノードとインターフェイス	273
L3Out のインターフェイスの変更	273
GUI を使用した L3Out のインターフェイスの変更	273

L3Out の SVI のカスタマイズ	275
SVI 外部カプセル化の範囲	275
SVI 外部カプセル化の範囲について	275
カプセル化スコープ構文	277
SVI 外部カプセル化の範囲のガイドライン	277
GUI を使用して SVI 外部カプセル化の範囲の設定	278
SVI での複数の L3Out のカプセル化のサポート	278
複数の SVI を異なるアクセスのカプセル化でグループ化する	279
注意事項と制約事項	280
GUI を使用して SVI で複数の L3Out のカプセル化を設定する	281
CLI を使用して SVI で複数の L3Out のカプセル化を設定する	282
REST API を使用した複数の SVI 付き L3Out のカプセル化の設定	282
SVI 自動状態	283
SVI 自動状態について	283
SVI 自動状態の動作のガイドラインと制限事項	284
GUI を使用した SVI 自動状態の設定	284
Cisco フローティング L3Out について	285
第 19 章	ルーティング プロトコルのサポート 287
ルーティング プロトコルのサポートについて	287
BGP 外部ルーテッド ネットワークと BFD のサポート	287
BGP レイヤ 3 外部ネットワーク接続設定のガイドライン	287
BGP の接続タイプとループバックのガイドライン	290
外部 BGP スピーカーに対する BGP プロトコル ピアリング	290
BGP 外部ルーテッド ネットワークの設定	292
GUI を使用した BGP L3Out の設定	292
BGP Max Path の設定	299
GUI を使用した BGP Max Path の設定	299
AS パス プリペンドの設定	301
AS パス プリペンドの設定	301
設定の AS パス Prepend GUI を使用して	301

AS オーバーライドの BGP 外部ルーテッド ネットワーク	303
BGP 自律システムのオーバーライドについて	303
GUI を使用して、BGP 外部ルーテッド ネットワークと有効になっている自律システム オーバーライドを設定する	304
BGP ネイバー シャットダウンおよびソフト リセット	304
BGP ネイバー シャットダウンとソフト リセットについて	304
GUI を使用した BGP ネイバー シャットダウンの設定	305
GUI を使用した BGP ネイバー ソフト リセットの設定	306
VRF ごと、ノード BGP ごとのタイマーの値の設定	308
ノード BGP タイマー値ごとの各 VRF	308
設定の高度な GUI を使用して BGP タイマーのノードごとの VRF あたり 不整合や障害のトラブルシューティング	309
BFD サポートの設定	310
双方向フォワーディング検出	311
サブインターフェイスの BFD の最適化	312
GUI を使用したセカンダリ IP アドレスでの双方向フォワーディング検出の構成	313
GUI を使用してリーフ スイッチの BFD をグローバルに設定する	314
GUI を使用してスパイン スイッチで BFD のグローバル設定	315
GUI を使用した BFD インターフェイスのオーバーライドの設定	316
GUI を使用して BFD コンシューマ プロトコルを設定する	319
BFD マルチホップ	321
BFD マルチホップ ポリシーの設定	322
マイクロ BFD	324
ポート チャネルでの マイクロ BFD の設定	325
OSPF 外部ルーテッド ネットワーク	327
OSPF レイヤ 3 Outside 接続	327
GUI を使用した管理テナントの OSPF L3Out の作成	328
EIGRP 外部ルーテッド ネットワーク	330
EIGRP レイヤ 3 Outside 接続について	330
EIGRP プロトコルのサポート	331
ガイドラインと EIGRP を設定するときの制限事項	333

GUI を使用したEIGRPの設定 334

第 20 章

ルート集約 337

はじめに 337

L3Out 外部 EPG レベルでのルート集約 338

VRF レベルでのルート フィルタリングと集約 338

BGP ルート集約ポリシー 338

VRF 内インポート ルート制御ポリシー 339

VRF エクスポート ルート制御ポリシー 340

注意事項と制約事項 341

GUI を使用した L3out 外部 EPG レベルでのルート要約の設定 342

GUI を使用した VRF でのルート制御ポリシーの構成 344

第 21 章

ルート マップおよびルート プロファイルによるルート制御 347

ルート制御プロファイル ポリシー 347

BGP ピアごとのルート制御について 349

BGP ピアごとのルート制御に関するガイドラインと制約事項 349

GUI を使用した BGP ピアごとのルート制御の設定 351

明示的なプレフィックス リストでルート マップ/プロファイル 354

ルート マップ/プロファイルについて 354

ルート マップ/プロファイルの明示的なプレフィックス リストのサポートについて 355

一致ルール 356

ルールの設定 360

明示プレフィックス リストの集約サポート 360

注意事項と制約事項 364

GUI を使用した、明示的なプレフィックス リストでルート マップ/プロファイルの設定 364

ルート制御プロトコル 367

インポート制御とエクスポート制御を使用するルーティング制御プロトコルの設定について 367

GUI を使用した、インポート制御とエクスポート制御を使用するルート制御プロトコルの設定 367

MP-BGP のインターリーク再配布	370
MP-BGP のインターリーク再配布の概要	370
GUI を使用したインターリーク再配布のルート マップ の設定	371
GUI を使用したインターリーク再配布のルート マップ の適用	371

第 22 章

ルーティングとサブネット範囲	373
L3Out EPG スコープと制御パラメータ	373
サブネットの範囲と集約コントロール	373
セキュリティ インポート ポリシー	374
静的 L3Out EPG	374
ダイナミック L3Out EPG 分類	375
DEC の注意事項と制限事項	376
GUI を使用したダイナミック L3Out EPG 分類の設定	376

第 23 章

トランジット ルーティング	381
中継 ACI ファブリックのルーティング	381
トランジット ルーティングの使用例	382
サポートされるトランジットの組み合わせのマトリックス	388
トランジット ルーティングの注意事項	390
中継ルーティングのガイドライン	390
トランジット ルート制御	396
サブネットの範囲と集約コントロール	398
トランジット ルーティングの設定	399
トランジット ルーティングの概要	399
GUI を使用した中継ルーティングの設定	401

第 24 章

共有サービス	409
共有レイヤ 3 Out	409
レイヤ 3 アウトからレイヤ 3 アウト内部 VRF への漏洩	413
拡張 GUI を使用した共有レイヤ 3 Out VRF 間リーキングの設定	414

第 25 章	L3Out の QoS	417
	L3Out QoS	417
	L3Out QoS ガイドラインと制約事項	417
	GUI を使用して L3Out に QoS ディレクトリを設定する	419
	GUI を使用した L3Outs の QoS コントラクトの設定	419

第 26 章	IP SLAs	421
	ACI IP SLA について	421
	IP SLA モニタリングポリシー	426
	TCP 接続動作	427
	ICMP エコー動作	427
	IP SLA ट्रック メンバー	428
	IP SLA ट्रック リスト	428
	IP SLA 設定コンポーネントの関連付けの例	429
	IP SLA のガイドラインと制約事項	431
	スタティック ルートの ACI IP SLA の設定および関連付け	432
	GUI を使用した IP SLA モニタリング ポリシーの設定	433
	GUI を使用した IP SLA ट्रック メンバーの設定	434
	GUI を使用した IP SLA ट्रック リストの設定	435
	GUI を使用したスタティック ルートとトラック リストの関連付け	436
	GUI を使用した、トラック リストとネクスト ホップ プロファイルの関連付け	437
	ACI IP SLA モニタリング情報の確認	438
	GUI を使用した IP SLA プロブ統計情報の確認	438

第 27 章	HSRP	441
	HSRP について	441
	Cisco APIC と HSRP について	442
	HSRP のバージョン	443
	注意事項と制約事項	444
	デフォルトの HSRP 設定	445

GUI を使用した HSRP の設定 446

第 28 章

Cisco ACI GOLF 449

Cisco ACI GOLF 449

Cisco ACI GOLF 449

Multi-Site サイト間の共有 GOLF 接続を使用する 453

複数のサイトで共有 APIC ゴルフ接続 453

GUI を使用した ACI GOLF の設定 454

DCIG への BGP EVPN タイプ 2 ホスト ルートの分散化 456

DCIG への BGP EVPN タイプ 2 のホストルートの配信 456

GUI を使用して DCIG への BGP EVPN タイプ 2 のホストルートを分散する 457

付録 A :

レイヤ 3 ネットワーキングの注意事項 459

レイヤ 3 ネットワーキングの注意事項 459

付録 B :

NX-OS スタイル CLI を使用したタスクの実行 463

Part I: レイヤ 3 の設定 463

NX-OS スタイルの CLI を使用した共通パーベイシブ ゲートウェイの設定 463

NX-OS スタイルの CLI を使用した共通パーベイシブ ゲートウェイの設定 463

NX-OS Style CLI を使用した IP エージングの設定 464

NX-OS スタイル CLI を使用した IP エージング ポリシーの設定 464

NX-OS スタイル CLI を使用したブリッジ ドメイン上のスタティック ルートの設定 464

NX-OS スタイル CLI を使用したブリッジ ドメイン上のスタティック ルートの設定 464

NX-OS Style CLI を使用した VRF ごとのデータプレーン IP ラーニングの設定 466

NX-OS-Style CLI を使用したデータプレーン IP ラーニングの設定 466

NX-OS Style CLI を使用した IPv6 ネイバー探索の設定 466

NX-OS スタイル CLI を使用したブリッジ ドメイン上の IPv6 ネイバー検索によるテナント、VRF、ブリッジ ドメインの設定 466

NX-OS スタイル CLI を使用したレイヤ 3 インターフェイス上の RA による IPv6 ネイバー探索 インターフェイス ポリシーの設定 467

NX-OS Style CLI を使用した Microsoft NLB の設定 470

NX-OS Style CLI を使用したユニキャスト モードでの Microsoft NLB の設定 470

NX-OS Style CLI を使用したマルチキャスト モードでのMicrosoft NLB の設定	471
NX-OS Style CLI を使用した IGMP モードでの Microsoft NLB の設定	472
NX-OS Style CLI を使用した IGMP スヌーピングの設定	473
NX-OS スタイル CLI を使用した IGMP スヌーピング ポリシーの設定とブリッジ ドメインへの割り当て	473
NX-OS スタイル CLI によりスタティック ポートで IGMP スヌーピングおよびマルチキャストの有効化	476
NX-OS スタイル CLI を使用した IGMP スヌーピングおよびマルチキャストグループへのアクセスの有効化	477
NX-OS Style CLI を使用した MLD スヌーピングの設定	479
NX-OS Style CLI を使用したブリッジ ドメインに対する MLD スヌーピング ポリシーの設定と割り当て	479
NX-OS Style CLI を使用した IP マルチキャストの設定	482
NX-OS スタイルの CLI を使用したレイヤ 3 マルチキャストの設定	482
NX-OS Style CLI を使用したレイヤ 3 IPv6 の設定	484
NX-OS スタイルの CLI を使用したマルチキャスト フィルタリングの構成	484
NX-OS Style CLI を使用したマルチポッドの設定	487
NX-OS CLI を使用したマルチポッドファブリックのセットアップ	487
NX-OS Style CLI を使用したリモートリーフスイッチの設定	490
NX-OS スタイル CLI を使用したリモートリーフスイッチの設定	490
パートII：外部ルーティング (L3Out) の設定	493
外部ネットワークへのルーテッド接続	493
NX-OS Style CLI を使用した MP-BGP ルートリフレクタの設定	493
L3Out のノードとインターフェイス	493
NX-OS Style CLI を使用したレイヤ 3 ルーテッドポートチャネルとサブインターフェイスポートチャネルの設定	493
NX-OS Style CLI を使用したスイッチ仮想インターフェイスの設定	500
NX-OS Style CLI を使用したルーティングプロトコルの設定	502
NX-OS Style CLI を使用した BFD サポート付き BGP 外部ルーテッドネットワークの設定	502
NX-OS Style CLI を使用した OSPF 外部ルーテッドネットワークの設定	512
NX-OS Style CLI を使用した EIGRP 外部ルーテッドネットワークの設定	514

NX-OS スタイル CLI を使用したルート集約の設定	518
NX-OS スタイル CLI を使用した BGP、OSPF、および EIGRP のルート集約の設定	518
NX-OS スタイルの CLI を使用したルートマップとルートプロファイルによるルート制御の構成	519
NX-OS Style CLI を使用した BGP ピアごとのルート制御の設定	519
NX-OS スタイル CLI を使用して、明示的なプレフィックスリストでルートマップ/プロファイルの設定	520
NX-OS スタイルの CLI を使用した、インポート制御とエクスポート制御を使用するルート制御プロトコルの設定	524
NX-OS Style CLI を使用したインターリーク再配布の設定	525
NX-OS スタイル CLI を使用したトランジットルーティングの設定	526
NX-OS スタイル CLI を使用したトランジットルーティングの設定	526
例：中継ルーティング	529
NX-OS Style CLI を使用した共有サービスの設定	532
NX-OS スタイル CLI を使用して共有 レイヤ 3 VRF 内リークを設定する - 名前が付けられた例	532
NX-OS Style CLI を使用した共有レイヤ 3 VRF 間リークの設定：名前を付けた例	533
NX-OS スタイルの CLI を使用した L3Out の QoS の設定	535
CLI を使用した L3Out での QoS の直接設定	535
CLI を使用した L3Out の QoS コントラクトの設定	536
NX-OS Style CLI を使用した ACI IP SLA の設定	537
NX-OS Style CLI を使用した IP SLA モニタリング ポリシーの設定	537
NX-OS Style CLI を使用した IP-SLA トラック メンバーの設定	538
NX-OS Style CLI を使用した IP-SLA トラック リストの設定	540
NX-OS Style CLI を使用したスタティックルートとトラック リストの関連付け	541
NX-OS Style CLI を使用したトラック リストとネクスト ホッププロファイルの関連付け	542
CLI を使用したトラック リストおよびトラック メンバー ステータスの表示	543
CLI を使用したトラック リストとトラック メンバーの詳細の表示	543
NX-OS Style CLI を使用した HSRP の設定	545
NX-OS スタイル CLI での Cisco APIC を使用してインラインパラメータで HSRP の設定	545

NX-OS スタイル CLI のテンプレートとポリシーを使用した Cisco APIC の HSRP の設定
546

NX-OS Style CLI を使用した Cisco ACI GOLF の設定 548

NX-OS スタイル CLI を使用した推奨される共有 GOLF 設定 548

NX-OS スタイル CLI を使用した Cisco ACI GOLF 設定の例: 549

NX-OS スタイル CLI を使用して DCIG への配布の BGP EVPN タイプ 2 のホストルート
の有効化 551

付録 C :

REST API を使用してタスクを実行する 553

Part I : レイヤ 3 の設定 553

REST API を使用した共通パーベイシブ ゲートウェイの設定 553

REST API を使用した共通パーベイシブ ゲートウェイの設定 553

REST API を使用した IP エージングの設定 554

REST API を使用した IP エージングの設定 554

REST API を使用したブリッジ ドメインのスタティック ルートの設定 554

REST API を使用してブリッジ ドメインでのスタティック ルートの設定 554

REST API を使用した IPv6 ネイバー 探索の設定 555

REST API を使用したブリッジ ドメインの IPv6 ネイバー探索対応のテナント、VRF、お
よびブリッジ ドメインの作成 555

REST API を使用したレイヤ 3 インターフェイス上の RA による IPv6 ネイバー探索イン
ターフェイス ポリシーの設定 556

REST API を使用したネイバー探索重複アドレス検出の設定 557

REST API を使用した Microsoft NLB の設定 558

REST API を使用したユニキャスト モードでの Microsoft NLB の設定 558

REST API を使用したマルチキャスト モードでの Microsoft NLB の設定 558

REST API を使用した IGMP モードでの Microsoft NLB の設定 559

REST API を使用した IGMP スヌーピングの設定 560

REST API を使用したブリッジ ドメインへの IGMP スヌーピング ポリシーの設定と割り
当て 560

REST API を使用した静的ポートでの IGMP スヌーピングとマルチキャストの有効化 561

IGMP スヌーピングを REST API を使用するマルチキャスト グループのアクセスを有効
化 561

REST API を使用した MLD スヌーピングの設定	562
REST API を使用した MLD スヌーピング ポリシーの設定とブリッジ ドメインへの割り当て	562
REST API を使用した IP マルチキャストの設定	563
REST API を使用したレイヤ 3 マルチキャストの設定	563
REST API を使用したレイヤ 3 IPv6 マルチキャストの設定	565
REST API を使用したマルチキャスト フィルタリングの設定	567
REST API を使用したマルチポッドの設定	568
REST API を使用したマルチポッド ファブリックのセットアップ	568
REST API を使用したリモート リーフ スイッチの設定	570
REST API を使用したリモート リーフ スイッチの設定	570
REST API を使用した SR-MPLS ハンドオフの設定	573
REST API を使用した SR-MPLS インフラ L3Out の設定	573
REST API を使用した SR-MPLS VRF L3Out の設定	575
REST API を使用した SR-MPLS カスタム QoS ポリシー	577
パートII : 外部ルーティング (L3Out) の設定	578
外部ネットワークへのルーテッド接続	578
REST API を使用した MP-BGP ルート リフレクタの設定	578
REST API を使用したループ防止のための BGP ドメインパス機能の設定	579
L3Out のノードとインターフェイス	580
REST API を使用したレイヤ 3 ルーテッド ポート チャネルとサブインターフェイス ポート チャネルの設定	580
REST API を使用したスイッチ仮想インターフェイスの設定	582
REST API を使用したルーティング プロトコルの設定	584
REST API を使用した BFD サポート付き BGP 外部ルーテッド ネットワークの設定	584
REST API を使用した OSPF 外部ルーテッド ネットワークの設定	596
REST API を使用した EIGRP 外部ルーテッド ネットワークの設定	597
REST API を使用したルート集約の設定	599
BGP、OSPF、および REST API を使用して EIGRP のルート集約の設定	599
REST API を使用したルート マップおよびルート プロファイルによるルート制御の設定	601
REST API を使用した BGP ピアごとのルート制御の設定	601

REST API を使用して、明示的なプレフィックス リストでルート マップ/プロファイル の設定	602
REST API を使用した、インポート制御とエクスポート制御によるルーティング制御ブ ロトコルの設定	603
REST API を使用したインターリンク再配布の設定	604
REST API を使用したトランジット ルーティングの設定	605
REST API を使用したトランジットルーティングの設定	605
REST API の例: 中継ルーティング	609
共有 L3Out	610
REST API を使用した共有サービスの設定	610
共有設定の 2 つのレイヤ REST API を使用して 2 つの Vrf に 3 が記録されます。	610
REST API を使用した L3Out の QoS の設定	611
REST API を使用した L3Out での QoS ディレクトリの設定	611
REST API を使用した L3Out の QoS コントラクトの設定	612
REST API を使用した SR-MPLS カスタム QoS ポリシー	613
REST API を使用した ACI IP SLA の設定	615
REST API を使用した IP SLA モニタリング ポリシーの設定	615
REST API を使用した IP-SLA ट्रック メンバーの設定	615
REST API を使用した IP-SLA ट्रック リストの設定	615
REST API を使用したスタティック ルートとトラック リストの関連付け	616
REST API を使用してネクスト ホップ プロファイルのトラック リストに関連付けをす る	616
REST API を使用した HSRP の設定	617
REST API を使用した APIC 内の HSRP の設定	617
REST API を使用した Cisco ACI GOLF の設定	619
REST API を使用した GOLF の設定	619
REST API を使用した DCIG への BGP EVPN タイプ 2 ホスト ルート配信の有効化	625



第 1 章

新規および変更情報

この章は、次の内容で構成されています。

- [新規および変更情報 \(1 ページ\)](#)

新規および変更情報

次の表は、現行リリースに至るまでにガイドの編成と特徴に加えられた主な変更点の概要を示しています。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

表 1: Cisco APIC リリース 6.0(1) の新機能と変更された動作

機能または変更	説明	参照先
最大 /28 のサブネットマスクのリモートプール	/28 までのサブネットマスクを使用してリモートプールを構成できるようになりました。	リモートリーフスイッチ (131 ページ)
セカンダリ IP アドレスでの双方向転送検出のサポート	セカンダリ IP アドレスで双方向転送検出 (BFD) を構成できるようになりました。	GUI を使用したセカンダリ IP アドレスでの双方向フォワーディング検出の構成 (313 ページ)

機能または変更	説明	参照先
BGP 自律システム (AS) 番号	<ul style="list-style-type: none">• [プライベート AS の削除 (Remove Private AS)] オプションを使用して、eBGP ルートの AS_path からプライベート AS 番号を削除できるようになりました。• BGP ピアごとのルートマップを作成する際の AS-Path マッチ句のサポート。	<p>GUI を使用したセカンダリ IP アドレスでの双方向フォワーディング検出の構成 (313 ページ)</p> <p>GUI を使用した BGP ピアごとのルート制御の設定 (351 ページ)</p>



第 1 部

レイヤ 3 の設定

- [Cisco ACI 転送 \(5 ページ\)](#)
- [レイヤ 3 ネットワーク設定の前提条件 \(11 ページ\)](#)
- [共通パーベイシブ ゲートウェイ \(13 ページ\)](#)
- [IP エージング \(17 ページ\)](#)
- [スタティック ルートブリッジドメイン \(19 ページ\)](#)
- [データプレーン IP アドレス学習 \(21 ページ\)](#)
- [IPv6 ネイバー探索 \(29 ページ\)](#)
- [Microsoft NLB \(37 ページ\)](#)
- [IGMP スヌーピング \(51 ページ\)](#)
- [MLD スヌーピング \(63 ページ\)](#)
- [IP Multicast : IP マルチキャスト \(69 ページ\)](#)
- [マルチポッド \(115 ページ\)](#)
- [リモート リーフ スイッチ \(131 ページ\)](#)
- [SR-MPLS ハンドオフ \(169 ページ\)](#)



第 2 章

Cisco ACI 転送

- ・ [ファブリック内での転送 \(5 ページ\)](#)

ファブリック内での転送

ACI ファブリックは現代のデータセンタートラフィックフローを最適化する

Cisco ACI アーキテクチャは、従来のデータセンター設計から来る制限を解放して、最新のデータセンターで増大する East-West トラフィックの需要に対応します。

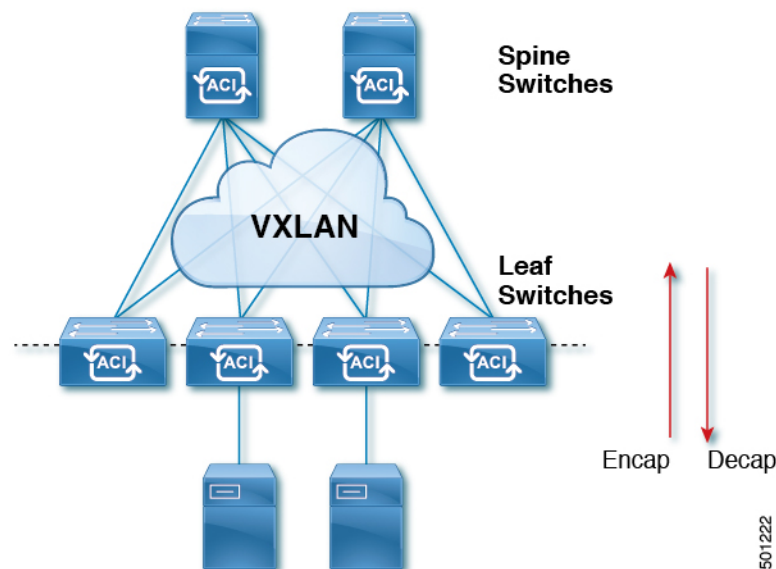
今日のアプリケーション設計は、データセンターのアクセスレイヤを通る、サーバ間の East-West トラフィックを増大させています。このシフトを促進しているアプリケーションには、Hadoop のようなビッグデータの分散処理の設計、VMware vMotion のようなライブの仮想マシンまたはワークロードの移行、サーバのクラスタリング、および多層アプリケーションなどが含まれます。

North-South トラフィックは、コア、集約、およびアクセスレイヤ、またはコラプストコアとアクセスレイヤが重要となる、従来型のデータセンター設計を推進します。クライアントデータは WAN またはインターネットで受信され、サーバの処理を受けた後、データセンターを出ます。このような方式のため、WAN またはインターネットの帯域幅の制限により、データセンターのハードウェアは過剰設備になりがちです。ただし、スパニングツリープロトコルが、ループをブロックするために要求されます。これは、ブロックされたリンクにより利用可能な帯域幅を制限し、トラフィックが準最適なパスを通るように強制する可能性があります。

従来のデータセンター設計においては、IEEE 802.1Q VLAN がレイヤ 2 境界の論理セグメンテーションまたはブロードキャストドメインを提供します。ただし、ネットワークリンクの VLAN の使用は効率的ではありません。データセンターネットワークでデバイスの配置要件は柔軟性に欠け、VLAN の最大値である 4094 の VLAN が制限となり得ます。IT 部門とクラウドプロバイダが大規模なマルチテナントデータセンターを構築するようになるにつれ、VLAN の制限は問題となりつつあります。

スパインリーフアーキテクチャは、これらの制限に対処します。ACIファブリックは、外界からは、ブリッジングとルーティングが可能な単一のスイッチに見えます。レイヤ3のルーティングをアクセスレイヤに移動すると、最新のアプリケーションが必要としている、レイヤ2の到達可能性が制限されます。仮想マシンワークロードモビリティや一部のクラスタリングのソフトウェアのようなアプリケーションは、送信元と宛先のサーバ間がレイヤ2で隣接していることを必要とします。アクセスレイヤでルーティングを行えば、トランクダウンされた同じVLANの同じアクセススイッチに接続したサーバだけが、レイヤ2で隣接します。ACIでは、VXLANが、基盤となるレイヤ3ネットワークインフラストラクチャからレイヤ2のドメインを切り離すことにより、このジレンマを解決します。

図1: ACIファブリック



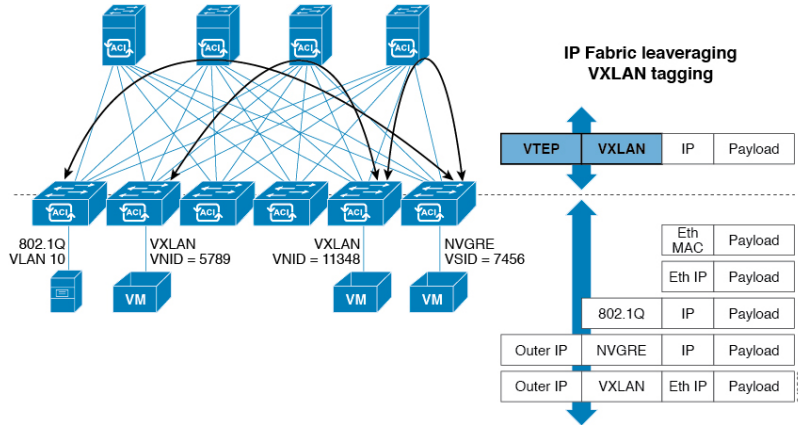
トラフィックがファブリックに入ると、ACIがカプセル化してポリシーを適用し、必要に応じてスパインスイッチ(最大2ホップ)によってファブリックを通過させ、ファブリックを出るときにカプセル化を解除します。ファブリック内では、ACIはエンドポイント間通信でのすべての転送について、Intermediate System-to-Intermediate System プロトコル (IS-IS) および Council of Oracle Protocol (COOP) を使用します。これにより、すべての ACI リンクがアクティブで、ファブリック内での等コストマルチパス (ECMP) 転送と高速再コンバージョンが可能になります。ファブリック内と、ファブリックの外部のルータ内でのソフトウェア定義ネットワーク間のルーティング情報を伝播するために、ACI はマルチプロトコル Border Gateway Protocol (MP-BGP) を使用します。

ACIでVXLAN

VXLANは、レイヤ2オーバーレイの論理ネットワークを構築するレイヤ3のインフラストラクチャ上でレイヤ2のセグメントを拡張する業界標準プロトコルです。ACIインフラストラクチャレイヤ2ドメインが隔離ブロードキャストと障害ブリッジドメインをオーバーレイ内に存在します。このアプローチは大きすぎる、障害ドメインの作成のリスクなしで大きくなるデータセンターネットワークを使用できます。

すべてのトラフィック、ACIファブリックはVXLANパケットとして正規化されます。入力でACI VXLANパケットで外部VLAN、VXLAN、およびNVGREパケットをカプセル化します。次の図は、ACIカプセル化の正規化を示します。

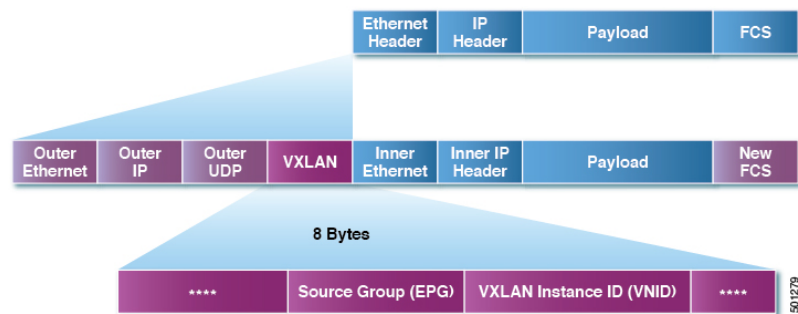
図2: ACIカプセル化の正規化



ACIファブリックでの転送は、カプセル化のタイプまたはカプセル化のオーバーレイネットワークによって制限または制約されません。ACIブリッジドメインのフォワーディングポリシーは、必要な場合に標準のVLAN動作を提供するために定義できます。

ファブリック内のすべてのパケットにACIポリシー属性が含まれているため、ACIは完全に分散された方法でポリシーを一貫して適用できます。ACIにより、アプリケーションポリシーのEPG IDが転送から分離されます。次の図に示すように、ACI VXLANヘッダーは、ファブリック内のアプリケーションポリシーを特定します。

図3: ACI VXLANのパケット形式



ACI VXLANパケットには、レイヤ2のMACアドレスとレイヤ3 IPアドレスの送信元と宛先フィールド、ファブリック内の効率的な拡張性の転送を有効にします。ACI VXLANパケットヘッダーの送信元グループフィールドは、パケットが属するアプリケーションポリシーエンドポイントグループ (EPG) を特定します。VXLAN インスタンス ID (VNID) は、テナントの仮想ルーティングおよび転送 (VRF) ドメインファブリック内で、パケットの転送を有効にします。VXLANヘッダーで24ビットVNIDフィールドでは、同じネットワークで一意的レイヤ2のセグメントを最大16個の拡張アドレス空間を提供します。この拡張アドレス空間は、大規模なマルチテナントデータセンターを構築する柔軟性IT部門とクラウドプロバイダーを提供します。

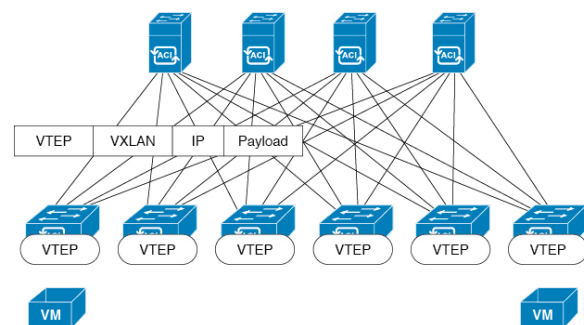
VXLANを有効にACIファブリック全体にわたってスケールでの仮想ネットワークインフラストラクチャのレイヤ3のアンダーレイ レイヤ2を展開します。アプリケーションエンドポイント ホスト柔軟に配置できます、アンダーレイ インフラストラクチャのレイヤ3 バウンダリのリスクなしでデータセンターネットワーク間をオーバーレイ ネットワーク、VXLANでレイヤ2の隣接関係を維持します。

サブネット間のテナントトラフィックの転送を促進するレイヤ3VNID

ACIファブリックは、ACIファブリックVXLANネットワーク間のルーティングを実行するテナントのデフォルトゲートウェイ機能を備えています。各テナントに対して、ファブリックはテナントに割り当てられたすべてのリーフスイッチにまたがる仮想デフォルトゲートウェイを提供します。これは、エンドポイントに接続された最初のリーフスイッチの入力インターフェイスで提供されます。各入力インターフェイスはデフォルトゲートウェイインターフェイスをサポートします。ファブリック全体のすべての入力インターフェイスは、特定のテナントサブネットに対して同一のルータのIPアドレスとMACアドレスを共有します。

ACIファブリックは、エンドポイントのロケータまたはVXLANトンネルエンドポイント(VTEP)アドレスで定義された場所から、テナントエンドポイントアドレスとその識別子を切り離します。ファブリック内の転送はVTEP間で行われます。次の図は、ACIで切り離されたIDと場所を示します。

図4: ACIによって切り離されたIDと場所



VXLANはVTEPデバイスを使用してテナントのエンドデバイスをVXLANセグメントにマッピングし、VXLANのカプセル化およびカプセル化解除を実行します。各VTEP機能には、次の2つのインターフェイスがあります。

- ブリッジングを介したローカルエンドポイント通信をサポートするローカルLANセグメントのスイッチインターフェイス
- 転送IPネットワークへのIPインターフェイス

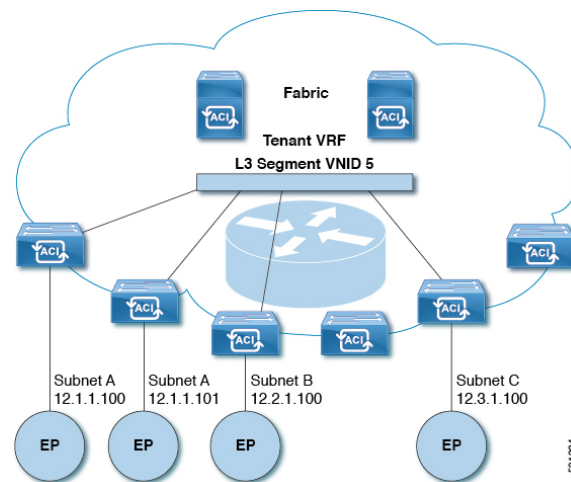
IPインターフェイスには一意のIPアドレスがあります。これは、インフラストラクチャVLANとして知られる、転送IPネットワーク上のVTEPを識別します。VTEPデバイスはこのIPアドレスを使用してイーサネットフレームをカプセル化し、カプセル化されたパケットを、IPインターフェイスを介して転送ネットワークへ送信します。また、VTEPデバイスはリモートVTEPでVXLANセグメントを検出し、IPインターフェイスを介してリモートのMAC Address-to-VTEP マッピングについて学習します。

ACIのVTEPは分散マッピングデータベースを使用して、内部テナントのMACアドレスまたはIPアドレスを特定の場所にマッピングします。VTEPはルックアップの完了後に、宛先リーフスイッチ上のVTEPを宛先アドレスとして、VXLAN内でカプセル化された元のデータパケットを送信します。宛先リーフスイッチはパケットをカプセル化解除して受信ホストに送信します。このモデルにより、ACIはスパニングツリープロトコルを使用することなく、フルメッシュでシングルホップのループフリートポロジを使用してループを回避します。

VXLANセグメントは基盤となるネットワークトポロジに依存しません。逆に、VTEP間の基盤となるIPネットワークは、VXLANオーバーレイに依存しません。これは送信元IPアドレスとして開始VTEPを持ち、宛先IPアドレスとして終端VTEPを持っており、外部IPアドレスヘッダーに基づいてパケットをカプセル化します。

次の図は、テナント内のルーティングがどのように行われるかを示します。

図5: ACIのサブネット間のテナントトラフィックを転送するレイヤ3 VNID



ACIはファブリックの各テナントVRFに単一のL3VNIDを割り当てます。ACIは、L3VNIDに従ってファブリック全体にトラフィックを転送します。出力リーフスイッチでは、ACIによってL3VNIDからのパケットが出力サブネットのVNIDにルーティングされます。

ACIのファブリックデフォルトゲートウェイに送信されてファブリック入力に到達したトラフィックは、レイヤ3VNIDにルーティングされます。これにより、テナント内でルーティングされるトラフィックはファブリックで非常に効率的に転送されます。このモデルを使用すると、たとえば同じ物理ホスト上の同じテナントに属し、サブネットが異なる2つのVM間では、トラフィックが(最小パスコストを使用して)正しい宛先にルーティングされる際に経由する必要があるは入力スイッチインターフェイスのみです。

ACIルートリフレクタは、ファブリック内での外部ルートの配布にマルチプロトコルBGP(MP-BGP)を使用します。ファブリック管理者は自律システム(AS)番号を提供し、ルートリフレクタにするスパインスイッチを指定します。



(注) Cisco ACIはIPフラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ3 Outside (L3Out) 接続、またはInter-Pod Network (IPN) を介したマルチポッド接続を設定する場合は、インターフェイスMTUがリンクの両端で適切に設定することを推奨します。Cisco ACI、Cisco NX-OS、およびCisco IOSなどの一部のプラットフォームでは、設定可能なMTU値はイーサネットヘッダー(一致するIP MTU、14-18イーサネットヘッダーサイズを除く)を考慮していません。また、IOS XRなどの他のプラットフォームには、設定されたMTU値にイーサネットヘッダーが含まれています。設定された値が9000の場合、Cisco ACI、Cisco NX-OS およびCisco IOSの最大IPパケットサイズは9000バイトになりますが、IOS-XRのタグなしインターフェイスの最大IPパケットサイズは8986バイトになります。

各プラットフォームの適切なMTU値については、それぞれの設定ガイドを参照してください。

CLIベースのコマンドを使用してMTUをテストすることを強く推奨します。たとえば、Cisco NX-OS CLIで、コマンド、`ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1` を使用してください。



第 3 章

レイヤ 3 ネットワーク設定の前提条件

この章は、次の内容で構成されています。

- [レイヤ 3 前提条件 \(11 ページ\)](#)

レイヤ 3 前提条件

このガイドのタスクを開始する前に、次のことを行ってください。

- ACI ファブリックと APIC コントローラがオンラインであり、APIC クラスタが形成され健全であることを確認します—詳細については、*Cisco APIC Getting Started Guide, Release 2.x* を参照してください。
- レイヤ 3 ネットワークを構成する管理者のファブリック管理者アカウントが使用可能であることを確認します—詳細については、*Cisco APIC Basic Configuration Guide* の *User Access, Authentication, and Accounting* および *Management* の章を参照してください。
- 目的のリーフ スイッチとスパイン スイッチ (必要なインターフェイスを使用可能) が使用可能であることを確認します—詳細については、*Cisco APIC Getting Started Guide, Release 2.x* を参照してください。

仮想スイッチのインストールと登録の詳細については、*Cisco ACI Virtualization Guide* を参照してください。

- レイヤ 3 ネットワークを消費するテナント、ブリッジドメイン、VRF、および EPG (アプリケーションプロファイルとコントラクトを含む) を設定します—詳細については、*Cisco APIC Basic Configuration Guide* の *Basic User Tenant Configuration* の章を参照してください。
- NTP、DNS サービス、および DHCP リレー ポリシーを設定します—詳細については、*Cisco APIC Basic Configuration Guide, Release 2.x* の *Provisioning Core ACI Fabric Services* の章を参照してください。



注意 ファブリックのリーフスイッチとスパインスイッチの間に1ギガビットイーサネット (GE) または10GEリンクを設置すると、帯域幅が不十分なために、パケットが転送されずにドロップされる可能性があります。これを避けるためには、リーフスイッチとスパインスイッチの間に40GEまたは100GEリンクを使用してください。

ブリッジドメインの設定

レイヤ3の設定 ブリッジドメイン [0] パネルのタブには次のパラメータを設定するには、管理者が使用できます。

- **ユニキャストルーティング** : この設定が有効になっているサブネットアドレスが設定されている場合は、ファブリックはデフォルトゲートウェイの機能を提供して、トラフィックをルーティングします。ユニキャストルーティングを有効にすると、マッピングデータベースがこのブリッジドメインのエンドポイントに付与されたIPアドレスとVTEPの対応関係を学習します。IP学習は、ブリッジドメイン内にサブネットが構成されているかどうかにかかわらず行われます。
- **サブネットアドレス** : このオプションは、ブリッジドメインのSVI IP アドレス (デフォルトゲートウェイ) を設定します。
- **制限のサブネットIPラーニング** : このオプションは、ユニキャストリバース転送パスチェックに似ています。このオプションを選択すると、ファブリックはブリッジドメインに設定されている1以外のサブネットからIPアドレスを学習されません。



注意 有効化 **サブネットに制限IPラーニング** がブリッジドメイン内のトラフィックを停止します。



第 4 章

共通パーベイスブ ゲートウェイ

この章は、次の内容で構成されています。

- [概要 \(13 ページ\)](#)
- [GUI を使用した共通パーベイスブ ゲートウェイの設定 \(14 ページ\)](#)

概要

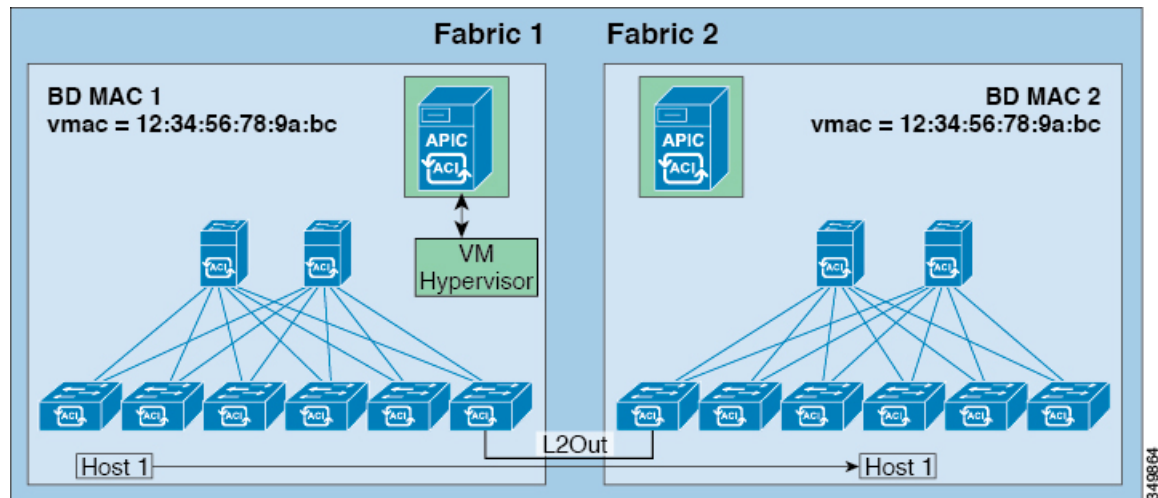


(注) Common Pervasive Gateway 機能は廃止されており、アクティブに維持されていません。

複数の Cisco ACI ファブリックを運用する場合は、共通パーベイスブ ゲートウェイ機能を使用してリーフスイッチを介して複数の個々の ACI ファブリックを相互接続するのではなく、マルチサイトを導入することを強く推奨します。Common Pervasive Gateway 機能は現在サポートされていません。これは、このトポロジでは L3 マルチキャストなどの他の多くの新機能の検証および品質保証テストが実行されないためです。したがって、Cisco ACI には Multi-Site の前に ACI ファブリックを相互接続するための共通パーベイスブ ゲートウェイ機能がありましたが、個別の APIC ドメインを相互接続する必要がある場合は、代わりに Multi-Site を使用して新しい ACI ファブリックを設計することを強く推奨します。

この例は、Cisco APIC を使用して、IPv4 共通パーベイスブ ゲートウェイを設定する方法について示しています。

ブリッジドメインごとに IPv4 共通ゲートウェイを使用して 2 つの ACI ファブリックを設定できます。これにより、1 つ以上の仮想マシン (VM) または従来型のホストを、ホストの IP アドレスを保持したまま、ファブリック間で移動できます。ファブリック間の VM ホストの移動は、VM ハイパーバイザによって自動的に行うことができます。ACI ファブリックは、同じ場所に配置することも、複数のサイト間でプロビジョニングすることもできます。ACI ファブリック間のレイヤ 2 接続は、ローカルリンクか、ブリッジ型ネットワークにわたるものになります。次の図は、基本的な共通パーベイスブ ゲートウェイ トポロジを示しています。



(注) 2つのCisco ACIファブリックを相互接続するために用いられるトポロジによっては、相互接続するデバイスが、ゲートウェイスイッチの仮想インターフェイス(SVI)の仮想MACアドレスを持つトラフィックの送信元を除外する必要があります。

GUIを使用した共通パーベシブゲートウェイの設定

始める前に

- テナントおよびVRFが作成されていること。
- ブリッジドメインの仮想MACアドレスとサブネットの仮想IPアドレスは、ブリッジドメインのすべてのCisco Application Centric Infrastructure (ACI) ファブリックで同じにする必要があります。複数のブリッジドメインを、接続されているCisco ACIファブリック間で通信するように設定できます。仮想MACアドレスと仮想IPアドレスは、ブリッジドメイン間で共有できます。
- Cisco ACIファブリック間で通信するように設定されているブリッジドメインは、[フラッド (flood)] モードである必要があります。
- BDに複数のEPGがある場合、ブリッジドメインの1つのEPGのみを、2つ目のファブリックに接続されているポートの境界リーフ上に設定する必要があります。
- 2つのCisco ACIファブリック間のパーベシブ共通ゲートウェイを有効にする相互接続されたレイヤ2ネットワークには、ホストを直接接続しないでください。

ステップ1 メニューバーで、[テナント]をクリックします。

ステップ2 [ナビゲーション (Navigation)] ペインで、[Tenant_name] > [ネットワーキング (Networking)] > [ブリッジドメイン (Bridge Domains)] の順に展開します。

ステップ3 [Bridge Domains] を右クリックし、[Create Bridge Domain] をクリックします。

ステップ4 [Create Bridge Domain] ダイアログボックスで、必要な操作を実行し、適切な属性を選択します。

- a) [Main] タブで、[Name] フィールドにブリッジドメインの名前を入力し、残りのフィールドに必要な値を選択します。
- b) [L3 configurations] タブで [Subnets] を展開し、[Create Subnets] ダイアログボックスの [Gateway IP] フィールドに IP アドレスを入力します。
たとえば、192.0.2.1/24 です。
- c) [Treat as virtual IP address] フィールドで、チェックボックスをオンにします。
- d) [Make this IP address primary] フィールドで、DHCP リレーにこの IP アドレスを指定するチェックボックスをオンにします。
このチェックボックスをオンにすると、DHCP リレーにのみ影響します。
- e) [OK] をクリックし、[次 (Next)] をクリックして [アドバンス/トラブルシューティング (Advanced/Troubleshooting)] タブに進み、[終了 (Finish)] をクリックします。

ステップ5 [Work] ペインで作成した Bridge Domain をダブルクリックし、次の操作を実行します。

- a) [ポリシー (Policy)] タブをクリックして、[L3 コンフィグレーション (L3 Configurations)] サブタブをクリックします。
- b) もう一度 [サブネット (Subnets)] を展開し、仮想 IP アドレスとして設定されているものと同じサブネットを使用して、[サブネットの作成 (Create Subnets)] ダイアログボックスの [ゲートウェイ IP (Gateway IP)] フィールドで物理 IP アドレスを作成します。

たとえば、仮想 IP アドレスに 192.0.2.1/24 を使用した場合、物理 IP アドレスには 192.0.2.2/24 を使用できます。

(注) 物理 IP アドレスは Cisco ACI ファブリック全体で一意である必要があります

- c) [送信 (Submit)] をクリックして [サブネットの作成 (Create Subnet)] ウィンドウで設定を完了します。

ステップ6 作成したブリッジドメインと同じブリッジドメインの [L3 コンフィグレーション (L3 Configurations)] タブで、[仮想 MAC アドレス (Virtual MAC Address)] フィールドをクリックし、[設定なし (Not Configured)] を適切な値に変更して、[送信 (Submit)] をクリックします。

(注) デフォルトブリッジドメインの MAC アドレス値はすべての Cisco ACI ファブリックで同じです。この設定では、ブリッジドメイン MAC 値が各 Cisco ACI ファブリックで一意である必要があります。

各ファブリックのブリッジドメイン MAC (pMAC) 値が一意であることを確認してください。

(注) この手順では、基本的に、このフィールドに入力した仮想 MAC アドレスと前の手順で入力した仮想 IP アドレスを関連付けます。将来のある時点で仮想 MAC アドレスを削除する場合は、前の手順で入力した IP アドレスの [仮想 IP アドレスとして扱う (Treat as virtual IP address)] フィールドのチェックも外す必要があります。

ステップ7 ブリッジドメインを別のファブリックに拡張するために L2Out EPG を作成するには、[ナビゲーション (Navigation)] ペインで **[L2Outs]** を右クリックし、**[L2Out の作成 (Create L2Out)]** をクリックして、次のアクションを実行します。

- a) **[Name]** フィールドに、ブリッジされる Outside の名前を入力します。
 - b) **[Bridge Domain]** フィールドで、すでに作成されているブリッジドメインを選択します。
 - c) **[Encap]** フィールドに、その他のファブリック l2out カプセル化に一致する VLAN カプセル化を入力します。
 - d) **[Path Type]** フィールドで、**[Port]**、**[PC]**、または **[VPC]** を選択して EPG を導入し、**[Next]** をクリックします。
 - e) 外部 EPG ネットワークを作成するには、**[Name]** フィールドをクリックしてネットワークの名前を入力し (QoS クラスの指定も可能)、**[Finish]** をクリックして共通パーベイスブ設定を完了します。
-



第 5 章

IP エージング

この章は、次の内容で構成されています。

- [概要 \(17 ページ\)](#)
- [GUI を使用した IP エージングポリシーの設定 \(17 ページ\)](#)

概要

IP エージング ポリシーは、エンドポイントの未使用の IP アドレスを追跡しエージングが行われます。トラッキングはブリッジドメインに設定されたエンドポイント保持ポリシーを使用して実行され、ローカルエンドポイント エージング間隔の 75% で、ARP 要求 (IPv4) やネイバー要請 (IPv6) を送信します。IP アドレスから応答を受信しなかった場合、その IP アドレスはエージングアウトします。

このドキュメントでは、IP エージング ポリシーを設定する方法について説明します。

GUI を使用した IP エージングポリシーの設定

このセクションでは、IP エージング ポリシーの有効と無効を切り替える方法について説明します。

ステップ 1 メニューバーで、**System** タブをクリックします。

ステップ 2 サブメニューバーで、**System Settings** をクリックします。

ステップ 3 ナビゲーション ウィンドウで、**Endpoint Controls** をクリックします。

ステップ 4 作業ウィンドウで、**Ip Aging** をクリックします。

IP Aging Policy が、**Administrative State** の **Disabled** ボタンが選択された状態で表示されます。

ステップ 5 **Administrative State** で、次のオプションのいずれかをクリックします:

- **Enabled**— IP エージングを有効にします。

- **Disabled**— IP エージングを無効にします。
-

次のタスク

エンドポイントの IP アドレスを追跡するために使用される間隔を指定するには、エンドポイント保持ポリシーを作成します。**Tenants > *tenant-name* > Policies > Protocol** に移動し、**End Point Retention** を右クリックし、**Create End Point Retention Policy** を選択します。



第 6 章

スタティック ルート ブリッジ ドメイン

この章は、次の内容で構成されています。

- [スタティック ルート ブリッジ ドメインについて \(19 ページ\)](#)
- [GUI を使用してブリッジ ドメインでのスタティック ルートを設定する \(20 ページ\)](#)

スタティック ルート ブリッジ ドメインについて

Cisco APIC リリース 3.0(2) では、ファイアウォールの背後にある仮想サービスへのルーティングを可能にする、パーベイシブ ブリッジ ドメイン (BD) でのスタティック ルート設定へのサポートが追加されました。

この機能は、通常の EPG の使用を通して、エンドポイント (EP) がパーベイシブ ブリッジ ドメインに直接には接続されていない IP アドレスへ到達することを可能にします。

スタティック ルートを設定すると、APIC は、それをブリッジ ドメインを使用しているすべてのリーフ スイッチ、およびそのブリッジ ドメインに関連付けられた契約を有しているすべてのリーフ スイッチに展開します。

エンドポイントの到達可能性は、APIC GUI、NX-OS スタイル CLI および REST API を使用して設定できます。

注意事項と制約事項

- サブネットマスクは、/32 (IPv6 の場合は /128) にしてファブリック内の 1 つの IP アドレスをポイントする必要があります。すでに定義されているブリッジ ドメインサブネット内にルートを追加しないでください。
- ネクストホップは、この EPG が関連付けられているのと同じブリッジ ドメイン内にある必要があります。
- この機能は、名前の末尾が EX である Cisco Nexus 9000 シリーズ スイッチとそれ以降の機種によりサポートされています (たとえば N9K-C93180LC-EX)。

GUIを使用してブリッジドメインでのスタティックルートを設定する

- スタティックルートのサブネットを作成するには、epg (fvAEPg で fvSubnet オブジェクト)、普及 BD (fvBD) 自体 BD しないに関連付けられているように構成されます。
- サブネットマスクが/32 にする必要があります (128/for IPv6) 1つの IP アドレスまたは1つのエンドポイントをポイントします。これは、パーベイシブ BD に関連付けられている EPG に含まれます。

始める前に

テナント、VRF、BD、および EPG の作成

-
- ステップ 1** メニューバーで、**Tenants** > *tenant-name* の順にクリックします。
 - ステップ 2** ナビゲーションウィンドウで **Application Profiles** を展開し、アプリケーションプロファイル名をクリックします。
 - ステップ 3** **Application EPGs** をクリックして、スタティックルートの EPG を展開します。
 - ステップ 4** **Subnets** を展開して、スタティックルートのサブネットを右クリックし、**Create Endpoints Behind EPG Subnet** を選択します。
 - ステップ 5** エンドポイントの **NextHop IP Address** を入力して、**Update** をクリックします。
 - ステップ 6** [送信 (Submit)] をクリックします。
-



第 7 章

データプレーン IP アドレス学習

この章は、次の内容で構成されています。

- データプレーン IP アドレス ラーニングの概要 (21 ページ)
- データプレーン IP アドレス ラーニングのガイドラインと制限事項 (22 ページ)
- 無効にするデータプレーン IP アドレス ラーニングの機能相互作用 (23 ページ)
- GUI を使用した VRF インスタンスごとのデータプレーン IP アドレス ラーニングの設定 (24 ページ)
- GUI を使用したエンドポイントごとのデータプレーン IP アドレス ラーニングの設定 (25 ページ)
- GUI を使用したサブネットごとのデータプレーン IP アドレス ラーニングの設定 (26 ページ)

データプレーン IP アドレス ラーニングの概要

エンドポイントの IP アドレスと MAC アドレスは、ARP、GARP、ND などの一般的なネットワーク方式を通じて () ファブリックによって学習されます。また、データプレーンを介して IP アドレスと MAC アドレスを学習する内部方式も使用します。Cisco Application Centric Infrastructure (ACI) では、データプレーン IP アドレスの学習がデフォルトで有効になっています。Cisco ACI

VRF インスタンスごとのデータプレーン IP アドレス ラーニングは、エンドポイント ラーニングと同じように Cisco ACI ネットワークに固有です。エンドポイント ラーニングが IP アドレスおよび MAC アドレスの両方として特定される一方、データプレーン IP ラーニングは VRF インスタンスのみの IP アドレスに固有です。Cisco Application Policy Infrastructure Controller (APIC) では、VRF インスタンス レベルでデータプレーン IP アドレス ラーニングを有効または無効にできます。

リリース 5.2(1) 以降では、より詳細な制御のために、特定のエンドポイントまたはサブネットのデータプレーン IP アドレス ラーニングをディセーブルにできます。Cisco APIC

データプレーン IP アドレス ラーニングのガイドラインと制限事項

VRF インスタンス、ブリッジ ドメイン サブネット、および EPG サブネットごとのデータプレーン IP アドレス学習には、次のガイドラインと制約事項が適用されます。

- データプレーン IP アドレス ラーニングを無効にすると、テナント VRF 内のリモート IP アドレスのすべてのエントリが削除されます。ローカル IP エントリはエージアウトされ、その後、データプレーンを通じて再学習されることはありませんが、コントロールプレーンからは引き続き学習できます。
- データプレーン IP アドレス ラーニングを無効にすると、すでに学習したローカル IP エンドポイントは保持され、動作を維持するにはコントロールプレーンの更新が必要になります (IP エージングも有効であると想定)。データプレーン レイヤ3 トラフィックは IP エンドポイントの動作を維持しません。
- EPG-to-EPG イントラ VRF インスタンス レイヤ3 トラフィックの場合、入力リーフスイッチは宛先クラスを解決できないため、ポリシーは常に出力リーフスイッチに適用されます。リモート IP アドレスは学習されません。
- EPG-to-EPG イントラ VRF インスタンス レイヤ2 トラフィックでは、スイッチはリモート MAC アドレスを学習できますが、リモート IP アドレスは学習できないため、入力リーフスイッチにポリシーを適用できます。
- データプレーン IP アドレスの学習がエンドポイントまたはサブネットに対して有効になっている場合、データプレーン IP アドレスは、CPU に到達しないエンドポイント間 ARP 要求を使用して学習されません。ただし、ブリッジ ドメイン SVI ゲートウェイへの ARP 要求は引き続き学習されます。
- データプレーン IP アドレス ラーニングが VRF インスタンスに対して有効になっている場合、ローカルおよびリモート MAC アドレスは、エンドポイント間 ARP 要求を使用して学習されます。

エンドポイントまたはサブネットごとのデータプレーン IP アドレス ラーニングの無効化には、次のガイドラインと制約事項が適用されます。

- 同じブリッジ ドメイン内のエンドポイント間に通信がある場合は、ブリッジドメインで L2 unknown Unicast プロパティを Flood に設定する必要があります。ARP フラッディングも有効にする必要があります。そうしないと、ローカル MAC アドレスとリモート MAC アドレスがエンドポイント間エンドポイント ARP 要求によって学習されないため、同じブリッジ ドメイン内のエンドポイント間の ARP は機能しません。
- フラッシュする代わりに、ローカル IP アドレスは dp-lrn-dis (データプレーン学習ディセーブル) 状態に変換されます。
- エンドポイントのサブネットがデータプレーン IP アドレス学習を無効に設定されている場合、エンドポイント データプレーン IP アドレス学習を有効にすることはできません。

たとえば、学習が無効になっているサブネット100.10.0.1/24と、学習が有効になっている100.10.0.100/32のEPGを持つブリッジドメインはありません。

- エンドポイントまたはサブネットでデータプレーンIPアドレスの学習が無効になっている場合、スイッチは、ルーティングされたレイヤ3データトラフィックからレイヤ2MACアドレスを学習または更新しません。レイヤ2MACアドレスは、レイヤ2データトラフィックまたはARPパケットからのみ学習されます。
- エンドポイントまたはサブネットのデータプレーンIPアドレス学習が無効になっている場合、GARPパケットからトリガーされたIPアドレス学習または移動は、ARPフラッドモードとGARPベースのエンドポイント移動検出が有効になっている場合にのみ可能です。

無効にするデータプレーンIPアドレスラーニングの機能相互作用

ここでは、無効にするデータプレーンIPアドレスラーニングとその他の機能との相互作用についての情報を示します。

- エニーキャスト
 - 有効：ローカルエニーキャストIPアドレスは、データプレーンとコントロールプレーンのどちらからでも学習できます。
 - 無効：ローカルエニーキャストIPアドレスはエージアウトしますが、コントロールプレーンとホストトラッキングから学習することができます。
 - リモートIPアドレスは、VRFインスタンスごとのデータプレーンIPアドレスラーニングの設定方法を問わず、エニーキャストで学習されません。
- 不正なエンドポイントの検出
 - 有効：不正なIPアドレスが生成され、移動は意図したとおりに検出されます。
 - 無効：リモートIPアドレスがフラッシュされ、不正なIPアドレスはエージアウトされます。不正なIPアドレスはローカルの移動では検出されません。検出される唯一の移動は、コントロールトラフィックからのものです。バウンスはCOOPから学習されますが、バウンスタイマーが時間切れになるとこれらはドロップされます。
- レイヤ4～レイヤ7サービス仮想IP (VIP) アドレス
 - 有効：レイヤ4からレイヤ7サービスVIPアドレスは期待どおりに機能します (VIPアドレスのエンドポイントIPアドレスラーニングはコントロールプレーン経由のみ)。次の機能ストリームを考えます。
 1. クライアントからロードバランサへ (レイヤ3トラフィック)
 2. サーバへのロードバランサ (レイヤ2トラフィック)

3. サーバからクライアント（レイヤ3）

EPGの背後のクライアント（IPエンドポイント）は、データ/コントロールプレーンを通じて学習されます。VIPアドレスはロードバランサEPGのコントロールプレーン経由でのみ学習されます。コントロールプレーン経由であっても、VIPアドレスは他のEPGでは学習されません。

• [Disabled] :

- クライアントからロードバランサ：VIPアドレスではリモートIPアドレスが学習されません。リモートIPアドレスはクリアされます。spine-proxyを使用します。VIPのIPアドレスが学習されると、spine-proxyルックアップは成功します。そうでない場合はVIPアドレスにグリーンリングを生成し、コントロールプレーンを通じて学習します。
- ロードバランサからサーバへ：影響なし。DSRの使用例では、ロードバランサ/サーバ間のブリッジだけがサポートされています。
- サーバからクライアント：クライアントのリモートIPアドレスはクリアされ、spine-proxyが使用されます。クライアントエントリのリモートIPアドレスがスパインスイッチで削除された場合、グリーンリングを通じて再学習されます。L3outの背後にあるクライアントの場合、レイヤ3リモートIPアドレスはありません。

GUIを使用したVRFインスタンスごとのデータプレーンIPアドレスラーニングの設定

このセクションでは、VRFインスタンスごとのデータプレーンIPラーニングを無効にする方法について説明します。

次の手順では、テナントとVRFインスタンスがすでに設定されていると仮定します。

ステップ1 [テナント (Tenants)] > [tenant_name] > [ネットワーキング (Networking)] > [VRFs] > [vrf_name] に移動します。

ステップ2 [VRF - vrf_name] 作業ペインで、[Policy] タブをクリックします。

ステップ3 [Policy] 作業ペインの下にスクロールし、[IP Data-plane Learning] を探します。

ステップ4 次のいずれかをクリックします。

- [無効化 (Disabled)] : VRFインスタンスでのデータプレーンIPアドレスラーニングを無効にします。
- [有効化 (Enabled)] : VRFインスタンスでのデータプレーンIPアドレスラーニングを有効にします。

ステップ5 [送信 (Submit)] をクリックします。

GUIを使用したエンドポイントごとのデータプレーンIPアドレスラーニングの設定

次の手順では、選択したエンドポイントグループのエンドポイントのデータプレーンIPアドレス学習を有効または無効にします。エンドポイントのデータプレーンIPアドレスラーニングを設定できるのは、EPGサブネットIPアドレスのマスクがIPv4アドレスの場合は/32、IPv6アドレスの場合は/128です。データプレーンIPアドレスの学習は、デフォルトで有効になっています。

ステップ1 メニューバーで、[テナント (Tenants)] > [すべてのテナント (ALL Tenants)] の順に選択します。 >

ステップ2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ3 既存のサブネットを変更する場合は、次のサブステップを実行します。

- a) ナビゲーションペインで、[テナント (Tenant)] *[tenant_name]* > [アプリケーション プロファイル (Application Profiles)] > *[app_profile_name]* > [アプリケーション EPG (Application EPGs)] > *[app_epg_name]* > [サブネット (Subnets)] > *[subnet_address]* の順に選択します。

選択したサブネットは、次の要件を満たしている必要があります。

- [デフォルト ゲートウェイ IP (Default Gateway IP)] フィールドのマスクは、IPv4 アドレスの場合は /32、IPv6 アドレスの場合は /128です。
 - [デフォルト SVI ゲートウェイなし (No Default SVI Gateway)] チェック ボックスをオンにする必要があります。
 - [Behind Subnet のタイプ (Type Behind Subnet)] は [なし (None)] または [エニキャスト MAC (Anycast MAC)] である必要があります。
- b) [ワーク (Work)] ペインの [IP データプレーンの学習 (IP Data-plane Learning)] で、[有効 (Enable)] または [無効 (Disable)] を選択します。

これにより、エンドポイントの IP アドレス データプレーンの学習が有効または無効になります。

ステップ4 新しいサブネットを作成する場合は、次のサブステップを実行します。

- a) ナビゲーションペインで、[テナント (Tenant)] *[tenant_name]* > [アプリケーション プロファイル (Application Profiles)] > *[app_profile_name]* > [アプリケーション EPG (Application EPGs)] > *[app_epg_name]* > [サブネット (Subnets)] の順に選択します。
- b) [サブネット (Subnets)] を右クリックし、[EPG サブネットの作成 (Create EPG Subnet)] を選択します。
- c) [デフォルト ゲートウェイ IP (Default Gateway IP)] フィールドには、IPv4 アドレスの場合は /32、IPv6 アドレスの場合は /128 のマスクを指定する必要があります。

- d) [デフォルト SVI ゲートウェイなし (No Default SVI Gateway)] チェック ボックスをオンにする必要があります。
- e) [Behind Subnet のタイプ (Type Behind Subnet)] ボタンで、[なし (None)] または[エニキャスト MAC (Anycast MAC)] を選択します。
- f) [IP データプレーンの学習 (IP Data-plane Learning)] トグルで、必要に応じて[有効化 (Enable)] または[無効化 (Disable)] を選択します。
これにより、エンドポイントの IP アドレス データ プレーンの学習が有効または無効になります。
- g) 必要に応じて、残りのフィールドに入力します。

ステップ 5 [送信 (Submit)] をクリックします。

GUI を使用したサブネットごとのデータ プレーン IP アドレス ラーニングの設定

次の手順では、サブネットのデータプレーン IP アドレス学習を有効または無効にします。データプレーン IP アドレスの学習は、デフォルトで有効になっています。

ステップ 1 メニュー バーで、[テナント (Tenants)] > [すべてのテナント (ALL Tenants)] の順に選択します。 >

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 既存のサブネットを変更する場合は、次のサブステップを実行します。

- a) [ナビゲーション (Navigation)] ペインで、[テナント (Tenant)] *tenant_name* > [ネットワーク (Networking)] > [ブリッジドメイン (Bridge Domains)] > [*bridgedomain_name*] > [サブネット (Subnets)] > [*subnet_address*] の順に選択します。

データプレーンの IP アドレスラーニングを無効にする場合は、[デフォルト SVI ゲートウェイなし (No Default SVI Gateway)] チェックボックスをオンにしないでください。

- b) [作業 (Work)] ペインの [IP データプレーンの学習 (IP Data-plane Learning)] で、[有効化 (Enable)] または [無効化 (Disable)] を選択します。

これにより、サブネットの IP アドレスデータプレーンの学習が有効または無効になります。

ステップ 4 新しいサブネットを作成する場合は、次のサブステップを実行します。

- a) [ナビゲーション (Navigation)] ペインで、[テナント (Tenant)] *tenant_name* > [ネットワーク (Networking)] > [ブリッジドメイン (Bridge Domains)] > [*bridgedomain_name*] > [サブネット (Subnets)] の順に選択します。
- b) [サブネット (Subnets)] を右クリックし、[サブネットの作成 (Create Subnet)] を選択します。
- c) [デフォルト ゲートウェイ IP (Default Gateway IP)] フィールドで、IP アドレスとマスクを入力します。
- d) データプレーンの IP アドレスラーニングを無効にする場合は、[デフォルト SVI ゲートウェイなし (No Default SVI Gateway)] チェックボックスをオンにしないでください。

- e) [IPデータプレーンの学習 (IP Data-plane Learning)] トグルで、必要に応じて [有効化 (Enable)] または [無効化 (Disable)] を選択します。

これにより、サブネットの IP アドレス データプレーンの学習が有効または無効になります。

- f) 必要に応じて、残りのフィールドに入力します。

ステップ 5 [送信 (Submit)] をクリックします。



第 8 章

IPv6 ネイバー探索

この章は、次の内容で構成されています。

- [ネイバー探索 \(29 ページ\)](#)
- [ブリッジドメインでの IPv6 ネイバー探索の設定 \(30 ページ\)](#)
- [レイヤ 3 インターフェイス上での IPv6 ネイバー探索の設定 \(32 ページ\)](#)
- [IPv6 ネイバー探索重複アドレス検出の設定 \(33 ページ\)](#)

ネイバー探索

IPv6 ネイバー探索 (ND) は、ノードのアドレスの自動設定、リンク上の他のノードの探索、他のノードのリンク層アドレスの判別、重複アドレスの検出、使用可能なルータと DNS サーバの検出、アドレスプレフィックスの探索、および他のアクティブなネイバーノードへのパスに関する到達可能性情報の維持を担当します。

ND 固有のネイバー要求/ネイバーアドバタイズメント (NS/NA) およびルータ要求/ルータアドバタイズメント (RS/RA) パケットタイプは、物理、層3サブインターフェイス、および SVI (外部およびパーベイシブ) を含むすべての ACI ファブリックのレイヤ3インターフェイスでサポートされます。APIC リリース 3.1(1x) まで、RS/RA パケットはすべてのレイヤ3インターフェイスの自動設定のために使用されますが、拡散型 SVI の設定のみ可能です。

APIC リリース 3.1(2x) より、RS/RA パケットは自動設定のため使用され、ルーテッドインターフェイス、レイヤ3サブインターフェイス、SVI (外部および拡散) を含むレイヤ3インターフェイスで設定できます。

ACI のブリッジドメイン ND は常にフラッドモードで動作します。ユニキャストモードはサポートされません。

ACI ファブリック ND サポートに含まれるもの：

- インターフェイスポリシー (nd:IfPol) は、NS/NA メッセージに関する ND タイマーと動作を制御します。
- ND プレフィックスポリシー (nd:PfxPol) コントロール RA メッセージ。
- ND の IPv6 サブネット (fv:Subnet) の設定。

- 外部ネットワークのNDインターフェイスポリシー。
- 外部ネットワークの設定可能NDサブネットおよびパーベイシブブリッジドメインの任意サブネット設定はサポートされません。

設定可能なオプションは次のとおりです。

- 隣接関係
 - 設定可能な静的 Adjacencies : (<vrf、L3Iface < ipv6 address> --> mac address)
 - 動的 Adjacencies : NS/NA パケットの交換経由で学習
- インターフェイス単位
 - ND パケットの制御 (NS/NA)
 - ネイバー要求間隔
 - ネイバー要求再試行回数
 - RA パケットの制御
 - RA の抑制
 - RA MTU の抑制
 - RA 間隔、RA 最小間隔、再送信時間
- プレフィックス単位 (RA でアドバタイズ) の制御
 - ライフタイム、優先ライフタイム
 - プレフィックス コントロール (自動設定、リンク上)
- ネイバー検索重複アドレスの検出 (DAD)

ブリッジドメインでのIPv6ネイバー探索の設定

GUIを使用して、ブリッジドメイン上にIPv6ネイバー探索対応のテナント、VRF、およびブリッジドメインを作成する

このタスクでは、テナント、VRF、およびブリッジドメイン (BD) を作成し、それらの中に2つの異なるタイプのネイバー探索 (ND) ポリシーを作成する方法を示します。これらはNDインターフェイスポリシーとNDプレフィックスポリシーです。NDインターフェイスポリシーはBDに導入されますが、NDプレフィックスポリシーは個々のサブネットに導入されません。各BDに独自のNDインターフェイスポリシーを適用することができます。NDインターフェイスポリシーは、デフォルトですべてのIPv6インターフェイスに導入されます。Cisco

APICには、使用可能なデフォルトのNDインターフェイスポリシーがすでに存在します。必要に応じて、代わりに使用するカスタムNDインターフェイスポリシーを作成できます。NDプレフィックスポリシーはサブネットレベルにあります。すべてのBDが複数のサブネットを持つことができ、各サブネットが異なるNDプレフィックスを持つことができます。

- ステップ1** メニューバーで、[テナント (TENANT)] > [テナントの追加 (Add Tenant)] の順にクリックします。
- ステップ2** [Create Tenant] ダイアログボックスで、次のタスクを実行します。
- [Name] フィールドに、名前を入力します。
 - [Security Domains +] アイコンをクリックして [Create Security Domain] ダイアログボックスを開きます。
 - [Name] フィールドに、セキュリティドメインの名前を入力します。 **Submit** をクリックします。
 - [Create Tenant] ダイアログボックスで、作成したセキュリティドメインのチェックボックスをオンにし、[Submit] をクリックします。
- ステップ3** [Navigation] ペインで、[Tenant-name] > [Networking] の順に展開します。
- ステップ4** [Work] ペインで、[VRF] アイコンをキャンバスにドラッグして [Create VRF] ダイアログボックスを開き、次の操作を実行します。
- [Name] フィールドに、名前を入力します。
 - [Submit] をクリックして VRF の設定を完了します。
- ステップ5** [ネットワークング (Networking)] 領域で、[ブリッジドメイン (Bridge Domain)] アイコンを [VRF] アイコンにつながらながらキャンバスにドラッグします。 [Create Bridge Domain] ダイアログボックスが表示されたら、次の操作を実行します。
- [Name] フィールドに、名前を入力します。
 - [L3 Configurations] タブをクリックし、[Subnets] を展開して [Create Subnet] ダイアログボックスを開き、[Gateway IP] フィールドにサブネットマスクを入力します。
- ステップ6** [Subnet Control] フィールドで、[ND RA Prefix] チェックボックスがオンになっていることを確認します。
- ステップ7** [ND Prefix policy] フィールドのドロップダウンリストで、[Create ND RA Prefix Policy] をクリックします。
- (注) すべてのIPv6インターフェイスに導入される使用可能なデフォルトポリシーがすでに存在しています。または、この例で示されているように、使用するNDプレフィックスポリシーを作成できます。デフォルトでは、IPv6ゲートウェイのサブネットはND RAメッセージのNDプレフィックスとしてアドバタイズされます。ユーザは、[ND RA prefix] チェックボックスをオフにして、ND RAメッセージでサブネットをアドバタイズしないことを選択できます。
- ステップ8** [Create ND RA Prefix Policy] ダイアログボックスで、次の操作を実行します。
- [Name] フィールドにプレフィックスポリシーの名前を入力します。

(注) 特定のサブネットに対して存在できるプレフィックスポリシーは1つのみです。サブネットは共通プレフィックスポリシーを使用できますが、各サブネットに異なるプレフィックスポリシーを適用することが可能です。
 - [Controller State] フィールドで、目的のチェックボックスをオンにします。

- c) [Valid Prefix Lifetime] フィールドで、プレフィックスを有効にする期間について目的の値を選択します。
 - d) [Preferred Prefix Lifetime] フィールドで、目的の値を選択します。[OK] をクリックします。
- (注) ND プレフィックス ポリシーが作成され、特定のサブネットに接続されます。

ステップ9 [ND policy] フィールドのドロップダウンリストで、[Create ND Interface Policy] をクリックし、次のタスクを実行します。

- a) [Name] フィールドにポリシーの名前を入力します。
- b) [Submit] をクリックします。

ステップ10 [OK] をクリックしてブリッジドメインの設定を完了します。

同様に、さまざまなプレフィックス ポリシーが適用された追加のサブネットを必要に応じて作成できます。

IPv6 アドレスのサブネットが BD に作成され、ND プレフィックス ポリシーが関連付けられています。

レイヤ3インターフェイス上でのIPv6ネイバー探索の設定

注意事項と制約事項

次のガイドラインと制限事項に適用ネイバー探索ルータ アドバタイズメント (ND RA) のプレフィックスのレイヤ3インターフェイス。

- NDRA 設定は、IPv6プレフィックスにのみ適用されます。IPv4プレフィックスでNDポリシーを設定しようとするは適用に失敗します。

GUIを使用して、レイヤ3インターフェイス上のRAのIPv6ネイバー探索インターフェイスポリシーの設定



- (注) 次の手順では、レイヤ3インターフェイスでIPv6ネイバー探索インターフェイスポリシーを関連付ける方法を表示します。この特定の例は、非VPCインターフェイスを使用して設定する方法を示しています。

始める前に

- テナント、VRF、BD が作成されていること。

- 外部ルーテッド ネットワークで、L3Out が作成されます。

-
- ステップ1 ナビゲーション**]ペインで、適切なテナントで、適切な外部ルーテッド ネットワークに移動します。
- ステップ2 [L3Outs]** で、 >[論理ノード プロファイル (Logical Node Profiles)] > [Logical Node Profile_name] > [論理インターフェイス プロファイル (Logical Interface Profiles)] を展開します。
- ステップ3** 適切な [論理インターフェイス プロファイル (Logical Interface Profile)] をダブルクリックし、 [作業 (Work)] ペインで [ポリシー (Policy)] > [ルーテッド インターフェイス (Routed Interfaces)] をクリックします。

(注) 作成論理インターフェイスプロファイルを持っていない場合は、ここにプロファイルを作成することができます。

ステップ4 Routed Interface ダイアログボックスで、次の操作を実行します:

- a) **NDRA プレフィックス** フィールドで、インターフェイスのNDRAプレフィックスを有効にするチェックボックスをチェックします。

有効にすると、ルーテッドインターフェイスは自動設定使用できます。

また、 **ND RA プレフィックス ポリシー** フィールドが表示されます。

- b) **ND RA Prefix Policy** フィールドで、ドロップダウンリストから、適切なポリシーを選択します。
- c) 必要に応じて、画面上の他の値を選択します。 [Submit] をクリックします。`

(注) **VPC インターフェイス** を使用してを設定する際に、 **VPC** の設定内のメンバは、その両方としてに、 **サイド A** と **サイド B** の両方の **ND RA プレフィックス** が有効にする必要があります。作業 () ペインで、 **論理インターフェイス プロファイル** 画面で、をクリックします **SVI ()** タブ。 **プロパティ**、有効にするチェックボックスをオン、 **ND RA プレフィックス** **サイド A** と **サイド B** の両方を選択、同一の **ND RA プレフィックス ポリシー** **サイド A** と **サイド B** の

IPv6 ネイバー探索重複アドレス検出の設定

ネイバー探索重複アドレス検出について

重複アドレス検出 (DAD) は、ネットワーク内で重複アドレスを検出するためにネイバー探索が使用するプロセスです。デフォルトでは、ACI ファブリック リーフ レイヤ3 インターフェイスで使用されているリンクローカルアドレスとグローバルサブネット IPv6 アドレスの DAD が有効になっています。オプションとして、REST API (`ipv6Dad="disabled"` 設定を使用) または GUI を通してノブを構成することにより、IPv6 グローバルサブネットの DAD プロセスを無効にすることができます。外部接続されたデバイスに境界リーフ冗長性を提供するため、異なる境界リーフ スイッチ上の L3Outs にわたって同じ共有セカンダリ アドレスが必要な場合には、このノブを構成します。このような場合、DAD プロセスを無効にすれば、DAD が複数の

境界リーフ スイッチ上の同じ共有セカンダリ アドレスを重複と見なすことを避けられます。このような場合にはDADプロセスを無効にしないと、共有セカンダリ アドレスがDUPLICATE DAD 状態に入り、使用できなくなることがあります。

GUI を使用したネイバー探索重複アドレス検出の設定

サブネットのネイバー探索重複アドレス検出プロセスを無効にするには、このセクションの手順に従ってください。

- ステップ 1** 適切なページに移動して、そのインターフェイスの DAD フィールドにアクセスします。次に例を示します。
- [テナント (Tenants)] > [テナント (Tenant)] > [ネットワーキング (Networking)] > [L3Outs] > [L3Out] > [論理ノード プロファイル (Logical Node Profiles)] > [ノード (node)] > [論理インターフェイス プロファイル (Logical Interface Profiles)] に移動し、設定するインターフェイスを選択します。
 - Routed Sub-interfaces* または *SVI* をクリックし、作成 (+) ボタンをクリックしてインターフェイスを設定します。

ステップ 2 このインターフェイスで、DAD エントリを次のように設定します:

- プライマリ アドレスでは、DAD エントリの値を **enabled** に設定します。
- 共有セカンダリ アドレスでは、DAD エントリの値を **disabled** に設定します。セカンダリ アドレスが境界リーフ スイッチ間で共有されていない場合には、そのアドレスの DAD を無効にする必要がないことに注意してください。

例 :

たとえば、SVI インターフェイスのこの設定を構成する場合には、次のようになります:

- サイド A の IPv6 DAD を **enabled** に設定します。
- サイド B の IPv6 DAD を **disabled** に設定します。

例 :

別の例として、ルーテッドサブインターフェイスの設定を構成する場合には、次のようになります:

- メインの [Select Routed Sub-Interface] ページで、ルーテッドサブインターフェイスの IPv6 DAD を **enabled** に設定します。
- [IPv4 Secondary/IPv6 Additional Addresses] エリアで作成 (+) ボタンをクリックして [Create Secondary IP Address] ページにアクセスし、IPv6 DAD の値を **disabled** に設定します。[OK] ボタンをクリックして、この画面での変更点を適用します。

ステップ 3 [Submit] ボタンをクリックして、変更を適用します。

ステップ 4 リーフ スイッチで `show ipv6 int` コマンドを入力して、設定がリーフ スイッチに正しくプッシュされたか確認してください。例 :

```
swtb23-leaf5# show ipv6 int vrf icmpv6:v1
IPv6 Interface Status for VRF "icmpv6:v1" (9)
```



```
vlan2, Interface status: protocol-up/link-up/admin-up, iod: 73
if_mode: ext
IPv6 address:
  2001:DB8:A::2/64 [VALID] [PREFERRED]
  2001:DB8:A::11/64 [VALID] [dad-disabled]
IPv6 subnet: 2001:DB8:A::/64
IPv6 link-local address: fe80::863d:c6ff:fe9f:eb8b/10 (Default) [VALID]
```



第 9 章

Microsoft NLB

この章は、次の内容で構成されています。

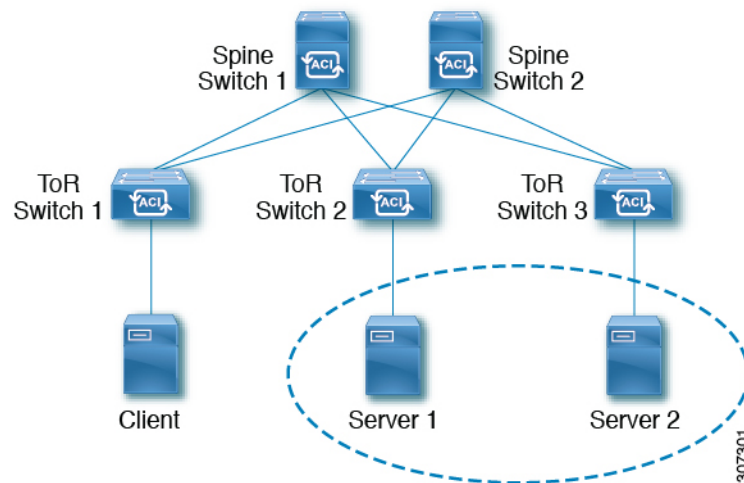
- [Microsoft NLB について \(37 ページ\)](#)
- [Cisco ACI Microsoft NLB サーバの設定 \(41 ページ\)](#)
- [Microsoft Network Load Balancing の注意事項と制限事項 \(45 ページ\)](#)
- [GUI を使用したユニキャスト モードでの Microsoft NLB の設定 \(46 ページ\)](#)
- [GUI を使用したマルチキャスト モードでの Microsoft NLB の設定 \(47 ページ\)](#)
- [GUI を使用した IGMP モードでの Microsoft NLB の設定 \(48 ページ\)](#)

Microsoft NLB について

Microsoft ネットワーク ロード バランシング (NLB) 機能は、クライアント トラフィックを多数のサーバに分散し、各サーバがアプリケーションの個別のコピーを実行します。ネットワーク ロード バランシングは、レイヤ2の不明なユニキャストまたはマルチキャストを使用して、着信ネットワーク トラフィックをすべてのクラスタ ホストに同時に分散します。

Microsoft NLB ノードのグループは、NLB クラスタと総称されます。NLB クラスタは、1つ以上の仮想IP (VIP) アドレスのサービスを提供します。NLB クラスタ内のノードは、ロードバランシング アルゴリズムを使用して、NLB VIP 宛ての特定のトラフィック フローを処理する個々のノードを決定します。クラスタ内のすべてのノードはトラフィックのすべてのパケットを受信しますが、1つのノードだけが要求を処理します。

次の図に、Microsoft NLB の実装方法を図で示します。Cisco APIC



この図では、サーバ1とサーバ2がMSNLBクラスタにあります。これらのサーバは、外部クライアントには単一ホストサーバとして表示されます。MSNLBクラスタ内のすべてのサーバがすべての着信要求を受信すると、MSNLBはサーバ間で負荷を分散します。

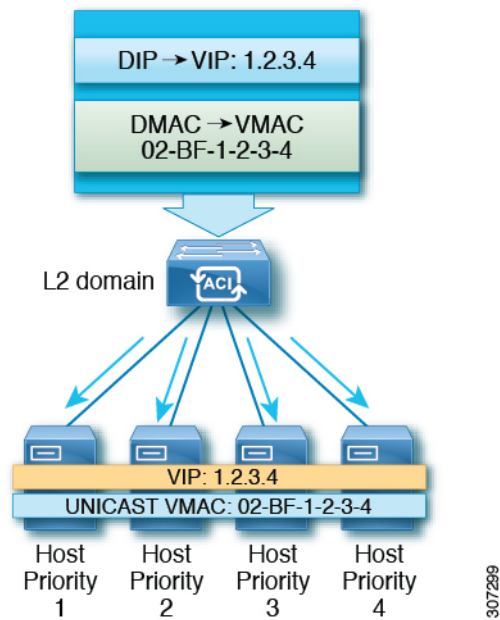
3種類の異なる動作モードでのMicrosoft NLBの機能：

- **ユニキャストモード**：このモードでは、各NLBクラスタVIPにユニキャストMACアドレスが割り当てられます。このモードは、トラフィックをクラスタに配信するために不明なユニキャストフラグディングに依存します。
- **マルチキャストモード**：このモードでは、各NLBクラスタVIPが非Internet Assigned Numbers Authority (IANA) マルチキャストMACアドレス (03xx.xxxx.xxxx) に割り当てられます。
- **IGMPモード**：このモードでは、NLBクラスタVIPが一意のIPv4マルチキャストグループアドレスに割り当てられます。このためのマルチキャストMACアドレスは、IPv4マルチキャストアドレスの標準MAC導出から導出されます。

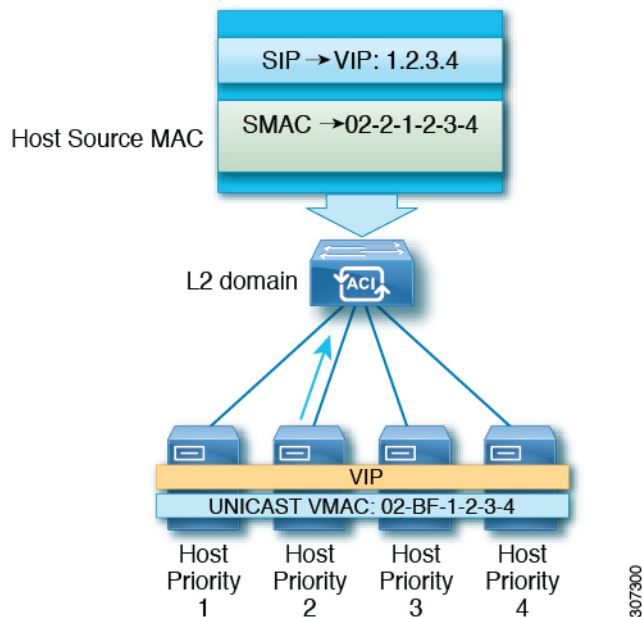
ユニキャストモードについて

ユニキャスト動作モードでは、ネットワーク負荷分散は、それが有効になっているネットワークアダプタ（クラスタアダプタと呼ばれる）のMACアドレスを再割り当てし、すべてのクラスタホストに同じMACアドレスが割り当てられます。このMACアドレスは、クラスタのプライマリIPアドレスから取得されます。たとえば、プライマリIPアドレスが1.2.3.4の場合、ユニキャストMACアドレスは02-BF-1-2-3-4に設定されます。

ネットワークロードバランシングのユニキャストモードでは、次の図に示すように、着信ネットワークトラフィックをすべてのクラスタホストに同時に配信します。

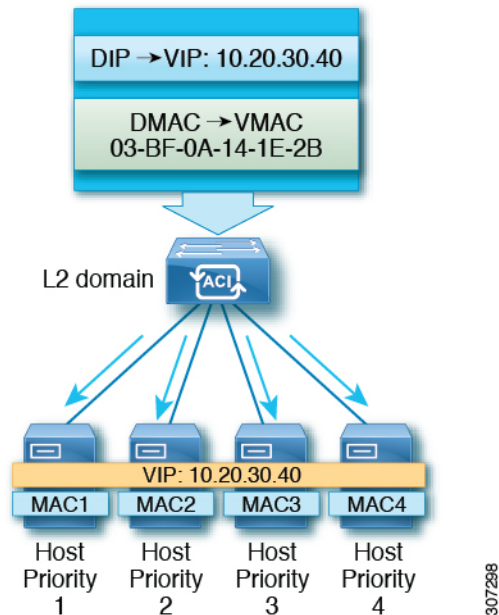


レイヤ2スイッチでは、すべてのスイッチポートで一意的な送信元MACアドレスが認識されるため、共通のMACアドレスを使用すると、通常は競合が発生します。この問題を回避するために、ネットワークロードバランシングは発信パケットの送信元MACアドレスを一意的に変更します。クラスタのMACアドレスが02-BF-1-2-3-4の場合、各ホストの送信元MACアドレスは02-x-1-2-3-4に設定されます。xはクラスタ内のホストの優先順位です。次の図に示します。



マルチキャストモードについて

ネットワークロードバランシングは、着信ネットワークトラフィックをすべてのクラスタホストに分散するためのマルチキャストモードも提供します。マルチキャストモードは、アダプタのMACアドレスを変更する代わりに、レイヤ2マルチキャストアドレスをクラスタアダプタに割り当てます。たとえば、マルチキャストMACアドレスは、クラスタのプライマリIPアドレス10.20.30.40に対して03-BF-0A-14-1E-28に設定できます。クラスタ通信には別のアダプタは必要ありません。

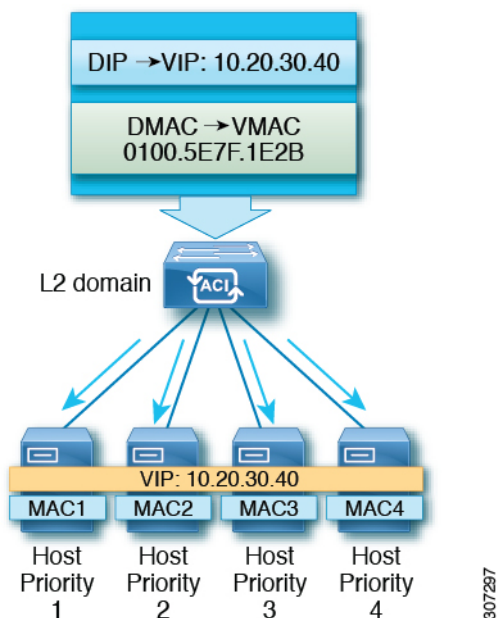


IGMPモードについて

Microsoft NLB サーバは、IGMP を使用してマルチキャストグループに参加するように設定することもできます。これをスイッチのクエリアおよびIGMPスヌーピングと組み合わせることで、マルチキャストメッセージのフラッドの範囲を最適化できます。

Microsoft NLB サーバは、マルチキャストグループアドレスにIGMP Joinを送信します。マルチキャストアドレスの最後の2つのオクテットは、クラスタIPの最後の2つのオクテットに対応します。たとえば、Microsoft NLB サーバが239.255.xxのマルチキャストアドレスにIGMP Joinを送信する状況では、次のようになります。

- クラスタ IP : 10.20.30.40
- IGMP が 239.255. に送信されました。 30.40
- クライアントからサーバ方向で使用される MAC : 0100.5E7F.1E28
- クラスタ通信には別のアダプタは必要ありません



307287

Cisco ACI Microsoft NLB サーバの設定

リリース 4.1 より前の Microsoft NLB 導入では、ファブリックはレイヤ2のみである必要があり、エンドポイントのレイヤ3ゲートウェイとして外部ルータを使用します。Cisco ACIリリース 4.1 以降、ファブリックは Microsoft NLB 導入のレイヤ3ゲートウェイになります。Cisco ACI

次の表に、各 Microsoft NLB 導入モードの導入に関する考慮事項の概要を示します。

表 2: Cisco ACI Microsoft NLB を使用した導入モード

	ユニキャストモード	マルチキャストモード	IGMPモード
Cisco ACI レイヤ2 ネットワークとして、レイヤ3ゲートウェイとして外部ルータを使用	スイッチ名の末尾に -EX、-FX、または -FX2 があるリーフスイッチモデルでサポートされます。	スイッチ名の末尾に -EX、-FX、または -FX2 が付いたリーフスイッチモデル、およびスイッチ名の末尾にサフィックスがないリーフスイッチモデルでサポートされます。	スイッチ名の末尾に -EX、-FX、または -FX2 が付いたリーフスイッチモデル、およびスイッチ名の末尾にサフィックスがないリーフスイッチモデルでサポートされます。ただし、Microsoft NLB トラフィックは IGMP によってスコープされず、代わりにフラッディングされます。
Cisco ACI レイヤ3ゲートウェイとして	リリース 4.1 以降でサポートされます。	リリース 4.1 以降でサポートされます。	リリース 4.1 以降でサポートされます。

次の表に、Cisco ACI をレイヤ2として使用してMicrosoft NLBを導入するために使用できる設定オプションの詳細を示します。

表 3: 3つの Microsoft NLB モードの外部ルータおよび ACI ブリッジドメインの設定

	ユニキャストモード	マルチキャストモード	IGMP モードリリース 3.2 では、Microsoft NLB マルチキャストモードと比較して Microsoft NLB IGMP モードを使用しても、複数宛先トラフィックのスコーピングに関して利点はありません。 ¹
ACI ブリッジドメインの設定	<ul style="list-style-type: none"> 不明なユニキャストフラッディング用に設定されたブリッジドメイン (hw-proxy 以外) No IP routing 	<ul style="list-style-type: none"> 不明なユニキャストフラッディング用に設定されたブリッジドメイン (hw-proxy 以外) No IP routing レイヤ3 不明なマルチキャスト: フラッディング (最適化されたマルチキャストフラッディングでも、Microsoft NLB トラフィックがフラッディングされる) IGMP スヌーピング設定: 該当なし 	<ul style="list-style-type: none"> 不明なユニキャストフラッディング用に設定されたブリッジドメイン (hw-proxy 以外) No IP routing レイヤ3 不明なマルチキャスト: オプションですが、将来の互換性のために設定可能 クエリア設定: オプションですが、将来の互換性のために有効にできます。ブリッジドメインの下にサブネットを設定します。IP ルーティングは不要です。 IGMP スヌーピング設定: オプションですが、将来の互換性のためにイネーブルにできます。
外部ルータ ARP テーブルの設定	<ul style="list-style-type: none"> 特別な ARP 設定なし 外部ルータが VIP から VMAC へのマッピングを学習する 	ユニキャスト VIP からマルチキャスト MAC へのスタティック ARP 設定	ユニキャスト VIP からマルチキャスト MAC へのスタティック ARP 設定

1

リリース 4.1 以降、Microsoft NLB サーバを接続するための設定は、次の一般的なタスクで構成されています。Cisco ACI

- VRF の設定。出力または入力モードで VRF を設定できます。
- Microsoft NLB サーバのブリッジドメイン (BD) を設定します。ハードウェア プロキシモードではなく、フラッディングモードで L2 ユニキャストを使用します。
- 同じ VIP を共有するすべての Microsoft NLB サーバの EPG を定義します。この EPG を以前に定義した BD に関連付ける必要があります。
- EPG でサブネットとして Microsoft NLB VIP を入力します。Microsoft NLB は、次のモードで設定できます。
 - ユニキャストモード：Microsoft NLB VIP 設定の一部としてユニキャスト MAC アドレスを入力します。このモードでは、クライアントから Microsoft NLB VIP へのトラフィックは、Microsoft NLB BD 内のすべての EPG にフラッディングされます。
 - マルチキャストモード：Microsoft NLB VIP 自体の設定時にマルチキャスト MAC アドレスを入力します。Microsoft NLB EPG の静的ポートに移動し、Microsoft NLB サーバが接続されている EPG ポートに Microsoft NLB マルチキャスト MAC を追加します。このモードでは、トラフィックはスタティック MAC バインディングを持つポートに転送されます。
 - IGMPモード：Microsoft NLB VIP 自体の設定時に Microsoft NLB グループアドレスを入力します。このモードでは、クライアントから Microsoft NLB VIP へのトラフィックは、Microsoft NLB グループアドレスの IGMP Join を受信するポートに転送されます。
- Microsoft NLB EPG とクライアント EPG 間のコントラクトの設定。Microsoft NLB EPG を契約のプロバイダー側として設定し、クライアント EPG を契約のコンシューマ側として設定する必要があります。

Microsoft NLB は、ルート プラス フラッディング ソリューションです。クライアントから Microsoft NLB VIP へのトラフィックは、まずコンシューマ ToR スイッチでルーティングされ、次に Microsoft NLB BD でプロバイダー ToR スイッチに向けてフラッディングされます。

トラフィックがコンシューマ ToR スイッチを出ると、トラフィックはフラッディングされ、コントラクトはフラッディングトラフィックに適用できません。したがって、契約の適用はコンシューマ ToR スイッチで行う必要があります。

入力モードの VRF の場合、境界リーフ スイッチ (コンシューマ ToR スイッチ) にポリシーがないため、L3Out から Microsoft NLB EPG への VRF 内トラフィックがコンシューマ ToR スイッチでドロップされることがあります。この問題を回避するには、次のいずれかのオプションを使用します。

- オプション 1：出力モードで VRF を設定します。出力モードで VRF を設定すると、ポリシーは境界リーフ スイッチにダウンロードされます。
- オプション 2：Microsoft NLB EPG と L3Out の L3external を優先グループに追加します。トラフィックは、コンシューマ ToR スイッチのデフォルト許可ポリシーにヒットします。
- オプション 3：アップ状態の未使用ポート、または境界リーフ スイッチ上の Microsoft NLB サーバに接続されているポートに Microsoft NLB EPG を展開します。これにより、Microsoft

NLB EPG は境界リーフ スイッチのローカルエンドポイントになります。ポリシーはローカルエンドポイント用にダウンロードされるため、境界リーフ スイッチにはポリシーがダウンロードされません。

- オプション 4 : 共有サービスを使用します。プロバイダーの Microsoft NLB VRF とは異なる、コンシューマ VRF に L3Out を展開します。Microsoft NLB EPG の Microsoft NLB VIP の場合は、[VRF 間で共有 (Shared VRFs)]ボックスをオンにします。コンシューマ VRF からの L3Out と Microsoft NLB EPG 間のコントラクトを設定します。共有サービスを使用すると、ポリシーは境界リーフ スイッチにダウンロードされません。

次の表に、Microsoft NLB モードでサポートされる EPG および BD 構成の詳細を示します。

表 4: Cisco ACI Microsoft NLB モードの EPG および BD の設定

	ユニキャスト モード	マルチキャスト モード	IGMP モード
ブリッジ ドメインの設定	<ul style="list-style-type: none"> • IP ルーティング • 不明なユニキャスト フラッディング用に設定されたブリッジ ドメイン (hw-proxy 以外) • ブリッジドメインの MAC アドレスは変更しないでください。 	<ul style="list-style-type: none"> • IP ルーティング • 不明なユニキャスト フラッディング用に設定されたブリッジ ドメイン (hw-proxy 以外) • ブリッジドメインの MAC アドレスは変更しないでください。 	<ul style="list-style-type: none"> • IP ルーティング • 不明なユニキャスト フラッディング用に設定されたブリッジ ドメイン (hw-proxy 以外) • ブリッジドメインの MAC アドレスは変更しないでください。
EPG の設定	<ul style="list-style-type: none"> • VIP のサブネット • サブネットの一部として定義されたユニキャスト MAC アドレス 	<ul style="list-style-type: none"> • VIP のサブネット • サブネットの一部として定義されたマルチキャスト MAC アドレス • サーバが存在するポートへのスタティック バインディング • 各パスのスタティック グループ MAC アドレス 	<ul style="list-style-type: none"> • VIP のサブネット • MAC アドレスを入力する必要はありません • ダイナミック グループまたはスタティック グループを選択できます • スタティック グループ オプションを選択した場合は、スタティック パスを入力し、各パスにマルチキャスト グループを入力します。
VMM ドメイン	VMM ドメインを入力できます。	マルチキャスト モードにはスタティック パスが必要であるため、この状況では VMM ドメインを使用できません。	ダイナミック グループ モードでは、VMM ドメインを使用できます。

Microsoft Network Load Balancing の注意事項と制限事項

次は、Microsoft Network Load Balancing (NLB) の注意事項と制限事項です。

- ブリッジドメインのポリシー > の詳細/トラブルシューティング プロパティで、Microsoft NLB VIP アドレスがそのブリッジドメインのいずれかの EPG で設定されている場合は、[マルチキャスト SMAC ノブを使用して ARP をドロップする] を無効にする必要があります。
- ブリッジドメインのマルチデスティネーションフラッドイングがドロップに設定されている場合、Microsoft NLB はサポートされません。
- レイヤ3 マルチキャストはサポートされていません (Microsoft NLB BD で PIM を有効にすることはできません)。
- IGMP の場合、許容されるモードグループは IPv4 です (IPv6 はサポートされません)。
- EX で終了する名前の Cisco Nexus 9000 シリーズスイッチ、およびそれ以降のみがサポートされています。
- Microsoft NLB では、共有サービスおよびマイクロセグメント (uSeg) EPG がサポートされています。
- Cisco ACI マルチサイト は現在サポートされていません。
- レイヤ2 不明ユニキャストフラッドイングモードで Microsoft NLB を設定する必要があります。

代わりにブリッジドメインをハードウェアプロキシ用に設定すると、Cisco ACI はブリッジドメインの設定を修正することでクリアされる障害を発生させます。ブリッジドメインがハードウェアプロキシ用に誤って設定されたままの場合、ACI は 30 秒ごとに障害のある設定を起動しようとはしますが、これはスイッチにとって不要なオーバーヘッドです。

- デフォルトの SVI MAC アドレスを使用して Microsoft NLB ブリッジドメインを設定する必要があります。レイヤ3 設定では、ブリッジドメインの MAC アドレスをデフォルト設定の 00:22:BD:F8:19:FF に設定する必要があります。Microsoft NLB ブリッジドメインのこのデフォルト SVI MAC アドレスは変更しないでください。
- ファブリックあたり 128 の Microsoft NLB VIP のハードウェア制限があります。
- Microsoft NLB 用に設定された仮想サーバは、すべてのモード (ユニキャスト、マルチキャスト、および IGMP) で静的バインディングを使用してに接続できます。Cisco ACI
- Microsoft NLB 用に設定された仮想化されたサーバは、ユニキャストモードと IGMP モードの VMM 統合を介して Cisco ACI に接続できます。
- Microsoft NLB ユニキャストモードは、エンドホストモードの Cisco UCS B シリーズブレードサーバの背後にある VMM 統合ではサポートされません。

ユニキャストモードの Microsoft NLB は、クラスタバウンドパケットの配信について不明なユニキャストのフラッドイングに依存します。ユニキャストモードは、ファブリック

インターコネクトがエンドホストモードの場合、Cisco UCS B シリーズブレードサーバでは機能しません。このモードでは、不明なユニキャストフレームがフラッディングされないためです。エンドホストモードでの Cisco UCS B シリーズブレードサーバのレイヤ2 転送動作の詳細については、以下を参照してください。

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/unified-computing/whitepaper_c11-701962.html

GUIを使用したユニキャストモードでの Microsoft NLB の設定

このタスクは、ブリッジドメインのすべてのポートに Microsoft NLB がフラッドするように設定します。

始める前に

これらの手順を進める前に次の使用可能な情報を準備してください。

- Microsoft NLB クラスタ VIP
- Microsoft NLB クラスタ MAC アドレス

ステップ 1 [ナビゲーション (Navigation)] ペインで、[テナント (Tenant)] > [tenant_name] > [アプリケーション プロファイル (Application Profiles)] > [app_profile_name] > [アプリケーション EPG (Application EPGs)] > [application_EPG_name] > [サブネット (Subnets)] の順に選択します。

ステップ 2 **Subnets** を右クリックして、**Create EPG Subnet** を選択します。

ステップ 3 **Create EPG Subnet** ダイアログ ボックスで、次のフィールドに入力します。

- Default Gateway IP** フィールドで Microsoft NLB cluster VIP を入力します。
たとえば、192.0.2.1/32 です。
- Scope** 領域で、共有サービスに **Shared between VRFs** のチェックをオンにします。
選択されている場合は、**Private to VRF** のチェックをオフにします。
- Subnet Control** で **No Default SVI Gateway** チェックボックスをオンにします。
- Type Behind Subnet** 領域で **EpNlb** をクリックします。
[モード (Mode)] フィールドが表示されます。
- [モード (Mode)] ドロップダウンリストから、[ユニキャストモードの NLB (NLB in unicast mode)] を選択します。
MAC Address フィールドが表示されます。
- [MAC アドレス (MAC Address)] フィールドに Microsoft NLB クラスタ MAC アドレスを入力します。

たとえば、00:01:02:03:04:05 です。

ステップ4 [送信 (Submit)] をクリックします。

GUIを使用したマルチキャストモードでの Microsoft NLB の設定

このタスクは、ブリッジドメインの特定のポートでのみ Microsoft NLB がフラッドするように設定します。

始める前に

これらの手順を進める前に次の使用可能な情報を準備してください。

- Microsoft NLB クラスタ VIP
- Microsoft NLB クラスタ MAC アドレス

ステップ1 [ナビゲーション (Navigation)] ペインで、[テナント (Tenant)] > [tenant_name] > [アプリケーション プロファイル (Application Profiles)] > [app_profile_name] > [アプリケーション EPG (Application EPGs)] > [application_EPG_name] > [サブネット (Subnets)] の順に選択します。

ステップ2 **Subnets** を右クリックして、**Create EPG Subnet** を選択します。

ステップ3 **Create EPG Subnet** ダイアログボックスで、次のフィールドに入力します。

- a) **Default Gateway IP** フィールドで Microsoft NLB cluster VIP を入力します。
たとえば、192.0.2.1/32 です。
- b) **Scope** 領域で、共有サービスに **Shared between VRFs** のチェックをオンにします。
選択されている場合は、**Private to VRF** のチェックをオフにします。
- c) **Subnet Control** で **No Default SVI Gateway** チェックボックスをオンにします。
- d) **Type Behind Subnet** 領域で **EpNlb** をクリックします。
[モード (Mode)] フィールドが表示されます。
- e) [モード (Mode)] ドロップダウン リストから、[スタティック マルチキャストモードの NLB (NLB in static multicast mode)] を選択します。
MAC Address フィールドが表示されます。
- f) [MAC アドレス (MAC Address)] フィールドに Microsoft NLB クラスタ MAC アドレスを入力します。
マルチキャストモードの Microsoft NLB クラスタ MAC アドレスの場合、クラスタ MAC アドレスは 03 で始まる必要があります。

たとえば、03:BF:01:02:03:04です。

- g) マルチキャストモードでこのフィールドに入力したMicrosoft NLB クラスタのMACアドレスをコピーします。

ステップ4 [送信 (Submit)] をクリックします。

ステップ5 [ナビゲーション (Navigation)] ペインで、[テナント (Tenant)] `[tenant_name]` > [アプリケーション プロファイル (Application Profiles)] > `[application_profile_name]` > [アプリケーション EPG (Application EPGs)] > `[application_EPG_name]` > [スタティック ポート (Static Ports)] > `[static_port]` の順に選択します。

ブリッジドメインでMicrosoft NLB をフラッドに設定するスタティックポートを選択します。

ステップ6 このポートのスタティックパス ページで、次のフィールドに入力します。

- a) [NLB スタティック グループ (NLB Static Group)] 領域で[+] (Create) をクリックし、コピーしたMACアドレスを[MAC アドレス (Mac Address)] フィールドに貼り付けます。3.g (48 ページ)
- b) [MAC アドレス (Mac Address)] フィールドの下にある[更新 (Update)] をクリックします。

ステップ7 [スタティックパス (Static Path)] ページで、[送信 (Submit)] をクリックします。

このMicrosoft NLB クラスタ MAC アドレスへのトラフィックは、このスタティックポートに送信されません。

GUIを使用したIGMPモードでのMicrosoft NLBの設定

このタスクは、ブリッジドメインの特定のポートでのみMicrosoft NLBがフラッドするように設定します。

始める前に

これらの手順を進める前に次の使用可能な情報を準備してください。

- Microsoft NLB クラスタ VIP

ステップ1 [ナビゲーション (Navigation)] ペインで、[テナント (Tenant)] > `[tenant_name]` > [アプリケーション プロファイル (Application Profiles)] > `[app_profile_name]` > [アプリケーション EPG (Application EPGs)] > `[application_EPG_name]` > [サブネット (Subnets)] の順に選択します。

ステップ2 Subnets を右クリックして、Create EPG Subnet を選択します。

ステップ3 Create EPG Subnet ダイアログ ボックスで、次のフィールドに入力します。

- a) **Default Gateway IP** フィールドでMicrosoft NLB cluster VIP を入力します。

たとえば、192.0.2.1/32です。

- b) **Scope** 領域で、共有サービスに **Shared between VRFs** のチェックをオンにします。

選択されている場合は、**Private to VRF** のチェックをオフにします。

- c) **Subnet Control** で **No Default SVI Gateway** チェックボックスをオンにします。
- d) **Type Behind Subnet** 領域で **EpNlb** をクリックします。

[モード (Mode)] フィールドが表示されます。

- e) [モード (Mode)] ドロップダウン リストから、**[IGMP モードの NLB (NLB in IGMP mode)]** を選択します。

[グループ ID (Group Id)] フィールドが表示されます。

- f) [グループ ID (Group Id)] フィールドに、Microsoft NLB マルチキャスト グループ アドレスを入力します。

Microsoft NLB マルチキャスト グループ アドレスの場合、アドレスの最後の 2 オクテットは、インスタンス クラスタ IP アドレスの最後の 2 オクテットに対応します。たとえば、インスタンス クラスタの IP アドレスが 10.20.30.40 の場合、このフィールドに入力する Microsoft NLB マルチキャスト グループ アドレスは 239.255.30.40 になります。

ステップ 4 [送信 (Submit)] をクリックします。`

Microsoft NLB クラスタ VIP へのトラフィックは、APIC から静的に、または NLB クラスタからの IGMP 参加に基づいて動的に設定された発信インターフェイス リストにフラッドされます。

ステップ 5 スタティック結合とダイナミック結合のどちらを使用するかを決定します。

スタティック結合とダイナミック結合を組み合わせで使用できます。一部のポートはスタティック結合を使用でき、他のポートはダイナミック結合を使用できます。

- **Dinamic Join** : ダイナミック結合では、それぞれのポートで Microsoft NLB クラスタによって結合が送信され、スイッチはその発信インターフェイス リストを使用して動的に起動します。
- **Static Join** : スタティック結合では、Microsoft NLB クラスタ VIP へのトラフィックは、次の手順で設定したポートに送信されます。

スタティック結合を使用する場合 :

1. [グループ ID (Group Id)] フィールドに入力した Microsoft NLB マルチキャスト グループ アドレスをコピーします。 [3.f \(49 ページ\)](#)
2. [ナビゲーション (Navigation)] ペインで、[テナント (Tenant)] > [tenant_name] > [アプリケーション プロファイル (Application Profiles)] > [app_profile_name] > [アプリケーション EPG (Application EPGs)] > [application_EPG_name] > [スタティック ポート (Static Ports)] > [static_port] の順に選択します。

ブリッジ ドメインで Microsoft NLB をフラッドに設定するスタティック ポートを選択します。

3. このポートの **スタティック パス** ページで、次のフィールドに入力します。

- **[IGMP スヌープ スタティック グループ (IGMP Snoop Static Group)]** 領域で **[+] (作成 (Create))** をクリックし、コピーした MAC アドレスを **[グループ アドレス (Group Address)]** フィールドに貼り付けます。 [3.f \(49 ページ\)](#)

- [グループ アドレス (Group Address)] フィールドの下にある [更新 (Update)] をクリックします。

4. スタティック パス ページで [送信 (Submit)] をクリックします。

ブリッジドメインではデフォルトでIGMP スヌーピングがオンになっています。これは、ブリッジドメインに関連付けられたIGMPスヌーピングポリシー「デフォルト」により、ポリシーの管理状態として[有効化 (Enabled)] になるためです。詳細については、[GUIを使用したIGMPスヌーピングポリシーの設定 \(55 ページ\)](#) を参照してください。



第 10 章

IGMP スヌーピング

- Cisco APIC および IGMP スヌーピングについて (51 ページ)
- IGMP スヌーピング ポリシーの設定と割り当て (55 ページ)
- IGMP スヌーピングの静的ポート グループの有効化 (57 ページ)
- IGMP スヌープ アクセス グループの有効化 (59 ページ)

Cisco APIC および IGMP スヌーピングについて

ACI ファブリックに IGMP スヌーピングを実装するには



- (注) ブリッジ ドメインで IGMP スヌーピングをディセーブルにしないことを推奨します。IGMP スヌーピングをディセーブルにすると、ブリッジ ドメインで不正なフラッドイン グが過度に発生し、マルチキャストのパフォーマンスが低下する場合があります。

IGMP スヌーピング ソフトウェアは、ブリッジ ドメイン内の IP マルチキャスト トラフィックを調べて、該当する受信側が常駐するポートを検出します。IGMP スヌーピングではポート情報を利用することにより、マルチアクセスブリッジドメイン環境における帯域幅消費量を削減し、ブリッジドメイン全体へのフラッドイングを回避します。デフォルトでは、IGMP スヌーピングがブリッジドメインでイネーブルにされています。

この図は、ホストへの接続を持つ ACI リーフ スイッチに含まれる IGMP ルーティング機能と IGMP スヌーピング機能を示しています。IGMP スヌーピング機能は、IGMP メンバーシップ レポートをスヌーピングし、メッセージを残し、必要な場合にのみ IGMP ルータ機能に転送します。

その結果、ACI ファブリックは送信元 IP アドレス 0.0.0.0 の IGMP レポートを送信します。



(注) IGMP スヌーピングの詳細については、RFC 4541 を参照してください。

仮想化のサポート

IGMP スヌーピングに対して、複数の仮想ルーティングおよび転送（VRF）インスタンスを定義できます。

リーフスイッチでは、**show** コマンドに VRF 引数を指定して実行すると、表示される情報のコンテキストを確認できます。VRF 引数を指定しない場合は、デフォルト VRF が使用されます。

APIC IGMP スヌーピング機能、IGMPv1、IGMPv2、および高速リーフ機能

IGMPv1 と IGMPv2 は両方とも、メンバーシップ レポート抑制をサポートします。つまり、同一サブネット上の2つのホストが同一グループのマルチキャストデータを受信する場合、他方のホストからメンバー レポートを受信するホストは、そのレポートを送信しません。メンバーシップ レポート抑制は、同じポートを共有しているホスト間で発生します。

各スイッチポートに接続されているホストが1つしかない場合は、IGMPv2 の高速脱退機能を設定できます。高速脱退機能を使用すると、最終メンバーのクエリーメッセージがホストに送信されません。APIC は、IGMP 脱退メッセージを受信すると、ただちに該当するポートへのマルチキャスト データ転送を停止します。

IGMPv1 では、明示的な IGMP 脱退メッセージが存在しないため、APIC の IGMP スヌーピング機能は、特定のグループについてマルチキャストデータを要求するホストが存続しないことを示すために、メンバーシップ メッセージ タイムアウトを使用する必要があります。



(注) 高速脱退機能がイネーブルになっている場合、他のホストの存在は確認されないため、IGMP スヌーピング機能は、最終メンバーのクエリーインターバル設定を無視します。

APIC IGMP スヌーピング ファンクションキーと IGMPv3

APIC での IGMPv3 スヌーピング ファンクションでは、完全な IGMPv3 スヌーピングがサポートされています。これにより、IGMPv3 レポートの（S、G）情報に基づいて、抑制されたフラグgingが提供されます。この送信元ベースのフィルタリングにより、デバイスは対象のマルチキャストグループにトラフィックを送信する送信元に基づいて、マルチキャストトラフィックの宛先ポートを制限できます。

デフォルトでは、IGMP スヌーピング機能は、ブリッジドメインでは、各 VLAN ポート上のホストを追跡します。この明示的なトラッキング機能は、高速脱退メカニズムをサポートして

います。IGMPv3ではすべてのホストがメンバーシップレポートを送信するため、レポート抑制機能を利用すると、デバイスから他のマルチキャスト対応ルータに送信されるトラフィック量を制限できます。レポート抑制を有効にしても、IGMPv1 または IGMPv2 ホストが同じグループをリクエストしなかった場合、IGMP スヌーピング機能はプロキシレポートを作成します。プロキシ機能により、ダウンストリームホストが送信するメンバーシップレポートからグループステートが構築され、アップストリームクエリアからのクエリーに応答するためにメンバーシップレポートが生成されます。

IGMPv3 メンバーシップレポートにはブリッジドメインのグループメンバの一覧が含まれていますが、最終ホストが脱退すると、ソフトウェアはメンバーシップクエリーを送信します。最終メンバーのクエリーインターバルについてパラメータを設定すると、タイムアウトまでのどのホストからも応答がなかった場合、IGMP スヌーピングはグループステートを削除します。

Cisco APIC および IGMP スヌーピング クエリア関数

マルチキャストトラフィックをルーティングする必要がないために、Protocol-Independent Multicast (PIM) がインターフェイス上でディセーブルになっている場合は、メンバーシップクエリーを送信するようにIGMP スヌーピングクエリア機能を設定する必要があります。APIC、IGMP スヌープポリシー内で定義マルチキャストのソースとレシーバが含まれているブリッジドメインでクエリアがないその他のアクティブなクエリアします。

Cisco ACI はデフォルトで、IGMP スヌーピングが有効になっています。さらに、ブリッジドメインサブネット制御は、「クエリア IP」を選択、リーフスイッチによって、クエリアとして動作およびクエリパケット送信を開始します。セグメントは、明示的なマルチキャストルータ (PIM が有効になっていません) があるときに ACI Leaf スイッチでクエリアを有効にする必要があります。ブリッジドメインで、クエリアが設定されている、使用される IP アドレスマルチキャストのホストが設定されている同じサブネットからにする必要があります。



-
- (注) クエリアのIPアドレスは、ブロードキャストIPアドレス、マルチキャストIPアドレス、または0 (0.0.0.0) にしないでください。
-

IGMP スヌーピングクエリアがイネーブルな場合は、定期的にIGMPクエリーが送信されるため、IPマルチキャストトラフィックを要求するホストからIGMPレポートメッセージが発信されます。IGMP スヌーピングはこれらのIGMPレポートを待ち受けて、適切な転送を確立します。

IGMP スヌーピングクエリアは、RFC 2236 に記述されているようにクエリア選択を実行します。クエリア選択は、次の構成で発生します。

- 異なるスイッチ上の同じVLANに同じサブネットに複数のスイッチクエリアが設定されている場合。
- 設定されたスイッチクエリアが他のレイヤ3SVIクエリアと同じサブネットにある場合。

APIC IGMP スヌーピング機能の注意事項と制約事項

APIC IGMP スヌーピング機能に関する注意事項および制約事項は次のとおりです：

- レイヤ3 IPv6 マルチキャスト ルーティングはサポートされていません。
- レイヤ2 IPv6 マルチキャスト パケットは、着信ブリッジ ドメインでフラッディングされます。
- IGMPv3 スヌーピングは、ブリッジ ドメインで PIM が有効になっている場合にのみ、グループと送信元エントリに基づいてマルチキャストを転送します。PIM が有効になっていない場合、転送はグループのみに基づいて行われます。

IGMP スヌーピング ポリシーの設定と割り当て

拡張 GUI のブリッジ ドメインへの IGMP スヌーピング ポリシーの設定と割り当て

IGMP スヌーピング機能を実装するには、IGMP スヌーピングポリシーを設定し、そのポリシーを1つまたは複数のブリッジ ドメインに割り当てます。

GUI を使用した IGMP スヌーピング ポリシーの設定

IGMP 設定を1つまたは複数のブリッジ ドメインに割り当てることが可能な IGMP スヌーピングポリシーを作成します。

- ステップ1 [テナント] タブと、IGMP スヌーピング サポートを設定することを意図したブリッジ ドメインのテナントの名前をクリックします。
- ステップ2 [ナビゲーション (Navigation)] ペインで、[ポリシー (Policies)] > [プロトコル (Protocol)] > [IGMP スヌープ (IGMP Snoop)] をクリックします。
- ステップ3 [IGMP スヌープ] を右クリックし、[IGMP スヌープ ポリシーの作成] を選択します。
- ステップ4 **Create IGMP Snoop Policy** ダイアログで、次のようにポリシーを設定します。
 - a) [Name] フィールドと [Description] フィールドに、ポリシーの名前と説明をそれぞれ入力します。
 - b) [管理状態 (Admin State)] フィールドで [有効化 (Enables)] または [無効化 (Disabled)] を選択して、この特定のポリシーの IGMP スヌーピングを有効または無効にします。
 - c) [ファストリーブ (Fast Leave)] を選択または選択解除し、このポリシーを通してクエリが即時ドロップする IGMP V2 を有効または無効にします。
 - d) [クエリアの有効化 (Enable querier)] を選択して、このポリシーを通して IGMP クエリア アクティビティを有効または無効にします。

(注) このオプションを効果的に有効にするには、ポリシーを適用するブリッジドメインに割り当てられるサブネットで**[サブネット制御:クエリアIP]**設定も有効にする必要があります。この設定のプロパティ ページへのナビゲーションパスは次のとおりです。**[テナント (Tenants)]>[tenant_name]>[ネットワーク (Networking)]>[ブリッジドメイン (Bridge Dmains)]>[bridge_domain_name]>[サブネット (Subnets)]>[subnet_subnet]**

- e) [クエリアバージョン (Querier Version)]フィールドで、[バージョン2 (Version 2)]または[バージョン3 (Version 3)]を選択して、この特定のポリシーのIGMPスヌーピングクエリアバージョンを選択します。
- f) このポリシーの**[最後のメンバのクエリ間隔]**値を秒で指定します。
IGMPv2 リーブ レポートを受信したら、IGMPがこの値を使用します。これは、少なくとも1個以上のホストをグループに残すことを意味します。リーブ レポートを受信した後、インターフェイスがIGMPファストリーブに設定されていないか確認し、されていない場合はout-of-sequenceクエリを送信します。
- g) このポリシーの**[クエリ間隔]**値を秒で指定します。
この値は、グループ内でレポートを確認できない場合、IGMP機能が特定のIGMP状態を保存する合計時間を定義するために使用されます。
- h) このポリシーの**[クエリの応答間隔]**値を秒で指定します。
ホストがクエリ パケットを受信すると、最大応答所要時間以下のランダムな値でカウントが開始されます。このタイマーの期限が切れると、ホストはレポートで応答します。
- i) このポリシーの**[クエリ カウントの開始]**を指定します。
スタートアップクエリー インターバル中に送信される起動時のクエリー数。有効範囲は1～10です。デフォルトは2です。
- j) このポリシーの**[クエリ間隔の開始]**を秒で指定します。
デフォルトでは、ソフトウェアができるだけ迅速にグループ ステートを確立できるように、このインターバルはクエリー インターバルより短く設定されています。有効範囲は1～18,000秒です。デフォルト値は31秒です。

ステップ5 [送信 (Submit)]をクリックします。

新しいIGMPスヌープポリシーは、**[プロトコルポリシー - IGMPスヌープ]** サマリ ページに一覧になっています。

次のタスク

このポリシーを有効にするには、ブリッジドメインに割り当てます。

GUIを使用したIGMPスヌーピングポリシーのブリッジドメインへの割り当て

IGMPスヌーピングポリシーをブリッジドメインに割り当てると、そのブリッジドメインは、そのポリシーで指定されたIGMPスヌーピングポリシーを使用するように設定されます。

始める前に

- テナントのブリッジドメインを設定します。
- ブリッジドメインにアタッチするIGMPスヌーピングポリシーを設定します。



(注) 割り当てられるポリシーで **Enable Querier** オプションを効果的に有効にするには、ポリシーを適用するブリッジドメインに割り当てられるサブネットで **Subnet Control: Querier IP** 設定も有効にする必要があります。この設定があるプロパティ ページへのナビゲーションパスは、**Tenants > tenant_name > Networking > Bridge Domains > bridge_domain_name > Subnets > subnet_name** です。

- ステップ 1** テナントのブリッジドメインでIGMPスヌープポリシーを設定するには、APICの **Tenants** タブをクリックして、テナントの名前を選択します。
- ステップ 2** APICのナビゲーションウィンドウで **Networking > Bridge Domains** をクリックして、ポリシー指定のIGMPスヌープ設定を適用するブリッジドメインを選択します。
- ステップ 3** メインの **Policy** タブで、**IGMP Snoop Policy** フィールドまでスクロールして、ドロップダウンメニューから適切なIGMPポリシーを選択します。
- ステップ 4** **Submit** をクリックします。

ターゲットのブリッジドメインは、指定されたIGMPスヌーピングポリシーに関連付けられます。

IGMPスヌーピングの静的ポートグループの有効化

静的ポートグループのIGMPスヌーピングを有効にする

IGMP静的ポートのグループ化により以前アプリケーションEPGに静的に割り当てられた事前プロビジョニングを有効にして、スイッチポートがIGMPマルチキャストトラフィックを受信および処理できます。この事前プロビジョニングは、通常IGMPスヌーピングスタックがポートを動的に学習するときに発生する参加遅延を防止します。

静的グループメンバーシップは、アプリケーション EPG に割り当てられている静的ポートでのみ事前プロビジョニングできます。

APIC GUI、CLI、および REST API インターフェイスを通じて、静的グループメンバーシップを設定できます。

前提条件: 静的ポートに EPG を導入する

ポートで IGMP スヌープ処理を有効にするには、前提条件として、ターゲットのポートを、関連付けられている EPG に静的に割り当てる必要があります。

ポートの静的な導入は、APIC GUI、CLI、または REST API インターフェイスを通じて構成できます。詳細については、『Cisco APIC レイヤ2 ネットワーキング設定ガイド』の次のトピックを参照してください：

- GUI を使用して特定のノードまたはポートへ EPG を導入する
- NX-OS スタイルの CLI を使用した APIC の特定のポートへの EPG の導入
- REST API を使用した APIC の特定のポートへの EPG の導入

GUI を使用した、スタティックポートでの IGMP スヌーピングとマルチキャストの有効化

IGMP スヌーピングとマルチキャストは、EPG に静的に割り当てられているポートで有効にできます。その後、これらのポートで有効にされている IGMP スヌーピングとマルチキャストへのアクセスを許可または拒否されるユーザのアクセスグループを作成し、割り当てることができます。

始める前に

EPG の IGMP スヌーピングおよびマルチキャストを有効にする前に、次のタスクを実行します：

- この機能を有効にし、その EPG に静的に割り当てるインターフェイスを指定します。



(注) スタティックポートの割り当てに関する詳細は、『Cisco APIC レイヤ2 ネットワーキング設定ガイド』の「GUI を使用した特定のノードまたはポートで EPG を展開する」を参照してください。

- IGMP スヌーピングとマルチキャストトラフィックの受信者とする IP アドレスを指定します。

ステップ1 Tenant > *tenant_name* > Application Profiles > *application_name* > Application EPGs > *epg_name* > Static Ports をクリックします。

このスポットに移動すると、ターゲット EPG に静的に割り当てたすべてのポートが表示されます。

ステップ2 IGMP スヌーピングのグループ メンバーに静的に割り当てるポートをクリックします。
Static Path ページが表示されます。

ステップ3 IGMP スヌープ スタティック グループの表で、+ をクリックして、IGMP スヌープ アドレス グループにエントリを追加します。

IGMP スヌープ アドレス グループにエントリを追加すると、ターゲットの静的ポートが指定されたマルチキャスト IP アドレスに関連付けられ、そのアドレスで受信した IGMP スヌープ トラフィックを処理できるようになります。

- a) **Group Address** フィールドに、このインターフェイスとこの EPG に関連付けるマルチキャスト IP アドレスを入力します。
- b) 当てはまる場合には、**Source Address** フィールドに、マルチキャスト ストリームの送信元となる IP アドレスを入力します。
- c) **Submit** をクリックします。

設定が完了したら、ターゲットインターフェイスは、それに関連付けられているマルチキャスト IP アドレスに送信される IGMP スヌーピング プロトコル トラフィックを処理できるようになります。

(注) ターゲットのスタティック ポートにさらにマルチキャストアドレスを関連付けるには、この手順を繰り返します。

ステップ4 [送信 (Submit)] をクリックします。

IGMP スヌープ アクセス グループの有効化

IGMP スヌープ アクセス グループの有効化

「アクセス-グループ」ができるストリームを制御するために使用任意ポート背後に参加します。

実際に所属するするポートの設定を適用できることを確認するには、アプリケーション EPG に静的に割り当てられているインターフェイスでアクセス グループ設定を適用できる EPG。

ルート マップ ベースのアクセス グループのみが許可されます。

APIC GUI、CLI、および REST API インターフェイスを通じて、IGMP スヌープ アクセス グループを設定できます。

GUI を使用して、IGMP スヌーピングとマルチキャストへのグループアクセスを有効にする

EPG に静的に割り当てられたポートで IGMP スヌーピングとマルチキャストを有効にしたら、ユーザのアクセスグループを作成して割り当て、それらのポートで有効にされた IGMP スヌーピングとマルチキャストトラフィックへのアクセスを許可または拒否することができます。

始める前に

EPG に IGMP スヌーピングおよびマルチキャストへのアクセスを有効にする前に、この機能を有効にし、それらを静的に EPG に割り当てるインターフェイスを識別します。



(注) スタティックポートの割り当てに関する詳細は、『Cisco APIC レイヤ 2 ネットワーキング設定ガイド』の「GUI を使用した特定のノードまたはポートで EPG を展開する」を参照してください。

ステップ 1 [テナント (Tenant)] > [tenant_name] > [アプリケーション プロファイル (Application Profiles)] > [application_name] > [アプリケーション EPG (Application EPGs)] > [epg_name] > [スタティックポート (Static Ports)] をクリックします。

このスポットに移動すると、ターゲット EPG に静的に割り当てたすべてのポートが表示されます。

ステップ 2 マルチキャストグループアクセスを割り当てる予定のポートをクリックして、**Static Port Configuration** ページを表示します。

ステップ 3 [アクション (Actions)] > [IGMP アドレスグループの作成 (Create IGMP Access Group)] をクリックして、IGMP スヌープアクセスグループテーブルを表示します

ステップ 4 IGMP スヌープアクセスグループのテーブルで + をクリックして、アクセスグループのエントリを追加します。

IGMP スヌープアクセスグループのエントリを追加すると、このポートへのアクセス権を持つユーザグループを作成すること、それをマルチキャスト IP アドレスと関連付け、そのアドレスで受信された IGMP スヌープトラフィックへのグループアクセスを許可または拒否することができます。

- [マルチキャスト向けルートマップポリシーの作成 (Create Route Map Policy for Multicast)] を選択して、[マルチキャスト向けルートマップポリシーの作成 (Create Route Map Policy for Multicast)] ウィンドウを表示します。
- Name** フィールドで、マルチキャストトラフィックの許可または拒否の対象となるグループの名前を割り当てます。
- Route Maps** テーブルで、+ をクリックして、ルートマップダイアログを表示します。
- Order** フィールドでは、このインターフェイスに対して複数のアクセスグループを設定している場合に、このインターフェイスでのマルチキャストトラフィックへのアクセスをどの順序で許可または拒否するかを反映する番号を選択します。番号の小さいアクセスグループの方が、番号の大きいアクセスグループよりも前の順番になります。

- e) **Group IP** フィールドには、このアクセスグループに対してトラフィックが許可または阻止される、マルチキャスト IP アドレスを入力します。
- f) **Source IP** フィールドでは、当てはまる場合に、送信元の IP アドレスを入力します。
- g) **Action** フィールドでは、ターゲットグループのアクセスを拒否する場合には **Deny** を、ターゲットグループのアクセスを許可する場合には **Permit** を選択します。
- h) [OK] をクリックします。
- i) [送信 (Submit)] をクリックします。

設定が完了すると、設定されている IGMP のスヌープアクセスグループは、ターゲットの静的ポートと、そのアドレスで受信したマルチキャストストリームへの許可または拒否アクセスを通して、マルチキャスト IP アドレスに割り当てられます。

- (注)
- その他のアクセスグループを設定し、ターゲットの静的ポートを通してマルチキャスト IP アドレスに関連付けるには、この手順を繰り返します。
 - 構成されているアクセスグループの設定を確認するには、[テナント (Tenant)] > [tenant_name] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [マルチキャスト向けルートマップ (Route Maps for Multicast)] > [route_map_access_group_name] を選択します。

ステップ5 [送信 (Submit)] をクリックします。

GUI を使用して、IGMP スヌーピングとマルチキャストへのグループアクセスを有効にする



第 11 章

MLD スヌーピング

この章は、次の内容で構成されています。

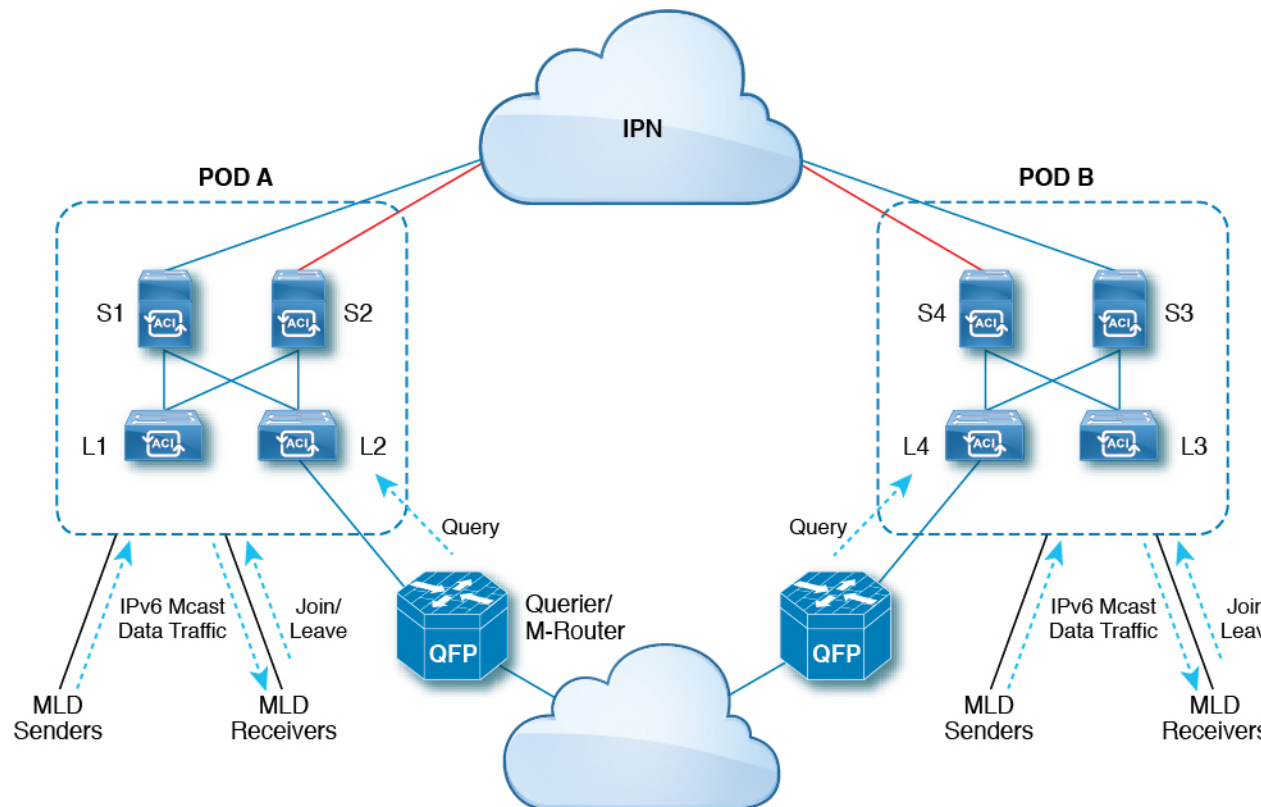
- [Cisco APIC および MLD スヌーピングについて \(63 ページ\)](#)
- [注意事項と制約事項 \(65 ページ\)](#)
- [GUIを使用したMLDスヌーピングポリシーの設定とブリッジドメインへの割り当て \(65 ページ\)](#)

Cisco APIC および MLD スヌーピングについて

マルチキャストリスナー検出 (MLD) スヌーピングにより、ホストとルータ間で IPv6 マルチキャストトラフィックを効率的に配信できます。これは、MLD クエリまたはレポートを送受信したポートのサブセットにブリッジドメイン内の IPv6 マルチキャストトラフィックを制限するレイヤ2機能です。このように、MLD スヌーピングは、マルチキャストトラフィックの受信に関心を示しているノードがないネットワークのセグメントでは帯域幅を節約できるという利点があります。これにより、ブリッジドメインでフラッドイングが生じることがなく、帯域幅の使用量が削減され、ホストとルータで不要なパケット処理を節約できます。

MLD スヌーピング機能は、IGMP スヌーピングと似ていますが、MLD スヌーピング機能は IPv6 マルチキャストトラフィックをスヌーピングし、MLDv1 (RFC 2710) および MLDv2 (RFC 3810) コントロールプレーンパケットで動作します。MLD は ICMPv6 のサブプロトコルであるため、MLD メッセージのタイプは ICMPv6 メッセージのサブセットであり、MLD メッセージは IPv6 パケット内で先頭の Next Header 値 58 により識別されます。MLDv1 のメッセージタイプには、リスナークエリ、マルチキャストアドレス固有 (MAS) クエリ、リスナーレポート、完了メッセージが含まれます。MLDv2 は、追加のクエリタイプであるマルチキャストアドレスおよびソース固有 (MASS) クエリを除き、MLDv1 と相互運用できるように設計されています。MLD で使用可能なプロトコルレベルタイマーは、IGMP で使用可能なものと同様です。

次の図に、MLD スヌーピング配置のさまざまなコンポーネントを示します。



次に、図のコンポーネントについて説明します。

- MLD 送信者（送信元）：IPv6 トラフィックをファブリックに送信するホスト。
- MLD レシーバ：IPv6 マルチキャストパケットの受信に関するホスト。セッションに参加するか、セッションから離脱するかを選択できます。
- クエリア/Mルータ：定期的クエリを送信し、グループメンバーシップデータベースを維持するルータまたはスイッチ。クエリアは定期的クエリを送信して、マルチキャストストリームへの参加に関心のあるユーザを特定します。Mルータ（マルチキャストルータ）は、ファブリック外の世界へのゲートウェイです。ファブリック内にマルチキャストデータトラフィックがある場合、そのストリームはマルチキャストルータを介してファブリックの外部に出ることができます。

MLD スヌーピングがディセーブルの場合、すべてのマルチキャストトラフィックは、関係があるかどうかに関係なく、すべてのポートにフラッドされます。MLD スヌーピングがイネーブルの場合、ファブリックは MLD インタレストに基づいて IPv6 マルチキャストトラフィックを転送します。不明な IPv6 マルチキャストトラフィックは、ブリッジドメインの IPv6 L3 不明マルチキャストフラッド設定に基づいてフラッドされます。

不明な IPv6 マルチキャストパケットを転送するには、次の 2 つのモードがあります。

- フラッドモード：ブリッジドメイン内のすべての EPG およびすべてのポートがフラッドパケットを受信します。

- OMF（最適化済みマルチキャストフラッディング）モード：マルチキャストルータポートのみがパケットを取得します。

注意事項と制約事項

MLD スヌーピング機能には、次のガイドラインと制約事項があります。

- MLD スヌーピングは、新世代 ToR スイッチでのみサポートされます。これらのスイッチモデルでは、スイッチ名の最後に「EX」、「FX」または「FX2」が付きます。
- ファブリック全体でスヌーピングされる最大 2000 の IPv6 マルチキャストグループのサポートが有効になります。
- ハードウェア転送は、MLDv2 の送信元固有のスヌープ エントリに対しても、（*、G）ルックアップで行われます。
- このリリースの MLD スヌーピングでは、次の機能はサポートされていません。
 - ブリッジドメインまたは VRF にわたる レイヤ3 マルチキャストルーティングは、IPv6 マルチキャストトラフィックではサポートされません。
 - スタティック MLD スヌーピング エントリ
 - ルートマップを介した MLD スヌープ エントリのアクセス フィルタ
 - VTEP（VL）の背後にある仮想エンドポイント

GUI を使用した MLD スヌーピング ポリシーの設定とブリッジドメインへの割り当て

MLD スヌーピング機能を実装するには、MLD スヌーピングポリシーを設定し、そのポリシーを1つまたは複数のブリッジドメインに割り当てます。

GUI を使用した MLD スヌーピング ポリシーの設定

MLD スヌーピング設定を1つまたは複数のブリッジドメインに割り当てることが可能な MLD スヌーピングポリシーを作成します。

-
- ステップ1 [テナント (Tenants)] タブと、MLD スヌーピングサポートを設定することを意図したブリッジドメインのテナントの名前をクリックします。
 - ステップ2 [ナビゲーション (Navigation)] ペインで、[ポリシー (Policies)] > [プロトコル (Protocol)] > [MLD スヌープ (MLD Snoop)] をクリックします。

ステップ3 [MLD スヌープ (MLD Snoop)] を右クリックし、[MLD スヌープ ポリシーの作成 (Create MLD Snoop Policy)] を選択します。

ステップ4 [MLD スヌープ ポリシーの作成 (Create MLD Snoop Policy)] ダイアログで、次のようにポリシーを設定します。

- a) [Name] フィールドと [Description] フィールドに、ポリシーの名前と説明をそれぞれ入力します。
- b) [管理状態 (Admin State)] フィールドで [有効化 (Enables)] または [無効化 (Disabled)] を選択して、このポリシー全体を有効または無効にします。
デフォルトでは、このフィールドは [無効化 (Disabled)] です。
- c) [コントロール (Control)] フィールドで [ファスト リーブ (Fast Leave)] を選択または選択解除し、このポリシーを通してクエリが即時ドロップする MLD v1 を有効または無効にします。
- d) [コントロール (Control)] フィールドで [クエリアの有効化 (Enable querier)] を選択または選択解除して、このポリシーを通して MLD クエリア アクティビティを有効または無効にします。

(注) このオプションを効果的に有効にするには、ポリシーを適用するブリッジドメインに割り当てられるサブネットに [サブネット制御: クエリア IP] 設定も有効にする必要があります。この設定のプロパティページへのナビゲーションパスは次のとおりです。[テナント (Tenants)] > [tenant_name] > [ネットワーク (Networking)] > [ブリッジドメイン (Bridge Dmains)] > [bridge_domain_name] > [サブネット (Subnets)] > [bd_subnet]

- e) このポリシーの [クエリ間隔] 値を秒で指定します。

クエリ間隔は、クエリアによって送信される全般的なクエリ間の間隔です。このフィールドのデフォルト値は 125 秒です。

- f) このポリシーの [クエリの応答間隔] 値を秒で指定します。

ホストがクエリ パケットを受信すると、最大応答所要時間以下のランダムな値でカウントが開始されます。このタイマーの期限が切れると、ホストはレポートを出して応答します。

これは、ホストが MLD クエリ メッセージに回答するまでの最大応答時間を制御するために使用されます。値を 10 秒未満に設定すると、ルータによる、グループのプルーンがより高速に行われるようになります。ただし、ホストの応答時間が短く制限されることになるため、ネットワークのバースト性が生じます。

- g) このポリシーの [最後のメンバのクエリ間隔] 値を秒で指定します。

MLDは、MLD Leave レポートを受信すると、この値を使用します。これは、少なくとも 1 個以上のホストをグループに残すことを意味します。リーブ レポートを受信した後、インターフェイスが IGMP ファスト リーブに設定されていないか確認し、されていない場合は out-of-sequence クエリを送信します。

このインターバル中に応答を受信されない場合、グループ ステータスは解除されます。この値を小さく設定すると、グループの最終メンバーまたは送信元が脱退したことを、より短時間で検出できます。有効範囲は 1 ~ 25 秒です。デフォルト値は 1 秒です。

- h) このポリシーの [クエリ カウントの開始 (Start Query Count)] の値を指定します。

スタートアップクエリインターバル中に送信される起動時のクエリー数。有効範囲は 1 ~ 10 です。デフォルトは 2 です。

- i) このポリシーの [クエリ間隔の開始] を秒で指定します。

デフォルトでは、ソフトウェアができるだけ迅速にグループ ステートを確立できるように、このインターバルはクエリーインターバルより短く設定されています。有効範囲は 1 ~ 18,000 秒です。デフォルト値は 31 秒です。

ステップ 5 [送信 (Submit)] をクリックします。

新しい MLD スヌープ ポリシーは、[プロトコル ポリシー - MLD スヌープ (Protocol Policies - MLD Snoop)] サマリー ページに表示されています。

次のタスク

このポリシーを有効にするには、ブリッジ ドメインに割り当てます。

GUI を使用した MLD スヌーピング ポリシーのブリッジ ドメインへの割り当て

MLD スヌーピング ポリシーをブリッジ ドメインに割り当てると、そのブリッジ ドメインは、そのポリシーで指定された MLD スヌーピング ポリシーを使用するように設定されます。

始める前に

- テナントのブリッジ ドメインを設定します。
- ブリッジ ドメインにアタッチする MLD スヌーピング ポリシーを設定します。



(注) 割り当てられるポリシーで **Enable Querier** オプションを効果的に有効にするには、ポリシーを適用するブリッジ ドメインに割り当てられるサブネットで **Subnet Control: Querier IP** 設定も有効にする必要があります。この設定のプロパティ ページへのナビゲーションパスは次のとおりです。 **Tenants > tenant_name > Networking > Bridge Dmains > bridge_domain_name > Subnets > bd_subnet**

ステップ 1 テナントのブリッジ ドメインで MLD スヌープ ポリシーを設定するには、APIC の [テナント (Tenants)] タブをクリックして、テナントの名前を選択します。

ステップ 2 APIC のナビゲーション ウィンドウで [ネットワーキング (Networking)] > [ブリッジ ドメイン (Bridge Domains)] をクリックして、ポリシー指定の MLD スヌープ設定を適用するブリッジ ドメインを選択します。

ステップ 3 メインの [ポリシー (Policy)] タブで、[MLD スヌープ ポリシー (MLD Snoop Policy)] フィールドまでスクロールして、ドロップダウン メニューから適切な MLD ポリシーを選択します。

ステップ 4 [送信 (Submit)] をクリックします。

ターゲットのブリッジ ドメインは、指定された MLD スヌーピング ポリシーに関連付けられます。

ステップ 5 ブリッジ ドメインのレイヤ 3 不明 IPv6 マルチキャスト宛先のノード転送パラメータを設定するには、次の手順を実行します。

- a) 設定したブリッジ ドメインを選択します。
- b) [ポリシー (Policy)] タブをクリックし、[全般 (General)] サブタブをクリックします。
- c) [IPv6 L3 不明なマルチキャスト (IPv6 L3 Unknown Multicast)] フィールドで、[フラッド (Flood)] または [最適化済みフラッド (Optimized Flood)] を選択します。

ステップ 6 スイッチ クエリア機能のリンクローカル IPv6 アドレスを変更するには、次の手順を実行します。

- a) 設定したブリッジ ドメインを選択します。
- b) [ポリシー (Policy)] タブをクリックして、[L3 コンフィギュレーション (L3 Configurations)] サブタブをクリックします。
- c) [リンクローカル IPv6 アドレス (Link-local IPv6 Address)] フィールドに、必要に応じてリンクローカル IPv6 アドレスを入力します。

ブリッジ ドメインのデフォルトのリンクローカル IPv6 アドレスは、内部的に生成されます。必要に応じて、このフィールドにブリッジ ドメインの別のリンクローカル IPv6 アドレスを設定します。



第 12 章

IP Multicast : IP マルチキャスト

この章は、次の内容で構成されています。

- [レイヤ 3 マルチキャスト \(70 ページ\)](#)
- [ファブリック インターフェイスについて \(73 ページ\)](#)
- [IPv4/IPv6 マルチキャスト ルーティングの有効化 \(74 ページ\)](#)
- [VRF GIPo の割り当て \(74 ページ\)](#)
- [指定フォワーダーとしての複数のボーダー リーフ スイッチ \(75 ページ\)](#)
- [PIM/PIM6 指定ルータの選定 \(76 ページ\)](#)
- [非境界リーフ スイッチの動作 \(77 ページ\)](#)
- [アクティブな境界リーフ スイッチ リスト \(77 ページ\)](#)
- [ブート時のオーバーロード動作 \(77 ページ\)](#)
- [ファーストホップ機能 \(78 ページ\)](#)
- [ラストホップ \(78 ページ\)](#)
- [高速コンバージェンス モード \(78 ページ\)](#)
- [ランデブー ポイントについて \(79 ページ\)](#)
- [Inter-VRF マルチキャストについて \(80 ページ\)](#)
- [ACI マルチキャスト機能のリスト \(81 ページ\)](#)
- [レイヤ 3 IPv4/IPv6 マルチキャストの設定のガイドライン、制約事項、および予想される動作 \(89 ページ\)](#)
- [GUI を使用したレイヤ 3 IPv4 マルチキャストの設定 \(92 ページ\)](#)
- [GUI を使用したレイヤ 3 IPv6 マルチキャストの設定 \(95 ページ\)](#)
- [BGP IPv4/IPv6 マルチキャスト アドレス ファミリーについて \(96 ページ\)](#)
- [マルチキャスト フィルタリングについて \(101 ページ\)](#)
- [SVI L3Out のレイヤ 3 マルチキャストについて \(108 ページ\)](#)

レイヤ3マルチキャスト



- (注) Cisco APIC リリース 4.2(1) 以前は、Cisco ACI はレイヤ3 マルチキャスト IPv4 をサポートしていました。Cisco APIC リリース 4.2(1) は、IPv6 マルチキャストを使用してマルチキャストアプリケーションを接続するためのサポートを追加します。IPv6 マルチキャストを使用すると、IPv6 マルチキャストアプリケーションは、Cisco ACI ファブリックの送信者から外部の受信者にマルチキャストを送信できます。

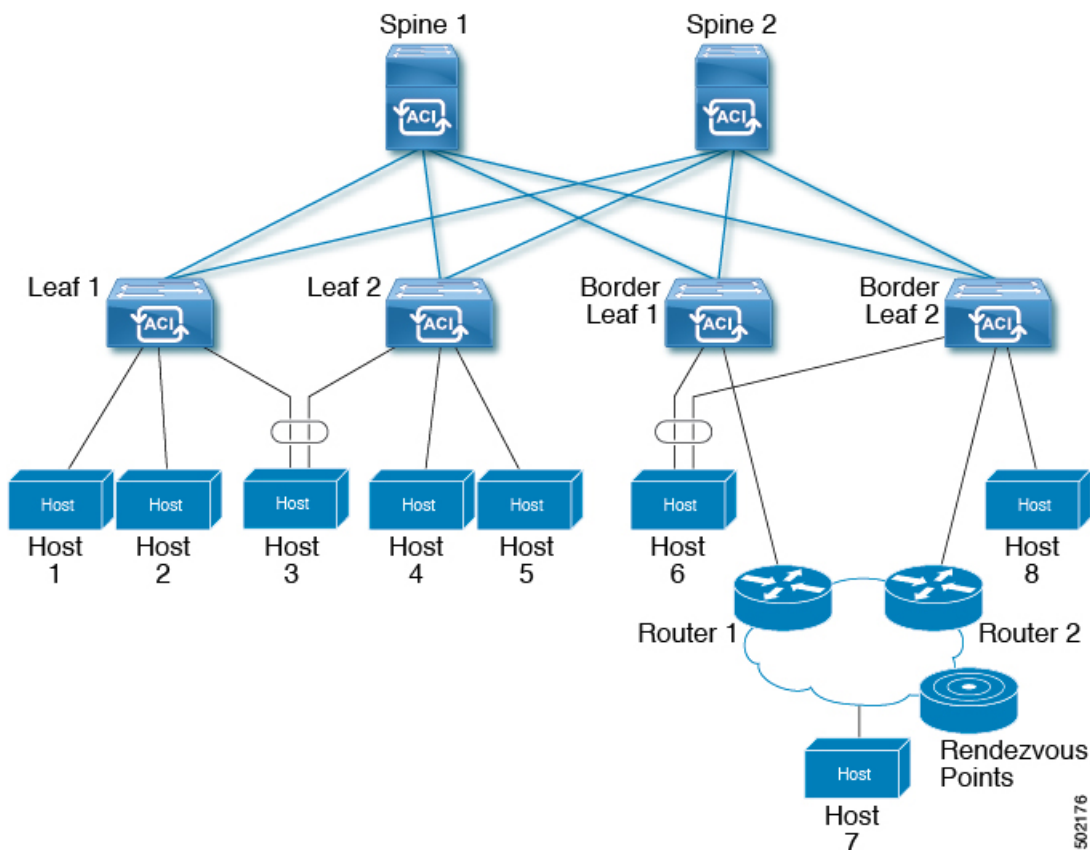
この章の情報は、レイヤ3 IPv6 マルチキャストの追加サポートを反映するように更新されました。

ACI ファブリックでは、ほとんどのユニキャストと IPv4/IPv6 マルチキャストルーティングが同じ境界リーフスイッチで稼働しており、ユニキャストルーティングプロトコル上でマルチキャストプロトコルが稼働しています。

このアーキテクチャでは、境界リーフスイッチのみが完全な Protocol Independent Multicast (PIM) または PIM6 プロトコルを実行します。非境界リーフスイッチは、インターフェイス上でパッシブモードの PIM/PIM6 を実行します。これらは、その他の PIM/PIM6 ルータとピアリングしません。境界リーフスイッチは、L3 Out を介してそれらの接続された他の PIM/PIM6 ルータとピアリングし、またそれら相互にもピアリングします。

次の図は、IPv4/IPv6 マルチキャストクラウド内のルータ1とルータ2に接続する境界リーフスイッチ1と境界リーフスイッチ2を示しています。IPv4/IPv6 マルチキャストルーティングを必要とするファブリック内の各 Virtual Routing and Forwarding (VRF) は、それぞれ別に外部マルチキャストルータとピアリングします。

図 7: マルチキャストクラウドの概要



リモートリーフスイッチでのレイヤ3マルチキャストのサポート

リリース 5.1(3) より以前では、ローカルリーフスイッチのシングルポッド、マルチポッド、およびマルチサイトトポロジでのレイヤ3マルチキャストルーティングがサポートされていました。リリース 5.1(3) 以降では、リモートリーフスイッチのレイヤ3マルチキャストルーティングもサポートされます。このサポートの一部として、リモートリーフスイッチは境界リーフスイッチまたは非境界リーフスイッチとして機能できます。

新しくサポートされたリモートリーフスイッチと以前にサポートされたローカルリーフスイッチには、レイヤ3マルチキャストルーティングまたはCiscoの実装に関して違いはありません。Cisco APIC/ACI マルチサイトオーケストレータのこの2つの主な違いは、トラフィックの転送方法に基づいています。

- 単一ファブリック内のローカルリーフスイッチ間のレイヤ3マルチキャストは、外部宛先IPアドレスがVRF GIPoマルチキャストアドレスであるVXLANマルチキャストパケットとして転送されます。
- リモートリーフスイッチとの間で送受信されるレイヤ3マルチキャストパケットは、VXLANユニキャストヘッドエンド複製パケットとしてカプセル化されます。

レイヤ3マルチキャストルーティングがVRFに対して有効になっている場合、VRF GIPo マルチキャストアドレスは、VRF が展開されているすべてのリーフスイッチでプログラムされます。レイヤ3マルチキャストパケットは、ポッド全体またはポッド間でマルチキャストパケットとして転送され、VRF が導入されているすべてのリーフスイッチで受信されます。リモートリーフスイッチの場合、レイヤ3マルチキャストパケットは、ヘッドエンド複製を使用して、VRF が導入されているすべてのリモートリーフスイッチに転送されます。このヘッドエンド複製は、マルチキャストソースが接続されているポッドまたはリモートリーフで行われます。たとえば、マルチキャスト送信元がローカルリーフスイッチに接続されている場合、これらのリモートリーフスイッチが他のポッドと関連付けられていても、そのポッド内のスパインスイッチの1つが選択され、VRF が導入されているすべてのリモートリーフスイッチにこれらのマルチキャストパケットが複製されます。レイヤ3マルチキャスト送信元がリモートリーフスイッチに接続されている場合、リモートリーフスイッチもヘッドエンド複製を使用して、マルチキャストパケットのコピーをすべてのポッドのスパイン、およびVRF が導入されているその他すべてのリモートリーフスイッチへ送信します。

ヘッドエンド複製を使用したマルチキャスト転送は、マルチキャストパケットをすべてのヘッドエンド複製トンネルの個別のユニキャストパケットとして複製します。リモートリーフスイッチ設計のレイヤ3マルチキャストでは、リモートリーフスイッチが接続されているIPネットワーク (IPN) に、マルチキャストトラフィック要件をサポートするのに十分な帯域幅があることを確認する必要があります。

リモートリーフスイッチは、PIM が有効または無効の L3Out 接続をサポートします。PIM 対応 L3Out を持つ VRF 内のすべてのリーフスイッチは、外部ソースおよびランデブーポイントに向けてファブリックから PIMJoin を送信できます。ファブリックに接続されたマルチキャストレシーバがグループの IGMP 加入を送信すると、ファブリックは PIM 対応境界リーフスイッチの1つを選択して加入を送信します (ストライプ勝者 (stripe winner) として)。グループのレシーバがメインポッドのローカルリーフスイッチに接続されている場合でも、PIM 対応 L3Out を備えたリモートリーフスイッチをグループのストライプ勝者として選択できます。レイヤ3マルチキャストトラフィックの準最適な転送の可能性があるため、リモートリーフスイッチに PIM 対応 L3Out を導入することは推奨されません。

注意事項と制約事項

- ポッドの冗長性は、リモートリーフスイッチによるレイヤ3マルチキャスト転送でサポートされます。リモートリーフスイッチが関連付けられているポッド内のすべてのスパインスイッチに障害が発生した場合、リモートリーフスイッチは別のポッド内のスパインスイッチへのコントロールプレーン接続を確立できます。
- リモートリーフスイッチは、ポッド内の少なくとも1つのスパインスイッチに接続する必要があります。リモートリーフスイッチがすべてのスパインスイッチへの接続を失った場合、レイヤ3マルチキャストトラフィックは転送されません。これには、同じリーフスイッチ上の送信者と受信者間のレイヤ3マルチキャストトラフィックが含まれます。

ファブリック インターフェイスについて

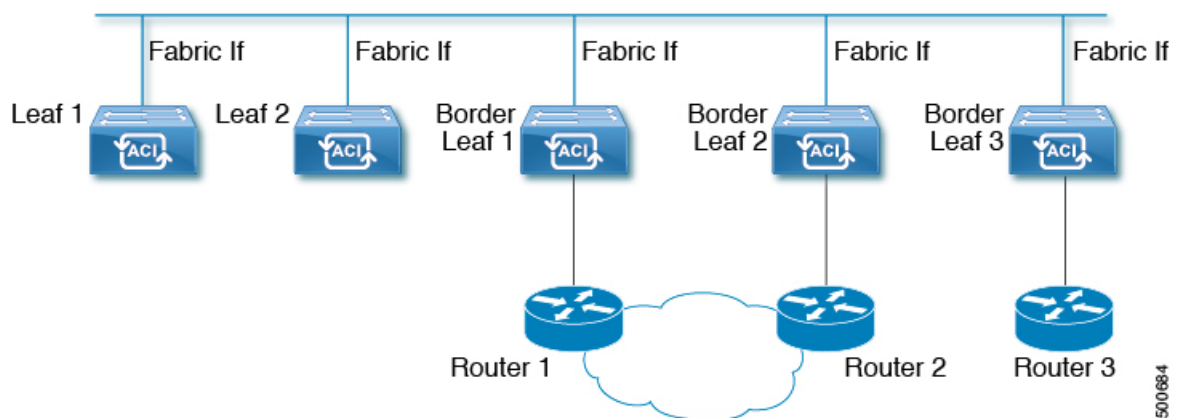
ファブリック インターフェイスはソフトウェアモジュール間の仮想インターフェイスであり、IPv4/IPv6 マルチキャスト ルーティングのファブリックを表します。インターフェイスは、宛先が VRF GIPo（グループ IP 外部アドレス）であるトンネルインターフェイスの形式を取ります。² PIM6 は、PIM4 が使用するものと同じトンネルを共有します。たとえば、境界リーフがグループのトラフィックの転送を担当する指定フォワーダの場合、ファブリック インターフェイスはグループの発信インターフェイス (OIF) となります。ハードウェアのインターフェイスに相当するものではありません。ファブリック インターフェイスの動作状態は、intermediate system-to-intermediate system (IS-IS) によって公開される状態に従ったものとなります。



- (注) マルチキャスト対応の各 VRF には、ループバック インターフェイスで構成された 1 つ以上の境界リーフ スイッチが必要です。PIM 対応の L3Out のすべてのノードで、一意の IPv4 ループバックアドレスを設定する必要があります。Router-ID ループバックまたは別の一意のループバック アドレスを使用できます。

ユニキャストルーティング用に設定された任意のループバックは再利用できます。このループバックアドレスは、外部ネットワークからルーティングする必要があり、VRF のファブリック MP-BGP (マルチプロトコル境界ゲートウェイ プロトコル) ルートに挿入されます。ファブリック インターフェイスの送信元 IP は、このループバックに、ループバック インターフェイスとして設定されます。次の図は、IPv4/IPv6 マルチキャストルーティング用のファブリックを示しています。

図 8: IPv4/IPv6 マルチキャストルーティング用のファブリック



500884

² GIPo (グループ IP 外部アドレス) とは、ファブリック内で転送されたすべてのマルチデスティネーション パケット (ブロードキャスト、未知のユニキャストおよびマルチキャスト) で、VXLAN パケットの外部 IP ヘッダーで使用される宛先マルチキャスト IP アドレスです。

IPv4/IPv6 マルチキャストルーティングの有効化

ファブリックで IPv4 または IPv6 マルチキャストルーティングを有効または無効にするプロセスは、次の3つのレベルで実行されます。Cisco ACI

- VRF レベル：VRF レベルでマルチキャストルーティングを有効にします。
- L3Out レベル：VRF で設定された1つ以上の L3Out に対して PIM/PIM6 を有効にします。
- ブリッジドメイン レベル：マルチキャストルーティングが必要な1つ以上のブリッジドメインに対して PIM/PIM6 を有効にします。

トップレベルでは、IPv4/IPv6 マルチキャストルーティングは、任意のマルチキャストルーティングが有効なブリッジドメインを持つ VRF で有効にする必要があります。IPv4/IPv6 マルチキャストルーティングが有効な VRF では、IPv4/IPv6 マルチキャストルーティングが有効なブリッジドメインおよび IPv4/IPv6 マルチキャストルーティングが無効なブリッジドメインの組み合わせにすることができます。IPv4 / IPv6 マルチキャストルーティングが無効になっているブリッジドメインは、VRF IPv4 / IPv6 マルチキャストパネルに表示されません。IPv4/IPv6 マルチキャストルーティングが有効な L3Out はパネル上でも表示されますが、IPv4/IPv6 マルチキャストルーティングが有効なブリッジドメインは常に IPv4/IPv6 マルチキャストルーティングが有効な VRF の一部になります。

Cisco Nexus 93128TX、9396PX、9396TX などのリーフスイッチでは、IPv4/IPv6 マルチキャストルーティングはサポートされていません。すべての IPv4/IPv6 マルチキャストルーティングと IPv4/IPv6 マルチキャストが有効な VRF は、製品 ID に -EX および -FX という名前を持つスイッチでのみ展開される必要があります。



(注) レイヤ3アウトポートとサブインターフェイスはサポートされません。外部 SVI のサポートは、リリースによって異なります。

- リリース 5.2(3) より前のリリースでは、外部 SVI はサポートされていません。リリース 5.2(3) より前のリリースでは、外部 SVI がサポートされていないため、PIM/PIM6 を L3-VPC で有効にできません。
- リリース 5.2(3) 以降では、SVI L3Out のレイヤ3 マルチキャストがサポートされます。PIM は、物理ポートおよびポートチャネルの SVI L3Out でサポートされますが、VPC ではサポートされません。

VRF GIPo の割り当て

VRF GIPo は、構成に基づいて暗黙的に割り当てられます。VRF に対して1つの GIPo が、そしてその VRF の下の各 BD に対して1つの GIPo があります。さらに、任意の GIPo は、複数の BD または複数の VRF の間で共有される可能性があります。しかし、VRF と BD の組み合わせ

せで共有されることはありません。APICは、この点を確認する必要があります。すでに処理され、VRF GIPo ツリーが構築された BD GIPoに加えて VRF GIPo を処理する場合には、IS-IS が変更されます。



(注) 同じ VRF の場合、VRF GIPo は IPv4 と IPv6 の両方に共通です。

PIM/PIM6 が有効な BD のすべてのマルチキャストトラフィックは、VRF GIPo を使用して、ファブリックに転送されます。これには、レイヤ2 およびレイヤ3 IPv4/IPv6 マルチキャストの両方が含まれます。マルチキャストが有効な BD 上のブロードキャストまたはユニキャストフラッドトラフィックは、引き続き BD GIPo を使用します。非 IPv4/IPv6 マルチキャストが有効な BD は、すべてのマルチキャスト、ブロードキャスト、およびユニキャストフラッドトラフィックで BD GIPo を使用します。

APIC GUI は、すべての BD と VRF で GIPo マルチキャストアドレスを表示します。表示されるアドレスは常に、/28 ネットワークアドレスとなります（最後の4ビットは0）。VXLAN パケットがファブリックで送信されると、宛先マルチキャスト GIPo アドレスは、この /28 ブロック内のアドレスとなり、16FTAG ツリーのいずれかを選択するために使用されます。これにより、ファブリック全体のマルチキャストトラフィックをロードバランシングします。

表 5: GIPo の使用方法

トラフィック	非 MC ルーティングが有効な BD	MC ルーティングが有効な BD
ブロードキャスト	BD GIPo	BD GIPo
不明なユニキャストフラディング	BD GIPo	BD GIPo
マルチキャスト	BD GIPo	VRF GIPo

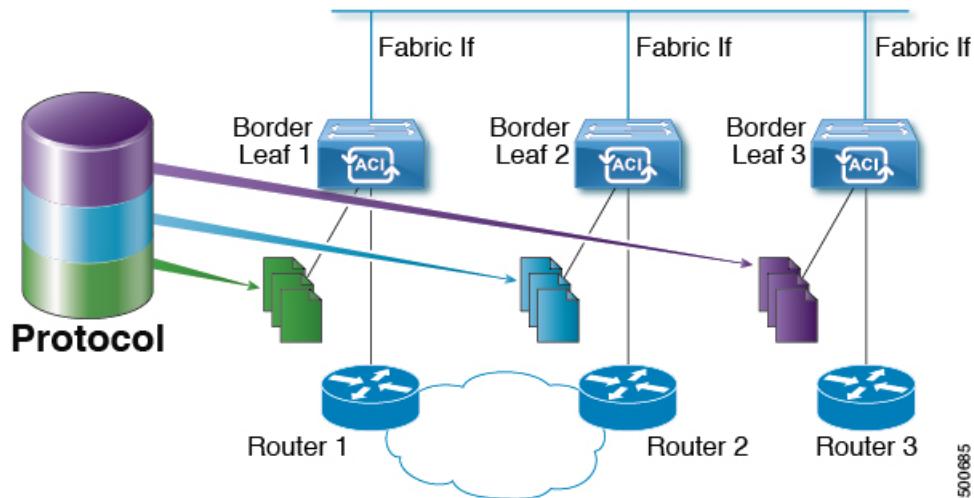
指定フォワーダーとしての複数のボーダーリーフスイッチ

ファブリック内に、IPv4/IPv6 マルチキャストルーティングを行う複数の境界スイッチ (BL) がある場合、境界リーフのうち1台だけが、外部 IPv4/IPv6 マルチキャストネットワークからのトラフィックを集めてファブリックに転送する、指定されたフォワーダーとして選択されます。これによってトラフィックの複数のコピーが発生することを防ぎ、複数の BL スイッチの間でバランスが取れるようにします。

このことは利用可能な BL スイッチにわたる、これはグループアドレスと VRF ネットワーク ID (VNID) としてのグループの所有権を、ストライピングすることによって行われます。グループの責任を担う BL は、外部ネットワークへの PIM/PIM6 の参加を送信して、ファブリックのレシーバの代わりにファブリックへのトラフィックを集めます。

ファブリックの各 BL は、その VRF の他のすべてのアクティブな BL スイッチのビューを持ちます。それでそれぞれの BL スイッチは、独立に矛盾なく、グループのストライピングを行えます。各 BL は、アクティブな BL スイッチのリストを取得するために、ファブリック インターフェイス上の PIM/PIM6 ネイバーの関係をモニターします。BL スイッチが削除または検出されたときには、その時点でのアクティブな BL スイッチ間で、グループの再ストライピングが行われます。ストライピングは、マルチポッド環境で GIPos を外部リンクにハッシュするために用いられる方法に似ています。それで、グループから BL へのマッピングは持続性があり、アップ時やダウン時の変化が少なくてすみます。

図 9: 指定されたフォワーダとしての複数の境界リーフのモデル



PIM/PIM6 指定ルータの選定

ACI ファブリックのレイヤ 3 IPv4/IPv6 マルチキャストでは、異なるインターフェイス タイプの PIM/PIM6 DR (代表ルータ) メカニズムは次の通りです。

- PIM/PIM6 が有効な L3 Out インターフェイス：これらのインターフェイス タイプの標準の PIM/PIM6 DR メカニズムに従います。
- [ファブリック インターフェイス]：このインターフェイスの DR 選定は、ストライピングにより決定される DR 機能ほど重要ではありません。PIM/PIM6 DR の選定は、引き続きこのインターフェイスに残ります。
- IPv4/IPv6 マルチキャストルーティングが有効なパーベイスブ BD：ファブリックのパーベイスブ BD はすべて、IPv4/IPv6 マルチキャストルーティングに関するスタブです。そのため、すべてのリーフスイッチで、vPC を含む普及 BD の SVI インターフェイスがセグメントの DR と見なされます。

非境界リーフスイッチの動作

非境界リーフスイッチ上のPIM/PIM6は、ファブリック インターフェイスとパーベイシブ BD SVIでは、パッシブモードで動作します。PIM/PIM6は新しいパッシブプローブモードになっており、*hellos* だけを送信します。これらのパーベイシブ BD SVIでは、PIM/PIM6 ネイバーは想定されていません。PIM/PIM6 がパーベイシブ BD から *hello* を受信した場合には、障害が発生するのが望ましい動作です。非境界リーフ スイッチ上の PIM/PIM6 は、パーベイシブ BD 上の *hellos* と、ファブリック インターフェイス上のソース登録パケットを除き、PIM/PIM6 プロトコルパケットを送信しません。

同時に、PIM/PIM6 はファブリック インターフェイス上の次の PIM/PIM6 パケットを受信して処理します:

- **PIM/PIM6 Hellos:** これはファブリック インターフェイス上でアクティブな BL リストを追跡するために使用されます。パーベイシブ BD 上では、フォールトを発生するために使用されます。
- **PIM BSR、Auto-RP アドバタイズメント:** PIM でのみサポートされ、PIM6 ではサポートされません。これはファブリック インターフェイスで受信され、RP からグループ範囲へのマッピングを収集するために処理されます。

アクティブな境界リーフスイッチ リスト

すべてのリーフ スイッチで、PIM/PIM6 はストライピングとその他の目的に使用されるアクティブな境界リーフ スイッチのリストを保持しています。境界リーフ スイッチ自体で、このアクティブな境界リーフ リストはアクティブな PIM/PIM6 のネイバー関係から導出されます。非境界リーフ スイッチで、リストファブリック インターフェイス上のモニター対象の PIM/PIM6 *Hello* メッセージを使用して PIM/PIM6 によりリストが生成されます。*Hello* メッセージの送信元 IP は、各境界リーフ スイッチに割り当てられた IPv4/IPv6 ループバック IP です。

ブート時のオーバーロード動作

境界リーフ スイッチが起動後、または接続を失った後に初めてファブリックへの接続を得たとき、境界リーフ スイッチが **COOP** リポジトリ情報を受信する機会を得るまでは、境界リーフ スイッチがアクティブな境界リーフ スイッチ リストの一部になることは望ましくありません。すべての IPv4/IPv6 マルチキャスト グループ メンバーシップ情報は、スパイン上の COOP データベースに保管されます。³境界リーフ スイッチがアクティブな境界リーフ スイッチのリストに加えられるのは望ましいことではありません。これは、PIM/PIM6 の *hello* メッセージの伝送を、設定されていない期間だけ遅らせることで実現できます。

³ 境界リーフはブート時にスパインからこの情報を取得します。

ファーストホップ機能

リーフスイッチへの直接接続は、PIM/PIM6 sparse モードに必要なファーストホップ機能进行处理します。

ラストホップ

ラストホップルータは受信側に接続されるもので、PIM/PIM6 の any-source マルチキャスト (ASM) が発生した場合、最短パスツリー (SPT) スイッチオーバーを実行する責任を負います。境界リーフスイッチはこの機能进行处理します。境界非リーフスイッチはこの機能には参加しません。

高速コンバージェンスモード

ファブリックはすべての境界リーフスイッチがルートへの接続性の外部で設定可能な高速コンバージェンスモードをサポートしています (の $RP(*, G)$ の送信元と (S, G))、外部ネットワークからのトラフィックを停止します。重複を防ぐためには、1人だけ、BL スイッチ転送トラフィック、ファブリックにします。ファブリックに、グループのトラフィックを転送する BL グループの代表フォワーダ (DF) と呼びます。グループのストライプ受賞は、DF を決定します。ストライプ受賞にルートへの到達可能性がある場合は、ストライプ受賞も DF です。ストライプで優先されるデータが、ルートへの外部接続を持たない場合、その BL は、ファブリック インターフェイス経由で PIM/PIM6 join を送信することによって、DF を選択します。外部からルートに到達可能なすべての非ストライプ優先 BL スイッチは PIM/PIM6 join を送信してトラフィックを引きこみませんが、ルート向けの RPF インターフェイスとしてファブリック インターフェイスを保持します。これは、結果、トラフィックをドロップされたが、外部のリンク上で BL スイッチに到達します。

高速コンバージェンスモードの利点はプログラミング右のリバースパス フォワーディング (RPF) インターフェイスの新しいストライプ受賞 BL スイッチのみに必要なアクションになどの損失のためのストライプ所有者変更がある場合にです。新しいストライプ優先から PIM/PIM6 ツリーに参加することによって発生する遅延はありません。これは、非ストライプ受賞の外部リンクで追加帯域幅の使用増やしますが機能します。



(注) 追加の帯域幅のコストが保存コンバージェンス時間を上回る導入では、高速コンバージェンスモードを無効にできます。

ランデブーポイントについて

ランデブーポイント（RP）は、IPv4/IPv6 マルチキャストネットワークドメイン内にあるユーザーが選択した IP アドレスで、IPv4/IPv6 マルチキャスト共有ツリーの共有ルートとして動作します。必要に応じて複数の RP を設定し、さまざまなグループ範囲をカバーすることができます。複数の RP を設定する場合は、各 RP を一意のグループ範囲に設定する必要があります。

マルチキャストルーティングが有効になっている VRF には、PIM 対応境界リーフスイッチが必要です。PIM は、L3Out レベルで PIM を有効にすることで、境界リーフスイッチに対して有効になります。L3Out に対して PIM を有効にすると、その L3Out で設定されているすべてのノードとインターフェイスに対して PIM が有効になります。

ACI は、次の RP 設定をサポートしています。

- **外部 RP** : RP は ACI ファブリックの外部にあります。
 - **スタティック RP** : IPv4/IPv6 マルチキャストグループ範囲の RP を静的に設定できます。この場合、ドメイン内のすべてのルータに RP のアドレスを設定する必要があります。
 - **Auto-RP** : ACI 境界リーフが Auto-RP フォワーダ、Auto-RP リスナーとして機能し、Auto-RP マッピングエージェントルートマップを適用できるようにします。
 - **BSR** : ACI 境界リーフを BSR フォワーダ、BSR リスナーとして機能させ、BSR メッセージをフィルタリングするためにルートマップを適用します。
- **ファブリック RP** : IPv4 マルチキャストにのみ適用されます。ファブリック RP は IPv6 マルチキャストではサポートされません。VRF 内のすべての PIM 対応ボーダーリーフスイッチで、PIM エニーキャスト RP ループバックインターフェイスをイネーブルにします。ファブリック RP 設定には、PIM 対応の L3Out（ループバックインターフェイスあり）が必要です。設定すると、外部ルータはファブリック RP を使用できます。Auto-RP および BSR はファブリック RP ではサポートされません。外部エニーキャスト RP メンバーとのファブリック RP ピアリングはサポートされていません。



(注) ファブリック RP には、次の制限があります。

- ファブリック RP は高速コンバージェンスモードをサポートしていません。
- ファブリック IP :
 - スタティック RP とファブリック RP 内のすべてのスタティック RP エントリで一意でなければなりません。
 - レイヤ 3 out ルータ ID のいずれかにすることはできません。

RP の設定については、次のセクションを参照してください。

- GUI を使用したレイヤ 3 IPv4 マルチキャストの設定 (92 ページ)
- NX-OS スタイルの CLI を使用したレイヤ 3 マルチキャストの設定 (482 ページ)
- REST API を使用したレイヤ 3 マルチキャストの設定 (563 ページ)

Inter-VRF マルチキャストについて



(注) Inter-VRF マルチキャストは、IPv6 マルチキャストではサポートされません。

マルチキャストネットワークを持つ一般的なデータセンターでは、マルチキャストのソースおよびレシーバは同じ VRF にあり、すべてのマルチキャストトラフィックはその VRF 内で転送されます。マルチキャストのソースとレシーバが異なる VRF に存在する使用例があります。

- 監視カメラは1つの VRF 内にありますが、カメラフィールドは異なる VRF 内のコンピュータで閲覧します。
- マルチキャスト コンテンツ プロバイダーは1つの VRF 内にありますが、組織のさまざまな部門は、異なる VRF でマルチキャスト コンテンツを受信します。

ACI リリース 4.0 は、送信元と受信側が異なる VRF 内にあることを可能にする inter-VRF マルチキャストのサポートを追加します。これにより受信側の VRF は、送信元 VRF のマルチキャストルートに対して、リバースパス フォワーディング (RPF) ルックアップを実行できるようになります。送信元 VRF で有効な RPF インターフェイスが形成されると、受信側の VRF で発信インターフェイス (OIF) が有効になります。すべての inter-VRF マルチキャストトラフィックは、送信元 VRF のファブリック内で転送されます。inter-VRF 転送と変換は、受信側が接続されているリーフスイッチで実行されます。



- (注)
- Any-source マルチキャストでは、使用される RP は送信元と同じ VRF 内にある必要があります。
 - Inter-VRF マルチキャストは、共有サービスと共有 L3Out 構成の両方をサポートします。ソースとレシーバは、異なる VRF の EPG または L3Out に接続できます。

ACI の場合、inter-VRF マルチキャストは受信側の VRF ごとに設定されます。受信側 VRF を持つすべての NBL/BL は、同じ inter-VRF 設定となります。直接接続されたレシーバを持つ各 NBL、および外部レシーバを持つ BL では、送信元 VRF が展開されている必要があります。コントロールプレーンのシグナリングとデータプレーンの転送は、レシーバを持つ NBL/BL 内の VRF 間で必要な変換と転送を行います。ファブリックで転送されるすべてのパケットは、送信元 VRF 内にあります。

Inter-VRF マルチキャストの要件

このセクションでは、Inter-VRF マルチキャストの要件について示します。

- 特定のグループのすべての送信元は、同じ VRF（送信元 VRF）でなければなりません。
- 送信元 VRF と送信元 EPG は、受信側 VRF があるすべてのリーフ上に存在する必要があります。
- ASM の場合：
 - RP は送信元（送信元 VRF）と同じ VRF 内になければなりません。
 - リリース 4.2(4) 以前で、送信元 VRF は、ファブリック RP を使用する必要があります。この制限は、リリース 4.2(4) 以降には適用されません。
 - 特定のグループ範囲の送信元およびすべての受信側 VRF で、同じ RP アドレス設定を適用する必要があります。

ACI マルチキャスト機能のリスト

ここでは、ACI マルチキャスト機能のリストと、類似の NX-OS 機能との比較を示します。

- [IGMP 機能 \(81 ページ\)](#)
- [IGMP スヌーピング機能 \(83 ページ\)](#)
- [MLD スヌーピング機能 \(84 ページ\)](#)
- [PIM 機能 \(インターフェイス レベル\) \(85 ページ\)](#)
- [PIM 機能 \(VRF レベル\) \(87 ページ\)](#)

IGMP 機能

ACI 機能名	NX-OS 機能	説明
V3 ASM を許可	ip igmp allow-v3-asm	SSM 範囲外のマルチキャスト グループの IGMP バージョン 3 送信元固有レポートの受け入れを許可します。この機能がイネーブルの場合、グループが設定された SSM 範囲外であっても、グループと送信元の両方を含む IGMP バージョン 3 レポートを受信すると、スイッチは (S, G) mroute エントリを作成します。ホストが SSM 範囲外の (*, G) レポートを送信する場合、または SSM 範囲の (S, G) レポートを送信する場合、この機能は不要です。

ACI 機能名	NX-OS 機能	説明
Fast Leave	ip igmp immediate-leave	デバイスからグループ固有のクエリーが送信されないため、所定の IGMP インターフェイスで IGMPv2 グループ メンバーシップの脱退のための待ち時間を最小限にできるオプション。即時脱退をイネーブルにすると、デバイスではグループに関する Leave メッセージの受信後、ただちにマルチキャストルーティングテーブルからグループ エントリが削除されます。デフォルトではディセーブルになっています。 注意：このコマンドは、所定のグループに対する BD/インターフェイスの背後に 1 つの受信者しか存在しない場合に使用します。
レポートリンクローカルグループ	ip igmp report-link-local-groups	224.0.0.0/24に含まれるグループに対して、レポート送信をイネーブルにします。非リンク ローカル グループには、常にレポートが送信されます。デフォルトでは、リンク ローカル グループにレポートは送信されません。
グループタイムアウト (秒)	ip igmp group-timeout	IGMPv2 のグループメンバーシップタイムアウトを設定します。有効範囲は 3 ~ 65,535 秒です。デフォルト値は 260 秒です。
クエリー間隔(秒)	ip igmp query-interval	IGMP ホストクエリーメッセージの送信頻度を設定します。有効範囲は 1 ~ 18,000 秒です。デフォルト値は 125 秒です。
クエリー応答間隔(秒)	ip igmp query-max-response-time	IGMP クエリーでアドバタイズされる応答時間を設定します。有効範囲は 1 ~ 25 秒です。デフォルトは 10 秒です。
最終メンバーカウント	ip igmp last-member-query-count	ホストの Leave メッセージを受信してから、IGMP クエリーが送信される回数を設定します。有効範囲は 1 ~ 5 です。デフォルトは 2 です。
最終メンバー応答時間 (秒)	ip igmp last-member-query-response-time	メンバーシップ レポートを送信してから、ソフトウェアがグループ ステートを解除するまでのクエリーインターバルを設定します。有効範囲は 1 ~ 25 秒です。デフォルト値は 1 秒です。
スタートアップクエリーの回数	ip igmp startup-query-count	ソフトウェアの起動時に使用されるクエリー数を設定します。有効範囲は 1 ~ 10 です。デフォルトは 2 です。
クエリアタイムアウト	ip igmp querier-timeout	クエリアとして処理を引き継ぐかどうかをソフトウェアが判断するための、クエリータイムアウト値を設定します。有効範囲は 1 ~ 65,535 秒です。デフォルト値は 255 秒です。
堅牢性変数	ip igmp robustness-variable	ロバストネス変数を設定します。ネットワークのパケット損失が多い場合は、この値を大きくします。有効値の範囲は、1~7です。デフォルトは 2 です。
バージョン	ip igmp version <2-3>	ブリッジドメインまたはインターフェイスでイネーブルにする IGMP のバージョン。有効な IGMP バージョンは 2 または 3 です。デフォルトは 2 です。

ACI 機能名	NX-OS 機能	説明
レポートポリシー ルート マップ*	ip igmp report-policy <route-map>	ルートマップポリシーに基づく、IGMP レポートのアクセスポリシー。 IGMP グループレポートは、ルートマップで許可されたグループに対してのみ選択されます
静的レポートルート マップ*	ip igmp static-oif	マルチキャスト グループを発信インターフェイスに静的にバインドし、スイッチハードウェアで処理します。グループアドレスのみを指定した場合は、(*, G) ステートが作成されます。送信元アドレスを指定した場合は、(S, G) ステートが作成されます。グループプレフィックス、グループ範囲、および送信元プレフィックスを示すルートマップポリシー名を指定できます。IGMPv3 をイネーブルにした場合にのみ、(S, G) ステートに対して送信元ツリーが作成されることに注意してください。
最大マルチキャストエ ントリ	ip igmp state-limit	IGMP レポートによって作成される BD またはインターフェイスの mroute 状態を制限します。 デフォルトは無効で、制限はありません。有効な範囲は1～4294967295です。
予約済みマルチキャスト エントリ	ip igmp state-limit <limit> reserved <route-map>	予約ポリシーにルート マップ ポリシー名を使用するように指定し、インターフェイスで許可される (*, G) および (S, G) エントリの最大数を設定します。
ステート制限ルート マップ*	ip igmp state-limit <limit> reserved <route-map>	予約済みマルチキャスト エントリ機能で使用

IGMP スヌーピング機能

ACI 機能名	NX-OS 機能	説明
IGMP スヌーピングの 管理状態	[no] ipigmp snooping	IGMP スヌーピング機能を有効または無効にします。PIM 対応ブリッジドメインでは無効にできません
Fast Leave	ip igmp snooping fast-leave	デバイスからグループ固有のクエリーが送信されないため、所定の IGMP インターフェイスで IGMPv2 グループ メンバーシップの脱退のための待ち時間を最小限にできるオプション。即時脱退をイネーブルにすると、デバイスではグループに関する Leave メッセージの受信後、ただちにマルチキャストルーティングテーブルからグループ エントリが削除されます。デフォルトではディセーブルになっています。 注意：このコマンドは、所定のグループに対する BD/インターフェイスの背後に1つの受信者しか存在しない場合に使用します。

ACI 機能名	NX-OS 機能	説明
クエリアの有効化	ip igmp snooping querier <ip address>	ブリッジドメインで IP IGMP スヌーピング クエリア機能をイネーブルにします。BD サブネット クエリア IP 設定とともに使用して、ブリッジドメインの IGMP スヌーピング クエリアを設定します。 注意：PIM 対応ブリッジドメインでは使用しないでください。ブリッジドメインで PIM が有効になっている場合、IGMP クエリア機能は自動的に有効になります。
クエリ間隔	ip igmp snooping query-interval	IGMP ホストクエリーメッセージの送信頻度を設定します。有効範囲は 1 ~ 18,000 秒です。デフォルト値は 125 秒です。
クエリ応答間隔	ip igmp snooping query-max-response-time	IGMP クエリーでアドバタイズされる応答時間を設定します。有効範囲は 1 ~ 25 秒です。デフォルトは 10 秒です。
最終メンバークエリ間隔	ip igmp snooping last-member-query-interval	メンバーシップ レポートを送信してから、ソフトウェアがグループステートを解除するまでのクエリーインターバルを設定します。有効範囲は 1 ~ 25 秒です。デフォルト値は 1 秒です。
開始クエリ数	ip igmp snooping startup-query-count	マルチキャストトラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、起動時に送信されるクエリー数に対してスヌーピングを設定します。有効範囲は 1 ~ 10 です。デフォルトは 2 です。
開始クエリ間隔 (秒)	ip igmp snooping startup-query-interval	マルチキャストトラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、起動時のスヌーピングクエリーインターバルを設定します。有効範囲は 1 ~ 18,000 秒です。デフォルト値は 31 秒です。

MLD スヌーピング機能

ACI 機能名	NX-OS 機能	説明
MLD スヌーピング管理状態	ipv6 mld snooping	IPv6 MLD スヌーピング機能。デフォルトは無効
Fast Leave	ipv6 mld snooping fast-leave	ブリッジドメインごとに高速脱退機能をオンまたはオフにできます。これは MLDv2 ホストに適用され、1つのホストだけがそのポートの背後で MLD を実行することがわかっているポートで使用されます。このコマンドはデフォルトでは無効になっています。
クエリアの有効化	ipv6 mld snooping querier	IPv6 MLD スヌーピングクエリア処理を有効または無効にします。MLD スヌーピングクエリアは、マルチキャストトラフィックをルーティングする必要がないため、PIM および MLD を設定していないブリッジドメイン内で MLD スヌーピングをサポートします。

ACI 機能名	NX-OS 機能	説明
クエリ間隔	ipv6 mld snooping query-interval	MLD ホストクエリーメッセージの送信頻度を設定します。有効範囲は 1 ~ 18,000 秒です。デフォルト値は 125 秒です。
クエリ応答間隔	ipv6 mld snooping query-interval	MLD クエリーでアドバタイズされる応答時間を設定します。有効範囲は 1 ~ 25 秒です。デフォルトは 10 秒です。
最終メンバークエリ間隔	ipv6 mld snooping last-member-query-interval	メンバーシップレポートを送信してから、ソフトウェアがグループステートを解除するまでのクエリー応答時間を設定します。有効範囲は 1 ~ 25 秒です。デフォルト値は 1 秒です。

PIM 機能（インターフェイス レベル）

ACI 機能名	NX-OS 機能	説明
認証	ip pim hello-authentication ah-md5	PIM IPv4 ネイバーの MD5 ハッシュ認証をイネーブルにします。
マルチキャストドメイン境界	ip pim border	インターフェイスを PIM ドメインの境界として設定し、対象のインターフェイスで、ブートストラップ、候補 RP、または Auto-RP の各メッセージが送受信されないようにします。デフォルトではディセーブルになっています。
パッシブ	ip pim passive	パッシブ設定がインターフェイスで設定されている場合、IP マルチキャストのインターフェイスが有効になります。PIM は、passive モードのインターフェイスで動作します。これは、リーフがインターフェイス上で PIM メッセージを送信せず、このインターフェイス全体にわたる他のデバイスからの PIM メッセージも受け入れないことを意味します。リーフは、ネットワーク上の唯一の PIM デバイスであると見なし、DR として機能します。IGMP の動作は、このコマンドの影響を受けません。
厳格な RFC 準拠	ip pim strict-rfc-compliant	設定すると、スイッチは不明なネイバーからの参加を処理せず、不明なネイバーに PIM 参加を送信しません。

ACI 機能名	NX-OS 機能	説明
指定ルータの遅延 (秒)	ip pimdr-delay	PIM hello メッセージでアドバタイズされる DR プライオリティを指定期間にわたり 0 に設定することで、指定ルータ (DR) の選定への参加を遅延させます。この遅延中、DR は変更されず、現在のスイッチにはそのインターフェイスでのすべてのマルチキャストの状態を把握する時間が与えられます。遅延期間が終了すると、DR 選出を再び開始するために、正しい DR プライオリティが hello パケットで送信されます。値は 1 ~ 65,535 です。デフォルト値は 3 です。 注意：このコマンドは、起動時のみ、または IP アドレスがインターフェイスの状態が変更された後にのみ、DR 選定に参加することを遅延させます。これは、マルチキャストアクセスの非 vPC レイヤ 3 インターフェイス専用です。
指定ルータの優先順位	ip pim dr-priority	PIM hello メッセージの一部としてアドバタイズされる指定ルータ (DR) プライオリティを設定します。有効範囲は 1 ~ 4294967295 です。デフォルトは 1 です。
Hello 間隔 (ミリ秒)	ip pim hello-interval	hello メッセージの送信インターバルを、ミリ秒単位で設定します。範囲は 1000 ~ 18724286 です。デフォルト値は 30000 です。
Join-Prune 間隔ポリシー (秒)	ip pim jp-interval	PIM Join および Prune メッセージを送信する間隔 (秒単位)。有効な範囲は 60 ~ 65520 です。値は 60 で割り切れる必要があります。デフォルト値は 60 です。
インターフェイスレベルのインバウンド Join-Prune フィルタポリシー*	ip pimjp-policy	ルートマップポリシーに基づく、インバウンド Join/Prune メッセージのフィルタリングをイネーブルにします。ここで、グループ、グループおよび送信元、および RP アドレスを指定できます。デフォルトでは、Join/Prune メッセージはフィルタリングされません。
インターフェイスレベルのアウトバウンド Join-Prune フィルタポリシー*	ip pim jp-policy	ルートマップポリシーに基づく、アウトバウンド Join/Prune メッセージのフィルタリングをイネーブルにします。ここで、グループ、グループおよび送信元、および RP アドレスを指定できます。デフォルトでは、Join/Prune メッセージはフィルタリングされません。
インターフェイスレベルのネイバーフィルタポリシー*	ip pim neighbor-policy	許可される PIM ネイバーの送信元アドレス/アドレス範囲を指定するルートマップポリシーに基づいて、隣接する PIM ネイバーを制御します。

PIM 機能 (VRF レベル)

ACI 機能名	NX-OS 機能	説明
スタティック RP	ippimrp-address	マルチキャストグループ範囲に、PIM スタティック RP アドレスを設定します。スタティック RP のマルチキャストグループ範囲をリストするオプションのルートマップポリシーを指定できます。ルートマップが設定されていない場合、スタティック RP は、設定された SSM グループ範囲を除くすべてのマルチキャストグループ範囲に適用されます。 モードは ASM です。
ファブリック RP	該当なし	ファブリック内のすべてのマルチキャスト対応境界リーフスイッチでエニーキャスト RP を設定します。エニーキャスト RP は、PIM エニーキャスト RP を使用して実装されます。スタティック RP のマルチキャストグループ範囲をリストするオプションのルートマップポリシーを指定できます。
Auto-RP Forward Auto-RP Updates	ip pim auto-rp forward	Auto-RP メッセージの転送をイネーブルにします。デフォルトではディセーブルになっています。
Auto-RP Listen to Auto-RP Updates	ip pim auto-rp listen	Auto-RP メッセージのリッスンをイネーブルにします。デフォルトではディセーブルになっています。
Auto-RP MA Filter *	ip pim auto-rp mapping-agent-policy	ルートマップポリシーに基づく境界リーフによって Auto-RP Discovery メッセージのフィルタリングをイネーブルにします。ここで、マッピングエージェント送信元アドレスを指定できます。この機能は、境界リーフが Auto-RP メッセージをリッスンするように設定されている場合に使用されます。デフォルトでは、Auto-RP メッセージはフィルタリングされません。
BSR Forward BSR Updates	ippimbsr forward	BSR メッセージの転送をイネーブルにします。デフォルトではディセーブルになっているため、リーフは BSR メッセージの転送を行いません。
BSR Listen to BRS Updates	ip pim bsr listen	BSR メッセージのリッスンをイネーブルにします。デフォルトではディセーブルになっているため、リーフは BSR メッセージのリッスンを行いません。
BSR Filter	ip pim bsr bsr-policy	ルートマップポリシーに基づく境界リーフによって BSR メッセージのフィルタリングをイネーブルにします。ここで、BSR 送信元を指定できます。このコマンドは、境界リーフが BSR メッセージをリッスンするように設定されている場合に使用できます。デフォルトでは、BSR メッセージはフィルタリングされません。
ASM ソース、グループ有効期限タイマーポリシー*	ip pim sg-expiry-timer <timer> sg-list	調整された有効期限タイマーのグループ/グループを指定するために、ASM ソース、グループ有効期限タイマーにルートマップを適用します。

ACI 機能名	NX-OS 機能	説明
ASM Source, Group Expiry Timer Expiry (sec)	ip pim sg-expiry-timer	プロトコル独立マルチキャストスパスモード (PIM-SM) (S, G) マルチキャストルートの (S, G) 期限切れタイマーの間隔を調節します。このコマンドは、断続的な送信元に対してデフォルトの 180 秒を超える SPT (送信元ベースのツリー) の永続性を作成します。指定できる範囲は 1 ~ 604801 秒です。
Register Traffic Policy: Max Rate	ip pim register-rate-limit	レート制限を毎秒の packets 数で設定します。指定できる範囲は 1 ~ 65,535 です。デフォルト設定は無制限です。
Register Traffic Policy: Source IP	ip pim register-source	登録メッセージの送信元 IP アドレスを設定するために使用されます。この機能は、RP がメッセージを送信できるネットワークで登録メッセージの送信元アドレスがルーティングされる場合に使用できます。これは、送信元が接続されているブリッジドメインが、ファブリックの外部にサブネットをアドバタイズするように設定されていない場合に発生することがあります。
SSM グループ範囲ポリシー*	ippimssm route-map	デフォルトの範囲 232.0.0.0/8 以外の異なる SSM グループ範囲を指定するために使用できます。デフォルトのグループ範囲のみを使用する場合は、このコマンドは不要です。デフォルト範囲を含め、SSM マルチキャストに最大 4 つの範囲を設定できます。
短時間でのコンバージェンス	該当なし	高速コンバージェンスモードが有効になっている場合、ファブリック内のすべての境界リーフは、外部ネットワークのルート (*, G) および送信元 (S, G) の RP) に向けて PIM Join を送信します。これにより、ファブリック内のすべての PIM 対応 BL が外部ソースからマルチキャストトラフィックを受信できますが、1 つの BL のみがトラフィックをファブリックに転送します。マルチキャストトラフィックをファブリックに転送する BL が指定フォワードです。グループのストライプ優先は、DF を決定します。高速コンバージェンスモードの利点は、BL の障害によりストライプの優先が変更された場合、新しい BL が join を送信してマルチキャスト状態を作成することで、外部ネットワークで遅延が発生しないことです。 注意：追加の帯域幅のコストが保存コンバージェンス時間を上回る場合、高速コンバージェンスモードを導入時に無効にできることに注意してください。
厳格な RFC 準拠	ip pim strict-rfc-compliant	設定すると、スイッチは不明なネイバーからの参加を処理せず、不明なネイバーに PIM 参加を送信しません。
MTU ポート	ippimmtu	PIM コントロールプレーントラフィックのフレームサイズを大きくし、コンバージェンスを向上させます。範囲は 1500 ~ 9216 バイトです。
リソースポリシーの上限	ip pim state-limit	VRF ごとに許可される最大 (*, G)/(S, G) エントリを設定します。範囲は 1 ~ 4294967295 です。

ACI 機能名	NX-OS 機能	説明
リソースポリシー予約済みルートマップ*	ip pim state-limit <limit> reserved <route-map>	リソースポリシーの最大制限の予約済みエントリに適用されるマルチキャストグループまたはグループと送信元を照合するルートマップポリシーを設定します。
Resource Policy Reserved Multicast Entries	ip pim state-limit <limit> reserved <route-map> <limit>	この VRF で許可される最大予約済み (*, G) および (S, G) エントリです。最大許可ステート数以下である必要があります。リソースポリシーの予約済みルートマップポリシーで使用されます。

レイヤ3 IPv4/IPv6 マルチキャストの設定のガイドライン、制約事項、および予想される動作

次のガイドラインと制限を確認します。

- [IPv4/IPv6 マルチキャストのガイドラインと制約事項 \(89 ページ\)](#)
- [IPv4 マルチキャストのガイドラインと制約事項 \(91 ページ\)](#)
- [IPv6 マルチキャストのガイドラインと制約事項 \(92 ページ\)](#)

IPv4/IPv6 マルチキャストのガイドラインと制約事項

IPv4 マルチキャストと IPv6 マルチキャストの両方に次の制限が適用されます。

- 第2世代リーフスイッチでレイヤ3 IPv4/IPv6 マルチキャスト機能がサポートされています。第2世代スイッチは、製品 ID に -EX、-FX、-FX2、-FX3、-GX、またはそれ以降のファイックスが付いたスイッチです。
- カスタム QoS ポリシーは、Cisco Application Centric Infrastructure (ACI) ファブリックの外部から送信された (L3Out から受信した) レイヤ3 マルチキャストトラフィックではサポートされません。
- ブリッジドメインでの PIMv4/PIM6 およびアドバタイズホストルートの有効化がサポートされています。
- レイヤ3 マルチキャストは VRF レベルで有効になり、マルチキャストプロトコルは VRF インスタンス内で機能します。各 VRF インスタンスでは、マルチキャストを個別に有効化または無効化できます。
- マルチキャストで VRF インスタンスが有効になると、有効になった VRF インスタンスの個別のブリッジドメインと L3Out を有効にしてマルチキャストを構成できます。デフォルトでは、マルチキャストはすべてのブリッジドメインと L3Out で無効になっています。
- 双方向 PIMv4/PIM6 は現在サポートされていません。
- マルチキャストルータは、パーペイシブブリッジドメインではサポートされていません。

- サポートされるルートスケールは2,000です。マルチキャストスケール番号は、IPv4とIPv6の両方を含む複合スケールです。合計ルート制限は、ルートカウントとして定義されます。各IPv4ルートは1としてカウントされ、各IPv6ルートは4としてカウントされます。より多くのマルチキャストスケールをサポートするノードプロファイルでも、IPv6ルートスケールは2,000のままです。
- PIMv4/PIM6は、レイヤ3ポートチャネルインターフェイスを含むレイヤ3 Out ルーテッドインターフェイスおよびルーテッドサブインターフェイスでサポートされます。PIMv4/PIM6はレイヤ3 Out SVI インターフェイスではサポートされません。
- L3OutでPIMv4/PIM6を有効にすると、暗黙的な外部ネットワークが設定されます。このアクションの結果、L3Outが導入され、外部ネットワークを定義していない場合でもプロトコルが発生する可能性があります。
- マルチキャスト送信元が孤立ポートとしてリーフAに接続され、リーフBにL3Outがあり、リーフAとリーフBがvPCペアにある場合、マルチキャスト送信元に関連付けられたEPGカプセル化VLANはリーフBに展開されます。
- ブリッジドメインに接続されている送信元からパケットを受信する入力リーフスイッチの動作は、レイヤ3 IPv4 または IPv6 マルチキャスト サポートによって異なります。
 - レイヤ3 IPv4 マルチキャスト サポートは、IPv4 マルチキャスト ルーティングのために有効になっているブリッジドメインに接続された送信元からのパケットを入力リーフスイッチが受信した場合、その入力リーフスイッチは、ルーテッドVRFインスタンスのコピーのみをファブリックに送信します（ルーテッドは、TTLが1ずつ減少し、送信元MACがパーベイシブサブネットMACで書き換えられることを意味します）。また、出力リーフスイッチも、関連するすべてのブリッジドメイン内の受信者へパケットをルーティングします。そのため、受信者のブリッジドメインが送信元と同じで、リーフスイッチが送信元とは異なる場合、その受信者は同じブリッジドメイン内ですが、ルーティングされたコピーを受け取り続けます。これは、送信元と受信者が同じブリッジドメインおよび同じリーフスイッチ上にあり、このブリッジドメインでPIMが有効になっている場合にも適用されます。

詳細については、次のリンク [ポッドの追加](#) で、既存のレイヤ2設計を活用するマルチポッドをサポートする、レイヤ3マルチキャストに関する詳細情報を参照してください。
 - レイヤ3 IPv6 マルチキャスト サポートは、IPv6 マルチキャスト ルーティングのために有効になっているブリッジドメインに接続された送信元からのパケットを入力リーフスイッチが受信した場合、その入力リーフスイッチは、ルーテッドVRFインスタンスのコピーのみをファブリックに送信します（ルーテッドは、TTLが1ずつ減少し、送信元MACがパーベイシブサブネットMACで書き換えられることを意味します）。また、出力リーフスイッチも、受信者へパケットをルーティングします。出力リーフは、パケット内のTTLを1だけ減らします。これにより、TTLが2回減少します。また、ASMの場合、マルチキャストグループに有効なRPが設定されている必要があります。
- VRF間マルチキャスト通信ではフィルタを使用できません。



(注) Cisco ACIはIPフラグメンテーションをサポートしていません。したがって、外部ルーターへのレイヤ3 Outside (L3Out) 接続、またはInter-Pod Network (IPN) を介したマルチポッド接続を設定する場合は、インターフェイスMTUがリンクの両端で適切に設定されていることが推奨されます。Cisco ACI、Cisco NX-OS、Cisco IOSなどの一部のプラットフォームでは、設定可能なMTU値はイーサネットヘッダー(一致するIP MTU、14-18イーサネットヘッダーサイズを除く)を考慮していません。また、IOS XRなどの他のプラットフォームには、設定されたMTU値にイーサネットヘッダーが含まれています。設定された値が9000の場合、Cisco ACI、Cisco NX-OS Cisco IOSの最大IPパケットサイズは9000バイトになりますが、IOS-XRのタグなしインターフェイスの最大IPパケットサイズは8986バイトになります。

各プラットフォームの適切なMTU値については、それぞれの設定ガイドを参照してください。

CLIベースのコマンドを使用してMTUをテストすることを強く推奨します。たとえば、Cisco NX-OS CLIで `ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1` などのコマンドを使用します。

IPv4 マルチキャストのガイドラインと制約事項

IPv4 マルチキャストには、特に次の制限が適用されます。

- Cisco ACI ファブリックのボーダー リーフスイッチがマルチキャストを実行しており、L3Outでマルチキャストを無効にしているときにユニキャスト到達可能性がある場合、外部ピアがCisco Nexus 9000 スイッチの場合、トラフィック損失が発生します。これは、トラフィックがファブリックに送信される場合(送信元はファブリックの外部にあり、受信者はファブリックの内部にある場合)、またはファブリックを通過する場合(送信元と受信者がファブリックの外部にあり、ファブリックが送信中の場合)に影響します。
- Any Source Multicast (ASM) と Source-Specific Multicast (SSM) はIPv4 向けにサポートされています。
- VRF インスタンスごとにルートマップでSSM マルチキャストの最大4つの範囲を設定できます。
- IGMP スヌーピングは、マルチキャストルーティングが有効になっているパーペシブブリッジドメインでは無効にできません。
- リリース 3.1(1x) で始まる、FEXにマルチキャストのレイヤ3はサポートされています。FEXポートに接続されているマルチキャストの送信元または受信先がサポートされていません。詳細については、テスト環境でFEXを追加する方法について、設定、次のURLをアプリケーションセントリックインフラストラクチャとファブリックエクステンダを参照してください: <https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/application-policy-infrastructure-controller-apic/200529-Configure-a-Fabric-Extender-with-Applica.html>。リリース 3.1(1x) 以降のレイヤ3 マルチキャストではFEXがサポートされていません。FEXポートに接続されているマルチキャストの送信元または受信先はサポートされていません。

IPv6 マルチキャストのガイドラインと制約事項

IPv6 マルチキャストには、特に次の制限が適用されます。

- Source Specific Multicast (SSM) はサポートされていますが、RFC 3306-Unicast-Prefix-based IPv6 Multicast Addresses で固定 SSM 範囲が指定されています。したがって、SSM の範囲は IPv6 では変更できません。
- VRF インスタンスごとにルートマップで SSM マルチキャストの最大4つの範囲を設定できます。
- Any Source Multicast (ASM) は IPv6 でサポートされます。
- IPv6 の OIF および VRF スケール番号は、IPv4 の場合と同じです。
- スタティック RP 設定のみの PIM6 をサポートしています。Auto-RP および BSR は PIM6 ではサポートされません。
- ファブリック内のレシーバはサポートされません。IPv6 マルチキャストを有効にする場合は、MLD スヌープポリシーを無効にする必要があります。MLD スヌーピングと PIM6 を同じ VRF インスタンスで有効にすることはできません。
- 現在、レイヤ3 マルチキャストリスナー検出 (MLD) は Cisco ACI ではサポートされていません。
- ファブリック ランデブーポイント (RP) は、IPv6 マルチキャストではサポートされません。
- Cisco Multi-Site Orchestrator のサポートは利用できません。

GUI を使用したレイヤ3 IPv4 マルチキャストの設定

このセクションでは、Cisco APIC GUI を使用してレイヤ3 マルチキャストを設定する方法について説明します。



- (注) [Work] ペインおよび各ダイアログボックスの右上隅にあるヘルプアイコン (?) をクリックすると、表示されているタブまたはフィールドについての情報が表示されます。

始める前に

- 目的の VRF、ブリッジドメイン、IP アドレスを持つレイヤ3 Out インターフェイスは、PIM および IGMP が有効になるように設定する必要があります。
- 基本的なユニキャストネットワークを設定する必要があります。

- ステップ1** [テナント (Tenants)]> [Tenant_name]> [ネットワーク (Networking)]> [VRFs]> [VRF_name]> [マルチキャスト (Multicast)]に移動します。
[Work] ペインに、**PIM is not enabled on this VRF. Would you like to enable PIM?** というメッセージが表示されます。
- ステップ2** **YES, ENABLE MULTICAST** をクリックします。
- ステップ3** インターフェイスを設定します。
- [Work] ペインから、[Interfaces] タブをクリックします。
 - [Bridge Domains] テーブルを展開して [Create Bridge Domain] ダイアログを表示し、各フィールドに適切な値を入力します。
 - Select** をクリックします。
 - [Interfaces] テーブルを展開し、[Select an L3 Out] ダイアログを表示します。
 - [L3 Out] ドロップダウン矢印をクリックして L3 Out を選択します。
 - Select** をクリックします。
- ステップ4** ランデブー ポイント (RP) を設定します。
- [Work] ペインで [Rendezvous Points] タブをクリックし、次のランデブー ポイント (RP) オプションから選択します。
 - **スタティック RP**
 - [Static RP] テーブルを展開します。
 - 各フィールドに適切な値を入力します。
 - [Update] をクリックします。
 - **ファブリック RP**
 - [Fabric RP] テーブルを展開します。
 - 各フィールドに適切な値を入力します。
 - [Update] をクリックします。
 - **Auto-RP**
 - 各フィールドに適切な値を入力します。
 - **ブートストラップ ルータ (BSR)**
 - 各フィールドに適切な値を入力します。
- ステップ5** パターン ポリシーを設定します。
- [Work] ペインで [Pattern Policy] タブをクリックし、[Any Source Multicast (ASM)] または [Source Specific Multicast (SSM)] オプションを選択します。
 - 各フィールドに適切な値を入力します。

- ステップ6** PIMを設定します。
- [PIM Setting] タブをクリックします。
 - 各フィールドに適切な値を入力します。
- ステップ7** IGMP設定を行います。
- IGMP Setting** タブをクリックします。
 - [IGMP Context SSM Translate Policy] テーブルを展開します。
 - 各フィールドに適切な値を入力します。
 - [Update] をクリックします。
- ステップ8** Inter-VRF マルチキャストを設定します。
- [Work] ペインの [Inter-VRF Multicast] タブをクリックします。
 - [Inter-VRF Multicast] テーブルを展開します。
 - 各フィールドに適切な値を入力します。
 - [Update] をクリックします。
- ステップ9** 完了したら、[送信 (Submit)] をクリックします。
- ステップ10** メニューバーで、[テナント (Tenants)] > [Tenant_name] > [ネットワークング (Networking)] > [VRFs] > [VRF_name] > [マルチキャスト (Multicast)] に移動し、次の操作を実行します。
- [作業 (Work)] ペインの [インターフェイス (Interfaces)] タブで、適切な L3 Out を選択し、[PIM ポリシー (PIM Policy)] ドロップダウンリストから、接続する適切な PIM ポリシーを選択します。
 - [送信 (Submit)] をクリックします。
- ステップ11** 設定を確認するには次のアクションを実行します:
- Work** ウィンドウで、**Interfaces** をクリックして、関連付けられた **Bridge Domains** を表示します。
 - Interfaces** をクリックして、関連付けられた **L3 Out** インターフェイスを表示します。
 - Navigation** ウィンドウで、**BD** に移動します。
 - Work** ウィンドウに、設定された IGMP ポリシーと PIM の機能が、先ほど設定されたように表示されます。
 - Navigation** ウィンドウに、L3 Out インターフェイスが表示されます。
 - Work** ウィンドウに、PIM の機能が先ほど設定されたように表示されます。
 - Work** ウィンドウで、**Fabric > Inventory > Protocols > IGMP** に移動して、設定した IGMP インターフェイスの動作状態を表示します。
 - [作業 (Work)] ウィンドウで、[ファブリック (Fabric)] > [インベントリ (Inventory)] > [ポッド名 (Pod name)] > [Leaf_Node] > [プロトコル (Protocols)] > [IGMP] > [IGMP ドメイン (IGMP Domains)] に移動して、マルチキャストが有効化/無効化されたノードのドメイン情報を表示します。

GUIを使用したレイヤ3 IPv6 マルチキャストの設定

始める前に

- 目的のVRF、ブリッジドメイン、IPv6アドレスを持つレイヤ3 Outインターフェイスは、PIM6が有効になるように設定する必要があります。レイヤ3 Outの場合、IPv6マルチキャストが機能するために、論理ノードプロファイルのノードにIPv6 ループバック アドレスが設定されます。
- 基本的なユニキャスト ネットワークを設定する必要があります。

-
- ステップ1** メニューバーで[テナント (Tenants)]>[Tenant_name]>[ネットワーキング (Networking)]>[VRFs]>[VRF_name]>[マルチキャスト IPv6 (Multicast IPv6)]に移動します。
[作業 (Work)] ペインで次のメッセージが表示されます。PIM6はこのVRFで有効化されていません。(PIM6 is not enabled on this VRF.) PIM6を有効化しますか？(Would you like to enable PIM6?)
- ステップ2** [はい、マルチキャスト IPv6を有効化します。(YES, ENABLE MULTICAST IPv6)]をクリックします。
- ステップ3** インターフェイスを設定します。
- a) [Work] ペインから、[Interfaces] タブをクリックします。
 - b) [ブリッジドメイン (Bridge Domains)] テーブルを展開して[ブリッジドメインの作成 (Create Bridge Domain)] ダイアログを表示し、ドロップダウンリストから適切なBDを選択します。
 - c) [選択 (Select)] をクリックします。
 - d) [インターフェイス (Interfaces)] テーブルを展開し、[L3Outの選択 (Select an L3 Out)] ダイアログボックスを表示します。
 - e) [L3 Out] ドロップダウン矢印をクリックしてL3 Outを選択します。
 - f) **Select** をクリックします。
- ステップ4** ランデブーポイント (RP) を設定します。
- a) [作業 (Work)] ペインで[ランデブーポイント (Rendezvous Points)] タブをクリックし、[スタティック RP (Static RP)] を選択します。
 - b) 各フィールドに適切な値を入力します。
 - c) [Update] をクリックします。
- ステップ5** パターンポリシーを設定します。
- a) [作業 (Work)] ペインで[パターンポリシー (Pattern Policy)] タブをクリックし、[任意の送信元マルチキャスト (ASM) (Any Source Multicast (ASM))] を選択します。
 - b) 各フィールドに適切な値を入力します。
- ステップ6** PIMを設定します。
- a) [PIM Setting] タブをクリックします。
 - b) 各フィールドに適切な値を入力します。
- ステップ7** 完了したら、[送信 (Submit)] をクリックします。

ステップ 8 メニューバーで、[テナント (Tenants)] > [Tenant_name] > [ネットワーキング (Networking)] > [VRFs] > [VRF_name] > [マルチキャスト IPv6 (Multicast IPv6)] に移動し、次の操作を実行します。

- a) [作業 (Work)] ペインの [インターフェイス (Interfaces)] タブで、適切な [L3 Out] を選択し、[PIM ポリシー (PIM Policy)] ドロップダウンリストから、接続する適切な PIM ポリシーを選択します。
- b) [送信 (Submit)] をクリックします。

ステップ 9 設定を確認するには次のアクションを実行します:

- a) **Work** ウィンドウで、**Interfaces** をクリックして、関連付けられた **Bridge Domains** を表示します。
- b) [ナビゲーション (Navigation)] ペインで、関連付けられている BD with IPv6 マルチキャストに移動します。
[作業 (Work)] ウィンドウに、PIM の機能が先ほど設定されたように表示されます。
- c) [ナビゲーション (Navigation)] ペインで、関連付けられている L3 Out インターフェイスに移動します。
[作業 (Work)] ペインで、PIM6 チェックボックスをオンにします。
- d) [作業 (Work)] ペインで、[ファブリック (Fabric)] > [インベントリ (Inventory)] > [ポッド (Pod)] [ノード (Node)] [プロトコル (Protocols)] > [PIM6] の順に移動し、[PIM] を展開します。
以前に作成された適切な PIM6 プロトコルで、関連付けられているネイバー、PIM インターフェイス、ルート、グループ範囲、および RP に関する情報を表示できます。これらすべてのオブジェクトが設定されていることを確認できます。

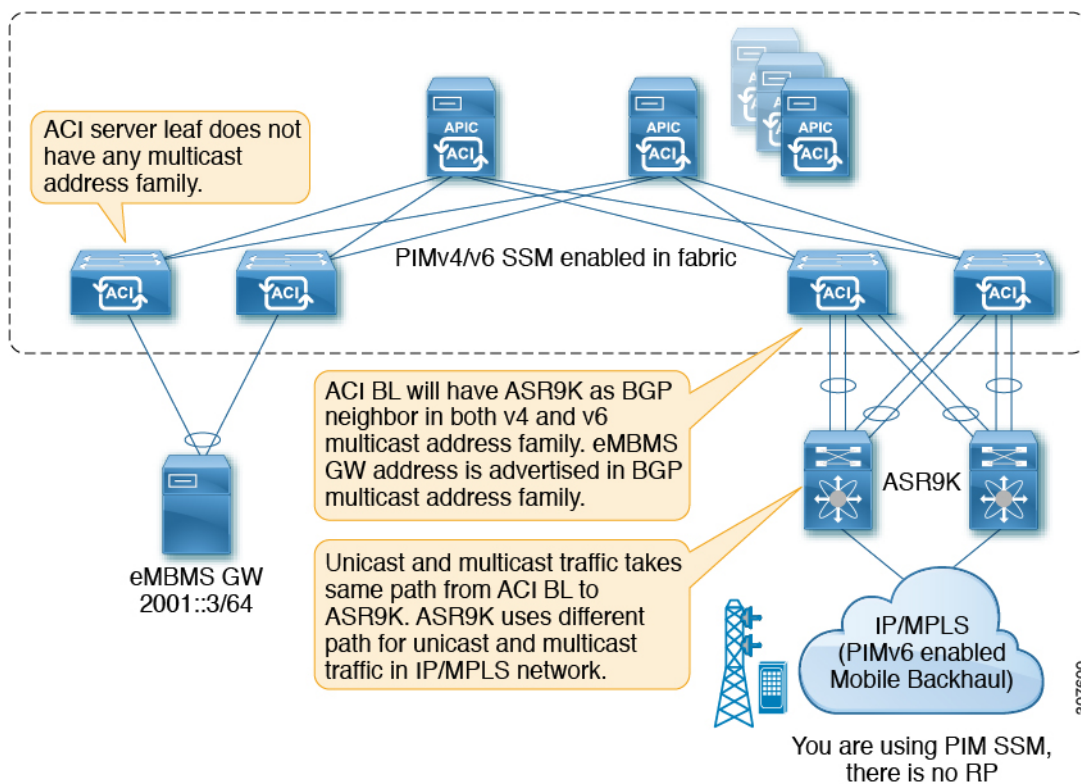
BGP IPv4/IPv6 マルチキャスト アドレス ファミリについて



(注) BGP IPv4/IPv6 マルチキャスト アドレス ファミリ機能の IPv4 バージョンは、Cisco APIC リリース 4.1 の一部として使用できました。

Cisco APIC リリース 4.2 (1) 以降、BGP マルチキャスト アドレス ファミリ機能は、ボーダーリーフスイッチ上のテナント VRF の BGP ピアに対する IPv6 のサポートを追加します。ピアが IPv4/IPv6 マルチキャスト アドレス ファミリでマルチキャスト ルートを伝送するために個別に使用されるかどうかを指定できます。

次の図に、この機能の実装方法を示します。



BGP IPv4/IPv6 マルチキャストアドレスファミリのガイドラインと制約事項

IPv6 の BGP マルチキャストアドレスファミリ機能のガイドラインと制約事項

- ランデブーポイント (RP) は、Cisco ACI ファブリックの外部にある IP アドレスです。ファブリック RP は IPv6 マルチキャストではサポートされません。
- マルチキャスト送信元は Cisco ACI ファブリック内にあり、レシーバはファブリック外にあります。
- 中継 L3Out は BGPv4/v6 アドレスファミリではサポートされません。

IPv4 と IPv6 の両方に対する BGP マルチキャストアドレスファミリ機能のガイドラインと制約事項

- Cisco ACI ファブリック内の BGPv4/v6 マルチキャストアドレスファミリはサポートされません。
- ユニキャストアドレスファミリが使用されている場合は、RP の到達可能性が存在する必要があります。PIM Source-Specific Multicast (SSM) の場合、RP は必要ありません。

GUI を使用した BGP IPv4/IPv6 マルチキャストの設定

次の手順では、GUI を使用して BGP IPv4/IPv6 マルチキャストアドレスファミリー機能を設定する方法について説明します。

始める前に

L3Out を設定する前に、次のような標準的な前提条件を満たします。

- テナント、ノード、ポート、AEP、機能プロファイル、レイヤ3 ドメインを設定します。
- ファブリック内でルートを伝播させるための、BGP ルート リフレクタ ポリシーを設定します。

ステップ1 L3Out で使用する VRF を特定するか、必要に応じて VRF を作成します。

[テナント (Tenants)] > [テナント (*tenant*)] > [ネットワーキング (Networking)] > [VRFs]

ステップ2 VRF で PIMv4 または PIMv6 を有効にします。

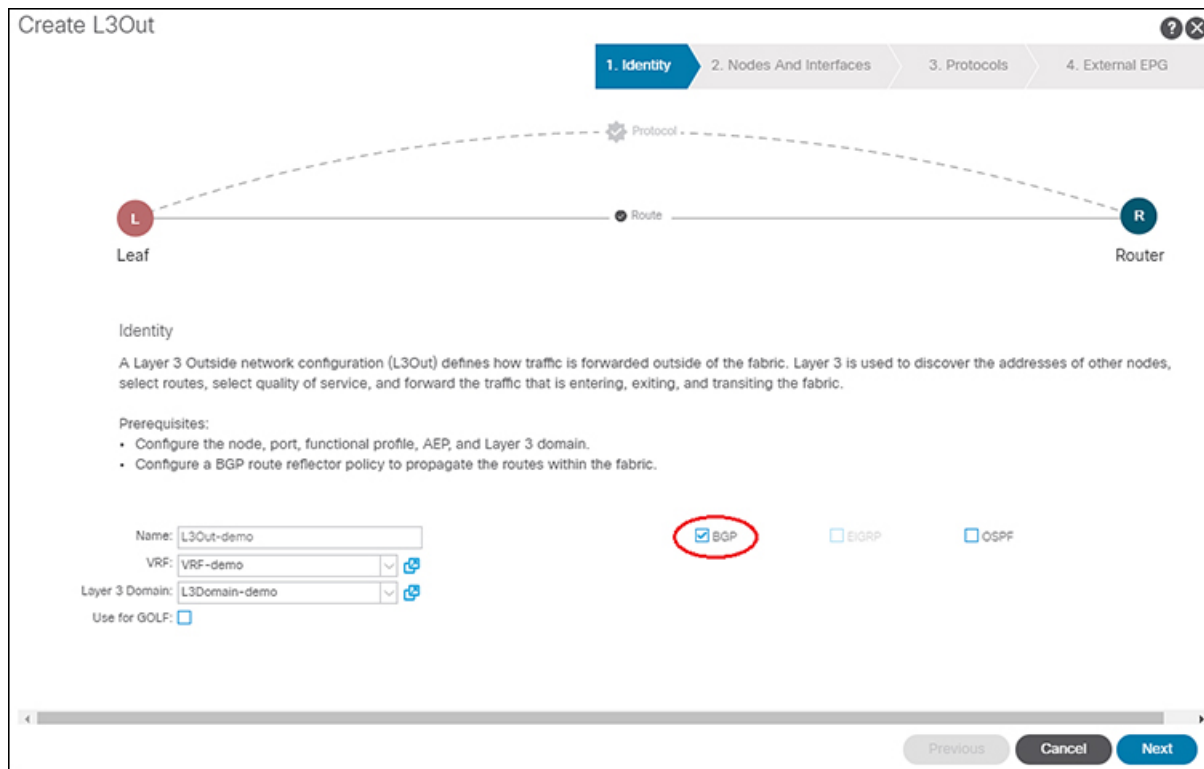
- VRF の下で PIMv4 を有効化するには、メニューバーで [テナント (Tenants)] > [*Tenant_name*] > [ネットワーキング (Networking)] > [VRFs] > [*VRF_name*] > [マルチキャスト (Multicast)] に移動します。
 - メッセージが表示された場合、この VRF で PIM が有効になっていません。[PIM を有効化しますか? (Would you like to enable PIM?)] をクリックし、[はい、マルチキャストを有効化します (Yes, enable Multicast)] をクリックします。
 - メインの [マルチキャスト (Multicast)] ウィンドウが表示されている場合は、[有効化 (Enable)] ボックスをオンにします (オンになっていない場合)。
- VRF の下で PIMv6 を有効化するには、メニューバーで [テナント (Tenants)] > [*Tenant_name*] > [ネットワーキング (Networking)] > [VRFs] > [*VRF_name*] > [マルチキャスト IPv6 (Multicast IPv6)] に移動します。
 - この VRF で「PIMv6 は有効化されていません (PIMv6 is not enabled)」というメッセージが表示される場合。[PIMv6 を有効化しますか? (Would you like to enable PIMv6?)] をクリックし、[はい、マルチキャスト IPv6 を有効化します (Yes, enable multicast IPv6)] をクリックします。
 - メインの [マルチキャスト IPv6 (Multicast IPv6)] ウィンドウが表示されている場合は、[有効化 (Enable)] ボックスをオンにします (オンになっていない場合)。

ステップ3 L3Out を作成し、L3Out の BGP を設定します。

- [ナビゲーション (Navigation)] ペインで [テナント (Tenant)] および [ネットワーキング (Networking)] を展開します。
- [L3Outs] を右クリックし、[L3Out の作成 (Create L3Out)] を選択します。
- L3Out の BGP を設定するために必要な情報を入力します。

[識別 (Identity)] ページ

- 前の手順で設定した VRF を選択します。
- L3Out 作成ウィザードの [識別 (Identity)] ページで [BGP] を選択して、L3Out 向け BGP プロトコルの設定を行います。



- d) 残りのページを続けて行い ([ノードとインターフェイス (Nodes and Interfaces)]、[プロトコル (Protocols)]、および [外部 EPG (External EPG)])、L3Out の設定を完了します。

ステップ 4 L3Out の設定が完了したら、BGP IPv4/IPv6 マルチキャスト アドレス ファミリ機能を設定します。

- a) BGP ピア接続プロファイル スクリーンに移動します。

[テナント (Tenants)] > [テナント (*tenant*)] > [ネットワーキング (Networking)] > [L3Outs] > [L3out-name] > [論理ノード プロファイル (Logical Node Profiles)] > [logical-node-profile-name] > [論理インターフェイス プロファイル (Logical Interface Profiles)] > [logical-interface-profile-name] > [BGP ピア接続プロファイル (BGP Peer Connectivity Profile)] [IP-address]

- b) [アドレス タイプ制御 (Address Type Controls)] フィールドまで下にスクロールし、次のように選択します。
- [AF Mcast] を選択します。
 - [AF Ucast] が選択されている場合は、選択したままにします。

Peer Connectivity Profile - BGP Peer Connectivity Profile

Properties

Address: [redacted]

Description: optional

BGP Controls:

Allow Self AS

AS override

Disable Peer AS Check

Next-hop Self

Send Community

Send Extended Community

Password: [redacted]

Confirm Password: [redacted]

Allowed Self AS Count: 3

Peer Controls: Bidirectional Forwarding Detection

Disable Connected Check

EBGP Multihop TTL: 1

Weight for routes from this neighbor: 0

Private AS Control: Remove all private AS

Remove private AS

Replace private AS with local AS

Address Type Controls: AF Mcast

AF Ucast

BGP Peer Prefix Policy: select a value

Remote Autonomous System Number: 8

Local-AS Number Confir: [redacted]

307998

- c) [送信 (Submit)] をクリックします。
- d) ピアの IPv4 または IPv6 マルチキャスト アドレス ファミリに再配布する必要があるサブネットを持つブリッジドメインに移動します。

[テナント (Tenants)] > [tenant] > [ネットワーク (Networking)] > [ブリッジドメイン (Bridge Domains)] > [bridge_domain-name]

- e) メイン ペインで、[ポリシー/全般 (Policy/General)] タブをクリックします。
- f) ブリッジドメインで PIMv4 または PIMv6 を有効にします。
 - ブリッジドメインで PIMv4 を有効にするには、[PIM] フィールドまでスクロールし、そのフィールドの横にあるチェックボックスをオンにして有効にします。
 - ブリッジドメインで PIMv6 を有効にするには、[PIMv6] フィールドまでスクロールし、そのフィールドの横にあるチェックボックスをオンにして有効にします。

Bridge Domain - demoBD

100

Properties

Advertise Host Routes:

Enable Legacy Mode:

Legacy Mode: No

VLAN: []

VRF: select a value [v]

Resolved VRF: common/default

L2 Unknown Unicast: Flood Hardware Proxy

L3 Unknown Multicast Flooding: Flood Optimized Flood

IPv6 L3 Unknown Multicast: Flood Optimized Flood

Multi Destination Flooding: Flood in BD Drop Flood in Encapsulation

PIM:

PIMv6:

IGMP Policy: select an option [v]

ARP Flooding:

IP Data-plane Learning: no yes

307696

g) [送信 (Submit)] をクリックします。

マルチキャストフィルタリングについて

ACIは、誰がマルチキャストフィードを受信でき、どのソースから受信できるかを制御するために使用できるコントロールプレーン構成をサポートしています。フィルタリングオプションには、IGMP レポートフィルタ、PIM Join または Prune フィルタ、PIM ネイバーフィルタ、およびランデブーポイント (RP) フィルタがあります。これらのオプションは、コントロールプレーンプロトコル (IGMP および PIM) に依存します。

一部の展開で、データプレーンレベルでマルチキャストストリームの送信および/または受信を制限することが望ましい場合があります。たとえば、LAN 内のマルチキャスト送信者が特定のマルチキャストグループにのみ送信できるようにするか、受信者がすべての可能な送信元から、または特定の送信元からの特定のマルチキャストグループを受信のみできるようにする必要があります。

Cisco APICリリース 5.0(1)以降では、マルチキャストフィルタリング機能を使用できるようになりました。これにより、二方向からのマルチキャストトラフィックをフィルタリングできます。

- [マルチキャスト フィルタリングの設定：ファースト ホップ ルータでの送信元フィルタリング \(102 ページ\)](#)
- [マルチキャスト フィルタリングの設定：ラストホップ ルータでの送信元 フィルタリング \(102 ページ\)](#)
- [同じブリッジ ドメインでの送信元と受信者の複合フィルタリング \(103 ページ\)](#)

マルチキャスト フィルタリングの設定：ファースト ホップ ルータでの送信元フィルタリング

ブリッジ ドメインでトラフィックを送信している送信元について、そのブリッジ ドメインのマルチキャスト送信元フィルタを設定している場合、送信元とグループは送信元フィルタ ルートマップのエントリの1つと照合されます。そのエントリに関連付けられているアクションに応じて、アクションが実行されます。

- 送信元およびグループが、ルートマップの **許可** アクションを持つエントリと一致する場合、ブリッジ ドメインはその送信元からそのグループへのトラフィック送信を許可します。
- 送信元およびグループが、ルートマップの **拒否** アクションを持つエントリと一致する場合、ブリッジ ドメインはその送信元からそのグループへのトラフィック送信をブロックします。
- ルート マップ内のどのエントリとも一致しない場合、ブリッジ ドメインは、デフォルト オプションとして、その送信元からそのグループへのトラフィックの送信をブロックします。つまり、ルート マップが適用されると、最後に暗黙の「deny all (すべて拒否)」ステートメントが常に有効になります。

シングルルートマップに複数のエントリを設定できます。ここで一部のエントリは **許可** アクションで設定、その他のエントリは **拒否** アクションで設定が可能です。すべてが同じルートマップ内で行われます。



- (注) 送信元フィルタがブリッジドメインに適用されると、送信元でマルチキャストトラフィックがフィルタリングされます。フィルタは、異なるブリッジドメイン内の受信先、同じブリッジドメイン内の受信先、および外部受信先がマルチキャストを受信するのを防ぎます。

マルチキャスト フィルタリングの設定：ラストホップ ルータでの送信元 フィルタリング

マルチキャスト送信元フィルタリングは、ブリッジドメイン内の受信者が特定のグループのマルチキャストを受信できる送信元を制限するために使用されます。この機能は、IGMPv3 がコントロールプレーンで提供するものと同様に、送信元またはグループのデータプレーン フィルタリング機能を提供します。

ブリッジ ドメインで **join** を送信する受信者について、そのブリッジ ドメインのマルチキャスト受信者フィルタを設定している場合、送信元とグループは受信者フィルタ ルートマップの

エントリの1つと照合されます。ここで、そのエントリに関連付けられているアクションに応じて、次のいずれかのアクションが実行されます。

- 送信元およびグループが、ルートマップの **許可** アクションを持つエントリと一致する場合、ブリッジドメインはその送信元からそのグループへのトラフィックの受信を許可します。
- 送信元およびグループが、ルートマップの **拒否** アクションを持つエントリと一致する場合、ブリッジドメインはその送信元からそのグループへのトラフィック受信をブロックします。
- ルートマップ内のどのエントリとも一致しない場合、ブリッジドメインは、デフォルトオプションとして、その送信元からそのグループへのトラフィックの受信をブロックします。つまり、ルートマップが適用されると、最後に暗黙の「deny all (すべて拒否)」ステートメントが常に有効になります。

シングルルートマップに複数のエントリを設定できます。ここで一部のエントリは **許可** アクションで設定、その他のエントリは **拒否** アクションで設定が可能です。すべてが同じルートマップ内で行われます。

同じブリッジドメインでの送信元と受信者の複合フィルタリング

同じブリッジドメインでマルチキャスト送信元フィルタリングとマルチキャスト受信者フィルタリングの両方を有効にすることもできます。この場合、1つのブリッジドメインがブロッキングを実行したり、トラフィックをグループ範囲に送信する際に送信元のフィルタリングを許可したり、送信元からグループ範囲へのトラフィックを受信する場合にフィルタリングを制限したり、フィルタリングを制限したりできます。

マルチキャスト フィルタリングのガイドラインと制約事項

マルチキャストフィルタリング機能のガイドラインと制約事項は次のとおりです。

- ブリッジドメインでマルチキャスト送信元フィルタリングまたはレシーバフィルタリングを有効にできますが、同じブリッジドメインでマルチキャスト送信元フィルタリングとレシーバフィルタリングの両方を有効にすることもできます。
- マルチキャストフィルタ処理は、IPv4でのみサポートされています。
- ブリッジドメインにマルチキャストフィルタを設定しない場合は、そのブリッジドメインで送信元フィルタまたは宛先フィルタ ルートマップを設定しないでください。デフォルトでは、ルートマップはブリッジドメインに関連付けられていません。これは、すべての送信元とグループが許可されることを意味します。送信元フィルタまたは宛先フィルタを持つルートマップがブリッジドメインに関連付けられている場合、そのルートマップ内の許可エントリのみが許可され、すべての拒否エントリがブロックされます（常に末尾に暗黙の「deny-all」ステートメントを含みます）。
- 空のルートマップをブリッジドメインに接続すると、ルートマップはデフォルトで **deny all** を想定するため、すべての送信元とグループがそのブリッジドメインでブロックされます。

- マルチキャストフィルタリング機能は、ブリッジドメインレベルで適用されます。ACIは、単一のブリッジドメインでの複数のEPGの設定をサポートします。この設定をブリッジドメインフィルタリング機能とともに使用すると、ブリッジドメインレベルの設定であるため、フィルタはブリッジドメイン内のすべてのEPGに適用されます。
- マルチキャストフィルタリング機能は、任意の送信元マルチキャスト（ASM）範囲にのみ使用することを目的としています。ただし、送信元固有のマルチキャスト（SSM）範囲をサポートしている場合は、IGMPv3を使用したSSM join itselfで送信元と結合をフィルタ処理することを推奨します。

マルチキャストフィルタ処理機能のSSM範囲を設定する場合は、次の制約事項が適用されます。

- **Bridge domain source filtering with SSM**：送信元フィルタリングはSSMではサポートされていません。
- **Bridge domain receiver filtering with SSM**：受信者フィルタリングはSSMグループ範囲で使用できます。受信者フィルタリングの主な使用例の1つは、特定の送信元からのマルチキャストストリームをフィルタリングすることです。この機能はすでにSSMプロトコルによって提供されているため、ほとんどの場合、SSMでは受信者フィルタリングは必要ありません。
- 送信元と受信者のフィルタリングでは、ルートマップエントリの順序付きリストが使用されます。ルートマップエントリは、一致するまで最も小さい番号から実行されます。一致がある場合、リスト内で最長一致ではない場合でも、プログラムは終了し、残りのエントリは考慮されません。

たとえば、次のエントリを持つ特定の送信元（192.0.3.1/32）の次のルートマップがあります。

表 6: ルートマップ

順位	送信元 IP	アクション
1	192.0.0.0/16	許可
2	192.0.3.0/24	拒否

ルートマップは、オーダー番号に基づいて評価されます。したがって、2番目のエントリ（192.0.3.0/24）が送信元IPと一致する場合でも、最初のエントリ（192.0.0.0/16）は、下位の番号が原因で照合されます。

GUIを使用したマルチキャストフィルタリングの設定

ブリッジドメインレベルでマルチキャストフィルタリングを設定します。このトピックの手順を使用して、ブリッジドメインレベルで送信元フィルタリングまたは受信者フィルタリング、あるいはその両方を設定します。

始める前に

- マルチキャストフィルタリングを設定するブリッジドメインはすでに作成されています。
- ブリッジドメインはPIM対応ブリッジドメインです。
- レイヤ3マルチキャストはVRFレベルで有効になります。

ステップ1 マルチキャストフィルタリングを設定するブリッジドメインに移動します。

[テナント (Tenant)] > [tenant-name] > [ネットワーキング (Networking)] > [ブリッジドメイン (Bridge Domains)] > [bridge-domain-name]

このブリッジドメインの [サマリ (Summary)] ページが表示されます。

ステップ2 [ポリシー (Policy)] タブを選択し、[全般 (General)] サブタブを選択します。

ステップ3 [全般 (General)] ウィンドウで、[PIM] フィールドを見つけ、PIMが有効になっていることを確認します ([PIM] フィールドの横にあるチェックボックスがオンになっていること)。

PIMが有効になっていない場合は、[PIM] フィールドの横にあるチェックボックスをオンにして有効にします。[送信元フィルタ (Source Filter)] フィールドと [宛先フィルタ (Destination Filter)] フィールドが使用可能になります。

(注) マルチキャストフィルタリングはIPv4 (PIM) でのみサポートされており、現時点ではIPv6 (PIM6) ではサポートされていません。

ステップ4 マルチキャスト [送信元] または [受信者] のフィルタリングを有効にするかどうかを決定します。

(注) 送信元フィルタリングと受信先フィルタリングの両方を同じブリッジドメインで有効にできません。

- ファーストホップルータでマルチキャスト [送信元] フィルタリングを有効にする場合は、[送信元フィルタ (Source Filter)] フィールドで、次のいずれかを選択します。
 - 既存のルートマップポリシー：送信元フィルタリングのマルチキャストの既存のルートマップポリシーを選択します。 [ステップ7 \(108 ページ\)](#)
 - 新しいルートマップポリシー：[マルチキャスト向けのルートマップポリシーの作成 (Create Route Map Policy for Multicast)] を選択し、に進みます。 [ステップ5 \(106 ページ\)](#)
- ラストホップルータでマルチキャスト [受信者] フィルタリングを有効にする場合は、[宛先フィルタ (Destination Filter)] フィールドで、次のいずれかを選択します。
 - 既存のルートマップポリシー：受信者フィルタリング用のマルチキャストの既存ルートマップポリシーを選択して [ステップ7 \(108 ページ\)](#) に移動します。
 - 新しいルートマップポリシー：[マルチキャスト向けのルートマップポリシーの作成 (Create Route Map Policy for Multicast)] を選択し、に進みます。 [ステップ6 \(107 ページ\)](#)

ステップ5 [マルチキャストのルートマップポリシーの作成 (Create Route Map Policy for Multicast)] オプションを選択して、最初のホップルータでマルチキャスト[送信元]フィルタリングを有効にした場合は、[マルチキャストのルートマップポリシーの作成 (Create Route Map Policy for Multicast)] ウィンドウが表示されます。このウィンドウに次の情報を入力します。

- a) [名前 (Name)] フィールドにこのルートマップの名前を入力し、必要に応じて[説明 (Description)] フィールドに説明を入力します。
- b) [ルートマップ (Route Maps)] 領域で、[+]をクリックします。

[ロールの作成 (Create a Role)] ウィンドウが表示されます。

- c) **Order** フィールドでは、このインターフェイスに対して複数のアクセスグループを設定している場合に、このインターフェイスでのマルチキャストトラフィックへのアクセスをどの順序で許可または拒否するかを反映する番号を選択します。

小さい番号のエントリは、大きい番号のエントリの前に並べられます。範囲は0～65535です。

- d) マルチキャスト送信元フィルタリングのためにトラフィックの送信を許可または拒否する方法を決定します。

- 特定の送信元から任意のグループへのマルチキャストトラフィックの送信を許可または拒否する場合は、[送信元 IP (Source IP)] フィールドに、トラフィックの送信元となる特定の送信元の IP アドレスを入力し、[グループ IP (Group IP)] フィールドは空のままにします。
- 任意の送信元から特定のグループへのマルチキャストトラフィックの送信を許可または拒否する場合は、[グループ IP (Group IP)] フィールドに、トラフィックの送信先のマルチキャスト IP アドレスを入力し、[送信元 IP (Source IP)] フィールドは空のままにします。
- 特定の送信元から特定のグループへのマルチキャストトラフィックの送信を許可または拒否する場合は、[グループ IP (Group IP)] フィールドと[送信元 IP (Source IP)] フィールドの両方に必要な情報を入力します。

(注) [RPIP] フィールドは、マルチキャスト送信元フィルタリングまたはマルチキャスト受信者フィルタリングには適用されません。このフィールドのエントリはマルチキャストフィルタリングでは無視されるため、この機能のこのフィールドには値を入力しないでください。

- e) [アクション (Action)] フィールドでは、ターゲット送信元のアクセスを拒否する場合には[拒否 (Deny)] を、ターゲット送信元のアクセスを許可する場合には[許可 (Permit)] を選択します。
- f) [OK] をクリックします。

[マルチキャストのルートマップポリシーの作成 (Create Route Map Policy for Multicast)] ウィンドウが再び表示され、設定したルートマップエントリが[ルートマップ (Route Maps)] テーブルに表示されます。

- g) このルートマップに追加のルートマップエントリを作成するかどうかを決定します。

1つのルートマップに対して複数のルートマップエントリを作成できます。各エントリには、独自のIPアドレスと関連アクションがあります。たとえば、同じルートマップ内に、[許可 (Permit)] アクションが適用されたIPアドレスのセットと、[拒否 (Deny)] アクションが適用されたIPアドレスの別のセットが必要な場合があります。

このルートマップに追加のルートマップ エントリを作成する場合は、[ルートマップ (Route Maps)] 領域で[+]をもう一度クリックし、に移動して、このルートマップの追加のルートマップ エントリを [ルートマップ エントリの作成 (Create Route Map Entry)] ウィンドウで必要な情報をフィルタリングするステップを繰り返します。5.c (106 ページ)

- h) このルートマップのすべてのルートマップ エントリを完了したら、[送信 (Submit)] をクリックします。ステップ 7 (108 ページ) に進みます。

ステップ 6 [マルチキャストのルートマップ ポリシーの作成 (Create Route Map Policy for Multicast)] オプションを選択して、ラストホップルータでのマルチキャスト宛先 (レシーバ) フィルタリングを有効にした場合は、[マルチキャストのルートマップ ポリシーの作成 (Create Route Map Policy for Multicast)] ウィンドウが表示されます。このウィンドウに次の情報を入力します。

- a) [名前 (Name)] フィールドにこのルートマップの名前を入力し、必要に応じて [説明 (Description)] フィールドに説明を入力します。
- b) [ルートマップ (Route Maps)] 領域で、[+]をクリックします。
[ロールの作成 (Create a Role)] ウィンドウが表示されます。

- c) **Order** フィールドでは、このインターフェイスに対して複数のアクセスグループを設定している場合に、このインターフェイスでのマルチキャストトラフィックへのアクセスをどの順序で許可または拒否するかを反映する番号を選択します。

小さい番号のエントリは、大きい番号のエントリの前に並べられます。範囲は 0 ~ 65535 です。

- d) マルチキャストレシーバフィルタリングで受信するトラフィックを許可するか拒否するかを決定します。
- 任意の送信元から特定のグループへのトラフィックの送信を許可または拒否する場合は、[グループ IP (Group IP)] フィールドに、トラフィックの送信先のマルチキャスト IP アドレスを入力し、[送信元 IP (Source IP)] フィールドは空のままにします。
 - 特定の送信元から任意のグループへのトラフィックの送信を許可または拒否する場合は、[送信元 IP (Source IP)] フィールドに、トラフィックの送信元となる特定の送信元の IP アドレスを入力し、[グループ IP (Group IP)] フィールドは空のままにします。
 - 特定の送信元から特定のグループへのトラフィックの受信を許可または拒否する場合は、[グループ IP (Group IP)] フィールドと [送信元 IP (Source IP)] フィールドの両方に必要な情報を入力します。

(注) [RPI] フィールドは、マルチキャスト送信元フィルタリングまたはマルチキャスト受信者フィルタリングには適用されません。このフィールドのエントリはマルチキャストフィルタリングでは無視されるため、この機能のこのフィールドには値を入力しないでください。

- e) [アクション (Action)] フィールドでは、ターゲットグループのアクセスを拒否する場合には [拒否 (Deny)] を、ターゲットグループのアクセスを許可する場合には [許可 (Permit)] を選択します。
- f) [OK] をクリックします。

[マルチキャストのルートマップポリシーの作成 (Create Route Map Policy for Multicast)] ウィンドウが再び表示され、設定したルートマップ エントリが [ルートマップ (Route Maps)] テーブルに表示されます。

- g) このルートマップに追加のルートマップエントリを作成するかどうかを決定します。

1つのルートマップに対して複数のルートマップエントリを作成できます。各エントリには、独自のIPアドレスと関連アクションがあります。たとえば、同じルートマップ内に、[許可 (Permit)]アクションが適用されたIPアドレスのセットと、[拒否 (Deny)]アクションが適用されたIPアドレスの別のセットが必要な場合があります。

このルートマップに追加のルートマップエントリを作成する場合は、[ルートマップ (Route Maps)]領域で[+]をもう一度クリックし、に移動して、このルートマップの追加のルートマップエントリを[ルートマップエントリの作成 (Create Route Map Entry)]ウィンドウで必要な情報をフィルタリングするステップを繰り返します。6.c (107 ページ)

- h) このルートマップのすべてのルートマップエントリを完了したら、[送信 (Submit)]をクリックします。ステップ7 (108 ページ)に進みます。

ステップ7 [ポリシー/全般 (Policy/General)]ページの右下隅にある[送信 (Submit)]をクリックします。

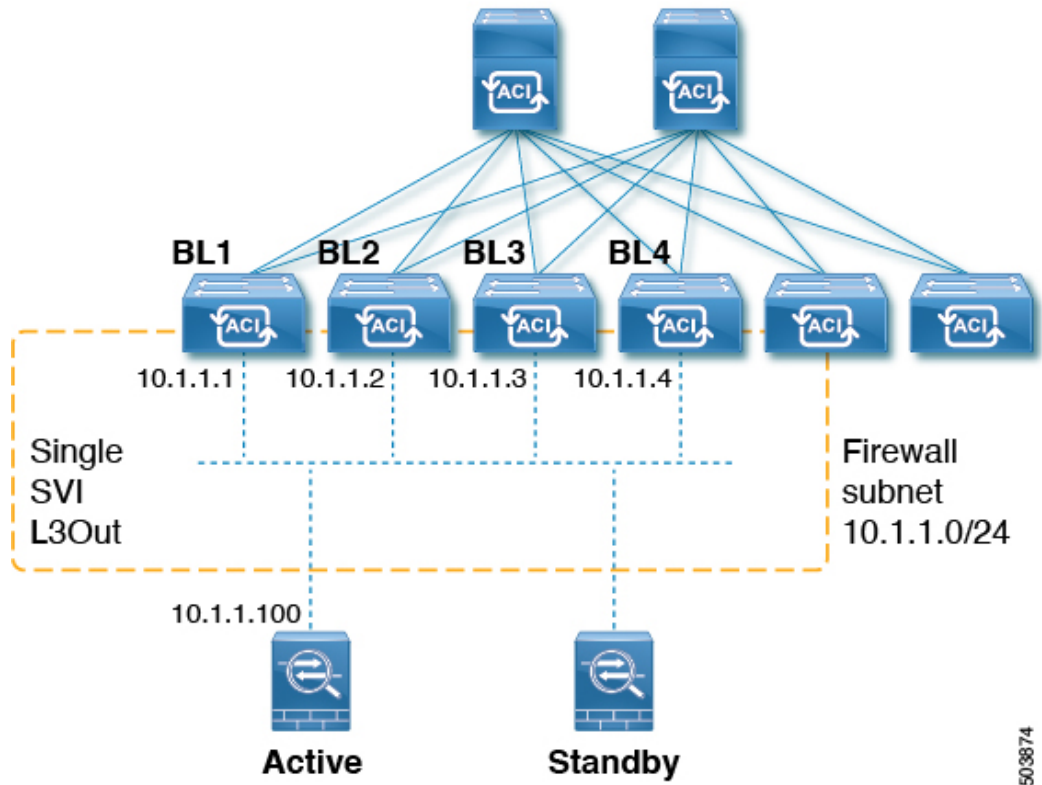
[ポリシー使用の警告 (Policy Usage Warning)]ウィンドウが表示されます。

ステップ8 [ポリシー使用の警告 (Policy Usage Warning)]ウィンドウのテーブルに表示されているノードとポリシーがこのポリシーの変更の影響を受けることを確認し、マルチキャストの送信元や宛先のフィルタリングを有効にし、[変更の送信 (Submit Changes)]をクリックします。

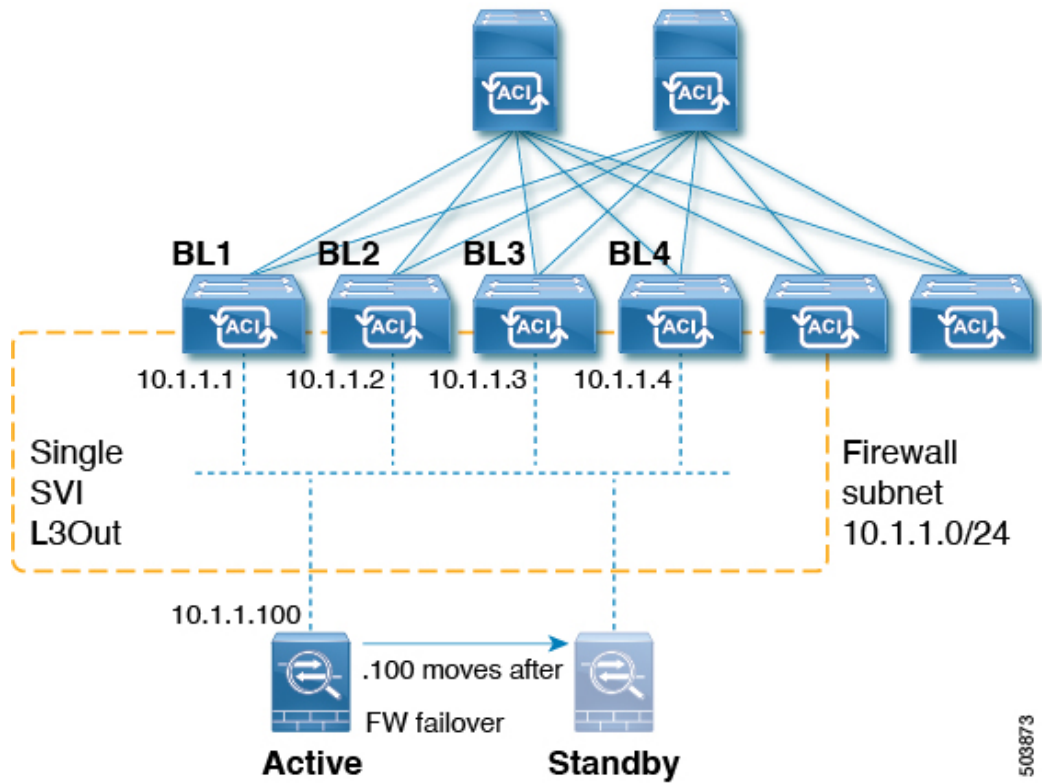
SVI L3Out のレイヤ3 マルチキャストについて

L3Out SVIでのレイヤ3 マルチキャストにより、L3Out SVIでPIMを有効にするためのサポートが追加されます。これにより、L3Out SVIで構成されたACI境界リーフスイッチは、外部マルチキャストルータまたはファイアウォールとのPIM隣接関係を確立できます。

ファイアウォールは通常、アクティブ/スタンバイペアで展開されます。ここでは、両方のファイアウォールが同じVLANとサブネット上のファブリックに接続されます。



503874



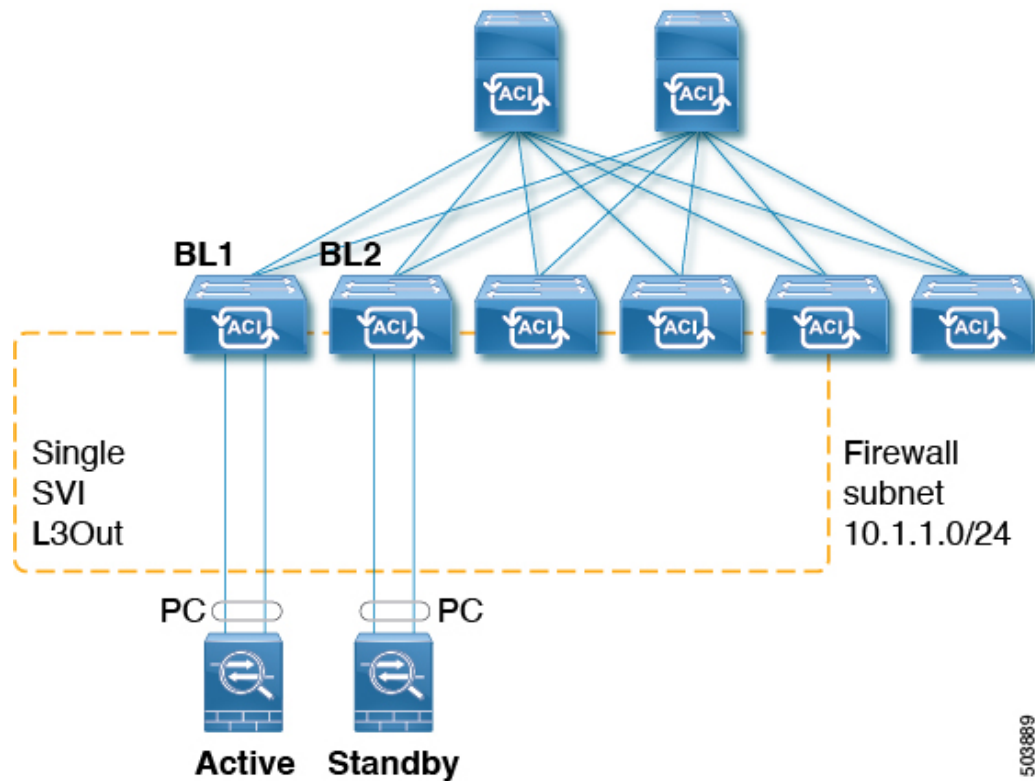
503873

これは LAN に似たトポロジであるため、ファブリック側に SVI L3Out が必要です。リリース 5.2(3) 以降では、SVI L3Out のレイヤ3 マルチキャストがサポートされます。

L3Out SVI は、SVI が展開されているすべての境界リーフスイッチでレイヤ3 SVI インターフェイスが構成されているインターフェイスタイプです。SVI が設定されている L3Out で PIM が有効になっている場合、SVI の一部である境界リーフスイッチで PIM プロトコルが有効になります。すべての SVI は、相互に、および外部の PIM 対応デバイスと PIM 隣接関係を形成します。

L3Out からファイアウォールへのトポロジ例

次の図は、ファイアウォールへの L3Out のトポロジ例を示しています。



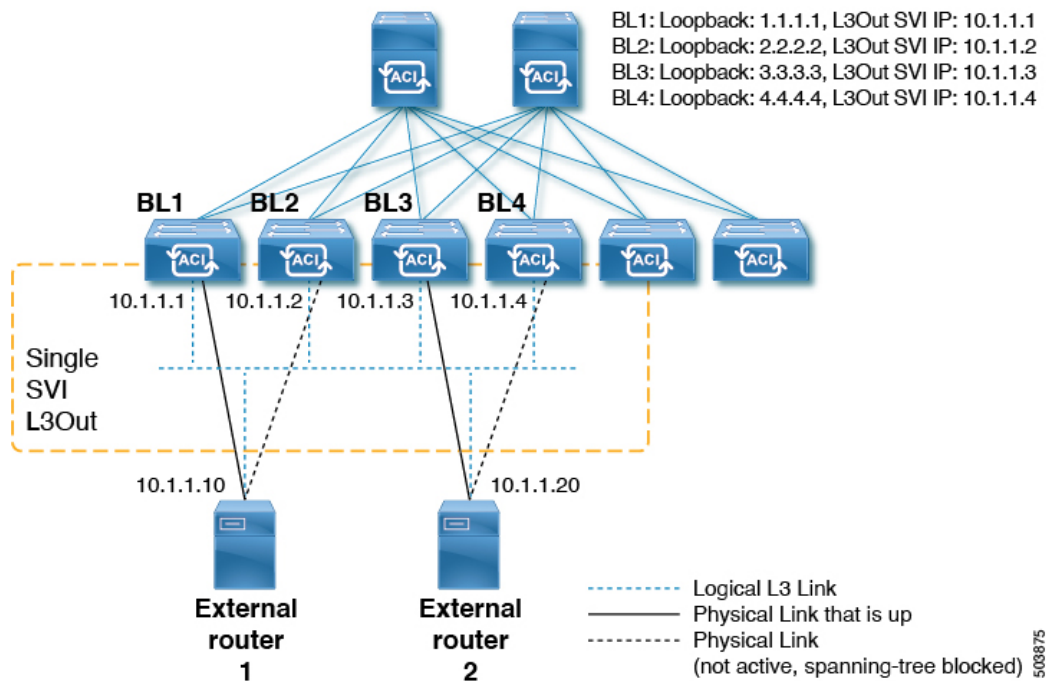
この例では、BL1、BL2 は、ファブリック上の境界リーフスイッチです。両方の境界リーフスイッチは、外部ファイアウォールに接続するのと同じ SVI L3Out 上にあります。各ファイアウォールは、ポートチャネル (非 vPC) を介して 2 つの境界リーフスイッチのいずれかに接続されます。

- 各境界リーフスイッチは、アクティブファイアウォールへの PIM ネイバー隣接関係を形成します。
- この例の BL2 は、L3Out 外部ブリッジドメインのファブリックトンネルを介してアクティブなファイアウォールにピアリングします。
- アクティブなファイアウォールは、BL1 と BL2 の両方に PIM 参加/プルーニングを送信できます。

- 2つの境界リーフスイッチの1つが PIM 加入をファイアウォールに送信します。ファイアウォールに向けて PIM Join を送信する境界リーフスイッチは、マルチキャストグループ（SSM のグループとソース）のストライプ勝者選択によって決定されます。
- BL2 は、マルチキャストグループのストライプ勝者として選択できます。トポロジ例の BL2 は、アクティブなファイアウォールに直接接続されていません。BL1 は BL2 に、ソースに直接接続されたリバースパスフォワーディング（RPF）であることを通知します。BL2 は BL1 経由で PIM を送信できます。BL2 は、ファイアウォールの IP アドレスの再帰ルックアップを実行できる必要があります。この機能は、接続されたホストの再配布機能によって提供されます。ファイアウォールサブネットに一致するルートマップは、L3Out での接続ホストの再配布用に構成する必要があります。

L3Out SVI から外部スイッチ/ルータへのトポロジ例

次の図は、外部スイッチまたはルータへの L3Out SVI のトポロジ例を示しています。



レイヤ3 マルチキャスト ステートおよびマルチキャスト データ トラフィックに関して、上記の図のコンポーネントは次のように影響を受けます。

- BL1、BL2、BL3、および BL4 は、ファブリック上の境界リーフスイッチです。これらの境界リーフスイッチはすべて、外部ボックスに接続する同じ SVI L3Out 上にあります。外部ボックスは、任意の外部スイッチまたはルータである可能性があります。
- 論理的には、レイヤ3 リンクは境界リーフスイッチと外部ルータの間でアップ状態です。したがって、SVI L3Out の境界リーフスイッチおよび外部ルータをまたがるユニキャストルーティングプロトコルまたは PIM に関して、フルメッシュ隣接関係が存在します。

- SVIL3Out はブリッジドメインであるため、境界リーフスイッチから外部ルータへの複数の物理接続がある場合でも、それらの間の1つのリンクだけがレイヤ2 レベルで各外部ルータにアップします。他のすべてのリンクは STP によってブロックされます。

たとえば、上の図では、レイヤ2 レベルの次のリンクだけがアップしています。

- BL1 と外部ルータ 1 間のリンク
- BL3 と外部ルータ 2 間のリンク

したがって、他のすべての境界リーフスイッチでは、IP アドレス 10.1.1.10 は BL1 を介してのみ到達可能であり、10.1.1.20 は BL3 を介してのみ到達可能です。

注意事項と制約事項

- PIM 対応の SVIL3Out には、接続されたホストルートマップを設定する必要があります。このルート マップは、直接接続されたすべての外部 PIM ネイバーと一致する必要があります。0.0.0.0/0 サブネットを使用できます。
- SVIL3Out 機能のレイヤ3 マルチキャストでは、次の領域がサポートされます。
 - サポート対象:
 - Protocol Independent Multicast (PIM) Any Source Multicast (ASM) および Source-Specific Multicast (SSM)
 - 物理インターフェイスを使用した SVI
 - ダイレクトポートチャネルを使用した SVI (非 vPC)
 - すべてのトポロジの組み合わせ:
 - Source Inside Receiver Inside (SIRI)
 - Source Inside Receiver Outside (SIRO)
 - Source Outside Outside Receiver Inside (SORI)
 - Source Outside Outside Receiver Outside (SORO)
 - サポート対象外:
 - SVIL3Out を介した VPC によるレイヤ3 マルチキャスト
 - SVI サブネットに直接接続された送信元または受信者ホスト (送信元または受信者ホストは SVIL3Out 上のルータの背後に接続されている必要があります)
 - ローカルリーフスイッチ (ACI メインデータセンタースイッチ) とリモートリーフスイッチ間のストレッチ SVIL3out はサポートされていません。
 - 複数のサイト (Cisco ACI マルチサイト) にまたがるストレッチ SVIL3Out
 - PIMv6 の SVIL3Out

- セカンダリ IP アドレス境界リーフ スイッチのセカンダリ IP アドレスに送信された場合、PIMの参加/プルーニングは処理されません。セカンダリ IP アドレスは、通常、静的ルーティング用の境界リーフ スイッチ間で共有 (仮想) IP アドレスを構成するために使用されます。PIM over SVI を設定するときはダイナミックルーティングを使用するか、各境界リーフ スイッチのプライマリ アドレスへのスタティック ルートを作成することをお勧めします。

GUI を使用した SVI L3Out 上のレイヤ3 マルチキャストの設定

ステップ1 レイヤ3 インターフェイス タイプとして [SVI] を設定した [L3Out の作成 (Create L3Out)] ウィザードを使用して、標準 L3Out を設定します。

- a) GUI の [ナビゲーション (Navigation)] ペインの、[テナント例 (Tenant Example)] で [ネットワーク (Networking)] [L3Out] の順に移動します。 >
- b) [L3Out の作成 (Create L3Out)] を右クリックして選択します。
- c) [L3Out の作成 (Create L3Out)] 画面の [識別 (Identity)] ウィンドウで、L3Out の名前を入力し、この L3Out に関連付ける VRF および L3 ドメインを選択します。
- d) [識別 (Identity)] ウィンドウに必要な情報を入力したら、[次へ (Next)] をクリックします。
[ノードとインターフェイス (Nodes and Interfaces)] ウィンドウが表示されます。
- e) [ノードとインターフェイス (Nodes and Interfaces)] ウィンドウの [インターフェイス タイプ: レイヤ 3 (Interface Types: Layer 3)] フィールドで、レイヤ3 インターフェイス タイプとして [SVI] を選択します。
- f) L3Out の設定が完了するまで、[L3Out の作成 (Create L3Out)] ウィザードを使用して個々のフィールドの設定を続けます。

ステップ2 設定された L3Out に移動します。

[テナント (Tenants)] > [tenant_name] > [ネットワーク (Networking)] > [L3Outs] > [L3Out_name]
設定された L3Out の [サマリー (Summary)] ページが表示されます。

ステップ3 [ポリシー (Policy)] タブをクリックし、次に [メイン (Main)] サブタブをクリックします。

設定された L3Out の [プロパティ (Properties)] ページが表示されます。

ステップ4 [再配布用のルート プロファイル (Route Profile for Redistribution)] フィールドで、[+] をクリックして再配布用のルート プロファイルを設定します。

ステップ5 [送信元 (Source)] フィールドで、[attached-host] を選択します。

ステップ6 [ルート マップ (Route Map)] フィールドで、すべてを許可するルート マップを設定します。

- a) [ルート制御のルート マップの作成 (Create Route Maps for Route Control)] をクリックします。
[ルート制御のルート マップの作成 (Create Route Maps for Route Control)] ウィンドウが表示されます。
- b) このルート マップの名前と説明を入力し、[コンテキスト (Contexts)] 領域で [+] をクリックします。
[ルート制御コンテキストの作成 (Create Route Control Context)] ウィンドウが表示されます。

- c) [ルート制御コンテキストの作成 (Create Route Control Context)] ウィンドウに必要なパラメータを設定し、[アクション (Action)] フィールドの値を [許可 (Permit)] に設定します。
- d) [関連付けられた一致ルール (Associated Match Rules)] 領域で [+] をクリックし、[ルートマップの一致ルールの作成 (Create Match Rule for a Route Map)] を選択して、このルート制御コンテキストの一致ルールを設定します。

[一致ルールの作成 (Create Match Rule)] ウィンドウが開きます。

- e) [一致プレフィックス (Match Prefix)] 領域で [+] をクリックします。
[一致ルート宛先ルールの作成 (Create Match Route Destination Rule)] ウィンドウが表示されます。
- f) [一致ルート宛先ルールの作成 (Create Match Route Destination Rule)] ウィンドウで、これらのフィールドに次の値を入力して、サブネットまたは 0.0.0.0/0 ルートおよび集約設定で一致する集約ルートをもつルールを設定します。

- IP : 0.0.0.0/0
- 集約 (Aggregate) : このフィールドのボックスをオンにします。[マスクより大きい (Greater Than Mask)] フィールドと [マスク未満 (Less Than Mask)] フィールドが表示されます。
- マスクより大きい : 0
- マスク未満 : 0

- g) [送信 (Submit)] をクリックして、この一致ルート宛先ルールを設定します。

ステップ7 すべてを許可するルートマップを設定したら、集約ルートまたは 0.0.0.0/0 ルートの集約エクスポートを行うエクスポートルート制御サブネットで外部EPGを設定します。

- a) 設定済みの外部 EPG に移動します。

[テナント (Tenants)] > [tenant_name] > [ネットワーキング (Networking)] > [L3Outs] > [L3Out_name] > [外部 EPG (External EPGs)] > [external_EPG_name]

設定された L3Out の [プロパティ (Properties)] ページが表示されます。デフォルトでは、[ポリシー/全般 (Policy / General)] ページが表示されます。

- b) [サブネット (Subnets)] 領域で、設定した 0.0.0.0/0 エントリをダブルクリックします。
設定されたサブネットの [プロパティ (Properties)] ウィンドウが表示されます。
- c) [ルート制御 (Route Control)] 領域で、次の項目を選択します。
 - [ルート制御サブネットのエクスポート (Export Route Control Subnet)] の隣のチェックボックスをオンにします。
 - [集約 (Aggregate)] 領域で、[エクスポートの集約 (Aggregate Export)] フィールドの横にあるボックスをオンにします。
- d) [送信 (Submit)] をクリックします。



第 13 章

マルチポッド

この章は、次の項で構成されています。

- [マルチポッドについて \(115 ページ\)](#)
- [マルチポッドのプロビジョニング \(116 ページ\)](#)
- [マルチポッド ファブリックの設定に関するガイドライン \(118 ページ\)](#)
- [マルチポッド ファブリックの設定 \(121 ページ\)](#)
- [Cisco Nexus 9000 シリーズ スイッチでのマルチポッド IPN 設定の例 \(125 ページ\)](#)
- [APIC を 1 つのポッドから別のポッドに移動する \(127 ページ\)](#)
- [OSPF IPN アンダーレイから BGP IPN アンダーレイへの移行 \(128 ページ\)](#)
- [マルチポッド スパインバックツーバック について \(130 ページ\)](#)

マルチポッドについて

マルチポッドは、隔離されたコントロールプレーンプロトコルを持つ複数のポッドで構成された、障害耐性の高いファブリックのプロビジョニングを可能にします。また、マルチポッドでは、さらに柔軟にリーフとスパインスイッチ間のフルメッシュ配線を行うことができます。たとえば、リーフスイッチが異なるフロアや異なる建物にまたがって分散している場合、マルチポッドでは、フロアごと、または建物ごとに複数のポッドをプロビジョニングし、スパインスイッチを通じてポッド間を接続することができます。

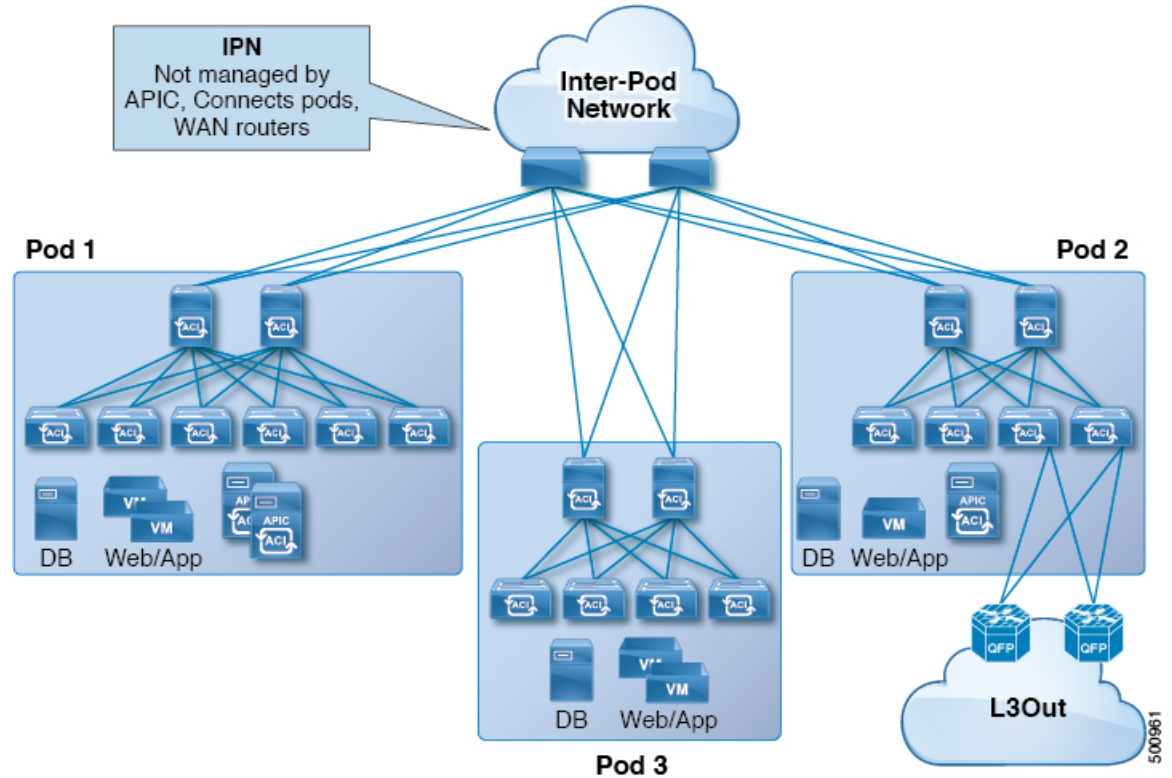
マルチポッドは、異なるポッドの ACI スパイン間のコントロールプレーン通信プロトコルとして MP-BGP EVPN を使用します。

Cisco APIC リリース 5.2(3) よりも前のリリースでは、物理スパインと IPN の間をピアリングするためにアンダーレイで OSPF が使用されます。Cisco APIC リリース 5.2(3) 以降、アンダーレイプロトコルは OSPF または BGP (eBGP のみ) または混合で、OSPF を使用するポッドと BGP を使用するポッドがあります。

WAN ルータは、ポッド間ネットワーク (IPN) でプロビジョニング可能で、スパインスイッチに直接接続されるか、境界リーフスイッチに接続されます。IPN に接続されるスパインスイッチは、ポッド内ので少なくとも 1 個のリーフスイッチに接続されます。

マルチポッドはすべてのポッドに単一の APIC クラスタを使用します。そのため、すべてのポッドが単一のファブリックとして機能します。ポッド全体にわたって個々の APIC コントローラが配置されますが、それらはすべて単一の APIC クラスタの一部です。

図 10: マルチポッドの概要



(注) Cisco APIC リリース 5.2(3) 以降、2つのポッドのみで構成されるファブリックは、IPN なしで直接接続できます。このマルチポッドスパインバックツーバックトポロジについては、[マルチポッドスパインバックツーバックについて \(130 ページ\)](#) を参照してください。

マルチポッドのプロビジョニング

IPN は APIC では管理されません。これは、次の情報が事前する必要があります。

- すべてのポッドの背表紙に接続されているインターフェイスを設定します。VLAN-4 でトラフィックをタグ付けするレイヤ3 サブインターフェイスを使用し、MTU をサイト間コントロールプレーンおよびデータプレーントラフィックに必要な最大 MTU より 50 バイト以上増やします。

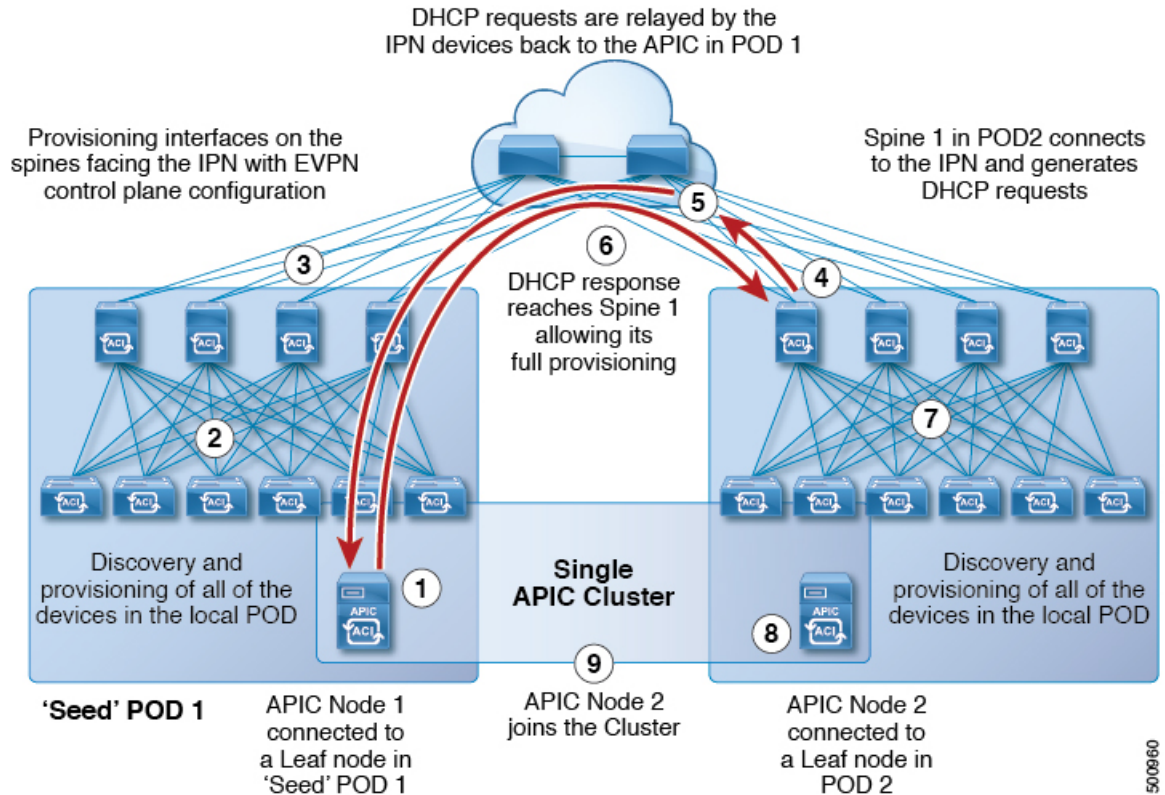
リモートリーフスイッチがいずれかのポッドに含まれている場合は、『Cisco ACI Remote Leaf Architecture White Paper』を参照してください。リモートリーフスイッチ (131 ページ) <https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-740861.html>

- IPN アンダーレイ プロトコルが OSPF の場合は、正しいエリア ID を持つサブインターフェイスで OSPF を有効にします。Cisco APIC リリース 5.2(3) 以降、IPN アンダーレイ プロトコルは OSPF または BGP (eBGP のみ) になることが可能です。
- すべての背表紙に接続されている IPN インターフェイスで DHCP リレーを有効にします。
- PIM をイネーブルにします。
- PIM 双方向としてブリッジドメイン GIPO 範囲の追加 (**bidir**) の範囲をグループ化 (デフォルトでは 225.0.0.0/15)。
グループを **bidir** モードが機能の転送を共有ツリーのみ。
- PIM として 239.255.255.240/28 を追加 **bidir** 範囲をグループ化します。
- PIM およびすべての背表紙に接続されたインターフェイスで IGMP を有効にします。



-
- (注) PIM **bidir** を展開する際には、どの時点であっても、特定のマルチキャストグループ範囲に対して、1つのアクティブな RP (ランデブーポイント) を設定することだけが可能です。RP の冗長性が活用することで実現するため、**ファントム RP** 設定します。希薄モードの冗長性を提供するために使用するエニーキャストまたは MSDP メカニズムはオプションではありませんマルチキャストソースの情報は、Bidir で利用可能なは不要であるため **bidir** 。
-

図 11: マルチポッドのプロビジョニング



マルチポッドファブリックの設定に関するガイドライン

マルチポッドファブリックを設定するには、次のガイドラインに従います。

- マルチポッドは次でサポートされます。
 - すべての ACI モード スパイン スイッチ
 - すべての Cisco Nexus 9000 シリーズ ACI モード リーフ スイッチ
 - すべての Cisco Nexus 9500 プラットフォーム ACI モード スイッチ ライン カードおよびファブリック モジュール
- 関連付けられたノードグループおよびレイヤ3アウトポリシーを作成します。
- スパインスイッチを変更する前に、マルチポッドトポロジに参加している運用「アップ」外部リンクが少なくとも1個あることを確認します。失敗すると、マルチポッド接続がダウンする可能性があります。
- セットアップを単一のポッド（ポッド1のみを含む）に変換する必要がある場合は、使用停止になっているポッドに接続されている APIC コントローラを再初期化し、ポッド1のリーフスイッチに接続する必要があります。マルチポッドは、初期セットアップスクリ

プトの実行後にクラスタに再参加できるようにします。手順については、[APIC を1つのポッドから別のポッドに移動する \(127 ページ\)](#) を参照してください。TEP プール設定を削除する必要があります。

- (ファブリック WAN のレイヤ 3 EVPN サービスとも呼ばれます)。Cisco ACI GOLF マルチポッドマルチポッド

GOLF の詳細については、[Cisco ACI GOLF \(449 ページ\)](#) を参照してください。

- ファブリックでは、APIC ノードは常に Pod 1 TEP プールからアドレス指定されるため、Pod 1 設定 (関連付けられている TEP プールを含む) は常に APIC 上に存在する必要があります。マルチポッドこれは、元の Pod 1 TEP プールがファブリックに追加される可能性のある他の Pod に再割り当てされないように、Pod 1 が物理的にデコミッションされるシナリオでも有効です。
- マルチポッドファブリック セットアップで、新しいスパイン スイッチがポッドに追加される場合、最初にポッド内の少なくとも 1 個のリーフ スイッチに接続する必要があります。これにより、APIC がスパイン スイッチを検出し、ファブリックに参加できるようにします。
- ポッドが作成されポッドにノードが追加された後、ポッドを削除するとファブリック内でアクティブなポッドから古いエントリになります。これは、APIC がオープンソース DHCP を使用しており、ポッドが削除されると APIC が削除できない一部のリソースを作成するため発生します。
- 個別のポッドに属するスパイン スイッチを直接バックツーバック リンクで接続すると、2 つのスパイン スイッチ間のピア インターフェイスで OSPF ネイバーシップが確立される場合があります。ピア インターフェイス間で不一致が発生し、いずれかのピアでダイレクトフラグが無効になっている場合、セッションは起動せず、転送は行われません。マルチポッドこの状況ではシステムが障害をスローしますが、これは予期された動作です。
- APIC リリース 2.2(2) 以前では、前方誤り訂正 (FEC) は、すべての 100G トランシーバがデフォルトで、デフォルトで有効です。QSFP-100G-LR4-S/QSFP-100G-LR4 トランシーバを設定に使用しないでください。マルチポッド ACI は、100G-LR4 光ファイバの FEC モードをデフォルトで有効にします。スパインが FEC モードを有効にできない IPN デバイスに接続する場合は、これらの光ファイバを使用するスパイン スイッチを使用しないでください。マルチポッド
- Cisco APIC リリース 5.2(3) 以降では、IPN アンダーレイ プロトコルを外部 BGP (eBGP) にすることができます。内部 BGP (iBGP) は、アンダーレイ プロトコルとしてサポートされていません。

OSPF と BGP の間で IPN アンダーレイとしてマルチポッド ファブリックを移行する準備をする場合は、次のガイドラインに従ってください。

- ACI ファブリックがクラウドサイトまたは GOLF ルータに接続されている場合、BGP アンダーレイはサポートされません。
- BGP アンダーレイは、IPv6 アドレス ファミリーではなく、IPv4 アドレス ファミリーのみをサポートします。

- Cisco APIC リリース 5.2(1) で導入された、レイヤ3 ネットワークを介したファブリックへの APIC クラスタ接続を展開する場合、IPN ネットワークは OSPF をアンダーレイ プロトコルとして使用するか、APIC がマルチポッドまたはリモート リーフ接続を提供するネットワークと同じネットワーク経路でファブリックに接続する場合は BGP アンダーレイを使用できます。
- ポリシーの名前を変更するなど、マルチポッド L3out を削除し再作成する場合、ファブリックのスパイン スイッチの一部でクリーン リロードを実行する必要があります。マルチポッド L3Out を削除することで、ファブリック内の1個以上のスパイン スイッチが APIC への接続を失う可能性があり、これらのスパイン スイッチが APIC から更新されたポリシーをダウンロードできなくなります。どのスパイン スイッチがそのような状態になるかは、展開されているトポロジによって異なります。この状態から回復するには、これらスパイン スイッチでクリーン リロードを実行する必要があります。スパイン スイッチでコマンドをリロードしたら、**setup-clean-config.sh** コマンドを使用してリロードを実行します。



(注) Cisco ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ3 Outside (L3Out) 接続、または Inter-Pod Network (IPN) を介したマルチポッド接続を設定する場合は、インターフェイス MTU がリンクの両端で適切に設定されていることが推奨されます。Cisco ACI、Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定可能な MTU 値はイーサネット ヘッダー (一致する IP MTU、14-18 イーサネット ヘッダー サイズを除く) を考慮していません。また、IOS XR などの他のプラットフォームには、設定された MTU 値にイーサネット ヘッダーが含まれています。設定された値が 9000 の場合、Cisco ACI、Cisco NX-OS Cisco IOS の最大 IP パケット サイズは 9000 バイトになりますが、IOS-XR のタグなしインターフェイスの最大 IP パケット サイズは 8986 バイトになります。

各プラットフォームの適切な MTU 値については、それぞれの設定ガイドを参照してください。

CLI ベースのコマンドを使用して MTU をテストすることを強く推奨します。たとえば、Cisco NX-OS CLI で `ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1` などのコマンドを使用します。

[システム (System)] > [システム設定 (System Settings)] > [コントロール プレーン MTU (Control Plane MTU)] のファブリックのノード (APIC および スイッチ) により送信された、コントロール プレーン (CP) のグローバル MTU を設定できます。

マルチポッド トポロジでは、ファブリック外部ポートの MTU 設定は CP MTU 値セット以上にする必要があります。そうしないと、ファブリックの外部ポートが CP MTU パケットをドロップする可能性があります。

IPN または CP MTU を変更する場合、CP MTU 値を変更し、次にリモートポッドのスパイン上の MTU 値を変更することをお勧めします。これで、MTU の不一致によりポッド間の接続が失われるリスクが減少します。これは、ポッド間の IPN デバイスのすべてのインターフェイスの MTU が、常にコントロールプレーンと VXLAN データプレーンの両方のトラフィックに十分

な大きさであることを保証するためです。データトラフィックの場合、VXLANによる余分な50バイトに注意してください。

ポッドをデコミッションするには、ポッドのすべてのノードをデコミッションします。詳細については、「Cisco APIC トラブルシューティングガイド」の「ポッドのデコミッションと再コミッション」を参照してください。

マルチポッドファブリックの設定

Cisco Application Policy Infrastructure Controller (APIC) 4.0(1)以降、GUIにウィザードが追加され、マルチポッド設定がシンプルになりました。GUIを使用してマルチポッドを設定するには、このセクションの手順に従います。

2つの物理ポッドの間にマルチポッドを設定する手順には、既存の物理ポッドが新しいポッドとインターポッドネットワーク (IPN) 経由で通信するための準備が含まれます。その後物理ポッドを追加したら、シスコ Cisco APIC がマルチポッドファブリックを作成します。

NX-OS スタイルの CLI と REST API を使用してマルチポッドを設定することもできます。手順については、このガイドの「[NX-OS CLI を使用したマルチポッドファブリックのセットアップ \(487 ページ\)](#)」および「[REST API を使用したマルチポッドファブリックのセットアップ \(568 ページ\)](#)」のセクションを参照してください。

IPN 接続のためのポッドの準備

新しいポッドを作成する前に、最初に、既存の物理ポッドから新しいポッドに通信できることを確認する必要があります。

ステップ 1 Cisco APICにログインします。

ステップ 2 [ファブリック (Fabric)] > [インベントリ (Inventory)] に移動します。

ステップ 3 [Quick Start] を展開し、[Add Pod] をクリックします。

ステップ 4 作業ペインで、[Add Pod] をクリックします。

ステップ 5 [Configure Interpod Connectivity STEP 1 > Overview] パネルで、ポッド間ネットワーク (IPN) 接続の設定に必要なタスクを確認し、[Get Started] をクリックします。

ステップ 6 [Configure Interpod Connectivity STEP 2 > IP Connectivity] ダイアログボックスで、次の手順を実行します。

- [L3 Outside 設定 (L3 Outside Configuration)] 領域の [名前 (Name)] フィールドがある場合、[名前 (Name)] ドロップダウンリストから既存のファブリック外部ルーティングプロファイルを選択します。
- [Spine ID] セレクタを使用して、スパインを選択します。
さらにスパインの ID を追加するには [+] (プラス記号) をクリックします。
- [Interfaces] 領域の [Interface] フィールドで、IPN への接続に使用されるスパインスイッチインターフェイス (スロットおよびポート) を入力します。

さらに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。

- d) [IPv4 Address] フィールドに、インターフェイスの IPv4 ゲートウェイ アドレスとネットワーク マスクを入力します。
- e) [MTU (bytes)] ドロップダウンリストで、外部ネットワークの最大伝送ユニットの値を選択します。範囲は 1500 ~ 9216 です。
- f) [次へ] をクリックします。

ステップ7 ポッド間接続の設定 **STEP 3> ルーティング プロトコル** ダイアログ ボックスで、物理スパインと IPN の間でピアリングするアンダーレイ プロトコルを設定します。Cisco APIC リリース 5.2(3) よりも前のリリースでは、Open Shortest Path First (OSPF) が唯一サポートされているアンダーレイです。これらの以前のリリース、または[アンダーレイ (Underlay)] として[OSPF]を選択した場合の以降のリリースでは、[OSPF] エリアで次のサブステップを実行します。

- a) [Use Defaults] をオンのままにするか、オフにします。
[デフォルトの使用 (Use Defaults)] チェックボックスをオンにすると、GUI は OSPF を設定するためのオプションフィールドを非表示にします。オフにした場合は、すべてのフィールドが表示されます。デフォルトでは、このチェックボックスはオフになっています。
- b) [Area ID] フィールドに OSPF エリア ID を入力します。
- c) [Area Type] 領域で、OSPF エリア タイプを選択します。
[NSSA エリア (NSSA area)] または [通常のエリア (Regular area)] から選択できます。スタブ エリアはサポートされていません。
- d) (オプション) [Area Cost] セレクタで、適切な OSPF エリア コスト値を選択します。このフィールドは、[デフォルトの使用 (Use Defaults)] チェックボックスがオフの場合にのみ表示されます。
- e) [Interface Policy] ドロップダウン リストで、OSPF インターフェイス ポリシーを選択するか設定します。
既存のポリシーを選択するか、[Create OSPF Interface Policy] ダイアログボックスでポリシーを作成できます。

ステップ8 Cisco APIC リリース 5.2(3) 以降、アンダーレイ プロトコルは OSPF または BGP になることが可能です。Cisco APIC リリース 5.2(3) より前のリリースの場合、または前の手順で[アンダーレイ (Underlay)] として[OSPF]を選択した場合は、この手順をスキップします。[ポッド間接続の設定 STEP 3> ルーティング プロトコル] ダイアログボックスで[アンダーレイ (Underlay)] として[BGP]を選択した場合、[BGP] エリアで、次の手順を実行して BGP アンダーレイを構成します。

MP-BGP エリアで、[デフォルトを使用] チェックボックスをオンのままにします。Multiprotocol Border Gateway Protocol (MP-BGP) を構成するための GUI のフィールドが非表示になります。

- a) [スパイン ID (Spine ID)]、[インターフェイス (Interface)]、および[IPv4 アドレス (IPv4 Address)] フィールドでは値は設定不可であることに注意してください。
- b) [ピア アドレス (Peer Address)] フィールドで、BGP ネイバーの IP アドレスを入力します。
- c) [リモート AS (Remote AS)] フィールドで、BGP ネイバーの自動システム (AS) 番号を入力します。
- d) [次へ] をクリックします。

ステップ9 [Configure Interpod Connectivity STEP 4> External TEP] ダイアログボックスで、次の手順を実行します。

- a) [Use Defaults] をオンのままにするか、オフにします。

[Use Defaults] チェックボックスをオンにすると、外部 TEP プールを設定するための GUI のオプションフィールドが非表示になります。オフにした場合は、すべてのフィールドが表示されます。デフォルトでは、このチェックボックスはオフになっています。

- b) [Pod] および [Internal TEP Pool] フィールドの設定できない値に注意してください。
- c) [External TEP Pool] フィールドに、物理ポッドの外部 TEP プールを入力します。
外部 TEP プールは、内部 TEP プール、または他のポッドに属する外部 TEP プールと重複しないようにする必要があります。
- d) [データプレーン TEP IP (Data Plane TEP IP)] フィールドに、ポッド間のトラフィックのルーティングに使用されるアドレスを入力します。このアドレスには、/32 サブネットマスクが必要です。
[外部 TEP プール (External TEP Pool)] を設定するときに生成されるデフォルトアドレスを受け入れることができます。別のアドレスを入力することもできますが、外部 TEP プールの外部にある必要があります。
- e) [ルータ ID (Router ID)] フィールドに、IPN ルータ IP アドレスを入力します。
- f) (オプション) [Loopback Address] フィールドに、IPN ルータループバック IP アドレスを入力します。
[Use Defaults] をオフにすると、Cisco APIC によって、[Unicast TEP IP] フィールドと [Spine ID] フィールドが設定できない状態で表示されます。
- g) [Finish] をクリックします。
[Summary] パネルが表示され、IPN 設定の詳細が表示されます。[View JSON] をクリックすると、REST API の設定を表示することもできます。REST API を保存して後で使用することができます。

次のタスク

次のいずれかを実行します。

- このまま直接ポッドの追加に進み、このガイドの「[マルチポッドファブリックを作成するポッドの追加 \(123 ページ\)](#)」の手順を続けることができます。
- [Configure Interpod Connectivity] ダイアログボックスを閉じてポッドを後で追加し、このガイドの「[マルチポッドファブリックを作成するポッドの追加 \(123 ページ\)](#)」の手順に戻ります。

マルチポッドファブリックを作成するポッドの追加

[物理ポッドの追加 (Add Physical Pod)] ダイアログを使用すると、マルチポッド環境を設定できます。新しい物理ポッド ID とトンネルエンドポイント (TEP) プールを定義します。また、新しいポッドネットワーク設定を行い、物理スパインのサブインターフェイスを設定します。

始める前に

ここまで次のタスクを実行しました。

- ノードグループおよび L3Out ポリシーが作成されました。

- ポッド間ネットワーク (IPN) を設定しました。設定の例については、このガイドの「[Cisco Nexus 9000 シリーズ スイッチでのマルチポッド IPN 設定の例 \(125 ページ\)](#)」を参照してください。
- 新しいポッドと IPN 経由で通信できるように既存のポッドを準備しました。このガイドの手順[IPN 接続のためのポッドの準備 \(121 ページ\)](#)を参照してください。
- IPN に接続するスパイン スイッチが、ポッド内にある少なくとも 1 個のリーフ スイッチにも接続することを確認しました。
- トンネルエンドポイント (TEP) プールを作成しました。このガイドの手順[IPN 接続のためのポッドの準備 \(121 ページ\)](#)を参照してください。

ステップ 1 Cisco Application Policy Infrastructure Controller (APIC) にログインします。

ステップ 2 次のいずれかを実行します。

- 手順「[IPN 接続のためのポッドの準備 \(121 ページ\)](#)」を完了して、まだ [Configure Interpod Connectivity] ダイアログボックスを閉じていない場合は、ステップ 3 ~ 5 を省略し、この手順のステップ 6 から再開します。
- 手順「[IPN 接続のためのポッドの準備 \(121 ページ\)](#)」を完了して、すでに [Configure Interpod Connectivity] ダイアログボックスを閉じた場合は、この手順のステップ 3 に進みます。

ステップ 3 [Fabric] > [Inventory] を選択します。

ステップ 4 [Quick Start] をクリックし、[Add Pod] をクリックします。

ステップ 5 作業ペインで、[Add Pod] をクリックします。

ステップ 6 [Add Physical Pod STEP 2 > Pod Fabric] ダイアログボックスで、次の手順を実行します。

a) [ポッド ID (Pod ID)] フィールドで、ポッド ID を選択します。

ポッド ID には任意の正の整数を指定できます。ただし、Cisco ACI ファブリック内で一意である必要があります。

b) [Pod TEP Pool] フィールドで、プールアドレスとサブネットを入力します。

ポッド TEP プールは、トラフィックのカプセル化識別子の範囲を表します。共有リソースであり、複数のドメインが使用できます。

c) [Spine ID] セレクタを使用して、スパイン ID を選択します。

複数のスパイン ID を選択するには [+] (プラス記号) アイコンをクリックします。

d) [Interfaces] 領域の [Interface] フィールドで、IPN への接続に使用されるスパイン スイッチ インターフェイス (スロットおよびポート) を入力します。

e) [IPv4 Address] フィールドに、インターフェイスの IPv4 ゲートウェイ アドレスとネットワーク マスクを入力します。

f) [MTU (bytes)] フィールドで、外部ネットワークの最大伝送ユニット (MTU) の値を選択します。

[+] (プラス記号) アイコンをクリックすると、もう 1 つのインターフェイスを設定できます。

ステップ7 [Add Physical Pod STEP 3 > External TEP] ダイアログボックスで、次の手順を実行します。

- a) [Use Defaults] チェックボックスをオンまたはオフのままにして、外部 TEP プールを設定するためのオプションフィールドを表示します。
- b) [Pod] フィールドと [Internal TEP Pool] フィールドの値はすでに設定済みであることがわかります。
- c) [External TEP Pool] フィールドに、物理ポッドの外部 TEP プールを入力します。
外部 TEP プールは内部 TEP プールと重ならないようにする必要があります。
- d) [Dataplane TEP IP] フィールドに、ポッド間のトラフィックのルーティングに使用されるアドレスを入力します。
- e) (オプション) [Unicast TEP IP] フィールドに、ユニキャスト TEP IP アドレスを入力します。

Cisco APIC によって、データプレーン TEP IP アドレスを入力するときにユニキャスト TEP IP アドレスが自動的に設定されます。

- f) (オプション) [Node] フィールドの値は設定できないことに注意してください。
- g) (オプション) [Router ID] フィールドに、IPN ルータ IP アドレスを入力します。

Cisco APIC によって、データプレーン TEP アドレスを入力するときにルータ IP アドレスが自動的に設定されます。

- h) [Loopback Address] フィールドに、ルータ ループバック IP アドレスを入力します。
ルータ IP アドレスを使用する場合は、[Loopback Address] は空白のままにします。
- i) [Finish] をクリックします。

Cisco Nexus 9000 シリーズ スイッチでのマルチポッド IPN 設定の例

Cisco APIC リリース 5.2(3) よりも前のリリースでは、IPN アンダーレイ プロトコルは OSPF です。Cisco APIC リリース 5.2(3) 以降、IPN アンダーレイ プロトコルは OSPF または BGP (eBGP のみ) になることが可能です。



- (注)
- ポッド間接続用の IPN での専用 VRF の展開はオプションですが、ベストプラクティスとして推奨されます。代わりにグローバルルーティングドメインを使用することもできます。
 - ip dhcp relay address 10.0.0.1 を示す設定例の領域では、この設定は Pod 1 の TEP プールが 10.0.0.0/x であるという前提に基づいています。

OSPF アンダーレイ プロトコルを使用した IPN の設定例

```
(pod1-spine1)-----2/7[ IPN-N9K ]2/9-----(pod2-spine1)

feature dhcp
feature pim

service dhcp
ip dhcp relay
ip pim ssm range 232.0.0.0/8

# Create a new VRF for Multipod.
vrf context fabric-mpod
  ip pim rp-address 12.1.1.1 group-list 225.0.0.0/15 bidir
  ip pim rp-address 12.1.1.1 group-list 239.255.255.240/28 bidir
  ip pim ssm range 232.0.0.0/8

interface Ethernet2/7
  no switchport
  mtu 9150
  no shutdown

interface Ethernet2/7.4
  description pod1-spine1
  mtu 9150
  encapsulation dot1q 4
  vrf member fabric-mpod
  ip address 201.1.2.2/30
  ip router ospf a1 area 0.0.0.0
  ip pim sparse-mode
  ip dhcp relay address 10.0.0.1
  ip dhcp relay address 10.0.0.2
  ip dhcp relay address 10.0.0.3
  no shutdown

interface Ethernet2/9
  no switchport
  mtu 9150
  no shutdown

interface Ethernet2/9.4
  description to pod2-spine1
  mtu 9150
  encapsulation dot1q 4
  vrf member fabric-mpod
  ip address 203.1.2.2/30
  ip router ospf a1 area 0.0.0.0
  ip pim sparse-mode
  ip dhcp relay address 10.0.0.1
  ip dhcp relay address 10.0.0.2
  ip dhcp relay address 10.0.0.3
  no shutdown

interface loopback29
  vrf member fabric-mpod
  ip address 12.1.1.1/32

router ospf a1
  vrf fabric-mpod
```

```
router-id 29.29.29.29
```

BGP アンダーレイ プロトコルを使用した IPN の設定例

Cisco APIC リリース 5.2(3) 以降、IPN アンダーレイ プロトコルは OSPF ではなく BGP になることが可能です。次の設定を前の例に追加し、OSPF 設定を削除できます。

```
router bgp 200
  router-id 29.29.29.29
  vrf fabric-mpod
  address-family ipv4 unicast
neighbor 201.1.2.3
  remote-as 65000
  address-family ipv4 unicast
  disable-peer-as-check
neighbor 203.1.2.3
  remote-as 65000
  address-family ipv4 unicast
  disable-peer-as-check
```

APIC を1つのポッドから別のポッドに移動する

マルチポッドのセットアップにおいて、APIC をあるポッドから別のポッドに移動するには、次の手順に従います。

ステップ1 クラスタ内の APIC をデコミッションします。

- メニューバーで、**System > Controllers** を選択します。
- Navigation** ウィンドウで、**Controllers > apic_controller_name > Cluster as Seen by Node** を展開します。
- Navigation** ウィンドウで、**apic_controller_name** をクリックします。これは、クラスタ内のものですが、デコミッションしているコントローラではありません。
- 継続する前に、**Work** ウィンドウで、クラスタの **Health State (Active Controllers サマリ テーブルに示されているもの)** が **Fully Fit** になっていることを確認します。
- Work** ウィンドウで、**Actions > Decommission** をクリックします。
- Yes** をクリックします。
解放されたコントローラは [Operational State] 列に [Unregistered] と表示されます。コントローラは稼働対象外になり、**Work** ウィンドウには表示されなくなります。

ステップ2 デコミッションされた APIC を目的のポッドに移動します。

ステップ3 次のコマンドを入力して、APIC をリブートします。

```
apic1# acidiag touch setup
apic1# acidiag reboot
```

ステップ4 APIC セットアップ スクリプトで、APIC ノードが移動されたポッド ID を指定します。

- Cisco Integrated Management Controller (CIMC) にログインします。

- b) ポッド ID のプロンプトで、ポッド ID を入力します。
- (注) **TEP Pool** のアドレス情報は変更しないでください。

ステップ5 APIC をリコミッションします。

- メニューバーで、**SYSTEM > Controllers** を選択します。
- Navigation** ウィンドウで、**Controllers > apic_controller_name > Cluster as Seen by Node** を展開します。
- 継続する前に、**Work** ウィンドウで、**Active Controllers** サマリ テーブルのクラスタの **Health State** が **Fully Fit** になっていることを確認します。
- Work** ウィンドウで、**Unregistered** と **Operational State** カラムに表示されている、デコミッションされたコントローラをクリックします。
- Work** ウィンドウで、**Actions > Commission** をクリックします。
- Confirmation** ダイアログボックスで **Yes** をクリックします。
- コミッションされた Cisco APIC コントローラが動作状態であり、ヘルス ステータスが、**Fully Fit** であることを確認します。

OSPF IPN アンダーレイから BGP IPN アンダーレイへの移行

Cisco APIC リリース 5.2(3) 以降、IPN アンダーレイ プロトコルは OSPF または BGP になることが可能です。ポッドを OSPF アンダーレイの使用から BGP アンダーレイに移行するには、既存の IPN 接続 L3Out の下の論理インターフェイス プロファイルに BGP インターフェイスを追加します。そのインターフェイスが実行中の BGP ピアに正常に接続されたら、OSPF インターフェイス プロファイルを削除できます。



- (注) OSPF と BGP の両方が Multi-Pod、Multi-Site、または リモート リーフのアンダーレイで使用されている場合、IPN ルータの OSPF から router-id を BGP に再配布しないでください。そうすると、ルーティンググループが生じ、スパインスイッチと IPN ルータの間の OSPF と BGP セッションを停止してしまいます。



- (注) アンダーレイ プロトコルの移行は中断を伴うアクションであり、メンテナンス期間中のみ実行する必要があります。

ステップ1 APIC メニューバーから、[テナント (Tenants)] > [インフラ (infra)] > [ネットワーキング (Networking)] > [L3Outs] > [使用する IPN L3Out (your IPN L3Out)] に移動します。ここで、[使用する IPN L3Out (your IPN L3Out)] は IPN に接続する L3Out です。

- ステップ 2** [Navigation] ペインで、[使用する *IPN L3Out* (*your IPN L3Out*)] を展開し [論理ノード プロファイル (Logical Node Profiles)] > [使用する *IPN* ノード プロファイル (*your IPN node profile*)] > [論理インターフェイス プロファイル (Logical Interface Profiles)] > [使用する *IPN* インターフェイス (*your IPN interface*)] に移動します。ここで [使用する *IPN* インターフェイス (*your IPN interface*)] は現在の IPN 接続の論理インターフェイス プロファイルです。
- [論理インターフェイスプロファイル (Logical Interface Profile)] テーブルが作業ペインに表示されます。
- ステップ 3** 作業ウィンドウで、[ポリシー (Policy)] タブをクリックし、[ポリシー (Policy)] タブの下にある [ルーテッドサブインターフェイス (Routed Sub-Interfaces)] タブをクリックします。
- ステップ 4** [ルーテッドサブインターフェイス (Routed Sub-Interfaces)] テーブルで、現在の IPN 接続のインターフェイスをダブルクリックします。
- [ルーテッドサブインターフェイス (Routed Sub-Interface)] ダイアログ ボックスが開きます。
- ステップ 5** [ルーテッドサブインターフェイス (Routed Sub-Interface)] ダイアログ ボックスで、次の操作を実行します:
- [BGPピア接続プロファイル (BGP Peer Connectivity Profiles)] バーの [+] アイコンをクリックして、BGP ピア接続を追加します。
- [ピア接続プロファイルの作成 (Create Peer Connectivity Profiles)] ダイアログ ボックスが開きます。
- [ピア IPv4 アドレス (Peer IPv4 Address)] フィールドで、BGP ピアの IP アドレスを入力します。
 - BGP ピア接続に必要なその他の設定を行います。
- (注) 移行を設定しているが、実際には移行していない場合は、[管理状態 (Admin State)] を [無効化 (Disabled)] に設定し、移行の準備ができたならこの手順に戻ります。移行はメンテナンス期間中に行う必要があります。
- [送信 (Submit)] をクリックして、[ルーテッドサブインターフェイス (Routed Sub-Interface)] ダイアログ ボックスに戻ります。
- ステップ 6** [ルーテッドサブインターフェイス (Routed Sub-Interface)] ダイアログ ボックスで、[送信 (Submit)] をクリックします。
- ステップ 7** [ナビゲーション (Navigation)] ペインで、[論理ノード プロファイル (Logical Node Profiles)] > [使用する *IPN* ノード プロファイル (*your IPN node profile*)] > [設定済みノード (Configured Nodes)] > [使用する *IPN* ノード (*your IPN node*)] に移動します。次の手順に従って、BGP ネイバーが UP であることを確認します。
- [使用する *IPN* ノード (*your IPN node*)] を展開し、[VRF-overlay-1 の BGP (BGP for VRF-overlay-1)] などの BGP エントリを見つけます。
 - [BGP] エントリを展開し、[ネイバー (Neighbors)] をクリックします。
 - [ネイバー (Neighbors)] テーブルで、[ピア IPv4 アドレス (Peer IPv4 Address)] で設定したピア IP アドレスを検索し、[状態 (State)] が「established」であることを確認します。
- ステップ 8** [ナビゲーション (Navigation)] ペインで、[論理インターフェイス プロファイル (Logical Interface Profile)] の下で現在の OSPF Interface Profile を右クリックして [削除 (Delete)] を選択します。
- (注) OSPF インターフェイス プロファイルを削除する前に、BGP ネイバーが UP であることを確認します。

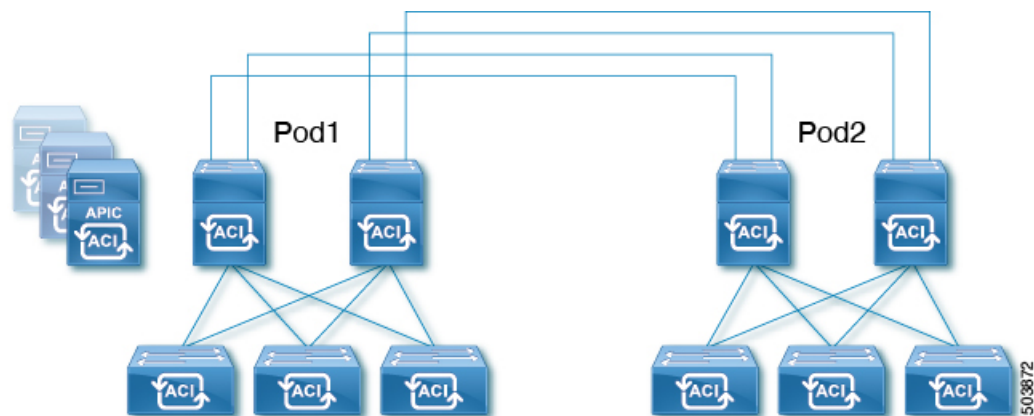
- ステップ9 [ナビゲーション (Navigation)]ペインで、[テナント (Tenants)]>[インフラ (infra)]>[ネットワーキング (Networking)]>[L3Outs]>[使用する IPN L3Out (your IPN L3Out)]に移動します。
- ステップ10 作業ウィンドウで、[ポリシー (Policy)]タブをクリックし、[ポリシー (Policy)]タブの下の [メイン (Main)]タブをクリックします。
- ステップ11 作業ウィンドウの [BGP/EIGRP/OSPF の有効化 (Enable BGP/EIGRP/OSPF)]セクションで、[OSPF] をオフにし、[BGP] をオンのままにします。
- ステップ12 [送信 (Submit)]をクリックします。

マルチポッドスパインバックツーバックについて

Cisco APIC リリース 5.2(3) 以降、ACI マルチポッドアーキテクチャが拡張され、2つのポッドのスパインをバックツーバック (「B2B」) リンクで直接接続できるようになりました。このソリューションを呼び出すと、小規模なACIマルチポッドの導入でIPN要件を削除できます。また、設定が必要な外部デバイスがないため、運用の簡素化とエンドツーエンドのファブリックの可視性も実現します。マルチポッドスパインバックツーバックマルチポッドスパインバックツーバック

トポロジでは、バックツーバック スパイン インターフェイスがインフラ テナントの L3Outとして実装されます。マルチポッドスパインバックツーバックこれらのリンクは通常、ポッド間の直接ケーブル接続またはダークファイバ接続で伝送されます。は、異なるポッドに属するスパインスイッチ間の Open Shortest Path First (OSPF) 接続のみをサポートします。マルチポッドスパインバックツーバック

次の図は、Pod1 と Pod2 の間にバックツーバック スパインが接続されたトポロジを示しています。マルチポッドスパインバックツーバック



詳細については、シスコのナレッジベース記事「Cisco ACI Multi-Podスパインバックツーバック」を参照してください。マルチポッドスパインバックツーバック <https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/kb/cisco-multipod-b2b.html>



第 14 章

リモート リーフ スイッチ

この章は、次の内容で構成されています。

- [ACI ファブリックのリモート リーフ スイッチについて \(131 ページ\)](#)
- [リモート リーフ スイッチのハードウェアの要件 \(140 ページ\)](#)
- [リモート リーフ スイッチの制約事項と制限事項 \(141 ページ\)](#)
- [WAN ルータとリモート リーフ スイッチ設定の注意事項 \(144 ページ\)](#)
- [GUI を使用してリモート リーフ スイッチのポッドとファブリック メンバーシップを設定する \(147 ページ\)](#)
- [ダイレクト トラフィック フォワーディングについて \(159 ページ\)](#)
- [リモート リーフ スイッチのフェールオーバー \(165 ページ\)](#)
- [リモートのリーフ スイッチのダウングレードする前に必要な前提条件 \(168 ページ\)](#)

ACI ファブリックのリモート リーフ スイッチについて

ACI ファブリックの展開では、ローカルスパインスイッチまたは APIC が接続されていない Cisco ACI リーフスイッチのリモートデータセンターに、ACI サービスと APIC 管理を拡張できません。

リモート リーフ スイッチがファブリックの既存のポッドに追加されます。メインデータセンターに展開されるすべてのポリシーはリモートスイッチで展開され、ポッドに属するローカルリーフスイッチのように動作します。このトポロジでは、すべてのユニキャストトラフィックはレイヤ 3 上の VXLAN を経由します。レイヤ 2 ブロードキャスト、不明なユニキャスト、マルチキャスト (BUM) メッセージは、WAN を使用するレイヤ 3 マルチキャスト (bidirectional PIM) を使用することなく、Head End Replication (HER) トンネルを使用して送信されます。スパインスイッチプロキシを使用する必要があるすべてのトラフィックは、メインデータセンターに転送されます。

APIC システムは、起動時にリモート リーフ スイッチを検出します。その時点から、ファブリックの一部として APIC で管理できます。



- (注)
- すべての inter-VRF トラフィック（リリース 4.0(1) 以前）は、転送される前にスパインスイッチに移動します。
 - リリース 4.1(2) 以前では、リモートリーフを解除する前に、vPC を最初に削除する必要があります。

リリース 4.0(1) でのリモートリーフスイッチの動作の特性

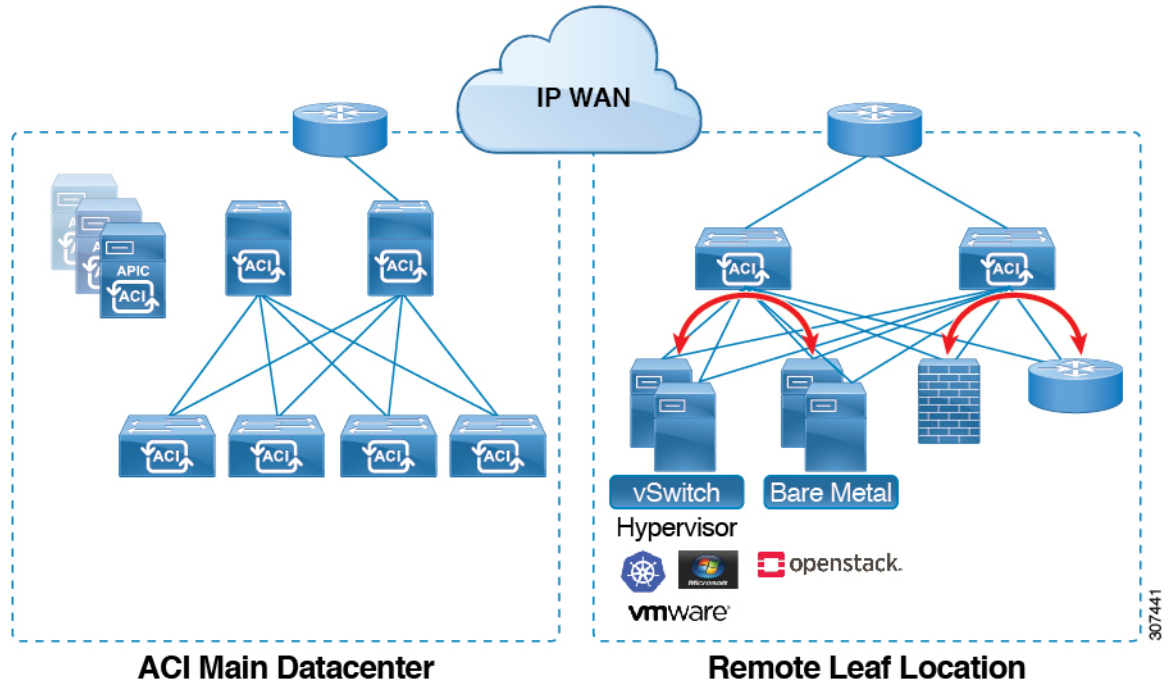
リリース 4.0(1) 以降、リモートリーフスイッチの動作には次の特徴があります。

- spine-proxy からサービスを切り離すことによって WAN 帯域幅の使用量を削減します。
 - PBR：ローカル PBR デバイスまたは vPC の背後にある PBR デバイスでは、ローカルスイッチングはスパインプロキシに移動せずに使用されます。ピアリモートリーフ上の孤立ポートの PBR デバイスでは、RL-vPC トンネルを使用します。これは、主要 DC へのスパインリンクが機能しているか否かを問わず該当します。
 - ERSPAN：ピア接続先 EPG では、RL-vPC トンネルが使用されます。ローカルな孤立ポートまたは vPC ポート上の EPG は、宛先 EPG へのローカルスイッチングを使用します。これは、主要 DC へのスパインリンクが機能しているか否かを問わず該当します。
 - 共有サービス：パケットはスパインプロキシパスを使用しないため WAN 帯域幅の使用量を削減します。
 - Inter-VRF トラフィックは上流に位置するルータ経由で転送され、スパインには配置されません。
 - この機能強化は、リモートリーフ vPC ペアにのみ適用されます。リモートリーフペアを介した通信では、スパインプロキシは引き続き使用されます。
- spine-proxy に到達不能な場合のリモートリーフロケーション内の（ToR グリーニングプロセスを通じた）不明な L3 エンドポイントの解像度。

リリース 4.1(2) でのリモートリーフスイッチ動作の特性

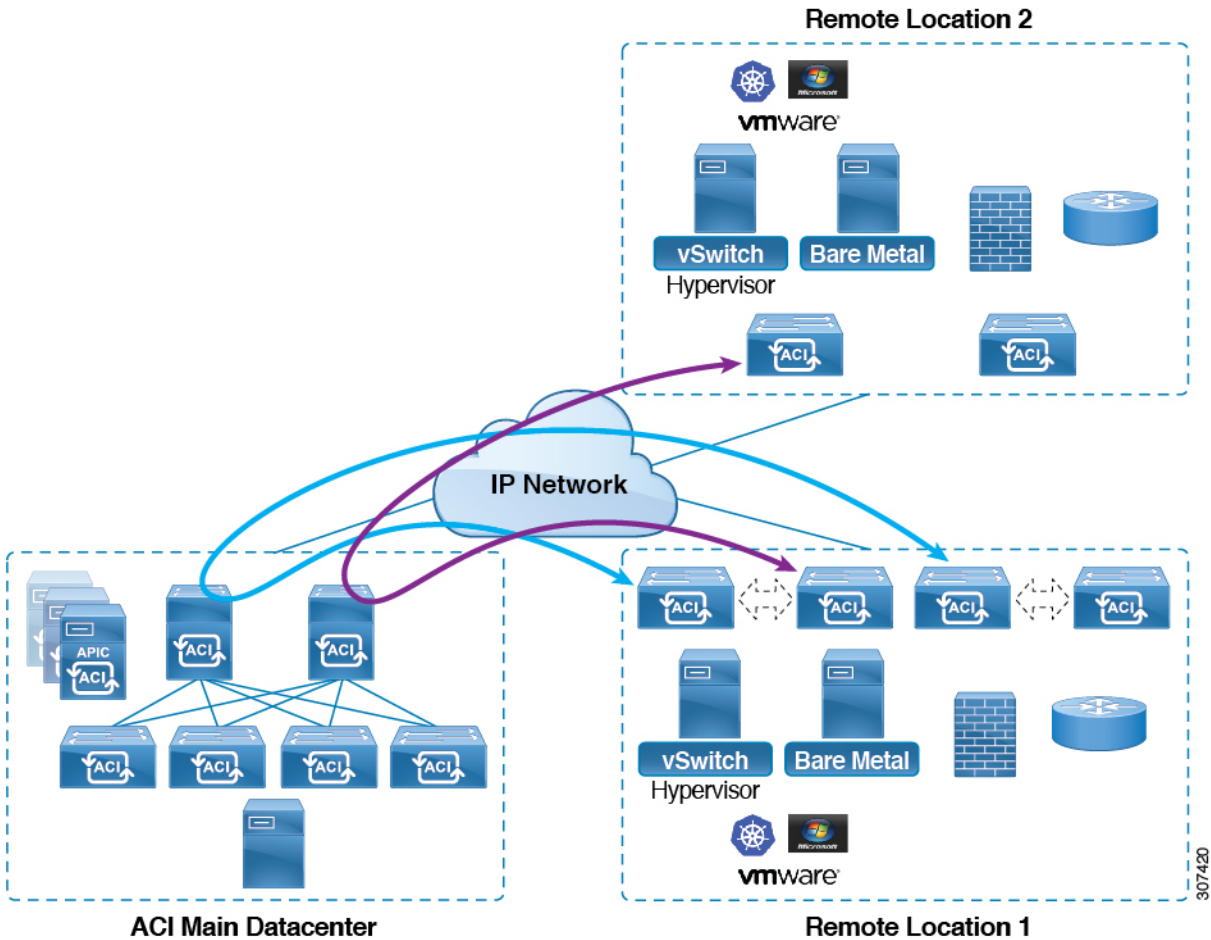
リリース 4.1(2) よりも前のリリースでは、次の図に示すように、リモートリーフロケーション上のすべてのローカルスイッチング（リモートリーフ vPC ピア内）トラフィックは、物理的または仮想的にエンドポイント間で直接スイッチングされます。

図 12: Local Switching Traffic : リリース 4.1(2) 以前



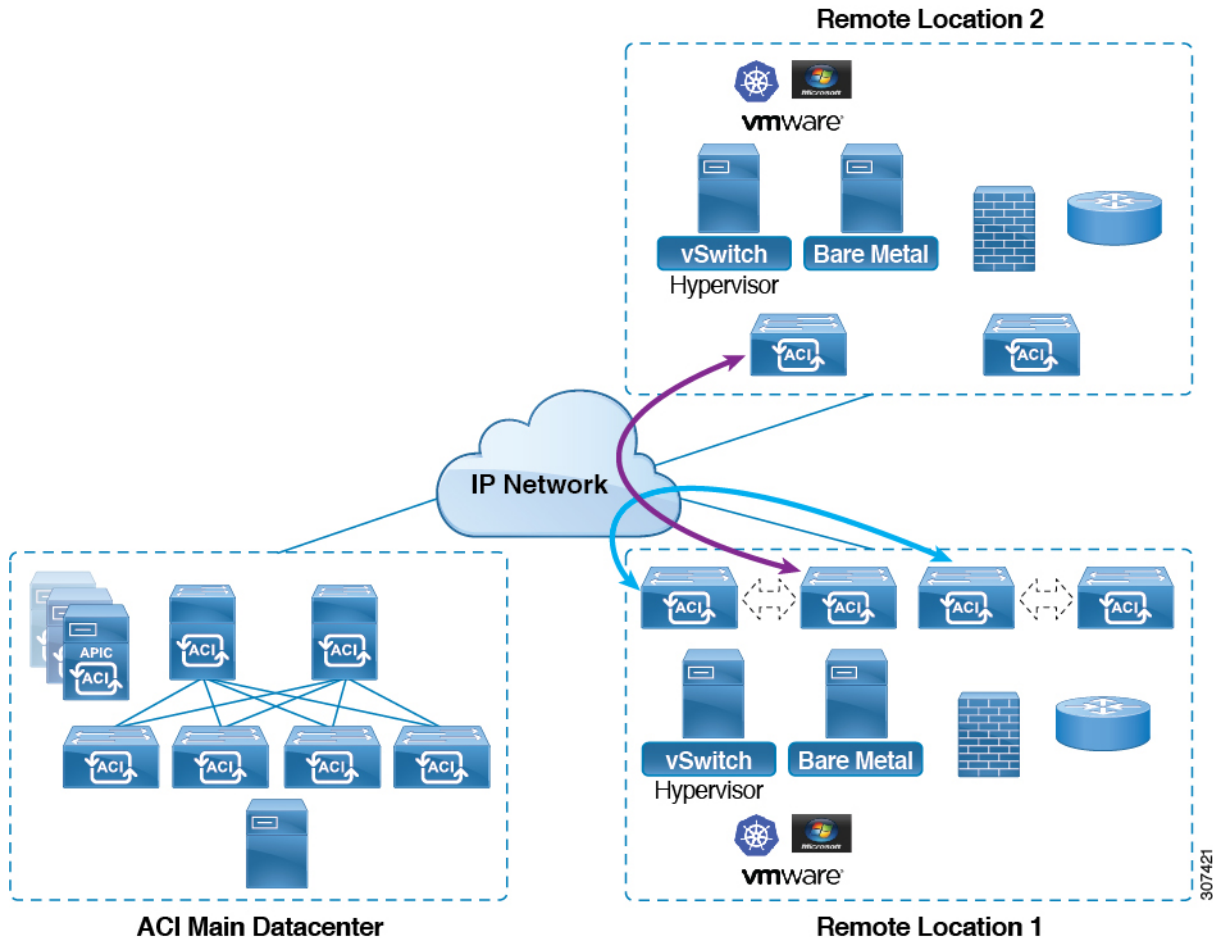
さらに、リリース4.1(2)よりも前では、次の図に示すように、リモートロケーション内またはリモートロケーション間のリモートリーフスイッチvPCペア間のトラフィックは、ACIメインデータセンターポッドのスパインスイッチに転送されます。

図 13: Remote Switching Traffic : リリース 4.1(2) より以前



リリース 4.1(2) 以降では、異なるリモートロケーションにあるリモートリーフスイッチ間の直接トラフィック転送がサポートされるようになりました。この機能は、次の図に示すように、リモートロケーション間の接続に一定レベルの冗長性と可用性を提供します。

図 14 : Remote Leaf Switch Behavior : リリース 4.1(2)



また、リリース 4.1(2) 以降でも、リモートリーフスイッチの動作には次の特徴があります。

- リリース 4.1(2) 以降、ダイレクトトラフィック転送では、シングルポッド設定内でスパインスイッチに障害が発生すると、次のようになります。
 - ローカルスイッチングは、上記の「ローカルスイッチングトラフィック：リリース 4.1(2) 以前」に示すように、リモートリーフスイッチ vPC ピア間の既存および新規のエンドポイントトラフィックに対して機能し続けます。
 - リモートロケーション間のリモートリーフスイッチ間のトラフィックの場合：
 - リモートリーフスイッチからスパインスイッチへのトンネルがダウンするため、新しいエンドポイントトラフィックは失敗します。リモートリーフスイッチから、新しいエンドポイントの詳細はスパインスイッチに同期されないため、同じまたは異なる場所にある他のリモートリーフスイッチペアは、COOP から新しいエンドポイント情報をダウンロードできません。
 - 単方向トラフィックの場合、既存のリモートエンドポイントは300秒後にエージングアウトするため、そのポイント以降のトラフィックは失敗します。ポッド内

のリモートリーフサイト内（リモートリーフ VPC ペア間）の双方向トラフィックは更新され、引き続き機能します。リモートロケーション（リモートリーフスイッチ）への双方向トラフィックは、900 秒のタイムアウト後に COOP によってリモートエンドポイントが期限切れになるため、影響を受けることに注意してください。

- 共有サービス（VRF 間）の場合、同じポッド内の 2 つの異なるリモートロケーションに接続されたリモートリーフスイッチに属するエンドポイント間の双方向トラフィックは、リモートリーフスイッチ COOP エンドポイントのエージェアウト時間（900 秒）後に失敗します。これは、リモートリーフスイッチからスパインへの COOP セッションがこの状況でダウンするためです。ただし、2 つの異なるポッドに接続されたリモートリーフスイッチに属するエンドポイント間の共有サービストラフィックは、COOP 高速エージングタイムである 30 秒後に失敗します。
- スパインスイッチへの BGP セッションがダウンするため、L3Out 間通信は続行できません。
- トラフィックが 1 つのリモートリーフスイッチから送信され、別のリモートリーフスイッチ（送信元の vPC ピアではない）に送信されるリモートリーフ直接単方向トラフィックがある場合は、300 秒のリモートエンドポイント（XREP）タイムアウトが発生するたびに、ミリ秒単位のトラフィック損失が発生します。
- ACI Multi-Site 設定を使用したリモートリーフスイッチでは、スパインスイッチに障害が発生しても、リモートリーフスイッチから他のポッドおよびリモートロケーションへのすべてのトラフィックが継続します。これは、この状況ではトラフィックが代替の使用可能なポッドを通過するためです。

リモートリーフスイッチの IPN での 10 Mbps 帯域幅のサポート

リモートリーフスイッチからのデータトラフィックのほとんどがローカルで、ポッド間ネットワーク（IPN）が管理目的でのみ必要な場合があります。このような状況では、100 Mbps の IPN は必要ない場合があります。これらの環境をサポートするために、リリース 4.2(4) 以降、IPN の最小帯域幅として 10 Mbps のサポートが利用可能になりました。

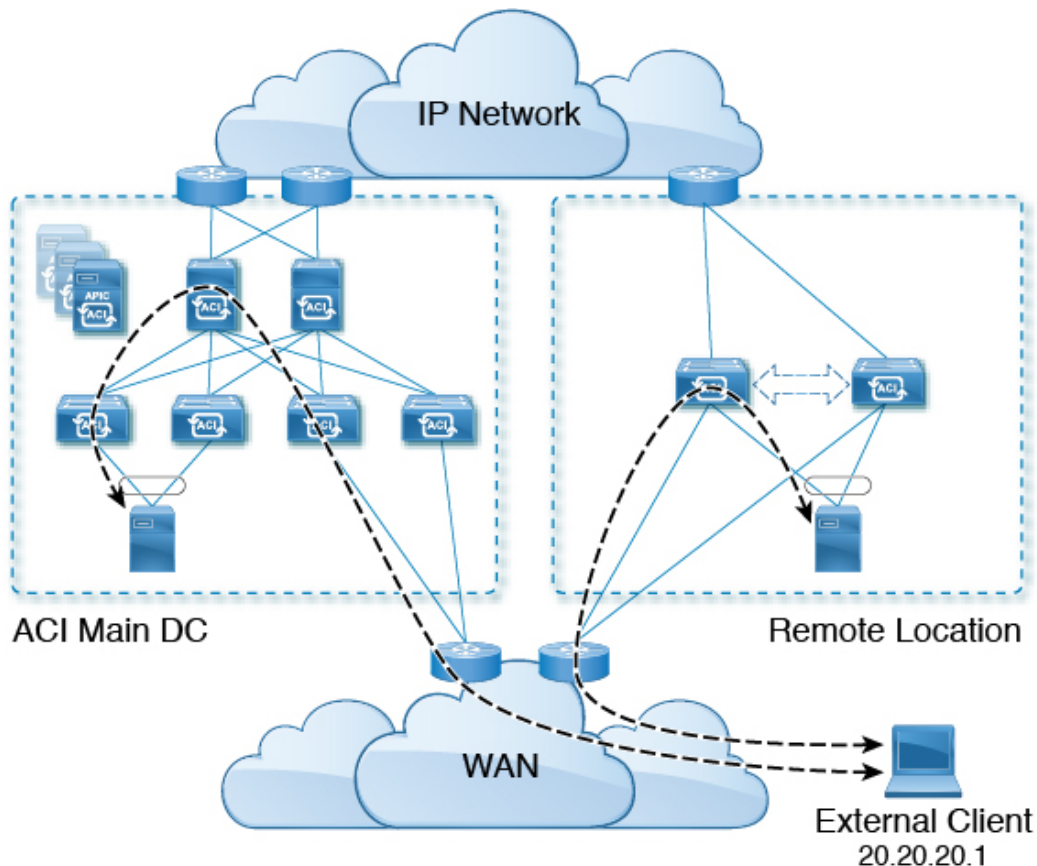
これをサポートするには、次の要件を満たす必要があります。

- IPN パスは、リモートリーフスイッチ（アップグレードおよびダウングレード、ディスクバリ、COOP、ポリシープッシュなどの管理機能）の管理にのみ使用されます。
- 「Cisco APIC GUI を使用した DSCP 変換ポリシーの作成」の項に記載されている情報に基づいて、Cisco ACI データセンターとリモートリーフスイッチペア間のコントロールおよび管理プレーントラフィックに優先順位を付けるために、QoS 設定を使用して IPN を設定します。
- データセンターおよびリモートリーフスイッチからのすべてのトラフィックは、ローカル L3Out を経由します。Cisco ACI

- EPGまたはブリッジドメインは、リモートリーフスイッチとACIメインデータセンター間で拡張されません。
- アップグレード時間を短縮するには、リモートリーフスイッチにソフトウェアイメージを事前にダウンロードする必要があります。

次の図に、この機能のグラフィカル表示を示します。

図 15: リモートリーフスイッチ動作 (リリース 4.2(4)) : IPNでのリモートリーフスイッチの管理

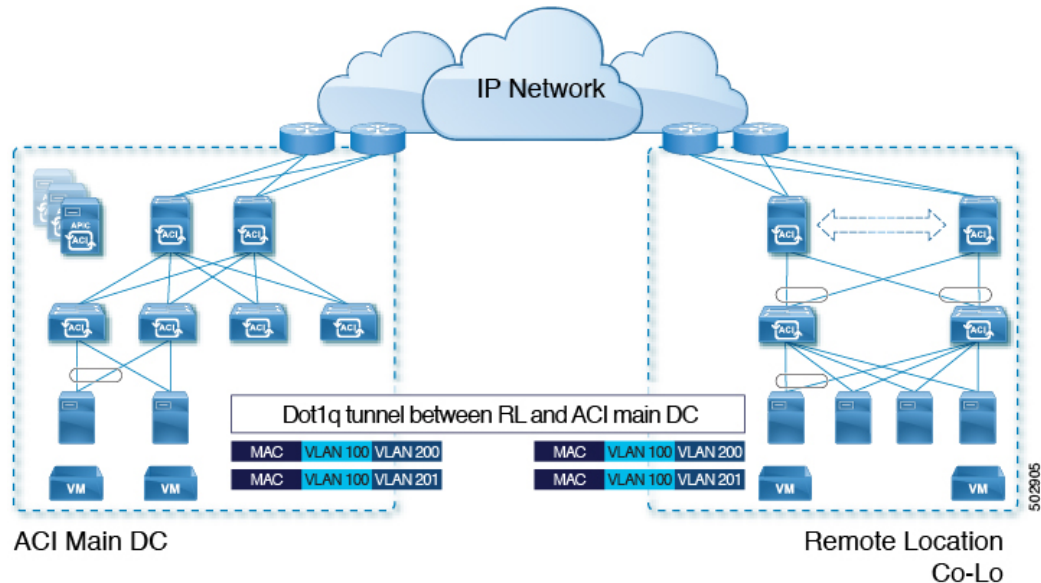


リモートリーフスイッチでの Dot1q トンネルのサポート

状況によっては、コロケーションプロバイダーが複数の顧客をホストしており、各顧客がリモートリーフスイッチペアごとに数千のVLANを使用している場合があります。リリース 4.2(4)以降では、リモートリーフスイッチとACIメインデータセンター間に 802.1Q トンネルを作成するためのサポートを利用できます。これにより、複数のVLANを単一の 802.1Q トンネルに柔軟にマッピングできるため、EPGの拡張要件が軽減されます。

次の図に、この機能のグラフィカル表示を示します。

図 16: リモートリーフスイッチの動作、リリース 4.2 (4) : リモートリーフスイッチでの 802.1Q トンネルサポート



Cisco APIC ドキュメンテーションのランディングページにある『Cisco APIC Layer 2 Networking Configuration Guide』の「802.1Q Tunnels」の章に記載されている手順を使用して、リモートリーフスイッチと ACI メインデータセンター間にこの 802.1Q トンネルを作成します。

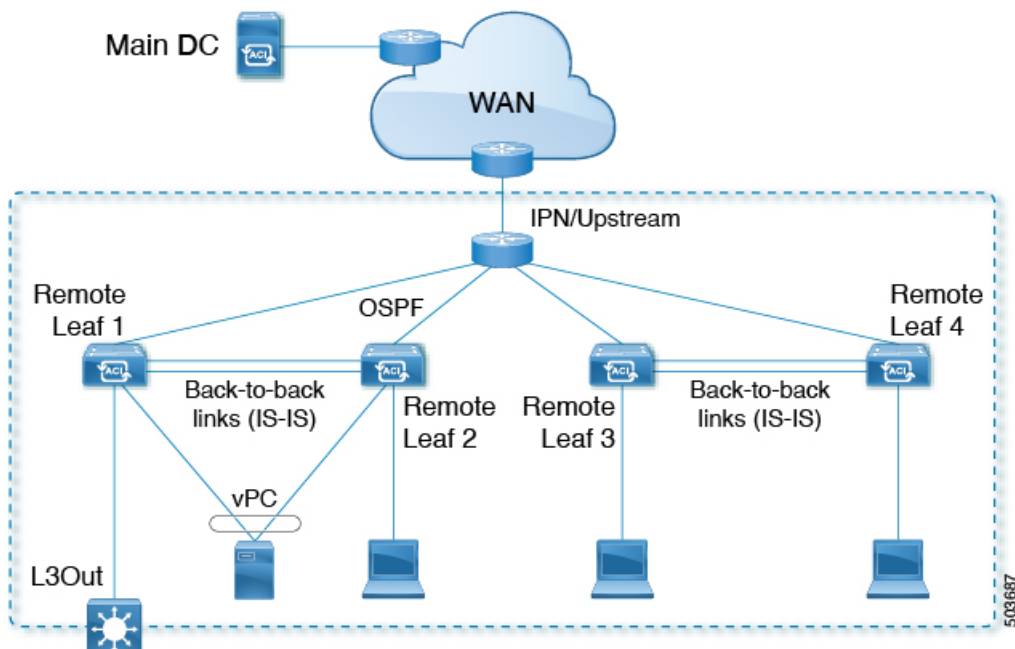
<https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>

ウィザードを使用するか（使用しない場合も）、REST API または NX-OS スタイル CLI を使用して、APIC GUI のリモートリーフスイッチを設定できます。

リモートリーフバックツーバック接続について

Cisco APIC リリース 5.2(1) 以降では、ファブリックリンクによってリモートリーフスイッチペアを相互に直接接続（「バックツーバック」）して、ローカルの東西トラフィックを伝送できます。重要な東西データトラフィックのシナリオの例は、次の図に示すように、vPC ペアの EPG から L3Out へのユニキャストトラフィックです。

図 17: リモートリーフバックツーバック接続



非 vPC 接続ホスト間のトラフィックのみがバックツーバックリンクを通過します。vPC に接続されたホストは、宛先に最も近いリモートリーフスイッチからローカルにトラフィックを送信できるため、このようなトラフィックはバックツーバックリンクを使用しません。

リモートリーフスイッチのペア間でアップリンクとバックツーバック接続がアクティブな場合、バックツーバックリンクが東西トラフィックに優先されますが、アップリンクは、主要なデータセンターにある他のリモートリーフスイッチおよびスイッチとの間でトラフィックを伝送します。

リモートリーフアーキテクチャでは、通常、隣接するリモートリーフスイッチ間でトラフィックをルーティングするためにスパインスイッチまたは IPN ルータが必要ですが、直接バックツーバックリーフ接続を使用すると、アップストリームデバイスの帯域幅を節約できます。

リモートリーフバックツーバック接続のガイドラインと制限事項

- リモートリーフスイッチ間のバックツーバックリンクは、中間デバイスのない直接リンクである必要があります。
- バックツーバック接続では、ファブリックポートまたはファブリックポートに変換された前面パネルポートを使用できます。
- リモートリーフスイッチは、ペアでのみバックツーバックリンクで接続できます。バックツーバックリンクによる3つ以上のリモートリーフスイッチの相互接続はサポートされていません。
- リモートリーフスイッチのペアがバックツーバックで接続され、ペアの1つがアップリンク接続を失った場合、同じリモートリーフスイッチは、バックツーバックリンクを介

して他のリモートリーフスイッチ経由で到達可能になります。この場合、メインデータセンターからのトラフィックもバックツーバックリンクで伝送されます。

- PTP および SyncE は、バックツーバックリンクではサポートされません。

リモートリーフバックツーバック接続の展開

Cisco APIC リリース 5.2(1) よりも前のリリースでは、リモートリーフスイッチファブリックポート間のバックツーバック接続により、配線エラーが発生しました。Cisco APIC リリース 5.2(1) では、次のいずれかの状況でこのような接続が自動的に認識されます。

- 2つのリモートリーフvPCピア間で接続が確立されます。
- 接続は、単一のリモートロケーションにあるvPCのメンバーではないリモートリーフスイッチ間で行われます。

このような場合、特別な設定は必要ありません。

リモートリーフスイッチのハードウェアの要件

リモートリーフスイッチの機能には、次のスイッチがサポートされています。

ファブリックスパインスイッチ

WAN ルータに接続された ACI メインデータセンターにスパインスイッチでの次のスパインスイッチがサポートされています。

- 固定スパインスイッチ Cisco Nexus 9000 シリーズ
 - N9K-C9316D-GX
 - N9K-C9332C
 - N9K-C9364C
 - N9K-C9364C-GX
- モジュールスパインスイッチでは、EX で終了する名前の Cisco Nexus 9000 シリーズスイッチ、およびそれ以降（たとえば N9K-X9732C-**EX**）のみがサポートされています。
- 古い生成スパインスイッチは、固定スパインスイッチ N9K C9336PQ または N9K X9736PQ ラインカードでモジュラスパインスイッチなどのメインデータセンターではサポートが次世代のみのスパインスイッチは、WAN への接続をサポートします。

リモートのリーフスイッチ

- リモートのリーフスイッチ、後で（たとえば N9K-C93180LC-EX）EX で終了する名前と Cisco Nexus 9000 シリーズスイッチのみがサポートされています。

- リモートのリーフスイッチする必要がありますにイメージを実行する、スイッチ13.1.x以降 (aci n9000 dk9.13.1.x.x.bin) 検出できる前にします。これにより、リーフスイッチでの手動アップグレードが必要があります。

リモート リーフスイッチの制約事項と制限事項

リモート リーフには、次の注意事項および制約事項が適用されます。

- リモートリーフソリューションでは、リモートリーフスイッチとメインデータセンターのリーフ/スパインスイッチの/32 トンネルエンドポイント (TEP) IP アドレスが、要約なしでメインデータセンターとリモートリーフスイッチ間でアドバタイズされる必要があります。
- リモートリーフスイッチを同じポッド内の別のサイトに移動し、新しいサイトに元のサイトと同じノード ID がある場合は、仮想ポートチャンネル (vPC) を削除して再作成する必要があります。
- Cisco N9K-C9348GC-FXP スイッチでは、ポート 1/53 または 1/54 でのみ最初のリモートリーフスイッチディスカバリを実行できます。その後、リモートリーフスイッチの ISN/IPN へのファブリックアップリンクに他のポートを使用できます。

ここでは、リモートリーフスイッチでサポートされるものとサポートされないものについて説明します。

- [Supported Features](#) (141 ページ)
- [サポートされない機能](#) (142 ページ)
- [リリース 5.0\(1\) の変更点](#) (144 ページ)
- [リリース 5.2\(3\) の変更点](#) (144 ページ)

Supported Features

vPC リモートリーフスイッチペア内の L3Out SVI のストレッチがサポートされています。

Cisco APIC リリース 4.2(4) 以降、802.1Q (Dot1q) トンネル機能がサポートされています。

Cisco APIC リリース 4.1(2) 以降、次の機能がサポートされています。

- ACI Multi-Site を使用したリモートリーフスイッチ
- 同じリモートデータセンター内の2つのリモートリーフ vPC ペア間またはデータセンター間でのトラフィック転送 (これらのリモートリーフペアが同じポッドまたは同じマルチポッドファブリックの一部であるポッドに関連付けられている場合)
- 主要な Cisco ACI データセンターポッドが2つのリモートロケーションの間の中継である場合、リモートロケーションでの L3Out の中継 (RL location-1 の L3Out と RLlocation-2 の L3Out がそれぞれのプレフィックスをアドバタイズしている)

Cisco APIC リリース 4.0(1) 以降、次の機能がサポートされています。

- Epg の Q-で-Q カプセル化のマッピング
- リモートリーフスイッチでの PBR トラッキング（システムレベルのグローバル GIPo が有効になっている場合）
- PBR の復元力のあるハッシュ
- Netflow
- MacSec の暗号化
- ウィザードのトラブルシューティング
- アトミック カウンタ

サポートされない機能

このリリースで、サポート対象外の次の機能を除き、ファブリックおよびテナントの完全なポリシーがリモートリーフスイッチでサポートされています。

- GOLF
- vPod
- フローティング L3Out
- ローカルリーフスイッチ（ACI 主要データセンタースイッチ）とリモートリーフスイッチ間の L3out SVI のストレッチ、または2つの異なるリモートリーフスイッチの vPC ペア間のストレッチ
- コピー サービスは、ローカルリーフスイッチに導入されている場合、および送信元または宛先がリモートリーフスイッチにある場合はサポートされません。この状況では、ルーティング可能な TEP IP アドレスはローカルリーフスイッチに割り当てられません。詳細については、『APIC ドキュメンテーション ページ』で入手可能な『Cisco APIC Layer 4 to Layer 7 Services Deployment Guide』の「Configuring Copy Services」の章の「Copy Services Limitations」を参照してください。<https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>
- レイヤ 2 (スタティック Epg) を除く接続外部
- VzAny 契約とサービスをコピーします。
- リモートのリーフスイッチの FCoE 接続
- ブリッジドメインまたは Epg のカプセル化をフラグディングします。
- Fast Link Failover ポリシーは、リーフスイッチとスパインスイッチ間の ACI ファブリックリンク用であり、リモートリーフ接続には適用されません。リモートリーフ接続のコンバージェンスを高速化するために、Cisco APIC リリース 5.2(1) で代替方法が導入されています。

- 遠隔地での管理対象のサービス グラフに接続されたデバイス
- トラフィック ストーム制御
- Cloud Sec 暗号化
- ファーストホップ セキュリティ
- レイヤ3 マルチキャスト リモート リーフ スイッチ上のルーティング
- メンテナンス モード
- TEP 間アトミック カウンタ

Multi-Site アーキテクチャでリモート リーフ スイッチをサイト間 L3Out 機能と統合する場合、次のシナリオはサポートされません。

- 別々のサイトに関連付けられたリモート リーフ スイッチのペアに展開された L3Out 間のトランジットルーティング
- リモート サイトに関連付けられたリモート リーフ スイッチのペアに展開された L3Out と通信するサイトに関連付けられたリモート リーフ スイッチのペアに接続されたエンドポイント
- リモート サイトに関連付けられたリモート リーフ スイッチのペアに展開された L3Out と通信するローカル サイトに接続されたエンドポイント
- リモート サイトに展開された L3Out と通信するサイトに関連付けられたリモート リーフ スイッチのペアに接続されたエンドポイント



(注) 異なるデータセンターサイトが同じマルチポッドファブリックの一部としてポッドとして展開されている場合、上記の制限は適用されません。

リモート リーフ スイッチ機能では、次の導入と設定がサポートされていません。

- 特定のサイト (APIC ドメイン) に関連付けられたリモート リーフ ノードとマルチサイト展開の別のサイトのリーフ ノード部分の間でブリッジドメインを拡張することはサポートされていません (これらのリーフ ノードがローカルまたはリモート)、この制限を強調表示するために障害が APIC に生成されます。これは、Multi-Site Orchestrator (MSO) でストレッチブリッジドメインを構成するときに、BUM フラッドイングが有効または無効であることとは無関係です。ただし、ブリッジドメインは、同じサイト (APIC ドメイン) に属するリモート リーフ ノードとローカル リーフ ノード間で常に拡張できます (BUM フラッドイングを有効または無効にします)。
- リモート リーフ スイッチ ロケーションおよび主要データセンター全体でのスパンニング ツリー プロトコル
- APIC は、リモート リーフ スイッチに直接接続されます。

- vPC ドメインでの、リモートリーフスイッチ上の孤立ポートチャンネルまたは物理ポート（この制限は、リリース 3.1 以降に適用します）。
- コンシューマ、プロバイダ、およびサービス ノードがすべてリモートリーフスイッチに接続されていて、vPC モードである場合、サービス ノード統合の有無に関わらず、リモートローケーション内でのローカルトラフィック転送のみサポートされます。
- スパインスイッチから IPN にアダプタイズされる /32 ループバックは、リモートリーフスイッチに向けて抑制/集約してはなりません。/32 ループバックは、リモートリーフスイッチにアダプタイズする必要があります。

リリース 5.0(1) の変更点

Cisco APIC リリース 5.0(1) 以降では、リモートリーフスイッチに次の変更が適用されています。

- 直接トラフィック転送機能はデフォルトでイネーブルになっており、ディセーブルにできません。
- リモートリーフスイッチの直接トラフィック転送を使用しない設定はサポートされなくなりました。リモートリーフスイッチがあり、Cisco リリース 5.0(1) にアップグレードする場合は、「Direct Traffic Forwarding について」の項に記載されている情報を確認し、その項の手順を使用して直接トラフィック転送をイネーブルにします。APIC

リリース 5.2(3) での変更点

Cisco APIC リリース 5.2(3) 以降では、リモートリーフスイッチに次の変更が適用されています。

- リモートリーフスイッチとアップストリームルータ間のピアへの IPN アンダーレイプロトコルは、OSPF または BGP のいずれかです。以前のリリースでは、OSPF アンダーレイのみがサポートされています。

WAN ルータとリモートリーフスイッチ設定の注意事項

リモートリーフが検出され APIC 管理に組み込まれる前に、WAN ルータとリモートリーフスイッチを設定する必要があります。

次の要件に従い、ファブリックスパインスイッチの外部インターフェイスとリモートリーフスイッチポートに接続する WAN ルータを接続します。

WAN ルータ

- エリア ID、タイプ、コストなど、同じ詳細を有するインターフェイスで OSPF を有効にします。
- メインファブリックの各 APIC の IP アドレスにつながるインターフェイスで DHCP リレーを設定します。

- スパインスイッチで VLAN 5 インターフェイスに接続する WAN ルータのインターフェイスは、通常のマルチポッドネットワークに接続するインターフェイス以外に、異なる VRF に存在する必要があります。

リモートリーフスイッチ

- ファブリックポートの1つから直接接続して、アップストリームルータにリモートリーフスイッチを接続します。アップストリームルータへの次の接続がサポートされています。

- 40 Gbps 以上の接続
- QSFP-SFP アダプタでは、1/10 G SFP がサポートされています

WAN の帯域幅は、リリースによって異なります。

- 4.2(4) 以前のリリースでは、WAN の帯域幅は最小で 100 Mbps、サポートされている最大遅延は 300 ミリ秒です。
- 4.2(4) 以降のリリースでは、WAN の帯域幅は最小で 10 Mbps、サポートされている最大遅延は 300 ミリ秒です。

- 上記が推奨されますが、vPC とリモートリーフスイッチのペアを接続する必要はありません。vPC の両端にあるスイッチは、同じリモートデータセンターのリモートリーフスイッチである必要があります。

- 一意の IP アドレスを持つ VLAN 4 でレイヤ 3 サブインターフェイスとしてノースバウンドインターフェイスを設定します。

リモートのリーフスイッチからルータに1個以上のインターフェイスを接続する場合、一意の IP アドレスで各インターフェイスを設定します。

- インターフェイスで OSPF をイネーブルにしますが、OSPF エリアタイプをスタブエリアとして設定しないでください。
- リモートリーフスイッチ内の TEP プールサブネットの IP アドレスは、ポッド TEP サブネットプールと重複しないようにする必要があります。使用されるサブネットは /24 以下である必要があります。
- マルチポッドがサポートされますが、リモートリーフ機能は必要ありません。
- 単一ポッドファブリックのポッドをリモートリーフスイッチに接続するとき、スパインスイッチから WAN ルータへ、リモートリーフスイッチから WAN ルータへ L3Out を設定し、これは両方ともスイッチインターフェイスで VLAN-4 を使用します。
- マルチポッドファブリックのポッドをリモートリーフスイッチに接続するとき、スパインスイッチから WAN ルータへ、リモートリーフスイッチから WAN ルータへ L3Out を設定し、これは両方ともスイッチインターフェイスで VLAN-4 を使用します。また、VLAN-5 を使用してマルチポッド内部 L3Out を設定し、リモートリーフスイッチを宛先としてポッドを通過するトラフィックをサポートします。VLAN 4 および VLAN 5 を使用

する限り、通常のマルチポッドおよびマルチポッド内部接続は、同じ物理インターフェースで設定できます。

- マルチポッド内部 L3Out を設定している場合、通常のマルチポッド L3Out として同じルータ ID を使用しますが、ルータ ID の [ループバックアドレスとしてルータ ID を使用する] オプションを選択解除して、異なるループバック IP アドレスを設定します。これで ECMP が機能します。
- 6.0(1) リリース以降、リモートリーフスイッチは、サブネットマスクが最大 /28 のリモートプールをサポートします。以前のリリースでは、リモートリーフスイッチは、サブネットマスクが最大 /24 のリモートプールをサポートしていました。リモートプールを削除できるのは、使用を停止し、そのプールを使用しているすべてのノードを含むファブリックから削除した後でのみです。

/28 リモート TEP プールは、2 つの vPC ペアを持つ最大 4 つのリモートリーフスイッチをサポートします。RMA の目的では、2 つの IP アドレスを未使用のままにしておくことをお勧めします。これらの 2 つの IP アドレスは、1 つのスイッチの RMA を行うのに十分です。次の表は、リモートリーフスイッチがこれらの IP アドレスをどのように使用するかを示しています。



- (注) 2 つの IP アドレスが内部ファブリックの使用に使用されません。

IP アドレスタイプ	数量
/28 プールで使用可能な使用可能な IP アドレスの合計	$16 - 2 = 14$
ファブリックが内部的に使用する IP アドレスの数	2
ノードで使用可能な使用可能な IP アドレスの合計	$14 - 2 = 12$
4 つのリモートリーフスイッチに必要な IP アドレスの数	$4 * 2 = 8$
2 つの vPC ペアに必要な IP アドレスの数	$2 * 1 = 2$
リモートプールで使用されている IP アドレスの合計	$8 + 2 = 10$
/28 リモートプールの空き IP アドレス	$12 - 10 = 2$

リモートリーフスイッチを廃止すると、2 つの IP アドレスが解放されますが、24 時間が経過した後でのみ再利用できます。

GUIを使用してリモートリーフスイッチのポッドとファブリックメンバーシップを設定する

IPN ルータとリモートスイッチを検出して接続するために、Cisco APIC を設定して有効にすることができます。ウィザードを使用するか、またはウィザードを使用せずに APIC GUI を使用する方法があります。

ウィザードを使用してリモートリーフスイッチのポッドとファブリックメンバーシップを設定する

IPN ルータとリモートスイッチを検出して接続するために、Cisco APIC を設定して有効にすることができます。このトピックで説明するようにウィザードを使用して、または APIC GUI を使用する代替の方法で行えます。「[GUIを使用してリモートリーフスイッチのポッドとファブリックメンバーシップを設定する\(ウィザードは使用しない\) \(154ページ\)](#)」を参照してください。

始める前に

- IPN と WAN ルータとリモートのリーフスイッチがアクティブで設定されています。[WAN ルータとリモートリーフスイッチ設定の注意事項 \(144ページ\)](#) を参照してください。



(注) ウィザードを起動する前に、物理ポッドと IPN 間の接続を設定することを推奨します。ポッド間接続の設定については、[IPN 接続のためのポッドの準備 \(121ページ\)](#) を参照してください。

- リモートリーフスイッチペアは、vPC で接続されています。
- リモートリーフスイッチは、14.1.x 以降 (aci-n9000-dk9.14.1.x.x.bin) のスイッチイメージを実行しています。
- リモートリーフスイッチを追加する予定のポッドが作成され、設定されています。
- ポッドをリモートリーフスイッチに接続するために使用するスパインスイッチは IPN ルータに接続されています。

ステップ 1 メニューバーで、**Fabric > Inventory** をクリックします。

ステップ 2 [ナビゲーション (Navigation)] ペインで、[クイックスタート (Quick Start)] を展開し、[リモートリーフの追加 (Add Remote Leaf)] をクリックします。

ステップ3 ワークペインの[リモートリーフ (Remote Leaf)] ペインで、[リモートリーフの追加 (Add Remote Leaf)] をクリックします。

[リモートリーフの追加 (Add Remote Leaf)] ウィザードが表示されます。

まだポッド間接続を設定していない場合は、[ポッド間接続の設定 (Configure Interpod Connectivity)] 画面が表示され、他のウィザード手順の順序はこの手順で説明されている順序とは異なります。この状況では、IP接続、ルーティングプロトコル、および外部TEPアドレスを設定します。ACIを別の場所に拡張する前に、ポッド間接続が前提条件となります。

ポッド間接続の設定については、[IPN接続のためのポッドの準備 \(121 ページ\)](#) を参照してください。

ステップ4 [リモートリーフの追加 (Add Remote Leaf)] ウィザードで、[概要 (Overview)] ページの情報を確認します。

このパネルには、ファブリック内のポッドにリモートリーフスイッチを追加するために必要な手順に関する高度な情報が表示されます。[概要 (Overview)] パネルに表示される情報、および後続のページで設定する領域は、既存の設定によって異なります。

- シングルポッドまたはマルチポッドの設定に新しいリモートリーフスイッチを追加する場合は、通常、[概要 (Overview)] パネルに次の項目が表示され、これらの後続のページでこれらの領域を設定します。

- 外部 TEP
- ポッドの選択
- ルーティングプロトコル
- リモートリーフ

また、新しいリモートリーフスイッチを追加するため、ダイレクトトラフィック転送機能が自動的に設定されます。

- すでにリモートリーフスイッチが設定されており、リモートリーフウィザードを使用してこれらの既存のリモートリーフスイッチを設定しているが、既存のリモートリーフスイッチがリリース4.1(2)より前のソフトウェアリリースからアップグレードされている場合、それらのリモートリーフスイッチは直接トラフィック転送機能を設定しないでください。この場合、[リモートリーフ直接コミュニケーションは有効化されていません (Remote Leaf Direct Communication is not enabled)] で始まる [概要 (Overview)] ページの上部に警告が表示されます。

この状況でウィザードを使用してリモートリーフスイッチを追加する場合、2つのオプションがあります。

- これらの既存のリモートリーフスイッチでの直接トラフィック転送機能を有効にします。これは、この状況で推奨される一連のアクションです。最初に、[リモートリーフスイッチのアップグレードおよび直接トラフィック転送の有効化 \(160 ページ\)](#) に記載されている手順に従って、スイッチの直接トラフィック転送機能を手動でイネーブルにする必要があります。これらの手順を使用して直接トラフィック転送機能を手動で有効にしたら、このリモートリーフスイッチウィザードに戻り、ウィザードのプロセスに従って、ファブリック内のポッドにリモートリーフスイッチを追加します。

- 直接トラフィック転送機能をイネーブルにせずに、リモートリーフスイッチを追加します。これは許容可能なオプションですが、推奨されません。直接トラフィック転送機能を有効にせずにリモートリーフスイッチを追加するには、リモートトラフィック転送機能を手動で有効にせずにリモートリーフスイッチウィザードの設定を続行します。

ステップ5 [概要 (Overview)]パネルの情報を確認したら、ページの右下隅にある[開始 (Get Started)]をクリックします。

- 新しいリモートリーフスイッチを追加すると、リリース 4.1(2)以降が実行され、直接トラフィック転送機能が自動的に設定され、[外部TEP (External TEP)]ページが表示されます。[ステップ6 \(149 ページ\)](#)に進みます。
- 直接トラフィック転送機能をイネーブルにせずにリモートリーフスイッチを追加する場合、またはスイッチをリリース 4.1(2)にアップグレードし、[リモートリーフスイッチのアップグレードおよび直接トラフィック転送の有効化 \(160 ページ\)](#)の指示に従ってスイッチで直接トラフィック転送機能を手動でイネーブルにした場合は、[ポッド選択](#)ページが表示されます。[ステップ7 \(150 ページ\)](#)に進みます。

ステップ6 外部TEP ページで、必要なパラメータを設定します。

外部TEPアドレスは、リモートロケーションと通信するために物理ポッドで使用されます。このページでは、異なるロケーションを接続するネットワーク全体でルーティング可能なサブネットを設定します。外部TEPプールは、他の内部TEPプール、リモートリーフTEPプール、または他のポッドからの外部TEPプールと重複できません。ウィザードは、外部TEPプールからポッド固有のTEPアドレスおよびスパインルータIDのアドレスを自動的に割り当てます。必要に応じて、提案されたアドレスを変更できます。

- a) [デフォルトを使用 (Use Defaults)]チェックボックスをオンのままにするか、必要に応じてオフにします。

オンにすると、ウィザードは自動的にデータプレーンおよびユニキャストTEPアドレスを割り当てます。[デフォルトを使用 (Use Defaults)]ボックスがオンの場合、これらのフィールドは表示されません。必要に応じて、提案されたアドレスを表示または変更するには、[デフォルトを使用 (Use Defaults)]ボックスをオフにします。

- b) [外部TEPプール (External TEP Pool)]フィールドに、物理ポッドの外部TEPを入力します。

外部TEPプールは内部TEPプールと重ならないようにする必要があります。

- c) [ユニキャストTEP IP (Unicast TEP IP)]フィールドで、必要に応じてこのフィールドに自動的に入力される値を変更します。

このアドレスは、外部TEPプールからCisco APICによって自動的に割り当てられ、リモートリーフスイッチからそのポッドのローカルリーフスイッチにトラフィックを送信するために使用されます。

Cisco APICによって、外部TEPプールアドレスを入力するときにユニキャストTEP IPアドレスが自動的に設定されます。

- d) マルチポッド構成の場合は、ポッドごとにこれらの手順を繰り返します。

- e) このページに必要な情報をすべて入力したら、ページの右下隅にある **[次 (Next)]** ボタンをクリックします。

[ポッド選択 (Pod Selection)] ページが表示されます。

ステップ7 **[ポッド選択 (Pod Selection)]** ページで、必要なパラメータを設定します。

リモートリーフスイッチは、Cisco ACI ファブリック内のいずれかのポッドに論理的に接続します。このページで、リモートリーフスイッチが関連付けられるポッドのポッドIDを選択します。リモートリーフスイッチにIPアドレスを割り当てるには、リモートリーフTEPプールが必要です。既存のリモートリーフTEPプールを選択するか、リモートリーフTEPプールを入力して新しいプールを作成します。リモートリーフTEPプールは、既存のTEPプールとは異なる必要があります。複数のリモートリーフペアを同じリモートTEPプールに含めることができます。

- a) **[ポッドID (Pod ID)]** フィールドで、リモートリーフスイッチが関連付けられるポッドのポッドIDを選択します。
- b) **[リモートリーフTEPプール (Remote Leaf TEP Pool)]** フィールドで、既存のリモートリーフTEPプールを選択するか、リモートリーフTEPプールを入力して、リモートリーフスイッチにIPアドレスを割り当てます。

[リモートリーフTEPプール (Remote Leaf TEP Pool)] フィールドの下にある **[既存のTEPプールの表示 (View existing TEP Pools)]** リンクをクリックして、既存のTEPプール (内部TEPプール、リモートリーフTEPプール、および外部TEPプール) を表示します。この情報を使用して、プールの重複または重複を回避します。

- c) このページに必要な情報をすべて入力したら、ページの右下隅にある **[次 (Next)]** ボタンをクリックします。

[ルーティングプロトコル (Routing Protocol)] ページが表示されます。

ステップ8 **[ルーティングプロトコル (Routing Protocol)]** ページで、リモートリーフスイッチとアップストリームルータ間でピアリングするアンダーレイプロトコルに必要なパラメータを選択して設定します。次のサブステップに従います。

- a) **[L3 Outside 設定 (L3 Outside Configuration)]** セクションの **[L3 Outside]** フィールドで、リモートリーフスイッチとアップストリームルータ間の接続を表す既存のL3Outを作成または選択します。複数のリモートリーフペアは、アップストリーム接続を表すために同じL3 Outsideを使用できます。

リモートリーフスイッチの設定では、マルチポッド設定で使用するL3Outとは異なるL3Outを使用または作成することを推奨します。

- b) Cisco APIC リリース 5.2(3)以降のリリースでは、**[アンダーレイ (Underlay)]** コントロールを **[OSPF]** または **[BGP]** に設定します。

Cisco APIC リリース 5.2(3)よりも前のリリースでは、OSPFが唯一サポートされているアンダーレイプロトコルであるため、選択する必要はありません。

(注) OSPFとBGPの両方がMulti-Pod、Multi-Site、またはリモートリーフのアンダーレイで使用されている場合、IPNルータのOSPFからrouter-idをBGPに再配布しないでください。そうすると、ルーティンググループが生じ、スパインスイッチとIPNルータの間のOSPFとBGPセッションを停止してしまいます。

c) 適切な次の構成手順を選択します。

- OSPF アンダーレイの場合は、ステップ **ステップ 9 (151 ページ)** で OSPF パラメータを構成し、ステップ **ステップ 10 (152 ページ)** をスキップします。
- BGP アンダーレイの場合は、ステップ **ステップ 9 (151 ページ)** をスキップし、ステップ **ステップ 10 (152 ページ)** の BGP パラメータを設定します。

ステップ 9 (OSPFアンダーレイの場合のみ) OSPFアンダーレイを設定するには、[**ルーティングプロトコル (Routing Protocol)**] ページで次の手順を実行します。

このページで、OSPF エリア ID、エリア タイプ、および OSPF インターフェイス ポリシーを設定します。OSPF インターフェイス ポリシーには、OSPF ネットワーク タイプ、インターフェイス コスト、タイマーなどの OSPF 固有の設定が含まれています。[**デフォルトの使用 (Use Defaults)**] チェックボックスをオフにして、OSPF 認証キーと OSPF エリア コストを設定します。

a) [**OSPF**] セクションで、[**デフォルトの使用 (Use Defaults)**] チェックボックスをオンのままにするか、必要に応じてオフにします。

チェックボックスはデフォルトでオンになります。チェックをオフにすると、エリア コストや認証設定などのオプションフィールドが表示されます。

b) 必要に応じて、IPN から設定情報を収集します。

たとえば、IPN から次のコマンドを入力して、特定の設定情報を収集できます。

```
IPN# show running-config interface ethernet slot/chassis-number
```

次に例を示します。

```
IPN# show running-config interface ethernet 1/5.11
...
ip router ospf infra area 0.0.0.59
...
```

c) [**Area ID**] フィールドに OSPF エリア ID を入力します。

前のステップの出力に示されている OSPF エリア 59 の情報を見ると、[**Area ID (エリア ID)**] フィールドに別のエリアに (たとえば、0) を入力し、別の L3Out を設定できます。リモートリーフスイッチに別のエリアを使用している場合は、別の L3Out を作成する必要があります。同じ OSPF エリア ID を使用している場合でも、別の L3Out を作成できます。

d) [**エリア タイプ (Area Type)**] フィールドで、OSPF エリア タイプを選択します。

次の OSPF タイプのいずれかを選択できます。

- [**NSSA エリア (NSSA area)**]]
- [**通常エリア (Regular area)**]]

(注) [エリア タイプ (Area Type)] フィールドのオプションとして [**スタブ エリア (Stub area)**] が表示される場合があります。ただし、スタブ エリアは IPN にルートを実アドバタイズしないため、スタブ エリアはインフラ L3Out でサポートされません。

[**通常エリア (Regular area)**] がデフォルトです。

- e) **[インターフェイスポリシー (Interface Policy)]** フィールドで、OSPF インターフェイス ポリシーを入力または選択します。

既存のポリシーを選択するか、**[OSPF インターフェイス ポリシーの作成 (Create OSPF Interface Policy)]** ダイアログ ボックスを使用して新しいポリシーを作成できます。OSPF インターフェイス ポリシーには、OSPF ネットワーク タイプ、インターフェイス コスト、タイマーなどの OSPF 固有の設定が含まれています。

- f) このページに必要な情報をすべて入力したら、ページの右下隅にある**[次へ (Next)]** ボタンをクリックします。

[リモートリーフ (Remote Leafs)] ページが表示されます。

ステップ 10 (BGP アンダーレイの場合のみ) 次の BGP フィールドが **[ルーティング プロトコル]** ページに表示される場合は、次のサブステップに従います。それ以外の場合は、**[次へ]** をクリックして続行します。

- a) **[BGP]** セクションで、**[デフォルトの使用 (Use Defaults)]** チェックボックスをオンのままにするか、必要に応じてオフにします。

チェックボックスはデフォルトでオンになります。チェックを外すと、ピアリング タイプ、ピアパスワード、ルート リフレクタ ノードなどのオプション フィールドが表示されます。

- b) **[スパイン ID (Spine ID)]**、**[インターフェイス (Interface)]**、および **[IPv4 アドレス (IPv4 Address)]** フィールドでは値は設定不可であることに注意してください。
- c) **[ピア アドレス (Peer Address)]** フィールドで、BGP ネイバーの IP アドレスを入力します。
- d) **[リモート AS (Remote AS)]** フィールドで、BGP ネイバーの自動システム (AS) 番号を入力します。
- e) このページに必要な情報をすべて入力したら、ページの右下隅にある**[次へ (Next)]** ボタンをクリックします。

[リモートリーフ (Remote Leafs)] ページが表示されます。

ステップ 11 **[リモートリーフ (Remote Leafs)]** ページで、必要なパラメータを設定します。

インターポッドネットワーク (IPN) は、Cisco ACI ロケーションを接続して、エンドツーエンドのネットワーク接続を提供します。これを実現するには、リモートリーフスイッチにアップストリームルータへの IP 接続が必要です。リモートリーフスイッチごとに、アップストリームルータおよび残りの Cisco ACI ファブリックとのコントロールプレーン通信を確立するために使用されるルータ ID を入力します。また、各リモートリーフスイッチの少なくとも 1 つのインターフェイスの IP 設定を指定します。複数のインターフェイスがサポートされます。

- a) **[シリアル (Serial)]** フィールドに、リモートリーフスイッチのシリアル番号を入力するか、ドロップダウンメニューから検出されたリモートリーフスイッチを選択します。
- b) **[ノード ID (Node ID)]** フィールドで、ノード ID をリモートリーフスイッチに割り当てます。
- c) **[名前 (Name)]** フィールドで、リモートリーフスイッチに名前を割り当てます。
- d) **[ルータ ID (Router ID)]** フィールドに、アップストリームルータおよびその他の Cisco ACI ファブリックとのコントロールプレーン通信を確立するために使用されるルータ ID を入力します。
- e) **[ループバックアドレス (Loopback Address)]** フィールドに、必要に応じて IPN ルータループバック IP アドレスを入力します。

ルータ ID アドレスを使用する場合は、このフィールドを空白のままにします。

- f) [インターフェイス (Interfaces)]セクションの[インターフェイス (Interface)]フィールドに、このリモートリーフスイッチのインターフェイス情報を入力します。
- g) [インターフェイス (Interfaces)]セクションの[IPv4 アドレス (IPv4 Address)]フィールドに、インターフェイスのIPv4 IP アドレスを入力します。
- h) [インターフェイス]セクションの[MTU]フィールドで、外部ネットワークの最大送信単位の値を割り当てます。
範囲は 1500 ~ 9216 です。
- i) BGP アンダーレイを選択した場合は、BGP ネイバーの IP アドレスを[ピア アドレス]フィールドに入力し、BGP ネイバーの自律システム (AS) 番号を[リモート AS]フィールドに入力します。
- j) 必要に応じて、追加のインターフェイスに関する情報を入力します。
[インターフェイス (Interfaces)]ボックス内の[+]をクリックして、複数のインターフェイスの情報を入力します。
- k) このリモートリーフスイッチに必要な情報をすべて入力したら、必要に応じて追加のリモートリーフスイッチの情報を入力します。
[インターフェイス (Interfaces)]ボックスの右側にある[+]をクリックして、複数のリモートリーフスイッチの情報を入力します。
- l) このページに必要な情報をすべて入力したら、ページの右下隅にある[次へ (Next)]ボタンをクリックします。
[確認 (Confirmation)]ページが表示されます。

ステップ 12 [確認 (Confirmation)]ページで、ウィザードが作成するポリシーのリストを確認し、必要に応じて任意のポリシーの名前を変更し、ページの右下隅にある[完了 (Finish)]をクリックします。

[リモートリーフサマリ (Remote Leaf Summary)]ページが表示されます。

ステップ 13 [リモートリーフサマリ (Remote Leaf Summary)]ページで、適切なボタンをクリックします。

- JSON ファイル内の設定の API を表示するには、[JSON の表示 (View JSON)]をクリックします。API をコピーして、後で使用するために保存できます。

- このページの情報に問題がなく、JSON ファイルを表示しない場合は、[OK] をクリックします。

ステップ 14 [ナビゲーション (Navigation)]ペインで、[ファブリックメンバーシップ (Fabric Membership)]をクリックし、[ノード保留レジストレーション (Nodes Pending Registration)]タブをクリックして、リモートリーフスイッチ設定のステータスを表示します。

追加したリモートリーフスイッチの[ステータス (Status)]カラムに[検出なし (Undiscovered)]と表示されます。

ステップ 15 IPN を使用してスパインスイッチにログインし、次のコマンドを入力します。

```
switch# show natable
```

次のような出力が表示されます。

```
----- NAT TABLE -----
```

Private Ip	Routeable Ip
10.0.0.1	192.0.2.100
10.0.0.2	192.0.2.101
10.0.0.3	192.0.2.102

ステップ 16 リモートリーフスイッチを接続する IPN サブインターフェイスで、各インターフェイスの DHCP リレーを設定します。

次に例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/5.11
switch(config-subif)# ip dhcp relay address 192.0.2.100
switch(config-subif)# ip dhcp relay address 192.0.2.101
switch(config-subif)# ip dhcp relay address 192.0.2.102
switch(config-subif)# exit
switch(config)# interface ethernet 1/7.11
switch(config-subif)# ip dhcp relay address 192.0.2.100
switch(config-subif)# ip dhcp relay address 192.0.2.101
switch(config-subif)# ip dhcp relay address 192.0.2.102
switch(config-subif)# exit
switch(config)# exit
switch#
```

ステップ 17 [ナビゲーション (Navigation)] ペインで、[ファブリックメンバーシップ (Fabric Membership)] をクリックし、[登録済みのノード (Registered Nodes)] タブをクリックして、リモートリーフスイッチ設定のステータスを表示します。

しばらくすると、追加したリモートリーフスイッチの [ステータス (Status)] カラムに [アクティブ (Active)] と表示されます。

GUIを使用してリモートリーフスイッチのポッドとファブリックメンバーシップを設定する(ウィザードは使用しない)

[リモートリーフの追加 (Add Remote Leaf)] ウィザード ([ウィザードを使用してリモートリーフスイッチのポッドとファブリックメンバーシップを設定する \(147 ページ\)](#) を参照) を使用してリモートリーフスイッチを設定することをお勧めしますが、代わりにこの GUI 手順を使用することもできます。

始める前に

- ルータ (IPN と WAN) とリモートのリーフスイッチはアクティブで設定されています。[WAN ルータとリモートリーフスイッチ設定の注意事項 \(144 ページ\)](#) を参照してください。
- リモートリーフスイッチは、13.1.x 以降 (aci n9000 dk9.13.1.x.x.bin) のスイッチイメージを実行しています。
- リモートリーフスイッチを追加する予定のポッドが作成され、設定されています。

- ポッドをリモートリーフスイッチに接続するために使用するスパインスイッチはIPNルータに接続されています。

ステップ1 次の手順で、リモートリーフスイッチのTEPプールを設定します:

- メニューバーで、[**ファブリック (Fabric)**] > [**インベントリ (Inventory)**] をクリックします。
- [ナビゲーション(Navigation)] ウィンドウで、[**ポッドファブリックセットアップポリシー (Pod Fabric Setup Policy)**] をクリックします。
- Fabric Setup Policy** パネルで、リモートリーフスイッチのペアを追加するポッドをダブルクリックします。
- [**リモートプール (Remote Pools)**] テーブルで[+] をクリックします。
- リモートTEPプールのリモートIDとサブネットを入力し、**Submit** をクリックします。
- Fabric Setup Policy** パネルで、**Submit** をクリックします。

ステップ2 次の手順で、IPNルータに接続されているスパインスイッチのL3Outを設定します:

- メニューバーで[**テナント (Tenants)**] > [**インフラ (infra)**] をクリックします。
- [ナビゲーション (Navigation)] ペインで[**ネットワークング (Networking)**] を展開し、[L3Outs] を右クリックして[L3Outの作成 (Create L3Out)] を選択します。
- Name** フィールドに、L3Outの名前を入力します。
- [**VRF**] ドロップダウンリストから[**overlay-1**] を選択します。
- [**L3ドメイン (L3 Domain)**] ドロップダウンリストで、先ほど作成した、外部ルーテッドドメインを選択します。
- [**制御の使用 (Use for control)**] で、[**リモートリーフ (Remote Leaf)**] を選択します。
- IPNアンダーレイプロトコルとしてBGPを使用するには、[**OSPF**] チェックボックスをオフにします。

Cisco APIC リリース 5.2(3) 以降、IPNアンダーレイプロトコルはOSPFまたはBGPになることが可能です。

- OSPFがIPNアンダーレイプロトコルとして使用されるようにするには、OSPFがデフォルトで選択されているOSPFエリアで、リモートリーフスイッチを追加するポッドがマルチポッドファブリックの一部である場合に、[**マルチポッドのリモートリーフの有効化 (Enable Multi Leaf with Multipod)**] の横にあるチェックボックスをオンにします。

このオプションは、マルチポッドのためのVLAN-5を使用する第2のOSPFインスタンスを有効にします。これにより、リモートリーフスイッチのルートが、スイッチが所属しているポッド内のみアドバタイズされるようにします。

- [**次へ (Next)**] をクリックして[**ノードとインターフェイス (Nodes and Interfaces)**] ウィンドウに移動します。

ステップ3 次の手順に従って、L3Outで使用されるスパインとインターフェイスの詳細を設定します:

- デフォルトの命名規則を使用するかどうかを決定します。

[**デフォルトの使用 (Use Defaults)**] フィールドで、デフォルトのノードプロファイル名およびインターフェイスプロファイル名を使用する場合は、チェックをオンにします。

GUI を使用してリモート リーフスイッチのポッドとファブリック メンバーシップを設定する (ウィザードは使用しない)

- デフォルトのノードプロファイル名は [L3Out-name _nodeProfile] です。ここで、[L3Out-name] は [識別 (Identity)] ページの [名前 (Name)] フィールドに入力した名前です。
- デフォルトのインターフェイス プロファイル名は L3Out-name _interfaceProfile です。ここで、L3Out-name は、[識別 (Identity)] ページの [名前 (Name)] フィールドに入力した名前です。

b) 次の詳細を入力します。

- **ノード ID** — IPN ルータに接続されているスパイン スwitch の ID。
- **ルータ ID** — IPN ルータの IP アドレス
- **外部制御ピアリング** — リモート リーフスイッチを追加するポッドがシングルポッドファブリックの場合には無効にします。

- c) [ノードとインターフェイス (Nodes and Interfaces)] ウィンドウに追加の必要な情報を入力します。
- d) [ノードとインターフェイス (Nodes and Interfaces)] ウィンドウで残りの追加の情報を入力したら、[次 (Next)] をクリックします。

[プロトコル (Protocols)] ウィンドウが表示されます。

ステップ 4 [L3Out の作成 (Create L3Out)] ウィザードの [プロトコル (Protocols)] ウィンドウに必要な情報を入力します。

- a) IPN アンダーレイ プロトコルとして BGP を選択した場合は、BGP ピアの [ピア アドレス (Peer Address)] と [リモート AS (Remote AS)] を入力します。
- b) IPN アンダーレイ プロトコルとして OSPF を選択した場合は、[ポリシー (Policy)] フィールドで OSPF ポリシーを選択します。
- c) [次へ (Next)] をクリックします。

[外部 EPG (External EPG)] ウィンドウが表示されます。

ステップ 5 [L3Out の作成 (Create L3Out)] ウィザードの [外部 EPG (External EPG)] ウィンドウに必要な情報を入力し、[完了 (Finish)] をクリックして [L3Out の作成 (Create L3Out)] ウィザードで必要な設定を完了します。

ステップ 6 [テナント (Tenants)] > [インフラ (infra)] > [ネットワーキング (Networking)] > [L3Outs] > [L3Out_name] > [論理ノード プロファイル (Logical Node Profiles)] > [bLeaf] > [論理インターフェイス プロファイル (Logical Interface Profiles)] > [portIf] > [OSPF インターフェイス プロファイル (OSPF Interface Profile)] に移動します。

ステップ 7 インターフェイス プロファイルの名前を入力します。

ステップ 8 [関連付けされた OSPF インターフェイス ポリシーの名前 (Associated OSPF Interface Policy Name)] フィールドで、以前に作成したポリシーを選択するか、[OSPF インターフェイス ポリシーの作成 (Create OSPF Interface Policy)] をクリックします。

- ステップ 9** a) **OSPF Profile** で、**OSPF Policy** をクリックし、前に作成したポリシーを選択します。または、**Create OSPF Interface Policy** をクリックします。
- b) **Next** をクリックします。

- c) [ルーテッドサブインターフェイス (Routed Sub-Interface)] をクリックし、[ルーテッドサブインターフェイス (Routed Sub-Interface)] テーブルの [+] をクリックして、以下の詳細を入力します:
- Node — インターフェイスが所在するスパインスイッチです。
 - Path — IPN ルータに接続されたインターフェイス
 - Encap — VLAN の場合には **4** を入力します。
- d) **OK** をクリックし、**Next** をクリックします。
- e) **External EPG Networks** テーブルの [+] をクリックします。
- f) 外部ネットワークの名前を入力し、**OK** をクリックします。
- g) **Finish** をクリックします。

ステップ 10 リモートリーフスイッチのファブリックメンバーシップ設定を完了するには、次の手順を実行します:

- a) [ファブリック (Fabric)] > [インベントリ (Inventory)] > [ファブリックメンバーシップ (Fabric Membership)] に移動します。

この時点で、新しいリモートリーフスイッチが、ファブリックに登録されているスイッチのリストに表示されるようになります。ただし、次の手順で説明する方法でノードアイデンティティポリシーを設定するまでは、これらはリモートリーフスイッチとは認識されません。

- b) それぞれのリモートリーフスイッチについて、リストのノードをダブルクリックし、次の詳細情報を設定し、**Update** をクリックします:
- Node ID — リモートリーフスイッチの ID
 - RL TEP Pool — 以前に設定した、リモートリーフ TEP プールの識別子
 - Node Name — リモートリーフスイッチの名前

リモートリーフスイッチごとにノードアイデンティティポリシーを設定すると、**Fabric Membership** テーブルに、remote leaf ロールを持つものとしてリストされます。

ステップ 11 次の手順で、リモートリーフロケーションの L3Out を設定します:

- a) [テナント (Tenants)] > [インフラ (infra)] > [ネットワーキング (Networking)] に移動します。
- b) [L3Outs] を右クリックして、[L3Out の作成 (Create L3Out)] を選択します。
- c) L3Out の名前を入力します。
- d) **OSPF** チェックボックスをオンにして OSPF を有効にし、IPN および WAN ルータと同じ方法で OSPF の詳細を設定します。

(注) リリース 4.1(2) 以降を実行している新しいリモートリーフスイッチを導入し、それらのリモートリーフスイッチで直接トラフィック転送を有効にする場合は、[マルチポッドのリモートリーフを有効化 (Enable Remote Leaf with Multipod)] チェックボックスをオンにしないでください。このオプションは、マルチポッドに VLAN-5 を使用する OSPF インスタンスを有効にしますが、このケースでは必要ありません。詳細については、「[ダイレクトトラフィックフォワーディングについて \(159 ページ\)](#)」を参照してください。

- e) **overlay-1 VRF** を選択します。

- ステップ 12** 次の手順で、ノードと、リモート リーフスイッチから WAN ルータに向かうインターフェイスを設定します:
- [L3Out の作成 (Create L3Out)] ウィザードの [ノードとインターフェイス (Nodes and Interfaces)] ウィンドウで、次の詳細を入力します。
 - Node ID — WAN ルータに接続されているリモート リーフの ID
 - Router ID— WAN ルータの IP アドレス
 - External Control Peering — リモート リーフスイッチがマルチポッドファブリック内のポッドに追加される場合にのみ、有効にしてください
- ステップ 13** [テナント (Tenants)]>[インフラ (infra)]>[ネットワーキング (Networking)]>[L3Outs]>[L3Out_name] >[論理ノードプロファイル (Logical Node Profiles)]>[bLeaf]>[論理インターフェイスプロファイル (Logical Interface Profiles)]>[portIf]>[OSPF インターフェイスプロファイル (OSPF Interface Profile)]に移動します。
- ステップ 14** [OSPF インターフェイスプロファイル (OSPF Interface Profiles)]で、リモートリーフスイッチを WAN ルータに接続するために使用されるルーテッドサブインターフェイスについて、次の詳細を設定します。
- Identity — OSPF インターフェイスのプロファイルの名前
 - Protocol Profiles — 以前に設定した OSPF プロファイル。または新たに作成
 - Interfaces — **Routed Sub-Interface** タブの、WAN ルータに向かうルーテッドサブインターフェイスのパスと IP アドレス
- ステップ 15** 次の手順で、ファブリック外部接続プロファイルを設定します。
- [テナント (Tenants)]>[インフラ (infra)]>[ポリシー (Policies)]>[プロトコル (Protocol)]に移動します。
 - Fabric Ext Connection Policies** を右クリックし、**Create Intrasite/Intersite Profile** を選択します。
 - 例に示されている形式で必須の [コミュニティ (Community)] 値を入力します。
 - [ファブリック外部ルーティングプロファイル (ファブリック外部ルーティングプロファイル)]で [+] をクリックします。
 - プロファイルの名前を入力し、すべてのリモートリーフスイッチのアップリンクインターフェイスサブネットを追加します。
 - Update** をクリックし、**Submit** をクリックします。
- ステップ 16** リモートのリーフスイッチが、apic 内で検出されたことを確認するには、[ファブリック (Fabric)]>[インベントリ (Inventory)]>[ファブリックメンバーシップ (Fabric Membership)]、または [ファブリック (Fabric)]>[インベントリ (Inventory)]>[ポッド (Pod)]>[トポロジー (Topology)]に移動します。
- ステップ 17** ファブリックとリモートリーフスイッチ間のリンクのステータスを表示するには、IPN ルータに接続されているスパインスイッチで、**show ip ospf neighbors vrf overlay-1** コマンドを入力します。
- ステップ 18** CLI を使用する APIC で、ファブリック内のリモートリーフスイッチのステータスを表示するには、**acdiag fmvread** という NX-OS スタイルのコマンドを入力します。

ダイレクトトラフィック フォワーディングについて

で説明されているように、直接トラフィック転送のサポートはリリース 4.1(2)以降でサポートされ、リリース 5.0(1)以降ではデフォルトで有効になっており、無効にすることはできません。リリース4.1(2)でのリモートリーフスイッチ動作の特性 (132 ページ) ただし、直接トラフィック転送を有効または無効にするために使用する方法は、リモートリーフスイッチで実行されているソフトウェアのバージョンによって異なります。

- リモートリーフスイッチが現在リリース 4.1(2)以降で実行されている場合 (リモートリーフスイッチが 4.1(2)より前のリリースで実行されていない場合)、[ウィザードを使用してリモートリーフスイッチのポッドとファブリックメンバーシップを設定する \(147 ページ\)](#) に移動してください。
- リモートリーフスイッチが現在 4.1(2)よりも前のリリースで稼働している場合は、に移動してスイッチをリリース 4.1(2)以降にアップグレードし、必要な設定変更を行い、それらのリモートリーフスイッチで直接トラフィック転送を有効にします。[リモートリーフスイッチのアップグレードおよび直接トラフィック転送の有効化 \(160 ページ\)](#)
- リモートリーフスイッチがリリース 4.1(2)以降で実行されており、直接トラフィック転送が有効になっているが、4.1(2)より前のリリースにダウングレードする場合は、に移動して、それらのリモートリーフスイッチをダウングレードする前に直接トラフィック転送機能を無効にします。[直接トラフィック転送を無効化、およびリモートリーフスイッチのダウングレード \(164 ページ\)](#)
- リモートリーフスイッチがリリース 5.0(1)より前のリリースで実行されており、リリース 5.0(1)以降にアップグレードする場合：
 1. リモートリーフスイッチが 4.1(2)より前のリリースで実行されている場合は、最初にリリース 4.1(2)にアップグレードし、で説明されている手順を使用してそれらのリモートスイッチで直接トラフィック転送を有効にします。[リモートリーフスイッチのアップグレードおよび直接トラフィック転送の有効化 \(160 ページ\)](#)
 2. リモートリーフスイッチがリリース 4.1(2)にあり、ダイレクトトラフィック転送が有効になっている場合は、リモートリーフスイッチをリリース 5.0(1)以降にアップグレードします。
- リモートリーフスイッチがリリース 5.0(1)以降で実行されており、直接トラフィック転送がデフォルトで有効になっている場合、直接トラフィック転送もサポートしている次の以前のリリースにダウングレードする必要があります。
 - リリース 4.2(x)
 - リリース 4.1(2)

直接トラフィック転送は、設定に応じてデフォルトで有効になっている場合とされていない場合があります。

- ルーティング可能なサブネットとルーティング可能な Ucast の両方がダウングレード前にすべてのポッドで有効にされていた場合、ダウングレード後も直接トラフィック転送はデフォルトで有効のままになります。
- ルーティング可能なサブネットがすべてのポッドで有効になっているが、ルーティング可能な Ucast が有効になっていない場合、ダウングレード後に直接トラフィック転送は有効になりません。

リモートリーフスイッチのアップグレードおよび直接トラフィック転送の有効化

リモートリーフスイッチが現在 4.1(2) よりも前のリリースで稼働している場合は、これらの手順に従ってスイッチをリリース 4.1(2) 以降にアップグレードし、必要な設定変更を行い、これらのリモートリーフスイッチで直接トラフィック転送を有効にします。



- (注) リリース 4.1(2) 以降にアップグレードする場合、アップグレード先のリリースに応じて、直接トラフィック転送の有効化はオプションまたは必須になります。
- リリース 5.0(1) よりも前のリリースにアップグレードする場合、ダイレクトトラフィック転送の有効化はオプションです。ダイレクトトラフィック転送機能をイネーブルにしなくても、スイッチをアップグレードできます。必要に応じて、アップグレードを行った後のある時点で、この機能を有効にできます。
 - リリース 5.0(1) 以降にアップグレードする場合は、直接トラフィック転送を有効にする必要があります。ダイレクトトラフィック転送は、リリース 5.0(1) 以降ではデフォルトで有効になっており、無効にすることはできません。

後日、リモートリーフスイッチのソフトウェアを、リモートリーフスイッチの直接トラフィック転送をサポートしないバージョン（リリース 4.1(2) よりも前のリリース）にダウングレードする必要がある場合は、[直接トラフィック転送を無効化、およびリモートリーフスイッチのダウングレード \(164 ページ\)](#) の手順に従って、リモートリーフスイッチのソフトウェアをダウングレードする前に、直接トラフィック転送機能を無効にします。

- ステップ 1** ファブリック内のすべてのノードをリリース 4.1(2) 以降にアップグレードします。Cisco APIC
- ステップ 2** 設定するルーティング可能なサブネットのルートがポッド間ネットワーク (IPN) で到達可能であること、およびサブネットがリモートリーフスイッチから到達可能であることを確認します。
- ステップ 3** ファブリック内のすべてのポッドでルーティング可能なサブネットを設定します。
- a) メニューバーで、**Fabric > Inventory** をクリックします。
 - b) [Navigation] ウィンドウで、**Pod Fabric Setup Policy** をクリックします。
 - c) [ファブリック セットアップ ポリシー (Fabric Setup Policy)] パネルで、ルーダブルサブネットを設定するポッドをダブルクリックします。

- d) APIC ソフトウェアのリリースに応じて、サブネットまたは TEP テーブルの情報にアクセスします。
- 4.2(3) よりも前のリリースでは、[ルータブル サブネット (Routable Subnets)] テーブルで [+] をクリックします。
 - 4.2(3) の場合のみ、[外部サブネット (External Subnets)] テーブルで [+] をクリックします。
 - 4.2(4) 以降では、[外部 TEP (External TEP)] テーブルで [+] をクリックします。
- e) 必要に応じて IP アドレスと予約アドレスを入力し、状態を **アクティブ** または **非アクティブ** に設定します。
- IP アドレスは、ロータブル IP スペースとして設定するサブネット プレフィックスです。
 - 予約アドレスは、スパインスイッチおよびリモートリーフスイッチに動的に割り当ててはいけないサブネット内のアドレスの数です。カウントは常にサブネットの最初の IP から始まり、順番に増加します。このプールからユニキャスト TEP (これらの手順の後で変換されます) を割り当てるとは、予約する必要があります。
- f) **[更新 (Update)]** をクリックして、新しい外部ルータブルサブネットをサブネットまたは TEP テーブルに追加します。
- g) **Fabric Setup Policy** パネルで、**Submit** をクリックします。
- (注) これらの設定を行った後、サブネットまたは TEP テーブルの情報を変更する必要がある場合に、*Cisco APIC Getting Started Guide* 内の「Changing the External Routable Subnet」の手順に従い、これらの変更を行います。

ステップ 4 各ポートのルータブル Ucast を追加します。

- a) メニューバーで、**[テナント (Tenants)] > [インフラ (infra)] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [ファブリック外部接続ポリシー (Fabric Ext Connection Policies)] > [intrasite-intersite_profile_name]** の順にクリックします。
- b) このサイト内/サイト間プロファイルのプロパティ ページで、**[ポッド接続プロファイル (Pod Connection Profile)]** 領域の **[+]** をクリックします。
- [ポッド接続プロファイルの作成 (Create Pod Connection Profile)] ウィンドウが表示されます。
- c) ポッドを選択し、**[ポッド接続プロファイルの作成 (Create Pod Connection Profile)]** ウィンドウに必要な情報を入力します。
- [ユニキャスト TEP (Unicast TEP)] フィールドに、IPN を介したユニキャスト トラフィックに使用される、ルーティング可能な TEP IP アドレス (プレフィックスのビット長を含む) を入力します。この IP アドレスは、特定のシナリオでユニキャスト トラフィックのそれぞれのポッドのスパインスイッチによって使用されます。たとえば、リモートリーフスイッチの直接展開にはユニキャスト TEP が必要です。

(注) リリース4.2(5)以降、APIC ソフトウェアは、次のいずれかの誤った設定がある場合、4.2(5)より前のリリースから4.2(5)以降へのアップグレード後に、適切な障害を自動的に発生させます。

- 予約アドレス数が0または0以外のポッドの外部 TEP プールの非予約部分のいずれかの IP アドレスで設定された1つのポッドのユニキャスト TEP IP アドレス
- 1つのポッドのユニキャスト TEP IP アドレスが、ファブリック内の他のポッドのユニキャスト TEP IP アドレスと一致します
- ユニキャスト TEP IP アドレスが、ファブリック内のすべてのポッドのリモートリーフ TEP プールと重複しています

この場合、障害をクリアするには、リリース4.2(5)以降へのアップグレード後に適切な設定変更を行う必要があります。何らかの設定のエクスポートを試行する前に、これらの設定を変更する必要があります。そうしないと、リリース4.2(5)以降からの設定のインポート、設定のロールバック、またはIDリカバリで障害が発生します。

ステップ5 [送信 (Submit)] をクリックします。

各ポッドにルーティング可能なサブネットとルーティング可能な Ucast を設定すると、次の領域が設定されます。

- スパインスイッチで、リモートリーフ マルチキャスト TEP インターフェイス (rl-mcast-hrep) とルーティング可能な CP TEP インターフェイス (rt-cp-etep) が作成されます。
- リモートリーフスイッチでは、プライベートリモートリーフ マルチキャスト TEP インターフェイス (rl-mcast-hrep) はそのままです。
- トラフィックは引き続きプライベートリモートリーフ マルチキャスト TEP インターフェイス (rl-mcast-hrep) を使用します。
- トラフィックは、新しく設定されたルーティング可能な Ucast TEP インターフェイスで再開されます。プライベートリモートリーフユニキャスト TEP インターフェイス (rl_ucast) トンネルがリモートリーフスイッチから削除されます。新しく設定されたユニキャスト TEP でトラフィックが収束しているため、サービスの中断は非常に短時間です。
- リモートリーフスイッチおよびスパインスイッチ COOP (オラクルプロトコル会議) セッションは、プライベート IP アドレスのままです。
- BGP ルートリフレクタは、ルーティング可能な CP TEP インターフェイス (rt-cp-etep) に切り替わります。

ステップ6 COOP が正しく設定されていることを確認します。

```
# show coop internal info global
# netstat -anp | grep 5000
```

ステップ7 リモートリーフスイッチのBGPルートリフレクタセッションが正しく設定されていることを確認します。


```
remote-leaf# show bgp vpnv4 unicast summary vrf all | grep 14.0.0
14.0.0.227 4 100 1292 1164 395 0 0 19:00:13 52
14.0.0.228 4 100 1296 1164 395 0 0 19:00:10 52
```

ステップ 8 リモートリーフスイッチの直接トラフィック転送を有効にします。

- メニューバーで、**[System]>[System Settings]** の順にクリックします。
- [Fabric Wide Setting]** をクリックします。
- [リモートリーフダイレクトトラフィック転送の有効化 (Enable Remote Leaf Direct Traffic Forwarding)]** でチェックボックスをクリックします。

これを有効にすると、リモートリーフスイッチが各リモートリーフスイッチの TEP 間で直接送信するようになるため、スパインスイッチはアクセス制御リスト (ACL) をインストールして、リモートリーフスイッチからのトラフィックが返送されないようにします。リモートリーフスイッチ間にトンネルが構築されている間、サービスが短時間中断する場合があります。

- [送信 (Submit)]** をクリックします。
- コンフィギュレーションが正しく設定されているか確認するには、スパインスイッチで次のコマンドを入力します。

```
spine# cat /mit/sys/summary
```

出力内容で次のハイライトされているラインを確認してください。コンフィギュレーションが正しく設定されているかの確認ができます (フル出力の省略形)。

```
...
podId : 1
remoteNetworkId : 0
remoteNode : no
rldirectMode : yes
rn : sys
role : spine
...
```

この時点で、次の領域が設定されます。

- ネットワークアドレス変換アクセスコントロールリスト (NAT ACL) は、データセンターのスパインスイッチで作成されます。
- リモートリーフスイッチでは、プライベートリモートリーフユニキャスト TEP インターフェイス (rl_ucast) およびリモートリーフマルチキャスト TEP インターフェイス (rl-mcast-hrep) トンネルが削除され、ルータブルトンネルが作成されます。
- 次の例に示すように、**rlRoutableMode** および **rldirectMode** 属性は **yes** に設定されます。

```
remote-leaf# moquery -d sys | egrep "rlRoutableMode|rldirectMode"
rlRoutableMode : yes
rldirectMode : yes
```

ステップ 9 リモートリーフスイッチに接続する IPN インターフェイスで DHCP が遅延するため、Cisco APIC のルータブル IP アドレスを追加します。

クラスタ内の各APICには、プールからアドレスが割り当てられます。これらのアドレスは、リモートリーフスイッチ側のインターフェイスにDHCPリレーアドレスとして追加する必要があります。これらのアドレスを検索するには、APIC CLI から次のコマンドを実行します。

```
remote-leaf# moquery -c infraWiNode | grep routable
```

ステップ 10 各リモートリーフスイッチを一度に1つずつ解放し、再起動して、ルーティング可能なIPアドレスで検出します。Cisco APIC

COOP 設定が Rountable CP TEP Interface (rt-cp-etep) に変更されます。各リモートリーフスイッチがデコミッションされて再コミッションされると、DHCP サーバ ID にルーティング可能なIPアドレスが割り当てられます。Cisco APIC

直接トラフィック転送を無効化、およびリモートリーフスイッチのダウングレード

リモートリーフスイッチがリリース 4.1(2) 以降で実行されており、直接トラフィック転送が有効になっているが、4.1(2) より前のリリースにダウングレードする場合は、リモートリーフスイッチをダウングレードする前に、直接トラフィック転送機能を無効にするこれらの手順に従います。

始める前に

ステップ 1 マルチポッド設定の場合は、VLAN-5 を使用してマルチポッド内部 L3Out を設定します。

ステップ 2 リモートリーフスイッチで直接トラフィック転送機能をイネーブルにしたときに削除された場合は、プライベートネットワークの到達可能性をプロビジョニングします。

たとえば、IPN でプライベート IP ルートの到達可能性を設定し、リモートリーフスイッチに接続された IPN のレイヤ 3 インターフェイスでのプライベート IP アドレスを DHCP リレーアドレスとして設定します。Cisco APIC

ステップ 3 次のポリシーをポストして、すべてのリモートリーフスイッチのリモートリーフスイッチの直接トラフィック転送を無効にします。

```
POST URL : https://<ip address>/api/node/mo/uni/infra/settings.xml
<imdata>
  <infraSetPol dn="uni/infra/settings" enableRemoteLeafDirect="no" />
</imdata>
```

これにより、MO が Cisco APIC にポストされ、設定が Cisco APIC からファブリック内のすべてのノードにプッシュされます。

この時点で、次の領域が設定されます。

- ネットワークアドレス変換アクセスコントロールリスト (NAT ACL) は、データセンターのスパインスイッチで削除されます。

- 次の例に示すように、**rlRoutableMode** および **rldirectMode** 属性は **no** に設定されます。

```
remote-leaf# moquery -d sys | egrep "rlRoutableMode|rldirectMode"  
rlRoutableMode : no  
rldirectMode : no
```

ステップ4 ファブリック内のポッドからルーティング可能なサブネットとルーティング可能な Ucast を削除します。

各ポッドからルーティング可能なサブネットとルーティング可能な Ucast を削除すると、次の領域が設定されます。

- スパインスイッチで、リモートリーフマルチキャスト TEP インターフェイス (**rl-mcast-hrep**) およびルーティング可能な CP TEP インターフェイス (**rt-cp-ctep**) が削除されます。
- リモートリーフスイッチでは、ルーティング可能なリモートリーフマルチキャスト TEP インターフェイス (**rl-mcast-hrep**) へのトンネルが削除され、プライベートリモートリーフマルチキャスト TEP インターフェイス (**rl-mcast-hrep**) が作成されます。リモートリーフユニキャスト TEP インターフェイス (**rl_ucast**) トンネルは、この時点でルーティング可能です。
- リモートリーフスイッチおよびスパインスイッチ COOP (オラクルプロトコルのカウンシル) およびルートリフレクタセッションはプライベートに切り替わります。
- ルーティング可能なリモートリーフユニキャスト TEP インターフェイス (**rl_ucast**) へのトンネルが削除され、プライベートリモートリーフユニキャスト TEP インターフェイス (**rl_ucast**) トンネルが作成されます。

ステップ5 各リモートリーフスイッチをデコミッションして再起動し、Cisco APIC のルーティング不可能な内部 IP アドレスで検出します。

ステップ6 ファブリック内のおよびすべてのノードを 4.1(2) より前のリリースにダウングレードします。Cisco APIC

リモートリーフスイッチのフェールオーバー

(APIC) リリース 4.2(2) 以降、リモートリーフスイッチはポッド冗長です。Cisco Application Policy Infrastructure Controllerつまり、マルチポッドのセットアップでは、ポッド内のリモートリーフスイッチがスパインスイッチへの接続を失うと、別のポッドに移動されます。これにより、元のポッドに接続されているリモートリーフスイッチのエンドポイント間のトラフィックが機能します。

リモートリーフスイッチはポッドに関連付けられ、ピン接続され、スパインプロキシパスは設定によって決定されます。以前のリリースでは、Council of Oracle Protocol (COOP) はマッピング情報をスパインプロキシに伝達していました。現在、スパインスイッチへの通信が失敗すると、COOPセッションは別のスパインスイッチのポッドに移動します。

以前は、Border Gateway Protocol (BGP) ルートリフレクタをポッドに追加しました。ここで、外部ルートリフレクタを使用し、ポッド内のリモートリーフスイッチが他のポッドと BGP 関係を持っていることを確認します。

リモートリーフスイッチのフェールオーバーは、デフォルトでは無効になっています。[システム (Systems)] [システム設定 (System Settings)] タブの (APIC) GUIで、リモートリーフポッド冗長性ポリシーを有効にします。Cisco Application Policy Infrastructure Controller > 冗長プリエンブションを有効にすることもできます。プリエンブションを有効にすると、リモートポッドがバックアップされると、リモートリーフスイッチは親ポッドに再関連付けされます。プリエンブションを有効にしない場合、リモートリーフは、親ポッドが復帰しても動作ポッドに関連付けられたままになります。



(注) あるポッドから別のポッドにリモートリーフスイッチを移動すると、数秒のトラフィックの中断が発生する可能性があります。

リモートリーフフェールオーバーの要件

ここでは、リモートリーフスイッチのフェールオーバーが機能するために満たす必要がある要件を示します。この要件は、この章のリモートリーフスイッチのハードウェア要件に追加されるものです。[リモートリーフスイッチのハードウェアの要件 \(140 ページ\)](#)

- フルメッシュモードではなく、ルートリフレクタモードでマルチポッドを設定します。
- リモートリーフスイッチのルート可能なIPアドレスで直接トラフィック転送を有効にします。
- 外部 Border Gateway Protocol (BGP) ルートリフレクタを設定します。
 - スパインスイッチ間の BGP セッションを減らすために、マルチポッドに外部ルートリフレクタを使用することを推奨します。

各ポッドの1つのスパインスイッチを外部ルートリフレクタ専用にすることができます。
- フルメッシュモードですべてのリモートリーフポッドの外部 BGP ルートリフレクタノードを設定します。
- すでにフルメッシュモードでマルチポッドを使用している場合は、フルメッシュを引き続き使用できます。ただし、リモートリーフスイッチのルートリフレクタを有効にします。

リモートリーフスイッチフェールオーバーの有効化

リモートリーフスイッチポッドの冗長性ポリシーを作成して、リモートリーフスイッチのフェールオーバーを有効にします。冗長プリエンブションを有効にすることもできます。この場合、ポッドがバックアップされると、リモートリーフスイッチと親ポッドが再度関連付けられます。

始める前に

リモートリーフスイッチのフェールオーバーをイネーブルにする前に、次のタスクを実行します。

- セクション「[リモートリーフフェールオーバーの要件（166ページ）](#)」の前提条件を満たします。
- リモートリーフダイレクト（RLD）を有効にします。
- すべてのポッドが（APIC）リリース 4.2(2) 以降を実行していることを確認します。Cisco Application Policy Infrastructure Controller
- すべてのポッドに少なくとも2つの Data Center Interconnect（DCI）対応スパインスイッチがあることを確認します。

製品名にサフィックス「EX」が付いた Cisco Nexus 9000 シリーズ スパイン スイッチを使用していることを確認します。たとえば、N9K-C93180YC-EX です。



- (注) ポッドに単一のリモートリーフスイッチがあり、スイッチがクリーンリロードされると、スイッチはスパインスイッチのフェールオーバーポッド（親設定ポッド）に接続されます。ポッドに複数のリモートリーフスイッチがある場合は、少なくとも1つのスイッチがクリーンリロードされていないことを確認します。これにより、他のリモートリーフスイッチは、リロードされなかったリモートリーフスイッチが存在するポッドに移動できます。

ステップ1 Cisco APIC にログインします。

ステップ2 [システム (System)] > [システム設定 (System Settings)] に移動します。

ステップ3 [システム設定 (System Settings)] ナビゲーションウィンドウで、[リモートリーフポッド冗長性ポリシー (Remote Leaf POD Redundancy Policy)] を選択します。

ステップ4 [リモートリーフポッド冗長性ポリシー (Remote Leaf POD Redundancy Policy)] 作業ウィンドウで、[リモートリーフポッド冗長性ポリシーの有効化 (Enable Remote Leaf Pod Redundancy Policy)] チェックボックスをオンにします。

ステップ5 (任意) [リモートリーフポッド冗長性プリエンプションの有効化 (Enable Remote Leaf Pod Redundancy pre-emption)] チェックボックスをオンにします。

ポッドが復旧すると、親ポッドにリモートリーフスイッチが再度関連付けられたチェックボックスをオンにします。このチェックボックスをオフのままにすると、親ポッドが復帰しても、リモートリーフは動作ポッドに関連付けられたままになります。

次のタスク

フェールオーバーが発生したときにリモートリーフスイッチで次のコマンドを入力し、どのポッドリモートリーフスイッチが動作しているかを確認します。

```
cat /mit/sys/summary  
moquery -c rlpodredRlSwitchoverPod
```

リモートのリーフスイッチのダウングレードする前に必要な前提条件



- (注) リモートノードの使用停止し、リモートリーフに関連するポリシー(を削除する必要がありますがあれば導入で、リモートのリーフスイッチリリース3.1(1)から以降、リモートリーフ機能をサポートしていない以前のリリースには、APICソフトウェアのダウングレードする場合、というプールにある)を含む前にダウングレードします。スイッチの使用停止の詳細については参照してください。使用停止およびスイッチの再稼働で、*Cisco APIC* [トラブルシューティングガイド](#)。

リモートリーフスイッチをダウングレードする前に、いずれかのタスクが完了することを確認します。

- vPC ドメインを削除します。
- SCVMM を使用している場合は、vTEP - 仮想ネットワークアダプタを削除します。
- リモートリーフノードの使用停止および10を待機-15分を完了するタスクの使用停止後。
- 削除に WAN L3out にリモートリーフ、テナントインフラ。
- Multipod を使用している場合、インフラ-l3out VLAN 5 とを削除します。
- リモートというプールを削除します。



第 15 章

SR-MPLS ハンドオフ

リリース 5.0(1) 以降、境界リーフスイッチでのセグメントルーティング (SR) マルチプロトコルラベルスイッチング (MPLS) ハンドオフは、新機能として使用できます。Cisco ACI



(注) このドキュメントの手順では、GUI と REST API を使用して SR-MPLS ハンドオフを設定する方法について説明します。現時点では、NX-OS スタイルの CLI を使用して SR-MPLS ハンドオフを設定することはできません。

- [ACI ハンドオフについて \(169 ページ\)](#)
- [SR-MPLS ハンドオフの ACI 実装について \(175 ページ\)](#)
- [SR-MPLS 設定モデルについて \(184 ページ\)](#)
- [注意事項と制約事項 \(189 ページ\)](#)
- [GUI を使用した SR-MPLS インフラ L3Out の設定 \(196 ページ\)](#)
- [GUI を使用した SR-MPLS VRF L3Out の設定 \(205 ページ\)](#)
- [GUI を使用した SR-MPLS カスタム QoS ポリシーの作成 \(208 ページ\)](#)
- [MPLS 統計情報の表示 \(210 ページ\)](#)
- [SR-MPLS グローバルブロック \(GB\) の設定 \(213 ページ\)](#)
- [IP ハンドオフ設定から SR ハンドオフ設定への移行 \(215 ページ\)](#)
- [ループ防止のための BGP ドメインパス機能について \(223 ページ\)](#)

ACI ハンドオフについて

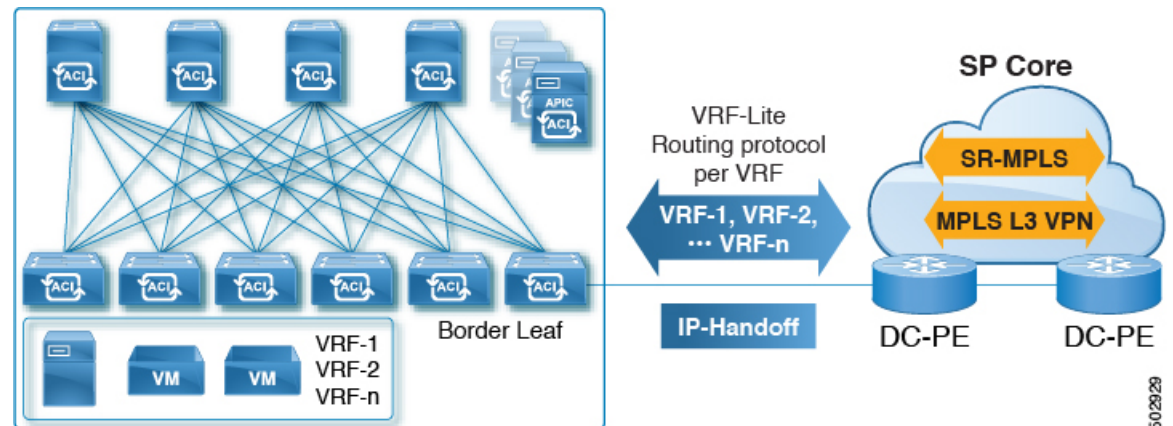
ここでは、IP ハンドオフを使用したリリース 5.0(1) より前のリリースでの ACI ハンドオフの処理方法と、リリース 5.0(1) 以降の SR-MPLS ハンドオフを使用した処理方法について説明します。Cisco APICCisco APIC

リリース 5.0(1) 以前の ACI ハンドオフ : IP ハンドオフ

リリース 5.0(1) 以前では、ACI 境界リーフ ノードをデータセンタープロバイダーエッジ (DC-PE) に接続する ACI ファブリックを設定するときに、マルチテナントネットワークを

使用する構成の場合は、複数の VRF があり、各 VRF にルーティングプロトコルが必要です。Cisco APIC また、各 VRF のインターフェイスを専用にする必要があります。このインターフェイスは、物理インターフェイスまたは論理インターフェイスのいずれかです。次の図に示すように、この設定は通常 VRF-Lite と呼ばれます。

図 18: IP ハンドオフを使用した DC-PE への ACI ハンドオフ (VRF-Lite)



この設定では、境界リーフスイッチは VRF-Lite を使用して DC-PE に接続されます。境界リーフスイッチと DC-PE 間のインターフェイスおよびルーティングプロトコルセッションの設定は、個別の VRF を使用して行われます。差別化サービスコードポイント (DSCP) は、発信トラフィックの境界リーフスイッチで設定されます。DC-PE では、DSCP は、トラフィックエンジニアリング (SR-TE) ポリシーのセグメントルーティングにマッピングされます。このポリシーは、トランスポートネットワーク経路でトラフィックを誘導するために使用されます。

境界リーフスイッチとデータセンターの間に多数のセッションがある場合、この設定は面倒になります。したがって、自動化と拡張性は、VRF-Lite を使用して設定する際の重要な課題です。

リリース 5.0(1) での ACI ハンドオフ : SR ハンドオフ

リリース 5.0(1) 以降、SR-MPLS ハンドオフを使用して、境界リーフスイッチと DC-PE ルータ間の ACI ファブリック接続を設定できるようになりました。Cisco APIC SR は他のオプションよりも優れたソリューションです。VXLAN などの他のオプションは SP コアでは一般的なテクノロジーではないため、SR はトランスポートデバイスよりもはるかに一般的で成熟したソリューションです。

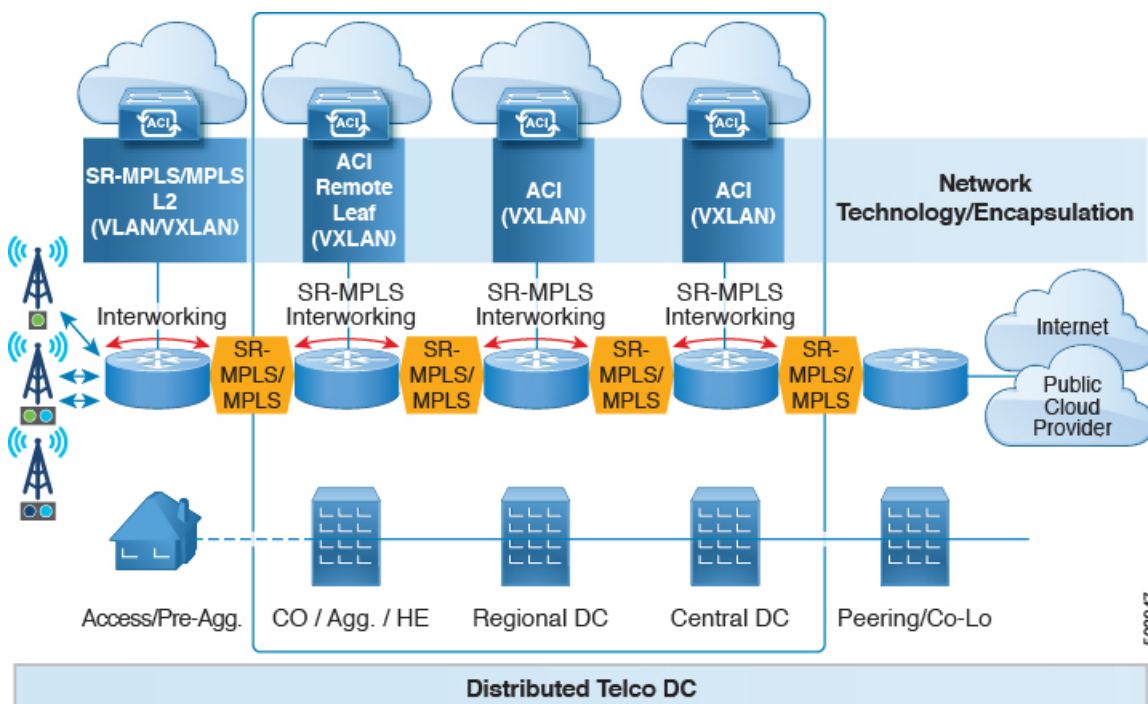
次のシナリオは、SR-MPLS を使用した DC-PE への ACI ハンドオフの設定がどのように役立つかを示しています。

- [統合セグメントルーティングの転送 \(171 ページ\)](#)
- [トランスポートネットワークでの DC-to-DC フローのモニタリング \(171 ページ\)](#)
- [複数の VRF の単一コントロールプレーンセッション \(172 ページ\)](#)

- [カラー コミュニティ (Color Community)] または [宛先プレフィックス (Destination Prefix)] を使用したトランスポートの SR-TE / Flex Algo (173 ページ)
- SR または MPLS による DC およびトランスポート QoS (174 ページ)

統合セグメントルーティングの転送

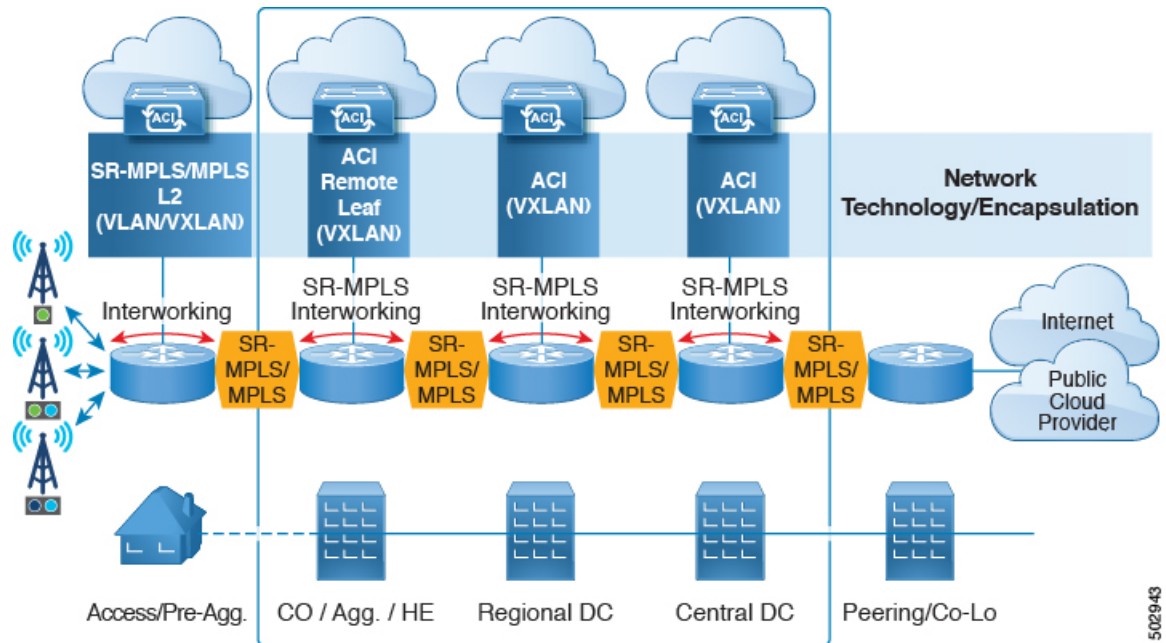
次のシナリオでは、異なる ACI DC ネットワークを相互接続するための統合 SR または MPLS トランスポート ネットワークの導入について説明します。VXLAN から SR-MPLS へのハンドオフは、ACI ネットワークと DC-PE ルータ間の各ロケーションで活用されます。



このシナリオでは、VXLAN は ACI ファブリック エリアで使用され、セグメントルーティングはトランスポートネットワークで使用されます。ACI ファブリック エリアの外部で VXLAN を使用するのではなく、同じ SR ベースのルーティングを使用することをお勧めします。この場合、トランスポートデバイスに対して SR ハンドオフまたは MPLS ハンドオフを実行します。ACI 境界で VXLAN を SR に変更すると、トランスポート デバイスは SR または MPLS を実行するだけでよく、VXLAN を実行する必要はありません。

トランスポート ネットワークでの DC-to-DC フローのモニタリング

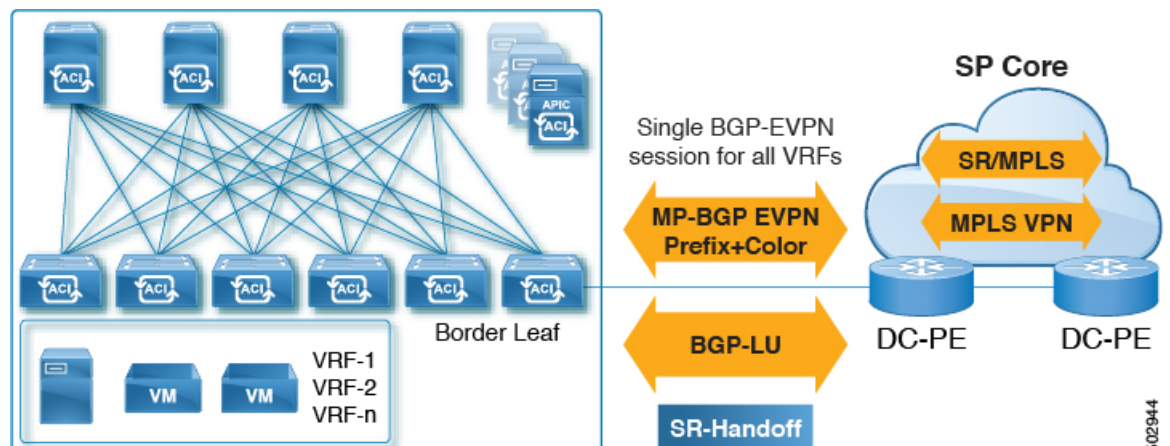
次のシナリオでは、DC-to-DC フローは VXLAN ではなくセグメントルーティングを使用してカプセル化されます。



このシナリオでは、トランスポート ネットワークに使用される既存のモニタリング ツールは MPLS トラフィックをモニタできますが、VXLAN パケットはモニタできません。ACI から SR-MPLS へのハンドオフを使用することで、トランスポート チームは既存のモニタリング ツールを使用して DC-to-DC フローをモニタできます。

複数の VRF の単一コントロールプレーンセッション

SR ハンドオフを使用すると、単一のコントロールプレーンセッション (MP-BGP EVPN) が、IP ハンドオフ設定で使用する必要がある VRF 単位のセッションではなく、すべての VRF に使用されます。これにより、ACI データセンターと DC-PE 間の複数の VRF の自動化とスケラビリティのオプションが向上します。

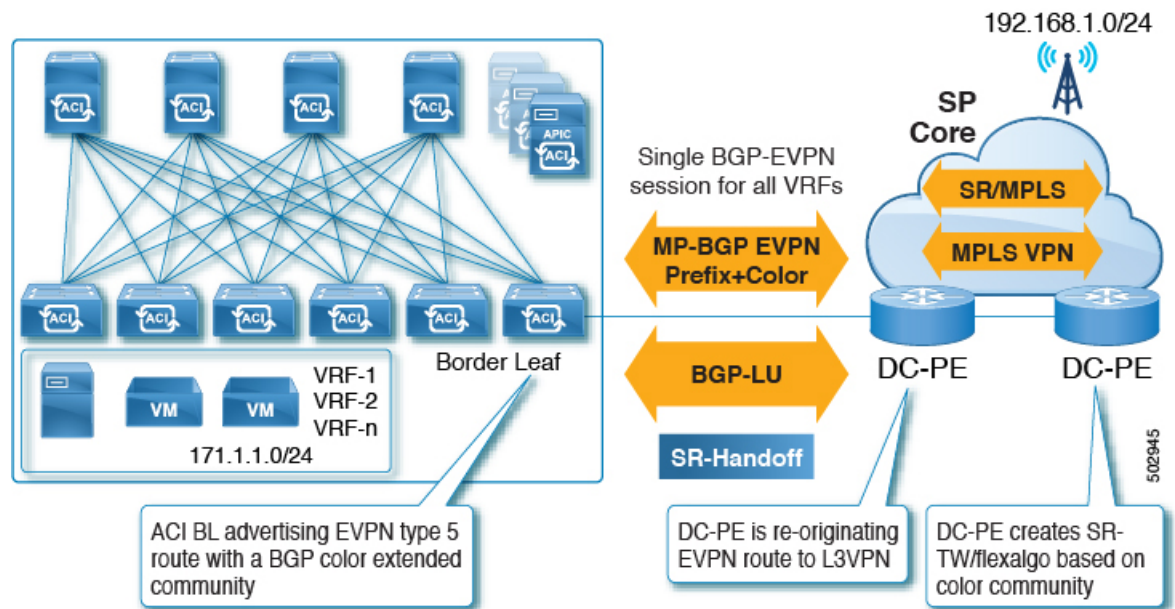


SR ハンドオフでは、VRF 単位のコントロールプレーンおよびデータプレーンセッションの代わりに単一のコントロールプレーンおよびデータプレーンセッションが使用され、Cisco ACI ファブリックから SP コアへの統合 SR トランスポートが使用されます。BGP ラベルユニ

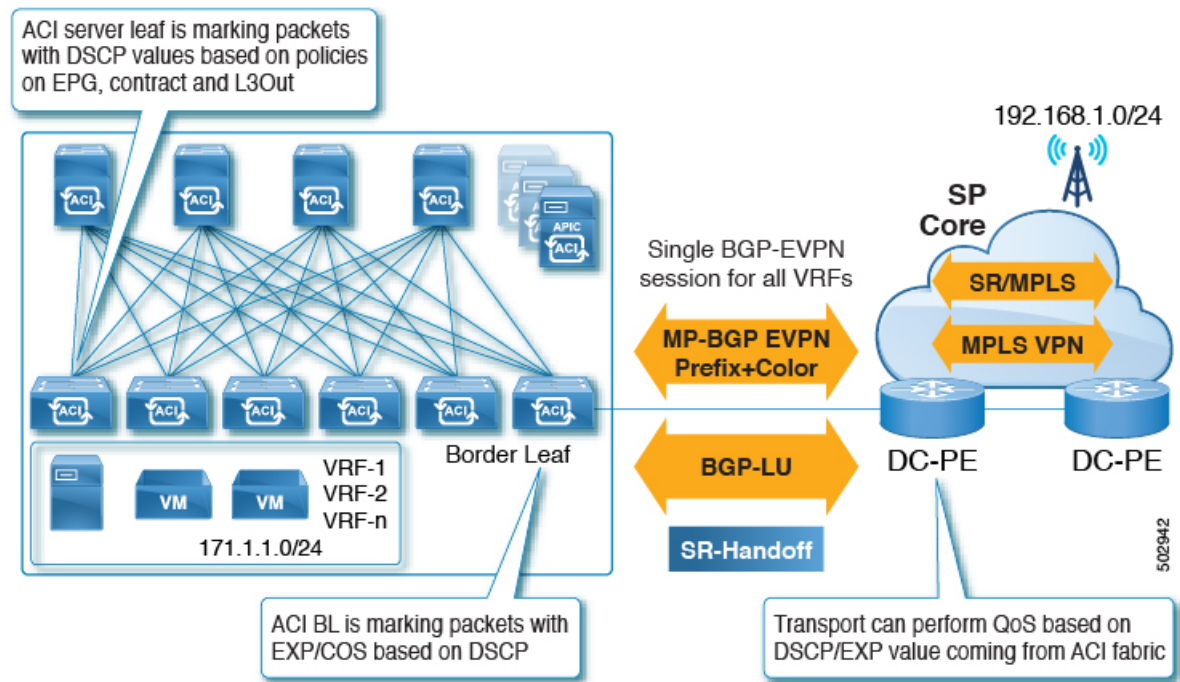
キャスト (BGPLU) アドレスファミリーは、アンダーレイラベル交換に使用されます。MP-BGP EVPN アドレスファミリーは、VRF 情報ごとにプレフィックスと MPLS ラベルを伝送します。

[カラーコミュニティ (Color Community)] または [宛先プレフィックス (Destination Prefix)] を使用したトランスポートの **SR-TE / Flex Algo**

SRハンドオフは、SPコアでSRのシグナリングを自動化するため、有益です。この場合、ACI境界リーフスイッチは、BGPカラー拡張コミュニティを持つEVPNタイプ5ルートでDC-PEにアドバタイズします。DC-PEは、ACI境界リーフスイッチから受信したカラーコミュニティまたは宛先プレフィックスに基づいてセグメントルーティングポリシーを作成できます。この機能により、DCとトランスポートネットワークをシームレスに統合できます。



同様に、次の図に示すように、ACI境界リーフスイッチからEVPNタイプ5プレフィックスをアドバタイズでき、DC-PEは宛先プレフィックスに基づいてSR-TEまたはFlex Algoルーティングポリシーを作成できます。



同様に、MPLS 入力ルールを使用して、ACI 境界リーフスイッチは、EXP 値に基づいてファブリックに着信する入力パケットを COS、DSCP、および QoS レベルでマーキングできます。QoS レベルはファブリック内の QoS アクションを定義します。

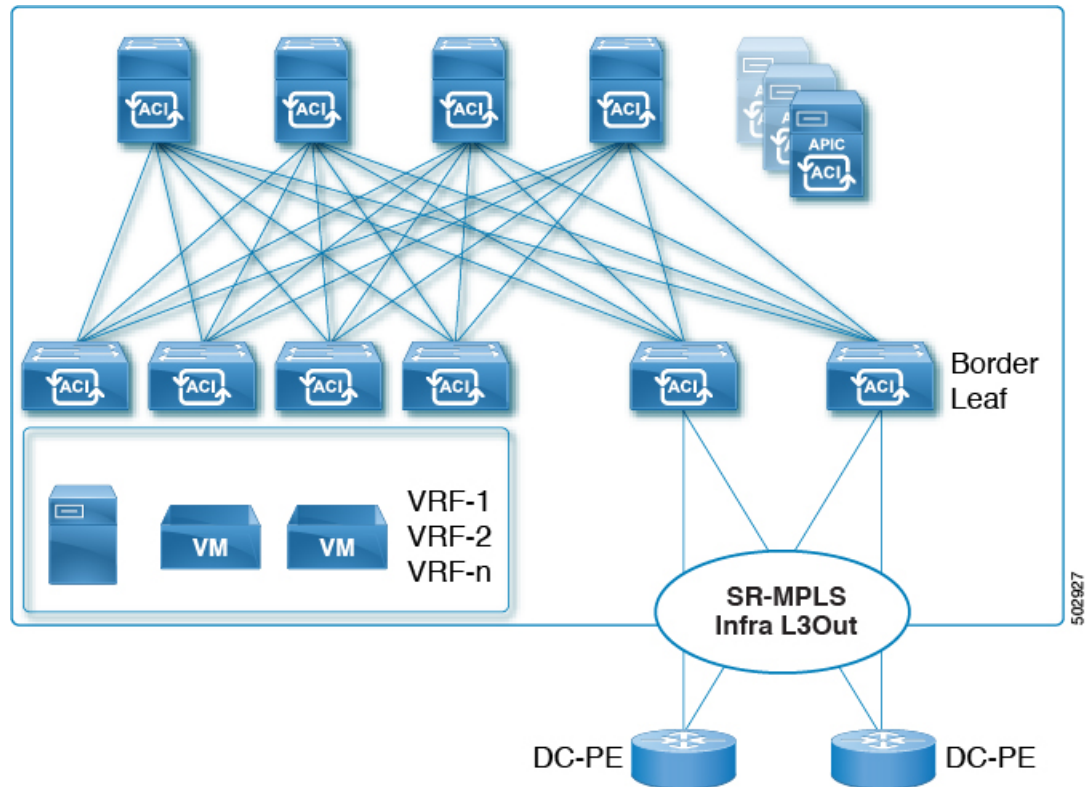
SR-MPLS ハンドオフの ACI 実装について

ACIは、Cisco APIC リリース 5.0(1) で導入された次の ACI コンポーネントを使用して SR-MPLS ハンドオフを実装します。

SR-MPLS インフラ L3Out

SR-MPLS インフラ L3Out は SR-MPLS 接続を提供します。境界リーフスイッチのインフラテナントで SR-MPLS インフラ L3Out を設定して、アンダーレイ MP-BGP EVPN セッションを SR-MPLS ハンドオフ用に設定します。テナント VRF は ACI SR-MPLS インフラ L3Out に選択的にマッピングされ、テナントサブネットを DC-PE ルータにアドバタイズし、DC-PE から MPLS VPN ルートをインポートします。SR-MPLS インフラ L3Out は、ポッドまたはリモートリーフスイッチサイトにスコープされ、ポッドまたはリモートリーフスイッチペアに拡張されません。

図 19: SR-MPLS インフラ L3Out



ポッドまたはリモートリーフスイッチサイトには、1つ以上のSR-MPLS インフラ L3Out を設定できます。

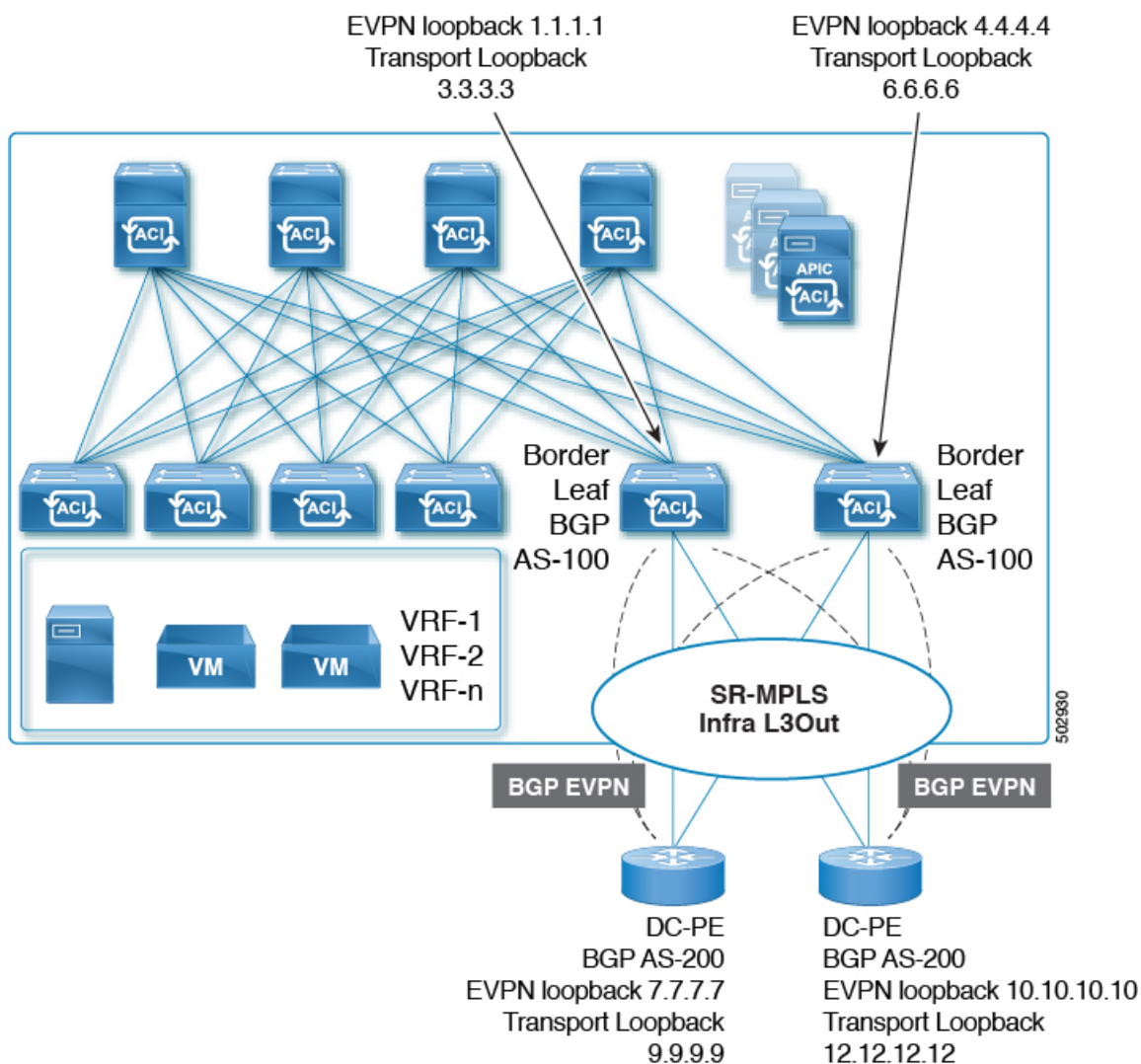
SR-MPLS インフラ L3Out の設定手順については、[GUI を使用した SR-MPLS インフラ L3Out の設定 \(196 ページ\)](#) を参照してください。

SR-MPLS インフラ L3Out の設定プロセスの一環として、次の領域を設定します。

- [ACI 境界リーフスイッチと DC-PE 間の MP-BGP EVPN セッション \(176 ページ\)](#)
- [BGP EVPN セッションのマルチホップ BFD \(178 ページ\)](#)
- [ACI 境界リーフスイッチおよびネクストホップルータでのアンダーレイ BGP セッション \(BGP ラベル付きユニキャストおよび IPv4 アドレスファミリ\) \(178 ページ\)](#)
- [BGP ラベル付きユニキャストセッションのシングルホップ BFD \(179 ページ\)](#)

ACI 境界リーフスイッチと DC-PE 間の MP-BGP EVPN セッション

次の図に示すように、境界リーフスイッチの EVPN ループバックと DC-PE ルータ間の MP-BGP EVPN セッションを設定するために必要な情報を提供する必要があります。



この領域では、次の設定が行われます。

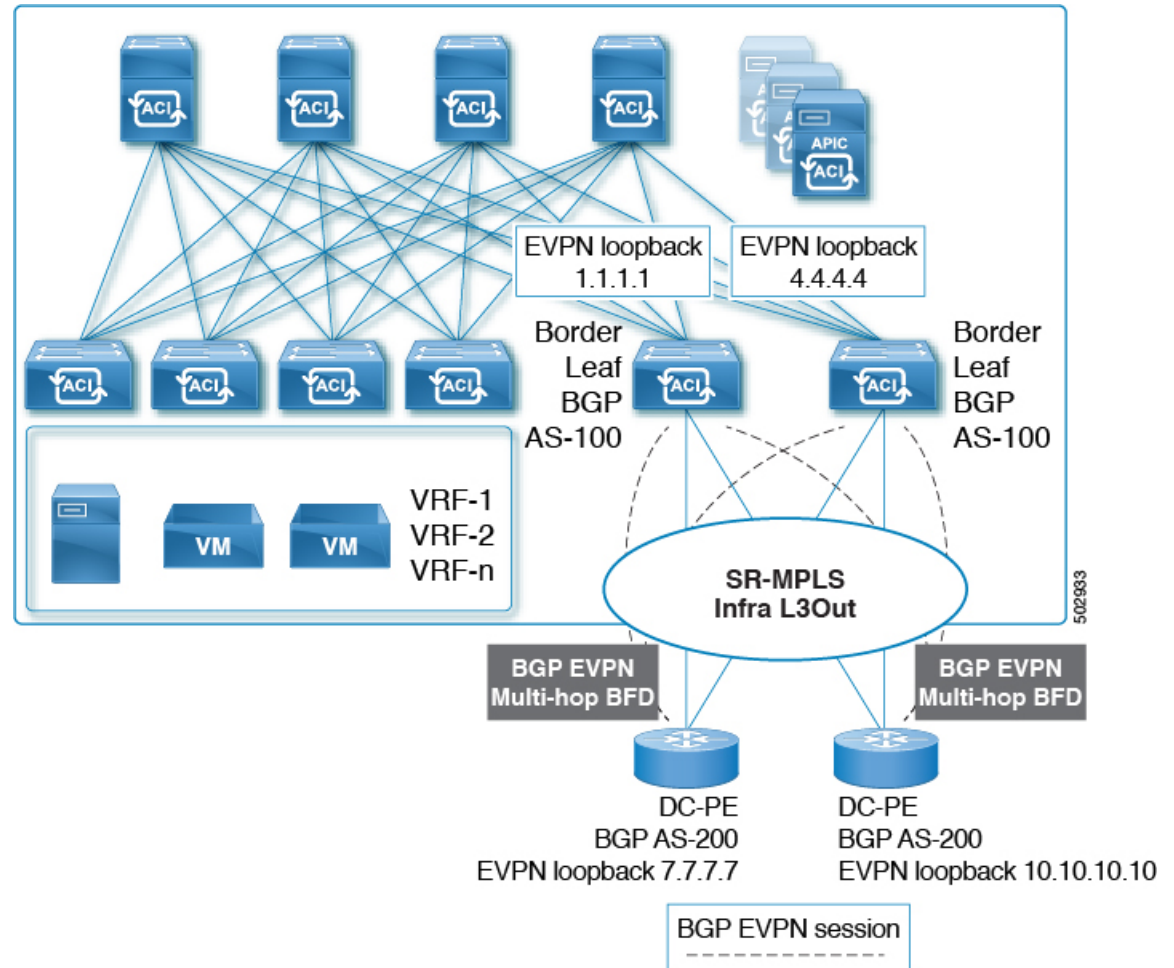
- BGP ラベル付きユニキャストアドレスファミリを使用したトランスポートループバックのラベルアドバタイズメント。
- SR-MPLS インフラ VRF の境界リーフスイッチ上の一意のルータ ID。
- ルータ ID は、BGP-EVPN ループバックおよびトランスポートループバックアドレスとは異なる必要があります。

図に示すように、MP-BGP EVPN とトランスポートのループバックに異なる IP アドレスを使用できますが、MP-BGP EVPN と ACI 境界リーフスイッチのトランスポートループバックに同じループバックを使用することを推奨します。

現時点では、eBGP セッションのみがサポートされていることに注意してください。

BGP EVPN セッションのマルチホップ BFD

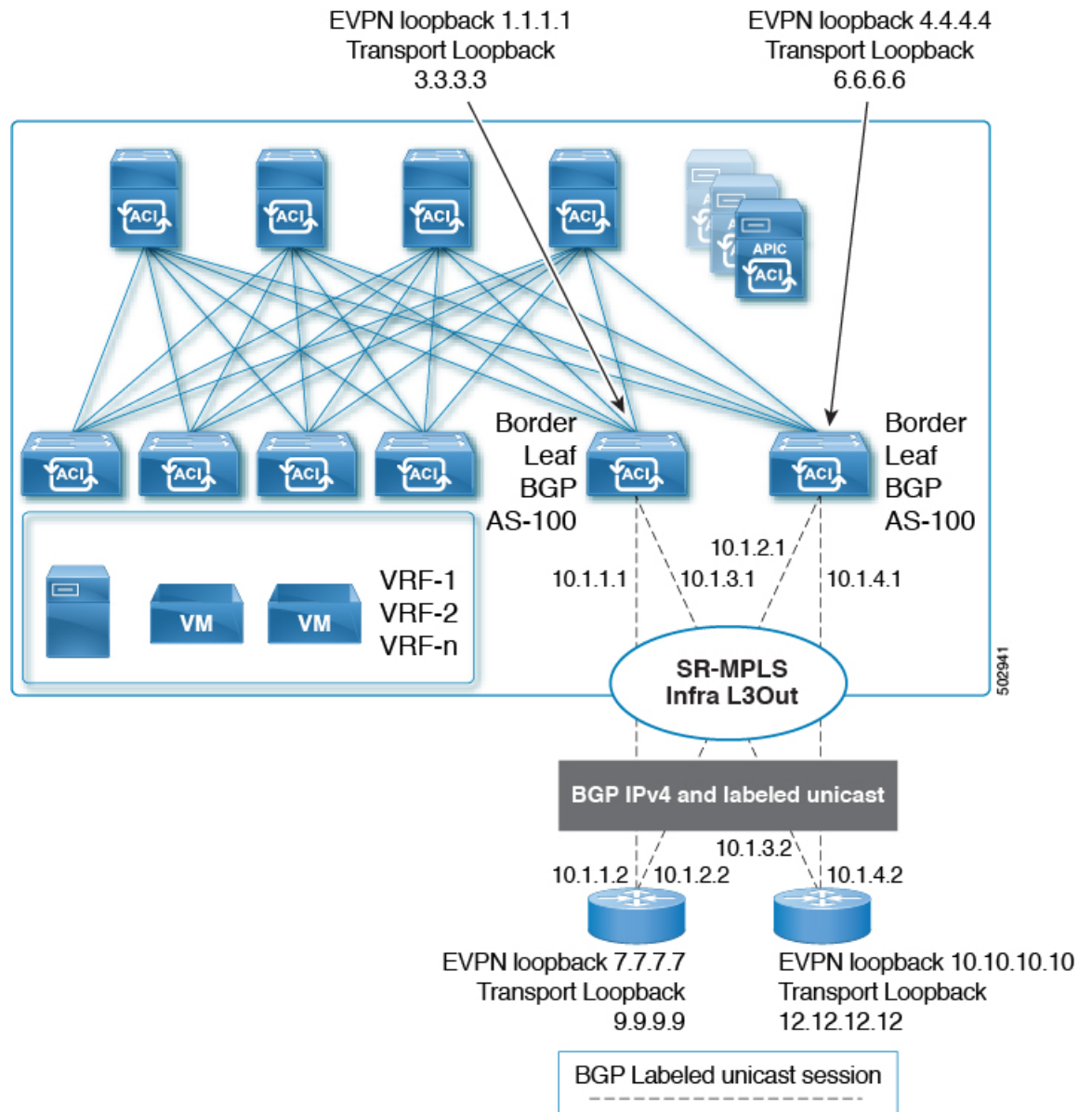
リリース5.0(1) から、次の図に示すように、マルチホップ BFD のサポートが可能になりました。この場合、EVPNループバック間にマルチホップ BFD EVPNセッションを設定できます。



ACI 境界リーフスイッチと DC-PE 間の BGP EVPN セッションでは、最小タイマーが 250 ミリ秒、検出乗数が 3 のマルチホップ BFD がサポートされます。要件に基づいてこのタイマー値を変更できることに注意してください。

ACI 境界リーフスイッチおよびネクストホップルータでのアンダーレイ BGP セッション (BGP ラベル付きユニキャストおよび IPv4 アドレス ファミリ)

また、次の図に示すように、ACI 境界リーフスイッチと DC-PE 間のインターフェイスごとに、BGP IPv4 とラベル付きユニキャストアドレス ファミリを設定します。

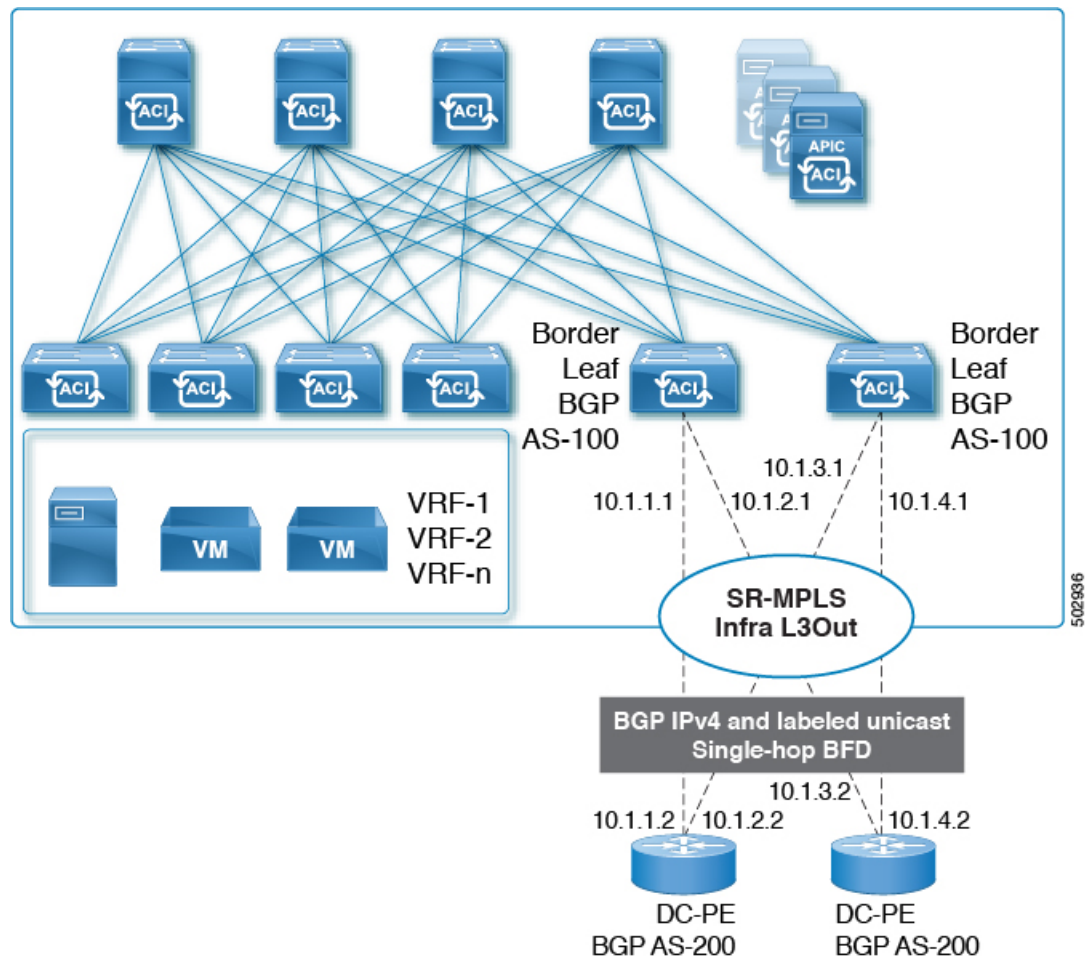


BGP IPv4アドレスファミリーはEVPN ループバックを自動的にアドバタイズし、BGP ラベル付きユニキャストアドレスファミリーはSR-MPLS ラベルを使用してSR トランスポート ループバックを自動的にアドバタイズします。

繰り返しますが、現時点ではeBGPセッションのみがサポートされています。

BGP ラベル付きユニキャストセッションのシングルホップ BFD

リンクがアップしたままで、リンクの転送機能が影響を受けるソフト障害に関連する問題を防ぐために、次に示すように、IPv4およびBGP ラベル付きユニキャストセッションのアンダーレイ BGPセッションのシングルホップBFDセッションを設定できます。次の図を参照してください。

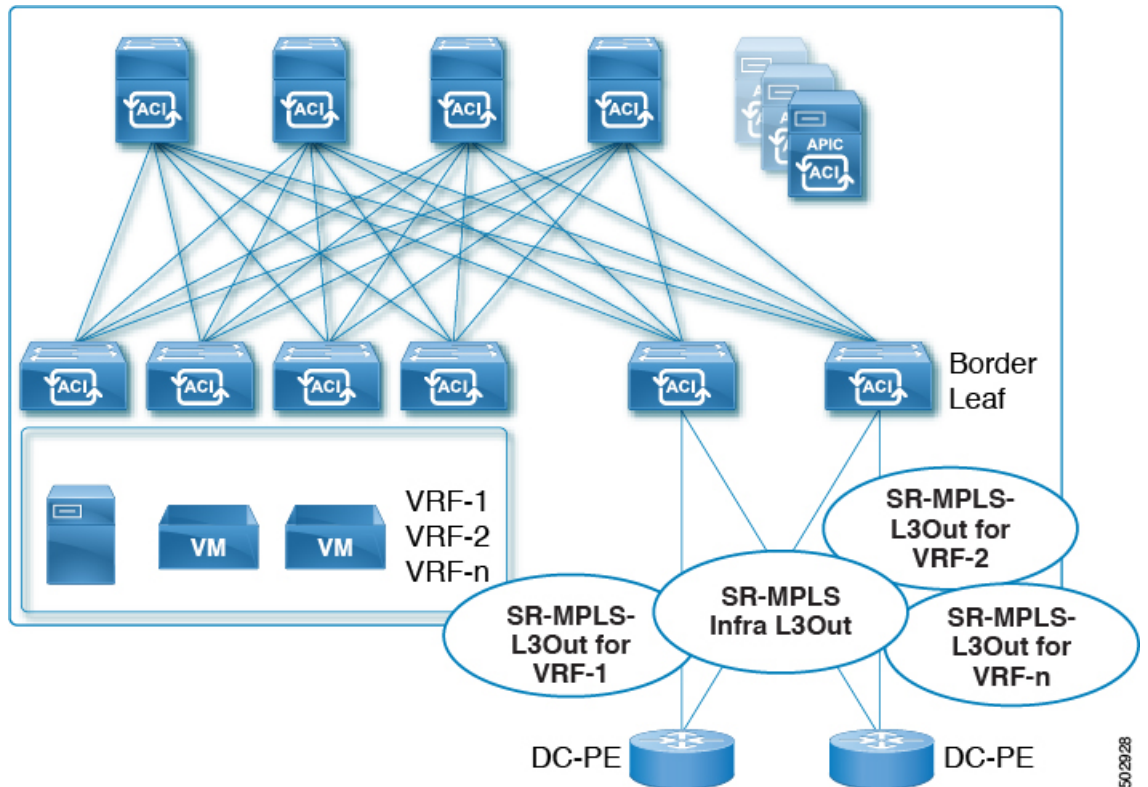


ACI 境界リーフ スイッチと DC-PE 間の BGP EVPN セッションでは、最小タイマーが 50 ミリ秒、検出乗数が 3 のシングルホップ BFD がサポートされます。要件に基づいてこのタイマー値を変更できることに注意してください。

SR-MPLS VRF L3Out

SR-MPLS トランスポートに対してプレフィックスをアドバタイズする必要がある各 VRF は、SR-MPLS インフラ L3Out に関連付ける必要があります。SR-MPLS インフラ L3Out に接続されている SR-MPLS VRF L3Out を使用して、これらのアソシエーションを設定します。

図 20 : User Tenant SR-MPLS L3Out



1つ以上の SR-MPLS VRF L3Out を同じ SR-MPLS インフラ L3Out に接続できます。SR-MPLS VRF L3Out を使用して、インポートおよびエクスポート ルート マップを設定し、次のことを実行できます。

- プレフィックスやコミュニティに基づいてルート ポリシーを適用する
- SR ネットワークにプレフィックスをアドバタイズする
- SR ネットワークから受信したプレフィックスを除外する

また、外部 EPG を各 SR-MPLS VRF L3Out テナントの 1つ以上のサブネットを設定します。これは次の目的で使用されます。

- セキュリティ ポリシー (コントラクト)
- ポリシーベース リダイレクト (PBR) ポリシー
- VRF 間のルート リーク

SR-MPLS VRF L3Out の設定手順については、[GUI を使用した SR-MPLS VRF L3Out の設定 \(205 ページ\)](#) を参照してください。

SR-MPLS カスタム QoS ポリシー

カスタム QoS ポリシーを使用して、MPLS ネットワークからのトラフィックを ACI ファブリック内で優先順位付けする方法を定義できます。これらのポリシーを使用して、MPLS L3Out を介してトラフィックがファブリックを離れるときに、トラフィックを再マーキングすることもできます。

カスタム QoS ポリシーを設定する場合、境界リーフ スイッチに適用される次の 2 つのルールを定義します。

- **入力ルール**：MPLS ネットワークに接続されている境界リーフ スイッチに着信するすべてのトラフィックは、MPLS Experimental ビット (EXP) 値に対してチェックされ、一致が検出されると、トラフィックは ACI QoS レベルに分類され、適切な CoS および Differentiated Services Code Point (DSCP) 値でマークされます。

値は、境界リーフでカスタム QoS 変換ポリシーを使用して取得されます。SR-MPLS からのトラフィックの元の DSCP 値は、再マーキングなしで保持されます。カスタムポリシーが定義されていないか、一致していない場合、デフォルトの QoS レベル (Level 13) が割り当てられます。

- **出力ルール**：トラフィックが境界リーフの MPLS インターフェイスから離れていくと、パケットの DSCP 値に基づいて照合され、一致が見つかると、MPLS EXP および CoS 値がポリシーに基づいて設定されます。

出力 MPLS QoS ポリシーが設定されていない場合、MPLS EXP はデフォルトでゼロになります。MPLS カスタム QoS ポリシーに基づいて設定されている場合は、EXP が再マーキングされます。

次の 2 つの図は、入力および出力ルールが適用されるタイミングと、内部 ACI トラフィックがファブリック内でパケットの QoS フィールドを再マーキングする方法を要約しています。

図 21: 入力 QoS

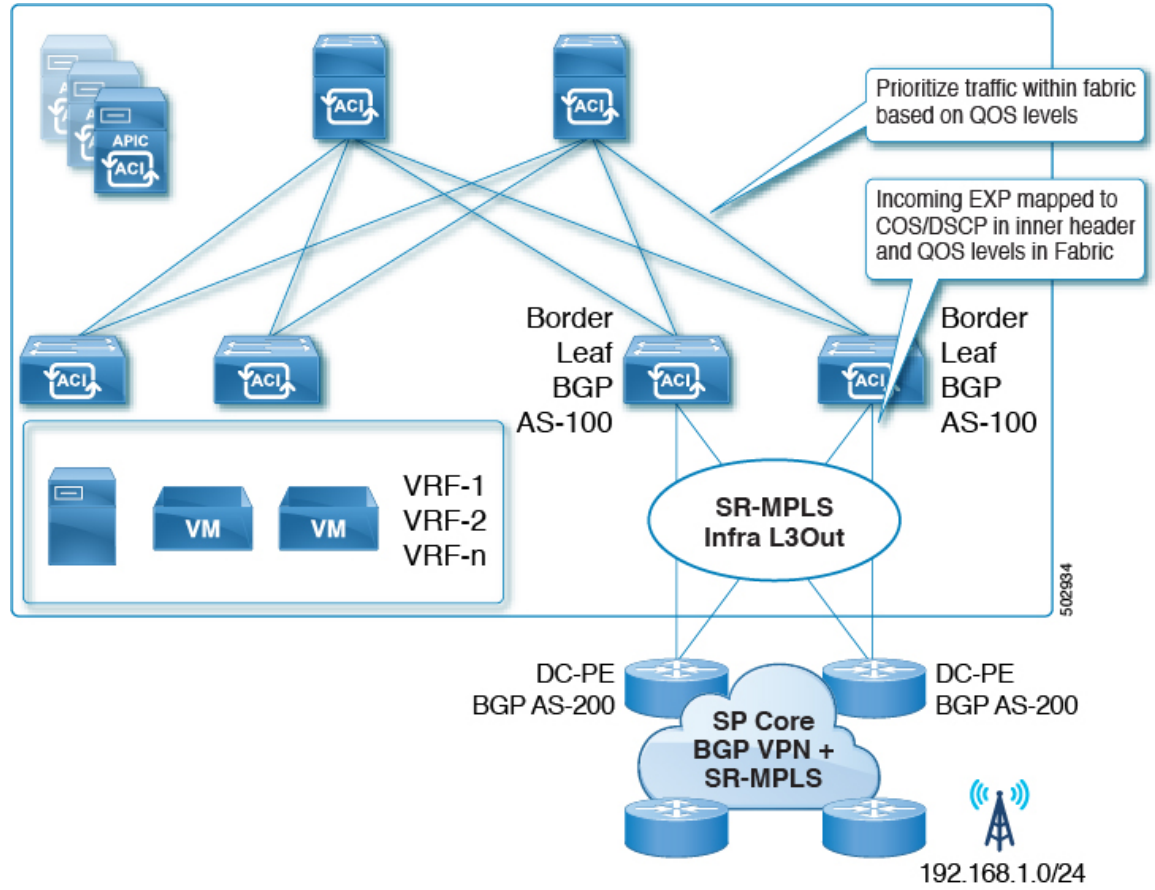
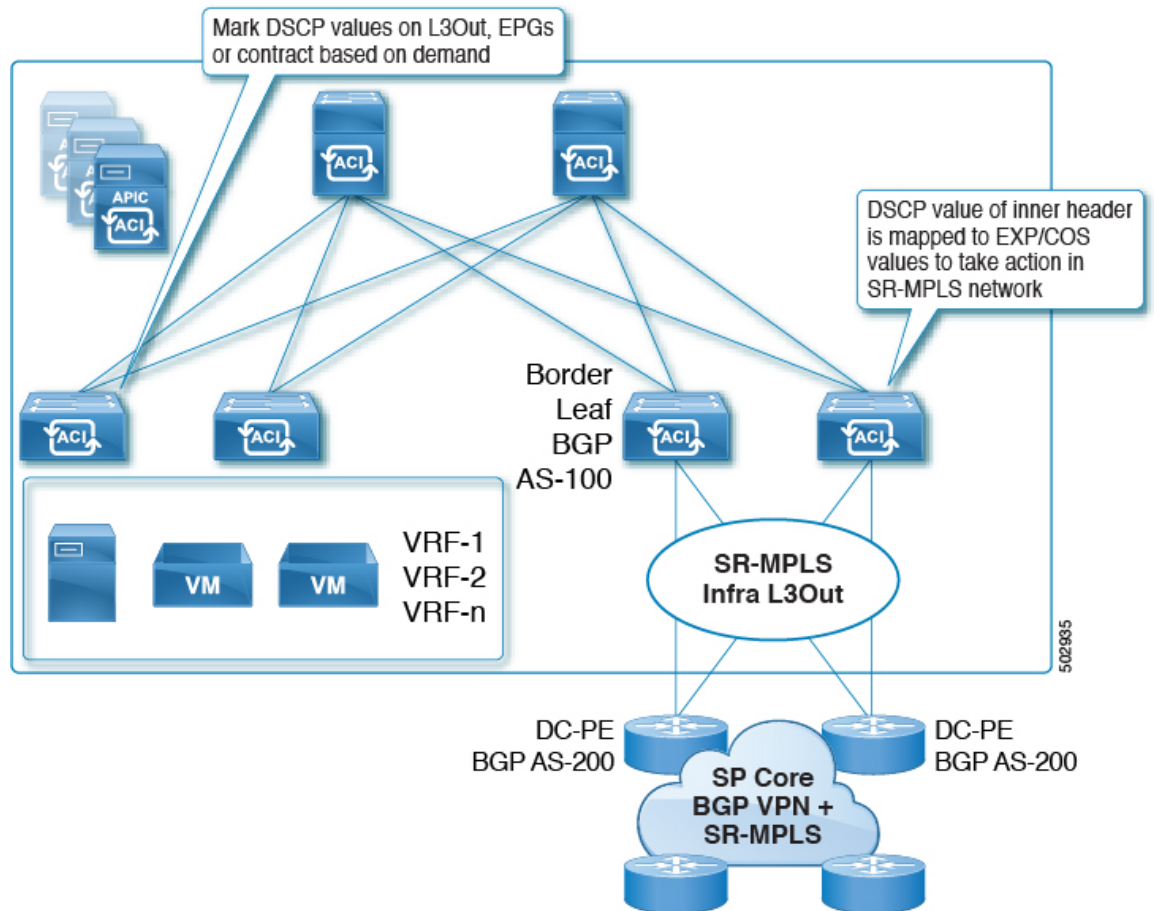


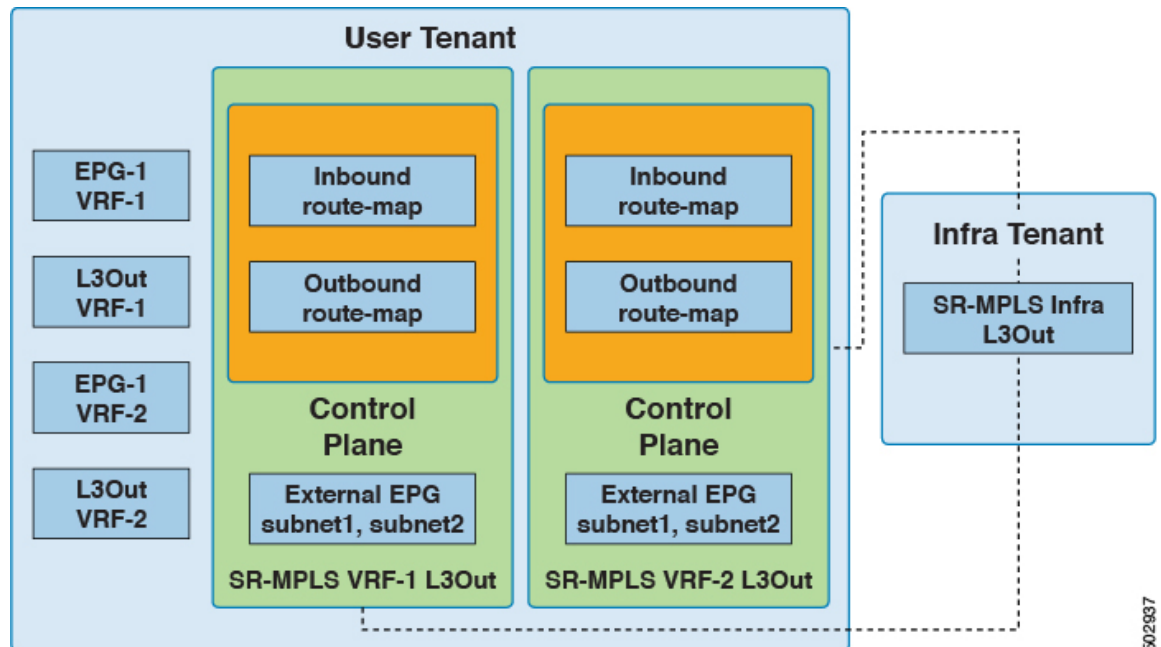
図 22: 入力 QoS



GUIを使用した SR-MPLS カスタム QoS ポリシーの作成 (208 ページ) の説明に従って、複数のカスタム QoS ポリシーを定義し、作成した各 SR-MPLS インフラ L3Out に適用できます。

SR-MPLS 設定モデルについて

次の図に、SR-MPLS ハンドオフの ACI 実装の設定モデルを示します。



SR-MPLS ハンドオフの設定は、次のテナント内で行われます。

- **Infra Tenant** : インフラテナントの下で、[SR-MPLS インフラ L3Out \(175 ページ\)](#) の説明に従って SR-MPLS インフラ L3Out を設定します。SR-MPLS インフラ L3Out では、ACI ファブリックと境界リーフスイッチに接続された外部デバイス間の接続を定義します。SR-MPLS インフラ L3Out でオーバーレイおよびアンダーレイ ノードパスを指定します。
- **ユーザテナント** : ユーザテナントの下に、図の左側の領域に示すように、複数の VRF、EPG、および L3Out がある場合があります。ユーザテナント内で、SR-MPLS ハンドオフ設定の一部として使用する SR-MPLS VRF L3Out を設定します。[SR-MPLS VRF L3Out \(180 ページ\)](#)

SR-MPLS VRF L3Out 内では、次のルートマップも設定します。

- **着信ルートマップ** : デフォルトでは、着信ルートマップのポリシーはすべてのプレフィックスを受け入れます。

明示的な着信ルートマップは、次のように設定できます。

- ファブリック内のアドバタイズメントを選択的に拒否するプレフィックスを一致させる
- プレフィックスとコミュニティを照合して、ファブリック内のアドバタイズメントを選択的に拒否する
- **アウトバウンドルートマップ** : ブリッジドメインサブネットを含む任意のプレフィックスをアドバタイズするために、アウトバウンドルートマップのポリシーを設定する必要があります。デフォルトでは、アウトバウンドルートマップのポリシーはプレフィックスをアドバタイズしません。

明示的なアウトバウンドルートマップは、次のように設定できます。

- SR-MPLS ネットワークにアダバタイズされるプレフィックスの照合
- SR-MPLS ネットワークにプレフィックスをアダバタイズするためのプレフィックスとコミュニティの照合
- プレフィックスやコミュニティの一致に基づいて、カラーコミュニティを含むコミュニティを設定します。

インバウンドルートマップとアウトバウンドルートマップの両方がコントロールプレーンで使用され、ファブリック内外で許可または拒否されるプレフィックスを設定します。

SR-MPLS VRF L3Out 内で、外部 EPG と、データプレーンに使用される該当の外部 EPG 内のサブネットも設定します。これらのサブネットは、ACIセキュリティポリシーを適用するために使用されます。外部 EPG サブネットは、フラグを使用して別の VRF のプレフィックスをリークするためにも使用されます。外部 EPG サブネットでルートリークとセキュリティフラグを有効にすると、そのサブネットは別の VRF にリークされる可能性があります。集約フラグを使用して外部 EPG サブネットを設定し、プレフィックスを別の VRF にリークすることもできます。この場合、リーフスイッチプレフィックスへのコントラクトを定義し、VRF 間の通信を許可する必要があります。

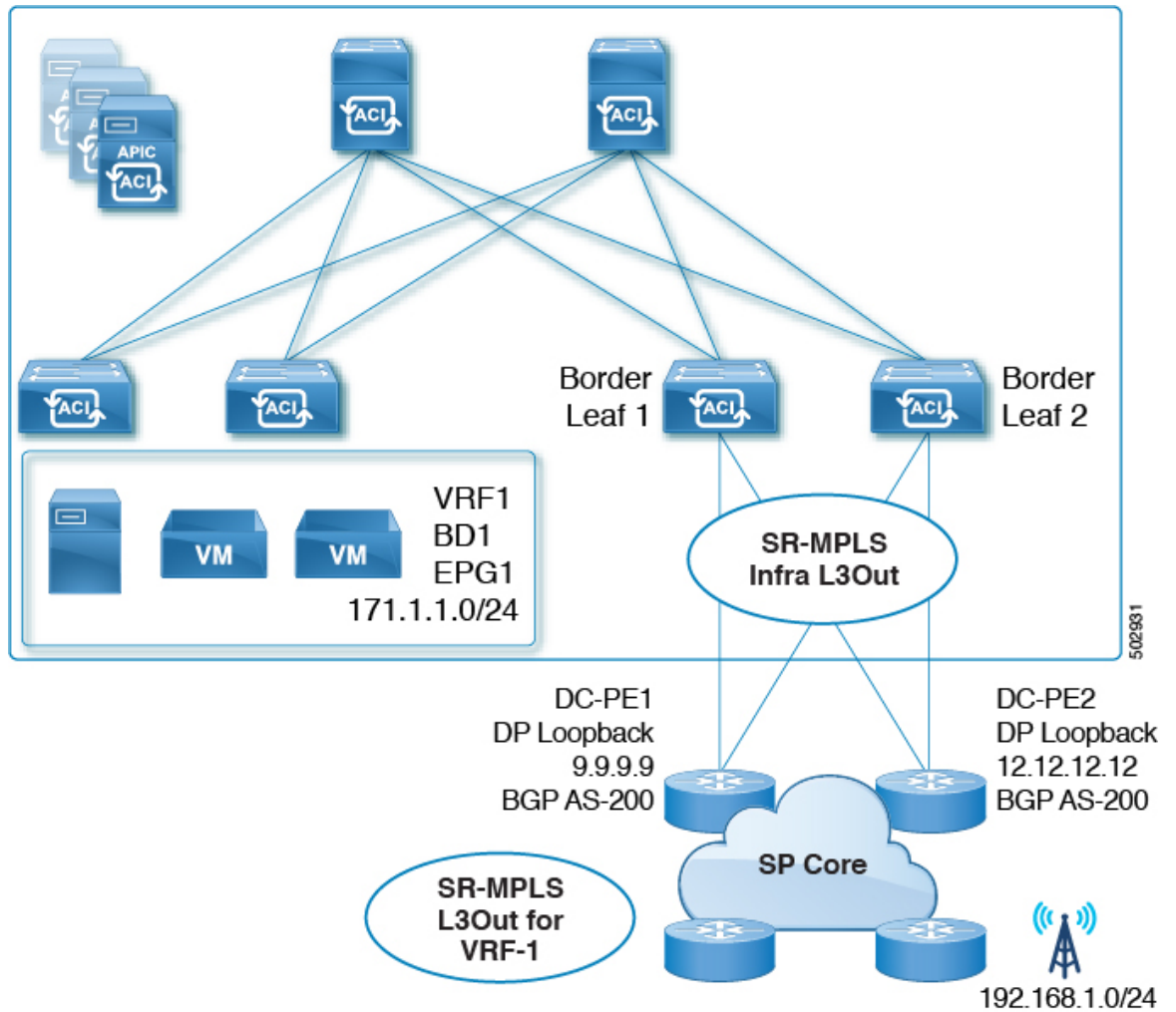


-
- (注) SR-MPLS VRF L3Out 上の外部 EPG は、ルートマップを適用してプレフィックスアダバタイズメントを拒否するなど、ルーティングポリシーには使用されません。
-

この例では、ユーザテナント内の SR-MPLS VRF-1 L3Out が SR-MPLS インフラ L3Out に接続され、ユーザテナント内の SR-MPLS VRF-2 L3Out も SR-MPLS インフラ L3Out に接続されます。

EPG to SR-MPLS L3Out

次の図は、EPG to SR-MPLS L3Out 設定の例を示します。

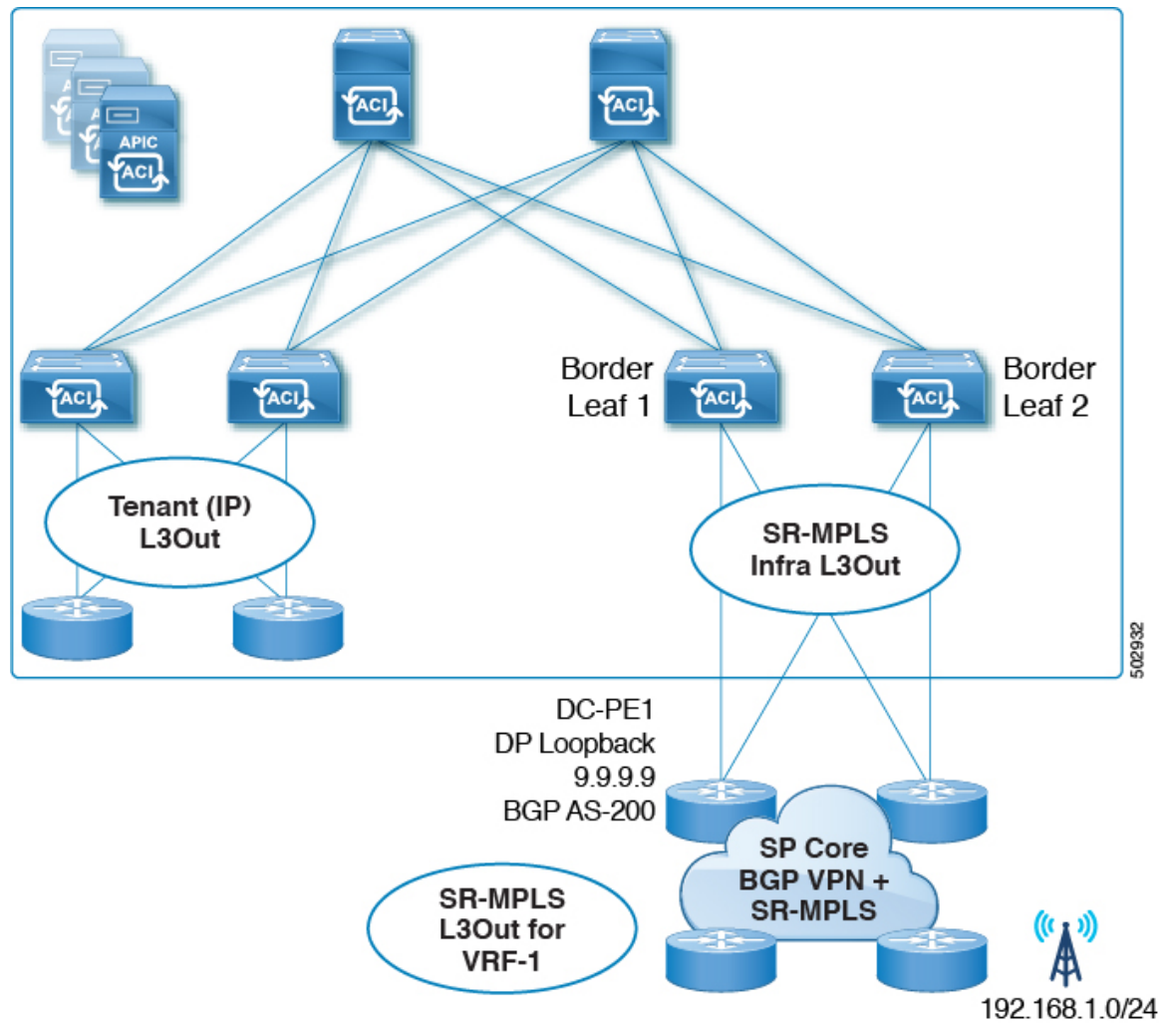


このシナリオでは、次の設定を行います。

- 境界リーフスイッチ（上図の BL1 と BL2）で SR-MPLS infra L3Out を設定します。
- EPG、ブリッジドメイン、およびユーザ VRF とともに、ユーザテナントで SR-MPLS VRF L3Out を設定します。
- プレフィックスのエクスポートおよびインポート用のルートマップを設定し、SR-MPLS VRF L3Out に適用します。
- EPG と SR-MPLS L3Out 間のトラフィック転送のために、EPG と SR-MPLS VRF L3Out で定義された外部 EPG の間に契約を設定し、適用します。

IP L3Out to SR-MPLS L3Out

次の図に、通常の IP L3Out と SR-MPLS L3Out の間の中継ルーティングを有効にする設定の例を示します。



このシナリオでは、前述の EPG から SR-MPLS L3Out への設定と同様の設定を行いますが、その違いは次のとおりです。

- 境界リーフスイッチ（上図の BL1 と BL2）で SR-MPLS infra L3Out を設定します。
- IP L3Out およびユーザ VRF とともに、ユーザテナントで SR-MPLS VRF L3Out を設定します。
- プレフィックスのエクスポートおよびインポート用のルートマップを設定し、SR-MPLS VRF L3Out に適用します。
- IP L3Out と SR-MPLS L3Out 間のトラフィック転送のために、IP L3Out と SR-MPLS VRF L3Out に関連付けられた外部 EPG 間にコントラクトを設定し、適用します。

注意事項と制約事項

次は、SR-MPLS ハンドオフ機能のガイドラインおよび制限事項です。

- [対応プラットフォーム \(189 ページ\)](#)
- [プラットフォームでの制限 \(189 ページ\)](#)
- [SR-MPLS インフラ L3Out のガイドラインと制約事項 \(190 ページ\)](#)
- [SR-MPLS VRF L3Out のガイドラインと制約事項 \(190 ページ\)](#)
- [MPLS スイッチングに関するガイドラインと制限事項 \(195 ページ\)](#)
- [SR-MPLS 統計情報のガイドラインと制約事項 \(196 ページ\)](#)

対応プラットフォーム

SR-MPLS ハンドオフ機能は、次のプラットフォームでサポートされます。

- **ボーダー リーフ スイッチ** : -FX スイッチ モデル以降 (たとえば、スイッチ名の末尾に「FX」、「FX2」、「FX3」、「GX」... が付いているスイッチ モデル)
- **スパイン スイッチ** :
 - ラインカード名の末尾に「LC-EX」、「LC-FX」、および「GX」が付いたモジュラ スパイン スイッチ モデル
 - 固定スパイン スイッチの Cisco Nexus 9000 シリーズ N9K-C9364C および N9K-C9332C
- **DC-PEルータ** :
 - Network Convergence System (NCS) 5500 シリーズ
 - ASR 9000 シリーズ
 - NCS 540 または 560 ルータ

プラットフォームでの制限

- FX プラットフォームでは、SR-MPLS 機能を有効にすると、MPLS が有効になっていない、または展開されていないポートを含むすべてのポートで MPLS 解析が有効になります。FX2 プラットフォーム以降では、MPLS 解析は、SR-MPLS が有効化または展開されているポートでのみ有効化されます。
- MPLS 解析が有効になっているポートでは、MPLS カプセル化パケットの純粋なレイヤ 2 スイッチングはサポートされていません。非 MPLS レイヤー 2 トラフィックは、問題なく、レイヤー 2 トランジットとして ACI ファブリックを使用できます。

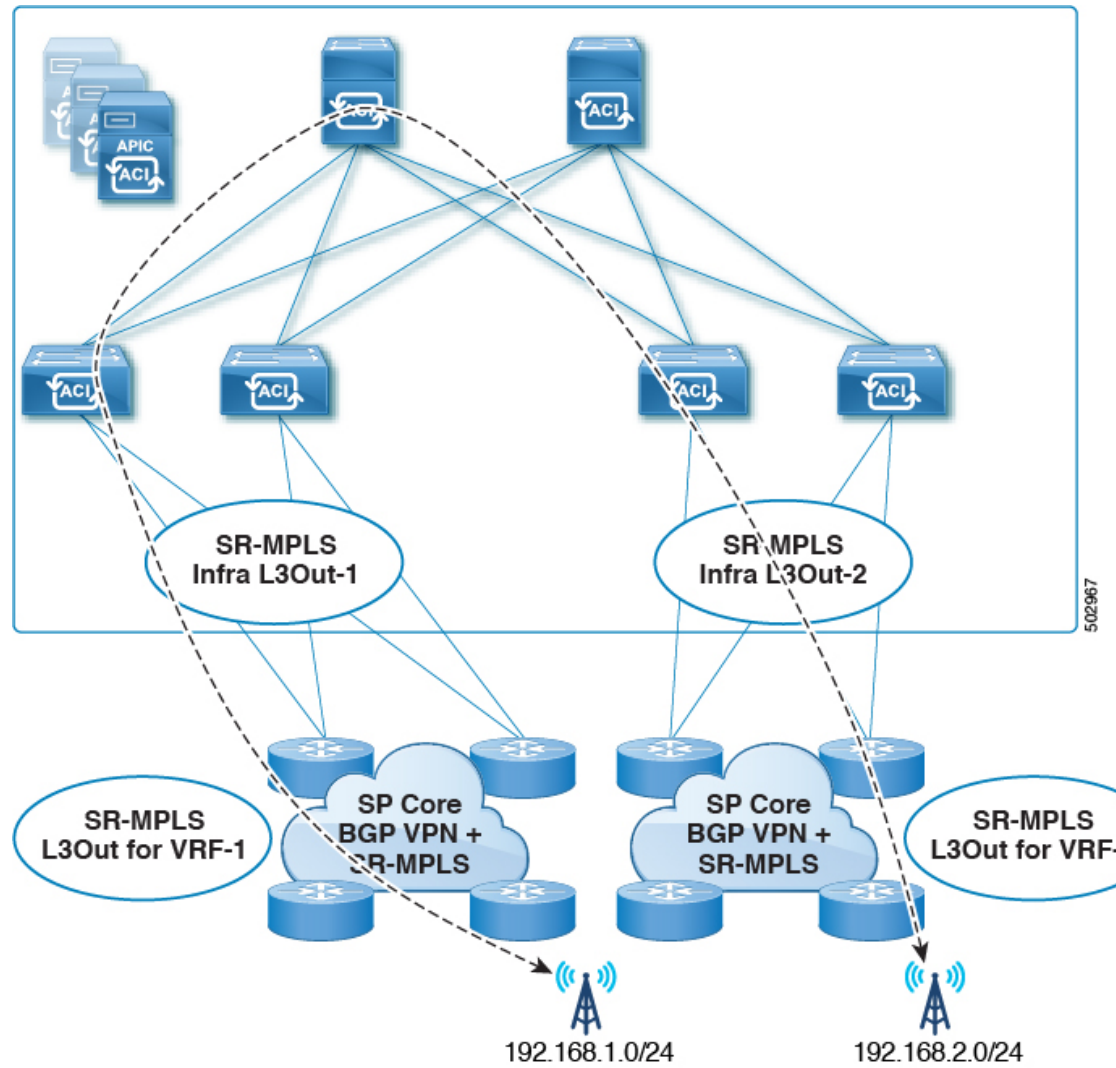
SR-MPLS インフラ L3Out のガイドラインと制約事項

- ボーダー リーフ スイッチが複数の SR-MPLS Infra L3Out にあることができる場合でも、ボーダー リーフ スイッチ/プロバイダ エッジ ルーターの組み合わせは1つの SR-MPLS L3Out になければなりません。ユーザ VRF/ボーダー リーフ スイッチ/プロバイダ エッジ ルートの組み合わせに対して1つのルーティング ポリシーのみが存在できるからです。
- 複数のポッドおよびリモート ロケーションから SR-MPLS 接続を確立する必要がある場合は、SR-MPLS 接続を使用するポッドおよびリモート リーフ ロケーションのそれぞれに異なる SR-MPLS インフラ L3Out があることを確認します。

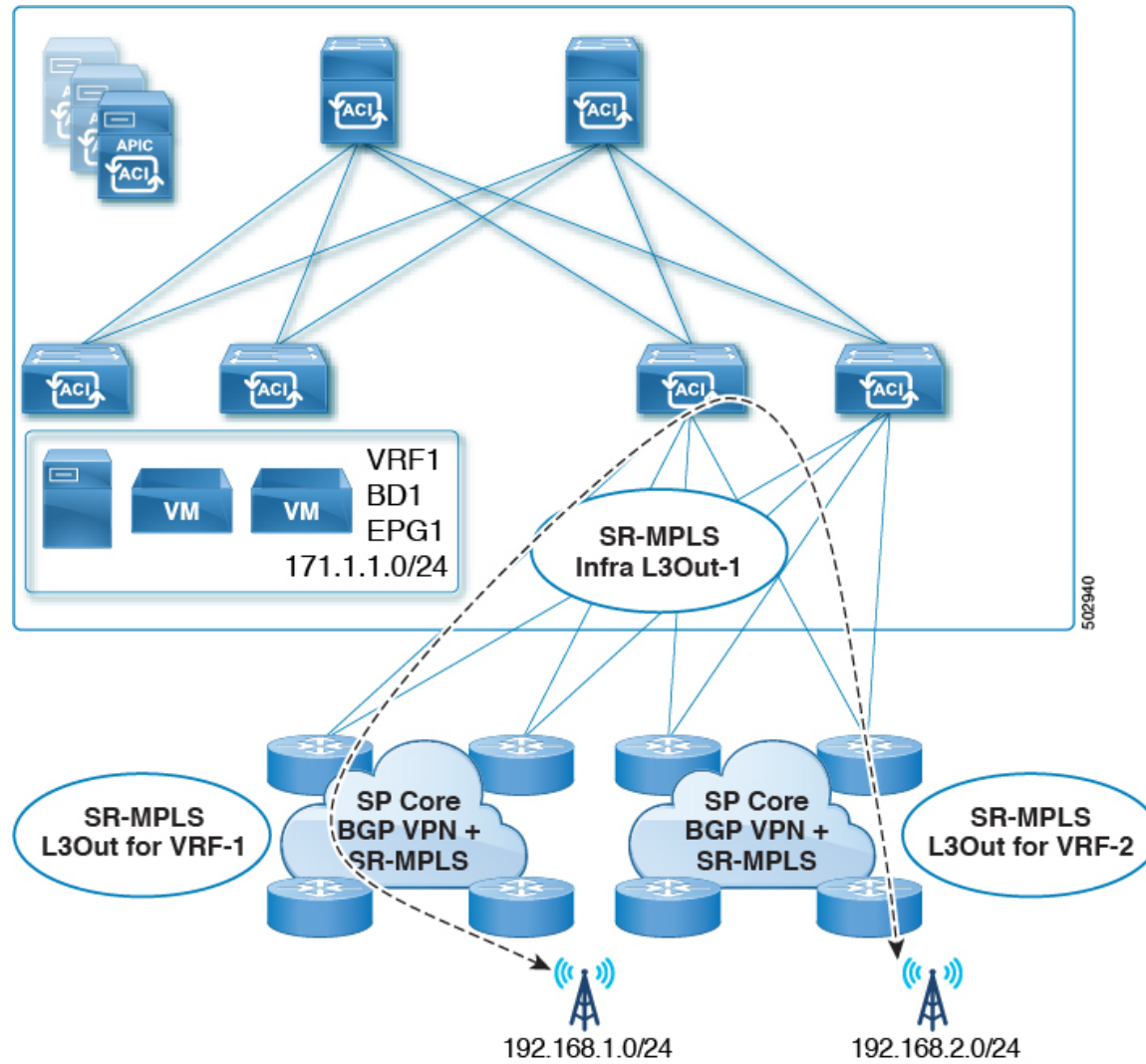
SR-MPLS VRF L3Out のガイドラインと制約事項

Routing Policy

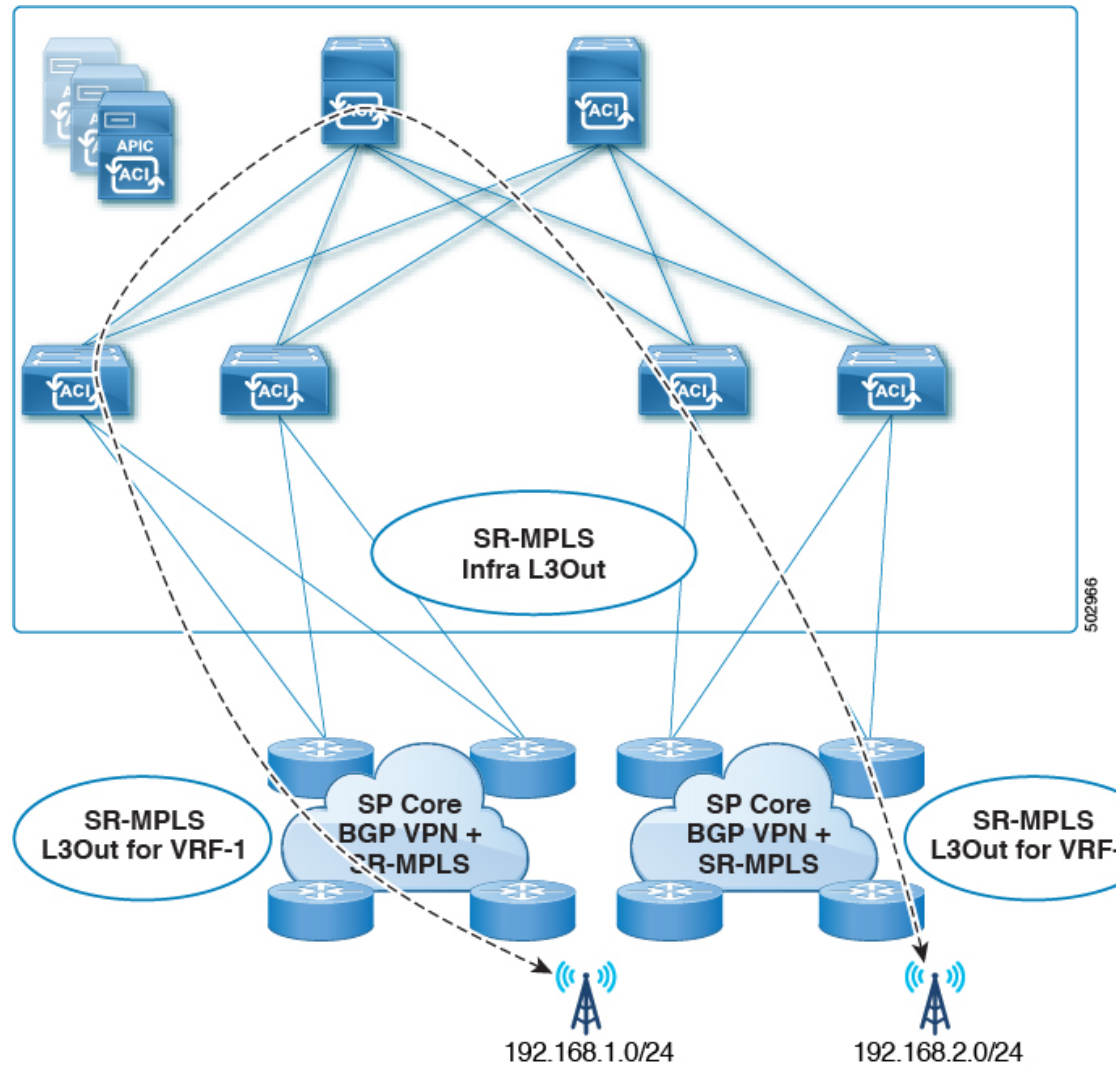
- 各 SR-MPLS VRF L3Out 内では、アウトバウンド ルート マップ (エクスポート ルーティング ポリシー) の定義は必須ですが、インバウンド ルート マップ (インポート ルーティング ポリシー) の定義はオプションです。
- SR-MPLS VRF L3Out に関連付けられているルーティング ポリシーは、グローバル タイプである必要があります。つまり、ブリッジ ドメイン サブ ネットを含むすべてのルートを明示的に追加する必要があります。
- ホストベース ルーティングは SR-MPLS ではサポートされません。
- 移行ルーティングがサポートされますが、一部の制約があります。
 - サポート対象：次の図に示すように、異なるボーダー リーフ ペアを使用する単一の VRF での SR-MPLS トラフィック。この設定では、各 SR-MPLS インフラ L3out (ボーダー リーフ ペア) を介して一意のプレフィックス範囲をアドバタイズする必要があります。また、トランスポート ネットワークにルーティング グループがないことを確認する必要があります (つまり、ファブリックがハブとして機能し、2つのトランスポート ネットワークがスポークとして機能している)。



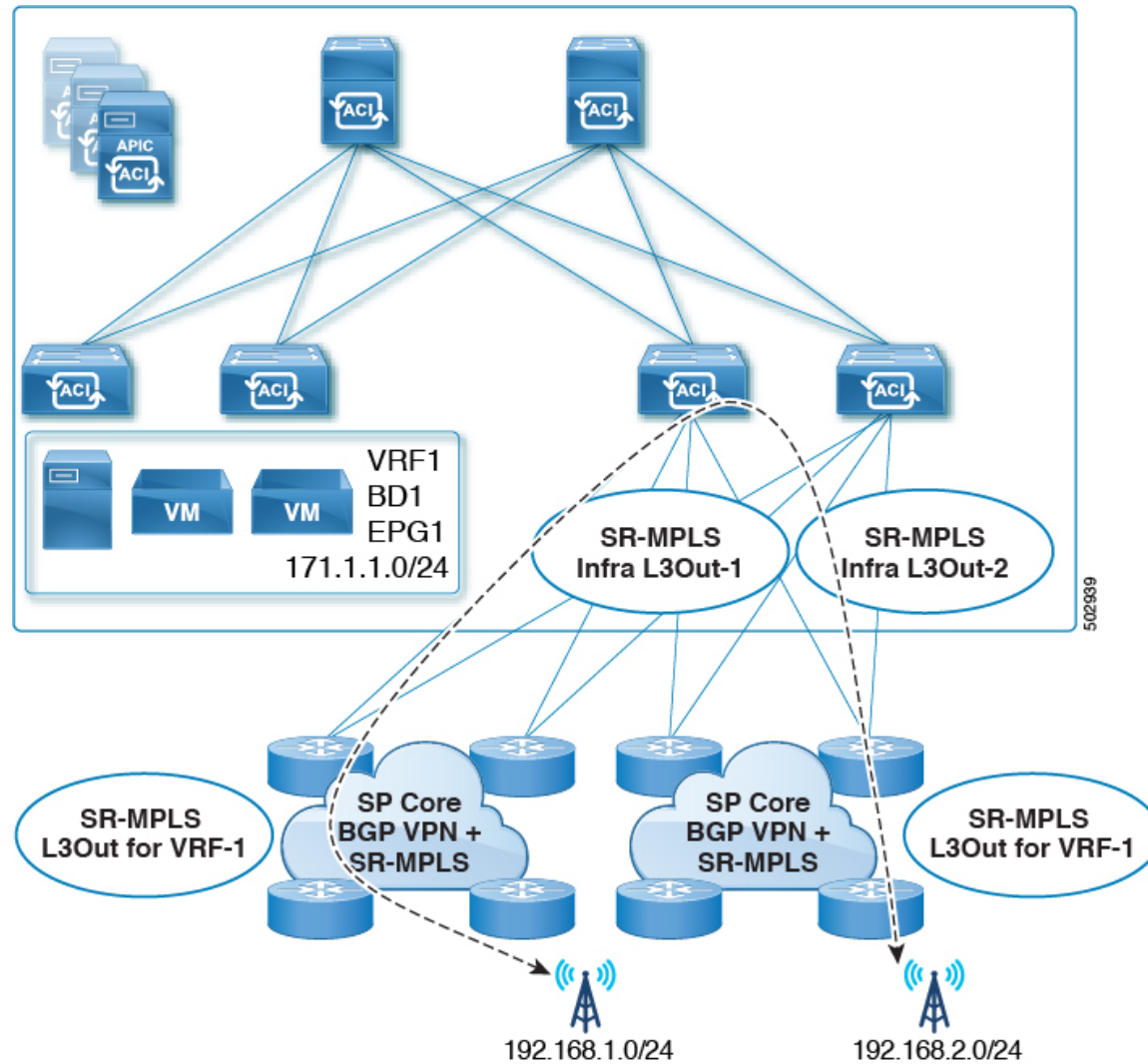
- サポート対象：次の図に示すように、同じ境界リーフ ペアと異なる VRF を持つ SR-MPLS トラフィック。



- サポート対象：次の図に示すように、異なる境界リーフペアと異なる VRF を持つ SR-MPLS トラフィック。



- 次の図に示すように、同じ VRF 内および同じ境界リーフ ペア上の SR-MPLS トラフィックを中継します。
 - リリース 5.1(1) よりも前のリリースではサポートされません。
 - リリース 5.1(1) 以降でサポートされます。システムでの一時的なループを回避するために、再発信されたルートが同じ Infra L3Out ピアにアダプタイズされないようにします。



- リーフスイッチが複数のSR-MPLS インフラ L3Out で設定されている場合、プレフィックスが単一のプレフィックスリスト (1つの一致ルール) で設定されていれば、同じサブネットをすべての L3Out からアドバタイズできます。その後、そのプレフィックスリストのルートマップは、すべての SR-MPLS VRF L3Out に関連付けられます。

たとえば、次のようなコンフィギュレーションがあるものとします。

- サブネット S1 と S2 を持つ単一のプレフィックスリスト P1
- ルートマップ R1 に関連付けられている SR-MPLS VRF L3Out 1 (プレフィックスリスト P1)
- ルートマップ R2 に関連付けられている SR-MPLS VRF L3Out 2 (プレフィックスリスト P1)

プレフィックスは同じプレフィックスリスト (P1) に設定されているため、異なる SR-MPLS VRF L3Out に関連付けられていても、プレフィックス リスト P1 内の同じサブネットが両方の L3Out からアドバタイズされます。

一方、次の設定を検討します。

- 2つのプレフィックス リスト
 - プレフィックス リスト P1、サブネット S1 および S2
 - プレフィックス リスト P2、サブネット S1 および S2
- ルート マップ R1 に関連付けられている SR-MPLS VRF L3Out 1 (プレフィックス リスト P1)
- ルート マップ R2 に関連付けられている SR-MPLS VRF L3Out 2 (プレフィックス リスト P2)

プレフィックスは2つのプレフィックスリスト (P1 と P2) で設定され、異なる SR-MPLS VRF L3Out に関連付けられているため、サブネット S1 と S2 は両方の L3Out からアドバタイズされません。

Security Policy

- SR-MPLS VRF L3Out 内で定義されている外部 EPG インスタンス プロファイルを使用してセキュリティ ポリシーを設定できます。外部 EPG インスタンス プロファイルには、1つ以上の SR-MPLS インフラ L3Out から SR-MPLS ネットワークを介して到達可能な IP プレフィックスが含まれており、同じセキュリティ ポリシーが必要です。
- 外部 EPG インスタンス プロファイルで 0/0 プレフィックスを設定して、外部 EPG の一部として、任意の外部 IP アドレスから発信された着信トラフィックフローを分類できます。
- 外部 EPG インスタンス プロファイルの外部 EPG を 1つ以上の SR-MPLS VRF L3Out に関連付けることができます。外部 EPG インスタンス プロファイルが複数の SR-MPLS インフラ L3Out の外部にある場合、複数の SR-MPLS VRF L3Out は同じ外部 EPG インスタンス プロファイルを指します。
- ローカル EPG と外部 EPG インスタンス プロファイル間、または異なる VRF L3Out に関連付けられた外部 EPG 間でコントラクトを設定する必要があります (中継ルーティングを有効にするため)。

MPLS スイッチングに関するガイドラインと制限事項

次に、MPLS QoS のデフォルトの動作を示します。

- サービスクラス (COS) の保持は、宛先ポートが MPLS ポートである ToR 内 MPLS 出力 QoS ポリシーではサポートされません。
- 境界リーフ スイッチ上のすべての受信 MPLS トラフィックは QoS レベル 3 (デフォルトの QoS レベル) に分類されます。

- 境界リーフ スイッチは、再マーキングなしで SR-MPLS からのトラフィックの元の DSCP 値を保持します。
- 境界リーフ スイッチは、デフォルトの MPLSEXP (0) のパケットを SR-MPLS ネットワークに転送します。

次に、MPLS カスタム QoS ポリシーを設定する際のガイドラインと制約事項を示します。

- データ プレーン ポリサー (DPP) は、SR-MPLS L3Out ではサポートされていません。
- レイヤ 2 DPP は、MPLS インターフェイスの入力方向で動作します。
- レイヤ 2 DPP は、出力カスタム MPLS QoS ポリシーがない場合、MPLS インターフェイスの出力方向で動作します。
- VRF レベルのポリシングはサポートされていません。

SR-MPLS 統計情報のガイドラインと制約事項

次に、SR MPLS 統計情報のガイドラインと制限事項を示します。

- SR-MPLS 統計情報を表示するには、リーフ スイッチで SR-MPLS 設定をイネーブルにするときに、ワンタイム ステートフル リロードを実行する必要があります。
- SR-MPLS インターフェイスの統計情報は、スイッチ名の末尾に「FX2」または「GX」がある境界リーフ スイッチ モデルでのみサポートされます。
- SR-MPLS VRF 統計情報は、スイッチ名の末尾が「FX」、「FX2」、または「GX」である境界リーフ スイッチ モデルでサポートされます。
- 15 分間の履歴統計の場合、15 分の間隔データを更新するのに 20 分かかることがあります。

GUI を使用した SR-MPLS インフラ L3Out の設定

- SR-MPLS インフラ L3Out は、境界リーフスイッチで設定され、SR-MPLS ハンドオフに必要なアンダーレイ BGP-LU およびオーバーレイ MP-BGP EVPN セッションを設定するために使用されます。
- SR-MPLS インフラ L3Out は、ポッドまたはリモートリーフ スイッチ サイトにスコープされます。
- ポッドまたはリモートリーフ スイッチ サイトには、1 つ以上の SR-MPLS インフラ L3Out を設定できます。

SR-MPLS インフラ L3Out を設定する場合は、次の項目を設定します。

- ノード

- リーフスイッチのみが SR-MPLS インフラ L3Out のノードとして設定できます（境界リーフスイッチおよびリモートリーフスイッチ）。
- 各 SR-MPLS インフラ L3Out は、1つのポッドからの境界リーフスイッチまたは同じサイトからのリモートリーフスイッチを持つことができます。
- 各境界リーフスイッチまたはリモートリーフスイッチは、複数の SR-MPLS ドメインに接続する場合、複数の SR-MPLS インフラ L3Out で設定できます。
- また、ノードの下にループバックインターフェイスを設定し、ループバックインターフェイスの下にノード SID ポリシーを設定します。

• インターフェイス

- サポートされるインターフェイスのタイプは次のとおりです。
 - ルーテッドインターフェイスまたはサブインターフェイス
 - ルーテッドポートチャネルまたはポートチャネルサブインターフェイス
- サブインターフェイスでは、任意の VLAN タグがサポートされます。
- また、SR-MPLS infra L3Out のインターフェイスエリアの下にアンダーレイ BGP ピアポリシーを設定します。

• QoS ルール

- MPLS 入力ルールと MPLS 出力ルールは、SR-MPLS インフラ L3Out の MPLS QoS ポリシーを使用して設定できます。
- MPLS QoS ポリシーを作成しない場合、入力 MPLS トラフィックにはデフォルトの QoS レベルが割り当てられます。

また、SR-MPLS インフラ L3Out を使用してアンダーレイとオーバーレイを設定します。

- アンダーレイ：インターフェイス設定の一部としての BGP ピア IP（BGP LU および IPv4 ピア）設定。
- オーバーレイ：論理ノードプロファイル設定の一部としての MP-BGP EVPN リモート IPv4 アドレス（MP-BGP EVPN ピア）設定。

始める前に

- [注意事項と制約事項（189 ページ）](#) で提供されている SR-MPLS ガイドラインと制約事項を確認します。特に、[SR-MPLS インフラ L3Out のガイドラインと制約事項（190 ページ）](#) で提供されているガイドラインと制約事項を確認してください。
- に示す手順を使用して、MPLS カスタム QoS ポリシーを設定します。[GUI を使用した SR-MPLS カスタム QoS ポリシーの作成（208 ページ）](#)

ステップ1 [テナント (Tenants)] > [インフラ (infra)] > [ネットワーキング (Networking)] > [SR-MPLS Infra L3Outs] に移動します。

ステップ2 [SR-MPLS Infra L3Outs] を右クリックし、[SR-MPLS インフラ L3Out の作成 (Create SR-MPLS Infra L3Out)] を選択します。

[接続 (Connectivity)] ウィンドウが表示されます。

Create SR-MPLS Infra L3Out

1. Connectivity 2. Nodes And Interfaces

Connectivity

SR-MPLS Infra Layer3 outside (L3out) is required to configure SR/MPLS handoff from ACI. SR-MPLS Infra L3out configures following important components of ACI to SR handoff:

- BGP EVPN session from ACI Border Leaf (BL) to remote BGP peer - ACI BL can advertise SR/MPLS labels for multiple VRFs using a single BGP session. BGP EVPN session is formed between EVPN loopbacks of BL and DC Provider Edge (DC-PE) router. By doing so removes the need for per VRF sub-interface and routing protocol session from BL to DC-PE. We recommend enabling Multi-hop BFD for faster convergence. Multiple BGP EVPN session can be configured on each BL.
- BGP-LU and IPv4 address family - To provide reachability to router (DC-PE) from BL. BGP-LU between ACI BL and router is used to advertise SR/MPLS labels for transport loopback of the ACI BL and router BGP-IPv4 address family between ACI BL and router is used to provide reachability between BGP-EVPN control plane loopbacks. We recommend enabling Single-hop BFD for faster convergence.
- MPLS custom QoS policy to the ingress and egress SR/MPLS QoS for the SR-MPLS handoff.

Prerequisites:

- Configure the node, port, functional profile, AEP, and Layer 3 domain.

Name: Layer 3 Domain:

Pod: MPLS Custom QoS Policy:

BGP-EVPN Connectivity

BFD Multihop Policy:

BGP-EVPN Remote IPv4 Address: Remote ASN: TTL:

Previous Cancel Next

ステップ3 [接続 (Connectivity)] ウィンドウで、必要な情報を入力します。

a) [名前 (Name)] フィールドに、SR-MPLS Infra L3Out の名前を入力します。

これは外部への接続を制御するポリシーに付ける名前です。名前では最大 64 文字までの英数字を使用できます。

(注) オブジェクトの作成後は、この名前は変更できません。

b) [レイヤ3 ドメイン (Layer 3 Domain)] フィールドで、既存のレイヤ3 ドメインを選択するか、[L3 ドメインの作成 (Create L3 Domain)] を選択して新しいレイヤ3 ドメインを作成します。

c) マルチポッド設定がある場合は、[ポッド (Pod)] フィールドでポッドを選択します。

マルチポッド設定がない場合は、選択をポッド1のままにします。

- d) (任意) [MPLS カスタム QoS ポリシー (MPLS Custom QoS Policy)] フィールドで、既存の QoS ポリシーを選択するか、[MPLS カスタム QoS ポリシーの作成 (Create MPLS Custom QoS Policy)] を選択して新しい QoS ポリシーを作成します。

新しい QoS ポリシーの作成の詳細については、を参照してください。 [GUI を使用した SR-MPLS カスタム QoS ポリシーの作成 \(208 ページ\)](#)

カスタム QoS ポリシーを作成しない場合は、次のデフォルト値が割り当てられます。

- 境界リーフスイッチ上のすべての着信 MPLS トラフィックは、QoS レベル3 (デフォルトの QoS レベル) に分類されます。
 - 境界リーフ スイッチは次の処理を実行します。
 - 再マーキングなしで SR-MPLS からのトラフィックの元の DSCP 値を保持します。
 - COS 保存が有効な場合、テナントトラフィックの元の COS 値を使用してパケットを MPLS ネットワークに転送します。
 - デフォルトの MPLS EXP 値 (0) のパケットを SR-MPLS ネットワークに転送します。
 - また、境界リーフスイッチは、SR ネットワークへの転送中に、アプリケーションサーバから着信するテナントトラフィックの元の DSCP 値を変更しません。
- e) [BGP-EVPN 接続 (BGP-EVPN Connectivity)] 領域に移動します。
- f) (任意) [BFD マルチホップポリシー (BFD Multihop Policy)] フィールドで、既存の BFD マルチホップポリシーを選択するか、[BFD マルチホップノードポリシーの作成 (Create BFD Multihop Node Policy)] を選択して新しいポリシーを作成します。
- 境界リーフスイッチから DC-PE への MP-BGP EVPN マルチホップセッションがある場合、BFD マルチホップポリシー オプションを有効にすると、BGP セッションは通常の BGP タイマーに依存しません。代わりに、BFD タイマーに基づいて、より速く終了します。詳細については、「[BGPEVPN セッションのマルチホップ BFD \(178 ページ\)](#)」を参照してください。
- g) [BGP-EVPN リモート IPv4 アドレス (BGP-EVPN Remote IPv4 Address)] フィールドに、MP-BGP EVPN リモート IPv4 アドレスを入力します。
- この BGP ピア IP アドレスは、オーバーレイ設定の一部です。これは、DC-PE のループバック アドレスです (リモート DC-PE ごとに 1 エントリ)。
- h) [リモート ASN (Remote ASN)] フィールドに、DC-PE のネイバー自律システムを一意に識別する番号を入力します。
- 自律システム番号は、1 ~ 4294967295 のプレーン形式で 4 バイトにすることができます。
- (注) ACI は asdot または asdot + 形式の AS 番号をサポートしていません。asdot または asdot + 形式の AS 番号の詳細については、『[Explaining 4-Byte Autonomous System \(AS\) ASPLAIN and ASDOT Notation for Cisco IOS](#)』を参照してください。 https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/border-gateway-protocol-bgp/white_paper_c11_516829.html
- i) [TTL] フィールドに、接続存続可能時間 (TTL) を入力します。

有効な範囲は 1 ~ 255 ホップです。

- j) [次へ (Next)] をクリックします。

[ノードとインターフェイス (Nodes and Interfaces)] ウィンドウが表示されます。

Create SR-MPLS Infra L3Out

1. Connectivity 2. Nodes And Interfaces

Nodes and Interfaces

Select the Border leaf (BL) switches for the SR-MPLS configuration. Configure BGP-EVPN control plane loopback, router id and transport loopback for each BL. Multiple interface can be configured for each BL, and for each interface of BL, BGP labeled unicast (BGP-LU) peer is configured. BGP IPv4 address family is automatically enabled once BGP-LU peer is configured. Single hop BFD can be enabled for each BGP-LU and IPv4 address family session.

Node Profile Name:

Interface Profile Name:

BFD Interface Policy:

Transport Data Plane:

Interface Types

Layer 3:

Layer 2:

Nodes

Node ID	Router ID	BGP-EVPN Loopback	MPLS Transport Loopback	Segment ID (SID) Index	
<input type="text" value="select an option"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="+ Hide Interfaces"/>

Interface	VLAN Encap	MTU (bytes)	IPv4 Address	Peer IPv4 Address	Remote ASN	
<input type="text" value="Select a port"/>	<input type="text"/>	<input type="text" value="9000"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="+"/>
			<small>BGP-Label Unicast Source address/mask</small>	<small>BGP-Label Unicast address</small>	<small>BGP-Label Unicast</small>	

ステップ 4 [ノードとインターフェイス (Nodes and Interfaces)] ウィンドウで、境界リーフノードとインターフェイスを設定するために必要な情報を入力します。

- a) [ノードプロファイル名 (Node Profile Name)] フィールドと [インターフェイス プロファイル名 (Interface Profile Name)] フィールドで、ノードプロファイル名とインターフェイス プロファイル名にデフォルトの命名規則を使用するかどうかを決定します。

デフォルトのノード プロファイル名は L3Out-name_nodeProfile で、デフォルトのインターフェイス プロファイル名は [L3Out-name_interfaceProfile] です。[L3Out-name] は、[接続 (Connectivity)] ページの [名前 (Name)] フィールドに入力した名前です。必要に応じて、これらのフィールドのプロファイル名を変更します。

- b) (任意) [BFD インターフェイス ポリシー (BFD Interface Policy)] フィールドで、既存の BFD インターフェイス ポリシーを選択するか、[BFD インターフェイス ポリシーの作成 (Create BFD Interface Policy)] を選択して新しい BFD インターフェイス ポリシーを作成します。
- c) [データプレーンのトランスポート (Transport Data Plane)] フィールドで、Cisco ACI境界リーフスイッチのハンドオフに使用するルーティングのタイプを決定します。

次のオプションがあります。

- **[MPLS]** : トランスポート デバイスへのハンドオフにマルチプロトコル ラベル スイッチング (MPLS) を使用するには、このオプションを選択します。
 - **[SR-MPLS]** : トランスポート デバイスへのハンドオフにセグメントルーティング (SR) マルチプロトコル ラベル スイッチング (MPLS) を使用するには、このオプションを選択します。
- d) **[インターフェイス タイプ (Interface Types)]** 領域で、**[レイヤ 3 (Layer 3)]** および **[レイヤ 2 (Layer 2)]** フィールドで必要な選択を行います。

次のオプションがあります。

- **レイヤ 3 :**
 - **インターフェイス :** 境界リーフ スイッチを外部ルータに接続するためのレイヤ 3 インターフェイスを設定するには、このオプションを選択します。
このオプションを選択すると、レイヤ 3 インターフェイスは、このページの **[レイヤ 2 (Layer 2)]** フィールドで選択した特定のオプションに応じて、物理ポートまたは直接ポートチャネルのいずれかになります。
 - **サブインターフェイス :** 境界リーフ スイッチを外部ルータに接続するようにレイヤ 3 サブインターフェイスを設定するには、このオプションを選択します。
このオプションを選択すると、このページの **[レイヤ 2 (Layer 2)]** フィールドで選択した特定のオプションに応じて、物理ポートまたはダイレクト ポートチャネルのいずれかに対して、レイヤ 3 サブインターフェイスが作成されます。
- **レイヤ 2 :**
 - **[ポート (Port)]**
 - **ダイレクトポートチャネル(Direct Port Channel)**

- e) **[ノード ID (Node ID)]** フィールドのドロップダウン メニューで、L3Out のリーフ スイッチ、またはノードを選択します。

マルチポッド設定の場合、前の画面で選択したポッドの一部であるリーフ スイッチ (ノード) のみが表示されます。

ルータ ID の設定方法を説明する警告メッセージが画面に表示される場合があります。

- このノードのルータ ID がまだ設定されていない場合は、に進み、このノードのルータ ID を設定する手順を参照してください。 [4.f \(202 ページ\)](#)
- このノードにルータ ID がすでに設定されている場合 (たとえば、以前に MP-BGP ルート リフレクタを設定していた場合)、次のオプションがあります。
 - **SR-MPLS 設定に同じルータ ID を使用します。** これは推奨オプションです。この場合、次の手順で使用するためにこの警告に表示されるルータ ID をメモし、このノードのルータ ID の設定手順を参照してください。 [4.f \(202 ページ\)](#)

- SR-MPLS 設定に別のルータ ID を使用します。この状況では、次の手順でルータ ID を入力する前に、既存のアプリケーションへのトラフィックの中断を回避するために、最初にノードをアクティブパスから外す必要があります。アクティブパスからノードを削除するには、次の手順を実行します。

1. ノードをメンテナンス モードにします。
2. の説明に従って、SR-MPLS 設定に別のルータ ID を入力します。4.f (202 ページ)
3. ノードをリロードします。

- f) [ルータ ID (Router ID)] フィールドに、Infra L3Out の境界リーフ スイッチ部分の一意のルータ ID (IPv4 または IPv6 アドレス) を入力します。

ルータ ID は、すべての境界リーフ スイッチと DC-PE で一意である必要があります。

で説明したように、ルータ ID がこのノードですでに設定されている場合、いくつかのオプションがあります。4.e (201 ページ)

- SR-MPLS 設定に同じルータ ID を使用する場合は、の警告メッセージに表示されたルータ ID を入力します。4.e (201 ページ)
- SR-MPLS 設定に同じルータ ID を使用しない場合、またはルータ ID がまだ設定されていない場合は、の境界リーフ スイッチ部分の IP アドレス (IPv4 または IPv6) をこのフィールドに入力します。一意のルータ ID である必要があることに注意してください。

ルータ ID のエントリを決定すると、[BGP-EVPN ループバック (BGP-EVPN Loopback)] フィールドと [MPLS トランスポート ループバック (MPLS Transport Loopback)] フィールドのエントリに、[ルータ ID (Router ID)] フィールドに入力したエントリが自動的に入力されます。

- g) (任意) 必要に応じて、[N ループバック (BGP-EVPN Loopback)] フィールドに IP アドレスを入力します。

BGP-EVPN セッションの場合、BGP-EVPN ループバックがコントロールプレーンセッションに使用されます。このフィールドを使用して、境界リーフ スイッチの EVPN ループバックと DC-PE 間の MP-BGP EVPN セッションを設定し、オーバーレイプレフィックスをアダプタイズします。MP-BGP EVPN セッションは、BP-EVPN ループバックと BGP-EVPN リモートピアアドレス ([接続 (Connectivity)] ウィンドウの [BGP-EVPN リモート IPv4 アドレス (BGP-EVPN Remote IPv4 Address)] フィールドで設定) の間で確立されます。

[BP-EVPN ループバック (BGP-EVPN Loopback)] フィールドには、[ルータ ID (Router ID)] フィールドに入力したものと同一エントリが自動的に入力されます。BGP-EVPN ループバック アドレスとしてルータ ID を使用しない場合は、BGP-EVPN ループバック アドレスに別の IP アドレスを入力します。

次の点に注意してください。

- BGP-EVPN セッションでは、[BGP-EVPN ループバック (BGP-EVPN Loopback)] フィールドに、[ルータ ID (Router ID)] フィールドに入力した IP アドレスとは異なる IP アドレスを使用することを推奨します。

- BGP-EVPN ループバックと MPLS トランスポートループバックに異なる IP アドレスを使用できますが、ACI 境界リーフスイッチの BGP-EVPN と MPLS トランスポートループバックに同じループバックを使用することを推奨します。

- h) [MPLS トランスポートループバック (MPLS Transport Loopback)] フィールドに、MPLS トランスポートループバックのアドレスを入力します。

MPLS トランスポートループバックは、ACI 境界リーフスイッチと DC-PE 間のデータプレーンセッションを構築するために使用されます。MPLS トランスポートループバックは、境界リーフスイッチから DC-PE ルータにアダプタイズされるプレフィックスのネクストホップになります。詳細については、「[ACI 境界リーフスイッチと DC-PE 間の MP-BGP EVPN セッション \(176 ページ\)](#)」を参照してください。

次の点に注意してください。

- BGP-EVPN セッションでは、[MPLS トランスポートループバック (MPLS Transport Loopback)] フィールドに、[ルータ ID (Router ID)] フィールドに入力した IP アドレスとは異なる IP アドレスを使用することを推奨します。
- BGP-EVPN ループバックと MPLS トランスポートループバックに異なる IP アドレスを使用できますが、ACI 境界リーフスイッチの BGP-EVPN と MPLS トランスポートループバックに同じループバックを使用することを推奨します。

- i) [セグメント ID (SID) インデックス (Segment ID (SID) Index)] フィールドに、SID インデックスを入力します。

SID インデックスは、MPLS トランスポートループバックの各ノードで設定されます。SID インデックス値は BGP-LU を使用してピアルータにアダプタイズされ、ピアルータは SID インデックスを使用してローカルラベルを計算します。

SID インデックス エントリでサポートされる値は 0 ～ 4294967295 です。SID インデックスは、セグメントルーティングドメイン全体で一意である必要があります。

- j) 上記の [レイヤ 2 (Layer 2)] 領域で [ポート (Port)] を選択した場合は、[インターフェイス (Interface)] フィールドが表示されます。ドロップダウンリストから [ポート (Port)] を選択します。
- k) 上記の [レイヤ 2 (Layer 2)] 領域で [ダイレクトポートチャネル (Direct Port Channel)] を選択した場合は、[PC パス (PC Paths)] フィールドが表示されます。ドロップダウンリストからポートチャネルを選択します。これは、インターフェイスプロファイルのポートチャネルエンドポイントへのパスです。
- l) 上記の [レイヤ 3 (Layer 3)] 領域で [サブインターフェイス (Sub-Interface)] を選択した場合は、[VLAN Encap] フィールドが表示されます。レイヤ 3 外部プロファイルに使用されるカプセル化を入力します。
- m) [MTU (bytes)] フィールドで、外部ネットワークの最大転送単位を入力します。

このフィールドの許容値は 576 ～ 9216 です。値を継承するには、このフィールドに **inherit** を入力します。

- n) [IPv4 アドレス (IPv4 Address)]フィールドに、BGP-Label ユニキャスト送信元の IP アドレスを入力します。
- これは、前の手順で設定したレイヤ3 インターフェイス/サブインターフェイス/ポートチャネルに割り当てられた IP アドレスです。
- o) [IPv4 アドレス (IPv4 Address)]フィールドに、BGP-Label ユニキャストピア IP アドレスを入力します。
- これは、境界リーフスイッチに直接接続されているルータのインターフェイスのIPアドレスです。
- p) [リモート ASN (Remote ASN)]フィールドに、直接接続されたルータの BGP-Label Autonomous System Number を入力します。
- q) SR-MPLS infra L3Out のこのノードに追加のインターフェイスを設定するかどうかを決定します。
- このSR-MPLS infra L3Out のこのノードに追加のインターフェイスを設定しない場合は、に進みます。 [4.s \(204 ページ\)](#)
 - このSR-MPLS infra L3Out のこのノードに追加のインターフェイスを設定する場合は、[インターフェイス (Interface)]領域で[+]をクリックして、このノードの別のインターフェイスに同じオプションを表示します。
- (注) このノードのインターフェイスに入力した情報を削除する場合、または誤って追加したインターフェイス行を削除する場合は、削除するインターフェイス行のごみ箱アイコンをクリックします。
- r) この SR-MPLS infra L3Out に追加のノードを設定するかどうかを決定します。
- この SR-MPLS infra L3Out の追加ノードを設定しない場合は、に進みます。 [4.s \(204 ページ\)](#)
 - この SR-MPLS infra L3Out に追加のノードを設定する場合は、[ノード (Nodes)]領域で[+]をクリックして、別のノードに同じオプションを表示します。
- (注) ノードに入力した情報を削除する場合、または誤って追加したノード行を削除する場合は、削除するノード行のごみ箱アイコンをクリックします。
- s) [ノードとインターフェイス (Nodes and Interfaces)]ウィンドウに残りの追加情報を入力したら、[完了 (Finish)]をクリックして、[SR-MPLS インフラ L3Out の作成 (Create SR-MPLS Infra L3Out)]ウィザードで必要な設定を完了します。

次のタスク

の手順に従って、SR-MPLS VRF L3Out を設定します。 [GUIを使用したSR-MPLS VRF L3Outの設定 \(205 ページ\)](#)

GUIを使用したSR-MPLS VRF L3Outの設定

この項の手順を使用して、SR-MPLS VRF L3Outを設定します。これは、前の手順で設定したSR-MPLS インフラ L3Outからのトラフィックの転送に使用されます。

- ユーザテナントVRFはSR-MPLSインフラL3Outにマッピングされ、テナントブリッジドメインサブネットをDC-PEルータにアドバタイズし、DC-PEから受信したMPLS VPNルートをインポートします。
- 各VRFのSR-MPLS VRF L3Outでルーティングポリシーとセキュリティポリシーを指定する必要があります。これらのポリシーは、1つ以上のSR-MPLSインフラL3Outをポイントします。
- VRFごとに1つのSR-MPLS VRF L3Outがサポートされます。

始める前に

- [注意事項と制約事項 \(189 ページ\)](#) で提供されているSR-MPLSガイドラインと制約事項を確認します。特に、[SR-MPLS VRF L3Outのガイドラインと制約事項 \(190 ページ\)](#) で提供されているガイドラインと制約事項を確認してください。
- [GUIを使用したSR-MPLSインフラL3Outの設定 \(196 ページ\)](#) の手順に従って、SR-MPLSインフラL3Outを設定します。

ステップ1 テナントの[SR-MPLS VRF L3Outの作成 (Create SR-MPLS VRF L3Out)]ウィンドウ ([テナント (Tenants)] [テナント (tenant)] [ネットワークング (Networking)] [SR-MPLS VRF L3Outs]) に移動してSR-MPLS VRF L3Outを設定します。 >>>

ステップ2 [SR-MPLS VRF L3Outs]を右クリックし、[SR-MPLS VRF L3Outの作成 (Create SR-MPLS VRF L3Out)]を選択します。

[SR-MPLS VRF L3Outの作成 (Create SR-MPLS VRF L3Out)]ウィンドウが表示されます。

図 23: SR-MPLS L3Out の作成

- ステップ 3** [名前 (Name)] フィールドに、SR-MPLS VRF L3Out の名前を入力します。
- これは外部への接続を制御するポリシーに付ける名前です。名前では最大 64 文字までの英数字を使用できます。
- (注) オブジェクトの作成後は、この名前は変更できません。
- ステップ 4** [VRF] フィールドで、既存の VRF を選択するか、[VRF の作成 (Create VRF)] をクリックして新しい VRF を作成します。
- ステップ 5** [SR-MPLS Infra L3Out] フィールドで、既存の SR-MPLS infra L3Out を選択するか、[SR-MPLS Infra L3Out の作成 (Create SR-MPLS Infra L3Out)] をクリックして新しい SR-MPLS infra L3Out を作成します。
- SR-MPLS インフラ L3Out の作成の詳細については、[を参照してください。GUI を使用した SR-MPLS インフラ L3Out の設定 \(196 ページ\)](#)
- ステップ 6** [外部 EPG (External EPGs)] 領域に移動し、[外部 EPG 名 (External EPG Name)] 領域で、この SR-MPLS VRF L3Out に使用する外部 EPG の一意の名前を入力します。
- ステップ 7** [サブネットとコントラクト (Subnets and Contracts)] 領域に移動し、この EPG 内の個々のサブネットを設定します。

(注) サブネットフィールドを設定しても、次のフィールドが表示されない場合は、[サブネットとコントラクトの表示 (Show Subnets and Contracts)] をクリックして次のフィールドを表示します。

- a) [IPプレフィックス (IP Prefix)] フィールドに、サブネットのIPアドレスとネットマスクを入力します。
- b) [インフラ VRF ポリシー (Inter VRF Policy)] フィールドで、VRF 間ポリシーを設定するかどうかを決定します。

- VRF 間ポリシーを設定しない場合は、に進みます。7.c (207 ページ)
- VRF 間ポリシーを設定する場合は、使用する適切な VRF 間ポリシーを選択します。

次のオプションがあります。

- [ルートリーク (Route Leaking)]

[ルートリーク (Route Leaking)] を選択すると、[集約 (Aggregate)] フィールドが表示されます。このオプションも有効にする場合は、[集約 (Aggregate)] の横にあるボックスをクリックします。

- セキュリティ。

[インター VRF ポリシー (Inter VRF Policy)] フィールドでは、上記の2つのオプションのいずれかまたは両方を選択できます。

- c) [提供されたコントラクト (Provided Contract)] フィールドで、既存のプロバイダー契約を選択するか、[コントラクトの作成 (Create Contract)] をクリックしてプロバイダ契約を作成します。
- d) [消費されたコントラクト (Consumed Contract)] フィールドで、既存のコンシューマコントラクトを選択するか、[コントラクトの作成 (Create Contract)] をクリックしてコンシューマコントラクトを作成します。
- e) この外部 EPG に追加のサブネットを設定するかどうかを決定します。

- この外部 EPG に追加のサブネットを設定しない場合は、に進みます。ステップ8 (207 ページ)
- この外部 EPG に追加のサブネットを設定する場合は、[サブネットとコントラクト (Subnet and Contracts)] 領域で [+] をクリックして、別のサブネットに同じオプションを表示します。

(注) サブネットに入力した情報を削除する場合、または誤って追加したサブネット行を削除する場合は、削除するサブネット行のゴミ箱アイコンをクリックします。

ステップ 8 この SR-MPLS VRF L3Out に使用する追加の外部 EPG を作成するかどうかを決定します。

- この SR-MPLS VRF L3Out に使用する追加の外部 EPG を設定しない場合は、に進みます。ステップ9 (208 ページ)
- この SR-MPLS VRF L3Out に使用する追加の外部 EPG を設定する場合は、[外部 EPG 名 (External EPG Name)] 領域で [+] をクリックして、別の外部 EPG に対して同じオプションを表示します。

(注) 外部 EPG に入力した情報を削除する場合、または誤って追加した外部 EPG エリアを削除する場合は、削除する外部 EPG エリアのゴミ箱アイコンをクリックします。

ステップ9 [ルートマップ (External EPG Name)] 領域で、発信および着信ルートマップを設定します。

各 SR-MPLS VRF L3Out 内：

- アウトバウンドルートマップ (エクスポートルーティングポリシー) の定義は必須です。これは、外部 DC-PE ルータにプレフィックスをアダプティブできるようにするために必要です。
 - デフォルトでは、DC-PE ルータから受信したすべてのプレフィックスがファブリックに許可されるため、インバウンドルートマップ (インポートルーティングポリシー) の定義はオプションです。
- a) [アウトバウンド (Outbound)] フィールドで、既存のエクスポートルートマップを選択するか、[ルート制御用ルートマップの作成 (Create Route Maps for Route Control)] をクリックして新しいエクスポートルートマップを作成します。
- b) [インバウンド (Inbound)] フィールドで、既存のインポートルートマップを選択するか、[ルート制御用ルートマップの作成 (Create Route Maps for Route Control)] をクリックして新しいインポートルートマップを作成します。

ステップ10 [SR-MPLS VRF L3Out の作成 (Create SR-MPLS VRF L3Out)] ウィンドウでの設定が完了したら、[送信 (Submit)] をクリックします。

GUIを使用したSR-MPLSカスタムQoSポリシーの作成

SR MPLS カスタム QoS ポリシーは、MPLS QoS 出力ポリシーで定義された着信 MPLS EXP 値に基づいて、SR-MPLS ネットワークから送信されるパケットのプライオリティを定義します。これらのパケットは、ACI ファブリック内にあります。また、MPLS QoS 出力ポリシーで定義された IPv4 DSCP 値に基づく MPLS インターフェイスを介して ACI ファブリックから離れるパケットの CoS 値および MPLS EXP 値をマーキングします。

カスタム出力ポリシーが定義されていない場合、デフォルトの Qos レベル (Level3) がファブリック内のパケットに割り当てられます。カスタム出力ポリシーが定義されていない場合、デフォルトの EXP 値 (0) がファブリックから離れるパケットにマーキングされます。

ステップ1 メニューバーから [Tenants (テナント)] > [インフラ (infra)] を選択します。

ステップ2 左側のペインで、[インフラ (infra)] [ポリシー (Policies)] [プロトコル (Protocol)] [MPLS カスタム QoS (MPLS Custom QoS)] を選択します。 > > >

ステップ3 [MPLS カスタム QoS (MPLS Custom QoS)] フォルダを右クリックし、[MPLS カスタム QoS ポリシーの作成 (Create MPLS Custom QoS Policy)] を選択します。

ステップ4 表示される [MPLS カスタム QoS ポリシーの作成 (Create MPLS Custom QoS Policy)] ウィンドウで、作成するポリシーの名前と説明を入力します。

- ステップ5** [MPLS入力ルール (MPLS Ingress Rule)] 領域で、[+]をクリックして入力QoS変換ルールを追加します。
- MPLS ネットワークに接続されている境界リーフ (BL) に着信するすべてのトラフィックは、MPLS EXP 値に対してチェックされ、一致が検出されると、トラフィックはACIQoS レベルに分類され、適切なCoSおよびDSCP値でマークされます。

- a) [優先順位 (Priority)] フィールドで、入力ルールの優先順位を選択します。
- これは、ACIファブリック内のトラフィックに割り当てるQoSレベルで、ACIはファブリック内のトラフィックのプライオリティを決めるために使用します。オプションの範囲はLevel1〜Level6です。デフォルト値はLevel3です。このフィールドで選択しない場合、トラフィックには自動的にLevel3の優先順位が割り当てられます。
- b) [EXP範囲開始 (EXP Range From)] と [EXP範囲終了 (EXP Range To)] フィールドで、照合する入力MPLSパケットのEXP範囲を指定します。

- c) **[ターゲット DSCP (Target DSCP)]** フィールドで、パケットが ACI ファブリック内にある場合にパケットに割り当てる DSCP 値を選択します。

指定された DSCP 値は、外部ネットワークから受信した元のトラフィックに設定されるため、トラフィックが宛先 ACI リーフ ノードで VXLAN カプセル化解除された場合にのみ再公開されます。

デフォルトは [未指定 (Unspecified)] です。つまり、パケットの元の DSCP 値が保持されます。

- d) **[ターゲット CoS (Target CoS)]** フィールドで、パケットが ACI ファブリック内にある場合にパケットに割り当てる CoS 値を選択します。

指定された CoS 値は、外部ネットワークから受信した元のトラフィックに設定されるため、トラフィックが宛先 ACI リーフ ノードで VXLAN カプセル化解除された場合にのみ再公開されます。

デフォルトは [未指定 (Unspecified)] です。つまり、ファブリックで CoS 保存オプションが有効になっている場合にのみ、パケットの元の CoS 値が保持されます。

- e) **[更新 (Update)]** をクリックして入力ルールを保存します。
f) 追加の入力 QoS ポリシールールについて、この手順を繰り返します。

ステップ 6 [MPLS 出カールール (MPLS Egress Rule)] 領域で、**[+]** をクリックして出力 QoS 変換ルールを追加します。

トラフィックが境界リーフの MPLS インターフェイスから離れていくと、パケットの DSCP 値に基づいて照合され、一致が見つかり、MPLS EXP および CoS 値がポリシーに基づいて設定されます。

- a) **[DSCP 範囲開始 (DSCP Range From)]** と **[DSCP 範囲終了 (DSCP Range To)]** ドロップダウンを使用して、出力 MPLS パケットのプライオリティを割り当てるために一致させる ACI ファブリック パケットの DSCP 範囲を指定します。
b) **[ターゲット EXP (Target EXP)]** ドロップダウンから、出力 MPLS パケットに割り当てる EXP 値を選択します。
c) **[ターゲット CoS (Target CoS)]** ドロップダウンから、出力 MPLS パケットに割り当てる CoS 値を選択します。
d) **[更新 (Update)]** をクリックして入力ルールを保存します。
e) 追加の出力 QoS ポリシールールについて、この手順を繰り返します。

ステップ 7 [OK] をクリックし、MPLS カスタム QoS の作成を完了します。

MPLS 統計情報の表示

次に、このトピックで説明する統計画面に表示するために選択できる MPLS 固有の統計情報を示します。

- [インターフェイスの SR-MPLS 統計情報の表示 \(211 ページ\)](#) で説明されているように、インターフェイス レベルでは、
- [VRS 向け SR-MPLS 統計情報の表示 \(212 ページ\)](#) で説明されているように、VRF レベルでは、

システム内のすべてのインターフェイスおよび VRF の統計情報を表示するには、次の場所に移動します。

[テナント (Tenants)] > [インフラ (infra)] > [ネットワーキング (Networking)] > [SR-MPLS Infra L3Outs]

[SR-MPLS インフラ L3Outs (SR-MPLS Infra L3Outs)] パネルが表示され、システムで設定されているすべての SR-MPLS infra L3Outs が表示されます。上位レベルの [SR-MPLS インフラ L3Out (SR-MPLS Infra L3Outs)] パネルで、表示する統計情報のタイプに応じて、適切な統計情報ページに移動します。

- [インターフェイス統計情報 (Interface Stats)] タブをクリックして、システム上のすべての MPLS インターフェイスの統計情報の概要を表示します。このウィンドウの各行には、特定のノード上の特定のインターフェイスの MPLS 統計情報が表示されます。



(注) メインの SR-MPLS infra L3Outs ページに表示されるインターフェイス統計情報は、スイッチ名の末尾に「FX2」または「GX」がある境界リーフスイッチモデル上のすべての SR-MPLS 対応インターフェイスのみを対象としています。

他のレベルの MPLS インターフェイス統計情報を確認するには、[インターフェイスの SR-MPLS 統計情報の表示 \(211 ページ\)](#) を参照してください。

- [VRF 統計情報 (VRF Stats)] タブをクリックして、システム上のすべての MPLS VRF の統計情報の要約を表示します。このウィンドウの各行には、特定のノードに設定された特定の VRF の MPLS 統計情報が表示されます。

SR-MPLS インフラ L3Out プロパティ ページで提供される VRF 統計情報は、SR-MPLS インフラ L3Out のプロバイダーラベルが消費される特定の境界リーフスイッチまたはリモートリーフスイッチの個々の VRF 統計情報です。

MPLS VRF 統計情報のその他のレベルについては、[VRS 向け SR-MPLS 統計情報の表示 \(212 ページ\)](#) を参照してください。

インターフェイスの SR-MPLS 統計情報の表示

次に、このトピックで説明する統計画面に表示するために選択できる MPLS 固有のインターフェイス統計情報を示します。

- Mpls 出力ドロップ バイト
- Mpls 出力許可バイト
- Mpls 出力ドロップ パケット
- Mpls 出力許可パケット
- Mpls 受信ドロップ バイト

- Mpls Ingress Admit Bytes
- Mpls 受信ドロップ パケット
- Mpls 受信許可パケット

統計情報ページに表示される統計情報のタイプを変更するには、チェックボックスをクリックして[統計情報の選択 (Select Stats)]ウィンドウを開きます。エントリを左コラムから右コラムに移動して別の統計情報を表示し、右コラムから左コラムへ移動してビューから特定の統計情報を削除します。

このページの統計情報のレイアウトを変更して、統計情報を表形式で表示するには、3本の横棒アイコンをクリックして[テーブル ビュー (Table View)]を選択します。

- SR-MPLS インフラ L3Out の SR-MPLS VRF L3Out 内のすべてのインターフェイスの詳細な集約インターフェイス統計情報を表示するには、その SR-MPLS インフラ L3Out に移動します。

[テナント (Tenant)] > [インフラ (infra)] > [ネットワーキング (Networking)] > [SR-MPLS Infra L3Outs] > [SR-MPLS_infra_L3Out_name]

特定の SR-MPLS インフラ L3Out の下にある SR-MPLS VRF L3Out のすべてのインターフェイスの詳細な集約インターフェイス統計情報を表示するには、[統計情報 (Stats)] タブをクリックします。

- 特定のリーフ スイッチの特定のインターフェイスの統計情報を表示するには、リーフ スイッチのそのインターフェイス領域に移動します。

[Fabric Inventory Pod # leaf_switch Interfaces] をクリックし、[ルーテッド インターフェイス (Routed Interfaces)] または [カプセル化されたルーテッド インターフェイス (Encapsulated Routed Interfaces)] をクリックします。 > > >

統計情報を取得する特定のインターフェイスをクリックし、[統計情報 (Stats)] タブをクリックします。

VRS 向け SR-MPLS 統計情報の表示

次に、このトピックで説明する統計画面に表示するために選択できる MPLS 固有の VRF 統計情報を示します。

- Mpls Vrf 出力ドロップ バイト
- Mpls Vrf 出力許可バイト
- Mpls Vrf 出力ドロップ パケット
- Mpls Vrf 出力許可パケット
- Mpls Vrf 受信ドロップ バイト
- Mpls Vrf 受信許可バイト
- Mpls Vrf 受信ドロップ パケット

- Mpls Vrf 受信許可パケット

統計情報ページに表示される統計情報のタイプを変更するには、チェックボックスをクリックして **[統計情報の選択 (Select Stats)]** ウィンドウを開きます。エントリを左コラムから右コラムに移動して別の統計情報を表示し、右コラムから左コラムへ移動してビューから特定の統計情報を削除します。

このページの統計情報のレイアウトを変更して、統計情報を表形式で表示するには、3本の横棒アイコンをクリックして **[テーブル ビュー (Table View)]** を選択します。

- 特定の VRF の詳細な集約 VRF 統計情報を表示するには、その VRF に移動します。

[テナント (Tenants)] > **[tenant_name]** > **[ネットワーキング (Networking)]** > **[VRFs]** > **[VRF_name]** の順にクリックします。

[統計情報 (Stats)] タブをクリックして、この特定の VRF の集約 VRF 統計情報を表示します。この VRF は SR-MPLS L3Out の 1 つで使用されており、この SR-MPLS L3Out には複数のリーフスイッチがあり、各リーフスイッチに複数のインターフェイスがあることに注意してください。このウィンドウに表示される統計情報は、この VRF で使用されているこの SR-MPLS L3Out 内のすべてのインターフェイスの集約です。

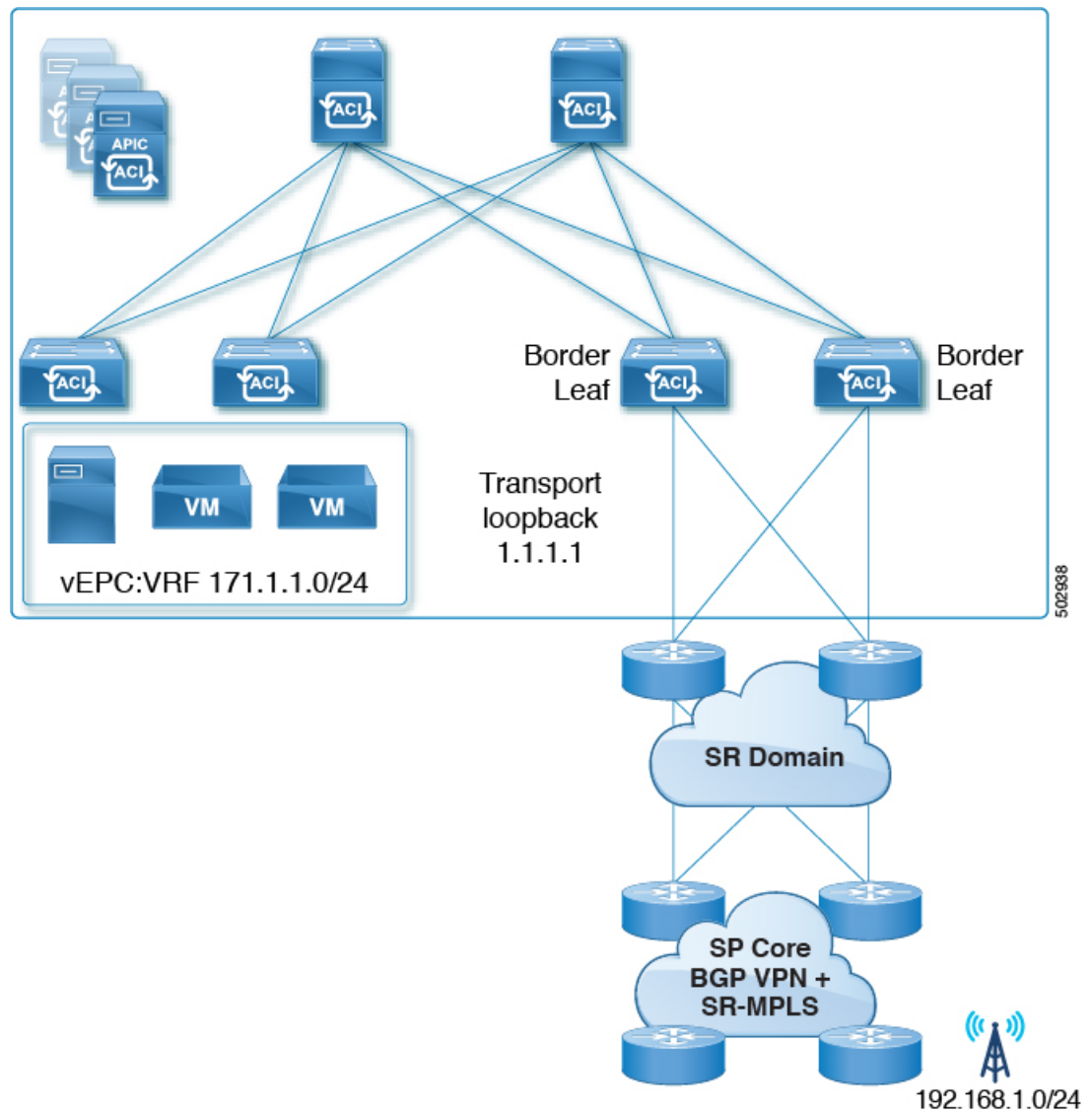
- 特定のリーフスイッチの VRF 統計情報を表示するには、そのリーフスイッチの VRF コンテキストに移動します。

[ファブリック (Fabric)] > **[インベントリ (Inventory)]** > **[ポッド # (Pod #)]** > **[leaf_switch]** > **[VRF コンテキスト (VRF Contexts)]** > **[VRF_context_name]**

[統計情報 (Stats)] タブをクリックして、この特定のリーフスイッチのこの VRF の統計情報を表示します。

SR-MPLS グローバルブロック (GB) の設定

次の図に示すように、ACIファブリックの境界リーフスイッチと DC-PE の間に SR ネットワークがある場合は、SR-MPLS グローバルブロック (GB) を設定します。



SR ドメイン内のすべてのノードで同じ SR-GB 設定を使用することを推奨します。

次に、SR-MPLS グローバルブロックを設定する際に考慮すべき重要なガイドラインを示します。

- 設定可能な SR-GB の範囲は 16000 ～ 471804 です。
- ACI ファブリックのデフォルトの SR-GB 範囲は 16000 ～ 23999 です。
- ACI は、アンダーレイ ラベルに対して常にヌルをアドバタイズします (トランスポート ループバック)。

ステップ 1 [SR-MPLS グローバル設定 (SR-MPLS Global Configurations)] ウィンドウに移動します。

[テナント (Tenants)] > [インフラ (infra)] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [MPLS グローバル設定 (MPLS Global Configurations)]

ステップ 2 メインの [SR-MPLS グローバル設定 (SR-MPLS Global Configurations)] 画面で [デフォルト (default)] をダブルクリックするか、左側のナビゲーションバーで [Mpls グローバル設定 (Mpls Global Configurations)] の下にある [デフォルト (default)] をクリックして、デフォルトの MPLS Global Configurations 画面にアクセスします。

デフォルトの [SR-MPLS グローバル設定] ウィンドウが表示されます。

SR-MPLS Global Configurations

Policy History

Properties

Name: default

Description: optional

SR Global Block Minimum: 16001

SR Global Block Maximum: 23999

Show Usage Reset Submit

ステップ 3 [SR グローバルブロック最小値 (SR Global Block Minimum)] フィールドに、SR-GB 範囲の最小値を入力します。

このフィールドの最小許容値は 16000 です。

ステップ 4 [SR グローバルブロック最大値 (SR Global Block Maximum)] フィールドに、SR-GB 範囲の最大値を入力します。

このフィールドの最大許容値は 471804 です。

ステップ 5 [送信 (Submit)] をクリックします。

IP ハンドオフ設定から SR ハンドオフ設定への移行

始める前に :

[リリース 5.0\(1\) 以前の ACI ハンドオフ : IP ハンドオフ \(169 ページ\)](#) で説明されているように、プレリリース 5.0(1) IP ハンドオフ設定を使用する、事前に設定された L3Out があること。

このタスクの概要：

これらの手順では、で説明したように、Cisco APIC リリース 5.0(1) で導入された新しい SR-MPLS コンポーネントを使用して、以前に IP ハンドオフ設定（で説明されています）で設定した L3Out を SR ハンドオフ設定に移行する手順を示します。リリース 5.0(1) 以前の ACI ハンドオフ：IP ハンドオフ（169 ページ）リリース 5.0(1) での ACI ハンドオフ：SR ハンドオフ（170 ページ）

これらの手順では、2つのハンドオフが同じ外部ネットワークインフラストラクチャへの接続に使用され、外部デバイスが両方の L3Out を使用して ACI ファブリックにアクセスできることを前提としています。現在、外部クライアントは IP ハンドオフ設定で使用されている L3Out を介して着信することができますが、この項の手順を完了すると、外部クライアントは SR-MPLS ハンドオフ設定で使用されている L3Out を介して着信することができます。



(注) これらの手順では、次の用語を使用して2つのタイプの L3Out を区別します。

- IP ベースの L3Out：リリース 5.0(1) より前の IP ハンドオフ設定を使用している、以前に設定されたユーザテナント L3Out に使用されます。
- SR-MPLS L3Out：Cisco APIC Release 5.0(1) で導入された新しい SR-MPLS コンポーネントを使用して設定された、新しく設定されたユーザテナント L3Out に使用されます。

このプロセスの一部として実行する全体的な手順は次のとおりです。

- IP ベースの L3Out 設定をミラーリングするために、SR-MPLS VRF L3Out で外部 EPG を設定します。これには、着信トラフィックを分類するためのサブネット設定と、外部 EPG によって提供または消費されるコントラクトが含まれます。
- インバウンドおよびアウトバウンドトラフィックをリダイレクトして、SR-MPLS L3Out を優先するようにします。
- IP ベースの L3Out を切断します。

次の項では、上記の各手順の詳細な手順を示します。

SR-MPLS VRF L3Outでの外部 EPG の設定

このタスクでは、SR-MPLS VRF L3Out で外部 EPG を設定して、IP ベースの L3Out 設定（以前に設定した、リリース 5.0(1) より前の IP ハンドオフ設定を使用する L3Out）をミラーリングします。これにはインバウンドトラフィックの分類のサブネット設定、および外部 EPG によって提供されるか消費されるコントラクトが含まれています。

始める前に

IP ハンドオフ設定から SR ハンドオフ設定への移行（215 ページ）に記載の情報について、確認してください。

ステップ1 新しいインフラ SR-MPLS L3Out をまだ作成していない場合は、作成します。

これらの手順については、を参照してください。[GUI を使用した SR-MPLS インフラ L3Out の設定 \(196 ページ\)](#)

ステップ2 新しいユーザ テナント SR-MPLS L3Out を作成します (まだ作成していない場合)。

これらの手順については、を参照してください。[GUI を使用した SR-MPLS VRF L3Out の設定 \(205 ページ\)](#) この L3Out は、以前に設定した IP ベースの L3Out と同じ VRF に関連付ける必要があります。

新しいユーザ テナント SR-MPLS L3Out を作成するプロセスの一環として、この SR-MPLS L3Out の外部 EPG を設定するように求められます。

- 新しい SR-MPLS L3Out の外部 EPG には、以前に設定した IP ベースの L3Out に対して現在持っているものと同じ IP プレフィックス情報を入力します。
- 以前に設定した IP ベースの L3Out に複数の外部 EPG が設定されている場合は、新しい SR-MPLS L3Out に追加の外部 EPG を作成し、各 EPG に同じ IP プレフィックス情報を一致させます。

最終的に、新しい SR-MPLS L3Out 用に設定する外部 EPG 設定は、付随するサブネット設定とともに、以前に IP ベースの L3Out 用に設定した外部 EPG およびサブネット設定と一致する必要があります。

新しいユーザ テナント SR-MPLS L3Out の作成手順を完了すると、2つの L3Out (BGP の2つのパス) が作成されます。

- プレリリース 5.0(1) IP ハンドオフ 設定を使用した、既存の、以前に設定した IP ベースの L3Out。内の [開始する前に (Before you begin)] 領域に記述があります。[IP ハンドオフ設定から SR ハンドオフ設定への移行 \(215 ページ\)](#)
- Cisco APIC リリース 5.0(1) で導入された新しい SR-MPLS コンポーネントを使用して作成した新しい SR-MPLS L3Out。

ステップ3 IP ベースの L3Out と同じセキュリティ ポリシーが SR-MPLS L3Out の外部 EPG に適用されていることを確認します。

非境界リーフ スイッチおよび境界リーフ スイッチでは、新しい SR-MPLS L3Out の作成時に設定した外部 EPG の新しいセキュリティ ポリシーにより、以前に設定された IP ベース L3Out のすべての EPG サブネット プレフィックスと衝突するすべてのサブネットで障害が発生します。これは、同じセキュリティ ポリシーが両方の L3Out の同じ外部 EPG に適用される限り、機能に影響を与えない障害です。

次のタスク

インバウンドおよびアウトバウンド トラフィックをリダイレクトし、に示す手順を使用して SR-MPLS L3Out を優先して開始するようにします。[SR-MPLS L3Out へのトラフィックのリダイレクト \(218 ページ\)](#)

SR-MPLS L3Out へのトラフィックのリダイレクト

このタスクでは、着信トラフィックと発信トラフィックをリダイレクトして、SR-MPLS L3Out の優先を開始するようにします。

始める前に

- [IPハンドオフ設定からSRハンドオフ設定への移行 \(215ページ\)](#) に記載の情報について、確認してください。
- に示す手順を使用して、IP ベースの L3Out 設定をミラーリングするように SR-MPLS VRF L3Out の外部 EPG を設定します。[SR-MPLS VRF L3Out での外部 EPG の設定 \(216ページ\)](#)

ステップ 1 以前に設定した IP ベースの L3Out の BGP ピア接続プロファイルに移動します。

[ナビゲーション (Navigation)]>[テナント (Tenants)]>[tenant_name_for_IP_handoff_L3Out]>[ネットワーク (Networking)]>[L3Outs]>[L3Out_name]>[論理ノード プロファイル (Logical Node Profiles)]>[logical_profile_name]>[論理インターフェイス プロファイル (Logical Interface Profiles)]>[logical_interface_profile_name]>[BGP_peer_connectivity_profile] の順に移動します。

ステップ 2 左側のナビゲーションバーで [BGP ピア接続プロファイル (BGP Peer Connectivity Profile)] をクリックすると、[BGP ピア接続プロファイル (BGP Peer Connectivity Profile)] ページが右側のメイン ウィンドウに表示されます。

ステップ 3 [BGP ピア接続プロファイル (BGP Peer Connectivity Profile)] ページに [ルート制御プロファイル (Route Control Profile)] 領域が表示されるまでページを下にスクロールします。

ステップ 4 既存の IP ベースの L3Out に対してルート制御ポリシーがすでに設定されているかどうかを確認します。

既存の IP ベースの L3Out に対してルート制御ポリシーが設定されている場合と設定されていない場合があります。ただし、新しい SR-MPLS L3Out の場合は、ルート制御ポリシーを設定する必要があります。既存の IP ベースの L3Out にルート制御ポリシーが設定されている場合は、新しい SR-MPLS L3Out にそれらのルート制御ポリシーを使用できます。それ以外の場合は、SR-MPLS L3Out の新しいルート制御ポリシーを作成する必要があります。

- [ルート制御プロファイル (Route Control Profile)] テーブルに 2 つのルート制御プロファイルが表示されている場合：
 - エクスポート ルート制御ポリシー。表の [方向 (Direction)] 列に [ルートエクスポート ポリシー (Route Export Policy)] と表示されます。
 - インポート ルート制御ポリシー。表の [方向 (Direction)] 列に [ルートインポート ポリシー (Route Import Policy)] と表示されます。

IP ベースの L3Out に対してルート制御ポリシーがすでに設定されています。[ステップ 5 \(220ページ\)](#) に進みます。

- [ルート制御プロファイル (Route Control Profiles)] テーブルに 2 つのルート制御プロファイルが表示されない場合は、SR-MPLS L3Out に使用する新しいルート マップを作成します。

- a) [ナビゲーション (Navigation)] ペインで、[テナント (Tenants)] > [tenant_name_for_IP_handoff_L3Out] > [ポリシー (Policies)] > [プロトコル (Protocol)] を展開します。
- b) [ルート制御のルートマップ (Route Maps for Route Control)] を右クリックし、[ルート制御のルートマップの作成 (Create Route Maps for Route Control)] を選択します。
- c) [ルート制御のルートマップの作成 (Create Route Maps for Route Control)] ダイアログボックスで、[名前 (Name)] フィールドに、ルートプロファイル名を入力します。
- d) [タイプ (Type)] フィールドで、[ルーティングポリシーのみ照合 (Match Routing Policy Only)] を選択する必要があります。
- e) [コンテキスト (Contexts)] 領域で [+] サインをクリックして、[ルート制御コンテキスト作成 (Create Route Control Context)] ダイアログボックスを表示し、次のアクションを実行します。
 1. 必要に応じて、[順序 (Order)] と [名前 (Name)] フィールドに入力します。
 2. [一致ルール (Match Rule)] フィールドで、[一致ルールの作成 (Create Match Rule)] をクリックします。
 3. [一致ルール (Match Rule)] ダイアログボックスの [名前 (Name)] フィールドに、一致ルールの名前を入力します。
 4. 該当するフィールド (一致Regexコミュニティ条件、一致コミュニティ条件、および一致プレフィックス) に必要な情報を入力し、[送信 (Submit)] をクリックします。
 5. [セットルール (Set Rule)] フィールドで、[ルートマップのセットルールの作成 (Create Set Rules for a Route Map)] をクリックします。
 6. [ルートマップのセットルールの作成 (Create Set Rules for a Route Map)] ダイアログボックスの [名前 (Name)] フィールドに、ルールの名前を入力します。
 7. 目的の属性および関連するコミュニティ、条件、タグ、および設定 (preferences) を選択します。[完了 (Finish)] をクリックします。
 8. [ルート制御コンテキストの作成 (Create Route Control Context)] ダイアログボックスで、[OK] をクリックします。
 9. [ルートマップの作成 (Create Route Map)] ダイアログボックスで、[送信 (Submit)] をクリックします。
- f) BGP ピア接続プロファイル スクリーンに移動します。

[テナント (Tenants)] > [tenant_name_for_IP_handoff_L3Out] > [ネットワーキング (Networking)] > [L3Outs] > [L3out-name] > [論理ノード プロファイル (Logical Node Profiles)] > [logical-node-profile-name] > [論理インターフェイス プロファイル (Logical Interface Profiles)] > [logical-interface-profile-name] > [BGP_peer_connectivity_profile]
- g) 左側のナビゲーションバーで [BGP ピア接続プロファイル (BGP Peer Connectivity Profile)] をクリックすると、[BGP ピア接続プロファイル (BGP Peer Connectivity Profile)] ページが右側のメインウィンドウに表示されます。
- h) [ルート制御プロファイル (Route Control Profile)] フィールドまで下にスクロールし、[+] をクリックして次の項目を設定します。

- [名前 (Name)] : ルート インポート ポリシー用に設定したルート マップを選択します。
- [方向 (Direction)] : [方向 (Direction)] フィールドで [ルート インポート ポリシー (Route Import Policy)] を選択します。

これらの手順を繰り返して、ルートエクスポートポリシーのルートマップを選択し、[方向 (Direction)] フィールドで [ルート エクスポート ポリシー (Route Export Policy)] を設定します。

ステップ 5 移行を実行する VRF の境界リーフ スイッチ内のすべてのピアにルート ポリシーを設定することにより、BGP に新しい SR パスを選択させます。

- 以前に設定された IP ベースの L3Out が eBGP 用に設定されている場合、IP ベースの L3Out ピアのルート インポート ポリシーとルート エクスポート ポリシーの両方に、追加の AS パス エントリ (ローカル エントリと同じ AS など) を設定します。これが最も一般的なシナリオです。

(注) 次の手順では、ルートマップにルールが設定されていないことを前提としています。ルートマップに設定済みのルールをすでに設定している場合は、既存の設定済みルールを編集して AS パス エントリを追加します ([AS パスの設定 (Set AS Path)] チェックボックスをオンにし、[AS 番号を付加 (Prepend AS)] を選択して、[+] をクリックして AS 番号を付加します)。

1. [テナント (Tenant)] > [tenant_name_for_IP_handoff_L3Out] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [セットルール (Set Rules)] の順に移動し、[ルートマップのセットルールの作成 (Create Set Rules for a Route Map)] を右クリックします。
[ルートマップの設定ルールの作成 (Create Set Rules For A Route Map)] ウィンドウが表示されます。
2. 設定ルールの A ルートマップの作成 ダイアログボックス、次のタスクを実行します。
 1. [名前 (Name)] フィールドに、これらの設定ルールの名前を入力します。
 2. [AS パスの設定 (Set AS Path)] チェックボックスをオンにし、[次へ (Next)] をクリックします。
 3. [AS パス (AS Path)] ウィンドウで [+] をクリックして [AS パスの設定を作成 (Create Set AS Path)] ダイアログボックスを開きます。
3. 基準に [AS 番号の付加 (Prepend AS)] を選択し、[+] をクリックして AS 番号を先頭に付加します。
4. AS 番号とその順序を入力し、クリックして **更新**。
5. [OK] をクリックします。
6. [ルートマップの設定ルールを作成 (Create Set Rules For A Rout Map)] ウィンドウで AS パスに基づく設定ルールの基準を確認し、[完了 (Finish)] をクリックします。
7. この既存の IP ベースの L3Out の [BGP ピア接続プロファイル (BGP Peer Connectivity Profile)] 画面に戻ります。
[テナント (Tenants)] > [tenant_name_for_IP_handoff_L3Out] > [ネットワーキング (Networking)] > [L3Outs] > [L3out-name] > [論理ノードプロファイル (Logical Node Profiles)] >

[*logical-node-profile-name*] > [論理インターフェイス プロファイル (Logical Interface Profiles)] > [*logical-interface-profile-name*] > [*BGP_peer_connectivity_profile*]

8. [ルート制御プロファイル (Route Control Profile)] 領域までスクロールし、この既存の IP ベースの L3Out に使用されているエクスポート ルート制御ポリシーとインポート ルート制御ポリシーの両方のルート プロファイル名を確認します。
 9. [テナント (Tenants)] > [*tenant_name_for_IP_handoff_L3Out*] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [ルート制御のルート マップ (Route Maps for Route Control)] の順に移動します。
 10. 最初に、この既存の IP ベースの L3Out に使用されているエクスポート ルート制御プロファイルを見つけ、そのルート プロファイルをクリックします。
このルート制御プロファイルのプロパティ ページがメイン パネルに表示されます。
 11. ページでルート制御コンテキスト エントリを見つけ、ルート制御コンテキスト エントリをダブルクリックします。
このルート制御コンテキストのプロパティ ページが表示されます。
 12. [セット ルール (Set Rule)] 領域で、追加の AS パス エントリを使用してこれらの手順で前に作成した設定ルールを選択し、[送信 (Submit)] をクリックします。
 13. 次に、この既存の IP ベースの L3Out に使用されている import ルート制御プロファイルを見つけ、そのルート プロファイルをクリックしてから、インポート ルート制御プロファイルの追加の AS パス エントリを使用してこれらの手順を繰り返します。これを行うと、外部ソースが優先を開始する必要がある着信トラフィックに影響します。
- 以前に設定された IP ベースの L3Out が iBGP 用に設定されている場合、SR-MPLS は eBGP のみをサポートするため、前の箇条書きの説明のように、eBGP が設定された SR-MPLS L3Out にトラフィックを誘導するためにローカル設定を使用する必要があります。IP ベースの L3Out ピアのルートインポートポリシーとルートエクスポートポリシーの両方を、より低いローカルプリファレンス値に設定します。
1. [テナント (Tenant)] > [*tenant_name_for_IP_handoff_L3Out*] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [セット ルール (Set Rules)] の順に移動し、[ルート マップのセット ルールの作成 (Create Set Rules for a Route Map)] を右クリックします。
[ルート マップの設定ルールの作成 (Create Set Rules For A Route Map)] ウィンドウが表示されます。
 2. [名前 (Name)] フィールドに、名前を入力します。
 3. [プリファレンスの設定 (Set Preference)] チェックボックスをオンにします。
[プリファレンス (Preferences)] フィールドが表示されます。
 4. BGP ローカルプリファレンス パス値を入力します。
範囲は 0 ~ 4294967295 です。
 5. [完了 (Finish)] をクリックします。

6. この既存の IP ベースの L3Out の [BGP ピア接続プロファイル (BGP Peer Connectivity Profile)] 画面に戻ります。
 [テナント (Tenants)]>[tenant_name_for_IP_handoff_L3Out]>[ネットワーキング (Networking)]>[L3Outs]>[L3out-name]>[論理ノード プロファイル (Logical Node Profiles)]>[logical-node-profile-name]>[論理インターフェイス プロファイル (Logical Interface Profiles)]>[logical-interface-profile-name]>[BGP_peer_connectivity_profile]
7. [ルート制御プロファイル (Route Control Profile)]領域までスクロールし、この既存の IP ベースの L3Out に使用されているエクスポートルート制御ポリシーとインポートルート制御ポリシーの両方のルート プロファイル名を確認します。
8. [テナント (Tenants)]>[tenant_name_for_IP_handoff_L3Out]>[ポリシー (Policies)]>[プロトコル (Protocol)]>[ルート制御のルート マップ (Route Maps for Route Control)]の順に移動します。
9. 最初に、この既存の IP ベースの L3Out に使用されているエクスポートルート制御プロファイルを見つけ、そのルート プロファイルをクリックします。
 このルート制御プロファイルのプロパティ ページがメイン パネルに表示されます。
10. ページでルート制御コンテキストエントリを見つけ、ルート制御コンテキスト エントリをダブルクリックします。
 このルート制御コンテキストのプロパティ ページが表示されます。
11. [セットルール (Set Rule)]領域で、BGP ローカルプリファレンス パスを使用してこれらの手順で作成した設定ルールを選択し、[送信 (Submit)]をクリックします。
12. 次に、この既存の IP ベースの L3Out に使用されているインポートルート制御プロファイルを見つけ、そのルート プロファイルをクリックしてから、インポートルート制御プロファイルの BGP ローカルプリファレンス パス エントリを使用してこれらの手順を繰り返します。

ステップ 6 トラフィックが SR-MPLS パスを選択していることを確認します。

ルーティングパスの選択は、SR-MPLS を使用する必要があります (BGP は、IP パスよりも SR-MPLS パスを選択する必要があります)。各 VRF の URIB のトラフィックとルートをモニタして、SR-MPLS パスが選択されていることを確認できます。

次のタスク

に示す手順を使用して、IP ベースの L3Out を切断します。 [IP ベースの L3Out の切断 \(222 ページ\)](#)

IP ベースの L3Out の切断

このタスクでは、IP ベースの L3Out を切断します。

始める前に

- [IP ハンドオフ設定から SR ハンドオフ設定への移行 \(215 ページ\)](#) に記載の情報について、確認してください。
- に示す手順を使用して、IP ベースの L3Out 設定をミラーリングするように SR-MPLS VRF L3Out の外部 EPG を設定します。[SR-MPLS VRF L3Out での外部 EPG の設定 \(216 ページ\)](#)
- インバウンドおよびアウトバウンドトラフィックをリダイレクトし、に示す手順を使用して SR-MPLS L3Out を優先して開始するようにします。[SR-MPLS L3Out へのトラフィックのリダイレクト \(218 ページ\)](#)

ステップ1 IP パスをクリーンアップします。

次のいずれかの方法を使用して、IP パスをクリーンアップできます。

- 以前に設定した IP ベースの L3Out の外部 EPG で一度に 1 つのサブネットを削除します。
- 以前に設定した IP ベースの L3Out の外部 EPG を削除します。

上記のいずれかの方法では、障害がクリアされ、SR-MPLS L3Out の外部 EPG が展開されます。

セキュリティポリシーを IP ベースの L3Out から SR-MPLS L3Out に変更するプロセスの一環として、最大 15 秒のドロップが発生する可能性があります。その期間が経過すると、ACI から外部へのアウトバウンドトラフィックは SR-MPLS パスを使用します。

以前に設定した IP ベースの L3Out が新しい SR-MPLS L3Out に正常に移行された場合は、以前に設定した IP ベースの L3Out を削除できます。

ステップ2 SR-MPLS に移行する追加の L3Out/VRF があるかどうかを確認します。

他のユーザ L3Out および VRF を SR-MPLS に移行するには、[IP ハンドオフ設定から SR ハンドオフ設定への移行 \(215 ページ\)](#) の手順を繰り返します。

[IP ハンドオフ設定から SR ハンドオフ設定への移行 \(215 ページ\)](#) の同じ手順を使用して、テナント GOLF L3Out とテナント SR-MPLS L3Out 間の移行を行うこともできます。

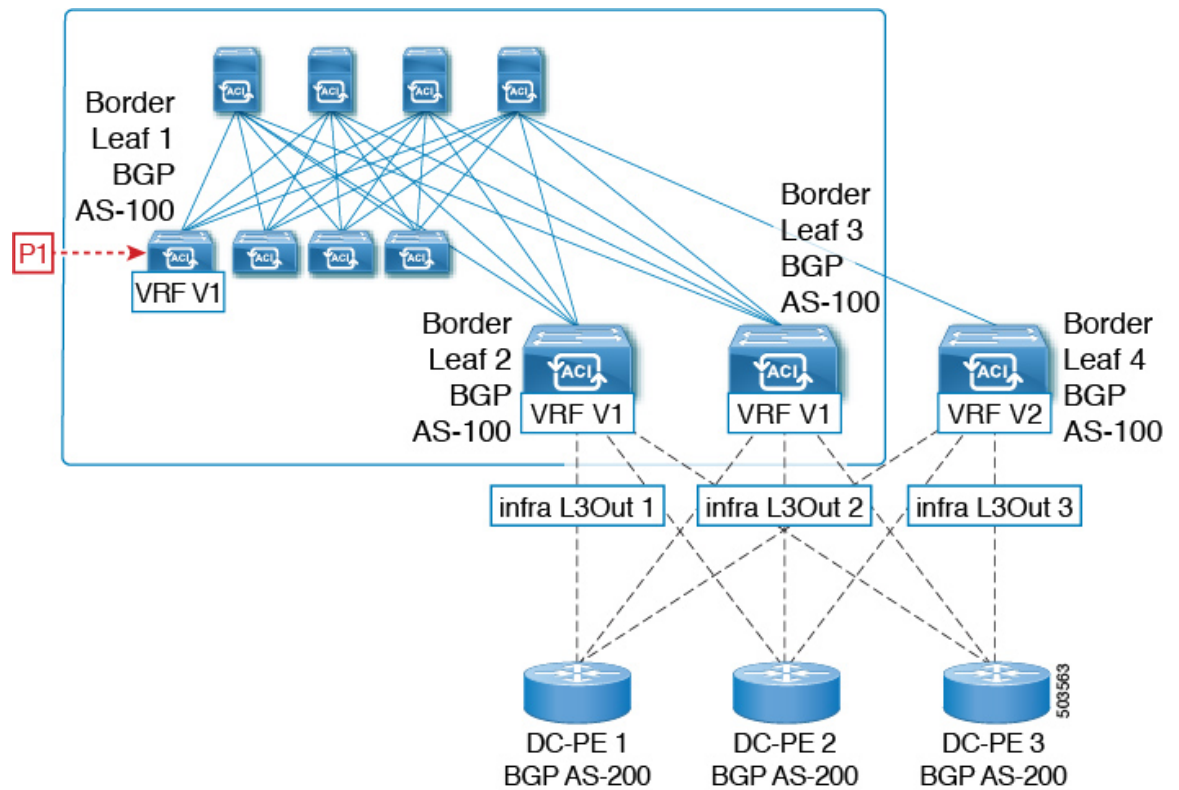
ループ防止のための BGP ドメインパス機能について

BGP ルーティングループは、次のようなさまざまな条件が原因で発生することがあります。

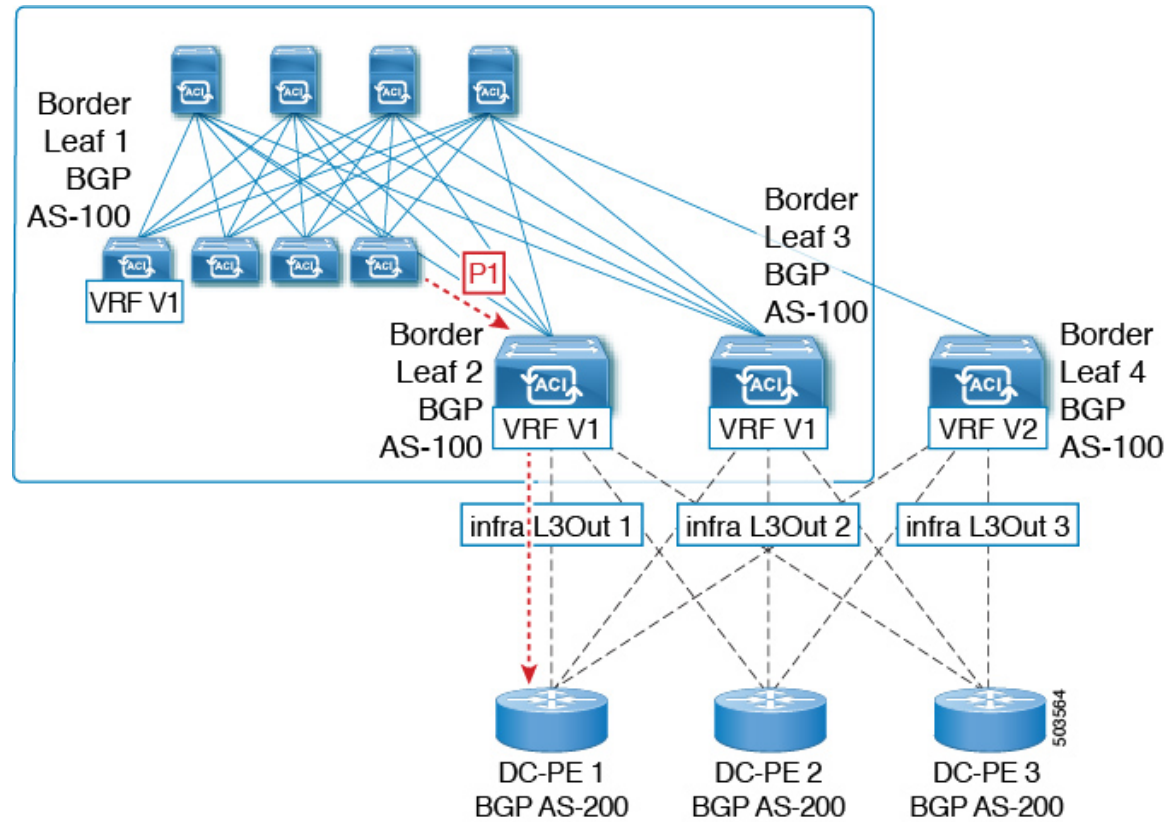
- AS パス チェックなどの既存の BGP ループ防止メカニズムの意図的な無効化
- 異なる VRF または VPN 間のルート リーク

次に、BGP ルーティングループが発生するシナリオの例を示します。

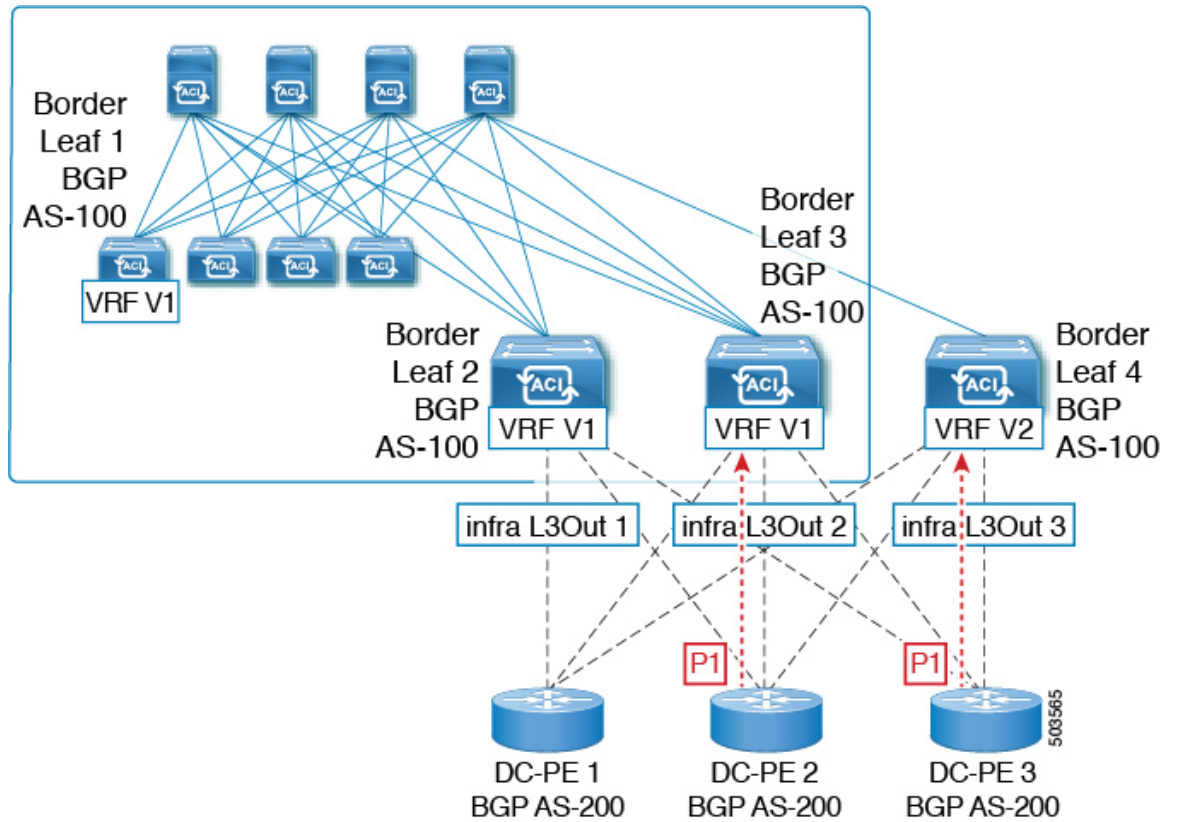
1. BGP IPL3Out ピアから受信したプレフィックス P1 は、Multiprotocol Border Gateway Protocol (MP-BGP) を使用して ACI ファブリックでアドバタイズされます。



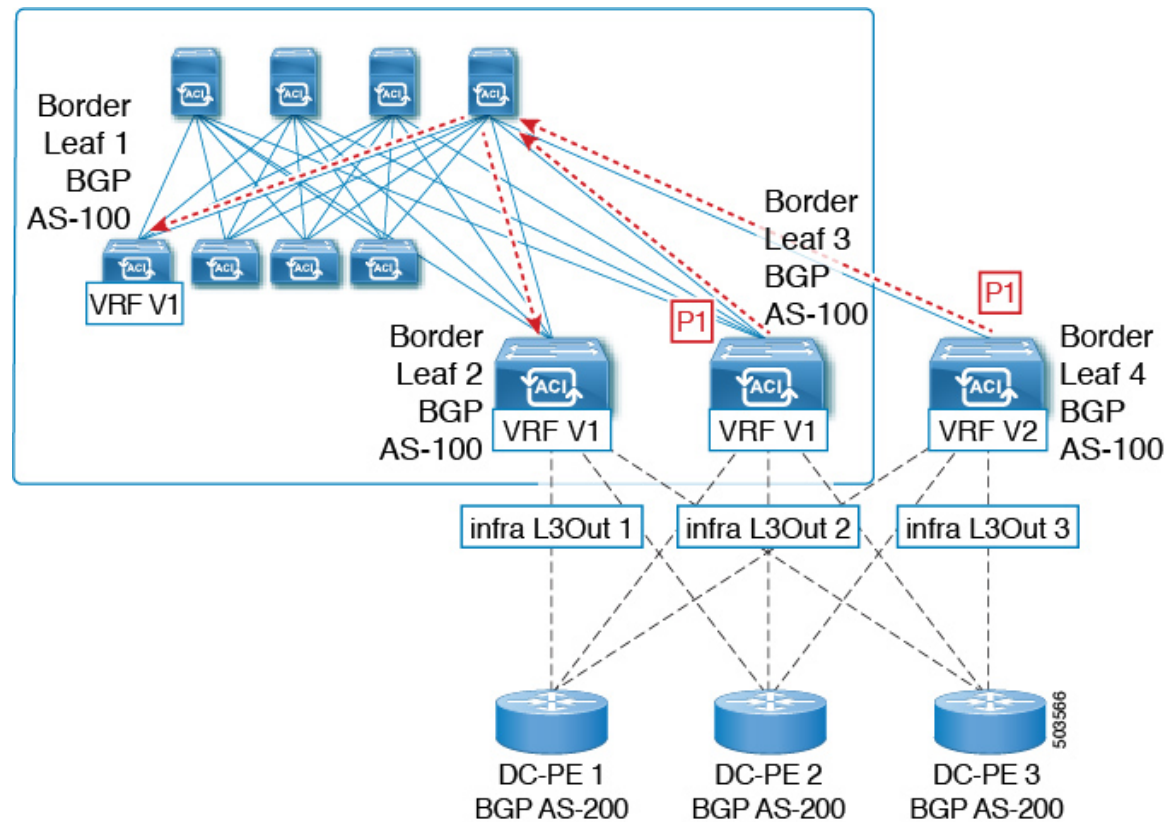
2. 中継のケースとして、このプレフィックスは SR-MPLS インフラ L3Out を介して外部にアドバタイズできます。



- このプレフィックスは、同じ VRF または異なる VRF のいずれかで、コアから ACI ファブリックにインポートできます。



4. BGP ルーティンググループは、同じ VRF から、または別の VRF からのリークによって、このインポートされたプレフィックスが発信元スイッチにアドバタイズされる時に発生します。



リリース 5.1(3) 以降では、新しい BGP ドメインパス機能を使用できます。これは、次の方法で BGP ルーティング ループを支援します。

- 同じ VPN または拡張 VRF 内、および異なる VPN または VRF 内のルートが通過する個別のルーティング ドメインを追跡します。
- ルートがすでに通過したドメイン内の VRF にループバックするタイミングを検出します（通常、ドメイン間のステッチングポイントである境界リーフスイッチだけでなく、場合によっては内部スイッチでも）。
- ループにつながる場合に、ルートがインポートまたは受け入れられないようにします。

ACI ファブリック内では、VRF スcopeはグローバルであり、設定されているすべてのスイッチに拡張されます。したがって、VRF のドメインからエクスポートされたルートは、他のスイッチの VRF に受信されないようにします。

次のコンポーネントは、ループ防止のために BGP ドメインパス機能で使用されます。

- **Routing domain ID** : ACI サイトのすべてのテナント VRF は、1 つの内部ファブリック ドメイン、各 SR-MPLS インフラ L3Out の各 VRF に 1 つのドメイン、および各 IP L3Out に 1 つのドメインに関連付けられます。BGP ドメインパス機能が有効になっている場合、これらの各ドメインには、次の形式で一意的なルーティング ドメイン ID が割り当てられます。Base:<variable>

- Base は、[BGP ルートリフレクタ ポリシー (BGP Route Reflector Policy)] ページの [ドメイン ID ベース (Domain ID Base)] フィールドに入力されたゼロ以外の値です。
- <variable> は、そのドメイン専用ランダムに生成された値です。
- **ドメインパス (Domain path)** : ルートが通過するドメインセグメントは、BGP ドメインパス属性を使用して追跡されます。
 - ルートを受信する送信元ドメインの VRF のドメイン ID がドメインパスの先頭に追加されます。
 - 送信元ドメイン ID はドメインパスの先頭に追加され、境界リーフスイッチのドメイン間でルートが再生成されます。
 - VRF のローカルドメイン ID のいずれかがドメインパスにある場合、外部ルートは受け入れられません。
 - ドメインパスは、次のように表される各ドメインセグメントとともに、オプションの遷移 BGP パス属性として伝送されます。 <Domain-ID:SAFI>
 - ACI 境界リーフスイッチは、ドメイン内のリンクを追跡するために、ローカルに発信されたルートと外部ルートの両方に VRF 内部ドメイン ID を付加します。
 - 内部ドメインからのルートをインポートし、競合する外部ドメイン ID を持つノードの VRF にインストールして、内部バックアップまたは中継パスを提供できます。
 - インフラ L3Out ピアの場合、ピアドメインのドメイン ID がルートのドメインパスに存在する場合、ピアへのルートのアダプタイズメントはスキップされます (アウトバウンドチェックは IP L3Out ピアには適用されません)
 - 境界リーフスイッチと非境界リーフスイッチはどちらもドメインパス属性を処理します。



(注) ループ防止のために BGP ドメインパス機能を設定するか、GUI または REST API を使用して、受信したドメインパスを送信するように設定をイネーブルにすることができます。ループ防止のために BGP ドメインパス機能を設定したり、NX-OS スタイルの CLI を介して受信ドメインパスを送信するように設定したりすることはできません。



(注) 以前のリリースからリリース 5.1(3) にアップグレードするときに、VRF 間共有サービス用に設定されたコントラクトがある場合、BGP ドメイン ID にリリース 5.1(3) にアップグレードする前に設定された契約で設定されています。このような状況では、契約を削除してから、契約を追加し直すと、BGP ドメインの更新が可能になります。これは、リリース 5.1(3) へのアップグレード前に設定された契約がある場合にのみ問題になります。これは、リリース 5.1(3) へのアップグレードの完了後に新しい契約を作成する場合は問題になりません。

GUIを使用したループ防止のためのBGPドメインパス機能の設定

始める前に

[ループ防止のためのBGPドメインパス機能について \(223ページ\)](#)に記載されている情報を使用して、BGPドメインパス機能に精通します。

ステップ1 ループ防止にBGPドメインパス機能を使用する場合は、BGPルートリフレクターにBGPドメインパス属性を設定します。

(注) ループ防止にBGPドメインパス機能を使用しないが、受信したドメインパスを送信する場合は、この手順でBGPドメインリフレクターのBGPドメインパス機能を有効にしないでください。代わりに、に直接移動して、適切なBGP接続ウィンドウの[ドメインパスの送信 (Send Domain Path)] フィールドのみを有効にします。 [ステップ2 \(230ページ\)](#)

a) [システム (System)] > [システム設定 (System Settings)] > [BGPルートリフレクター (BGP Route Reflector)] の順に移動します。

[BGPルートリフレクター (BGP Route Reflector)] ウィンドウが表示されます。このウィンドウで[ポリシー (Policy)] ページタブが選択されていることを確認します。

b) [ドメインIDベース (Domain ID Base)] フィールドを見つけます。

c) [ドメインIDベース (Domain ID Base)] フィールドに数値を入力します。

- BGPドメインパス機能を有効にするには、1 ~ 4294967295 の値を入力します。ACIファブリックがマルチサイト環境の一部である場合は、この[ドメインIDベース (Domain ID Base)] フィールドでこのACIファブリックに固有の一意の値を使用してください。
- BGPドメインパス機能を無効にするには、この[ドメインIDベース (ID Base)] フィールドに0を入力します。

ループ防止のBGPドメインパス機能が有効になっている場合は、Base:<variable>形式の暗黙のルーティングドメインIDが割り当てられます。

- [ベース (Base)] は、この[ドメインIDベース (Domain ID Base)] フィールドに入力したゼロ以外の値です。
- <変数 (variable) > は、VRFまたはL3Out用にランダムに生成された値で、ループ防止のBGPドメインパス機能に使用されます。

このルーティングドメインIDは、次のドメインを識別するためにBGPに渡されます。

- VRF : そのテナントのVRFウィンドウの[ポリシー (Policy)] タブにある[ルーティングドメインID (Routing Domain ID)] フィールドに示されているように、各VRFにランダムに生成された値を使用して内部ドメインIDによって識別されます。
- IP L3Out : IP L3Outの[BGPピア接続プロファイル (BGP Peer Connectivity Profile)] ウィンドウの[ルーティングドメインID (Routing Domain ID)] フィールドに示されているように、各IP L3Outに対してランダムに生成された値を使用して、外部ドメインIDによって識別されます。

- SR-MPLS infra L3Out : 各 SR-MPLS VRFL3Out のウィンドウの [SR-MPLS Infra L3Outs] テーブルの [ルーティングドメイン ID (Routing Domain ID)] 列に示されているように、各 SR-MPLS infra L3Out の各 VRF にランダムに生成された値を使用して、外部ドメイン ID によって識別されます。

Domain-Path 属性は、パス内のルーティングドメイン ID に基づいてループをチェックするために着信方向で処理されます。Domain-Path 属性はピアに送信されます。これは、次の手順で説明するように、IP L3Out または SR-MPLS infraL3Out の BGP ピアレベルの [ドメインパスの送信 (Send Domain Path)] フィールドを使用して個別に制御されます。

ステップ 2 BGP ドメインパス属性をピアに送信するには、適切な BGP 接続ウィンドウで [ドメインパスの送信 (Send Domain Path)] フィールドを有効にします。

ループ防止のために BGP ドメインパス機能を使用する場合は、最初に [ドメインベース ID (Domain Base ID)] を設定してから、ここで [ドメインパスの送信 (Send Domain Path)] フィールドを有効にします。ステップ 1 (229 ページ) ループ防止のために BGP ドメインパス機能を使用しない場合でも、受信したドメインパスを送信する場合は、ここで [ドメインパスの送信 (Send Domain Path)] フィールドのみを有効にします (その場合は [ドメインベース ID (Domain Base ID)] を設定しないでください)。ステップ 1 (229 ページ)

- IP L3Out ピアの [ドメインパスの送信 (Send Domain Path)] フィールドを有効にするには、次の手順を実行します。

1. IP L3Out ピアの [BGP ピア接続プロファイル (BGP Peer Connectivity Profile)] ウィンドウに移動します。

[テナント (Tenant)] > [tenant_name] > [ネットワーク (Networking)] > [L3Outs] > [L3Out_name] > [論理ノードプロファイル (Logical Node Profile)] > [log_node_prof_name] > [論理インターフェイスプロファイル (Logical Interface Profile)] > [log_int_prof_name] > [BGP ピア (BGP Peer)] > [address]-ノード (Node) -[<node_ID>]

この設定された L3Out の [BGP ピア接続プロファイル (BGP Peer Connectivity Profile)] ウィンドウが表示されます。

2. [BGP ピア接続プロファイル (BGP Peer Connectivity Profile)] ウィンドウで [BGP 制御 (BGP Controls)] 領域を見つけます。
3. [BGP 制御 (BGP Controls)] 領域で、[ドメインパスの送信 (Send Domain Path)] フィールドの横にあるボックスをクリックします。
4. [送信 (Submit)] をクリックします。

このアクションは、BGP ドメインパス属性をピアに送信します。

- SR-MPLS インフラ L3Out ピアの [ドメインパスの送信 (Send Domain Path)] フィールドを有効にするには、次の手順を実行します。

1. [テナント (Tenant)] > [infra] > [ネットワーク (Networking)] > [SR-MPLS Infra L3Outs] > [SR-MPLS-infra-L3Out_name] > [論理ノードプロファイル (Logical Node Profiles)] > [log_node_prof_name] の順に移動します。

この設定済み SR-MPLS インフラ L3Out の [論理ノードプロファイル (Logical Node Profile)] ウィンドウが表示されます。

2. [BGP-EVPN 接続プロファイル (BGP-EVPN Connectivity Profile)] 領域を見つけ、新しいBGP-EVPN 接続ポリシーを作成するか、または既存のBGP-EVPN 接続ポリシーの[ドメインパスの送信 (Send Domain Path)] フィールドを有効にするかを決定します。
 - 新しいBGP-EVPN 接続ポリシーを作成する場合は、[BGP-EVPN 接続プロファイル (BGP-EVPN Connectivity Profile)] 領域のテーブルの上にある [+] をクリックします。[BGP-EVPN 接続ポリシーの作成 (Create BGP-EVPN Connectivity Policy)] ウィンドウが表示されます。
 - 既存のBGP-EVPN 接続ポリシーの[ドメインパスの送信 (Send Domain Path)] フィールドを有効にする場合は、[BGP-EVPN 接続プロファイル (BGP-EVPN Connectivity Profile)] 領域のテーブルでそのポリシーをダブルクリックします。[BGP-EVPN 接続ポリシー (BGP-EVPN Connectivity Policy)] ウィンドウが表示されます。
3. ウィンドウで[BGP 制御 (BGP Controls)] 領域を見つけます。
4. [BGP 制御 (BGP Controls)] 領域で、[ドメインパスの送信 (Send Domain Path)] フィールドの横にあるボックスをクリックします。
5. [送信 (Submit)] をクリックします。

このアクションは、BGP ドメインパス属性をピアに送信します。

ステップ3 適切なエリアに移動して、さまざまなドメインに割り当てられたルーティング ID を確認します。

- VRF ドメインに割り当てられたルーティング ID を確認するには、次の手順を実行します。

Tenant tenant_name Networking VRFs VRF_name をクリックし、その VRF の[ポリシー (Policy)] タブをクリックして、[VRF] ウィンドウの[ルーティング ドメイン ID (Routing Domain ID)] フィールドのエントリを見つけます。 >>>
- IP L3Out ドメインに割り当てられたルーティング ID を確認するには、次の手順を実行します。

[テナント (Tenants)] > [tenant_name] > [ネットワーキング (Networking)] > [L3Outs] > [L3Out_name] > [論理ノード プロファイル (Logical Node Profiles)] > [log_node_prof_name] > [BGP ピア (BGP Peer)] の順に移動し、その後[BGP ピア接続プロファイル (BGP Peer Connectivity Profile)] ウィンドウの[ルーティング ドメイン ID (Routing Domain ID)] フィールドでエントリを見つけます。
- SR-MPLS インフラ L3Out ドメインに割り当てられたルーティング ID を確認するには、次の場所に移動します。

[テナント (Tenants)] [tenant_name] [ネットワーキング (Networking)] [SR-MPLS VRF L3Outs] [SR-MPLS_VRF_L3Out_name] をクリックし、[SR-MPLS VRFL3Out] のウィンドウで [SR-MPLS Infra L3Outs] テーブルの [ルーティング ドメイン ID (Routing Domain ID)] カラムのエントリを見つけます。 >>>



第 II 部

外部ルーティング（L3Out）の設定

- WAN およびその他の外部ネットワーク フォワーディング (235 ページ)
- 外部ネットワークへのルーテッド接続 (251 ページ)
- L3Out のノードとインターフェイス (273 ページ)
- ルーティング プロトコルのサポート (287 ページ)
- ルート集約 (337 ページ)
- ルート マップおよびルート プロファイルによるルート制御 (347 ページ)
- ルーティングとサブネット範囲 (373 ページ)
- トランジット ルーティング (381 ページ)
- 共有サービス (409 ページ)
- L3Out の QoS (417 ページ)
- IP SLAs (421 ページ)
- HSRP (441 ページ)
- Cisco ACI GOLF, on page 449



第 16 章

WAN およびその他の外部ネットワーク フォワーディング

この章は、次の内容で構成されています。

- ネットワーク ドメイン (235 ページ)
- ルータ ピアリングおよびルート配布 (236 ページ)
- ルートのインポートとエクスポート、ルート集約、ルートコミュニティの一致 (237 ページ)
- ACI のルート再配布 (242 ページ)
- ACI ファブリック内のルート配布 (242 ページ)
- 外部レイヤ 3 Outside 接続タイプ (243 ページ)
- レイヤ 3 外部接続の設定のモードについて (246 ページ)
- L3Out ネットワーク インスタンス プロファイルで設定されているサブネットで有効な制御 (247 ページ)
- ACI レイヤ 3 Outside ネットワークのワークフロー (249 ページ)

ネットワーク ドメイン

ファブリック管理者は、ポート、プロトコル、VLAN プール、およびカプセル化を設定するドメインポリシーを作成します。これらのポリシーは、単一テナント専用にすることも、共有することもできます。ファブリック管理者が ACI ファブリック内にドメインを設定すると、テナント管理者はテナント エンドポイント グループ (EPG) をドメインに関連付けることができます。

以下のネットワーク ドメイン プロファイルを設定できます。

- VMM ドメイン プロファイル (vmmDomP) は、仮想マシンのハイパーバイザ統合のために必要です。
- 物理ドメイン プロファイル (physDomP) は、ベア メタル サーバ接続と管理アクセスに使用します。

- ブリッジド外部ネットワーク ドメインプロファイル (l2extDomP) は通常、ACI ファブリックのリーフ スイッチにブリッジド外部ネットワーク トランク スイッチを接続するために使用されます。
- ルーテッド外部ネットワーク ドメインプロファイル (l3extDomP) は、ACI ファブリックのリーフ スイッチにルータを接続するために使用されます。
- ファイバチャネルドメインプロファイル(fcDomP)は、ファイバチャネルのVLANとVSANを接続するために使用されます。

ドメインは VLAN プールに関連付けられるように設定されます。その後、EPG は、ドメインに関連付けられている VLAN を使用するように設定されます。

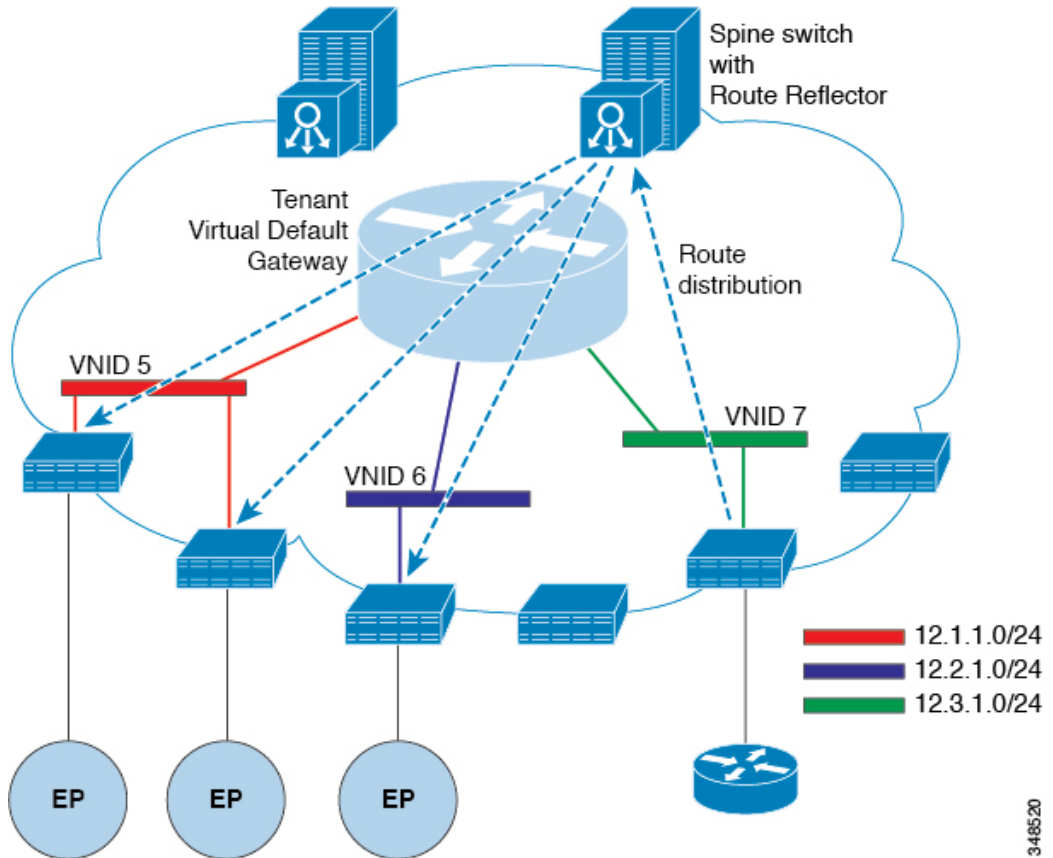


- (注) EPG ポートと VLAN の設定は、EPG が関連付けられているドメイン インフラストラクチャ設定で指定されている設定に一致する必要があります。一致しない場合、APIC でエラーが発生します。そのようなエラーが発生した場合は、ドメイン インフラストラクチャ設定が EPG ポートと VLAN の設定に一致していることを確認してください。

ルータ ピアリングおよびルート配布

次の図に示すように、ルーティング ピア モデルを使用すると、リーフ スイッチ インターフェイスが外部ルータのルーティング プロトコルとピアリングするように静的に設定されます。

図 24: ルータのピアリング



ピアリングによって学習されるルートは、スパインスイッチに送信されます。スパインスイッチはルートリフレクタとして動作し、外部ルートを同じテナントに属するインターフェイスを持つすべてのリーフスイッチに配布します。これらのルートは、最長プレフィクス照合 (LPM) により集約されたアドレスで、外部ルータが接続されているリモートのリーフスイッチのVTEP IP アドレスが含まれるリーフスイッチの転送テーブルに配置されます。WAN ルートには転送プロキシはありません。WAN ルートがリーフスイッチの転送テーブルに適合しない場合、トラフィックはドロップされます。外部ルータがデフォルトゲートウェイではないため、テナントのエンドポイント (EP) からのパケットは ACI ファブリックのデフォルトゲートウェイに送信されます。

348520

ルートのインポートとエクスポート、ルート集約、ルートコミュニティの一致

サブネットルートのエクスポートまたはインポート設定オプションは、次に説明するスコープおよび集約オプションに従って指定できます。

ルーティング対象サブネットについては、以下のスコープ オプションが使用可能です。

- エクスポート ルート制御サブネット：エクスポート ルート方向を制御します。
- インポート ルート制御サブネット：インポート ルート方向を制御します。



(注) インポートルートコントロールは、BGP と、OSPF が EIGRP ではなく、サポートされています。

- 外部 EPG (セキュリティ インポート サブネット) の外部サブネット: どの外部サブネットが、特定の外部 L3Out EPG (`l3extInstP`) の一部として適用されるコントラクトを保持するか指定します。サブネットの `l3extInstP` 外部 EPG として分類、サブネット上の範囲を「インポートセキュリティ」に設定する必要があります。この範囲のサブネットを決定する IP アドレスが関連付けられています、 `l3extInstP` 。これが決定されると、契約は、他のどの Epg でその外部のサブネットが通信を許可を決定します。たとえば、レイヤ 3 外部の外部ネットワーク (`L3extOut`) の ACI スイッチでトラフィックが開始する場合、 `l3extInstP` に関連付けられている送信元 IP アドレスを判断するための検索が行われます。このアクションより一般的なサブネット上で複数の特定のサブネットが優先されるようにで最長プレフィックス一致 (ほか) に基づいて行われます。
- 共有ルート制御サブネット — 共有サービス設定においては、この特性が有効になっているサブネットだけが、コンシューマ EPG の Virtual Routing and Forwarding (VRF) にインポートされます。これは VRF 間の共有サービスのルート方向を制御します。
- 共有セキュリティ インポート サブネット：インポート対象サブネットに共有コントラクトを適用します。デフォルトの仕様では、外部 EPG 用外部サブネットが設定されています。

ルート対象サブネットを集約することができます。集約が設定されていない場合は、サブネットが正確に照合されます。たとえば、サブネットが 11.1.0.0/16 の場合、11.1.1.0/24 ルートにはポリシーが適用されず、ルートが 11.1.0.0/16 である場合のみ適用されます。すべてのサブネットを 1 つずつ定義する作業は面倒でエラーが発生しやすいので、それを回避するために、サブネットのセットを 1 つのエクスポート、インポートまたは共有ルートポリシーに集約することができます。現時点では、0/0 サブネットのみ集約可能です。0/0 に集約を指定すると、次の選択オプションに基づき、すべてのルートがインポート、エクスポートされ、異なる VRF と共有されます:

- 集約エクスポート — VRF (サブネット 0/0) のすべての中継ルートをエクスポートします。
- 集約インポート — 所定の L3 ピア (サブネット 0/0) のすべて着信ルートをインポートします。



(注) BGP、OSPF が EIGRP の集約インポートルート制御はサポートされません。

- 集約共有ルート — 1 つの VRF で学習されているルートを別の VRF にアドバタイズする必要がある場合、サブネットとの正確な一致、またはサブネットマスクに従った方法で共有

できます。集約共有ルートでは、複数のサブネットマスクを使用して、どの特定のルートグループを VRF 間で共有するかを決定できます。たとえば、10.1.0.0/16 と 12.1.0.0/16 を指定してこれらのサブネットを集約することができます。あるいは、0/0 を使用すると、複数の VRF のすべてのサブネット ルートを共有できます。



- (注) 第 2 世代のスイッチの VRF 機能間で正常にルートが共有されます (N9K-93108TC-EX など、スイッチ モデル名の最後やその後に「EX」や「FX」がつく Cisco Nexus N9K)。第 1 世代のスイッチですが、ルートを保存する物理的な 3 進コンテンツ対応メモリ (TCAM) にルートの解析を完全にサポートするだけの容量がないため、この設定のパケットは失敗する可能性があります。

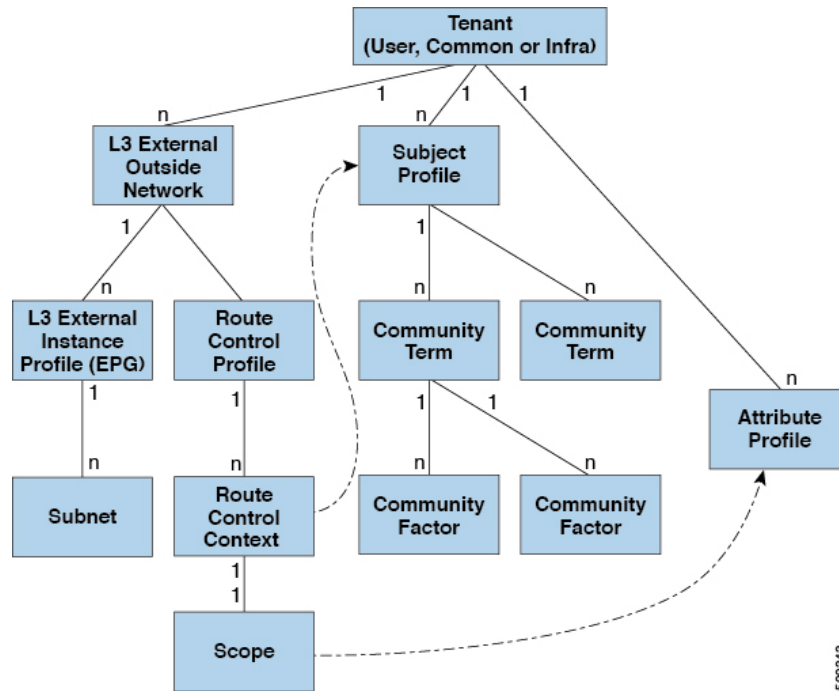
ルート集約では、多数の具体的なアドレスを 1 つのアドレスに置き換えることで、ルートテーブルが簡素化します。たとえば、10.1.1.0/24、10.1.2.0/24、10.1.3.0/24 は 10.1.0.0/16 に置き換えられます。ルート集約ポリシーにより、ボーダー リーフ スイッチとそのネイバー リーフ スイッチの間でルートを効率的に共有することができます。BGP、OSPF、あるいは EIGRP のルート集約ポリシーは、ブリッジドメインまたは中継サブネットに適用されます。OSPF では、エリア間ルート集約と外部ルート集約がサポートされます。集約ルートはエクスポートされません。ファブリック内でのアドバタイズは行われません。上記の例では、ルート集約ポリシーが適用され、EPG が 10.1.0.0/16 サブネットを使用している場合、10.1.0.0/16 の範囲全体がすべての隣接リーフ スイッチと共有されます。



- (注) 同じリーフ スイッチで 2 つの L3extOut ポリシーに OSPF を設定している場合 (1 つはレギュラーで、もう 1 つはバックボーン) には、VRF 内の全エリアに集約が適用されるため、一方の L3extOut で設定されているルート集約ポリシーが両方の L3extOut ポリシーに適用されます。

次の図に示すように、ルート制御プロファイルは、プレフィックススペースおよびコミュニティベースの一致に基づいて、ルート マップを取得します。

図 25: ルートコミュニティ マッチング



ルート制御プロファイル (rtctrlProfile) は、許可される対象を指定します。ルート制御コンテキストは一致対象を指定し、スコープは設定すべき対象を指定します。サブジェクトプロファイルには、コミュニティ マッチの仕様が含まれます。これは複数の l3extOut で使用できます。サブジェクトプロファイル (subjP) には、それぞれ 1 つまたは複数のコミュニティファクタ (コミュニティ) を含む複数のコミュニティタームを含めることができます。これにより、次のブール演算を指定することができます。

- 複数コミュニティターム間の論理的 OR
- 複数コミュニティターム間の論理的 AND

たとえば、北東と呼ばれるコミュニティタームに、それぞれ多くのルートを含む複数のコミュニティが含まれているとします。また、南東という別のコミュニティタームにも、さまざまなルートが多数含まれているとします。管理者は、そのどちらかあるいは両方を一致させることを選択できます。コミュニティファクタタイプには、レギュラーまたは拡張を使用できます。拡張タイプのコミュニティファクタを使用する際には、仕様間の重複がないよう注意する必要があります。

ルート制御プロファイルのスコープ部分は、属性プロファイル (rtctrlAttrP) を参照して、適用すべき設定-アクション (プリファレンス、ネクストホップ、コミュニティなど) を指定します。ルートを l3extOut から学習した場合は、ルートの属性を変更できます。

上の図は、l3extOut に rtctrlProfile が含まれているケースを示しています。rtctrlProfile はテナントの下にも配置できます。この例では、l3extOut に、自身をテナント下の rtctrlProfile と関連付ける相互リンク関係ポリシー (l3extRsInterleakPol) が設定されています。この設定により、再利用、rtctrlProfile 複数の l3extOut 接続します。BGP 属性

(BGP は、ファブリック内で使用される)は、それを OSPF からは、ファブリックを学習ルートの追跡することもできます。L3extOut 下で定義された `rtctr1Profile` の優先順位は、テナント下で定義されたものよりも高くなります。

`rtctr1Profile` には、組み合わせ可能およびグローバルという 2 つのモードがあります。デフォルトの組み合わせ可能モードでは、パーベイシブサブネット (`fvSubnet`) および外部サブネット (`l3extSubnet`) に一致/設定メカニズムを組み合わせるルートマップをレンダリングします。グローバルモードはテナント内のすべてのサブネットに適用され、そのほかのポリシー属性の設定が無効になります。グローバル `rtctr1Profile` では、明示的な (0/0) サブネットを定義しなくても、すべての動作が許可されます。グローバル `rtctr1Profile` は、コミュニティやネクストホップといった異なるサブネット属性を使用してマッチングが行われる非プレフィックスベースの一致ルールと一緒に使用されます。1 つのテナント下で複数の `rtctr1Profile` ポリシーを設定できます。

`rtctr1Profile` ポリシーによって、デフォルトインポートおよびデフォルトエクスポートのルート制御の拡張が可能になります。集約インポートあるいはエクスポートルートを伴う **Layer 3 Outside** ネットワークには、サポート対象デフォルトエクスポート/デフォルトインポートおよびサポート対象 0/0 集約ポリシーを指定するインポート/エクスポートポリシーを設定できます。すべてのルート (着信または発信) に `rtctr1Profile` ポリシーを適用するには、一致ルールのないグローバルデフォルト `rtctr1Profile` を定義します。

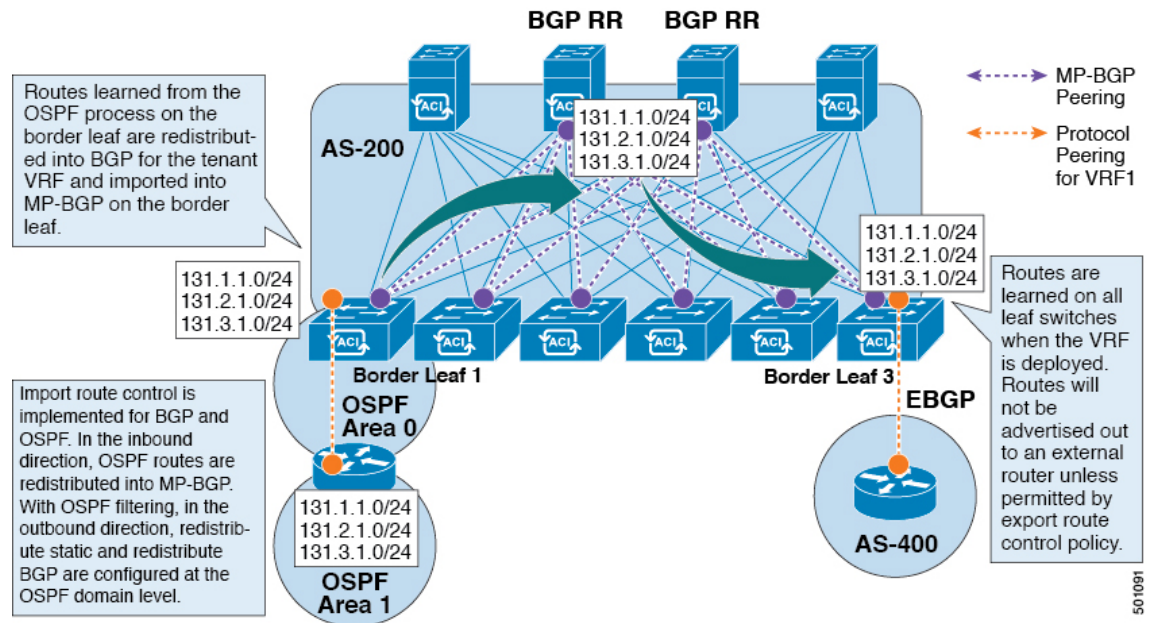


- (注) 1 つのスイッチ上で複数の `l3extOut` 接続を設定することは可能ですが、スイッチは 1 つのルートマップしか持つことができないため、スイッチで設定されているすべてのレイヤ 3 外側ネットワークが同じ `rtctr1Profile` を使用する必要があります。

プロトコル相互リンクと再配布ポリシーは、ACI ファブリック BGP ルートで共有される外部学習ルートを制御します。設定属性はサポートされています。これらのポリシーは L3extOut 単位、ノード単位、VRF 単位でサポートされます。相互リンクポリシーは、L3extOut 内のルーティングプロトコルによって学習されたルートに適用されます。現在のところ、相互リンクと再配布ポリシーは、OSPF v2 および v3 でサポートされています。ルート制御ポリシー `rtctr1Profile` は、相互リンクポリシーによって消費される場合、グローバルとして定義する必要があります。

ACI のルート再配布

図 26: ACI のルート再配布



- 境界リーフの OSPF プロセスで学習されたルートは、テナント VRF 用に BGP に再配布され、それらは境界リーフの MP-BGP にインポートされます。
- インポート ルート制御は、BGP および OSPF ではサポートされていますが、EIGRP ではサポートされていません。
- エクスポート ルート制御は、OSPF、BGP、および EIGRP でサポートされています。
- ルートは、VRF が導入されている境界リーフで学習されます。ルートは、エクスポート ルート制御で許可されていない限り、外部レイヤ 3 Outside 接続にアダプタイズされません。



(注) ブリッジ ドメイン/EPG のサブネットが [Advertise Externally] に設定されている場合、サブネットは境界リーフの静的ルートとしてプログラムされます。スタティック ルートがアダプタイズされると、ルーティング プロトコルに直接注入されない外部ネットワークとして EPG のレイヤ 3 ネットワーク ルーティング プロトコルに再配布されます。

ACI ファブリック内のルート配布

ACI は以下のルーティング メカニズムをサポートします。

- スタティック ルート
- OSPFv2 (IPv4)
- OSPFv3 (IPv6)
- iBGP
- eBGP (IPv4 および IPv6)
- EIGRP (IPv4 および IPv6) プロトコル

ACI は、外部ルータに接続する際に VRF-Lite の実装をサポートします。サブインターフェイスを使用して、境界リーフは 1 つの物理インターフェイスを持つ複数のテナントへのレイヤ 3 Outside 接続を提供できます。VRF-Lite の実装では、テナントごとに 1 つのプロトコルセッションが必要です。

ACI ファブリック内の外部ルートを伝播するために、ACI ファブリック内のリーフスイッチとスパインスイッチの間に Multiprotocol BGP (MP-BGP) が実装されています。単一ファブリック内で多数のリーフスイッチをサポートするために、BGP ルートリフレクタテクノロジーが導入されています。リーフスイッチとスパインスイッチはすべて 1 つの BGP 自律システム (AS) 内にあります。境界リーフが外部ルートを学習すると、MP-BGP アドレスファミリ VPN バージョン 4 または VPN バージョン 6 に特定の VRF の外部ルートを再配布できます。アドレスファミリ VPN バージョン 4 を使用して、MP-BGP は VRF ごとに別の BGP ルーティングテーブルを維持します。MP-BGP 内で、境界リーフは BGP ルートリフレクタであるスパインスイッチにルートをアドバタイズします。その後、ルートは VRF (APIC GUI の用語ではプライベート ネットワーク) がインスタンス化されているすべてのリーフに伝播されます。

外部レイヤ 3 Outside 接続タイプ

ACI は、以下の外部レイヤ 3 Outside 接続オプションをサポートします。

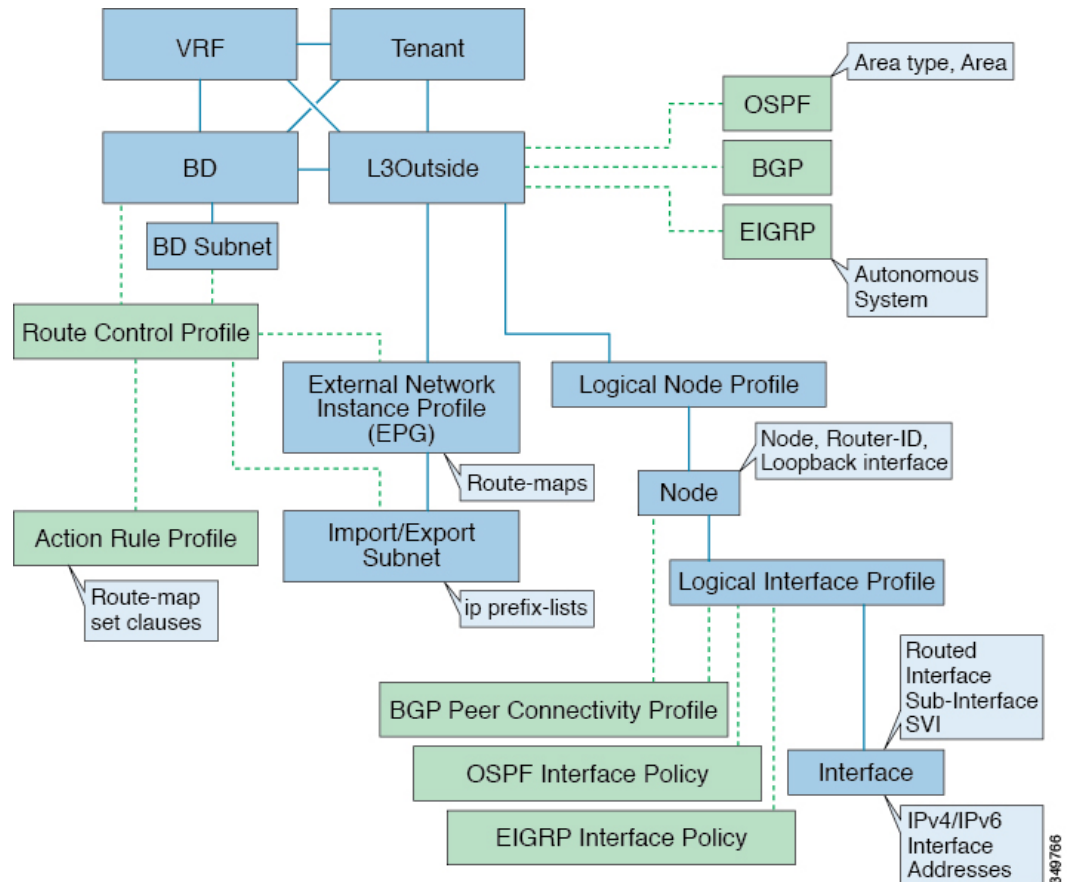
- スタティック ルーティング (IPv4 および IPv6 でサポート)
- 標準および NSSA エリアの OSPFv2 (IPv4)
- 標準および NSSA エリアの OSPFv3 (IPv6)
- iBGP (IPv4 および IPv6)
- eBGP (IPv4 および IPv6)
- BGP (IPv4 および IPv6)

外部レイヤ 3 Outside 接続は、以下のインターフェイスでサポートされます。

- レイヤ 3 ルーテッド インターフェイス
- 802.1Q タギング対応のサブインターフェイス：サブインターフェイスを使用すると、複数のプライベート ネットワークに対するレイヤ 2 外部接続を提供できます。

- スイッチ仮想インターフェイス (SVI) : SVI インターフェイスを使用すると、レイヤ 2 とレイヤ 3 をサポートする同じ物理インターフェイスをレイヤ 2 外部接続とレイヤ 3 外部接続に使用できます。

図 27: ACI レイヤ 3 管理対象オブジェクト



L3Outside 接続に使用される管理対象オブジェクトは、次のとおりです。

- 外部レイヤ 3 Outside (L3ext) : ルーティングプロトコルオプション (OSPF エリアタイプ、エリア、EIGRP 自律システム、BGP)、プライベートネットワーク、外部物理ドメイン。
- 論理ノードプロファイル : 外部レイヤ 3 Outside 接続に対して 1 つ以上のノードが定義されたプロファイル。ルータ ID とループバックインターフェイスの設定はプロファイルで定義されます。



(注) 複数の外部レイヤ 3 Outside 接続間の同じノードには同じルータ ID を使用してください。



(注) 単一の L3Out 内では、ノードは、1つの論理ノードプロファイルの一部でのみあり得ます。単一の L3Out 内に複数の論理ノードプロファイルの一部であるノードを構成すると、1つの論理ノードプロファイルからループバックアドレスがプッシュされるものの、他方からはそうならないなど、予測できない動作が生じる可能性があります。既存の論理インターフェイスプロファイルの下の追加パスのバインディングを使用します。または、既存の論理ノードのプロファイルの下に新しい論理インターフェイスプロファイルを作成してください。

- 論理インターフェイス プロファイル：IPv4 および IPv6 インターフェイスの IP インターフェイス設定。これは、ルートインターフェイス、ルーテッドサブインターフェイス、および SVI でサポートされます。SVI は、物理ポート、ポート チャネルまたは vPC で設定できます。
- OSPF インターフェイス ポリシー：OSPF のネットワーク タイプ、優先順位などの詳細が含まれています。
- EIGRP インターフェイス ポリシー：タイマー、スプリット ホライズン タイマーなどの詳細が含まれています。
- BGP ピア接続プロファイル：ほとんどの BGP ピア設定、リモート AS、ローカル AS、および BGP ピア接続オプションが設定されるプロファイル。BGP ピア接続プロファイルは、ノードプロファイルの下の論理インターフェイスプロファイルまたはループバック インターフェイスに関連付けることができます。これは、BGP ピアリングセッションの update-source 設定を決定します。
- 外部レイヤ 3 Outside EPG (l3extInstP)：外部 EPG はプレフィックス ベースの EPG または InstP と呼ばれます。インポートおよびエクスポートのルート制御ポリシー、セキュリティインポートポリシー、およびコントラクトの関連付けは、このプロファイルで定義されます。単一 L3Out の下に複数の外部 EPG を設定できます。単一外部レイヤ 3 Outside 接続で別のルートまたはセキュリティ ポリシーが定義されている場合、複数の外部 EPG を使用できます。1つの外部 EPG または複数の外部 EGP がルート マップにまとめられません。外部 EPG で定義されるインポート/エクスポートサブネットは、ルート マップの IP プレフィックスリストの match 句と関連しています。外部 EPG は、インポートセキュリティサブネットとコントラクトが関連付けられる場所でもあります。これは、この L3out のトラフィックの許可またはドロップに使用されます。
- アクションルールプロファイル：アクションルールプロファイルは、L3Out のルートマップの set 句を定義するために使用されます。サポートされる set 句は、BGP communities (standard および extended)、Tags、Preference、Metric、および Metric type です。
- ルート制御プロファイル：ルート制御プロファイルは、アクションルールプロファイルを参照するために使用されます。これは、アクションルールプロファイルの順序付きプ

ロファイルにすることができます。ルート制御プロファイルは、テナント BD、BD サブネット、外部 EPG、または外部 EPG サブネットで参照できます。

BGP、OSPF、および EIGRP L3Out 用の追加のプロトコル設定が存在します。これらの設定は、GUI の [ACI Protocol Policies] セクションでテナントごとに設定されます。



- (注) 外部 EPG (中継ルーティング ケース) の間でポリシーの適用を設定する際には、エクスポート ルート制御、集約エクスポート、および外部のセキュリティのために、デフォルトプレフィックスである 0/0 で 2 番目の外部 EPG (InstP) を設定する必要があります。さらに、優先グループを除外し、中継 InstPs 間では任意の契約 (または適切な契約) を使用する必要があります。

レイヤ 3 外部接続の設定のモードについて

APIC は設定のための複数のユーザ インターフェイス (UI) をサポートしているので、1 つの UI を使用して設定を作成し、その後、別の UI を使用して設定を変更する場合は、予期しないインタラクションが潜んでいます。ここでは、さらに他の APIC のユーザ インターフェイスを使用した可能性がある場合、APIC NX-OS スタイルの CLI を使用してレイヤ 3 外部接続を設定するための考慮事項を説明します。

APIC NX-OS スタイルの CLI を使用してレイヤ 3 外部接続を設定する場合、次の 2 つのモードを選択することができます。

- よりシンプルな暗黙 モードは、APIC GUI または REST API と互換性がありません。
- 名前付き (または明示) モードは、APIC GUI および REST API と互換性があります。

いずれの場合も、設定は互換性がない UI では読み取り専用であると考えてください。

モードの違いについて

どちらのモードでも、構成設定は API の **l3extOut** クラスのインスタンスである内部コンテナ オブジェクト「L3 Outside」 (または「L3Out」) 内で定義されます。2 つのモード間の主な違いは、このコンテナ オブジェクト インスタンスの命名にあります。

- 暗黙モード: コンテナのネーミングは潜在的であり、CLI コマンドには表示されません。CLI は、これらのオブジェクトを内部的に作成し保持します。
- 名前付きモード: 名前はユーザーが決定します。名前付きモードの CLI コマンドには、追加の **l3Out** フィールドがあります。名前付き L3Out がを正常に設定され障害を回避するためには、ユーザーが外部レイヤ 3 用の API オブジェクト モデルを理解する必要があります。



- (注) 「名前付きモードセクションを使用したレイヤ3外部接続の設定」セクションの手順を除き、このガイドでは、暗黙モードの手順を説明します。

注意事項および制約事項

- 同じ APIC インターフェイスでは、両方のモードを、次の制限でレイヤ3外部接続を設定するために一緒に使用することができます。テナント VRF、およびリーフの特定の組み合わせのレイヤ3外部接続設定は、1つのモードを介してのみ実行できます。
- 特定のテナント VRF の場合、外部 L3 EPG を配置できるポリシー ドメインは、名前付きモードまたは暗黙モードのいずれかになります。推奨する設定方式は、特定のテナント VRF が、レイヤ3外部接続用に展開されたすべてのノード全体で、特定のテナント VRF の組み合わせに対して1つのモードだけを使用することです。モードは、異なるテナントまたは異なる VRF 全体で変えることができ、制限は適用されません。
- 場合によっては、Cisco APIC クラスタへの着信設定で不整合が検証されます。外部から確認できる設定 (L3Out を通過するノースバウンドトラフィック) も検証の対象です。設定が無効な場合は、「Invalid Configuration」エラー メッセージが表示されます。
- 外部レイヤ3機能は、次の例外を除いて、両方の設定モードでサポートされます
 - L4 ~ L7 サービス アプライアンスを使用したルーティング ピ어링とルートヘルスインジェクション (RHI) は、名前付きモードでのみをサポートされます。名前付きモードは、ルーティング ピ어링が含まれるテナント VRF のすべての境界リーフスイッチ全体で使用する必要があります。
- 暗黙モード CLI 手順を使用して作成されたレイヤ3外部ネットワーク オブジェクト (l3extOut) は、「_ui_」で始まる名前で識別され、GUI で読み取り専用としてマークされます。CLI は、インターフェイス、プロトコル、ルートマップ、EPG などの機能で、これらの外部 L3 ネットワークを分割します。REST API を介して実行される設定変更は、この構造を破棄することができ、CLI を介してさらなる変更を防ぐことができます。

このようなオブジェクトを削除する手順については、『*APIC Troubleshooting Guide*』の「*Troubleshooting Unwanted _ui_ Objects*」を参照してください。

L3Out ネットワーク インスタンス プロファイルで設定されているサブネットで有効な制御

L3Out ネットワーク インスタンス プロファイルで設定されているサブネットに対して以下の制御を有効にすることができます。

表 7: ルート制御オプション

ルート制御設定	用途	オプション (Options)
エクスポート ルート制御	ルートマップと IP プレフィックスリストを使用して、どの外部ネットワークがファブリックからアドバタイズされるかを制御します。IP プレフィックスリストは、定義されているサブネットごとに BL スイッチに作成されます。エクスポート制御ポリシーは、デフォルトで有効になっており、BGP、EIGRP、および OSPF でサポートされています。	特定の一致(プレフィックスとプレフィックス長)。
インポート ルート制御	ファブリックに許可されているサブネットを制御します。ルールを設定してルートをフィルタリングすることができます。BGP および OSPF ではサポートされますが、EIGRP ではサポートされません。サポートされていないプロトコルのインポート制御ポリシーを有効にすると、自動的に無視されます。インポート制御ポリシーは、デフォルトでは有効になっていませんが、 [L3Out の作成 (Create L3Out)] パネルで有効にすることができます。 [Identity] タブで、 [Route Control Enforcement: Import] を有効にします。	特定の一致(プレフィックスとプレフィックス長)。
セキュリティインポートサブネット	2つのプレフィックス ベースの EPG 間をパケットが流れるようにするために使用されません。ACL で実装されます。	ACL のプレフィックスまたはワイルドカードによる一致ルールを使用します。

ルート制御設定	用途	オプション (Options)
集約エクスポート	すべてのプレフィックスを外部ピアにアドバタイズできるようにするために使用されます。0.0.0.0/le 32 IP プレフィックスリストで実装されます。	0.0.0.0/0 サブネット (すべてのプレフィックス) の場合にのみサポートされます。
集約インポート	外部 BGP ピアからの着信であるすべてのプレフィックスを許可するために使用されます。0.0.0.0/0 le 32 IP プレフィックスリストで実装されます。	0.0.0.0/0 サブネット (すべてのプレフィックス) の場合にのみサポートされます。

L3Out接続からすべての中継ルートをアドバタイズすることをお勧めします。この場合、プレフィックス0.0.0.0/0の集約エクスポートオプションを使用します。この集約エクスポートオプションを使用すると、APICシステムがエクスポートルートマップのマッチ句として使用するIPプレフィックスリストエントリ (permit 0.0.0.0/0 le 32) が作成されます。出力を表示するには、**show route-map <outbound route-map>** および **show ip prefix-list <match-clause>** コマンドを使用します。

集約共有ルートを有効にすると、ある VRF で学習されたルートを別の VRF にアドバタイズする必要がある場合、サブネットを正確に一致させることでルートを共有するか、集約サブネットマスクを使用してルートを共有できます。複数のサブネットマスクを使用して、特定のルートグループを VRF 間で共有するかどうかを判断できます。たとえば、10.1.0.0/16 と 12.1.0.0/16 を指定してこれらのサブネットを集約することができます。あるいは、0/0 を使用すると、複数の VRF のすべてのサブネット ルートを共有できます。

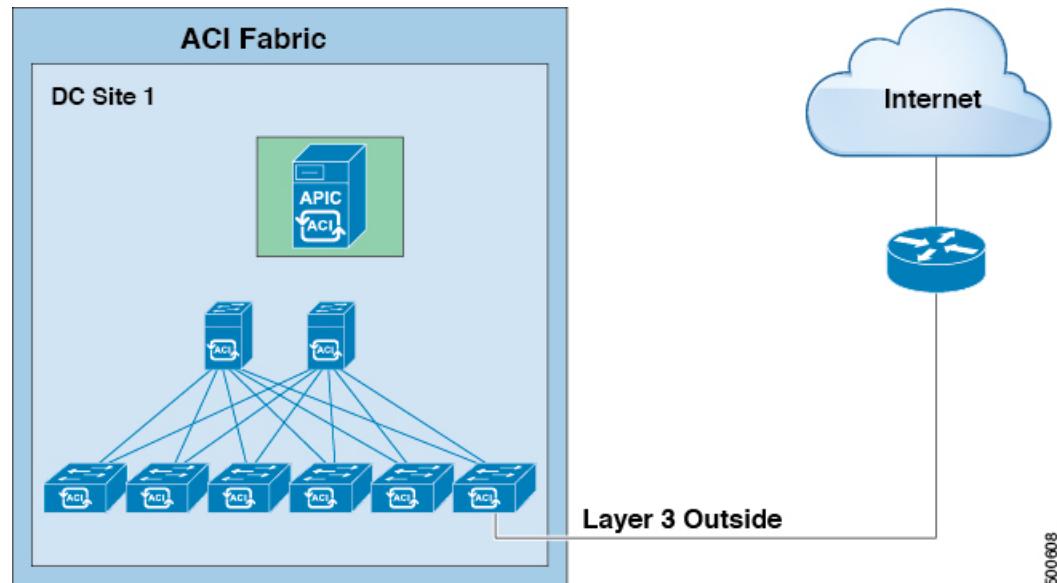


- (注) 第2世代のスイッチの VRF 機能間で正常にルートが共有されます (N9K-93108TC-EX など、スイッチモデル名の最後やその後に「EX」や「FX」がつく Cisco Nexus N9K)。第1世代のスイッチですが、ルートを保存する物理的な3進コンテンツ対応メモリ (TCAM) にルートの解析を完全にサポートするだけの容量がないため、この設定のパケットは失敗する可能性があります。

ACI レイヤ 3 Outside ネットワークのワークフロー

このワークフローでは、レイヤ 3 Outside (L3Out) ネットワーク接続を設定するために必要なステップの概要を示します。

図 28: レイヤ 3 Outside ネットワーク接続



1. 前提条件

- インフラセキュリティドメインに読み取り/書き込みアクセス権限があることを確認します。
- 必要なインターフェイスを持つターゲットリーフスイッチが使用できることを確認します。

レイヤ 3 Outside ネットワークの設定

次の L3Out シナリオのいずれかを選択します。

- 単一のテナント内で消費される L3Out について、BGP または OSPF の設定の指示に従います。
- 複数のテナント間で消費 (共有) される L3Out について、「共有レイヤ 3 Out」のガイドラインに従います。
- L3Out の中継ルーティング使用例については、ACI 中継ルーティング手順に従ってください。

注：この機能には APIC リリース 1.2 (1x) 以降が必要です。



第 17 章

外部ネットワークへのルーテッド接続

この章は、次の内容で構成されています。

- [外部ネットワークへルーテッドされた接続について \(251 ページ\)](#)
- [L3Out ウィザードの作成 \(253 ページ\)](#)
- [アダプタイズ ホスト ルート \(267 ページ\)](#)
- [ルート リフレクタの設定 \(270 ページ\)](#)

外部ネットワークへルーテッドされた接続について

ネットワーク構成 (L3Out) 外部レイヤ 3 では、ファブリック以外のトラフィックを転送する方法を定義します。レイヤ 3 はし、他のノードのアドレスを見つける、ルートを選択して、サービスの品質を選択して、入力して、終了、およびファブリックを移動する際は、トラフィックを転送に使用されます。



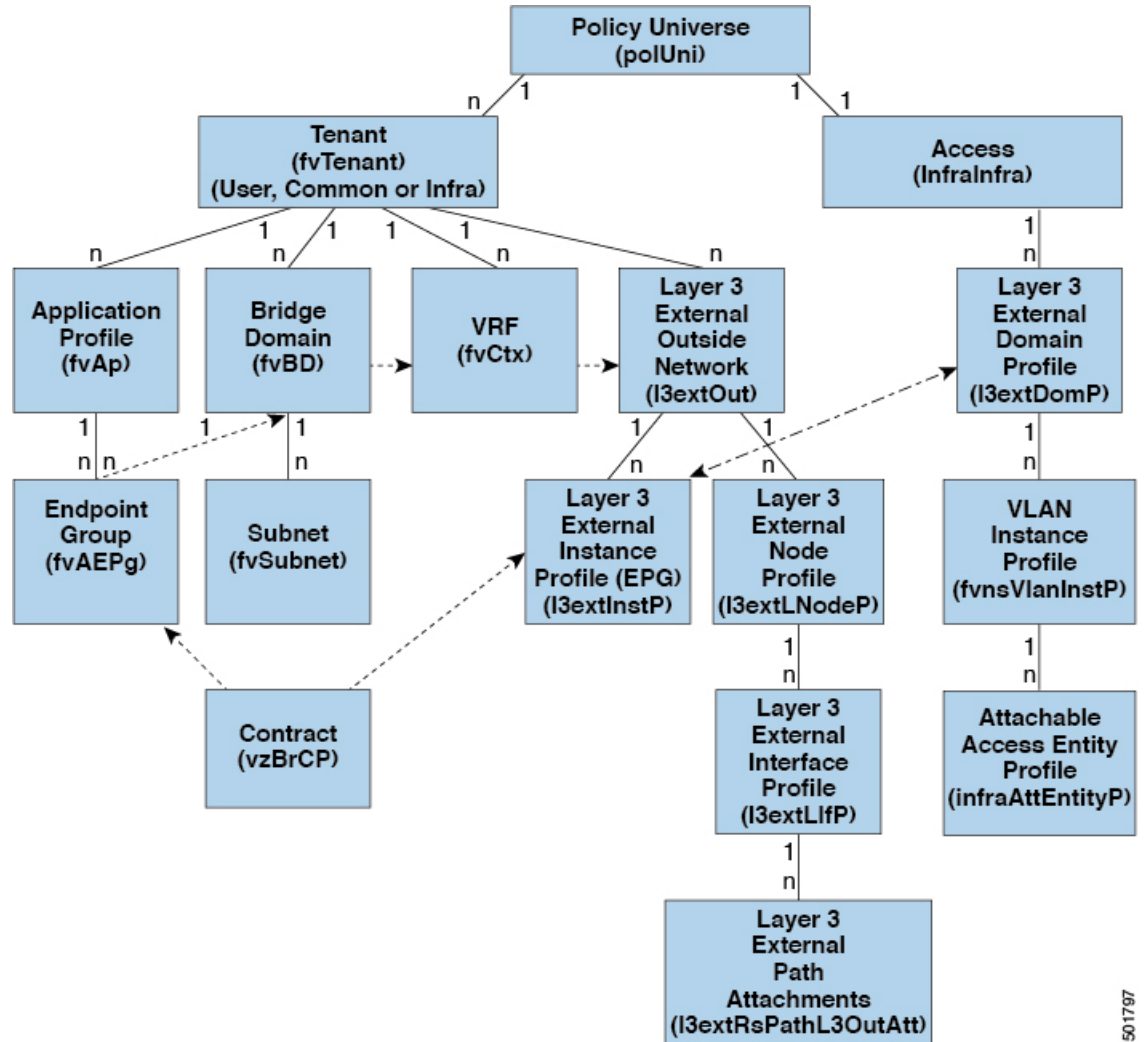
(注) ガイドラインとの設定と接続の外部レイヤ 3 を維持するための注意事項は、次を参照してください。 [レイヤ 3 ネットワーキングの注意事項 \(459 ページ\)](#)。

L3Outs の種類についての詳細は、[外部レイヤ 3 Outside 接続タイプ \(243 ページ\)](#) を参照してください。

外部ネットワークへのルーテッド接続のためのレイヤ 3 Out

外部ネットワークへのルーテッド接続は、次の図の階層で示すようにファブリック アクセス (infraInfra) 外部ルーテッド ドメイン (l3extDomP) をレイヤ 3 外部外側ネットワーク (l3extOut) のテナント レイヤ 3 外部インスタンス プロファイル (l3extInstP または外部 EPG) に関連付けることによって有効になります。

図 29: レイヤ 3 外部接続のポリシー モデル



レイヤ 3 外部アウトサイドネットワーク (l3extOut オブジェクト) には、ルーティングプロトコルのオプション (BGP、OSPF、または EIGRP またはサポートされている組み合わせ) およびスイッチとインターフェイス固有の設定が含まれています。l3extOut にルーティングプロトコル (たとえば、関連する仮想ルーティングおよび転送 (VRF) およびエリア ID を含む OSPF) が含まれる一方で、レイヤ 3 外部インターフェイスのプロファイルには必要な OSPF インターフェイスの詳細が含まれます。いずれも OSPF のイネーブル化に必要です。

l3extInstP EPG は、コントラクトを通してテナント EPG に外部ネットワークを公開します。たとえば、Web サーバのグループを含むテナント EPG は、l3extOut に含まれるネットワーク設定に応じてコントラクトを介して l3extInstP EPG と通信できます。外部ネットワーク設定は、ノードを L3 外部ノードプロファイルに関連付けることで複数のノードに容易に再利用できます。同じプロファイルを使用する複数のノードをフェールオーバーやロードバランシングのために設定できます。ノードを複数の l3extOuts に追加することで、l3extOuts に関連付けられている VRF がノードでも展開されます。拡張性に関する情報については、現行の「*Verified Scalability Guide for Cisco ACI*」を参照してください。

L3Out ウィザードの作成

APIC リリース 4.2(1) には、L3Out を設定するための簡単なワークスルーを提供する新しい Create L3Out ウィザードが導入されています。

Create L3Out ウィザードは、ACI ファブリックが外部レイヤ 3 ネットワークに接続する方法を定義する L3Out の設定プロセスを合理化します。[L3Out の作成 (Create L3Out)] ウィザードを使用して、次のページで L3Out コンポーネントに必要な基本設定を行います。

- [識別 (Identity)] ページ : このページは、L3Out の基本設定、およびスタティック ルーティングとダイナミック ルーティング プロトコルの設定に使用します。
- [ノードとインターフェイス (Nodes and Interfaces)] ページ : このページは、レイヤ 3 およびレイヤ 2 インターフェイスタイプのノードプロファイルとインターフェイスプロファイルを設定するために使用されます。
- [プロトコル (Protocols)] ページ : このページは、[識別 (Identity)] ページで選択したプロトコルに基づいて特定のポリシーを設定するために使用します。
- [外部 EPG (External EPG)] ページ : このページは、外部 EPG のコントラクトとサブネットを設定するために使用します。

L3Out の設定例

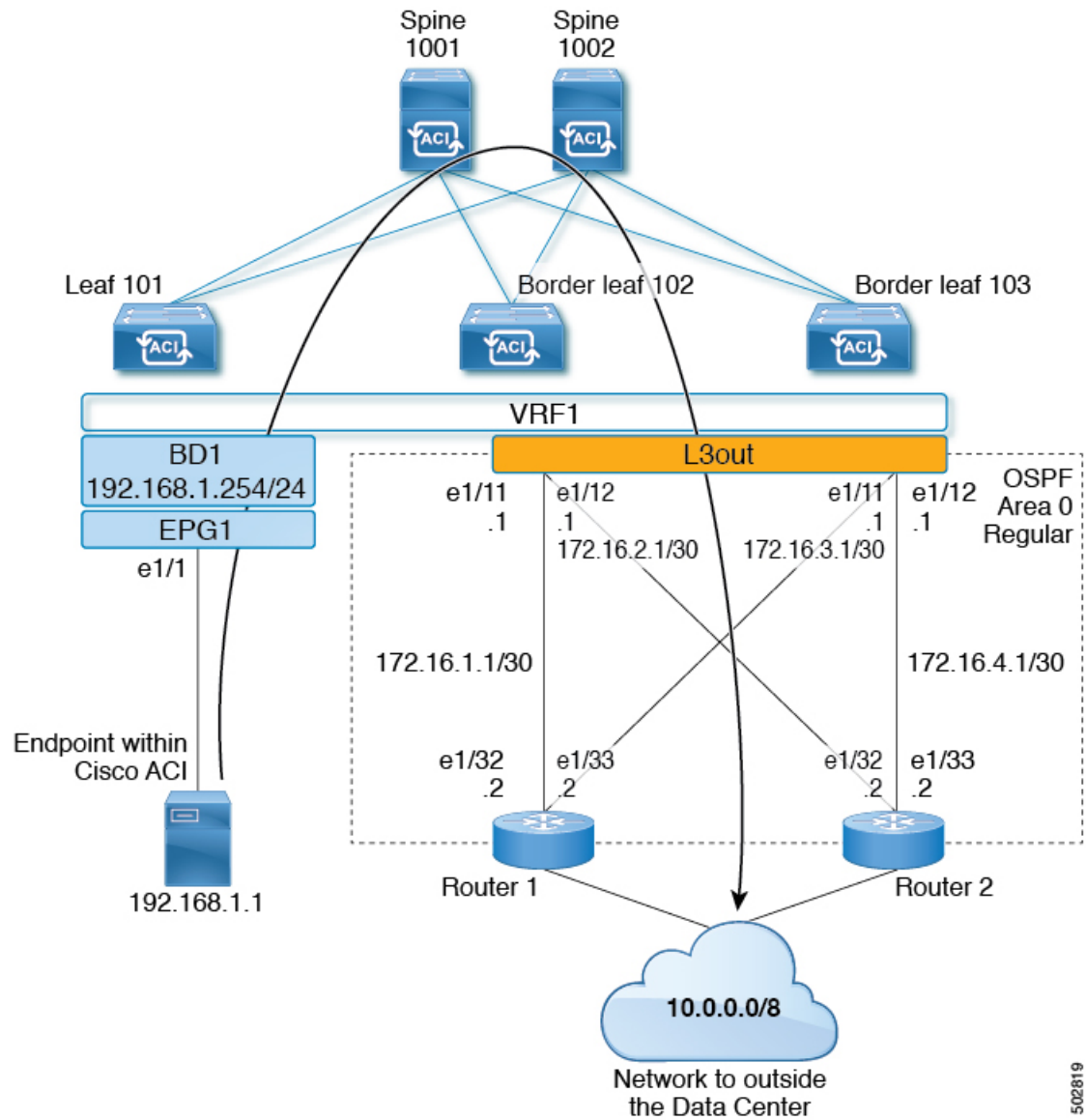
[L3Out の作成 (Create L3Out)] ウィザードを使用して L3Out を設定する場合は、さまざまなオプションを使用できます。次に、2 つの外部ルータで OSPF L3Out を設定する L3Out 設定の例を示します。これは、一般的な設定プロセスを理解するのに役立ちます。



(注) この例では、Cisco APIC リリース 4.2(x) および関連する GUI 画面を使用します。

トポロジの例

図 30: 2つの外部ルータがある OSPF L3Out のトポロジ例



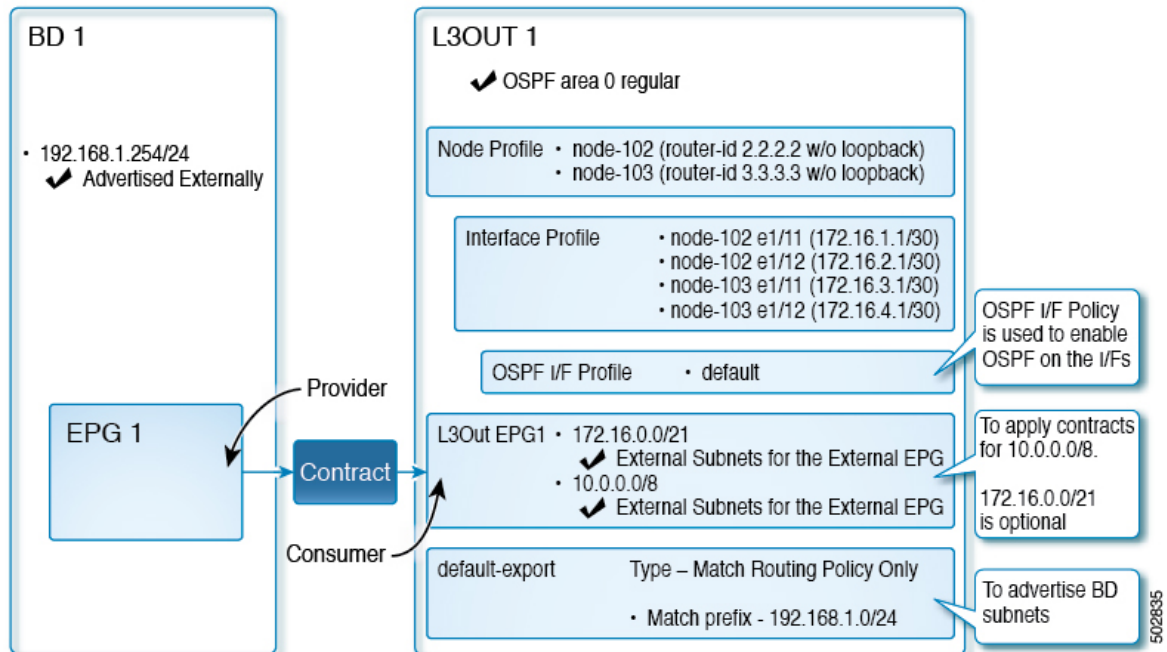
この基本的な L3Out の例は、次の方法を示しています。

- 次の仕様で L3Out を設定します。
 - エリア 0 の OSPF
 - 2 台の外部ルータを使用
 - ルーテッドインターフェイス
 - 2 つの境界リーフ スイッチ

502819

- デフォルトルートマップ (default-export) を使用して BD サブネットをアドバタイズします。
- EPG1 と外部ルート (10.0.0/8) 間のコントラクトとの通信を許可する

図 31: OSPF 構成図

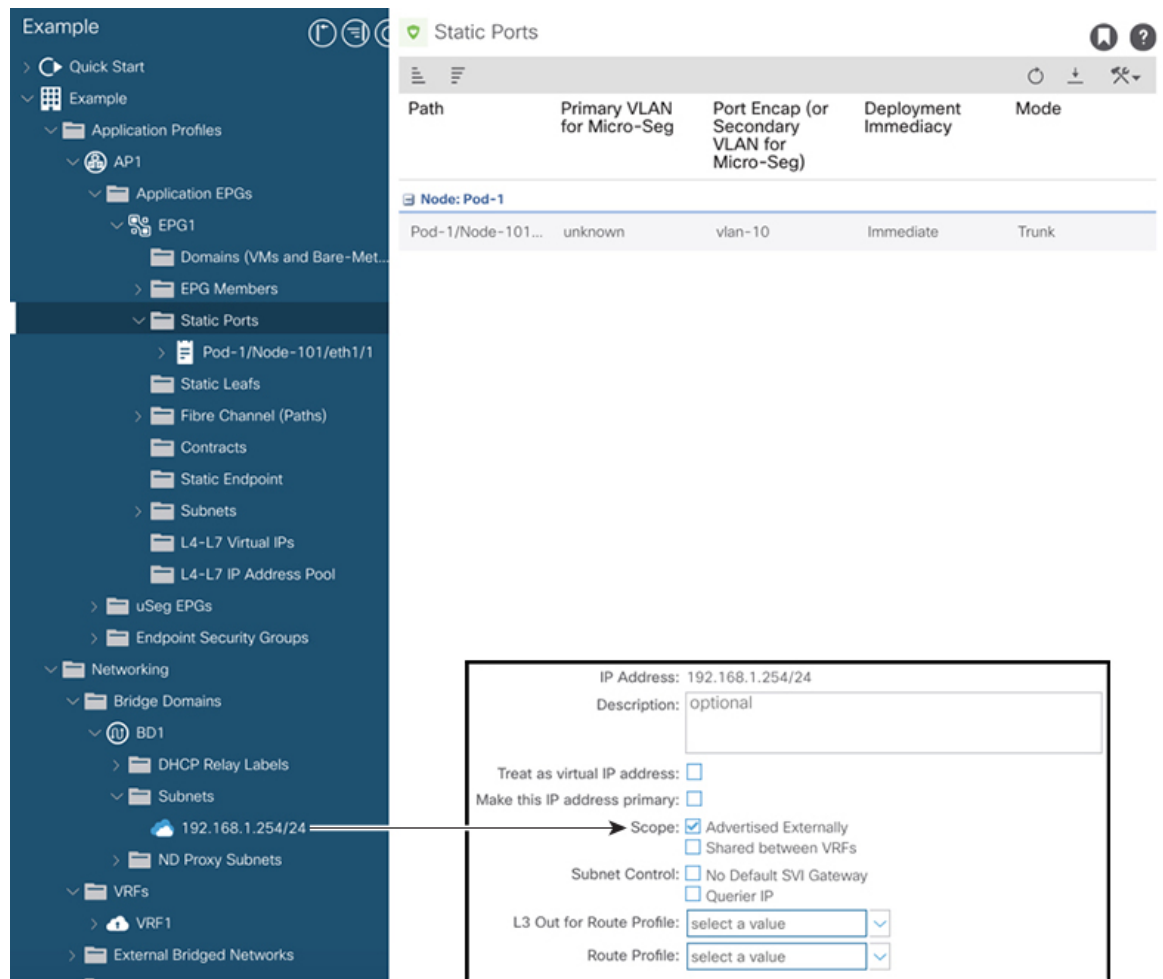


上記の図は、のトポロジ例の設定を示しています。図 30: 2つの外部ルータがある OSPF L3Out のトポロジ例 (254 ページ) この例の設定フローは次のとおりです。

1. L3Out : これにより、
 - L3Out 自体 (OSPF パラメータ)
 - ノード、インターフェイス、OSPF I/F プロファイル
 - 外部 EPG の範囲の外部サブネットを持つ L3Out EPG
2. BD サブネットのアドバタイズ :
 - **default-export** route-map
 - **Advertise Externally** スコープを持つ BD サブネット
3. EPG-L3Out コミュニケーションを許可 (Allow EPG-L3Out communication) : これは、EPG1 と L3Out EPG1 間のコントラクトを使用します。

前提条件

図 32: 前提条件として作成されたオブジェクトの画面例



- この設定例では、L3Out 設定部分のみに焦点を当てています。VRF、BD、EPG、アプリケーションプロファイル、アクセスポリシー（レイヤ 3 ドメインなど）などの他の設定は対象外です。上記のスクリーンショットは、次のような前提条件のテナント設定を示しています。

- VRF1
- サブネット 192.168.1.254/24 の BD1
- エンドポイントへのスタティックポートを持つ EPG1

Create L3Out Wizard を使用した L3Out の作成例

このタスクでは、「トポロジの例」で説明する OSPF L3Out を作成します。このタスクに続いて、示すように、2つの境界リーフスイッチと2つの外部ルータとの OSPF ネイバーシップ

を設定します。Cisco ACI 図 30 : 2 つの外部ルータがある OSPF L3Out のトポロジ例 (254 ページ)

ステップ 1 GUI の [ナビゲーション (Navigation)] ペインの、[テナント例 (Tenant Example)] で [ネットワーキング (Networking)] [L3Out] の順に移動します。 >

ステップ 2 [L3Out の作成 (Create L3Out)] を右クリックして選択します。

ステップ 3 [L3Out の作成 (Create L3Out)] スクリーンで、[識別 (Identity)] タブを選択して次のアクションを実行

します。

- [名前 (Name)] フィールドで、L3Out の名前を入力します。(EXAMPLE_L3Out1)
- [VRF] フィールドおよび[L3 ドメイン (L3 Domain)] フィールドで、適切な値を選択します。(VRF1, EXAMPLE_L3DOM)
- [OSPF] フィールドで、チェック ボックスをオンにします。
- [OSPF 領域 ID (OSPF Area ID)] フィールドで、値 0 またはテキスト [バックボーン (backbone)] を選択します。
- [OSPF 領域タイプ (OSPF Area Type)] フィールドで、[レギュラー領域 (Regular area)] を選択します。
- 残りのフィールドはデフォルト値のままにします。

ステップ 4 [次へ (Next)] をクリックして [ノードとインターフェイス (Nodes and Interfaces)] 画面を表示し、次の操作を実行します。

Create L3Out

1. Identity 2. Nodes And Interfaces 3. Protocols 4. External EPG

Nodes and Interfaces

The L3Out configuration consists of node profiles and interface profiles. An L3Out can span across multiple nodes in the fabric. All nodes used by the L3Out can be included in a single node profile and is required for nodes that are part of a VPC pair. Interface profiles can include multiple interfaces. When configuring dual stack interfaces a separate interface profile is required for the IPv4 and IPv6 configuration, that is automatically taken care of by this wizard.

Use Defaults:

Interface Types

Layer 3: Routed Routed Sub SVI Floating SVI

Layer 2: Port Direct Port Channel

Nodes

Node ID	Router ID	Loopback Address	Hide Interfaces
leaf2 (Node-102)	2.2.2.2	<input type="text"/>	<input type="button" value="+ Hide Interfaces"/>
Interface	IP Address	MTU (bytes)	
eth1/11	172.16.1.1/30 address/mask	inherit	<input type="button" value="+"/>
eth1/12	172.16.2.1/30 address/mask	inherit	<input type="button" value="+"/>
leaf3 (Node-103)	3.3.3.3	<input type="text"/>	<input type="button" value="+ Hide Interfaces"/>
Interface	IP Address	MTU (bytes)	
eth1/11	172.16.3.1/30 address/mask	inherit	<input type="button" value="+"/>
eth1/12	172.16.4.1/30 address/mask	inherit	<input type="button" value="+"/>

Click + icon to add another node

Click + icon to add another interface

Previous Cancel Next

- [インターフェイス タイプ (Interface Types)] 領域の [レイヤ 3 (Layer 3)] フィールドと [レイヤ 2 (Layer 2)] フィールドで、選択内容が上記のスクリーンショットの選択内容と一致することを確認します。
- [ノード (Nodes)] 領域で、[ノード ID (Node ID)] フィールドのドロップダウンリストからノード ID を選択します。(leaf2 (Node 102))
- [ルータ ID (Router ID)] フィールドに、適切なルータ ID を入力します。(2.2.2.2)
[ループバック アドレス (Loopback Address)] フィールドは、入力したルータ ID 値に基づいて自動的に入力されます。ループバック アドレスは必要ないため、値を削除し、フィールドを空白のままにします。
- [インターフェイス (Interface)] フィールドで、インターフェイス ID を選択します。(eth1/11)
- [IP アドレス (IP Address)] フィールドに、関連付けされた IP アドレスを入力します。(172.16.1.1/30)
- [MTU] フィールドはデフォルト値のままにします。(inherit)
- [MTU] フィールドの横にある [+] アイコンをクリックして、ノード leaf2 のインターフェイスを追加します。(Node-102)
- [インターフェイス (Interface)] フィールドで、インターフェイス ID を選択します。(eth1/12)

- i) [IP アドレス (IP Address)] フィールドに、関連付けされた IP アドレスを入力します。(172.16.2.1/30)
- j) [MTU] フィールドはデフォルト値のままにします。(inherit)

ステップ 5 別のノードを追加するには、[ループバック アドレス (Loopback Address)] フィールドの横にある [+] アイコンをクリックし、次の操作を実行します。

(注) [+] アイコンをクリックすると、以前に入力した領域の下に新しい [ノード (Nodes)] 領域が表示されます。

- a) [ノード (Nodes)] 領域で、[ノード ID (Node ID)] フィールドのドロップダウンリストからノード ID を選択します。(leaf3 (Node-103))
- b) [Router ID] フィールドに、ルータ ID を入力します。(3.3.3.3)

[ループバック アドレス (Loopback Address)] フィールドは、入力したルータ ID 値に基づいて自動的に入力されます。ループバック アドレスは必要ないため、値を削除し、フィールドを空白のままにします。

- c) [インターフェイス (Interface)] フィールドで、インターフェイス ID を選択します。(eth1/11)
- d) [IP Address] フィールドに、IP アドレスを入力します。(172.16.3.1/30)
- e) [MTU] フィールドはデフォルト値のままにします。(inherit)
- f) [MTU] フィールドの横にある [+] アイコンをクリックして、ノード leaf3 のインターフェイスを追加します。(Node-103)
- g) [インターフェイス (Interface)] フィールドで、インターフェイス ID を選択します。(eth1/12)
- h) [IP アドレス (IP Address)] フィールドに、関連付けされた IP アドレスを入力します。(172.16.4.1/30)
- i) [MTU] フィールドはデフォルト値のままにします。(inherit)、[次へ (Next)] をクリックします。各インターフェイスのノード、インターフェイス、および IP アドレスを指定しました。

ステップ 6 [次へ (Next)] をクリックして、[プロトコル (Protocols)] 画面を表示します。

この画面では、hello-interval、network-type などを設定するための OSPF インターフェイス レベル ポリシーを指定できます。

Create L3Out

1. Identity 2. Nodes And Interfaces 3. Protocols 4. External EPG

Protocol Associations

OSPF

Node ID: 102		Hide Policy <input type="checkbox"/>
Interface	Policy	
1/11,1/12	select a value	

Node ID: 103		Hide Policy <input type="checkbox"/>
Interface	Policy	
1/11,1/12	select a value	

Previous Cancel Next

この例では、何も選択されていません。したがって、デフォルト ポリシーが使用されます。デフォルトの OSPF インターフェイス プロファイルは、ネットワーク タイプとして Unspecified を使用します。デ

Create L3Out Wizard を使用した L3Out の作成例

フォルトはブロードキャストネットワークタイプです。サブインターフェイスのポイントツーポイントネットワークタイプでこれを最適化するには、「OSPF インターフェイスレベルパラメータの変更（任意）」を参照してください。

ステップ 7 [次へ (Next)] をクリックします。

[外部 EPG (External EPG)] 画面に L3Out EPG の詳細が表示されます。この設定では、コントラクトに適用する EPG にトラフィックを分類します。

ステップ 8 [外部 EPG (External EPG)] スクリーンで次のアクションを実行します。

Create L3Out ? ✕

1. Identity 2. Nodes And Interfaces 3. Protocols **4. External EPG**

External EPG

The L3Out Network or External EPG is used for traffic classification, contract associations, and route control policies. Classification is matching external networks to this EPG for applying contracts. Route control policies are used for filtering dynamic routes exchanged between the ACI fabric and external devices, and leaked into other VRFs in the fabric.

Name:

Provided Contract:

Consumed Contract:

Default EPG for all external networks:

Subnets

IP Address	Scope	Name	Aggregate	Route Control Profile	Route Summarization Policy
10.0.0.0/8	External Subnets for the External EPG				
172.16.0.0/21	External Subnets for the External EPG				

Previous Cancel Finish

a) [外部 EPG (External EPG)] 領域で、[名前 (Name)] フィールドに、外部 EPG の名前を入力します。(L3Out_EPG1)

b) [提供されたコントラクト (Provided Contract)] フィールドでは、値を選択しないでください。

この例では、通常の EPG (EPG1) がプロバイダーであるため、L3Out_EPG1 に提供されるコントラクトはありません。

c) [消費されたコントラクト (Consumed Contract)] フィールドで、ドロップダウンリストから、[デフォルト (default)] を選択します。

ステップ 9 [すべての外部ネットワークのデフォルト EPG (Default EPG for all external networks)] フィールドで、チェックボックスをオフにし、次の操作を実行します。

a) [サブネット (Subnets)] 領域の [+] アイコンをクリックして、[サブネットの作成 (Create Subnet)] ダイアログボックスを表示します。

b) [IP アドレス (IP Address)] フィールドに、サブネットを入力します。(10.0.0.0/8)

c) [外部 EPG 分類 (External EPG Classification)] フィールドで、[外部 EPG の外部サブネット (External Subnets for the External EPG)] のチェックボックスをオンにします。[OK] をクリックします。

ステップ 10 [サブネット (Subnets)] 領域の [+] アイコンをもう一度クリックして [サブネットの作成 (Create Subnet)] ダイアログボックスを表示し、次の操作を実行します。

(注) これはオプションの設定ですが、エンドポイントがこれらの IP と通信する必要がある場合に備えて、L3Out インターフェイス サブネットを指定することをお勧めします。

a) [IP アドレス (IP Address)] フィールドに、サブネットを入力します。(172.16.0.0/21)

このサブネットは、L3Out内のすべてのインターフェイスをカバーします。代わりに、各ルーテッドインターフェイスの個々のサブネットを使用できます。

- b) [外部 EPG 分類 (External EPG Classification)] フィールドで、[外部 EPG の外部サブネット (External Subnets for the External EPG)] のチェックボックスをオンにします。[OK] をクリックします。
- c) [完了 (Finish)] をクリックします。

L3Out OSPF が展開されました。

確認 : Create L3Out Wizard を使用した L3Out の作成例

ウィザードを使用した設定が GUI にどのように表示されるかを確認し、設定が正確であることを確認します。Cisco APIC

ステップ 1 [作業 (Work)] ペインで、[Tenant_name] > [ネットワーキング (Networking)] > [L3Outs] > [EXAMPLE_L3Out1] の順に移動し、次のようにスクロールして詳細を表示します。

GUI のこの場所で、[L3Out の作成 (Create L3Out)] ウィザードの [識別 (Identity)] 画面で設定されている VRF、ドメイン、OSPF パラメータなどの主要な L3Out パラメータを確認します。

The screenshot displays the configuration details for the L3Out 'EXAMPLE_L3Out1'. The configuration includes:

- VRF:** VRF1
- Resolved VRF:** Example/VRF1
- L3 Domain:** EXAMPLE_L3_DOM
- Route Profile for Interleak:** select a value
- Enable BGP/EIGRP/OSPF:** BGP (unchecked), OSPF (checked), EIGRP (unchecked)
- OSPF Area ID:** 0
- OSPF Area Control:** Send redistributed LSAs into NSSA area (checked), Originate summary LSA (checked), Suppress forwarding address in translated LSA (unchecked)
- OSPF Area Type:** NSSA area (selected), Regular area, Stub area
- OSPF Area Cost:** 1

Nodes:

Node ID	Router ID	Loopback Address
topology/pod-1/node-102	2.2.2.2	
topology/pod-1/node-103	3.3.3.3	

Routed Interfaces:

Path	IP Address	Secondary IP Address	MAC Address	MTU (bytes)
Pod-1/Node-102/eth1/11	172.16.1.1/30		00:22:BD:F8:19:FF	inherit
Pod-1/Node-102/eth1/12	172.16.2.1/30		00:22:BD:F8:19:FF	inherit
Pod-1/Node-103/eth1/11	172.16.3.1/30		00:22:BD:F8:19:FF	inherit
Pod-1/Node-103/eth1/12	172.16.4.1/30		00:22:BD:F8:19:FF	inherit

ステップ 2 OSPF がエリア ID やエリア タイプなどの指定されたパラメータで有効になっていることを確認します。

ステップ 3 [論理ノードプロファイル (Logical Node Profiles)]の下に、EXAMPLE_L3Out1_nodeProfile が作成され、ルータ ID で境界リーフ スイッチが指定されます。

ステップ 4 [論理インターフェイスプロファイル (Logical Interface Profile)]の下に、EXAMPLE_L3Out1_interfaceProfile が作成されます。

この例では、インターフェイス ID、IP アドレスなどのインターフェイスパラメータをルーテッドインターフェイスとして確認します。デフォルトの MAC アドレスが自動的に入力されます。OSPF インターフェイスプロファイルは、OSPF インターフェイス レベルのパラメータに対しても作成されます。

レビューが完了しました。

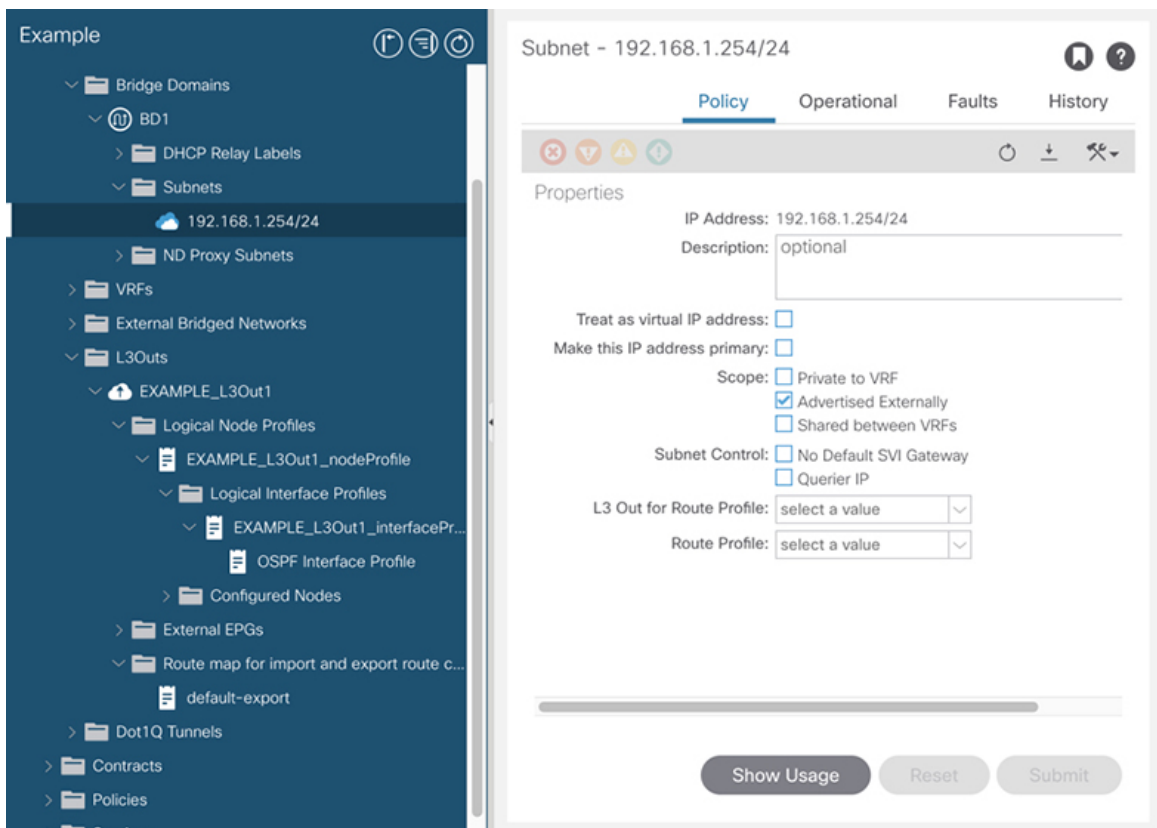
ルートマップによる BD サブネットのアドバタイズの設定

この例では、ルートマップ default-export を IP プレフィックスリストとともに使用して、BD サブネットをアドバタイズします。

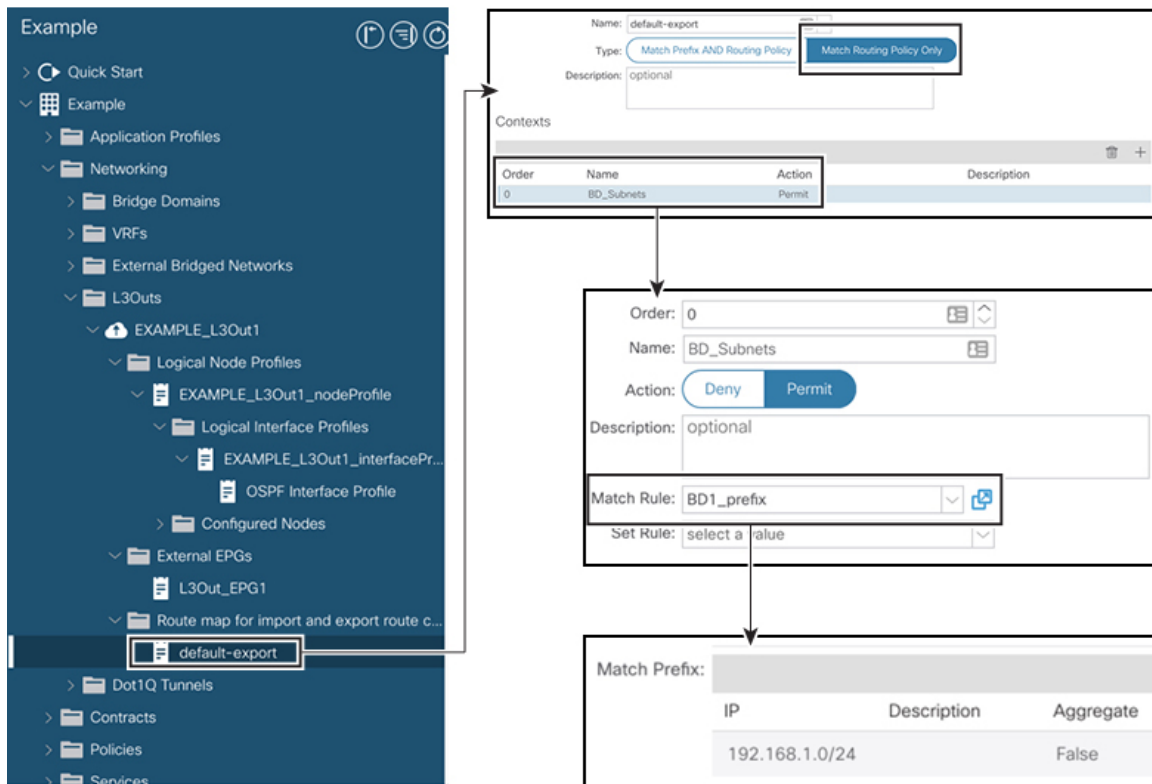


(注) このデフォルトエクスポートルートマップは、特定のものに関連付けられることなく、L3Out (EXAMPLE_L3Out1) に適用されます。

ステップ 1 アドバタイズされる BD サブネットを有効にするには、[テナント (Tenant)][ネットワーク (Networks)][ブリッジドメイン (Bridge Domains)][BD1][サブネット (Subnets)][192.168.1.254/24]に移動し、[外部的にアドバタイズ (Advertised Externally)]の範囲を選択します。> > > >



ステップ 2 L3Out (EXAMPLE_L3Out1) の下にルートマップを作成するには、[ルート制御のインポートおよびエクスポート向けルートマップ (Route map for import and export route control)] に移動します。



ステップ 3 右クリックして [ルート制御のインポートおよびエクスポート向けルートマップの作成 (Create Route map for import and export route control)] を選択します。

ステップ 4 [ルート制御のインポートおよびエクスポート向けルートマップの作成 (Create Route map for import and export route control)] ダイアログボックスの [名前 (Name)] フィールドで、[default-export] を選択します。

ステップ 5 [タイプ (Type)] フィールドで、[ルートポリシーの一致のみ (Match Routing Policy Only)] を選択します。

(注) [ルーティングポリシーのみ照合 (Match Routing Policy Only)] : この [タイプ (Type)] を default-export ルートマップで選択すると、すべてのルートアドバタイズメント設定がこのルートマップによって実行されます。外部 EPG で設定された BD アソシエーションおよびエクスポートルート制御サブネットは適用されません。この L3Out からアドバタイズされるすべてのルートに対して、このルートマップ内のすべての一致ルールを設定する必要があります。

[プレフィックスおよびルーティングポリシーの照合 (Match Prefix and Routing Policy)] : この [タイプ (Type)] を default-export ルートマップで選択すると、ルートアドバタイズメントは、外部 EPG で定義された BD から L3Out へのアソシエーションおよびエクスポートルート制御サブネットに加えて、このルートマップで設定されたすべての一致ルールと照合されます。

ルートプロファイルを使用する場合は、メンテナンスが容易なシンプルな設定のために [ルーティングポリシーのみ照合 (Match Routing Policy Only)] を使用することを推奨します。

ステップ 6 [コンテキスト (Contexts)] 領域で [+] アイコンをクリックして、[ルート制御コンテキストの作成 (Create Route Control Context)] ダイアログボックスを表示し、次のアクションを実行します。

- a) [順序 (Order)]フィールドで、順序を設定します。(0)
この例では、注文は1つだけです。
- b) [名前 (Name)]フィールドに、コンテキスト ポリシーの名前を入力します。(BD_Subnets)
- c) [アクション (Action)]フィールドで[許可 (Permit)]を選択します。
これにより、設定するプレフィックスを許可するルート マップが有効になります。

この例では、IP プレフィックス リスト **[BD1_prefix]** を必要とする一致ルールが必要です。この IP プレフィックス リストは、アドバタイズされた BD サブネットを指します。

ステップ 7 [一致ルール (Match Rule)]フィールドで、次の操作を実行して IP プレフィックス リストを作成します。

- a) [ルートマップの一致ルールの作成 (Create Match Rule for a Route-Map)]を選択します。
- b) [名前 (Name)]フィールドに、名前 **[BD1_prefix]** を入力します。
- c) [プレフィックスの一致 (Match Prefix)]領域で、[+] アイコンをクリックし、BD サブネット (192.168.1.0/24) を入力します。

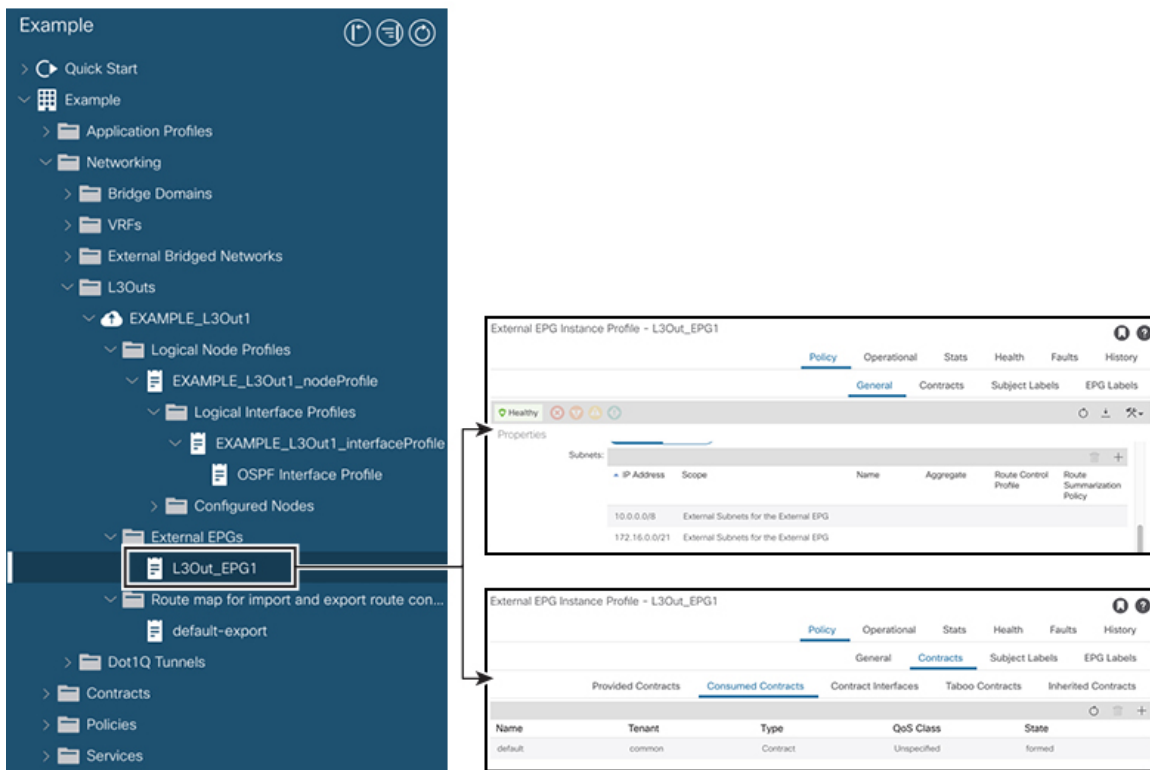
コントラクトの確認

このタスクでは、エンドポイント (192.168.1.1) と外部プレフィックス (10.0.0.0/8、およびオプシオンで 172.16.0.0/21) 間の通信を有効にするためのコントラクトを確認します。この例では、エンドポイントの EPG は EPG1 で、外部プレフィックスの外部 EPG は L3Out_EPG1 です。

必要な設定は、[L3Out の作成 (Create L3Out)] ウィザードにすでに表示されています。

ステップ 1 L3Out で [外部 EPG (External EPGs)] > [L3Out_EPG1] に移動します。

OSPF インターフェイス レベルパラメータの変更 (任意)

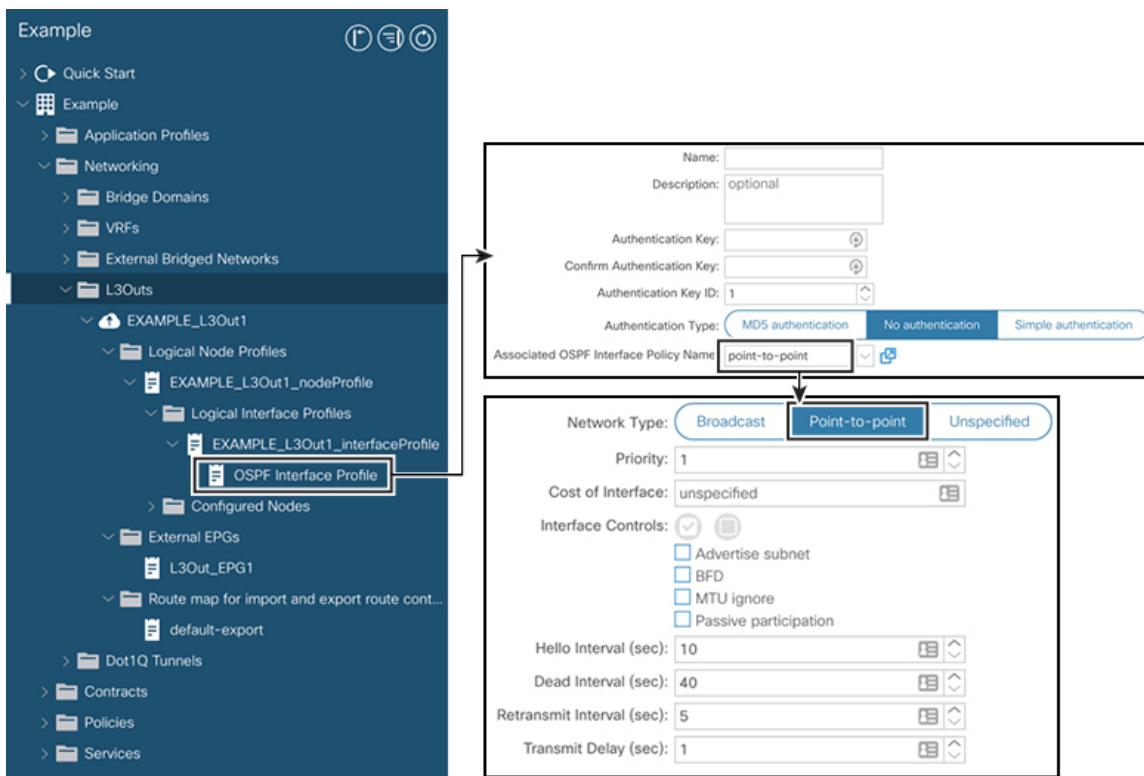


- ステップ 2** [作業 (Work)]ペインの [外部 EPG インスタンス プロファイル (External EPG Instance Profile)]領域の [ポリシー全般 (Policy General)]サブタブで、[プロパティ (Properties)]を確認し、外部 EPG の [外部サブネットワーク (External Subnets)]で 2 つのサブネットワークが表示されることを確認します。 >
- ステップ 3** 次に、[コントラクト (Contracts)]サブタブをクリックし、前に指定した契約が正しく使用されていることを確認します。さらにコントラクトを追加する場合は、GUIでこの場所からアクションを実行できます。
- ステップ 4** [アプリケーションプロファイル (Application Profile)][アプリケーション EPG (Application EPGs)][EPG1] [コントラクト (Contracts)]に移動し、EPG1 が適切なコントラクトを提供していることを確認します。 >>

OSPF インターフェイス レベルパラメータの変更 (任意)

Hello Interval、OSPF ネットワーク タイプなどの OSPF インターフェイス レベルのパラメータを変更する場合は、OSPF インターフェイス プロファイルで設定できます。ノードレベルの OSPF パラメータはすでに設定されています。

- ステップ 1** L3Out で、[論理インターフェイス プロファイル (Logical Interface Profile)]の [EXAMPLE_L3Out1_interfaceProfile] に移動します。 >>



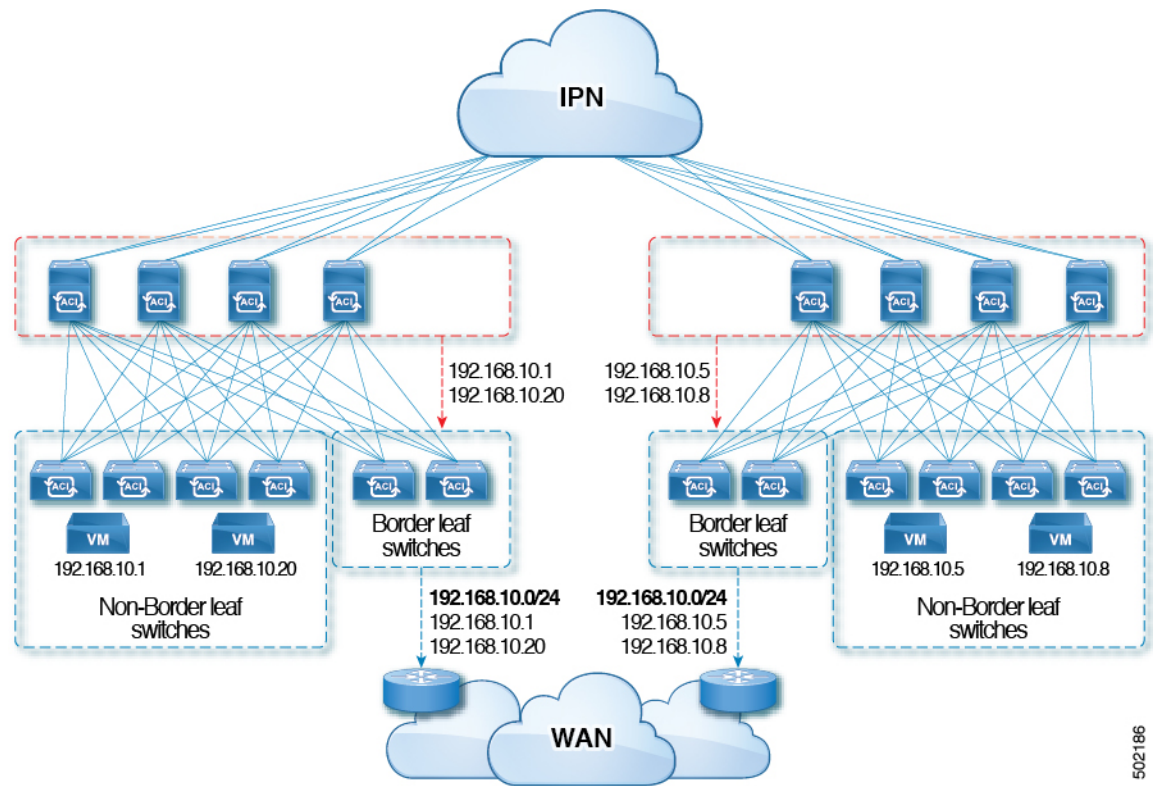
ステップ 2 [ワーク (Work)]ペインの[プロパティ (Properties)]領域で、使用する OSPF インターフェイス ポリシーを選択します。

これにより、OSPF インターフェイス レベルのパラメータが変更されます。

アドバタイズ ホスト ルート

BDでアドバタイズホストルートを有効にすると、個々のホストルート (/32 および /128 のプレフィックス) が境界リーフスイッチ (BL) からアドバタイズされます。BDは、L3out またはホストルートに一致する明示的なプレフィックスリストに関連付けられている必要があります。ホストルートは、ファブリック外のホストルートをアドバタイズするように設定する必要があります。

境界リーフスイッチとサブネットは、個々のエンドポイント (EP) プレフィックスをアドバタイズします。ルート情報は、ホストがローカル POD に接続されている場合のみアドバタイズされます。EP がローカル POD から離れた、または EP が EP データベースから削除された場合 (その EP がリモートリーフに接続されていた場合であっても)、ルートアドバタイズメントはその時に撤回されます。



502186

アドバタイズホストルートの設定ガイドラインと制限事項を次に示します。

- ホストルートがアドバタイズされると、VRF トランジットルートタグが設定されて、ルートがファブリックにアドバタイズされてインストールされないようにします。このループ保護が正常に機能するためには、外部ルータが別の L3Out にアドバタイズする場合、このルートタグを保持する必要があります。
- ブリッジドメインが、内部リーク用に設定された同じサブネットを持つ EPG に関連付けられている場合は、EPG サブネットで「外部アドバタイズ」フラグも有効にする必要があります。
- 第2世代以降のスイッチ（N9K-93108TC-EX など、スイッチモデル名の最後やその後に「EX」、「FX」または「FX2」がつく Cisco Nexus N9K スイッチ）で、アドバタイズホストルート機能がサポートされます。
- ホストルートのアドバタイズメントは、BD から L3out へのアソシエーションと明示的なルートマップ設定の両方をサポートしています。設定するホストルートを個々にまたは範囲を定めて確実に制御しながら設定できるため、明示的なルートマップの設定を使用することをお勧めします。
- SITE-1 の EP/ホストルートは、他の SITE の境界リーフを介してアドバタイズされません。
- EP がエージングするかデータベースから削除されると、ホストルートは境界リーフから撤回されます。

- EP を SITE または POD 全体で移動させる場合、ホスト ルートを最初の SITE/POD から撤回し、新しい POD/SITE でアドバタイズしてください。
- いずれかの BD サブネットの下の特定の BD で学習された EP は、同じ POD 内の境界リーフ上で L3out からアドバタイズされます。
- EP は、境界リーフ経由のローカル POD 内でのみ、ホスト ルートとしてアドバタイズされます。
- ある POD から別の POD にホスト ルートがアドバタイズされることはありません。
- リモート リーフでは、EP がリモート リーフ内でローカルで学習された場合、同じ POD 内のリモート リーフ スイッチに導入された L3out を通じてのみ、それらの EP はアドバタイズされます。
- リモート リーフの EP/ホスト ルートは、主要 POD または別の POD の境界リーフ スイッチを通じてアドバタイズされません。
- 主要 POD の EP/ホスト ルートは、同じ POD または別の POD のリモート リーフ スイッチの L3out を通じてアドバタイズされません。
- BD サブネットでは、[外部にアドバタイズ (Advertise Externally)] オプションが有効になっている必要があります。
- BD が L3out に関連付けられているか、または L3out に明示的なルートマップが設定された一致する BD サブネットがなければなりません。
- L3out では、指定された BD の EPG と外部 EPG の間に契約が必要です。



(注) BD/EPG と外部 EPG の間に契約がない場合、境界リーフに BD サブネットおよびホスト ルートがインストールされません。

- アドバタイズホスト ルートは、共有サービスでサポートされます。例：導入された EPG1/BD1 は VRF 1 で、L3out は別の VRF 2 でアドバタイズできます。EPG と L3out の間に共有契約を提供することで、ホスト ルートは 1 つの VRF-1 から別の VRF-2 にプルされます。
- BD でアドバタイズホスト ルートを有効にした場合、ルートマップを使用して BD サブネット上でカスタム タグを設定することはできません。
- BD でアドバタイズホスト ルートが有効になっており、BD が L3Out に関連付けられている場合、BD サブネットはパブリックとしてマークされます。BD の下に不正な EP が存在する場合、その EP は L3Out でアドバタイズされます。

ルートリフレクタの設定

ACIファブリックのルートリフレクタは、マルチプロトコルBGP (MP-BGP) を使用してファブリック内に外部ルートを配布します。ACIファブリックでルートリフレクタをイネーブルするには、ファブリックの管理者がルートリフレクタになるスパインスイッチを選択して、自律システム (AS) 番号を提供する必要があります。冗長性を確保するために、ポッドあたり少なくとも2つのスパインノードをMP-BGPルートリフレクタとして設定することを推奨します。

ルートリフレクタがACIファブリックで有効になったら、管理者は、レイヤ3 Out (L3Out) というコンポーネントを使用してリーフノードを介して外部ネットワークへの接続を設定できます。L3Outで設定されたリーフノードは、境界リーフと呼ばれます。境界リーフは、L3Outで指定されたルーティングプロトコルを介して、接続された外部デバイスとルートを交換します。L3Out経由でスタティックルートを設定することもできます。

L3Outとスパインルートリフレクタの両方が展開されると、境界リーフノードはL3Outを介して外部ルートを学習し、それらの外部ルートはスパインMP-BGPルートリフレクタを介してファブリック内のすべてのリーフノードに配布されます。

リーフでサポートされるルートの最大数については、ご使用のリリースの『Cisco APICの検証済みスケーラビリティガイド』を参照してください。

GUIを使用したMP-BGPルートリフレクタの設定

-
- ステップ 1** メニューバーで、[System] > [System Settings] の順に選択します。
- ステップ 2** [ナビゲーション (Navigation)] ペインで、[BGPルートリフレクタ (BGP Route Reflector)] を右クリックして、[ルートリフレクタノードの作成 (Create Route Reflector Node)] をクリックします。
- ステップ 3** [ルートリフレクタノードの作成 (Create Route Reflector Node)] ダイアログボックスで、[スパインノード (Spine Node)] ドロップダウンリストから、適切なスパインノードを選択します。Submit をクリックします。
- (注) 必要に応じてスパインノードを追加するには、上記の手順を繰り返してください。
- スパインスイッチがルートリフレクタノードとしてマークされます。
- ステップ 4** **BGP Route Reflector** プロパティエリアの **Autonomous System Number** フィールドで、適切な番号を選択します。Submit をクリックします。
- (注) 自律システム番号は、Border Gateway Protocol (BGP) がルータに設定されている場合は、リーフが接続されたルータ設定に一致する必要があります。スタティックまたは Open Shortest Path First (OSPF) を使用して学習されたルートを使用している場合は、自律システム番号値を任意の有効な値にできます。
- ステップ 5** メニューバーで、[ファブリック (Fabric)] > [ファブリックポリシー (Fabric Policies)] > [ポッド (Pods)] > [ポリシーグループ (Policy Groups)] をクリックします。

- ステップ 6** [ナビゲーション (Navigation)] ペインで、[ポリシー グループ (Policy Groups)] を展開して右クリックし、[POD ポリシー グループの作成 (Create POD Policy Group)] をクリックします。
- ステップ 7** [ポッド ポリシー グループの作成 (Create Pod Policy Group)] ダイアログ ボックスで、[名前 (Name)] フィールドに、ポッド ポリシー グループの名前を入力します。
- ステップ 8** [BGP Route Reflector Policy] ドロップダウン リストで、適切なポリシー (デフォルト) を選択します。 [Submit] をクリックします。`
BGP ルート リフレクタのポリシーは、ルート リフレクタのポッド ポリシー グループに関連付けられ、BGP プロセスはリーフ スイッチでイネーブルになります。
- ステップ 9** メニュー バーで、[ファブリック (Fabric)] > [ファブリック ポリシー (Fabric Policies)] > [プロファイル (Profiles)] > [ポッド プロファイル デフォルト (Pod Profile default)] > [デフォルト (default)] を選択します。
- ステップ 10** [Work] ペインで、[Fabric Policy Group] ドロップダウン リストから、前に作成されたポッド ポリシーを選択します。 [Submit] をクリックします。`
ポッド ポリシー グループが、ファブリック ポリシー グループに適用されました。

MP-BGP ルート リフレクタ 設定の確認

ステップ 1 次の操作を実行して、設定を確認します。

- セキュア シェル (SSH) を使用して、必要に応じて各リーフ スイッチへの管理者としてログインします。
- `show processes | grep bgp` コマンドを入力して、状態が S であることを確認します。
状態が NR (実行していない) である場合は、設定が正常に行われませんでした。

ステップ 2 次の操作を実行して、自律システム番号がスパイン スイッチで設定されていることを確認します。

- SSH を使用して、必要に応じて各スパイン スイッチへの管理者としてログインします。
- シェル ウィンドウから次のコマンドを実行します。

例 :

```
cd /mit/sys/bgp/inst
```

例 :

```
grep asn summary
```

設定した自律システム番号が表示される必要があります。自律システム番号の値が 0 と表示される場合は、設定が正常に行われませんでした。



第 18 章

L3Out のノードとインターフェイス

- [L3Out のインターフェイスの変更 \(273 ページ\)](#)
- [L3Out の SVI のカスタマイズ \(275 ページ\)](#)
- [Cisco フローディング L3Out について \(285 ページ\)](#)

L3Out のインターフェイスの変更

GUI を使用した L3Out のインターフェイスの変更

この手順では、L3Out インターフェイスを変更します。



- (注) フィールドに入力する手順は、必ずしも GUI に表示される順序と同じ順序でリストされているわけではありません。

始める前に

- Cisco ACI ファブリックが設置され、Cisco APIC がオンラインになっており、Cisco APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる Cisco APIC ファブリック管理者アカウントが使用可能であること。
- ターゲットリーフスイッチが Cisco ACI ファブリックに登録され、使用可能であること。
- ポートチャネルは、L3Out インターフェイスにポートチャネルが使用される場合に設定されます。

ステップ 1 メニューバーで、[テナント (Tenants)] > [すべてのテナント (ALL Tenants)] の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

- ステップ 3** ナビゲーションペインで、[tenant_name]>[ネットワーク (Networking)]>[L3Outs]>[L3Outs]>[論理ノード プロファイル (Logical Node Profiles)]> node_profile > [論理インターフェイス プロファイル (Logical Interface Profiles)] の順に移動し、変更したいプロファイルを選択します。
- ステップ 4** [インターフェイスタイプ] タブを選択：[ルーテッドサブインターフェイス (Routed Sub-Interfaces)]、[ルーテッドインターフェイス (Routed Interfaces)]、[SVI]、または [浮動 SVI (Floating SVI)] を選択します。
- ステップ 5** 既存のインターフェイスをダブルクリックして変更するか、[作成 (Create)] (+) ボタンをクリックして新しいインターフェイスを論理インターフェイス プロファイルに追加します。
- ステップ 6** 浮動 SVI 以外のインターフェイス タイプの場合は、次のサブステップを実行します。m
- a) [パス タイプ (Path Type)] フィールドで新しいインターフェイスを追加し、適切なパス タイプを選択します。

ルーテッドサブインターフェイスまたはルーテッドインターフェイス タイプの場合、ポートまたはダイレクトポートチャネルを選択します。SVI インターフェイス タイプの場合、ポート、ダイレクトポートチャネル、または仮想ポートチャネルを選択します。
 - b) [ノード (Node)] ドロップダウンリストから、ノードを選択します。

(注) これは、非ポートチャネルパスタイプにのみ適用されます。[パスタイプ (Path Type)] を [ポート (Port)] として選択した場合は、この手順を実行します。それ以外の場合は、次のステップに進みます。
 - c) [パス (Path)] ドロップダウンリストからインターフェイス ID またはポートチャネル名を選択します。

インターフェイス ID の例は eth 1/1 です。ポートチャネル名は、各直接または仮想ポートチャネルのインターフェイスポリシーグループ名です。
- ステップ 7** 浮動 SVI インターフェイス タイプの場合、[アンカーノード] ドロップダウンリストでノードを選択します。
- ステップ 8** (任意) [説明 (Description)] フィールドに、L3Out インターフェイスの説明を入力します。
- ステップ 9** ルーテッドサブインターフェイス、SVI および浮動 SVI インターフェイスの場合、[[カプセル化 (Encap)] ドロップダウンリストで、[VLAN] を選択し、このエントリの整数値を入力します。
- ステップ 10** SVI および浮動 SVI インターフェイス タイプの場合は、次のサブステップを実行します。
- a) [カプセル化範囲 (Encap Scope)] ボタンで、レイヤ 3 Outside プロファイルに使用されるカプセル化の範囲を選択します。
 - **VRF** : 特定の VLAN カプセル化の同じ VRF インスタンス内のすべてのレイヤ 3 外部で同じトランジット VLAN を使用します。これはグローバル値です。
 - **Local** : レイヤ 3 外部ごとに一意のトランジット VLAN を使用します。
 - b) [自動状態 (Auto State)] ボタンについては、この機能を有効にするか無効にするかを選択します。
 - **disabled** : インターフェイスが対応する VLAN で動作していない場合、SVI がアクティブであることを意味します。

- **enabled** : VLAN インターフェイスが VLAN で複数のポートを有する場合、SVI は浮動 SVI は VLAN のすべてのポートがダウンするとダウン状態になります。

c) [モード] ボタンで、VLAN タギング モードを選択します。

- ステップ 11 **IPv4 Primary / IPv6 Preferred Address** フィールドに、レイヤ 3 外側プロファイルにアタッチされているパスのプライマリ IP アドレスを入力します。
- ステップ 12 **[IPv4 セカンダリ/IPv6 追加アドレス]** テーブルで、+ をクリックして、レイヤ 3 外側プロファイルにアタッチされているパスのセカンダリ IP アドレスを入力します。
- ステップ 13 (任意) **Link-local Address** フィールドに、IPv6 リンクローカルアドレスを入力します。これは、システムによって生成された IPv6 リンクローカルアドレスをオーバーライドします。
- ステップ 14 **[MAC アドレス]** フィールドに、レイヤ 3 外側プロファイルにアタッチされているパスの MAC アドレスを入力します。
- ステップ 15 **[MTU (バイト)]** フィールドで、外部ネットワークの最大転送単位を設定します。指定できる範囲は 576 ~ 9216 です。値を継承するには、*inherit* フィールドに入力します。
- ステップ 16 **[ターゲット DSCP]** ドロップダウンリストで、レイヤ 3 アウトサイドプロファイルに接続されているパスのターゲット Differentiated Services Code Point (DSCP) を選択します。
- ステップ 17 [送信 (Submit)] をクリックします。

L3Out の SVI のカスタマイズ

SVI 外部カプセル化の範囲

SVI 外部カプセル化の範囲について

レイヤ 3 アウト設定のコンテキストでは、スイッチ仮想インターフェイス (SVI) は ACI リーフスイッチとルータ間に接続性を提供するように設定されます。

デフォルトで単一のレイヤ 3 アウトが SVI インターフェイスで設定されている場合、VLAN のカプセル化はファブリック内の複数のノードに範囲が及びます。これは、図で示されるように SVI インターフェイスが同じ外部カプセル化 (SVI) を使用する限り、レイヤ 3 アウト SVI が展開されているファブリックで、ACI ファブリックがすべてのノード上に同じブリッジドメイン (VXLAN VN) を設定するため発生します。

ただし、異なるレイヤ 3 アウトが展開されている場合、同じ外部カプセル化 (SVI) を使用している場合でも ACI ファブリックは異なるブリッジドメインを使用します。

図 33: ローカル範囲のカプセル化と 1 個のレイヤ 3 アウト

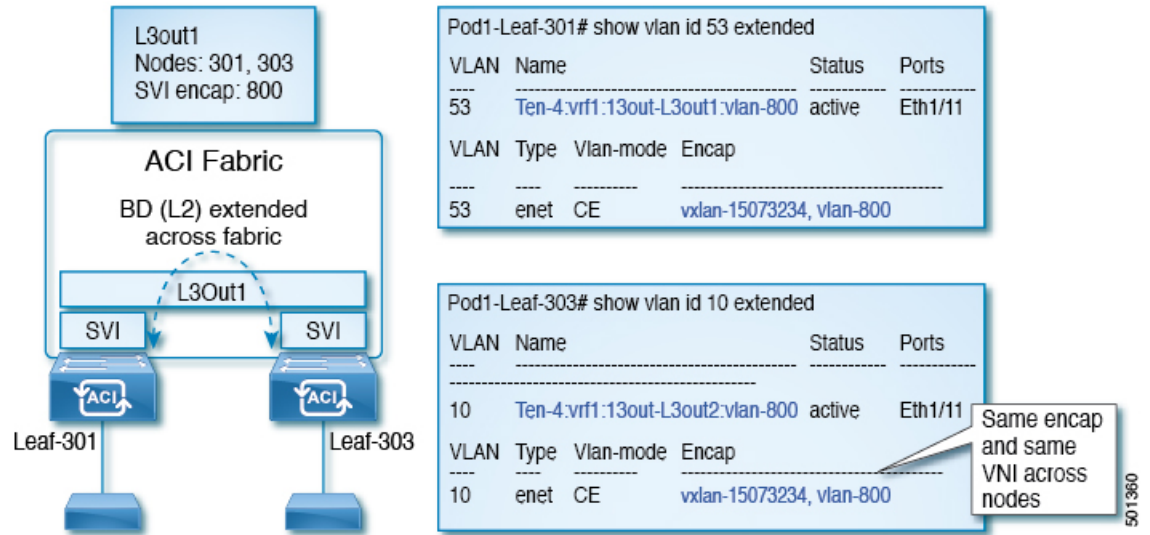
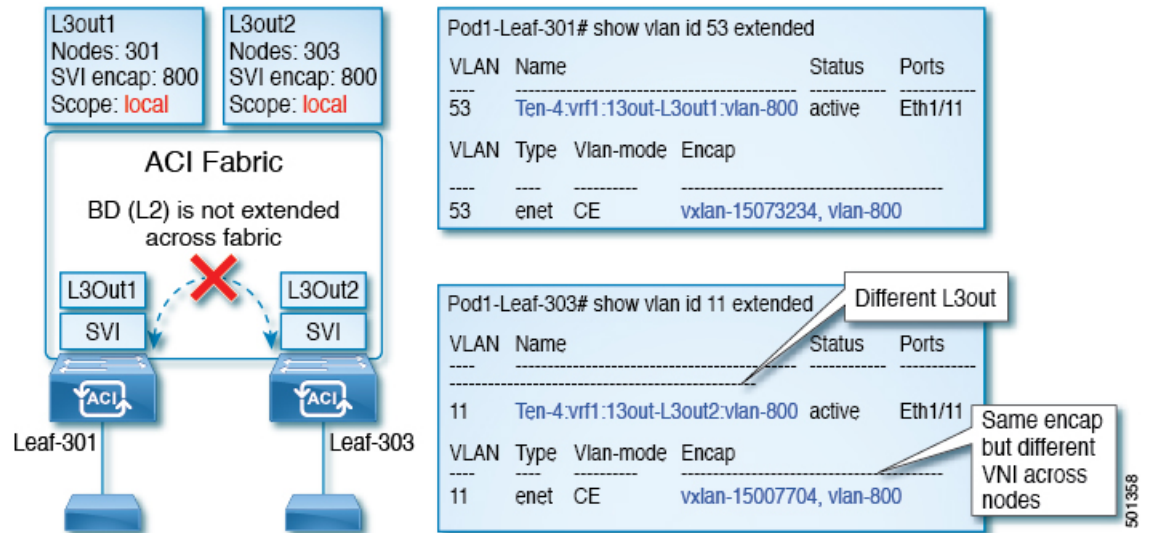


図 34: ローカル範囲のカプセル化と 2 個のレイヤ 3 アウト

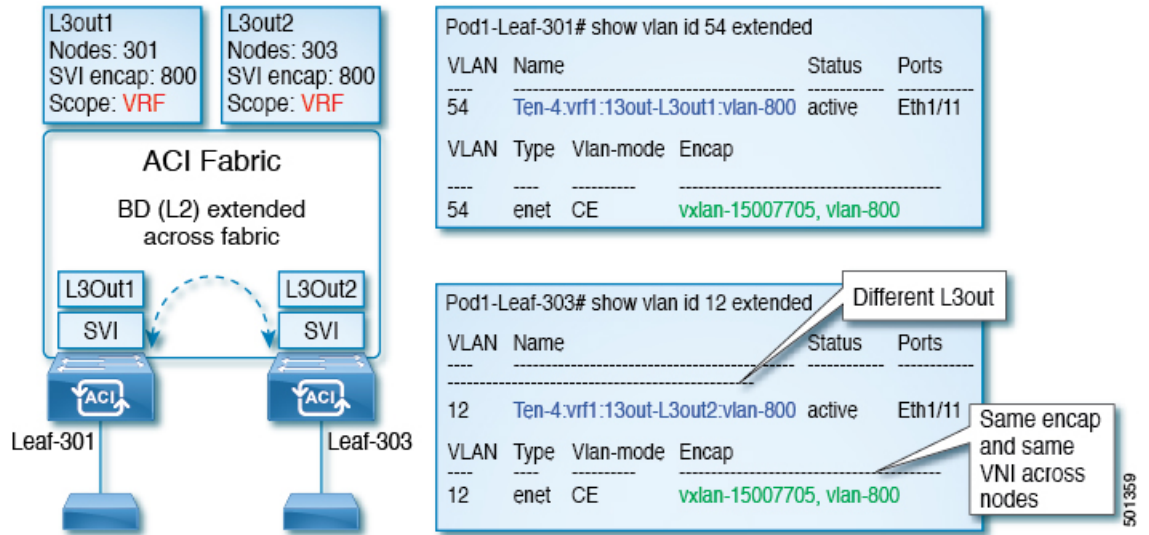


Cisco APIC リリース 2.3 以降、同じ外部カプセル化 (SVI) を使用して、2 個以上のレイヤ 3 アウトを展開する場合の動作を選択できるようになりました。

カプセル化の範囲は、ローカルまたは VRF として設定できます。

- ローカル範囲 (デフォルト) : 例の動作が「ローカル範囲のカプセル化および 2 個のレイヤ 3 アウト」というタイトルの図に表示されます。
- VRF 範囲 : ACI ファブリックが、同じ外部カプセル化 (SVI) が展開されているすべてのノードとレイヤ 3 アウト上で同じブリッジドメイン (VXLAN VNI) を設定します。「VRF 範囲のカプセル化および 2 個のレイヤ 3 アウト」というタイトルの図の例を参照してください。

図 35: VRF 範囲のカプセル化および 2 個のレイヤ 3 アウト



カプセル化スコープ構文

レイヤ 3 Out プロファイルで使用されるカプセル化の範囲を設定するためのオプションは次のとおりです。

- **Ctx**]: 特定の VLAN のカプセル化の同じ VRF に、すべてのレイヤ 3 が記録されるで同じ外部 SVI。これはグローバル値です。
- **ローカル** : レイヤ 3 Out ごとの一意の外部 SVI。これはデフォルト値です。

CLI、API、および GUI 構文間のマッピングは次のとおりです。

表 8: カプセル化スコープ構文

CLI	API	GUI
l3out	local	local
vrf	ctx	VRF



(注) カプセル化の範囲を設定する CLI コマンドでは、名前付きのレイヤ 3 アウト設定、VRF が設定されている場合にのみサポートされます。

SVI 外部カプセル化の範囲のガイドライン

SVI 外部カプセル化の範囲を使用する際には、次のガイドラインに従ってください:

- 同じノード上にレイヤ 3 Out を設定するためには、両方のレイヤ 3 Out の OSPF エリアが異なっている必要があります。

- 同じノード上にレイヤ 3 Out を設定するためには、両方のレイヤ 3 Out の BGP ピア設定が異なる必要があります。

GUI を使用して SVI 外部カプセル化の範囲の設定

始める前に

- テナントと VRF が設定されています。
- L3Out が設定されていて、L3Out で論理ノードプロファイルが設定されています。

ステップ 1 メニューバーで、> **Tenants** > *Tenant_name* をクリックします。

ステップ 2 [ナビゲーション (Navigation)] ペインで、[ネットワークング (Networking)] [L3Outs] [L3Out_name] [論理ノードプロファイル (Logical Node Profiles)] [LogicalNodeProfile_name] [論理インターフェイスプロファイル (Logical Interface Profiles)] をクリックします。> > > >

ステップ 3 [ナビゲーション (Navigation)] ウィンドウで、[論理インターフェイス プロファイル (Logical Interface Profile)] を右クリックし、[インターフェイス プロファイルの作成 (Create Interface Profile)] をクリックします。

ステップ 4 [Create Interface Profile] ダイアログボックスで、次の操作を実行します。

- Step 1 Identity** 画面の **Name** フィールドで、インターフェイス プロファイルの名前を入力します。
- 残りのフィールドに、適切なオプションを選択し] をクリックして **次**。
- ステップ 2 プロトコル プロファイル** 画面、目的のプロトコルを選択するには、プロファイルの詳細、および] をクリックして **次**。
- ステップ 3 インターフェイス** 画面で、をクリックして、**SVI**] タブをクリックして、+ を開くにアイコン、**選択 SVI** ダイアログボックス。
- インターフェイスの指定**] 領域で、目的、さまざまなフィールド値を選択します。
- Encap スコープ** フィールドで、目的のカプセル化範囲の値を選択します。[OK] をクリックします。
デフォルト値は **Local** です。

SVI 外部のカプセル化の範囲は、指定されたインターフェイスで設定されます。

SVI での複数の L3Out のカプセル化のサポート

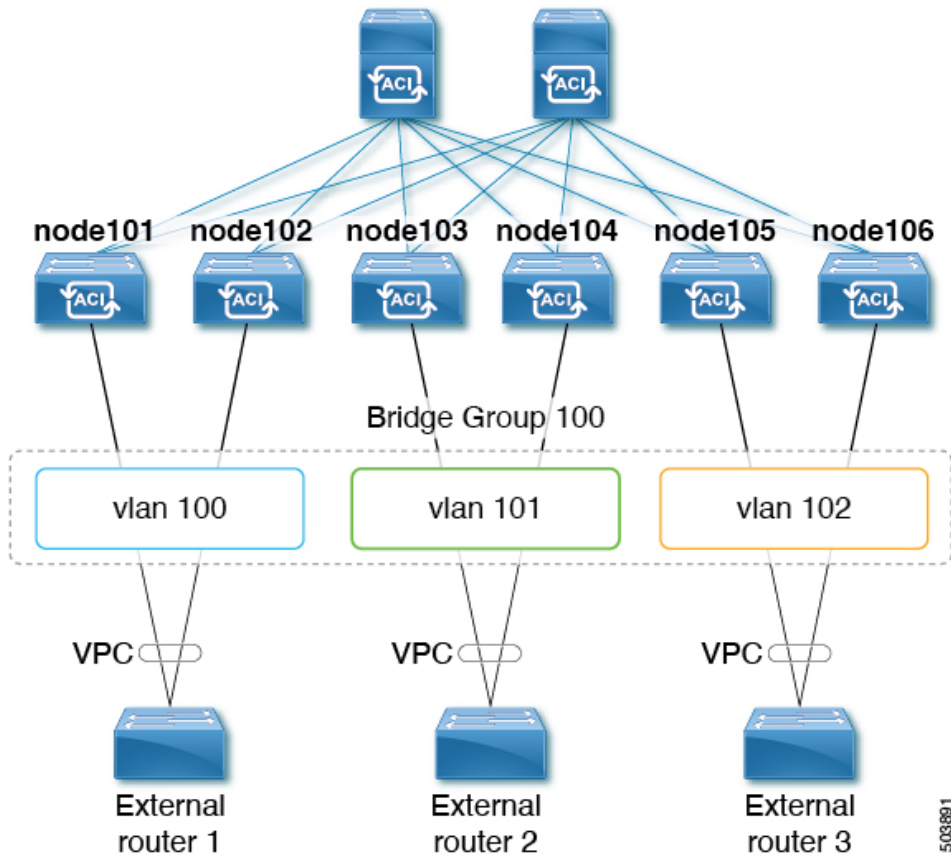
リリース 5.2(3) より前では、SVI で設定された L3Out は、外部ブリッジドメインごとに 1 つの VLAN カプセル化に制限されます。

リリース 5.2(3) 以降、さまざまな外部 VLAN カプセル化を使用するためのサポートが利用可能になりました。異なる外部カプセル化インスタンスはすべて、単一のレイヤ 2 ドメインの一部として扱われます。それぞれが異なるカプセル化を使用する複数の SVI で設定された L3Out は、単一の外部ブリッジドメインにグループ化できます。この単一の外部ブリッジドメインは、単一の VXLAN ネットワーク識別子 (VNID) を使用し、単一のブロードキャストドメイン

になります。異なるカプセル化で構成された SVI は、同じサブネット内の IP アドレスを使用できます。

複数の SVI を異なるアクセスのカプセル化でグループ化する

次の図は、複数の SVI が異なるアクセス カプセル化でグループ化されている設定を示しています。



この使用ケースでは：

- 次のリーフ スイッチは VPC ペアです。
 - node101 および node102
 - node103 および node104
 - node105 および node106

複数の SVI をレイヤ 2 ブリッジ グループにグループ化する上記の使用例を設定します。

1. VPC ペアごとに 3 つの通常の SVI を作成します。
 - リーフ スイッチ node101 および node102 に通常の SVI **svi-100** を作成します。
 - リーフ スイッチ node103 および node104 に通常の SVI **svi-101** を作成します。

- リーフ スイッチ **node105** および **node106** に通常の SVI **svi-102** を作成します。
2. リーフ スイッチをアクセス カプセル化に構成します。
 - アクセス カプセル化 **vlan100** を使用してリーフ スイッチ **node101** および **node102** を設定します。
 - アクセス カプセル化 **vlan101** でリーフ スイッチ **node103** および **node104** を設定します。
 - アクセス カプセル化 **vlan102** を使用してリーフ スイッチ **node105** および **node106** を設定します。
 3. 通常の SVI **svi-100**、**svi-101**、および **svi-102** をグループ化して、単一のレイヤ 2 ブロードキャスト ドメインの一部として動作させます。
 1. ブリッジドメイン プロファイルを作成します。
ブリッジドメイン プロファイルは、新しい MO *l3extBdProfile* で表されます。
 2. ブリッジドメイン プロファイルの一意の名前文字列を指定します。
 3. 同じブリッジドメイン プロファイルにグループ化する必要がある通常および SVI のそれぞれを関連付けます。
この関連付けには、*l3extBdProfileCont* と *l3extRsBdProfile* の 2 つの新しい MO を使用できます。

注意事項と制約事項

- レイヤ 2 ループは、外部デバイス/ハイパーバイザによってブロックされます。ループを防止するためにスパンニングツリープロトコルに依存する外部スイッチでこの機能を使用すると、ループが発生する可能性があります。
- SVI は、外部ブリッジドメイン プロファイルの設定後に削除され、再度追加されます。
- 外部ブリッジドメイン プロファイルは L3Out スコープです。ノードでは、同じ外部ブリッジドメイン プロファイルに 2 つの異なるアクセス カプセル化マッピングを設定することはできません。
- ブリッジドメインのグループ化は、カプセル化スコープ **ctx** (APIC GUI の **VRF** オプション) ではサポートされていません。
- 異なる回線カプセル化を持つグループ化された SVI は、共通ノードを共有できません。
- リリース 5.2(3) から SVI による L3Out の複数のカプセル化がサポートされていない以前のリリースにダウングレードする場合、複数のカプセル化や外部ブリッジドメイン プロファイルで設定された L3Out で次のアクションが実行されます。
 - 複数のカプセル化サポートに使用される新しいアロケータ (*l3extBdProfileEncapAllocator*) が削除されます。

- すべての外部ブリッジドメインプロファイル (新しい *l3extBdProfile* MO) が削除されます。
- すべての新しい *l3extBdProfileCont* MO が削除されます。
- すべての新しい *l3extRsBdProfile* MO が削除されます。

GUI を使用して SVI で複数の L3Out のカプセル化を設定する

ステップ 1 通常の SVI を作成し、リーフスイッチをカプセル化にアクセスして構成します。

これらの手順については、[GUI を使用して SVI 外部カプセル化の範囲の設定 \(278 ページ\)](#) を参照してください。

ステップ 2 SVI グループ化に使用される外部ブリッジグループプロファイルを作成します。

- a) [テナント (Tenants)] > [tenant-name] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [外部ブリッジグループプロファイル (External Bridge Group Profiles)] に移動します。
設定済みの外部ブリッジグループプロファイルを示すページが表示されます。
- b) [外部ブリッジグループプロファイル (External Bridge Group Profiles)] を右クリックし、[外部ブリッジグループプロファイルの作成 (Create External Bridge Group Profile)] を選択します。
[外部ブリッジグループプロファイルの作成 (Create External Bridge Group Profile)] ページが表示されます。
- c) 外部ブリッジグループプロファイルの名前を入力し、[送信 (Submit)] をクリックします。
すでに設定されている外部ブリッジグループプロファイルを示すページが、新しい外部ブリッジグループプロファイルで更新されます。

ステップ 3 通常の SVI をブリッジドメインプロファイルに関連付けます。

- a) [テナント (Tenants)] > [tenant-name] > [ネットワーク (Networking)] > [L3Outs] > [L3Out-name] > [論理ノードプロファイル (Logical Node Profile)] > [log-node-profile-name] > [論理インターフェイスプロファイル (Logical Interface Profile)] > [log-int-profile-name] に移動します。
この論理インターフェイスプロファイルの [全般 (General)] ページが表示されます。
- b) [SVI] タブをクリックします。
設定済みのスイッチ仮想インターフェイスを示すページが表示されます。
- c) 外部ブリッジドメインプロファイルに関連付けるスイッチ仮想インターフェイスをダブルクリックします。
このスイッチ仮想インターフェイスの一般情報が表示されます。
- d) [外部ブリッジグループプロファイル (External Bridge Group Profile)] フィールドで、このスイッチ仮想インターフェイスに関連付ける外部ブリッジドメインプロファイルを選択します。
- e) [送信 (Submit)] をクリックします。

CLI を使用して SVI で複数の L3Out のカプセル化を設定する

CLI を使用して SVI で複数の L3Out のカプセル化を設定する

ステップ 1 通常の SVI を作成し、リーフ スイッチをカプセル化にアクセスして構成します。

これらの手順については、[NX-OS スタイル CLI を使用して、SVI インターフェイスのカプセル化スコープの設定 \(500 ページ\)](#) を参照してください。

ステップ 2 CLI を使用して APIC にログインし、コンフィギュレーション モードとテナント コンフィギュレーション モードを開始します。

```
apic1#
apic1# configuration
apic1(config)# tenant <tenant-name>
apic1(config-tenant)#
```

ステップ 3 次のコマンドを入力して、SVI グループ化に使用する外部ブリッジ プロファイルを作成します。

```
apic1(config-tenant)# external-bridge-profile <bridge-profile-name>
apic1(config-tenant-external-bridge-profile)# ?
```

ステップ 4 次のコマンドを入力して、通常の SVI をブリッジ ドメイン プロファイルに関連付けます。

```
apic1(config)# leaf <leaf-ID>
apic1(config-leaf)# interface vlan <vlan-num>
apic1(config-leaf-if)# vrf member tenant <tenant-name> vrf <VRF-name>
apic1(config-leaf-if)# ip address <IP-address>
apic1(config-leaf-if)# external-bridge-profile <bridge-profile-name>
```

REST API を使用した複数の SVI 付き L3Out のカプセル化の設定

ステップ 1 通常の SVI を作成し、リーフ スイッチをカプセル化にアクセスして構成します。

これらの手順については、[REST API を使用して、SVI インターフェイスのカプセル化スコープの設定 \(582 ページ\)](#) を参照してください。

ステップ 2 次の例のような投稿を入力して、SVI グループ化に使用する外部ブリッジ プロファイルを作成します。

```
<fvTenant name="t1" dn="uni/tn-t1" >
  <l3extBdProfile name="bd100" status=""/>
</fvTenant>
```

ステップ 3 次の例のように投稿を入力して、通常の SVI をブリッジ ドメイン プロファイルに関連付けます。

```
<fvTenant name="t1">
  <l3extOut name="l1">
    <l3extLNodeP name="n1">
      <l3extLIfP name="i1">
        <l3extRsPathL3OutAtt encap="vlan-108"
          tDn="topology/pod-1/paths-108/pathep-[eth1/10]"
```



```

        ifInstT="ext-svi">
        <l3extBdProfileCont>
            <l3extRsBdProfile tDn="uni/tn-t1/bdprofile-bd100" status=""/>
        </l3extBdProfileCont>
        </l3extRsPathL3OutAtt>
    </l3extLIfP>
</l3extLNodeP>
</l3extOut>
</fvTenant>

```

ステップ 4 フローティング ノードの個別のカプセル化を指定するには、次の例のような投稿を入力します。

```

<fvTenant name="t1">
  <l3extOut name="l1">
    <l3extLNodeP name="n1">
      <l3extLIfP name="i1">
        <l3extVirtualLIfP addr="10.1.0.1/24"
          encaps="vlan-100"
          nodeDn="topology/pod-1/node-101"
          ifInstT="ext-svi">
          <l3extRsDynPathAtt floatingAddr="10.1.0.100/24"
            encaps="vlan-104"
            tDn="uni/phys-phyDom"/>
        </l3extVirtualLIfP>
      </l3extLIfP>
    </l3extOut>
  </fvTenant>

```

SVI 自動状態

SVI 自動状態について



- (注) この機能は、APIC リリース 2.2(3x) リリースおよび APIC リリース 3.1 (1) で使用できません。APIC リリース 3.0(x) ではサポートされていません。

スイッチ仮想インターフェイス (SVI) は、デバイスの VLAN のブリッジング機能とルーティング機能間の論理インターフェイスを表します。SVI は、物理ポート、直接ポートチャネル、仮想ポートチャネルのメンバーを有することができます。SVI 論理インターフェイスは VLAN に関連付けられ、VLAN ポート メンバーシップを有します。

SVI の状態はメンバーに依存しません。Cisco APIC の SVI のデフォルトの自動状態動作は、自動状態の値が無効になっているときに最新の状態になっていることを意味します。これは、インターフェイスが対応する VLAN で動作していない場合、SVI がアクティブであることを意味します。

SVI 自動状態の値を有効に変更する場合、関連する VLAN のポート メンバーに依存します。VLAN インターフェイスが VLAN で複数のポートを有する場合、SVI は VLAN のすべてのポートがダウンするとダウン状態になります。

表 9: SVI 自動状態

SVI 自動状態	SVI 状態の説明
ディセーブル	インターフェイスが対応する VLAN で動作していない場合、SVI がアップ状態であることを意味します。 無効がデフォルトの SVI 自動状態の値です。
イネーブル	SVI は、関連付けられている VLAN のポートメンバによって異なります。VLAN インターフェイスに複数のポートを含む場合、SVI は VLAN のすべてのポートがダウンするとダウン状態になります。

SVI 自動状態の動作のガイドラインと制限事項

次のガイドラインをお読みください。

- SVI の自動状態の動作を有効化または無効化にすると、SVI あたりの自動状態の動作を設定します。これらはグローバル コマンドではありません。

GUI を使用した SVI 自動状態の設定

始める前に

- テナントと VRF が設定されています。
- L3Out が設定されており、L3Out の論理ノードプロファイルと論理インターフェイスプロファイルが設定されています。

ステップ 1 メニューバーで、> **Tenants** > **Tenant_name** をクリックします。

ステップ 2 [ナビゲーション (Navigation)] ペインで、[ネットワークング (Networking)] [L3Outs] [L3Out_name] [論理ノードプロファイル Logical Node Profiles] [LogicalNodeProfile_name] [論理インターフェイスプロファイル (Logical Interface Profiles)] をクリックします。> > > > >

ステップ 3 **Navigation** ウィンドウで、**Logical Interface Profile** を展開し、適切な論理インターフェイスプロファイルをクリックします。

ステップ 4 [作業 (Work)] ペインで、[+] 記号をクリックして [SVI] ダイアログボックスを表示します。

ステップ 5 付加的な SVI を追加するには、**SVI** ダイアログボックスで、以下の手順を実行します:

- Path Type** フィールドで、適切なパスタイプを選択します。
- Path** フィールドで、ドロップダウンリストから適切な物理インターフェイスを選択します。
- Encap** フィールドで、適切な値を選択します。
- Auto State** フィールド (**Work** ウィンドウ) で SVI を選択し、自動状態を表示または変更します。

デフォルト値は **Disabled** です。

- (注) 既存 SVI の自動状態の値を確認または変更するには、適切な SVI を選択して、値を確認または変更します。

Cisco フローティング L3Out について

Cisco Application Policy Infrastructure Controller (APIC) リリース 4.2(1) 以降、仮想環境で複数のレイヤ 3 外部ネットワーク接続 (L3Out) 論理インターフェイスパスを指定する必要がなくなりました。

このフローティング L3Out 機能を使用すると、論理インターフェイスを指定せずに L3Out を設定できます。この機能により、仮想マシンがホスト間を移動する際に、ルーティングを維持するために複数の L3Out 論理インターフェイスを設定する必要がなくなります。フローティング L3Out は、VMware vSphere 分散スイッチ (VDS) でサポートされています。

Cisco APIC リリース 5.0(1) 以降、物理ドメインがサポートされています。

詳細については、「フローティング L3Out を使用して外部ネットワーク接続を簡素化する」のナレッジベース記事を参照してください。

<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/Cisco-ACI-Floating-L3Out.html>



第 19 章

ルーティング プロトコルのサポート

この章は、次の内容で構成されています。

- [ルーティング プロトコルのサポートについて \(287 ページ\)](#)
- [BGP 外部ルーテッド ネットワークと BFD のサポート \(287 ページ\)](#)
- [OSPF 外部ルーテッド ネットワーク \(327 ページ\)](#)
- [EIGRP 外部ルーテッド ネットワーク \(330 ページ\)](#)

ルーティング プロトコルのサポートについて

Cisco ACI ファブリック内のルーティングは、BGP (BFD サポート) および OSPF または EIGRP ルーティング プロトコルを使用して実装されます。

IP 送信元ルーティングは ACI ファブリックではサポートされません。

BGP 外部ルーテッド ネットワークと BFD のサポート

ここでは、BFD をサポートする BGP 外部ルーテッド ネットワークの詳細について説明します。

BGP レイヤ 3 外部ネットワーク接続設定のガイドライン

BGP 外部ルーテッド ネットワークを設定するときは、以下のガイドラインに従ってください。

- BGP 直接ルート エクスポートの動作は、リリース 3.2(1) 以降に変更されました。この場合 ACI は、エクスポート ルート マップ節を照合するときに、発信元ルート タイプ (スタティック、ダイレクトなど) を評価しません。その結果、アウトバウンド ネイバー ルート マップに常に含まれる「match direct」 deny 節は、直接ルートと一致なくなり、ユーザ定義のルート マップ節が一致するかどうかに基づいて直接ルートがアドバタイズされるようになりました。

したがって、直接ルートはルート マップを介して明示的にアドバタイズする必要があります。そうしないと、アドバタイズされている直接ルートが暗黙的に拒否されます。

- L3Out の BGP ピア接続プロファイルの [BGP 制御 (BGP Controls)] フィールドの [AS オーバーライド (AS override)] オプションは、リリース 3.1(2) で導入されました。これにより、ACI は AS_PATH 内のリモート AS を ACI BGP AS で上書きできます。ACI では、通常、eBGP L3Out から同じ AS 番号を持つ別の eBGP L3Out への中継ルーティングを実行するときに使用されます。

ただし、eBGP ネイバーの AS 番号が異なる場合に [AS オーバーライド (AS override)] オプションを有効にすると、問題が発生します。この状況では、ピアに反映するときに AS_PATH から peer-as を削除します。

- BGP 外部ルーテッドネットワークを設定する場合、着信アップデートにはローカル AS 番号が付加されますが、BGP プロセスは他の eBGP ピアに送信されたときに最後にローカル AS 番号を付加します。これを行わない場合は、L3Out の BGP ピア接続プロファイルの [Local-AS 番号の設定 (Local-AS Number Config)] フィールドに [no-prepend] 設定を設定します。
- ファブリック MP-BGP ルート リフレクタ プロファイルに割り当てられている AS とは異なる AS 番号をアドバタイズするために、ローカル AS 機能を使用します。L3Out の BGP ピア接続プロファイルの [Local-AS 番号の設定 (Local-AS Number Config)] フィールドで [replace-as] オプションを有効にすると、ローカル AS 番号で設定されたネイバーには、BGP プロセスからローカルに設定された AS 番号ではなくアドバタイズされている別の AS 番号だけが表示されます。
- 現時点では、ACI ファブリックを介した BGP L3Out 間の通信はブロックされませんが、このシナリオではサポートされません。
 - 両方の L3Out が同じ ASN にあります。
 - L3Out は ACI ファブリックとの iBGP セッションを形成しています
- ルーティングプロトコルの L3Out のルーター ID は、ルーテッドインターフェイス、サブインターフェイス、SVI などの L3Out インターフェイスと同じ IP アドレスまたは同じサブネットにすることはできません。ただし、必要に応じて、ルータ ID を L3Out ループバック IP アドレスの 1 つと同じにすることができます。
- 同じ VRF の同じリーフスイッチに同じルーティングプロトコルの複数の L3Out がある場合、それらのルータ ID は同じである必要があります。ルータ ID と同じ IP アドレスを持つループバックが必要な場合は、それらの L3Out の 1 つだけにループバックを構成できます。
- L3Out の BGP ピアを定義するには、次の 2 つの方法があります。
 - ループバック IP アドレスに BGP ピアを関連付ける論理ノードプロファイル レベル (l3extLNodeP) の BGP ピア接続プロファイル (bgpPeerP) を介した方法。BGP ピアがこのレベルで設定されている場合は、BGP 接続にループバックアドレスが想定されます。そのため、ループバック アドレス設定が欠落していると、障害が発生します。

- BGP ピアをそれぞれのインターフェイスまたはサブインターフェイスに関連付け、論理インターフェイス プロファイル レベル (l3extRsPathL3OutAtt) で BGP ピア接続プロファイル (bgpPeerP) を介した方法。
- IPv6 を使用したループバックを介したピアリングを有効にするには、ユーザが IPv6 アドレスを設定する必要があります。
- 自律システム機能は eBGP ピアでしか使用できません。この機能では、ルータが実際の ASに加えて、2番目の自律システム (AS) のメンバであるように見せることができます。ローカル ASを使用すると、ピアリングの調整を変更せずに2つの ISP をマージできます。マージされた ISP 内のルータは、新しい自律システムのメンバになりますが、使用者に対しては古い自律システム番号を使用し続けます。
- リリース 1.2 (1x) 以降、BGP l3extOut 接続のテナント ネットワーキング プロトコル ポリシーは、最大プレフィックス制限を使用して設定できます。これにより、ピアから受信されるルートプレフィックスの数をモニタし、制限することができます。最大プレフィックス制限を超えると、ログエントリの記録、それ以降のプレフィックスの拒否、固定期間中にカウントがしきい値未満になった場合の接続の再起動、または接続のシャットダウンを行うことができます。一度に1つのオプションだけを使用できます。デフォルト設定では20,000プレフィックスに制限され、その後は新しいプレフィックスは拒否されます。拒否オプションが導入されると、BGPは設定されている制限よりも1つ多くプレフィックスを受け入れ、APIC でエラーが発生します。



(注) Cisco ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ 3 Outside (L3Out) 接続、または Inter-Pod Network (IPN) を介した マルチポッド接続を設定する場合は、インターフェイス MTU がリンクの両端で適切に設定されていることが推奨されます。Cisco ACI、Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定可能な MTU 値はイーサネット ヘッダー (一致する IP MTU、14-18 イーサネット ヘッダー サイズを除く) を考慮していません。また、IOS XR などの他のプラットフォームには、設定された MTU 値にイーサネット ヘッダーが含まれています。設定された値が 9000 の場合、Cisco ACI、Cisco NX-OS Cisco IOS の最大 IP パケットサイズは 9000 バイトになりますが、IOS-XR のタグなしインターフェイスの最大 IP パケットサイズは 8986 バイトになります。

各プラットフォームの適切な MTU 値については、それぞれの設定ガイドを参照してください。

CLI ベースのコマンドを使用して MTU をテストすることを強く推奨します。たとえば、Cisco NX-OS CLI で `ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1` などのコマンドを使用します。

BGP の接続タイプとループバックのガイドライン

ACI では次の BGP 接続の種類をサポートし、それらのループバックのガイドラインをまとめています。

BGP 接続タイプ	ループバックが必要	ルータ ID と同じループバック	スタティック ルートまたは OSPF ルートが必要
直接 iBGP	非対応	N/A	いいえ
iBGP ループバック ピアリング	はい (L3Out ごとに個別のループバック)	いいえ (同じノードに複数のレイヤ 3 Out がある場合)	はい
直接 eBGP	非対応	N/A	いいえ
eBGP ループバック ピアリング (マルチホップ)	はい (L3Out ごとに個別のループバック)	いいえ (同じノードに複数のレイヤ 3 Out がある場合)	はい

外部 BGP スピーカーに対する BGP プロトコル ピアリング

ACI は、iBGP と eBGP を使用して境界リーフと外部 BGP スピーカーの間のピアリングをサポートします。ACI は、BGP ピアリングで以下の接続をサポートします。

- OSPF 上の iBGP ピアリング
- OSPF 上の eBGP ピアリング
- 直接接続上の iBGP ピアリング
- 直接接続上の eBGP ピアリング
- スタティック ルート上の iBGP ピアリング



(注) BGP ピアリングで OSPF が使用される場合、OSPF は BGP ピアリング アドレスへのルートの学習とアドバタイズのみで使用されます。レイヤ 3 Outside ネットワーク (EPG) に適用されるすべてのルート制御が BGP プロトコル レベルで適用されます。

ACI は、外部ピアへの iBGP および eBGP 接続用に多数の機能をサポートします。BGP 機能は、[BGP Peer Connectivity Profile] で設定されます。

BGP ピアの接続プロファイル機能について、次の表で説明します。



(注) ACI は、次の BGP 機能をサポートしています。以下にリストされていない NX-OS BGP 機能は、現在 ACI ではサポートされていません。

表 10: BGP ピアの接続プロファイル機能

BGP 機能	機能の説明	NX-OS での同等のコマンド
Allow Self-AS	Allowed AS Number Count 設定と併用されます。	allowas-in
Disable peer AS check	アドバタイズ時のピア AS 番号のチェックを無効にします。	disable-peer-as-check
Next-hop self	常にローカルピアアドレスにネクストホップ属性を設定します。	next-hop-self
Send community	ネイバーにコミュニティ属性を送信します。	send-community
Send community extended	ネイバーに拡張コミュニティ属性を送信します。	send-community extended
Password	BGP MD5 認証。	password
Allowed AS Number Count	Allow Self-AS 機能と併用されます。	allowas-in
Disable connected check	直接接続された EBGp ネイバーの接続チェックを無効にします (EBGP ネイバーがループバックからピアリングすることを許可)。	
TTL	EBGP マルチホップ接続の TTL 値を設定します。これは EBGp でのみ有効です。	ebgp-multihop <TTL>
Autonomous System Number	ピアのリモート自律システム番号。	neighbor <x.x.x.x> remote-as

BGP 機能	機能の説明	NX-OS での同等のコマンド
Local Autonomous System Number Configuration	ローカル AS 機能を使用するときのオプション (No Prepend+replace-AS+dual-AS など)。	
Local Autonomous System Number	ファブリック MP-BGP ルート リフレクタ プロファイルに割り当てられている AS とは異なる AS 番号をアドバタイズするために使用されるローカル AS 機能。これは EBGp ネイバーの場合にのみサポートされ、ローカル AS 番号がルート リフレクタ ポリシー AS と異なっている必要があります。	local-as xxx <no-prepend> <replace-as> <dual-as>
Site of Origin	site-of-origin (SoO) は、ルーティング グループを防ぐためにルートを学習するサイトを一意に識別するために使用される BGP 拡張コミュニティ属性です。	soo<value>

BGP 外部ルーテッド ネットワークの設定

BGP 外部ルーテッド ネットワークを設定するには、次の項の手順を使用します。

GUI を使用した BGP L3Out の設定

始める前に

BGP L3Out を設定するテナント、VRF、およびブリッジ ドメインはすでに作成されており、VRF の作成時に [BGP ポリシーの設定 (Configure BGP Policies)] オプションを選択しました。

-
- ステップ 1** [ナビゲーション (Navigation)] ペインで、[Tenant_name]>[ネットワーキング (Networking)]>[L3Outs] の順に展開します。
- ステップ 2** 右クリックして、[L3Out の作成 (Create L3Out)] をクリックします。
[L3Out の作成 (Create L3Out)] ウィザードが表示されます。

- ステップ 3** [L3Out の作成 (Create L3Out)] ウィザードの [識別 (Identity)] ウィンドウに必要な情報を入力します。
- [名前 (Name)]、[VRF]、および [L3 ドメイン (L3 Domain)] フィールドに必要な情報を入力します。
 - ルーティング プロトコルのチェック ボックスがある領域で、[BGP] を選択します。
 - [次 (Next)] をクリックして [ノードとインターフェイス (Nodes and Interfaces)] ウィンドウに移動します。
- ステップ 4** [L3Out の作成 (Create L3Out)] ウィザードの [ノードとインターフェイス (Nodes and Interfaces)] ウィンドウに必要な情報を入力します。
- [レイヤ 3 (Layer 3)] 領域で、[ルーテッド (Routed)] を選択します。
 - [ノード ID (Node ID)] フィールドのドロップダウン メニューで、L3Out のノードを選択します。
これらの例のトポロジでは、ノード 103 を使用します。
 - [Router ID] フィールドに、ルータ ID を入力します。
 - (任意) 必要に応じて、ループバック アドレスに別の IP アドレスを設定できます。
[ルータ ID (Router ID)] フィールドに入力したエントリと同じ内容が [ループバック アドレス (Loopback Address)] フィールドに自動で入力されます。これは以前のビルドでの [ループバック アドレスのルータ ID の使用 (Use Router ID for Loopback Address)] と同等です。ループバック アドレスにルータ ID を使用しない場合は、ループバック アドレスに別の IP アドレスを入力します。または、ループバック アドレスにルータ ID を使用しない場合は、このフィールドを空のままにします。
 - [ノードとインターフェイス (Nodes and Interfaces)] ウィンドウに追加の必要な情報を入力します。
このウィンドウに表示されるフィールドは、[レイヤ 3 (Layer 3)] および [レイヤ 2 (Layer 2)] 領域で選択したオプションによって異なります。
 - [ノードとインターフェイス (Nodes and Interfaces)] ウィンドウで残りの追加の情報を入力したら、[次 (Next)] をクリックします。
[プロトコル (Protocols)] ウィンドウが表示されます。
- ステップ 5** [L3Out の作成 (Create L3Out)] ウィザードの [プロトコル (Protocols)] ウィンドウに必要な情報を入力します。
- [BGP ループバック ポリシー (BGP Loopback Policies)] および [BGP インターフェイス ポリシー (BGP Interface Policies)] 領域で、次の情報を入力します。
 - **ピア アドレス (Peer Address)** : ピア IP アドレスを入力します
 - **EBGP Multihop TTL (EBGP マルチホップ TTL)** : 接続の存続可能時間 (TTL) を入力します。範囲は 1 ~ 255 ホップです。ゼロの場合、TTL は指定されません。デフォルトは 1 です。
 - **リモート ASN (Remote ASN)** : ネイバー自律システムを固有に識別する番号を入力します。自律システム番号は、1 ~ 4294967295 のプレーン形式で 4 バイトにすることができます。
(注) ACI は asdot または asdot + 形式の AS 番号をサポートしていません。
 - [次へ (Next)] をクリックします。
[外部 EPG (External EPG)] ウィンドウが表示されます。

ステップ 6 [L3Out の作成 (Create L3Out)] ウィザードで [外部 EPG (External EPG)] ウィンドウに必要な情報を入力します。

- a) **Name** フィールドに、外部ネットワークの名前を入力します。
- b) [提供済みコントラクト (Provided Contract)] フィールドで、提供済みコントラクトの名前を入力します。
- c) [消費済みコントラクト (Consumed Contract)] フィールドで、消費済みコントラクトの名前を入力します。
- d) [すべての外部ネットワークのデフォルト EPG (Default EPG for all external network)] フィールドで、この L3Out 接続からのすべての中継ルートをアドバタイズしない場合はオフにします。

このボックスをオフにすると、[Subnets] 領域が表示されます。次の手順に従って、必要なサブネットとコントロールを指定します。

- e) [+] アイコンをクリックして [サブネット (Subnet)] を展開し、[サブネットの作成 (Create Subnet)] ダイアログ ボックスで次の操作を実行します。
- f) **IP address** フィールドに、外部ネットワークの IP アドレスとサブネット マスクを入力します。

(注) 前のステップで入力した内容に応じて、IPv4 または IPv6 のアドレスを入力します。

外部サブネットを作成するときに、プレフィックス EPG の BGP ループバックの両方を設定するか、またはどちらも設定しない必要があります。BGP ループバックを 1 つのみ設定すると、BGP ネイバーシップは確立されません。

- g) [名前 (Name)] フィールドに、サブネットの名前を入力します。
- h) [Scope] フィールドで、[Export Route Control Subnet]、[Import Route Control Subnet]、および [Security Import Subnet] のチェックボックスをオンにします。[OK] をクリックします。

(注) BGP でインポート制御を適用する場合は、[Import Route Control Subnet] チェックボックスをオンにします。

- i) [サブネットの作成 (Create Subnet)] ウィンドウで必要な設定が完了したら、[OK] をクリックします。
- j) [完了 (Finish)] をクリックして、[L3Out の作成 (Create L3Out)] ウィザードに必要な設定の入力を完了させます。

ステップ 7 (任意) 必要に応じて、[BGP ピア接続プロファイル (BGP Peer Connectivity Profile)] ウィンドウに移動して、BGP 外部ルーテッドネットワークの追加設定を行います。

[テナント (Tenants)] > [tenant_name] > [ネットワークング (Networking)] > [L3Outs] > [L3Out_name] > [論理ノード プロファイル (Logical Node Profiles)] > [log_node_prof_name] > [BGP ピア (BGP Peer)] / <address>

この L3Out の [BGP ピア接続プロファイル (BGP Peer Connectivity Profile)] が表示されます。

- a) [BGP Controls] フィールドで、目的の制御をオンにします。

ピアは、ピアに送信される境界ゲートウェイ プロトコル (BGP) 属性を指定します。ピア制御オプションは次のとおりです。

- 自身の AS を許可 (Allow Self AS) : 自律番号チェックを自身で有効にします。これにより、同じ AS 番号が使用されている場合に BGP ピアが更新を挿入できます。

- **AS オーバーライド (AS override)** : BGP AS オーバーライド機能をイネーブルにして、デフォルト設定をオーバーライドします。AS オーバーライド機能では、発信元のルータからの AS 番号を、アウトバウンドルートの AS パスの BGP ルータ送信の AS 番号に置き換えます。アドレスファミリごとにこの機能を有効にできます (IPv4 または IPv6)。

(注) :

AS オーバーライド機能を有効にするには、[ピア AS チェックを無効化 (Disable Peer AS Check)] チェックボックスもオンにする必要があります。

- **ピア AS チェックを無効化 (Disable Peer AS Check)** : ピア自律番号チェックを無効にします。このチェックボックスをオンにすると、アドバタイジングルータが AS パスでレシーバの AS 番号を見つけた場合、そのルータはレシーバにルートを送信しません。

(注) :

AS オーバーライド機能を有効にするには、[ピア AS チェックを無効化 (Disable Peer AS Check)] チェックボックスをオンにする必要があります。

- **Next-hop Self** : BGP ネクスト ホップ属性を自身に送信します。
- **コミュニティの送信 (Send Community)** : ピアに BGP コミュニティ属性を送信します。
- **拡張コミュニティの送信 (Send Extended Community)** : ピアに BGP 拡張コミュニティ属性を送信します。
- **ドメインパスの送信 (Send Domain Path)** : BGP ドメインパスをピアに送信します。

- b) [パスワード (Password)] フィールドと [パスワードの確認 (Confirm Password)] フィールドに、管理パスワードを入力します。
- c) [自身の AS 番号カウントを許可 (Allow Self AS Number Count)] フィールドで、ローカル自律システム番号 (ASN) の許可される発生回数を選択します。
値の範囲は 1 ~ 10 です。デフォルトは 3 です。
- d) [ピア制御 (Peer Controls)] フィールドに、ネイバー チェック パラメータを入力します。
次のオプションがあります。
 - [双方向フォワーディングの検出 (Bidirectional Forwarding Detection)] : ピアの BFD を有効にします。
 - [接続チェックの無効化 (Disable Connected Check)] : ピア接続のチェックを無効にします。
- e) [アドレスタイプ制御 (Address Type Controls)] フィールドで、必要に応じて BGP IPv4/IPv6 アドレスファミリ機能を設定します。
 - [AF Mcast] : マルチキャストアドレスファミリ機能を有効にする場合にオンにします。
 - [AF Ucast] : ユニキャストアドレスファミリ機能が有効にする場合にオンにします。
- f) 必要に応じて、[ルーティングドメイン ID (Routing Domain ID)] のエントリをメモします。

[ルーティング ドメイン ID (Routing Domain ID)] フィールドの値は、[BGP ルートリフレクタ ポリシー (BGP Route Reflector Policy)] ページに入力されたグローバルドメイン ID ベース値を反映します。詳細については、「ループ防止のための BGP ドメインパス機能について (223 ページ) 」を参照してください。

- g) [EBGP マルチホップ TTL (EBGP Multihop TTL)] フィールドに、接続存続可能時間 (TTL) を入力します。

範囲は 1 ~ 255 ホップです。ゼロの場合、TTL は指定されません。デフォルトは 1 です。

- h) [このネイバーからのルートの重み付け (Weight for routes from this neighbor)] フィールドで、ピアからのルートに許可される重みを選択します。

ルータにローカルに割り当てられた重みが、最適パスの選択に使用されます。範囲は 0 ~ 65535 です。

- i) [プライベート AS 制御 (Private AS Control)] フィールドで、プライベート AS 制御を設定します。

これらのオプションは、ACIBGPAS がパブリック AS 番号である場合、または [no-Prepend+replace-as] オプションを指定した [Local-AS 番号設定 (Local-AS Number Config)] が、指定された BGP ピア接続プロファイル (BGP ネイバー コンフィギュレーション) 。[プライベート AS 制御 (Private AS Control)] 機能は自身のローカルプライベート AS を削除しないため、[replace-as] オプションを使用して、実際のローカルプライベート AS を AS_PATH から削除します。

次のオプションがあります。

- **[プライベート AS の削除 (Remove private AS)]** : 発信 eBGP ルート更新ではこのネイバーを更新する際に、AS_PATH からすべてのプライベート AS 番号を削除します。eBGP ルートにプライベート AS 番号とパブリック AS 番号がある場合は、このオプションを使用します。パブリック AS 番号は保持されます。

ネイバーのリモート AS が AS_PATH にある場合、このオプションは適用されません。

このオプションを有効にするには、[プライベート AS の削除 (Remove private AS)] を有効にする必要があります。

- **[プライベート AS の削除 (Remove private AS)]** : このネイバーへの発信 eBGP ルート更新では、AS_PATH にプライベート AS 番号しかない場合、このオプションはすべてのプライベート AS 番号を削除します。eBGP ルートにプライベート AS 番号のみがある場合は、このオプションを使用します。

ネイバーのリモート AS が AS_PATH にある場合、このオプションは適用されません。

- **プライベート AS をローカル AS と置換 (Replace private AS with local AS) :** このネイバーへの発信 eBGP ルート更新では、このオプションは、パブリック AS またはネイバー リモート AS が AS_PATH に含まれているかどうかに関係なく、AS_PATH 内のすべてのプライベート AS 番号を ACI ローカル AS に置き換えます。

このオプションを有効にするには、[すべてのプライベート AS を削除 (Remove all private AS)] を有効にする必要があります。

- j) [BGP ピア プレフィックス ポリシー (BGP Peer Prefix Policy)] フィールドで、既存のピア プレフィックス ポリシーを選択するか、新しいポリシーを作成します。
- ピア プレフィックス ポリシーは、ネイバーから受信できるプレフィックスの数と、許可されるプレフィックスの数を越えた場合に実行するアクションを定義します。この機能は、外部 BGP ピアで一般的に使用されますが、内部 BGP ピアにも適用できます。
- k) [Site of Origin] フィールドに、このピアを識別するための拡張コミュニティ値を入力します。

Site-of-Origin (SoO) 拡張コミュニティは、サイトを発信元とするルートを識別し、そのプレフィックスの再アドバタイズメントが送信元のサイトに戻されることを防ぐために使用される BGP 拡張コミュニティ属性です。この SoO 拡張コミュニティは、ルータがルートを学んだサイトを一意に識別します。BGP は、ルートに関連付けられた SoO 値を使用し、ルーティングループを防止できます。

有効な形式：

- extended:as2-nn2:<2-byte number>:<2-byte number>

例：extended:as2-nn2:1000:65534

- extended:as2-nn4:<2-byte number>:<4-byte number>

例：extended:as2-nn4:1000:6554387

- extended:as4-nn2:<4-byte number>:<2-byte number>

例：extended:as4-nn2:1000:65504

- extended:ipv4-nn2:<IPv4 address>:<2-byte number>

例：extended:ipv4-nn2:1.2.3.4:65515

(注) ユーザテナント L3Out の SoO を設定する場合は、ACI ファブリック内で設定されたグローバルファブリック、ポッド、またはマルチサイト SoO と同じ SoO 値を設定しないようにしてください。スイッチで次のコマンドを実行すると、ファブリック内に設定されたファブリック、ポッド、およびマルチサイト SoO の値を表示できます。

```
show bgp process vrf overlay-1 | grep SOO
```

- l) [リモート自律システム番号 (Remote Autonomous System Number)] フィールドで、ネイバー自律システムを一意に識別する番号を選択します。
- 自律システム番号は、1 - 4294967295 のプレーン形式で 4 バイトにすることができます。
- (注) ACI は asdot または asdot + 形式の AS 番号をサポートしていません。
- m) [ローカル AS 番号設定 (Local-AS Number Config)] フィールドで、ローカル自律システム番号 (ASN) 設定を選択します。

グローバル AS ではなくローカル AS 番号を使用すると、関連付けられたネットワーク内のルーティング デバイスが以前の AS に属しているように見えます。設定は次のとおりです。

- no-Prepend+replace-as+dual-as：ローカル AS での先頭付加を許可せず、両方の AS 番号で置き換えられます。

注：AS パスの先頭に 1 つ以上の自律システム (AS) 番号を付加できます。AS 番号は、ルートが発信元である実際の AS 番号がパスに追加された後に、パスの先頭に追加されます。AS パスの前に付加すると、AS パスが短く見えるため、BGP よりも優先度が低くなります。

- no-prepend：ローカル AS でのプリペンドを許可しません。
- no options：ローカル AS の変更を許可しません。
- no-Prepend+replace-as：ローカル AS での先頭追加を許可せず、AS 番号を置き換えます。

- n) [ローカル AS 番号 (Local-AS Number)] フィールドで、目的の値を選択します。

eBGP ピアのローカル自律システム機能の場合にオプションが必要です。ローカル自律システム番号は、1 ~ 4294967295 のプレーン形式で 4 バイトにすることができます。

(注) ACI は asdot または asdot+ 形式の AS 番号をサポートしていません。

- o) [管理状態 (Admin State)] フィールドで、[無効化 (Disabled)] または [有効化 (Enabled)] を選択します。

[管理状態 (Admin State)] フィールドでは、対応する BGP ネイバーをシャットダウンできます。この機能を使用すると、BGP ピア設定を削除せずに BGP セッションがシャットダウンされます。

次のオプションがあります。

- 無効化：BGP ネイバーの管理状態を無効にします。
- 有効化：BGP ネイバーの管理状態を有効にします。

- p) [ルート制御プロファイル (Route Control Profile)] フィールドで、BGP ピアごとにルート制御ポリシーを設定します。

[+] をクリックして、次を設定します。

- [名前 (Name)]：ルート制御プロファイル名を選択します。
- [方向 (Direction)]：次のいずれかのオプションを選択します。
 - ルートインポートポリシー
 - ルートエクスポートポリシー

- q) [送信 (Submit)] をクリックします。

ステップ 8 [テナント (Tenants)] > [tenant_name] > [ネットワーク (Networking)] > [L3Outs] > [L3Out_name] に移動します。

ステップ 9 [ポリシー/メイン (Policy/Main)] タブをクリックし、次の操作を実行します。

- a) (任意) [Route Control Enforcement] フィールドで、[mport] チェックボックスをオンにします。

(注) BGP でインポート制御を適用する場合は、このチェックボックスをオンにします。

- b) [Route Control for Dampening] フィールドを展開し、目的のアドレスファミリタイプとルートダンピングポリシーを選択します。[Update] をクリックします。

このステップでは、ポリシーはステップ 4 で作成することができます。または、ポリシー名が選択されているドロップダウンリストで [ルート プロファイルの作成 (Create route profile)] をするオプションがあります。

- ステップ 10** [テナント (Tenants)] > [tenant_name] > [ネットワーキング (Networking)] > [L3Outs] > [L3Out_name] に移動します。
- ステップ 11** [ルート制御のインポートおよびエクスポートのルートマップ (Route Map for import and export rout control)] を右クリックし、[ルート制御のインポートおよびエクスポートのルートマップの作成 (Create Route Map for import and export rout control)] を選択します。
- ステップ 12** このウィンドウに必要な情報を入力し、[コンテキスト (Context)] 領域で [+] をクリックして [ルート制御コンテキストの作成 (Create Route Control Context)] ウィンドウを表示します。
- [Name] フィールドに、ルート制御 VRF の名前を入力します。
 - [Set Attribute] ドロップダウンリストから、[Create Action Rule Profile] を選択します。
- アクションルールを作成するときに、必要に応じてルート ダンプニング属性を設定します。

BGP Max Path の設定

次の機能を使用すると、等コスト マルチパスのロード バランシングを有効にするルート テーブルへのパスの最大数を追加できます。

GUI を使用した BGP Max Path の設定

始める前に

適切なテナントと BGP 外部ルーティング ネットワークが作成され、使用可能になります。

手順の概要

- APIC GUI にログインし、メニューバーで [テナント (Tenants)] > [tenant_name] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [BGP] > [BGP アドレス ファミリ コンテキスト (BGP Address Family Context)] の順にクリックし、[BGP アドレス ファミリ コンテキスト ポリシーの作成 (Create BGP Address Family Context Policy)] を右クリックします。
- [BGP アドレス ファミリ コンテキスト ポリシーの作成 (Create BGP Address Family Context Policy)] ダイアログ ボックスで、次のタスクを実行します。
- [テナント (Tenants)] > [tenant_name] > [ネットワーキング (Networking)] > [VRFs] > [vrf_name] の順にクリックします。
- 対象の VRF の設定の詳細を確認します。
- [アドレス ファミリごとの BGP コンテキスト (BGP Context Per Address Family)] フィールドを見つけ、[BGP アドレス ファミリ タイプ (BGP Address Family Type)] 領域で、IPv4 unicast address family または IPv6 unicast address family を選択します。

6. **[BGP Address Family Context]** ドロップダウンリストで作成した [BGP Address Family Context] にアクセスし、それをサブジェクト VRF に関連付けます。
7. [送信 (Submit)] をクリックします。

手順の詳細

ステップ 1 APIC GUI にログインし、メニューバーで [テナント (Tenants)] > [tenant_name] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [BGP] > [BGP アドレス ファミリ コンテキスト (BGP Address Family Context)] の順にクリックし、**[BGP アドレス ファミリ コンテキスト ポリシーの作成 (Create BGP Address Family Context Policy)]** を右クリックします。

ステップ 2 **[BGP アドレス ファミリ コンテキスト ポリシーの作成 (Create BGP Address Family Context Policy)]** ダイアログ ボックスで、次のタスクを実行します。

次のフィールドの許容値については、Cisco APIC ドキュメンテーションページの 『Verified Scalability Guide for Cisco APIC』 を参照してください。 <https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller/tsd-products-support-series-home.html>

- a) [Name] フィールドにポリシーの名前を入力します。
- b) **[eBGP 距離 (eBGP Distance)]** フィールドに、eBGP ルートの [管理距離 (Administrative Distance)] の値を入力します。
- c) **[iBGP 距離 (iBGP Distance)]** フィールドに、iBGP ルートの [管理距離 (Administrative Distance)] の値を入力します。
- d) [ローカル距離 (Local Distance)] フィールドに、ローカル距離の値を入力します。
- e) **[eBGP 最大 ECMP (eBGP Max ECMP)]** フィールドに、eBGP ロードシェアリングの等コストパスの最大数の値を入力します。
- f) **[iBGP 最大 ECMP (iBGP Max ECMP)]** フィールドに、iBGP ロードシェアリングの等コストパスの最大数の値を入力します。
- g) [ホスト ルート リークの有効化 (Enable Host Route Leak)] フィールドで、ボックスをクリックして、DCIG への EVPN タイプ 2 (MAC/IP) ホスト ルートの配布を有効にします。
- h) エントリを更新した後、**[Submit]** をクリックします。

ステップ 3 [テナント (Tenants)] > [tenant_name] > [ネットワーキング (Networking)] > [VRFs] > [vrf_name] の順にクリックします。

ステップ 4 対象の VRF の設定の詳細を確認します。

ステップ 5 [アドレス ファミリごとの BGP コンテキスト (BGP Context Per Address Family)] フィールドを見つけ、[BGP アドレス ファミリ タイプ (BGP Address Family Type)] 領域で、IPv4 unicast address family または IPv6 unicast address family を選択します。

ステップ 6 **[BGP Address Family Context]** ドロップダウンリストで作成した [BGP Address Family Context] にアクセスし、それをサブジェクト VRF に関連付けます。

ステップ 7 [送信 (Submit)] をクリックします。

AS パス プリペンドの設定

次の項の手順を使用して、AS パスのプリペンドを設定します。

AS パス プリペンドの設定

BGP ピアは、AS パス アトリビュートの長さを増やすことで、リモートピアでベストパス選択の影響を与えることができます。番号として指定桁の前に付加して AS パス アトリビュートの長さを向上するために使用するメカニズムを提供する AS パス Prepend。

AS パス前に付加は、ルートマップを使用してアウトバウンド方向にのみ適用できます。パスとして前に付加が機能しない iBGP セッションで。

AS パス Prepend 機能は、次のように変更を有効に。

プリペンド	ルートマップと一致するルートの AS パスに、指定した AS 番号を付加します。 (注) <ul style="list-style-type: none"> • 1 個以上の AS 番号を設定できます。 • 4 バイト番号がサポートされています。 • 合計を prepend は 32 の AS 番号。AS 番号は、AS パスアトリビュートに挿入されます順序を指定する必要があります。
Prepend-最後-として	最後の前に付加 AS パス 1 から 10 までの範囲に番号として。

次の表では、AS パス Prepend の実装の選択基準について説明します。

プリペンド	1	指定された AS 番号を追加します。
Prepend-最後-として	2	最後の AS 番号を AS パスに付加します。
デフォルト	Prepend(1)	指定された AS 番号を追加します。

設定の AS パス Prepend GUI を使用して

始める前に

構成済みのテナント

手順の概要

1. APIC GUI にログインしメニューバーで、[テナント (Tenants)] > [tenant_name] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [設定ルール (Set Rules)] の順にクリックし、[ルートマップの設定ルールの作成 (Create Set Rules for a Route Map)] を右クリックします。
2. 設定ルールの A ルートマップの作成 ダイアログボックス、次のタスクを実行します。

3. 基準に [AS 番号の付加 (Prepend AS)] を選択し、[+] をクリックして AS 番号を先頭に付加します。
4. AS 番号とその順序を入力し、クリックして **更新**。 [+] をクリックして複数の AS 番号の先頭を追加する必要があるかどうかを繰り返します。
5. AS 番号の先頭を追加する設定が完了したら、基準 [AS 番号の末尾を追加 (Prepend Last-AS)] を選択し、指定された回数の数を AS 番号の末尾に付加します。
6. [カウント](1-10) を入力します。
7. [OK] をクリックします。
8. [ルート マップの設定ルールを作成 (Create Set Rules For A Rout Map)] ウィンドウで AS パスに基づく設定ルールの基準を確認し、[完了 (Finish)] をクリックします。
9. APIC GUI メニューバーで、[テナント (Tenants)] [tenant_name] [ポリシー (Policies)] [プロトコル (Protocol)] [設定ルール (Set Rules)] の順にクリックし、プロファイルを右クリックします。 > > >
10. 確認、 **AS パスの設定** 画面の下部の値します。

手順の詳細

-
- ステップ 1** APIC GUI にログインしメニューバーで、[テナント (Tenants)] > [tenant_name] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [設定ルール (Set Rules)] の順にクリックし、[ルート マップの設定ルールの作成 (Create Set Rules for a Route Map)] を右クリックします。
- [ルート マップの設定ルールの作成 (Create Set Rules For A Route Map)] ウィンドウが表示されます。
- ステップ 2** 設定ルールの A ルート マップの作成 ダイアログボックス、次のタスクを実行します。
- a) [Name] フィールドに、名前を入力します
 - b) [AS パスの設定 (Set AS Path)] チェックボックスをオンにし、[次へ (Next)] をクリックします。
 - c) [AS パス (AS Path)] ウィンドウで [+] をクリックして [AS パスの設定を作成 (Create Set AS Path)] ダイアログ ボックスを開きます。
- ステップ 3** 基準に [AS 番号の付加 (Prepend AS)] を選択し、 [+] をクリックして AS 番号を先頭に付加します。
- ステップ 4** AS 番号とその順序を入力し、クリックして **更新**。 [+] をクリックして複数の AS 番号の先頭を追加する必要があるかどうかを繰り返します。
- ステップ 5** AS 番号の先頭を追加する設定が完了したら、基準 [AS 番号の末尾を追加 (Prepend Last-AS)] を選択し、指定された回数の数を AS 番号の末尾に付加します。
- ステップ 6** [カウント](1-10) を入力します。
- ステップ 7** [OK] をクリックします。
- ステップ 8** [ルート マップの設定ルールを作成 (Create Set Rules For A Rout Map)] ウィンドウで AS パスに基づく設定ルールの基準を確認し、[完了 (Finish)] をクリックします。
- ステップ 9** APIC GUI メニューバーで、[テナント (Tenants)] [tenant_name] [ポリシー (Policies)] [プロトコル (Protocol)] [設定ルール (Set Rules)] の順にクリックし、プロファイルを右クリックします。 > > >
- ステップ 10** 確認、 **AS パスの設定** 画面の下部の値します。
-

AS オーバーライドの BGP 外部ルーテッド ネットワーク

AS オーバーライドを使用して BGP 外部ルーテッド ネットワークを設定するには、次の項の手順を使用します。

BGP 自律システムのオーバーライドについて

BGP のループ防止は、自律システム パスの自律システム番号を確認することで行われます。受信側のルータが受信した BGP パケットの自律システム パスで独自の自律システム番号が表示される場合、パケットは廃棄されます。受信側のルータでは、パケットが独自の自律システムから発信され、最初に発信元から同じ場所に達したことが想定されます。この設定では、ルーティング ループが発生しないようにするためのデフォルトです。

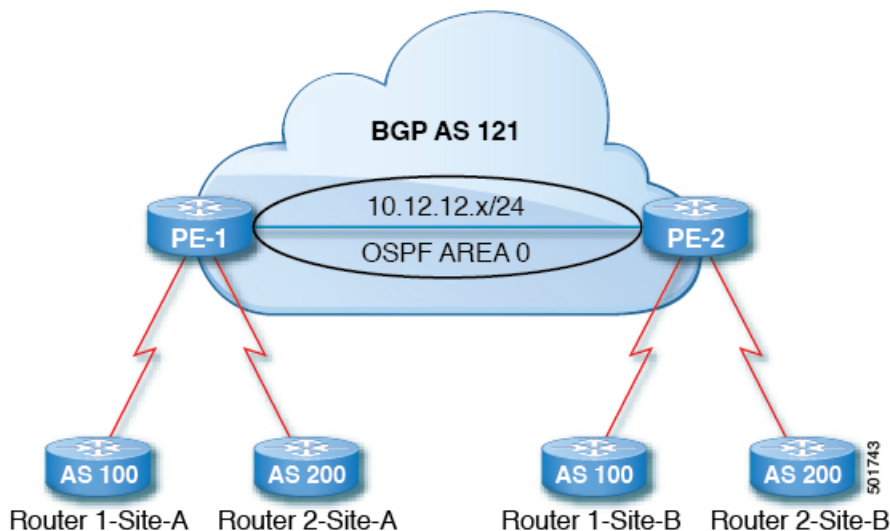
別の自立システム番号によりリンクする同一の自律システム番号を持つさまざまなサイトや禁止ユーザーのサイトを使用する場合、デフォルトルートのループが発生しないようにする設定によって問題が発生する可能性があります。このようなシナリオでは、その他のサイトが受信した場合 1 つのサイトからのルーティング更新は廃棄されます。

このような状況の発生を防ぐため、Cisco APIC リリース 3.1(2m) 以降、BGP 自律システムのオーバーライド機能を有効にして、デフォルトの設定をオーバーライドすることができます。同時に、ピア AS チェックの無効化も有効にする必要があります。

自律システム オーバライド機能では、発信元のルータからの自律システム番号を、アウトバウンドルートの AS パスの BGP ルータ送信の自律システム番号に置き換えます。アドレスファミリごとにこの機能を有効にできます (IPv4 または IPv6)。

自律システム オーバライド機能は、GOLF レイヤ 3 設定および非 GOLF レイヤ 3 の設定でサポートされています。

図 36: 自律システム オーバライド機能を説明するトポロジ例



ルータ 1 およびルータ 2 は、複数のサイトを持つ 2 つの顧客です (サイト A とサイト B)。顧客ルータ 1 は AS 100 で動作し、顧客ルータ 2 は AS 200 で動作します。

GUI を使用して、BGP 外部ルーテッド ネットワークと有効になっている自律システム オーバーライドを設定する

上の図は、次のような自律システム (AS) オーバーライドプロセスを示しています。

1. ルータ A サイト 1 では、AS100 でルート 10.3.3.3 をアドバタイズします。
2. ルータ PE-1 は、AS100 として PE2 へ内部ルートとして反映します。
3. ルータ PE-2 は AS121 で 10.3.3.3 をプリペンドし (AS パスの 100 を 121 に置き換えます)、プレフィックスをプロパゲートします。
4. ルータ 2 サイト B は 10.3.3.3 更新プログラムを承認します。

GUI を使用して、BGP 外部ルーテッド ネットワークと有効になっている自律システム オーバーライドを設定する

始める前に

- テナント、VRF、およびブリッジ ドメインが作成されています。
- 非 GOLF 設定の外部ルーテッド ネットワーク、論理ノード プロファイル、および BGP ピア接続プロファイルが作成されています。

ステップ 1 メニューバーで、[テナント (Tenants)] > [Tenant_name] > [ネットワーキング (Networking)] > [L3Outs] > [Non-GOLF Layer 3 Out_name] > [論理ノード プロファイル (Logical Node Profiles)] を選択します。

ステップ 2 Navigation ウィンドウで、適切な **BGP Peer Connectivity Profile** を選択します。

ステップ 3 [作業 (Work)] ペインで、[BGP ピア接続プロファイル (BGP Peer Connectivity Profile)] の [プロパティ (Properties)] 下の [BGP 制御 (BGP Controls)] フィールドで、次の手順を実行します:

- a) **AS override** フィールドのチェック ボックスをオンにして、**Autonomous System override** 機能を有効にします。
- b) **Disable Peer AS Check** フィールドのチェック ボックスをオンにします。

(注) AS オーバーライド機能を有効にするには、**AS override** および **Disable Peer AS Check** チェック ボックスをオンにする必要があります。

- c) 必要に応じてその他のフィールドを選択します。

ステップ 4 [送信 (Submit)] をクリックします。

BGP ネイバー シャットダウンおよびソフト リセット

BGP ネイバーのシャットダウンとソフト リセットを設定するには、次の項の手順を使用します。

BGP ネイバー シャットダウンとソフト リセットについて

リリース 4.2(1) 以降、次の機能がサポートされるようになりました。

- [BGP ネイバー シャットダウン \(305 ページ\)](#)
- [BGP ネイバー ソフト リセット \(305 ページ\)](#)

BGP ネイバー シャットダウン

BGP ネイバー シャットダウン機能は、NX-OS の `neighbor shutdown` コマンドに似ており、対応する BGP ネイバーをシャットダウンします。このポリシーを使用して、BGP ネイバーの管理状態を無効または有効にします。この機能を使用すると、BGP ピア設定を削除せずに BGP セッションがシャットダウンされます。

BGP ネイバー ソフト リセット

BGP ネイバー ソフト リセット機能は、BGP ルート リフレッシュ機能を使用して、保存されているルーティング テーブル アップデート情報に依存しない着信および発信 BGP ルーティング テーブル アップデートのダイナミック ソフト リセットを自動的にサポートします。ソフト ダイナミック インバウンド リセットとソフト アウトバウンド リセットを有効にするには、このポリシーを使用します。

GUI を使用した BGP ネイバー シャットダウンの設定

次の手順では、GUI を使用して BGP ネイバー シャットダウン機能を使用する方法について説明します。

始める前に

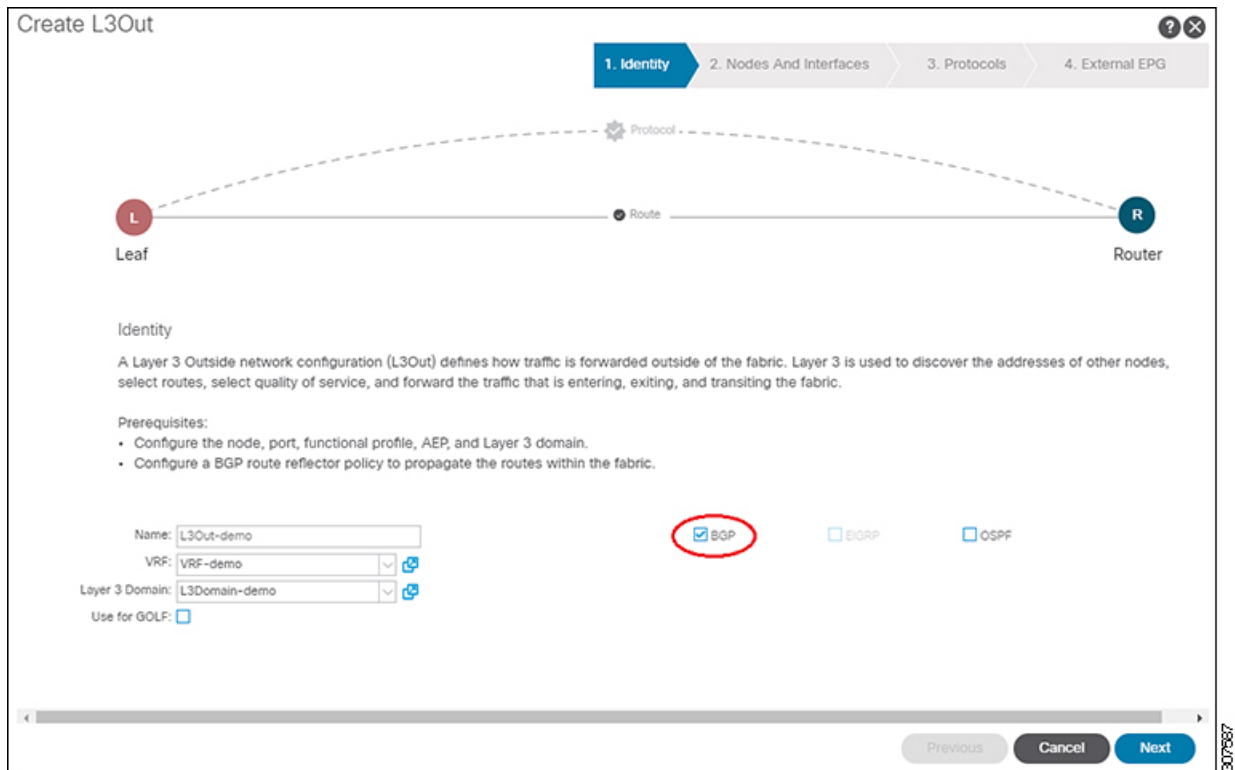
L3Out を設定する前に、次のような標準的な前提条件を満たします。

- ノード、ポート、AEP、機能プロファイル、レイヤ 3 ドメインを設定します。
- ファブリック内でルートを伝播させるための、BGP ルート リフレクタ ポリシーを設定します。

ステップ 1 L3Out を作成し、L3Out の BGP を設定します。

- a) [ナビゲーション (Navigation)] ペインで [テナント (Tenant)] および [ネットワーキング (Networking)] を展開します。
- b) [L3Outs] を右クリックし、[L3Out の作成 (Create L3Out)] を選択します。
- c) L3Out の BGP を設定するために必要な情報を入力します。

この L3Out の BGP プロトコルを設定するには、L3Out 作成ウィザードの [識別 (Identity)] ページで [BGP] を選択します。



- d) 残りのページを続けて行い ([ノードとインターフェイス (Nodes and Interfaces)]、[プロトコル (Protocols)]、および [外部 EPG (External EPG)])、L3Out の設定を完了します。

ステップ 2 L3Out の設定が完了したら、BGP ネイバーのシャットダウンを設定します。

- a) BGP ピア接続プロファイル画面に移動します。

[テナント (Tenants)] > [テナント (*tenant*)] > [ネットワーク (Networking)] > [L3Outs] > [L3out-name] > [論理ノードプロファイル (Logical Node Profiles)] > [logical-node-profile-name] > [論理インターフェイスプロファイル (Logical Interface Profiles)] > [logical-interface-profile-name] > [BGP ピア接続プロファイル (BGP Peer Connectivity Profile)] [IP-address]

- b) [管理状態 (Admin State)] フィールドまでスクロールし、このフィールドで適切な選択を行います。
- 無効化 : BGP ネイバーの管理状態を無効にします。
 - 有効化 : BGP ネイバーの管理状態を有効にします。

GUI を使用した BGP ネイバー ソフトリセットの設定

次の手順では、GUI を使用して BGP ネイバー ソフトリセット機能を使用する方法について説明します。

始める前に

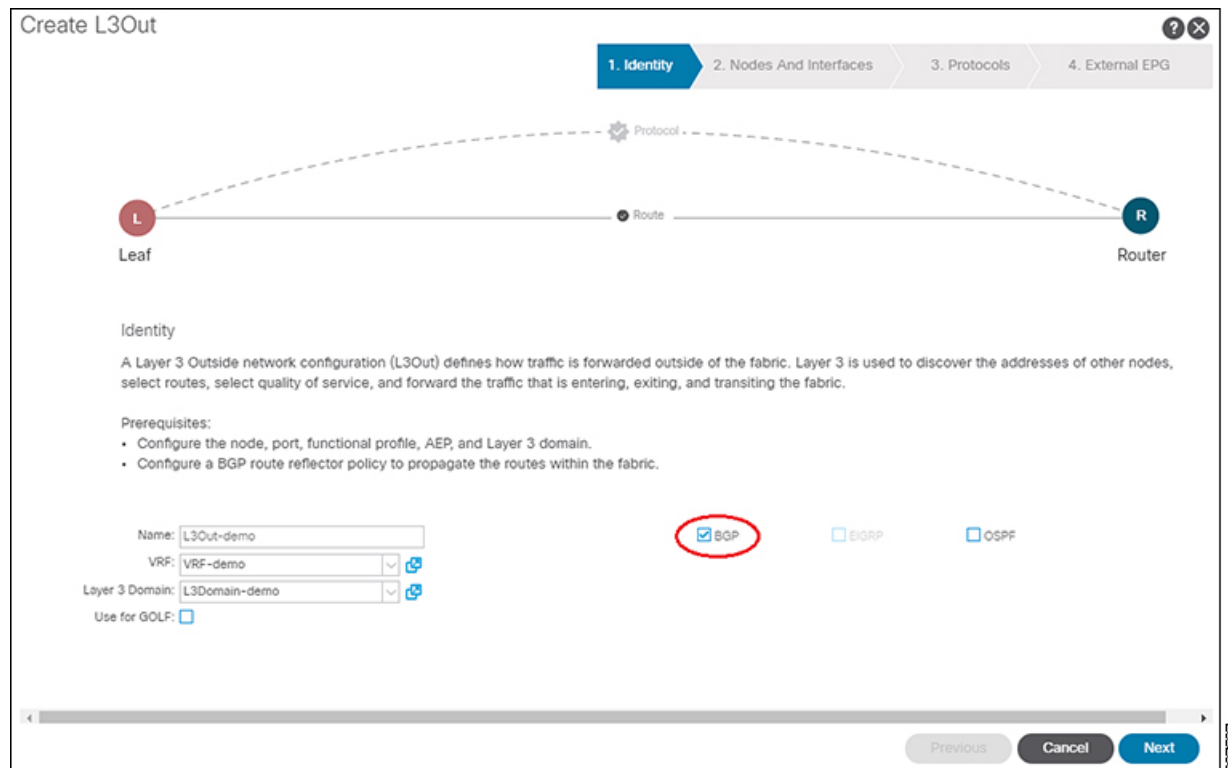
L3Out を設定する前に、次のような標準的な前提条件を満たします。

- ノード、ポート、AEP、機能プロファイル、レイヤ 3 ドメインを設定します。
- ファブリック内でルートを伝播させるための、BGP ルート リフレクタ ポリシーを設定します。

ステップ 1 L3Out を作成し、L3Out の BGP を設定します。

- [ナビゲーション (Navigation)] ペインで [テナント (Tenant)] および [ネットワーキング (Networking)] を展開します。
- [L3Outs] を右クリックし、[L3Out の作成 (Create L3Out)] を選択します。
- L3Out の BGP を設定するために必要な情報を入力します。

この L3Out の BGP プロトコルを設定するには、L3Out 作成ウィザードの [識別 (Identity)] ページで [BGP] を選択します。



- 残りのページを続けて行い ([ノードとインターフェイス (Nodes and Interfaces)]、[プロトコル (Protocols)]、および [外部 EPG (External EPG)])、L3Out の設定を完了します。

ステップ 2 L3Out の設定が完了したら、BGP ネイバーのソフトリセットを設定します。

- [BGP ピア エントリ (BGP Peer Entry)] 画面に移動します。

[テナント (Tenants)] > [テナント (*tenant*)] > [ネットワーキング (Networking)] > [L3Outs] > [L3out-name] > [論理ノードプロファイル (Logical Node Profiles)] > [logical-node-profile-name] > [設定済みノード (Configured Nodes)] > [ノード (*node*)] > [BGP for VRF-]vrf-name > [ネイバー (Neighbors)]

- b) 適切なネイバー エントリを右クリックし、[BGP ピアのクリア (Clear BGP Peer)] を選択します。
[BGP をクリア (Clear BGP)] ページが表示されます。
- c) [モード (Mode)] フィールドで、[ソフト (Soft)] を選択します。
[方向 (Direction)] フィールドが表示されます。
- d) [方向 (Direction)] フィールドで適切な値を選択します。
 - Incoming : ソフト ダイナミック インバウンド リセットを有効にします。
 - Outgoing : ソフト アウトバウンド リセットを有効にします。

VRF ごと、ノード BGP ごとのタイマーの値の設定

ノードごとの BGP タイマー値を設定するには、次の項の手順を使用します。

ノード BGP タイマー値ごとの各 VRF

この機能を紹介する前に、特定の VRF について、すべてのノードには同じ BGP タイマーの値が使用されます。

ノード BGP タイマー値ごとの各 VRF 機能の導入により、BGP タイマーを定義し、各ノードベースの VRF ごとに関連付けることが可能です。ノードでは複数の VRF を所持することが可能で、それぞれ、fvCtx に対応しています。ノード設定 (l3extLNodeP) には、BGP プロトコルプロファイル (bgpProtP) の設定が含まれており、希望の BGP コンテキスト ポリシーを参照します (bgpCtxPol)。これにより、同じ VRF 内のさまざまなノードが異なる BGP タイマーの値を含めることが可能になります。

各 VRF ではノードに bgpDom の具体的な MO を含みます。その名前 (プライマリ キー) は、VRF<fvTenant>:<fvCtx> です。属性として BGP タイマーの値が含まれています (例: holdIntvl、kaIntvl、maxAsLimit)。

有効なレイヤ 3 アウト設定を作成するために必要なすべての手順は、ノード BGP タイマーごとの各 VRF に正常に適用する必要があります。たとえば、次のような MO は必須です:

fvTenant、fvCtx、l3extOut、l3extInstP、LNodeP、bgpRR。

ノードでは、BGP タイマー ポリシーは次のアルゴリズムに基づいて選択されます。

- BgpProtP が指定されると、bgpProtP の下で参照される bgpCtxPol を使用します。
- それ以外の場合、指定されると対応する fvCtx の下で参照される bgpCtxPol を使用します。
- それ以外の場合、指定されるとテナントでデフォルト ポリシーを使用します。例:
uni/tn-<tenant>/bgpCtxP-default。

- それ以外の場合、テナント common の下の default ポリシーを使用します。例：
uni/tn-common/bgpCtxP-default。これはプログラム済みです。

設定の高度な GUI を使用して BGP タイマーのノードごとの VRF あたり

BGP タイマーが特定のノードに設定されているときに、ノードで BGP タイマー ポリシーを使用し、VRF に関連付けられている BGP ポリシー タイマーはすべて無視されます。

始める前に

テナントと VRF はすでに設定されています。

- ステップ 1** メニューバーで、[テナント (Tenant)] > [Tenant_name] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [BGP] > [BGP タイマー (BGP Timers)] を選択し、[BGP タイマーポリシーの作成 (Create BGP Timers Policy)] を右クリックします。
- ステップ 2** [BGP タイマーポリシーの作成 (Create BGP Timers Policy)] ダイアログボックスで、次の操作を実行します:
 - a) **Name** フィールドに、BGP タイマーポリシーの名前を入力します。
 - b) 使用可能なフィールドには、必要に応じて、適切な値を選択します。[Submit] をクリックします。`
BGP タイマーポリシーが作成されます。
- ステップ 3** [テナント (Tenant)] > [Tenant_name] > [ネットワークング (Networking)] > [L3Outs] に移動し、[L3Out の作成 (Create L3Out)] を右クリックします。
Create L3Out ウィザードが表示されます。次の操作を実行して、BGP を有効にした L3Out を作成します。
- ステップ 4** [L3Out の作成 (Create L3Out)] ウィザードの [識別 (Identity)] ウィンドウに必要な情報を入力します。
 - a) **Name** フィールドに L3Out の名前を入力します。
 - b) **VRF** ドロップダウンリストから VRF を選択します。
 - c) [L3 ドメイン (L3 Domain)] ドロップダウンリストから、適切なドメインを選択します。
 - d) ルーティングプロトコルのチェックボックスがある領域で、[BGP] を選択します。
 - e) **Next** をクリックして **Nodes and Interfaces** ウィンドウに移動します。
 - f) [L3Out の作成 (Create L3Out)] ウィザードの残りのウィンドウに進み、L3Out の作成プロセスを完了します。
- ステップ 5** L3Out を作成したら、作成した L3Out の論理ノードプロファイル ([テナント (Tenant)] [Tenant_name] [ネットワークング (Networking)] [L3Outs] [L3Out_name] [論理ノードプロファイル (Logical Node Profiles)] [LogicalNodeProfile-name]) に移動します。 > > > >
- ステップ 6** [論理ノードプロファイル (Logical Node Profile)] ウィンドウで、[BGP プロトコルプロファイルの作成 (Create BGP Protocol Profile)] の横にあるチェックボックスをオンにします。
[ノード指定 BGP プロトコルプロファイルの作成 (Create Node Specific BGP Protocol Profile)] ウィンドウが表示されます。
- ステップ 7** **BGP タイマー** フィールドに、ドロップダウンリストから、この特定のノードに関連付ける BGP タイマーポリシーを選択します。[送信 (Submit)] をクリックします。`

特定の BGP タイマー ポリシーは、ノードに適用されます。

(注) BGP タイマーポリシーと、既存のノードのプロファイルに関連付ける、ノードのプロファイルをクリックし、タイマー ポリシーを関連付けます。

タイマー ポリシーが具体的に選択していない場合、**BGP タイマー** されたノードのプロファイルが存在する自動的に VRF に関連付けられている BGP タイマー ポリシーは、このノードに適用を取得し、ノードのフィールドします。

ステップ 8 設定を確認するには、**Navigation** ウィンドウで、次の手順を実行します:

- a) [テナント (Tenants)] > [Tenant_name] > [ネットワーク (Networking)] > [L3Outs] > [L3Out_name] > [論理ノード プロファイル (Logical Node Profiles)] > [LogicalNodeProfile-name] > [プロトコル プロファイル (Protocol Profiles)] の順に移動します。
- b) 作業] ペインで、ノードのプロファイルに関連付けられている BGP プロトコルプロファイルが表示されます。

不整合や障害のトラブルシューティング

特定の状況下では、次のような不整合や障害が発生する可能性があります:

異なるレイヤ 3 Out (l3Out) が同じ VRF (fvCtx) に関連付けられているか、同じノードで bgpProtP が異なるポリシー (bgpCtxPol) に関連付けられていると、障害が発生します。次の例では、同じ Layer 3 Out (out1 と out2) が同じ VRF (ctx1) に関連付けられています。out1 の下では、node1 は BGP タイマー プロトコル pol1 に関連付けられており、out2 の下では、node1 は別の BGP タイマー プロトコル pol2 に関連付けられています。。この場合、障害が発生します。

```
tn1
  ctx1
    out1
      ctx1
        node1
          protp pol1

    out2
      ctx1
        node1
          protp pol2
```

このような障害が発生した場合は、設定を変更して、BGP タイマー ポリシー間の競合を削除してください。

BFD サポートの設定

BFD サポートを設定するには、次の項の手順を使用します。

双方向フォワーディング検出

双方向フォワーディング検出 (BFD) を使用して、ピアリングルータの接続をサポートするように設定された ACI ファブリック境界リーフ スイッチ間の転送パスのサブセカンド障害検出時間を提供します。

BFD は、次のような場合に特に役立ちます。

- ルータ同士の間で直接的な接続がない場合に、レイヤ 2 デバイスまたはレイヤ 2 クラウド経由でピアリングルータが接続されているとき。転送パスに障害があっても、ピアルータにはそれがわからない可能性があります。プロトコルの制御に利用できるメカニズムは hello タイムアウトですが、タイムアウトまでには数十秒、さらには数分の時間がかかる場合があります。BFD では、障害を 1 秒未満で検出することが可能です。
- 信頼できる障害検出に非対応の物理メディア (共有イーサネットなど) 経由でピアリングルータが接続されているとき。この場合も、ルーティングプロトコルは、時間のかかる hello タイマーに頼るしかありません。
- 1 組のルータの間で多くのプロトコルが実行されているとき、各プロトコルは、独自のタイムアウトでリンク障害を検出する独自の hello メカニズムを持っています。BFD は、すべてのプロトコルに均一のタイムアウトを指定し、それによってコンバージェンス時間の一貫性を保ち、予測可能にします。

次に示す BFD の設定のガイドラインおよび制限事項に従ってください。

- APIC リリース 3.1 (1) 以降、リーフおよびスパイン スイッチ間の BFD は IS-IS のファブリック インターフェイスでサポートされています。さらに、スパイン スイッチの BFD 機能は、OSPF ルートとスタティック ルートでサポートされます。
- Cisco APIC リリース 5.2(4) 以降、BFD 機能は、ルーテッド インターフェイスで設定されているセカンダリ IPv4/IPv6 サブネットを使用して到達可能なスタティック ルートでサポートされています。サブネットに複数のアドレスが設定されている場合、スタティック BFD セッションは L3Out インターフェイスのセカンダリ サブネットから発信できません。共有サブネット アドレス (vPC シナリオに使用) と浮動 L3Out に使用される浮動 IP アドレスは、サブネットの追加アドレスとして許可され、自動的にスキップされ、静的 BFD セッションの発信元には使用されません。



(注) セッションのソースに使用されているセカンダリ アドレスを変更するには、同じサブネットに新しいアドレスを追加し、後で以前のアドレスを削除します。

- BFD は -EX および -FX ラインカード (または新しいバージョン) のモジュラ スパイン スイッチでサポートされ、また BFD は Nexus 9364C 非モジュラ スパイン スイッチ (または新しいバージョン) でサポートされます。
- VPC ピア間の BFD はサポートされません。

- APIC リリース 5.0(1) 以降、BFD マルチホップはリーフ スイッチでサポートされます。BFD マルチホップ セッションが合計に含まれるようになったため、BFD セッションの最大数は変更されません。
- APIC リリース 5.0(1) 以降、ACI は C ビット対応 BFD をサポートしています。BFD がコントロールプレーンに依存しているかいないかは、受信する BFD パケットの C ビットによって判別されます。
- ループバック アドレス ピアでの iBGP 上の BFD はサポートされません。
- インターフェイス ポリシーで BFD サブインターフェイス最適化を有効化できます。このフラグを1つのサブインターフェイスに立てることにより、その物理インターフェイス上のすべてのサブインターフェイスの最適化が有効になります。
- BGP プレフィクス ピアの BFD はサポートされません。



(注) Cisco ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルーターへのレイヤ 3 Outside (L3Out) 接続、または Inter-Pod Network (IPN) を介したマルチポッド接続を設定する場合は、インターフェイス MTU がリンクの両端で適切に設定されていることが推奨されます。Cisco ACI、Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定可能な MTU 値はイーサネット ヘッダー (一致する IP MTU、14-18 イーサネット ヘッダー サイズを除く) を考慮していません。また、IOS XR などの他のプラットフォームには、設定された MTU 値にイーサネット ヘッダーが含まれています。設定された値が 9000 の場合、Cisco ACI、Cisco NX-OS Cisco IOS の最大 IP パケットサイズは 9000 バイトになりますが、IOS-XR のタグなしインターフェイスの最大 IP パケットサイズは 8986 バイトになります。

各プラットフォームの適切な MTU 値については、それぞれの設定ガイドを参照してください。

CLI ベースのコマンドを使用して MTU をテストすることを強く推奨します。たとえば、Cisco NX-OS CLI で `ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1` などのコマンドを使用します。

サブインターフェイスの BFD の最適化

サブインターフェイスの BFD は最適化できます。BFD により、設定されているすべてのサブインターフェイスのセッションが作成されます。BFD により、設定されている最小の VLAN ID を持つサブインターフェイスがマスター サブインターフェイスとして設定され、そのサブインターフェイスは親インターフェイスの BFD セッション パラメータを使用します。残りのサブインターフェイスは `slow timer` を使用します。

最適化サブインターフェイス セッションでエラーが検出されると、BFD により、その物理インターフェイスのすべてのサブインターフェイスがダウンとマークされます。

BFD モニタ対象リンクの一端または両端で BFD エコー機能を設定できます。エコー機能は設定された `slow timer` に基づいて必要最小受信間隔を遅くします。[`RequiredMinEchoRx`] BFD セッ

ションパラメータは、エコー機能がディセーブルの場合、ゼロに設定されます。slow timer は、エコー機能がイネーブルの場合、必要最小受信間隔になります。



(注) サブインターフェイスの1つがフラップすると、その物理インターフェイスのサブインターフェイスが影響を受け、1 秒間ダウンします。

GUI を使用したセカンダリ IP アドレスでの双方向フォワーディング検出の構成

この手順では、GUIを使用して、セカンダリ IP アドレスで双方向フォワーディング検出 (BFD) を構成します。

- ステップ 1 メニューバーで、[テナント (Tenants)] > [すべてのテナント (ALL Tenants)] の順に選択します。 >
- ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。
- ステップ 3 ナビゲーション ペインから、[tenant_name] > [ネットワーク (Networking)] > [L3Outs] > [l3out_name] > [論理ノード プロファイル (Logical Node Profiles)] > [node_profile_name] > [論理インターフェイス プロファイル (Logical Interface Profiles)] > [interface_profile_name] の順に移動します。
- ステップ 4 [Work] ペインで、必要に応じて [Policy (ポリシー)] > [ルーテッド サブインターフェイス (Routed Sub-interfaces)]、[Policy (ポリシー)] > **Routed Interfaces** または [Policy (ポリシー)] > [SVI] を選択します。
- ステップ 5 インターフェイスをダブルクリックして、そのプロパティを編集します。
- ステップ 6 インターフェイスのタイプに応じて、次のサブステップのいずれかを実行します。
 - a) インターフェイスがルーテッドサブインターフェイスまたはルーテッドインターフェイス、または [パス タイプ (Path Type)] が [ポート (Port)] または [ダイレクトポートチャネル (Direct Port Channel)] に設定されたスイッチ仮想インターフェイス (SVI) である場合は、[IPv4 セカンダリ/IPv6 追加アドレス (IPv4 secondary/IPv6 Additional Addresses)] テーブルで、+ をクリックし、IP を入力します。アドレスとサブネットを選択し、[送信 (Submit)] をクリックします。
 - b) インターフェイスがスイッチ仮想インターフェイス (SVI) で、パス タイプが仮想ポートチャネルに設定されている場合は、サイド B の IPv4 セカンダリ/IPv6 追加アドレス テーブルで、+ をクリックし、IP アドレスとサブネットを入力して、[OK] をクリックします。
- ステップ 7 [ナビゲーション] ペインで、[tenant_name] > [ネットワーク (Networking)] > [L3Outs] > [l3out_name] > [論理ノード プロファイル (Logical Node Profiles)] > [node_profile_name] > [構成済みノード (Configured Nodes)] > [node_name] を選択します。
- ステップ 8 [静的ルート (Static Routes)] テーブルで、[+] をクリックして、次のサブステップを実行します。
 - a) [プレフィックス (Prefix)] フィールドに、外部ネットワークに割り当てられている静的ルートの IP アドレスとマスクを入力します。
 - b) [BFD] チェックボックスをオンにします。
 - c) [次のホップアドレス (Next Hop Addresses)] テーブルで、[+] をクリックし、[次のホップアドレス (Next Hop Addresses)] フィールドに、インターフェイスに指定したセカンダリ IP アドレスから到達可能な IP アドレスを入力します。
 - d) 必要に応じて、残りのフィールドを入力します。

GUI を使用してリーフスイッチの BFD をグローバルに設定する

- e) [OK] をクリックします。

ステップ 9 必要に応じて、残りのフィールドに入力します。

ステップ 10 [送信 (Submit)] をクリックします。

GUI を使用してリーフスイッチの BFD をグローバルに設定する

ステップ 1 メニューバーで、[Fabric] > [Access Policies] の順に選択します。

ステップ 2 [ナビゲーション (Navigation)] ペインで、[ポリシー (Policies)] > [スイッチ (Switch)] > [BFD] の順に展開します。

設定を双方向フローディング検出 (BFD) には、使用可能な 2 つの種類があります:

- BFD IPV4
- BFD IPV6

これらの BFD 設定ごとに、デフォルトポリシーを使用するか、特定のスイッチ(またはスイッチのセット)用に新しいポリシーを作成できます。

(注) デフォルトでは、APIC コントローラはシステムの起動時にデフォルトのポリシーを作成します。これらのデフォルトポリシーはグローバルなもので、双方向転送検出 (BFD) の設定ポリシーです。デフォルトグローバルポリシー内の属性は、作業ウィンドウで設定できます。または、これらデフォルトのポリシーの値を変更することもできます。ただし、いったんデフォルトのグローバルポリシーを変更すると、システム全体(すべてのスイッチ)に影響することに注意してください。デフォルトではありませんが、特定のスイッチ(またはスイッチの設定)の特定の設定を使用する場合は、次の手順の説明に従って、スイッチのプロファイルを作成します。

ステップ 3 特定のグローバル BFD ポリシー (デフォルトではないもの) 向けにスパインスイッチプロファイルを作成するには、[ナビゲーション (Navigation)] ペインで、[スイッチ (Switches)] > [リーフスイッチ (Leaf Switches)] > [プロファイル (Profiles)] の順に展開します。

リーフスイッチ - プロファイル (Leaf Switches - Profiles) 画面が [作業 (Work)] ペインに表示されます。

ステップ 4 [作業 (Work)] ペインの右側、アクションアイコンの下で、リーフプロファイルの作成 (Create Leaf Profile) を選択します。

[Create Leaf Profile] ダイアログボックスが表示されます。

ステップ 5 Create Leaf Profile ダイアログボックスで、次の操作を実行します:

- a) **Name** フィールドに、リーフスイッチプロファイルの名前を入力します
- b) (任意) [説明 (Description)] フィールドに、プロファイルの説明を入力します。
- c) (任意) [リーフセクタ (Leaf Selectors)] ツールバーで、[+] をクリックします。
- d) [名前 (Name)] (スイッチに名前を付けます)、[ブロック (Blocks)] (スイッチを選択します)、および [ポリシーグループ (Policy Group)] ([アクセススイッチポリシーグループの作成 (Create Access Switch Policy Group)]) に適切な値を入力します。
Create Access Switch Policy Group ダイアログボックスが表示されます。ここでは、ポリシーグループの識別プロパティを指定できます。

- ステップ 6** (リーフ セレクタを設定する場合) [アクセス スイッチ ポリシー グループの作成 (Create Access Switch Policy Group)] ダイアログ ボックスで次のアクションを実行します。
- [Name] フィールドにポリシー グループの名前を入力します。
 - (任意) [説明 (Description)] フィールドで、ポリシー グループの説明を入力します。
 - BFD ポリシー タイプ (**BFD IPV4 Policy** または **BFD IPV6 Policy**) を選択し、値 (**default** または **Create BFD Global Ipv4 Policy**) を特定のスイッチまたはスイッチのセットに対して選択します。
 - [更新 (Update)] をクリックします。
- ステップ 7** [次へ (Next)] をクリックして [関連付け (Associations)] へ進みます。
- (任意) [関連付け (Associations)] メニューで、リーフ プロファイルをリーフ インターフェイス プロファイルおよびアクセス モジュール プロファイルに関連付けることができます。
- ステップ 8** [完了 (Finish)] をクリックします。
- BFD グローバルポリシーを作成するもう 1つの方法は、**BFD IPV4** または **BFD IPV6** のいずれかを右クリックします (**Navigation** ウィンドウにあります)。
- ステップ 9** 作成した BFD グローバル コンフィギュレーションを確認するには、[ナビゲーション (Navigation)] ペインで、[ポリシー (Policies)] > [スイッチ (Switch)] > [BFD] の順に展開します。

GUI を使用してスパインスイッチで BFD のグローバル設定

- ステップ 1** メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
- ステップ 2** [ナビゲーション (Navigation)] ペインで、[ポリシー (Policies)] > [スイッチ (Switch)] > [BFD] の順に展開します。
- 設定を双方向フォワーディング検出 (BFD) には、使用可能な 2つの種類があります：
- BFD IPV4
 - BFD IPV6
- これらの BFD 設定ごとに、デフォルトポリシーを使用するか、特定のスイッチ (またはスイッチのセット) 用に新しいポリシーを作成できます。
- (注) デフォルトでは、APIC コントローラはシステムの起動時にデフォルトのポリシーを作成します。これらのデフォルトポリシーはグローバルなもので、双方向転送検出 (BFD) の設定ポリシーです。デフォルト グローバルポリシー内の属性は、作業ウィンドウで設定できます。または、これらデフォルトのポリシーの値を変更することもできます。ただし、いったんデフォルトのグローバルポリシーを変更すると、システム全体 (すべてのスイッチ) に影響することに注意してください。デフォルトではありませんが、特定のスイッチ (またはスイッチの設定) の特定の設定を使用する場合は、次の手順の説明に従って、スイッチのプロファイルを作成します。
- ステップ 3** 特定のグローバル BFD ポリシー (デフォルトではないもの) 向けにスパインスイッチ プロファイルを作成するには、[ナビゲーション (Navigation)] ペインで、[スイッチ (Switches)] > [スパインスイッチ (Spine Switches)] > [プロファイル (Profiles)] の順に展開します。
- スパインスイッチ : プロファイル 画面が [作業 (Work)] ペインに表示されます。

ステップ 4 [作業 (Work)] ペインの右側、アクションアイコンの下で、[スパインプロファイルの作成 (Create Spine Profile)] を選択します。

Create Spine Profile ダイアログボックスが表示されます。

ステップ 5 **Create Spine Profile** ダイアログボックスで、次の操作を実行します:

- a) **Name** フィールドに、スイッチプロファイルの名前を入力します。
- b) **Description** フィールドの隣に、プロファイルの説明を入力します。(この手順は任意です)。
- c) (任意) [スパインセクタ (Spine Selectors)] ツールバーで、[+] をクリックします。
- d) [名前 (Name)] (スイッチに名前を付けます) 、[ブロック (Blocks)] (スイッチを選択します) 、および [ポリシーグループ (Policy Group)] ([スパインスイッチポリシーグループの作成 (Create Spine Switch Policy Group)]) に適切な値を入力します。

スパインスイッチポリシーグループの作成 ダイアログボックスはポリシーグループ id のプロパティを指定できますが表示されます。

ステップ 6 (スパインセクタを設定する場合) [スパインスイッチポリシーグループの作成 (Create Spine Switch Policy Group)] ダイアログボックスで次のアクションを実行します。

- a) [Name] フィールドにポリシーグループの名前を入力します。
- b) (任意) [説明 (Description)] フィールドで、ポリシーグループの説明を入力します。
- c) BFD ポリシータイプ (**BFD IPv4 Policy** または **BFD IPv6 Policy**) を選択し、値 (**default** または **Create BFD Global Ipv4 Policy**) を特定のスイッチまたはスイッチのセットに対して選択します。
- d) [更新 (Update)] をクリックします。

ステップ 7 [次へ (Next)] をクリックして [関連付け (Associations)] へ進みます。

(任意) [関連付け (Associations)] メニューで、スパインプロファイルをスパインインターフェイスプロファイルに関連付けることができます。

ステップ 8 [完了 (Finish)] をクリックします。

BFD グローバルポリシーを作成するもう 1 つの方法は、**BFD IPv4** または **BFD IPv6** のいずれかを右クリックします (**Navigation** ウィンドウにあります)。

ステップ 9 作成した BFD グローバルコンフィギュレーションを確認するには、[ナビゲーション (Navigation)] ペインで、[ポリシー (Policies)] > [スイッチ (Switch)] > [BFD] の順に展開します。

GUI を使用した BFD インターフェイスのオーバーライドの設定

明示的な双方向フォワーディング検出 (BFD) を設定できる、3 つのサポート対象のインターフェイス (ルーテッドレイヤインターフェイス、外部インターフェイス SVI とルーテッドサブインターフェイス) があります。グローバルコンフィギュレーションを使用しないで、さらに特定のインターフェイスの明示的な設定をしたい場合、特定のスイッチまたは一連のすべてのインターフェイスに適用される独自のグローバルコンフィギュレーションを作成できます。特定のインターフェイス上の特定のスイッチの粒度がさらに必要な場合、このインターフェイスオーバーライド設定を使用する必要があります。



- (注) BFD インターフェイス ポリシーが親ルーテッドインターフェイスに設定されている場合、デフォルトでは、親インターフェイスと同じアドレス ファミリを持つすべてのルーテッドサブインターフェイスがこのポリシーを継承します。継承された設定のいずれかを上書きする必要がある場合は、サブインターフェイスで明示的な BFD インターフェイスポリシーを設定します。ただし、親インターフェイスで **Admin State** または **Echo Admin State** が無効になっている場合、サブインターフェイスでプロパティをオーバーライドすることはできません。

始める前に

テナントはすでに作成されています。

- ステップ 1** メニュー バーで、 **Tenant** を選択します。
- ステップ 2** [ナビゲーション (Navigation)] ペイン (クイック スタートの下)、作成したテナント [Tenant_name] > [ネットワーク キング (Networking)] > [L3Outs] を展開します。
- ステップ 3** [L3Outs] を右クリックし、[L3Out の作成 (Create L3Out)] を選択します。
[L3Out の作成 (Create L3Out)] ウィザードが表示されます。
- ステップ 4** [L3Out の作成 (Create L3Out)] ウィザードの [識別 (Identity)] ウィンドウに必要な情報を入力します。
- [名前 (Name)]、[VRF]、および [L3 ドメイン (L3 Domain)] フィールドに必要な情報を入力します。
 - ルーティング プロトコルのチェック ボックスがある領域で、[BGP] を選択します。
 - [次 (Next)] をクリックして [ノードとインターフェイス (Nodes and Interfaces)] ウィンドウに移動します。
- ステップ 5** [L3Out の作成 (Create L3Out)] ウィザードの [ノードとインターフェイス (Nodes and Interfaces)] ウィンドウに必要な情報を入力します。
- [レイヤ 3 (Layer 3)] 領域で、[ルーテッド (Routed)] を選択します。
 - [ノード ID (Node ID)] フィールドのドロップダウン メニューで、L3Out のノードを選択します。
これらの例のトポロジでは、ノード 103 を使用します。
 - [Router ID] フィールドに、ルータ ID を入力します。
 - (任意) 必要に応じて、ループバック アドレスに別の IP アドレスを設定できます。
[ルータ ID (Router ID)] フィールドに入力したエン트리と同じ内容が [ループバック アドレス (Loopback Address)] フィールドに自動で入力されます。これは以前のビルドでの [ループバック アドレスのルータ ID の使用 (Use Router ID for Loopback Address)] と同等です。ループバック アドレスにルータ ID を使用しない場合は、ループバック アドレスに別の IP アドレスを入力します。または、ループバック アドレスにルータ ID を使用しない場合は、このフィールドを空のままにします。
 - [ノードとインターフェイス (Nodes and Interfaces)] ウィンドウに追加の必要な情報を入力します。
このウィンドウに表示されるフィールドは、[レイヤ 3 (Layer 3)] および [レイヤ 2 (Layer 2)] 領域で選択したオプションによって異なります。

- f) [ノードとインターフェイス (Nodes and Interfaces)] ウィンドウで残りの追加の情報を入力したら、[次 (Next)] をクリックします。
- [プロトコル (Protocols)] ウィンドウが表示されます。

ステップ 6 [L3Out の作成 (Create L3Out)] ウィザードの [プロトコル (Protocols)] ウィンドウに必要な情報を入力します。

- a) [BGP ループバック ポリシー (BGP Loopback Policies)] および [BGP インターフェイス ポリシー (BGP Interface Policies)] 領域で、次の情報を入力します。
- **ピア アドレス (Peer Address)** : ピア IP アドレスを入力します
 - **EBGP Multihop TTL (EBGP マルチホップ TTL)** : 接続の存続可能時間 (TTL) を入力します。範囲は 1 - 255 ホップです。ゼロの場合、TTL は指定されません。デフォルトは 0 です。
 - **リモート ASN (Remote ASN)** : ネイバー自律システムを固有に識別する番号を入力します。自律システム番号は、1 - 4294967295 のプレーン形式で 4 バイトにすることができます。
- (注) ACI は asdot または asdot + 形式の AS 番号をサポートしていません。

- b) [OSPF] 領域で、デフォルト OSPF ポリシー、以前に作成した OSPF ポリシー、または [OSPF インターフェイス ポリシーの作成 (Create OSPF Interface Policy)] を選択します。
- c) [次へ (Next)] をクリックします。
- [外部 EPG (External EPG)] ウィンドウが表示されます。

ステップ 7 [L3Out の作成 (Create L3Out)] ウィザードで [外部 EPG (External EPG)] ウィンドウに必要な情報を入力します。

- a) **Name** フィールドに、外部ネットワークの名前を入力します。
- b) [提供済みコントラクト (Provided Contract)] フィールドで、提供済みコントラクトの名前を入力します。
- c) [消費済みコントラクト (Consumed Contract)] フィールドで、消費済みコントラクトの名前を入力します。
- d) [すべての外部ネットワークのデフォルト EPG (Default EPG for all external network)] フィールドで、この L3Out 接続からのすべての中継ルートをアドバタイズしない場合はオフにします。
- このボックスをオフにすると、[Subnets] 領域が表示されます。次の手順に従って、必要なサブネットとコントロールを指定します。
- e) [完了 (Finish)] をクリックして、[L3Out の作成 (Create L3Out)] ウィザードに必要な設定の入力を完了させます。

ステップ 8 [テナント (Tenants)] > [tenant_name] > [ネットワーキング (Networking)] > [L3Outs] > [L3Out_name] > [論理ノード プロファイル (Logical Node Profiles)] > [logical_node_profile_name] > [論理インターフェイス プロファイル (Logical Interface Profiles)] > [logical_interface_profile_name] の順に移動します。

ステップ 9 [論理インターフェイス プロファイル (Logical Interface Profile)] ウィンドウで、[BFD インターフェイス プロファイルの作成 (Create BFD Interface Profile)] フィールドまで下にスクロールし、このフィールドの横にあるボックスをオンにします。

ステップ 10 [BFD インターフェイス プロファイルの作成 (Create BFD Interface Profile)] ウィンドウで、BFD の詳細を入力します。

- 認証タイプ フィールドで、選択 **No authentication** または キー **SHA1** 。

認証 (SHA1 のキーを選択) により、入力を選択すると、**認証キー ID** を入力してください、**の認証キーを** (パスワード)、再入力して、パスワードを確認 **キーの確認** 。

- [BFD インターフェイス ポリシー (BFD Interface Policy)] フィールドで、[一般的な/デフォルト (common/default)] 設定 (デフォルト BFD ポリシー) のいずれかを選択、または、[BFD インターフェイス ポリシーの作成 (Create BFD Interface Policy)] を選択することによって自分の BFD ポリシーを作成します。

選択した場合 **BFD インターフェイス ポリシーの作成**、**BFD インターフェイス ポリシーの作成** BFD インターフェイス ポリシーの値を定義するダイアログボックスが表示されます。

ステップ 11 [Submit] をクリックします。

ステップ 12 設定したインターフェイス レベルの BFD ポリシーを確認するには、[ポリシー (Policies)] > [プロトコル (Protocol)] > [BFD] に移動します。

GUI を使用して BFD コンシューマ プロトコルを設定する

この手順では、BFD 機能の消費者であるコンシューマプロトコル (OSPF、BGP、EIGRP、スタティック ルート、および IS-IS) での双方向フォワーディング検出 (BFD) を有効にする方法を説明します。これらのプロトコルで BFD を使用するには、それらのフラグを有効にする必要があります。



(注) これらの 4 つのコンシューマ プロトコルは、左側のナビゲーション ペインの [テナント (Tenant)] > [ポリシー (Policies)] > [プロトコル (Protocol)] の下にあります。

始める前に

テナントはすでに作成されています。

ステップ 1 [L3Out の作成 (Create L3Out)] ウィザードを使用して L3Out を作成します。

ステップ 2 メニュー バーで、[テナント (Tenant)] を選択します。

ステップ 3 BGP プロトコルの BFD を設定するには、[ナビゲーション (Navigation)] ペイン (Quick Start の下) で、作成したテナント、[Tenant_name] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [BGP] > [BGP ピア プレフィックス (BGP Peer Prefix)] を展開します。

ステップ 4 **Work** ウィンドウの右側の [ACTIONS] の下で、[Create BGP Peer Prefix Policy] を選択します。[Create BGP Peer Prefix Policy] ダイアログボックスが表示されます。

(注) 左のナビゲーション ウィンドウで **[BGP Peer Prefix]** を右クリックして **[Create BGP Peer Prefix]** を選択し、ポリシーを作成することもできます。

- ステップ 5** **[Name]** フィールドに名前を入力し、残りのフィールドに値を入力して BGP ピア プレフィックス ポリシーを定義します。
- ステップ 6** **[送信 (Submit)]** をクリックします。
作成した BGP ピア プレフィックス ポリシーは、左のナビゲーション ウィンドウの **[BGP Peer Prefix]** の下に表示されます。
- ステップ 7** **[テナント (Tenants)]** > **[tenant_name]** > **[ネットワーク (Networking)]** > **[L3Outs]** > **[L3Out_name]** > **[論理ノード プロファイル (Logical Node Profiles)]** > **[logical_node_profile_name]** > **[論理インターフェイス プロファイル (Logical Interface Profiles)]** > **[logical_interface_profile_name]** > **[BGP ピア接続プロファイル (BGP Peer Connectivity Profile)]** の順に移動します。
- ステップ 8** **[BGP ピア接続プロファイル (BGP Peer Connectivity Profile)]** ウィンドウで、**[BGP ピア プレフィックス ポリシー (BGP Peer Prefix Policy)]** フィールドまでスクロールし、作成した BGP ピア プレフィックス ポリシーを選択します。
- ステップ 9** **[ピア制御 (Peer Controls)]** フィールドで、**[双方向フォワーディング検出 (Bidirectional Forwarding Detection)]** を選択して BGP コンシューマ プロトコルの BFD を有効にします (またはオフにして BFD を無効にします)。
- ステップ 10** OSPF プロトコルの BFD を設定するには、**[ナビゲーション (Navigation)]** ペインで、**[ポリシー (Policies)]** > **[プロトコル (Protocol)]** > **[OSPF]** > **[OSPF インターフェイス (OSPF Interface)]** に移動します。
- ステップ 11** **Work** ウィンドウの右側の、**[ACTIONS]** の下で、**[Create OSPF Interface Policy]** を選択します。
[Create OSPF Interface Policy] ダイアログボックスが表示されます。
- (注) 左のナビゲーション ウィンドウで **[OSPF Interface]** を右クリックして **[Create OSPF Interface Policy]** を選択し、ポリシーを作成することもできます。
- ステップ 12** **[Name]** フィールドに名前を入力し、残りのフィールドに値を入力して OSPF インターフェイス ポリシーを定義します。
- ステップ 13** このダイアログボックスの **[Interface Controls]** セクションでは、BFD の有効と無効を切り替えることができます。有効にするには、図のように、**[BFD]** の隣のボックスをオンにして OSPF コンシューマ プロトコルにフラグを追加します (またはボックスをオフにして BFD を無効にします)。
- ステップ 14** **[送信 (Submit)]** をクリックします。
- ステップ 15** EIGRP プロトコルの BFD を設定するには、**[ナビゲーション (Navigation)]** ペインで、**[tenant_name]** > **[ポリシー (Policies)]** > **[プロトコル (Protocol)]** > **[EIGRP]** > **[EIGRP インターフェイス (EIGRP Interface)]** に移動します。
- ステップ 16** **Work** ウィンドウの右側の、**[ACTIONS]** の下で、**[Create EIGRP Interface Policy]** を選択します。
[Create EIGRP Interface Policy] ダイアログボックスが表示されます。
- (注) 左のナビゲーション ウィンドウで **[EIGRP Interface]** を右クリックして **[Create EIGRP Interface Policy]** を選択し、ポリシーを作成することもできます。
- ステップ 17** **[Name]** フィールドに名前を入力し、残りのフィールドに値を入力して OSPF インターフェイス ポリシーを定義します。

- ステップ 18** このダイアログボックスの **[Control State]** セクションでは、BFD の有効と無効を切り替えることができます。有効にするには、図のように、**[BFD]** の隣のボックスをオンにして EIGRP コンシューマプロトコルにフラグを追加します (またはボックスをオフにして BFD を無効にします)。
- ステップ 19** **[送信 (Submit)]** をクリックします。
- ステップ 20** スタティックルートプロトコルで BFD を設定するには、**[ナビゲーション (Navigation)]** ペインで **[ネットワーク (Networking)]** > **[L3Outs]** > **[L3Out_name]** > **[設定済みのノード (Configured Nodes)]** に戻り、設定済みのノードをクリックして **[ノード関連付け (Node Association)]** ウィンドウを表示します。
- ステップ 21** **[Static Routes]** セクションで、**[+]** (展開) ボタンをクリックします。**[Create Static Route]** ダイアログボックスが表示されます。このセクションで、必要なフィールドの値を入力します。
- ステップ 22** **[Route Control]** の隣で、**[BFD]** の隣のボックスをオンにして有効にします (または、無効にする場合にはオフにします)。
- ステップ 23** **[送信 (Submit)]** をクリックします。
- ステップ 24** IS-IS プロトコルの BFD を設定するには、**[ナビゲーション (Navigation)]** ペインで **[ファブリック (Fabric)]** > **[ファブリック ポリシー (Fabric Policies)]** > **[ポリシー (Policies)]** > **[インターフェイス (Interface)]** > **[L3 インターフェイス (L3 Interface)]** に移動します。
- ステップ 25** **Work** ウィンドウの右側の、**[ACTIONS]** の下で、**[Create L3 Interface Policy]** を選択します。**[Create L3 Interface Policy]** ダイアログボックスが表示されます。
- (注) 左のナビゲーション ウィンドウで **[L3 Interface]** を右クリックして **[Create EIGRP Interface Policy]** を選択し、ポリシーを作成することもできます。
- ステップ 26** **[Name]** フィールドに名前を入力し、残りのフィールドに値を入力して L3 インターフェイス ポリシーを定義します。
- ステップ 27** BFD ISIS ポリシーを有効にするには、**[BFD ISIS ポリシー設定 (BFD ISIS Policy Configuration)]** フィールドで **[有効化 (enabled)]** をクリックします。
- ステップ 28** **[送信 (Submit)]** をクリックします。

BFD マルチホップ

BFD マルチホップでは、複数ホップ (最大 255 ホップ) の宛先に対する 1 秒未満の転送障害検出が可能になります。リリース 5.0(1) 以降、APIC は IPv4 の BFD マルチホップおよび IPv6 の BFD マルチホップを、RFC5883 に準拠してサポートします。BFD マルチホップセッションは、固有のソースと宛先アドレス ペア間で設定されます。BFD マルチホップセッションは、シングルホップ BFD セッションの場合、インターフェイスではなく、送信元と宛先の間で作成されます。

BFD マルチホップは TTL フィールドを BGP によってサポートされる最大制限に設定し、受信時に値のチェックを行いません。ACI リーフは、BFD マルチホップパケットが通過できるホップ数には影響しませんが、ホップ数は 255 に制限されます。

BFD マルチホップの注意事項と制約事項

- BFDマルチホップのデフォルトおよび最小送信/受信インターバル タイマーは 250 ミリ秒です。
- デフォルトの最小検出乗数は 3 です。
- エコー モードは BFD マルチホップではサポートされません。

BFD マルチホップ ポリシーの設定

ポリシーの目的に応じて、GUI の複数の場所で BFD マルチホップ ポリシーを設定できます。

- **グローバル ポリシー**：デフォルトでは、APIC コントローラはシステムの起動時にデフォルトのポリシーを作成します。これらのデフォルト ポリシーは、グローバル BFD マルチホップ設定ポリシーです。デフォルト グローバル ポリシー内の属性は、[作業 (Work)] ペインで設定できます。または、これらデフォルトのポリシーの値を変更することもできます。ただし、いったんデフォルトのグローバル ポリシーを変更すると、システム全体 (すべてのスイッチ) に影響が及びます。デフォルトではありませんが、特定のスイッチまたはスイッチのセットの特定の設定を使用する場合は、スイッチプロファイルを作成し、そのスイッチプロファイル内で BFD マルチホップの値を変更します。

次の GUI の場所で、IPv4 または IPv6 のグローバル BFD マルチホップ設定ポリシーを作成または変更できます。

- [ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] > [ポリシー (Policies)] > [スイッチ (Switch)] > [BFD マルチホップ (BFD Multihop)] > [BFD マルチホップ IPv4 (BFD Multihop IPv4)] : [BFD グローバル IPv4 MH ポリシーの作成 (Create BFD Global IPv4 MH Policy)] を右クリックして選択します。
- [ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] > [ポリシー (Policies)] > [スイッチ (Switch)] > [BFD マルチホップ (BFD Multihop)] > [BFD マルチホップ IPv6 (BFD Multihop IPv6)] : [BFD グローバル IPv6 MH ポリシーの作成 (Create BFD Global IPv6 MH Policy)] を右クリックして選択します。
- **ノードポリシー**：BFD マルチホップ ノードポリシーは、ノードプロファイルの下のインターフェイスに適用されます。

この GUI の場所で BFD マルチホップ ノードポリシーを作成または変更できます。

- [テナント (Tenants)] > [テナント (tenant)] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [BFD マルチホップ (BFD Multihop)] > [ノードポリシー (Node Policies)] : [BFD マルチホップ ノードポリシーの作成 (Create BFD Multihop Node Policy)] を右クリックして選択します。
- **インターフェイス ポリシー**：BFD マルチホップ インターフェイス ポリシーは、インターフェイスプロファイルの下のインターフェイスに適用されます。

この GUI の場所で BFD マルチホップ インターフェイス ポリシーを作成または変更できます。

- [テナント (Tenants)]>[テナント (tenant)]>[ポリシー (Policies)]>[プロトコル (Protocol)]>[BFD マルチホップ (BFD Multihop)]>[インターフェイス ポリシー (Interface Policies)] : [BFD マルチホップ インターフェイス ポリシーの作成 (Create BFD Multihop Interface Policy)] を右クリックして選択します。
- グローバルポリシーの上書き : デフォルトのグローバル設定を使用せず、特定のインターフェイスで明示的な設定を行う場合は、独自のグローバル設定を作成できます。この設定は、特定のスイッチまたはスイッチセットのすべてのインターフェイスに適用されます。特定のインターフェイス上の特定のスイッチの粒度がさらに必要な場合、このインターフェイス オーバーライド設定を使用する必要があります。

次の GUI ロケーションで、ノードプロファイルまたはインターフェイス プロファイルの BFD マルチホップ オーバーライド ポリシーを作成または変更できます。

- [テナント (Tenants)]>[テナント (tenant)]>[ネットワーク (Networking)]>[L3Outs]>[l3out]>[論理ノードプロファイル (Logical Node Profiles)]>[logical_node_profile] : [BFD インターフェイス プロトコル プロファイルの作成 (Create BFD Interface Protocol Profile)] を右クリックして選択し、BFD マルチホップ ノードポリシーを指定します。
- [テナント (Tenants)]>[テナント (tenant)]>[ネットワーク (Networking)]>[L3Outs]>[l3out]>[論理ノードプロファイル (Logical Node Profiles)]>[logical_node_profile]>[論理インターフェイス プロファイル (Logical Interface Profiles)]>[logical_interface_profile] : [MH-BFD インターフェイス プロトコル プロファイルの作成 (Create MH-BFD Interface Protocol Profile)] を右クリックして選択し、BFD マルチホップ インターフェイス ポリシーを指定します。
- [テナント (Tenants)]>[インフラ (infra)]>[ネットワーク (Networking)]>[SR-MPLS Infra L3Outs]>[l3out]>[論理ノードプロファイル (Logical Node Profiles)]>[logical_node_profile]>[論理インターフェイス プロファイル (Logical Interface Profiles)]>[logical_interface_profile] : [MH-BFD インターフェイス プロトコル プロファイルの作成 (Create MH-BFD Interface Protocol Profile)] を右クリックして選択し、BFD マルチホップ インターフェイス ポリシーを指定します。

ステップ 1 BFD マルチホップ ポリシーを作成または設定する GUI の場所に移動します。

ステップ 2 既存のプロファイルまたはポリシーを編集するか、ダイアログ ボックスを起動して新しいプロファイルを作成します。

ステップ 3 プロファイルで、BFD マルチホップ セッションの [認証タイプ (Authentication Type)] を選択します。認証なしまたは SHA-1 認証を要求するように選択できます。

ステップ 4 新しいポリシーを作成する場合は、ダイアログ ボックスで設定を行います。

- a) ポリシーの [名前 (Name)] を入力します。
- b) [管理状態 (Admin State)] を [有効 (Enabled)] に設定します。
- c) [検出乗数 (Detection Multiplier)] の値を設定します。

セッションがダウンしたと BFD が宣言する前に失われた可能性のある連続するパケットの最小数を指定します。範囲は 1 ～ 50 パケットです。デフォルトは 3 です。

- d) [最小送信間隔 (Minimum Transit Interval)] の値を設定します。

送信されるパケットの最小間隔時間。指定できる範囲は 250 ～ 999 ミリ秒です。デフォルトは 250 です。

- e) [最大受信間隔 (Maximum Receive Interval)] の値を設定します。

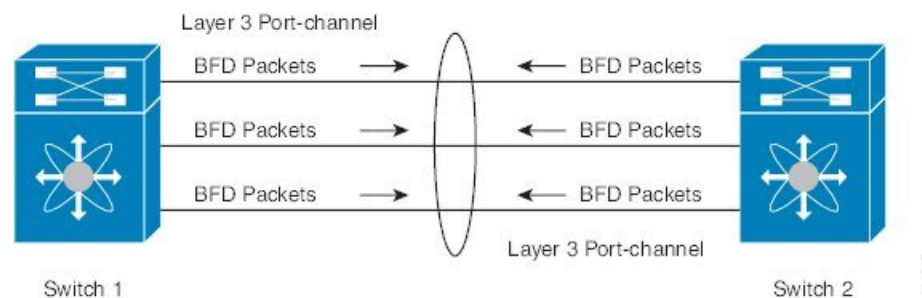
受信されたパケットの最大インターバル時間。指定できる範囲は 250 ～ 999 ミリ秒です。デフォルトは 250 です。

- f) [送信 (Submit)] をクリックします。

マイクロ BFD

Cisco APIC リリース 5.2(3) 以降、IETF RFC 7130 で定義されているように、APIC はマイクロ BFD をサポートします。Bidirectional Forwarding Detection (BFD) がポートチャネルで設定されている場合、キープアライブパケットは使用可能なメンバーリンクで送信されます。キープアライブパケットは残りのリンクを通過するだけであるため、単一のメンバーリンクの障害は検出されない場合があります。マイクロ BFD は、次の図に示すように、ポートチャネルの各メンバーリンクで個別の BFD セッションを確立する BFD の拡張機能です。

図 37: マイクロ BFD ポートチャネルでのセッション



リンク単位の BFD セッションがメンバーリンクで障害を検知すると、障害が発生したリンクは転送テーブルから削除されます。このメカニズムは、障害検出を高速化し、ポートチャネルで障害が発生したリンクを特定します。

に関する注意事項と制限事項 マイクロ BFD

- マイクロ BFD は、同じポートチャネルでマルチホップ BFD と同時に実行できますが、シングルホップ BFD では実行できません。
- マイクロ BFD は、シングルホップ BFD 実装です。スイッチのメインポートチャネルとスイッチのピアの間にレイヤ 2 スイッチが存在する場合は機能しません。

- マイクロ BFD は、第 1 世代のリーフ スイッチではサポートされていません。第 1 世代のスイッチは、PID (製品識別子) に -EX や -FX などのサフィックスが含まれていないスイッチです。
- マイクロ BFD は、ポートチャネル上のルーテッドインターフェイスでのみサポートされます。
- クライアントプロトコルは、マイクロ BFD が有効になっている同じポートチャネル上のサブインターフェイスで実行できます。
- マイクロ BFD は、FEX ポートまたはファブリック ポートではサポートされません。
- BFD エコーは、マイクロ BFD セッションではサポートされません。
- マイクロ BFD が有効になっているデュアル IP スタック ポートチャネル (IPv4 および IPv6) では、IPv4 アドレスまたは IPv6 アドレスのいずれかを使用してマイクロ BFD を設定する必要がありますが、両方は必須ではありません。IPv4 と IPv6 の両方のマイクロ BFD セッションを設定することはできません。
- Cisco APIC リリース 5.2(3) 以降、Cisco APIC では、L3 ポートチャネルのメインインターフェイスと同じ L3 ポートチャネル上のサブインターフェイスを使用できます。ただし、L3 ポートチャネルのメインインターフェイスを作成または削除すると、ポートチャネルの物理メンバーポートがフラップします。これにより、ポートチャネルサブインターフェイスがすでにアクティブな場合、トラフィックが失われます。

ポートチャネルでのマイクロ BFD の設定

この手順では、L3Outポートチャネルインターフェイスを有効に変更します。ポートチャネルの各メンバーリンクで個別のBFDセッションを確立します。マイクロ BFD

始める前に

- ダイレクトポートチャネルが L3Out インターフェイスに設定されています。

ステップ 1 [テナント (Tenants)] > [tenant_name] > [ネットワーキング (Networking)] > [L3Outs] > [L3Out_name] > [論理ノード プロファイル (Logical Node Profiles)] > [logical_node_profile_name] > [論理インターフェイス プロファイル (Logical Interface Profiles)] の順に移動します。

ステップ 2 変更する [論理インターフェイス プロファイル (Logical Interface Profile)] を選択します。

ステップ 3 [ルーテッドインターフェイス (Routed Interfaces)] タブを選択します。

マイクロ BFD は、ポートチャネル上のルーテッドインターフェイスでのみサポートされます。

ステップ 4 [ルーテッドインターフェイス (Routed Interfaces)] セクションで、既存のインターフェイスをダブルクリックして変更するか、[+] アイコンをクリックして新しいインターフェイスを論理インターフェイスプロファイルに追加します。

この手順の残りの手順では、既存の論理インターフェイスでのイネーブル化についてのみ説明します。マイクロ BFD 論理インターフェイス プロファイルに新しいインターフェイスを追加する場合は、[GUI を使用した L3Out のインターフェイスの変更 \(273 ページ\)](#) を参照してください。

ステップ 5 選択したインターフェイスの設定済みプロパティで、選択した [パス タイプ (Path Type)] が [ダイレクトポートチャネル (Direct Port Channel)] であることを確認します。

マイクロ BFD は、ポートチャネルでのみ適用できます。

ステップ 6 [Micro BFD の有効化 (Enable Micro BFD)] チェックボックスをオンにします。

ステップ 7 [Micro BFD 宛先アドレス (Micro BFD Destination Address)] にポートチャネルの宛先 IP アドレスを入力します。

ステップ 8 [Micro BFD 開始タイマー (秒) (Micro BFD Start Timer (sec))] に 60 ~ 3600 秒の値を入力します。

開始タイマーは、BFD セッションの確立を可能にするためにメンバーリンクでの BFD モニタリングのアクティブ化を遅延させます。タイマーはオプションです。タイマーが設定されていない場合、アクティブセッションは遅延しません。

ステップ 9 [送信 (Submit)] をクリックします。

次のタスク

次の例に示すように、CLI を使用してマイクロ BFD セッションを確認できます。

```
leaf4# show port-channel database interface port-channel 3
port-channel3
Last membership update is successful
4 ports in total, 4 ports up
First operational port is Ethernet1/44
Age of the port-channel is 0d:22h:46m:03s
Time since last bundle is 0d:22h:42m:43s
Last bundled member is Ethernet1/44
Ports: Ethernet1/41 [on] [up]
Ethernet1/42 [on] [up]
Ethernet1/43 [on] [up]
Ethernet1/44 [on] [up] *
```

```
leaf4# show bfd neighbors vrf tenant1:vrf1

OurAddr NeighAddr
LD/RD RH/RS Holddown(mult) State Int Vrf Type

2003:190:190:1::1 2003:190:190:1::2
1090519041/0 Up 6000(3) Up Po3 tenant1:vrf1 singlehop

2003:190:190:1::1 2003:190:190:1::2
1090519042/2148074790 Up 180(3) Up Eth1/44 tenant1:vrf1 singlehop

2003:190:190:1::1 2003:190:190:1::2
1090519043/2148074787 Up 180(3) Up Eth1/41 tenant1:vrf1 singlehop

2003:190:190:1::1 2003:190:190:1::2
1090519044/2148074789 Up 180(3) Up Eth1/43 tenant1:vrf1 singlehop

2003:190:190:1::1 2003:190:190:1::2
```

```
1090519045/2148074788 Up 180(3) Up Eth1/42 tenant1:vrf1 singlehop
```

OSPF 外部ルーテッド ネットワーク

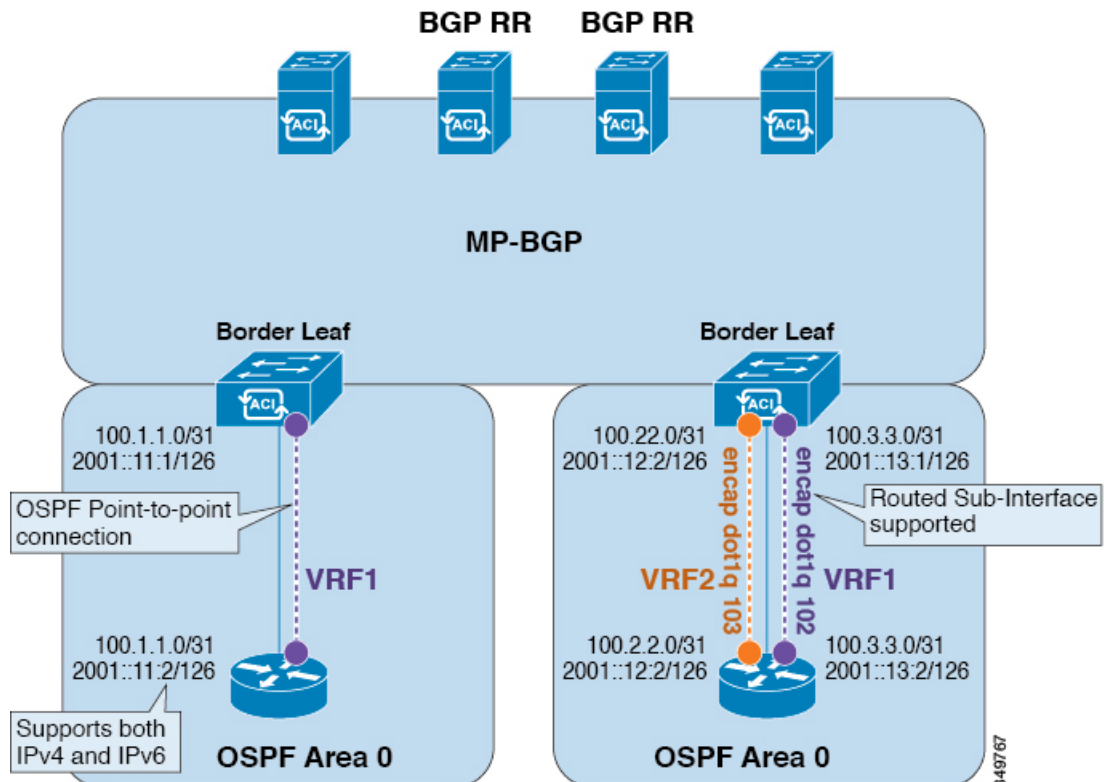
OSPF 外部ルーテッド ネットワークを設定するには、次の項の手順を使用します。

OSPF レイヤ 3 Outside 接続

OSPF レイヤ 3 Outside 接続は、標準または NSSA エリアです。バックボーン (エリア 0) エリアも、OSPF レイヤ 3 Outside 接続エリアとしてサポートされます。ACI は、IPv4 の OSPFv2 と IPv6 の OSPFv3 の両方をサポートします。OSPF レイヤ 3 Outside を作成するときに、OSPF バージョンを設定する必要はありません。インターフェイス プロファイル設定 (IPv4 または IPv6 アドレッシング) に基づいて、正しい OSPF プロセスが自動的に作成されます。IPv4 と IPv6 の両方のプロトコルが同じインターフェイス (デュアルスタック) でサポートされますが、2 つの個別インターフェイス プロファイルを作成する必要があります。

レイヤ 3 Outside 接続は、ルーテッドインターフェイス、ルーテッドサブインターフェイス、および SVI でサポートされます。SVI は、レイヤ 2 とレイヤ 3 両方のトラフィックで物理接続を共有する必要がある場合に使用されます。SVI は、物理ポート、ポートチャネル、および仮想ポートチャネル (vPC) でサポートされています。

図 38: OSPF レイヤ 3 Out 接続



SVI がレイヤ 3 Outside 接続に使用されると、外部ブリッジドメインが境界リーフスイッチに作成されます。外部ブリッジドメインは、ACI ファブリック上の 2 つの VPC スイッチ間の接続を可能にします。これにより、両方の VPC スイッチが、相互の、および外部 OSPF デバイスとの OSPF 隣接関係を確立できます。

ブロードキャストネットワークで OSPF を実行する場合、障害が発生したネイバーを検出する時間は dead 間隔（デフォルトは 40 秒）です。障害が発生した後でネイバー隣接関係を再確立する場合にも、代表ルータ（DR）の選定が原因で時間がかかる可能性があります。



- (注)
- 1 つの vPC ノードへのリンクまたはポートチャネルに障害が発生しても、OSPF 隣接関係がダウンすることはありません。OSPF 隣接関係は、その他の vPC ノードを介してアクセスできる外部ブリッジドメインによりアップ状態を維持することができます。
 - OSPF 時間ポリシーまたは BGP、OSPF、または EIGRP アドレスファミリーポリシーが L3Out に適用されると、次の動作を観察できます。
 - L3Out とポリシーが同じテナントで定義されている場合、動作に変更はありません。
 - 共通テナント以外のユーザーテナントで L3Out が設定されている場合、L3Out VRF インスタンスは共通テナントに解決され、ポリシーが共通テナントで定義されている場合、デフォルト値のみが適用されます。ポリシーの変更は有効になりません。
 - 境界リーフスイッチが 2 つの外部スイッチと OSPF 隣接関係を形成し、2 つのスイッチの 1 つでルート損失が発生し、隣接スイッチでは発生しない場合、Cisco ACI 境界リーフスイッチは両方のネイバーのルートを再コンバージェンスします。

GUI を使用した管理テナントの OSPF L3Out の作成

- ルータ ID と論理インターフェイスプロファイルの IP アドレスが異なっていて重複していないことを確認します。
- 次の手順は、管理テナントの OSPF L3Out を作成するためのものです。テナントの OSPF L3Out を作成するには、テナントを選択し、テナント用の VRF を作成する必要があります。
- 詳細については、『*Cisco APIC and Transit Routing*』を参照してください。

ステップ 1 メニューバーで、[Tenants] > [mgmt] の順に選択します。

ステップ 2 [ナビゲーション (Navigation)] ペインで、[ネットワークング (Networking)] > [L3Outs] を展開します。

ステップ 3 [L3Outs] を右クリックし、[L3Out の作成 (Create L3Out)] をクリックします。

[L3Out の作成 (Create L3Out)] ウィザードが表示されます。

ステップ 4 [L3Out の作成 (Create L3Out)] ウィザードの [識別 (Identity)] ウィンドウで、次の操作を実行します。

- a) [Name] フィールドに、名前 (RtdOut) を入力します。
- b) [VRF] フィールドのドロップダウンリストから、VRF (inb) を選択します。
(注) このステップでは、ルーテッド Outside をインバンド VRF に関連付けます。
- c) [L3 ドメイン (L3 Domain)] ドロップダウンリストから、適切なドメインを選択します。
- d) [OSPF] チェックボックスをオンにします。
- e) [OSPF Area ID] フィールドに、エリア ID を入力します。
- f) [OSPF Area Control] フィールドで、適切なチェックボックスをオンにします。
- g) [OSPF Area Type] フィールドで、適切なエリア タイプを選択します。
- h) [OSPF Area Cost] フィールドで、適切な値を選択します。
- i) [次へ (Next)] をクリックします。

[ノードとインターフェイス (Nodes and Interfaces)] ウィンドウが表示されます。

ステップ 5 [ノードとインターフェイス (Nodes and Interfaces)] ウィンドウで、次の操作を実行します。

- a) [デフォルトを使用 (Use Defaults)] ボックスをオフにします。
これにより、[ノードプロファイル名 (Node Profile Name)] フィールドを編集できます。
- b) [ノード プロファイル名 (Node Profile Name)] フィールドに、ノードプロファイルの名前を入力します (borderLeaf)。
- c) [Node ID] フィールドで、ドロップダウンリストから、最初のノードを選択します (leaf1)。
- d) [Router ID] フィールドに、一意のルータ ID を入力します。
- e) ループバックアドレスにルータ ID を使用しない場合は、[ループバックアドレス (Loopback Address)] フィールドで別の IP アドレスを使用するか、空のままにします。
(注) [ルータ ID (Router ID)] フィールドに入力したエン트리と同じ内容が [ループバック アドレス (Loopback Address)] フィールドに自動で入力されます。これは以前のビルドでの [ループバックアドレスのルータ ID の使用 (Use Router ID for Loopback Address)] と同等です。ループバック アドレスにルータ ID を使用しない場合は、別の IP アドレスを使用するか、このフィールドを空のままにします。
- f) 必要に応じて、このノードの [インターフェイス (Interface)]、[IP アドレス (IP Address)]、[インターフェイス プロファイル名 (Interface Profile Name)]、および [MTU] フィールドに適切な情報を入力します。
- g) [ノード (Nodes)] フィールドで、[+] アイコンをクリックして、別のノードの 2 番目のフィールドセットを追加します。
(注) 2 つ目のノード ID を追加します。
- h) [Node ID] フィールドで、ドロップダウンリストから、最初のノードを選択します (leaf1)。
- i) [Router ID] フィールドに、一意のルータ ID を入力します。

- j) ループバックアドレスにルータ ID を使用しない場合は、[ループバックアドレス (Loopback Address)] フィールドで別の IP アドレスを使用するか、空のままにします。

(注) [ルータ ID (Router ID)] フィールドに入力したエントリと同じ内容が [ループバック アドレス (Loopback Address)] フィールドに自動で入力されます。これは以前のビルドでの [ループバック アドレスのルータ ID の使用 (Use Router ID for Loopback Address)] と同等です。ループバック アドレスにルータ ID を使用しない場合は、別の IP アドレスを使用するか、このフィールドを空のままにします。

- k) 必要に応じて、このノードの [インターフェイス (Interface)]、[IP アドレス (IP Address)]、[インターフェイス プロファイル名 (Interface Profile Name)]、および [MTU] フィールドに適切な情報を入力します。
- l) [次へ (Next)] をクリックします。
- [プロトコル (Protocols)] ウィンドウが表示されます。

ステップ 6 [プロトコル (Protocols)] ウィンドウの [ポリシー (Policy)] 領域で、[デフォルト (default)] をクリックし、[次 (Next)] をクリックします。

[外部 EPG (External EPG)] ウィンドウが表示されます。

ステップ 7 [外部 EPG (External EPG)] ウィンドウで次のアクションを実行します。

- a) [Name] フィールドに、外部ネットワークの名前 (extMgmt) を入力します。
- b) [すべての外部ネットワークのデフォルト EPG (Default EPG for all external network)] フィールドをオフにします。

[サブネット (Subnets)] 領域が表示されます。

- c) [+] をクリックして [サブネットの作成 (Create Subnet)] ダイアログ ボックスにアクセスします。
- d) [サブネットの作成 (Create Subnet)] ダイアログ ボックスで、[IP アドレス (IP address)] フィールドに、サブネットの IP アドレスとマスクを入力します。
- e) [Scope] フィールドで、目的のチェックボックスをオンにします。[OK] をクリックします。
- f) [外部 EPG (External EPG)] ダイアログ ボックスで、[完了 (Finish)] をクリックします。

(注) [作業 (Work)] ペインの [L3Outs] 領域に、[L3Out] アイコン (RtdOut) が表示されます。

EIGRP 外部ルーテッド ネットワーク

EIGRP 外部ルーテッド ネットワークを設定するには、次の項の手順を使用します。

EIGRP レイヤ 3 Outside 接続について

この例は、Cisco APIC を使用して、拡張内部ゲートウェイルーティングプロトコル (EIGRP) を設定する方法を示しています。次の情報は、EIGRP を設定するときに適用されます:

- テナント、VRF、およびブリッジドメインがすでに作成されている必要があります。
- レイヤ 3 外部テナント ネットワークがすでに設定されている必要があります。
- 外部ルーテッドのルート制御プロファイルがすでに設定されている必要があります。
- EIGRP VRF ポリシーは EIGRP ファミリ コンテキスト ポリシーと同じです。
- EIGRP はエクスポート ルート制御プロファイルをサポートしています。ルート制御に関する設定はすべてのプロトコルで共通です。

サブネット ルートをネットワーク レベルのルートへ自動的に要約するよう (ルート要約)、EIGRP を設定できます。たとえば、192.31.7.0 のサブネットが設定されているインターフェイス上で、サブネット 131.108.1.0 が 131.108.0.0 としてアドバタイズされるように設定することができます。自動集約は、EIGRP プロセスに設定されているネットワーク ルータ設定コマンドが 2 つまたはそれ以上ある場合に実行されます。デフォルトでは、この機能は有効です。詳細については、「*Route Summarization*」を参照してください。

EIGRP プロトコルのサポート

EIGRP プロトコルは、Cisco Application Centric Infrastructure (ACI) ファブリック内の他のルーティング プロトコルと同様にモデル化されています。

サポートされる機能

サポートされる機能は次のとおりです。

- IPv4 および IPv6 ルーティング
- 各アドレス ファミリの仮想ルーティングおよび転送 (VRF) とインターフェイスの制御
- ノード間の OSPF による再配布
- VRF ごとのデフォルト ルート リーク ポリシー
- パッシブ インターフェイスおよびスプリット ホライズンのサポート
- エクスポートされたルートにタグを設定するためのルート マップ制御
- EIGRP インターフェイス ポリシーの帯域幅および遅延設定オプション
- 認証サポート

サポートされない機能

次の機能はサポートされていません。

- スタブ ルーティング
- BGP 接続に使用される EIGRP
- 同じノード上の複数の EIGRP L3extOut

- インターフェイスごとの集約 (EIGRP サマリー ポリシーは、L3Out で設定されたすべてのインターフェイスに適用されます)
- インターフェイスごとのインポートおよびエクスポート用配布リスト

EIGRP 機能のカテゴリ

EIGRP の機能は、次のように大きく分類できます。

- プロトコル ポリシー
- L3extOut の設定
- インターフェイス設定
- ルート マップ サポート
- デフォルト ルート サポート
- 中継サポート

EIGRP をサポートしているプライマリ管理対象オブジェクト

次のプライマリ管理対象オブジェクトは、EIGRP サポートを提供します。

- **EIGRP アドレス ファミリ コンテキスト ポリシー** `eigrpCtxAfPol` : `fvTenant` (テナント/プロトコル) で設定されているアドレス ファミリ コンテキスト ポリシー
- `fvRsCtxToEigrpCtxAfPol` : 所定のアドレス ファミリ (IPv4 または Ipv6) についての VRF から `eigrpCtxAfPol` への関係。関係は、アドレス ファミリごとに 1 つのみ存在できます。
- `eigrpIfPol` : `fvTenant` で設定される EIGRP インターフェイス ポリシー。
- `eigrpExtP` : L3extOut 上で EIGRP のフラグを有効にします。
- `eigrpIfP` : `l3extLIIfP` に接続された EIGRP インターフェイス プロファイル。
- `eigrpRsIfPol` : EIGRP インターフェイス プロファイルから `eigrpIfPol` への関係。
- `Defrtleak` : L3extOut 下のデフォルト ルート リーク ポリシー。

テナントでサポートされる EIGRP プロトコル ポリシー

テナント下では次の EIGRP プロトコル ポリシーがサポートされます。

- **EIGRP インターフェイス ポリシー** (`eigrpIfPol`) : インターフェイス上の所定のアドレス ファミリに適用される設定が含まれます。インターフェイス ポリシーでは次の設定が可能です。
 - 秒単位の `hello` 間隔
 - 分単位の `hold` 間隔
 - 次のインターフェイス制御フラグのうち 1 つ以上。

- スプリット ホライズン
 - パッシブ
 - ネクスト ホップ セルフ
- **EIGRP アドレス ファミリ コンテキスト ポリシー (eigrpCtxAfPol)** : 所定の VRF 内の所定のアドレスファミリの設定が含まれます。eigrpCtxAfPol は、テナントプロトコルポリシー下で設定され、テナント下の 1 つ以上の VRF に適用できます。eigrpCtxAfPol は、VRF-per-address ファミリの関係を通して VRF で有効にできます。所定のアドレスファミリに関係がない場合、あるいは関係に記述されている eigrpCtxAfPol が存在しない場合は、[共通] テナント下に作成されたデフォルトの VRF ポリシーがそのアドレスファミリに使用されます。

次の設定では、eigrpCtxAfPol で許可されます。

- 内部ルートのアドミニストレーティブ ディスタンス
- 外部ルートのアドミニストレーティブ ディスタンス
- 最大許容 ECMP パス数
- アクティブ タイマー間隔
- メトリック バージョン (32 ビット/64 ビット メトリック)

ガイドラインと EIGRP を設定するときの制限事項

EIGRP を設定する場合は、次の注意事項に従ってください。

- 外部同じレイヤ 3 の EIGRP および BGP を設定することはサポートされていません。
- 外部同じレイヤ 3 の EIGRP や OSPF を設定することはサポートされていません。
- 1 つ EIGRP レイヤ 3 Out VRF あたりノードごとでできますががあります。ノードで複数の Vrf を導入している場合、自身レイヤ 3 Out 各 VRF ことができます。
- 複数の EIGRP ピア、1 つレイヤ 3 Out からサポートされます。これにより、1 つレイヤ 3 Out と同じノードから複数の EIGRP デバイスに接続できます。

次の設定では、EIGRP ネイバーがフラップします。

- VRF の EIGRP アドレス ファミリ コンテキストによるアドミニストレーティブ ディスタンスまたはメトリック スタイル (ワイド/ナロー) の変更
- 内部で使用されるテーブルマップを更新する次の設定を設定します。
 - VRF のルート タグの変更
 - EIGRP L3Out と同じ境界リーフ スイッチ上の同じ VRF 内の OSPF L3Out のインポート方向ルート制御の設定 (たとえば、ルート制御適用「インポート」オプションの有効化または無効化、インポート方向)。この機能は EIGRP ではサポートされ

ていないため、このような設定はEIGRPL3Out自体では許可されないことに注意してください。ただし、OSPF L3Out の設定は、同じ VRF とリーフ スイッチの EIGRP L3Out に影響を与えます。これは、OSPF のインポートルート制御が、同じ境界リーフ スイッチ上の同じ VRF の EIGRP と他の目的で共有されるテーブルマップを使用するためです。

GUI を使用したEIGRPの設定

- ステップ 1** メニュー バーで、[Tenants]> [All Tenants] の順に選択します。
- ステップ 2** **Work** ウィンドウで、テナントをダブルクリックします。
- ステップ 3** [ナビゲーション (Navigation)] ペインで、[Tenant_name]> [ポリシー (Policies)]> [プロトコル (Protocol)]> [EIGRP] を展開します。
- ステップ 4** 右クリックして **EIGRP アドレス ファミリ コンテキスト]** を選択します **EIGRP アドレス ファミリ コンテキストのポリシーを作成** します。
- ステップ 5** **Create EIGRP Address Family Context Policy** ダイアログボックスで、以下の操作を実行します:
- Name** フィールドに、コンテキスト ポリシーの名前を入力します。
 - アクティブ間隔 (分)** フィールドで、インターバル タイマーを選択します。
 - 外部距離**、および **内部距離** フィールドで、適切な値を選択します。
 - パスの上限** フィールドで、[インターフェイス (ノードごと/リーフ スイッチごと) 間の値を適切なロード バランシングを選択します。
 - メトリック スタイル** フィールドで、適切なメトリック スタイルを選択します。[Submit] をクリックします。
- Work** ウィンドウに、コンテキスト ポリシーの詳細が表示されます。
- ステップ 6** VRF のコンテキスト ポリシーを適用する、 **ナビゲーション]** ペインで、[展開 ネットワーキング > Vrf]。
- ステップ 7** 適切な VRF を選択し、[作業 (Work)] ペインの [ポリシー (Policy)] タブで [アドレス ファミリごとの EIGRP コンテキスト (EIGRP Context Per Address Family)] を展開します。
- ステップ 8** **EIGRP アドレス ファミリ タイプ** ドロップダウンリスト、IP バージョンを選択します。
- ステップ 9** **EIGRP アドレス ファミリ コンテキスト** ドロップダウンリスト、コンテキスト ポリシーを選択します。Update をクリックし、Submit をクリックします。
- ステップ 10** レイヤ 3 Out 内の EIGRP を有効にするには、[ナビゲーション (Navigation)] ペインで、[ネットワーキング (Networking)]> [L3Out] をクリックして目的のレイヤ 3 外部ネットワークをクリックします。
- ステップ 11** [作業 (Work)] ペインの [ポリシー (Policy)] タブで [EIGRP] のチェックボックスをオンにして EIGRP 自律システム番号を入力します。[送信 (Submit)] をクリックします。
- ステップ 12** EIGRP インターフェイス ポリシーを作成するには、[ナビゲーション (Navigation)] ペインで、[Tenant_name]> [ポリシー (Policies)]> [プロトコル (Protocol)]> [EIGRP] をクリックして次のアクションを実行します。
- 右クリックして **EIGRP インターフェイス**、をクリックし、**EIGRP インターフェイス ポリシーの作成** します。

- b) **Create EIGRP Interface Policy** ダイアログボックスで、**Name** フィールドにポリシーの名前を入力します。
- c) **制御状態** フィールドは、1 つまたは複数の制御を有効にする目的のチェック ボックスをチェックします。
- d) **Helloインターバル (秒)** フィールドで、目的の間隔を選択します。
- e) **保留間隔 (秒)** フィールドで、目的の間隔を選択します。[Submit] をクリックします。`
- f) **Bandwidth** フィールドで、目的の帯域幅を選択します。
- g) **遅延** フィールドで、10 マイクロ秒またはピコセル秒で、目的の遅延を選択します。

作業] ペインで、EIGRP インターフェイス ポリシーの詳細が表示されます。

ステップ 13 ナビゲーション] ペインで、適切な外部ルーテッドネットワークの EIGRP が有効になってクリック展開論理ノード **プロファイル** および次の操作の実行します。

- a) 適切なノードとそのノードの下にインターフェイスを展開します。
- b) インターフェイスを右クリックし、をクリックして **EIGRP インターフェイス プロファイル** の作成します。
- c) **EIGRP インターフェイス プロファイル** の作成 ダイアログボックスで、**EIGRP ポリシー** フィールドで、目的の EIGRP インターフェイス ポリシーを選択します。[Submit] をクリックします。`

(注) EIGRP の VRF ポリシーおよび EIGRP インターフェイス ポリシーは、EIGRP が有効になっているときに使用するプロパティを定義します。EIGRP の VRF ポリシーおよび EIGRP インターフェイス ポリシーは、新しいポリシーを作成しない場合にもデフォルトポリシーとして利用できます。したがって、ポリシーのいずれかを明示的に選択しない場合は、EIGRP が有効になっているとき、デフォルトのポリシーが自動的に利用されます。

これで EIGRP の設定は完了です。



第 20 章

ルート集約

この章は、次の内容で構成されています。

- [はじめに \(337 ページ\)](#)
- [L3Out 外部 EPG レベルでのルート集約 \(338 ページ\)](#)
- [VRF レベルでのルート フィルタリングと集約 \(338 ページ\)](#)
- [注意事項と制約事項 \(341 ページ\)](#)
- [GUI を使用した L3out 外部 EPG レベルでのルート要約の設定 \(342 ページ\)](#)
- [GUI を使用した VRF でのルート制御ポリシーの構成 \(344 ページ\)](#)

はじめに

ルート集約では、多数の具体的なアドレスを1つのアドレスに置き換えることで、ルートテーブルが簡素化します。たとえば、10.1.1.0/24、10.1.2.0/24、10.1.3.0/24 は 10.1.0.0/16 で置き換えることができます。ルート集約ポリシーにより、ボーダーリーフスイッチとそのネイバーリーフスイッチの間でルートを効率的に共有することができます。

Cisco APIC 5.2(4) リリース以降、ACI では 2 つの形式のルート集約がサポートされています。

- L3Out 外部 EPG レベルでのルート要約：

L3Out 外部 EPG レベルでのルート集約のこの設定により、外部 L3Out ピアのみへのルート集約が可能になります。

- VRF レベルでのルート フィルタリングと集約：

Cisco APIC 5.2(4) リリース以降、Cisco APIC は、ファブリックでアドバタイズされるルートのルートフィルタリングと集約を実行して、ファブリックのスケール要件を軽減するオプションも提供します。この機能は、VRF レベルで構成されます。VRF レベルでルートの集約を有効にすると、ACIファブリックへのルートの集約、および外部BGPL3Outピアへのルートの集約を実現するのに役立ちます。

上記の両方の要約形式の詳細については、以降のセクションで説明します。

L3Out 外部 EPG レベルでのルート集約

BGP、OSPF、あるいはEIGRPのルート集約ポリシーは、ブリッジドメインまたは中継サブネットに適用されます。OSPFでは、エリア間ルート集約と外部ルート集約がサポートされません。集約ルートはエクスポートされます。ファブリック内でのアドバタイズは行われません。

L3Out 外部 EPG でルート集約を有効にすると、ACI ファブリック内ではなく、L3Out ピアのみへのルート集約を実現できます。ACI ファブリックおよび外部 L3Out ピアへのルートの集約を実現するには、[VRF レベルでのルートフィルタリングと集約 \(338 ページ\)](#) を参照してください。

また、このルート集約が設定されている場合、集約プレフィックスは外部 L3Out ピアにアドバタイズされ、より具体的なプレフィックスは L3Out ピアにアドバタイズされません。

VRF レベルでのルート フィルタリングと集約

デフォルトでは、境界リーフ ノードは直接接続されたスタティック ルート、およびルーティング プロトコルから多くのプレフィックスを受け取り、これらのプレフィックスは MP-BGP で再配布され、これらのプレフィックスはすべてのリーフ スイッチとスパイン スイッチにアドバタイズされます。リーフ スイッチは、LPM で構成された VRF のすべてのプレフィックスをプログラムします。この機能を使用すると、管理者は VRF のプレフィックスを LPM テーブルに選択的にインポートしたり、VRF のプレフィックスを MP-BGP または L3Out ピアにエクスポートしたりできます。

Cisco APIC 5.2(4) リリース以降、Cisco APIC は、ファブリックでアドバタイズされるルートを要約またはフィルタリングして、ファブリックのスケール要件を軽減するオプションを提供します。

以下のルート制御ポリシーが VRF 配下に追加されます。

BGP ルート集約ポリシー

このポリシーを使用すると、サブネットが外部ルーターから直接学習されるかどうかに関係なく、プレフィックスをより大きなサブネットに集約できます。ポリシーには、集約されたサブネットのみをアドバタイズするか、サブネット内のすべてのプレフィックスをアドバタイズするかを指定するオプションが用意されています。このポリシーは、L3Out ピアと MP-BGP の集約を制御します。

以下の構成がこのポリシーで使用可能です。

- ノード：ルート プロファイルを適用する必要がある境界リーフ ノードのリスト。
 - ポリシーを展開するには、少なくとも1つの境界リーフを構成する必要があります。
 - スパイン スイッチはこのポリシーでサポートされていません。
 - VRF、境界リーフ ペアごとに複数のポリシーを設定できます。

- このポリシーはvPC非認識です。したがって、vPCペアのノード間で異なるポリシーを構成できます。
- このポリシーは、ユニキャスト アドレス ファミリーにのみ適用されます。
- サブネット：各サブネットがテナントの下で構成された BGP ルート要約ポリシーを指すサブネットのリスト。
 - ポリシーを展開するには、少なくとも1つのサブネットを構成する必要があります。
 - 同じノードの異なるルート集約ポリシーに関連付けられているサブネット間に重複があってはなりません。
- BGPルート要約ポリシーの作成（テナントの下）：集約されたルートのみをアドバタイズするための新しいオプションが提供されています。ルート集約ポリシー制御状態オプションを使用して、ピアへの集約プレフィックスのみのアドバタイズを有効にするか、ピアへの集約プレフィックスと特定のプレフィックスの両方のアドバタイズを許可することができます。
- ルート集約が VRF と l3extSubnet の同じサブネットに構成されている場合、障害が発生します。したがって、ファブリックのアップグレードまたはスイッチのリロードの前に、この障害をクリアすることを強くお勧めします。

BGP ルート集約ポリシーを設定する手順は、[GUI を使用した VRF でのルート制御ポリシーの構成 \(344 ページ\)](#) で提供されています。

VRF 内インポート ルート制御ポリシー

このポリシーにより、ルーティング テーブルに登録するプレフィックスを制御できます。

以下の構成がこのポリシーで使用可能です。

- ノード：ルート プロファイルを適用する必要があるリーフ ノードのリスト。
 - ポリシーを展開するには、少なくとも1つのリーフを構成する必要があります。
 - このポリシーでは、スパイン スイッチはサポートされていません。
 - VRF、リーフ ノードに設定されているインポート ルート制御ポリシーがない場合、MP-BGP からの VRF のすべてのプレフィックスがノードのルーティング テーブルに登録されます。
 - このポリシーはvPC非認識です。したがって、vPCペアのノード間で異なるポリシーを構成できます。
- ルート マップ: テナントの既存のルート プロファイル構成を構成するのと同じ方法で構成します。次のルート マップの `match` 句と `set` 句は、インポート ルート制御構成に適用されます。

Match 句：

- IP プレフィックス リスト
- コミュニティ
- 拡張コミュニティ (マッチオンカラー拡張コミュニティの一致はサポートされていません)
- 正規表現コミュニティ
- 正規表現拡張コミュニティ
- 正規表現 AS パス

Set 句 :

- コミュニティ
- Extended Community
- タグ
- 重量
- プリファレンス
- メトリック

ルート集約またはファブリック エクスポート制御が MP-BGP のプレフィックスを抑制するように設定されている場合、このポリシーは、リーフのインポートルート制御ポリシーによって許可されている場合でも、レシーバー リーフのルーティング テーブルで更新されません。

VRF 間インポート ルート制御ポリシーを設定する手順は、[GUI を使用した VRF でのルート制御ポリシーの構成 \(344 ページ\)](#) で提供されています。

VRF エクスポート ルート制御ポリシー

このポリシーにより、ファブリックにアダプタイズされるプレフィックスを制御できます。

以下の構成がこのポリシーで使用可能です。

- ノード : ルート プロファイルを適用する必要がある境界リーフ ノードのリスト。
 - ポリシーを展開するには、少なくとも1つの境界リーフを構成する必要があります。
 - スパイン スイッチはこのポリシーでサポートされていません。
 - VRF、ボーダー リーフ ペアに設定されているエクスポート ルート制御ポリシーがない場合、ボーダー リーフから MP-BPG への VRF のすべてのプレフィックスがアダプタイズされます。
 - このポリシーはvPC非認識です。したがって、vPCペアのノード間で異なるポリシーを構成できます。

- ルートマップ: テナントの既存のルートプロファイル構成を構成するのと同じ方法で構成します。次のルートマップの `match` および `set` 句は、エクスポートルート制御設定に適用されます。

Match 句 :

- IP プレフィックス リスト
- コミュニティ
- 拡張コミュニティ (マッチオンカラー拡張コミュニティの一致はサポートされていません)
- 正規表現コミュニティ
- 正規表現拡張コミュニティ

Set 句 :

- コミュニティ
- 拡張コミュニティ (拡張コミュニティを **None** に設定することを除く)
- 重量
- プリファレンス
- メトリック

VRF エクスポートルート制御ポリシーを設定する手順は、[GUIを使用したVRFでのルート制御ポリシーの構成 \(344 ページ\)](#) に提供されています。

注意事項と制約事項

外部 EPG で設定されたルート集約ポリシーにより、同じ境界リーフ スイッチに接続され、同じ VRF にあるすべての BGP ピアに集約されたプレフィックスがアドバタイズされます。これには、同じ境界リーフ スイッチと VRF 条件が満たされている場合に、異なる L3Out に属する BGP ピアが含まれます。

この動作を行わず、集約ルートを受信する BGP ピアを制限する場合は、該当する L3Out のアウトバウンドルートマップを使用して、該当するルートをブロックします。

GUI を使用した L3out 外部 EPG レベルでのルート要約の設定

このセクションでは、L3Out 外部 EPG に関連付けられたルート集約を設定する手順について説明します。これらの構成手順を使用してルート集約を有効にすると、ACI ファブリック内ではなく、L3Out ピアのみへのルート集約を実現できます。

また、ルート集約が構成されている場合、集約プレフィックスは外部 L3Out ピアにアダプタイズされ、より具体的なプレフィックスは L3Out ピアにアダプタイズされません。

ACI ファブリックおよび外部 L3Out ピアへの ルートの集約を達成するには、[GUI を使用した VRF でのルート制御ポリシーの構成 \(344 ページ\)](#) を参照してください。

始める前に

次の設定のそれぞれに対して、L3 Out がすでに作成されていること。L3 Out については、外部ルーテッドネットワーク、サブネット、およびルート集約ポリシーを作成することができます。

ステップ 1 次のように、GUI を使用して BGP ルート集約を設定します:

- a) メニューバーで、**[テナント (Tenants)] > common** を選択します。
- b) **[ナビゲーション (Navigation)]** ペインで、**[ネットワーキング (Networking)] > [L3Outs]** を展開します。
- c) **[L3Outs]** を右クリックし、**[L3Out の作成 (Create L3Out)]** を選択します。
[L3Out の作成 (Create L3Out)] ウィザードが表示されます。
- d) **[作業 (Work)]** ペインで、必要な情報 ([名前 (Name)]、[VRF]、および [L3 ドメイン (L3 Domain)]) を入力し、[BGP] の横にあるチェックボックスをオンにします。
- e) **[次へ (Next)]** をクリックします。
[ノードとインターフェイス (Nodes and Interfaces)] ウィンドウが表示されます。
- f) **[ノードとインターフェイス (Nodes and Interfaces)]** ウィンドウで、適切なフィールドに入力し、**[次へ (Next)]** をクリックします。
[プロトコル (Protocols)] ウィンドウが表示されます。
- g) **[プロトコル (Protocols)]** ウィンドウで、適切なフィールドに入力し、**[次 (Next)]** をクリックします。
[外部 EPG (External EPG)] ウィンドウが表示されます。
- h) **[名前 (Name)]** フィールドに名前を入力し、**[すべての外部ネットワークのデフォルト EPG (Default EPG for all external network)]** フィールドをオフにします。
[サブネット (Subnets)] フィールドが表示されます。
- i) **[ルート集約ポリシー (Route Summarization Policy)]** の上にある **[+]** をクリックします。
Create Subnet ダイアログボックスが表示されます。
- j) **Specify the Subnet** ダイアログボックスでは、次の方法で、ルート集約ポリシーをサブネットに関連付けることができます。

例 :

- IP アドレスを **IP Address** フィールドに入力します。
- **Export Route Control Subnet** の隣のチェック ボックスをオンにします。
- **External Subnets for the External EPG** の隣のチェック ボックスをオンにします。
- **BGP Route Summarization Policy** ドロップダウンメニューで、既存の (デフォルトの) ポリシーを選択する場合には **default** を、新しいポリシーを作成する場合には **Create BGP route summarization policy** を選択します。
- **Create BGP route summarization policy** を選択した場合には、**Create BGP Route Summarization Policy** ダイアログボックスが表示されます。[名前 (Name)]フィールドに名前を入力し、[AS-SET 情報の生成 (Generate AS-SET information)]で [制御状態 (Control State)]チェック ボックスをオンにし、[送信 (Submit)]をクリックして [OK]、[完了 (Finish)]をクリックします。

(注) [より詳細な制御状態をアドバタイズしない] オプションと [アドレス タイプ制御 (Address Type Contr)]オプションは、ポリシーが VRF ルート制御ポリシーに適用されている場合にのみ適用されます。ここでは、AF Ucast と AF Mcast の両方がデフォルトで有効になっています。

ステップ 2 GUI を使用して、次のように OSPF のエリア間および外部の集約を設定します。

- a) メニューバーで、[テナント (Tenants)]> **common** を選択します。
- b) [ナビゲーション (Navigation)]ペインで、[ネットワークング (Networking)]> [L3Outs]> [外部 EPG (External EPGs)]を展開し、設定済みの外部 EPG をクリックします。
設定された外部 EPG の概要情報が表示されます。
- c) 作業ウィンドウで、+ 記号 (**Route Summarization Policy** の上) をクリックします。
Create Subnet ダイアログボックスが表示されます。
- d) **Specify the Subnet** ダイアログボックスでは、次の方法で、ルート集約ポリシーをサブネットに関連付けることができます。

例 :

- IP アドレスを **IP Address** フィールドに入力します。
- **Export Route Control Subnet** の隣のチェック ボックスをオンにします。
- **External Subnets for the External EPG** の隣のチェック ボックスをオンにします。
- **OSPF Route Summarization Policy** ドロップダウンメニューで、既存の (デフォルトの) ポリシーを選択する場合には **default** を、新しいポリシーを作成する場合には **Create OSPF route summarization policy** を選択します。
- **Create OSPF route summarization policy** を選択した場合には、**Create OSPF Route Summarization Policy** ダイアログボックスが表示されます。名前を **Name** フィールドに入力し、**Inter-Area Enabled** の隣のチェック ボックスをオンにし、**Cost** の隣に値を入力し、**SUBMIT** をクリックします。

ステップ 3 次のように、GUI を使用して EIGRP の集約を設定します。

- a) メニューバーで、**Tenants > common** を選択します。

- b) [ナビゲーション (Navigation)] ペインで、[ネットワークング (Networking)] > [L3Outs] を展開します。
- c) [L3Outs] を右クリックし、[L3Out の作成 (Create L3Out)] を選択します。
[L3Out の作成 (Create L3Out)] ダイアログ ボックスが表示されます。
- d) 作業ウィンドウで、**EIGRP** の隣のチェック ボックスをオンにします。
- e) **Name** フィールドに名前を入力し、**NEXT** をクリックします。
External EPG Networks ダイアログボックスが表示されます。
- f) 作業ウィンドウで、+ 記号をクリックします。
Define an External Network ダイアログボックスが表示されます。
- g) **Name** フィールドに名前を入力し、+ 記号 (**Route Summarization Policy** の上のもの) をクリックします。
Create Subnet ダイアログボックスが表示されます。
- h) **Specify the Subnet** ダイアログボックスでは、次の方法で、ルート集約ポリシーをサブネットに関連付けることができます。

例 :

- IP アドレスを **IP Address** フィールドに入力します。
- **Export Route Control Subnet** の隣のチェック ボックスをオンにします。
- **External Subnets for the External EPG** の隣のチェック ボックスをオンにします。
- **EIGRP Route Summarization** の隣のチェック ボックスをオンにし、**OK** をクリックし、**OK** をクリックし、**FINISH** をクリックします。

GUI を使用した VRF でのルート制御ポリシーの構成

このセクションでは、VRF のルート集約を構成する手順について説明します。これには、ルート集約ポリシー、VRF 内インポートルート制御、および VRF エクスポートルート制御を構成する手順が含まれます。

このセクションの手順を使用してルートの集約を有効にすると、ACI ファブリックへのルートと、外部 BGP L3Out ピアへのルートの集約を実現できます。さらに、このセクションの手順を使用して設定されたルート集約では、有効になっている制御状態オプションに基づいて、より具体的なプレフィックスが集約プレフィックスと共にアドバタイズされる場合とされない場合があります。

ステップ 1 [テナント (Tenants)] > [tenant_name] > [ネットワークング (Networking)] > [VRF] > [vrf_name] に移動します。

ステップ 2 [VRF - vrf_name] 作業ペインで、[ルート コントロール (Route Control)] タブをクリックします。

ステップ 3 VRF レベルでルート フィルタリングと集約をどのように設定するかを決定します。

- BGP ルート集約ポリシーを設定するには、[ステップ 4 \(345 ページ\)](#) に進みます。

- VRF 間インポート ルート制御ポリシーを設定するには、[ステップ 5 \(345 ページ\)](#) に進みます。
- VRF エクスポート ルート制御ポリシーを設定するには、[ステップ 6 \(345 ページ\)](#) に進みます。

ステップ 4 次のように、GUI を使用して、ルート集約ポリシーを構成します。

- a) [ルート集約ポリシー (Route Summarization Policy)] の上にある [+] をクリックします。
[ルート集約ポリシーの作成 (Create Route Summarization Route)] ダイアログボックスが表示されます。
- b) [名前] フィールドに名前を入力し、[ノード] リストからスイッチを選択します。
- c) [サブネット (Subnet)] の隣の [+] をクリックします。
[サブネットと要約ポリシーの関連付けの作成 (Create Association of Subnet to Summarization Policy)] ダイアログボックスが表示されます。
- d) [サブネット (Subnet)] フィールドに、IP アドレスを入力します。
- e) **BGP ルート サマリー ポリシー** リストからポリシーを選択します。
[ルート集約ポリシーの作成 (Create Route Summarization Route)] ダイアログボックスが表示されます。
- f) [名前 (Name)] フィールドに名前を入力し、適切な [制御状態 (Control State)] および [アドレス タイプ コントロール (Address Type Controls)] オプションを選択します。

BGP ルート集約ポリシー設定の [より詳細な制御状態をアドバタイズしない (Do not advertise more specifics control option)] オプションが有効になっている場合、集約プレフィックスはアドバタイズされ、より具体的なプレフィックスはピアにアドバタイズされません。[より詳細にアドバタイズしない (Do not advertise more specifics)] オプションが有効になっていない場合、集約プレフィックスとより詳細なプレフィックスの両方がピアにアドバタイズされます。

- g) [送信 (Submit)] をクリックして、以前の構成を確認します。

(注) 集約プレフィックスが L3Out ピアから、およびルート集約ポリシー構成を使用してボーダー リーフでローカルに発信された集約プレフィックスから学習される場合、ローカルで発信された集約プレフィックスよりも外部で学習された集約プレフィックスを BGP ベストパスとして優先する場合、L3Out ピアから発信されるすべてのルートは、32769 以上に設定する必要があります。

ステップ 5 次のように、GUI を使用して Intra-VRF インポート ルート構成ポリシーを設定します。

- a) [VRF 間インポート ルート構成ポリシー (Intra-VRF Import Route Configuration Policy)] の横にある [+] をクリックします。
[VRF インポート ルート制御ポリシーの作成 (Create VRF Import Route Control Policy)] ダイアログボックスが表示されます。
- b) [名前] フィールドに名前を入力し、[ノード] リストからスイッチを選択します。
- c) [インポートするルート プロファイル (Route Profile for Import)] リストからポリシーを選択します。
- d) [送信 (Submit)] をクリックします。

ステップ 6 次のように、GUI を使用して VRF エクスポート ルート構成ポリシーを構成します。

- a) **VRF エクスポート ルート構成ポリシー** の横にある [+] をクリックします。
[VRF エクスポート ルート コントロール ポリシーの作成 (Create VRF Export Route Control Policy)] ダイアログボックスが表示されます。
- b) [名前] フィールドに名前を入力し、[ノード] リストからスイッチを選択します。

- c) [エクスポートするルート プロファイル (Route Profile for Export)] リストからポリシーを選択します。
 - d) [送信 (Submit)] をクリックします。
-



第 21 章

ルート マップおよびルート プロファイル によるルート制御

この章は、次の内容で構成されています。

- [ルート制御プロファイル ポリシー \(347 ページ\)](#)
- [BGP ピアごとのルート制御について \(349 ページ\)](#)
- [明示的なプレフィクス リストでルート マップ/プロファイル \(354 ページ\)](#)
- [ルート制御プロトコル \(367 ページ\)](#)
- [MP-BGP のインターリーク再配布 \(370 ページ\)](#)

ルート制御プロファイルポリシー

ACI ファブリックは、ファブリックの内部と外部にアダプタイズされるルート用に、ルートマップの `set` 句もサポートします。ルートマップの `set` ルールは、ルート制御プロファイルポリシーとアクションルールプロファイルで設定されます。

ACI は以下の `set` オプションをサポートします。

表 11: アクションルールプロファイルのプロパティ (ルートマップの `set` 句)

プロパティ	OSPF	EIGRP	BGP	注
コミュニティの設定			○	標準コミュニティと拡張コミュニティをサポートします。
追加のコミュニティを設定			○	標準コミュニティと拡張コミュニティをサポートします。

プロパティ	OSPF	EIGRP	BGP	注
ルート タグ	はい	はい		BD のサブネットのみでサポートされます。中継プレフィックスには、常にタグ 4294967295 が割り当てられます。
優先順位			○	BGP ローカルプリファレンスを設定します。
メトリック	はい		はい	BGP の MED を設定します。EIGRP のメトリックを変更しますが、EIGRP 複合メトリックは指定できません。
メトリック タイプ	○			OSPF タイプ 1 と OSPF タイプ 2。

ルートプロファイルポリシーは、レイヤ 3 Outside 接続の下に作成されます。ルート制御ポリシーは、以下のオブジェクトで参照できます。

- テナント BD サブネット
- テナント BD
- 外部 EPG
- 外部 EPG のインポート/エクスポート サブネット

以下に、BGP のインポート ルート制御を使用し、2 つの異なるレイヤ 2 Outside から学習した外部ルートのローカルプリファレンスを設定する例を示します。AS300 への外部接続用のレイヤ 3 Outside 接続は、インポート ルート制御を適用して設定されています。アクションルールプロファイルの設定では、[Local Preference] ウィンドウの [Action Rule Profile] でローカルプリファレンスが 200 に設定されています。

レイヤ 3 Outside 接続の外部 EPG は、0.0.0.0/0 インポート集約ポリシーを使用してすべてのルートを許可するように設定されています。これは、インポート ルート制御が適用されていますが、どのプレフィックスもブロックされてはならないためです。ローカルプリファレンスの設定を許可するために、インポート ルート制御が適用されています。また、[Route Control Profile] ウィンドウの [External EPG] で [Action Rule Profile] を参照するルートプロファイルを使用して、別のインポート サブネット 151.0.1.0/24 が追加されています。

MP-BGP テーブルを表示するには、`show ip bgp vrf overlay-1` コマンドを使用します。スパインの MP-BGP テーブルには、プレフィックス `151.0.1.0/24` とローカルプリファレンス `200`、および `BGP 300` レイヤ 3 Outside 接続の境界リーフの次のホップが表示されます。

`default-import` と `default-export` という、2つの特殊なルート制御プロファイルがあります。名前 `default-import` および `default-export` を使用して設定すると、ルート制御プロファイルはインポートとエクスポート両方のレイヤ 3 Outside レベルで自動的に適用されます。`default-import` および `default-export` のルート制御プロファイルは、`0.0.0.0/0` 集約を使用して設定することはできません。

ルート制御プロファイルは、次の順序でファブリック ルートに適用されます。

1. テナント BD サブネット
2. テナント BD
3. レイヤ 3 Outside

ルート制御プロファイルは、次の順序で中継ルートに適用されます。

1. 外部 EPG プレフィックス
2. 外部 EPG
3. レイヤ 3 Outside

BGP ピアごとのルート制御について

ルート制御ポリシーは、外部ネットワークにアドバタイズされるルート（エクスポート）またはファブリックに許可されるルート（インポート）を決定します。Cisco Application Policy Infrastructure Controller (APIC) リリース 4.2(1) よりも前の Cisco APIC リリースでは、これらのポリシーを、L3Out プロファイル (l3extInstP) の下の L3Out レベル、または L3Out (l3extSubnet) の下の L3Out サブネットを介して設定するため、これらのポリシーは L3Out に含まれるすべてのノードまたはパス向けに設定されるプロトコルに適用されます。この設定では、L3Out に複数のノードプロファイルが設定され、それぞれに BGP ネイバーが指定された複数のノードまたはパスがあります。このため、個々のポリシーを各プロトコルエンティティに適用する方法はありません。

Cisco APIC リリース 4.2(1) 以降では、BGP ピアごとのルート制御機能が導入され、より詳細なルートのエクスポートおよびインポート制御が必要とされるこの状況に対処し始めています。

Cisco APIC リリース 6.0(1) 以降、一致ルールの作成中に `Match AS` パスパラメータを設定できます。1つのルートマップで、複数の AS パスアクセスリスト名を一致させることができます。

BGP ピアごとのルート制御に関するガイドラインと制約事項

BGP ピアごとのルート制御機能のガイドラインと制約事項を次に示します。

- テナントの BGP ピアごとに使用されるルート プロファイルを設定する必要があります。
- ルートマップの一致を設定する方法、ルールまたはルートプロファイルを設定する方法、およびこれらの各コンポーネントの動作は、以前のリリースから変更されていません。
- この機能のルートプロファイルは、[ルーティングポリシーのみ照合 (Match Routing Policy Only)] (グローバルポリシー) にのみ設定できます。ルートプロファイルは、BGP ピアごとのルートマップを生成する唯一の情報源です。この機能のルートプロファイルを [プレフィックスおよびルーティングポリシーの照合 (Match Prefix and Routing Policy)] に設定することはできません。

また、BD サブネットをエクスポートする場合は、プレフィックス リストで BD サブネットを明示的に指定する必要があります。

- 特定の方向の BGP ピアに関連付けることができるルート制御プロファイルは 1 つだけです。
- デフォルト ポリシーは、これらのルートマップではサポートされていません (名前付きルート プロファイルのみを BGP ピアに適用できます)。
- BGP ピアのルート制御プロファイルを指定すると、その情報だけに基づいてルートマップが生成されます。L3Out プロファイル (l3extInstP) または L3Out の下の L3Out サブネット (l3extSubnet) を介して設定されたルート制御プロファイルは、このルートマップに関与しません。同様に、BGP ピアごとのルート制御プロファイル設定がない場合、L3Out の下のルート制御プロファイルが有効になります。
- 一致プレフィックスリストでプライベート BD サブネットを指定すると、そのサブネットが含まれます。プライベート BD サブネットを除外するために追加の設定を行う必要はありません。
- 一致プレフィックスリストで 0.0.0.0/0 を設定すると、BD サブネットを含むすべてのプレフィックスに一致します。
- Cisco APIC は、境界リーフスイッチにルートマップを作成して展開します。<tenant name> _<route profile name> _<L3Out name> -<direction>。たとえば、次の設定のルート マップがあります。

- [テナント名 (Tenant name)]: t1
- [ルート プロファイル名 (Route profile name)]: rp1
- [L3Out name]: l3out1
- [方向 (Direction)]: import

will have this as the route map name: **t1_rp1_l3out1-in**

- BGP ピアごとのルート制御機能を設定しても、共有サービス ルートマップの動作には影響しません。
- APIC ソフトウェアをアップグレードまたはダウングレードする場合は、次の点に注意してください。

- **APIC ソフトウェアのアップグレード** : APIC ソフトウェアをアップグレードする前に L3Out でルートプロファイルを設定した場合、L3Out のルートプロファイルは、BGP ピアごとのルートプロファイルを設定するまで正常に動作し続けます。上記が適用されます。
- **APIC ソフトウェアのダウングレード** : BGP ピアごとのルート プロファイルを設定し、その後で APIC ソフトウェアをダウングレードする場合は、ダウングレードに進む前にポリシーを削除する必要があります。

GUI を使用した BGP ピアごとのルート制御の設定

次の手順では、GUI を使用して BGP ピア単位のルート制御を設定する方法について説明します。

始める前に

- ノード、ポート、AEP、機能プロファイル、レイヤ 3 ドメインを設定します。
- ファブリック内でルートを伝播させるための、BGP ルート リフレクタ ポリシーを設定します。

ステップ 1 テナントおよび VRF の作成

- メニューバーで **[Tenants] > [Add Tenant]** の順に選択します。
[テナントの作成 (Create Tenant)] ダイアログ ボックスが表示されます。
- Name** フィールドに、テナント名を入力します。
- In the **VRF Name** フィールドに、VRF 名を入力します。
- Submit** をクリックします。

ステップ 2 ブリッジ ドメインを作成します。

- [ナビゲーション (Navigation)] ペインで [テナント (Tenant)] および [ネットワーク (Networking)] を展開します。
- Bridge Domains** を右クリックして、**Create Bridge Domain** を選択します。
- Name** フィールドに、ブリッジ ドメイン (BD) の名前を入力します。
- (オプション) [Advertise Host Routes] ボックスをクリックすると、すべての導入済み境界リーフでアドバタイズメントが有効になります。
- VRF** フィールドのドロップダウンリストから、作成した VRF を選択します (この例では v1)。
- Next** をクリックします。
- + アイコンを **Subnets** でクリックします。
- Gateway IP** フィールドに、BD のサブネットを入力します。
- Scope** フィールドで、**Advertised Externally** を選択します。

後ほど作成した後に、**L3 Out for Route Profile** を追加します。

(注) [ホストルータのアドバタイズ (Advertise Host Routes)] が有効になっている場合、ルートマップもすべてのホストルートを一致させます。

- j) **OK** をクリックします。
- k) **Next** をクリックし、**Finish** をクリックします。

ステップ 3 アプリケーション EPG の作成

- a) **Application Profiles** を右クリックし、**Create Application Profile** を選択します。
- b) アプリケーションの名前を入力します。
- c) EPG の + アイコンをクリックします。
- d) EPG の名前を入力します。
- e) BD ドロップダウンリストで、以前に作成したブリッジドメインを選択します。
- f) **Update** をクリックします。
- g) [送信 (Submit)] をクリックします。

ステップ 4 BGP ピアごとのルートマップとして使用されるテナントレベルのルートマップを作成します。

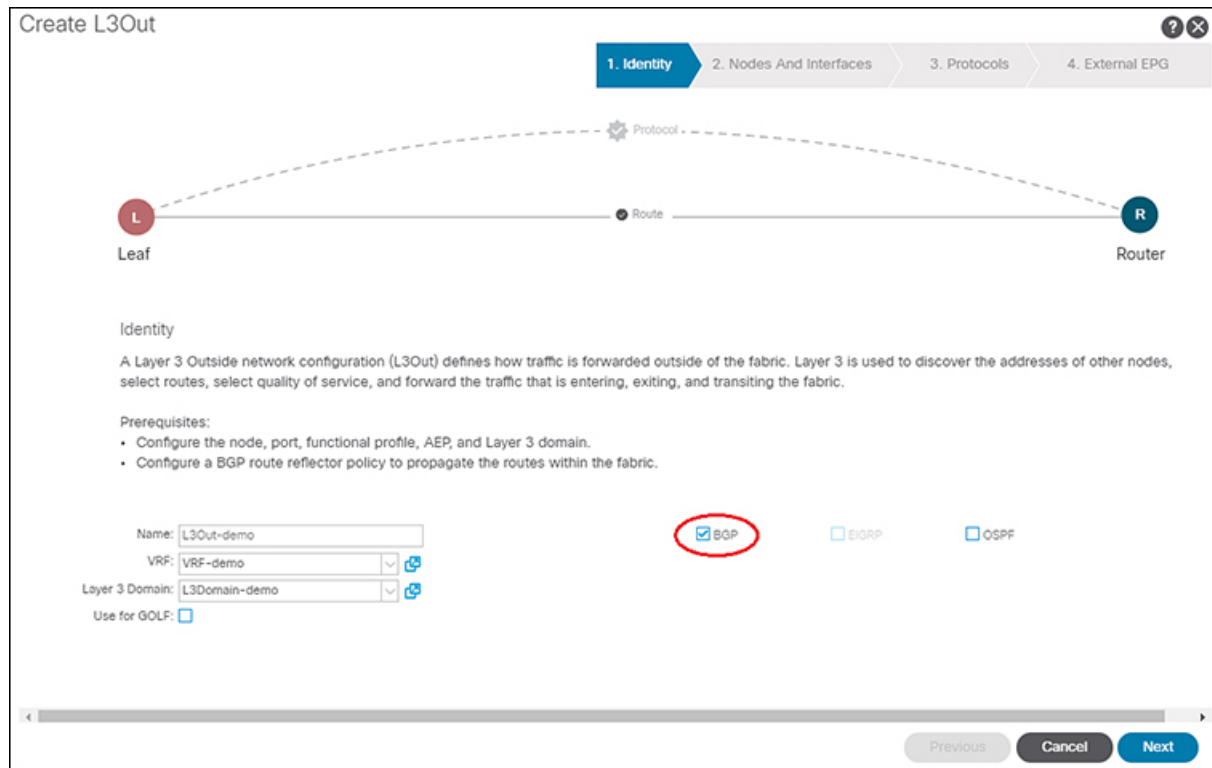
- a) [ナビゲーション (Navigation)] ペインで、[テナント (Tenants)] > [Tenant_name] > [ポリシー (Policies)] > [プロトコル (Protocol)] を展開します。
- b) [BGP ダンプニング、リーク間のルートマップ (Route Maps for BGP Dampening, Inter-leak)] を右クリックし、[BGP ダンプニング、リーク間のルートマップの作成 (Create Route Maps for BGP Dampening, Inter-leak)] を選択します。
- c) [BGP ダンプニング、リーク間のルートマップの作成 (Create Route Maps for BGP Dampening, Inter-leak)] ダイアログボックスで、[名前 (Name)] フィールドに、ルートプロファイル名を入力します。
- d) [タイプ (Type)] フィールドで、[ルーティングポリシーのみ照合 (Match Routing Policy Only)] を選択する必要があります。
- e) [コンテキスト (Contexts)] 領域で [+] サインをクリックして、[ルート制御コンテキスト作成 (Create Route Control Context)] ダイアログボックスを表示し、次のアクションを実行します。
 1. 必要に応じて、[順序 (Order)] と [名前 (Name)] フィールドに入力します。
 2. [一致ルール (Match Rule)] フィールドで、[一致ルールの作成 (Create Match Rule)] をクリックします。
 3. [一致ルール (Match Rule)] ダイアログボックスの [名前 (Name)] フィールドに、一致ルールの名前を入力します。
 4. 該当するフィールド (一致 **Regex** コミュニティ条件、一致コミュニティ条件、および一致プレフィックス、一致 **AS** パス **Regex** 条件) に必要な情報を入力し、[送信 (Submit)] をクリックします。
 5. [セットルール (Set Rule)] フィールドで、[ルートマップのセットルールの作成 (Create Set Rules for a Route Map)] をクリックします。
 6. [ルートマップのセットルールの作成 (Create Set Rules for a Route Map)] ダイアログボックスの [名前 (Name)] フィールドに、ルールの名前を入力します。

7. 目的の属性および関連するコミュニティ、条件、タグ、および設定 (preferences) を選択します。[完了 (Finish)] をクリックします。
8. [ルート制御コンテキストの作成 (Create Route Control Context)] ダイアログボックスで、[OK] をクリックします。
9. [BGP ダンプニング、インターリークのルートマップの作成 (Create Route Maps for BGP Dampening, Inter-leak)] ダイアログボックスで、[送信 (Submit)] をクリックします。

ステップ 5 L3Out を作成し、L3Out の BGP を設定します。

- a) [ナビゲーション (Navigation)] ペインで [テナント (Tenant)] および [ネットワーキング (Networking)] を展開します。
- b) [L3Outs] を右クリックし、[L3Out の作成 (Create L3Out)] を選択します。
- c) L3Out の BGP を設定するために必要な情報を入力します。

この L3Out の BGP プロトコルを設定するには、L3Out 作成ウィザードの [識別 (Identity)] ページで [BGP] を選択します。



- d) 残りのページを続けて行い ([ノードとインターフェイス (Nodes and Interfaces)], [プロトコル (Protocols)], および [外部 EPG (External EPG)])、L3Out の設定を完了します。

ステップ 6 L3Out の設定が完了したら、BGP ピアごとのルート制御機能を設定します。

- a) BGP ピア接続プロファイル画面に移動します。

[テナント (Tenants)] > [テナント (tenant)] > [ネットワーキング (Networking)] > [L3Outs] > [L3out-name] > [論理ノード プロファイル (Logical Node Profiles)] > [logical-node-profile-name] > [論理

インターフェイス プロファイル (Logical Interface Profiles)] > [logical-interface-profile-name] > [BGP
ピア接続プロファイル (BGP Peer Connectivity Profile)]] / [IP-address

- b) [ルート制御プロファイル (Route Control Profile)] フィールドまで下にスクロールし、[+] をクリックして次の項目を設定します。
- [名前 (Name)] : 設定したルートマップを選択します。 [ステップ 4 \(352 ページ\)](#)
 - [方向 (Direction)] : 次のいずれかのオプションを選択します。
 - ルートインポートポリシー
 - ルートエクスポートポリシー

明示的なプレフィクス リストでルート マップ/プロファイル

ルート マップ/プロファイルについて

ルートプロファイルは、関連付けられているセットアクションルールと一致する論理アクションルールの順序付きのセット (rtctrlCtxP) を定義する論理ポリシーです。ルートプロファイルでは、ルート マップの論理抽象です。複数のルート プロファイルは、1 個のルート マップにマージすることができます。ルートプロファイルには、以下のいずれかのタイプを指定できます。

- プレフィックスとルーティング ポリシーと一致: 普及サブネット (fvSubnet) と外部のサブネット (l3extSubnet) がルート プロファイルと組み合わせるし、マージされ、1 つのルート マップ (またはルート マップ エントリ) になります。一致するプレフィックスとルーティング ポリシーは、デフォルト値です。
- 一致ルーティング ポリシーのみ: は、ルート プロファイルは、ルート マップを生成する情報の唯一のソースと、その他のポリシー属性が上書きされます。



- (注) 明示的なプレフィクス リストを使用すると、「ルーティング ポリシーのみを一致」にルート プロファイルのタイプを設定する必要があります。

一致後の設定プロファイルが定義されていると、レイヤ 3 Out でルート マップを作成する必要があります。ルート マップは以下のいずれかの方法で作成できます。

- エクスポート ルート コントロールでは、「デフォルトエクスポート」ルート マップとインポート ルート制御の「デフォルト インポート」ルート マップを作成します。

- (デフォルトエクスポートまたはデフォルトインポートしないという名前)他のルートマップを作成し、l3extInstPs またはサブネット、l3extInstP の下の 1 つまたは複数の関係を設定します。
- いずれにしても、ルートマップ内で rtctrlSubjP を指しているによって明示的なプレフィックス リストでルートマップに一致します。

エクスポートとインポートルートマップでは、設定と一致のルールは、グループ間の相対シーケンス (rtctrlCtxP) とともにグループにまとめられます。一致の各グループの下でさらに、いづれかに関係ステートメント (rtctrlCtxP) を設定し、または一致プロファイルの詳細については、使用可能な (rtctrlSubjP)。

(たとえば BGP プロトコル)は、アウトのレイヤ 3 で有効になっているすべてのプロトコルは、エクスポートを使用し、ルート フィルタリングのマップをインポートルート。

ルートマップ/プロファイルの明示的なプレフィックスリストのサポートについて

Cisco APIC では、公開ブリッジドメイン (BD) サブネットと外部の中継ネットワークのインバウンドおよびアウトバウンドルート コントロールは、明示的なプレフィックス リストを通して提供されます。レイヤ 3 アウトのインバウンドおよびアウトバウンドルート コントロールは、ルート マップ/プロファイル (rtctrlProfile) によって管理されます。ルート マップ/プロファイル ポリシーは、Cisco ACI ファブリックでレイヤ 3 アウトを完全に管理するプレフィックス リストをサポートしています。

プレフィックス リストのサブネットは、ブリッジドメイン公開サブネットまたは外部のネットワークを表すことがあります。明示的なプレフィックス リストは別の方法を示し、次の代わりに使用できます。

- BD を介して BD サブネットをレイヤ 3 アウト関係にアドバタイズします。

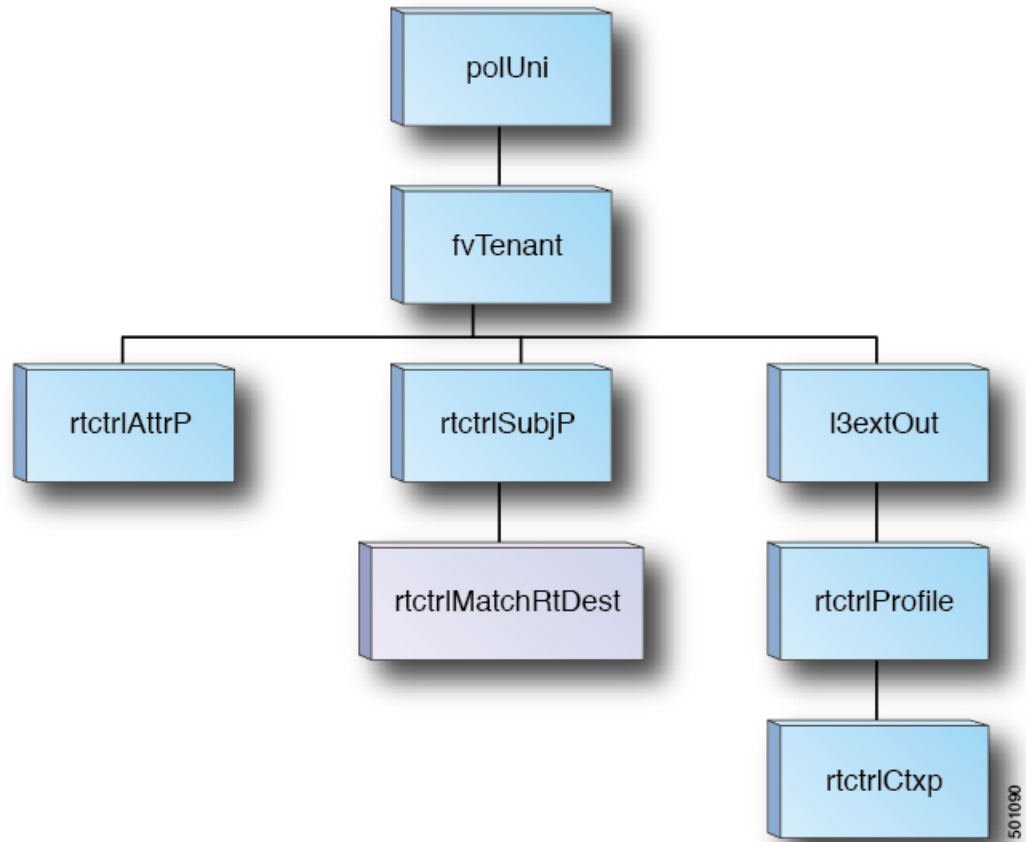


(注) BD のサブネットは、アドバタイズされるサブネットに公開としてマークする必要があります。

- 中継トラフィックと外部ネットワークをアドバタイジングするため、エクスポート/インポート ルート コントロールにより l3extInstP でサブネットを指定します。

明示的なプレフィックス リストは一致ルートの宛先 (rtctrlMatchRtDest) と呼ばれる新しい一致タイプで定義されます。使用例は次の API の例で説明します。

図 39: API の外部ポリシー モデル



明示的なプレフィックスリストを使用する場合の一致ルール、ルール設定に関する追加情報は次の通りです。

一致ルール

- テナント (fvTenant) で、ルートマップフィルタリングの一致プロファイル (rtctrlSubjP) を作成できます。各一致プロファイルは1個以上の一致ルールを含めることができます。一致ルールでは、複数の一致タイプをサポートしています。Cisco APIC リリース 2.1(x) 以前、サポートされていた一致タイプは明示的なプレフィックスリストおよびコミュニティリストでした。

Cisco APIC リリース 2.1(x) より、明示的なプレフィック一致または一致ルートの宛先 (rtctrlMatchRtDest) がサポートされています。

一致プレフィックスリスト (rtctrlMatchRtDest) は、オプションの集約フラグで1つまたは複数のサブネットがサポートされています。集約フラグは、設定で言及されているマスクから始めて、プレフィックスのアドレスファミリで許可されている最大数のマスクに達するまで、プレフィックスが複数のマスクと一致できるようにするために使用されます。

これは、NX-OS ソフトウェアのプレフィックスリストの「le」オプションに相当します (たとえば 10.0.0.0/8 le 32)。

プレフィックスリストは、次のケースに対応するために使用できます。

- すべて許可 (集約フラグでは 0.0.0.0/0、0.0.0.0/0 le 32 と同等)
- 1 つ以上の特定のプレフィックス (たとえば 10.1.1.0/24)
- 1 つ以上の集約フラグを伴うプレフィックス (たとえば 10.1.1.0/24 le 32 と同等)。



(注) 一致プレフィックス「0.0.0.0/0 with aggregate flag」を持つルートマップがエクスポート方向の L3Out EPG で使用される場合、ルールはダイナミックルーティングプロトコルからの再配布にのみ適用されます。したがって、ルールは次のものには適用されません (OSPF や EIGRP などのルーティングプロトコル)。

- ブリッジドメイン (BD) のサブネット
- 境界リーフスイッチに直接接続されたサブネット
- L3Out で定義されたスタティックルート

- 明示的なプレフィックス一致ルールは、1 つ以上のサブネットを含めることができます。これらのサブネットとしては、ブリッジドメインパブリックサブネットまたは外部ネットワークがあり得ます。またサブネットは、最大サブネットマスクまで集約することもできます (IPv4 では /32、IPv6 では /128)。
- さまざまなタイプの複数の一致ルールが存在する場合 (一致コミュニティや明示的なプレフィックスの一致など)、一致ルールは、個々の一致タイプすべての一致ステートメントが一致する場合だけを許可します。これは AND フィルタと等価です。明示的なプレフィックス一致はサブジェクトプロファイル (rtctrlSubjP) に含まれ、サブジェクトプロファイル下に他の一致ルールが存在する場合には論理 AND を形成します。
- 特定の一致タイプ (一致プレフィックスリスト) 内では、少なくとも 1 つの一致ルールステートメントが一致する必要があります。複数の明示的なプレフィックス一致 (rtctrlMatchRtDest) は、論理 OR を形成する同じサブジェクトプロファイル (rtctrlSubjP) 下で定義することができます。

一致プレフィックスの機能拡張

Cisco APIC リリース 4.2(3) 以降、一致ルールを作成し、集約を有効にすると、[一致プレフィックス (Match Prefix)] フィールドに 2 つの新しいフィールドが使用できるようになりました。リリースに基づいて、これらのフィールドには、次の表に示すように異なる命名規則があります。

リリース	フィールド
Cisco APIC リリース 4.2(3)	[開始プレフィックス (From Prefix)]
	[終了プレフィックス (To Prefix)]
Cisco APIC リリース 5.2(2)	[大きいマスク (Greater Than Mask)]
	[小さいマスク (Less Than Mask)]
Cisco APIC リリース 5.2(6)	[以上マスク (Greater Equal Mask)]
	[以下マスク (Less Equal Mask)]

プレフィックス一致ルールを作成して集約を有効にする場合は、これらのフィールドを使用してマスク範囲を指定します。次に、これらのフィールドを使用する状況の例を示します。

- すべて許可 (0.0.0.0/0、マスク長 24 ~ 30、0.0.0.0/0 ge 24 le 30 に相当)
- 特定の IP アドレスと 28 より大きいネットマスクを持つプレフィックス (たとえば、10.1.1.0/24 ge 28 と同等)

次の表に、これら2つの新しいフィールドを使用するさまざまなシナリオと、各シナリオの結果の詳細を示します。次の点に注意してください。

- [以上マスク (Greater Equal Mask)]と[以下マスク (Less Equal Mask)]フィールドは、[集約 (Aggregate)] オプションを [一致ルート宛先ルールの作成 (Create Match Route Destination Rule)] ウィンドウで選択した場合にのみ使用できます。
- 値 0 を [以上マスク (Greater Equal Mask)] および [以下マスク (Less Equal Mask)] フィールドに設定した場合、未指定と見なされ、次のデフォルト値が使用されます。
 - 以上マスク =0
 - 以下マスクは、IP アドレス ファミリが IPv4 か IPv6 かによって、32 または 128 になります。

この状況は、従来の動作を前提としており、これらのプロパティが存在しない古い設定のインポートをサポートします。詳細については、次の表の 2 列目を参照してください。

IPアドレス/ ネットマスク	集約	以上マスク エ ントリ (fromPfxLen)	以下マスク エ ントリ (toPfxLen)	結果	その他の情報
192.0.2.0/24	イネーブルに なっていない	なし	なし	192.0.2.0/24	完全一致:
192.0.2.0/24	有効	0	0	192.0.2.0/24 le 32	従来の動作

IPアドレス/ ネットマスク	集約	以上マスク エ ントリ (fromPfxLen)	以下マスク エ ントリ (toPfxLen)	結果	その他の情報
192.0.2.0/24	有効	24	不適切な値 ([以上マスク (Greater Equal Mask)] エントリに指 定した値のため にエラーが 発生した)	エラー：無効 な設定です。	[以上マスク (Greater Equal Mask)] エントリは、 ネットマスク 長よりも大き い必要があります。
192.0.2.0/24	有効	28	30	192.0.2.0/24 ge 28 le 30	これらの新しい フィールド による新しい 動作
192.0.2.0/24	有効	30	0	192.0.2.0/24 ge 30	これらの新しい フィールド による新しい 動作
192.0.2.0/24	有効	28	28	192.0.2.0/24 eq 28	これらの新しい フィールド による新しい 動作
192.0.2.0/24	有効	0	28	192.0.2.0/24 le 28	これらの新しい フィールド による新しい 動作
192.0.2.0/24	有効	30	28	エラー：無効 な設定です。	[以上マスク (Greater Equal Mask)] エントリを[以 下マスク (Less Equal Mask)]エン トリより大き くすることは できません。

ルールの設定

設定ポリシーは、設定コミュニティおよび設定タグなど明示的なプレフィックスで実施される設定ルールを定義するために作成する必要があります。

明示プレフィックス リストの集約サポート

一致するプレフィックスリストの各プレフィックス (rtctrlMatchRtDest) は、1つのプレフィックス リスト エントリに一致する複数のサブネットをサポートするように集約できます。

集約されたプレフィックスと BD プライベート サブネット

明示的なプレフィックスリストマッチ内のサブネットは、集約されたマッチまたは正確なマッチにより BD プライベート サブネットとマッチする可能性があります。プライベート サブネットは明示的なプレフィックス リストを使用するルーティング プロトコルを通してアドバタイズされることはありません。BD サブネットの範囲は、BD サブネットをアドバタイズするため明示プレフィックス リスト機能に対して「public」に設定する必要があります。

集約による 0.0.0.0/0 の動作の違い

集約設定を使用した 0.0.0.0/0 は、「0.0.0.0/0 le 32」に相当する IP プレフィックス リストを作成します。集約設定の 0.0.0.0/0 は、主に次の 2 つの状況で使用できます。

- L3Out ネットワーク (L3Out EPG) 下の L3Out サブネットの「Aggregate Export」スコープを持つ「Export Route Control Subnet」
- 「default-export」という名前のルートマップに割り当てられた明示的なプレフィックス リスト (Match Prefix ルール)

L3Out サブネット下の「Export Route Control Subnet」スコープで使用すると、ルート マップはダイナミック ルーティング プロトコルから学習したルートのみに一致します。BD サブネットまたは直接接続されたネットワークには一致しません。

明示的なルート マップ設定で使用すると、ルート マップは BD サブネットや直接接続ネットワークを含むすべてのルートに一致します。

上記の 2 つの状況で予想される動作と予期しない (一貫性のない) 動作を理解するには、次の例を検討してください。

シナリオ 1

最初のシナリオでは、次のような設定ポストを使用して、ルート マップ (名前は rpm_with_catch_all) を設定します。

```
<l3extOut annotation="" descr="" dn="uni/tn-t9/out-L3-out" enforceRtctrl="export"
name="L3-out" nameAlias="" ownerKey="" ownerTag="" targetDscp="unspecified">
  <rtctrlProfile annotation="" descr="" name="rpm_with_catch_all" nameAlias=""
ownerKey="" ownerTag="" type="combinable">
    <rtctrlCtxP action="permit" annotation="" descr="" name="catch_all" nameAlias=""
order="0">
      <rtctrlScope annotation="" descr="" name="" nameAlias="">
```

```

        <rtctrlRsScopeToAttrP annotation="" tnRtctrlAttrPName="set_metric_type"/>
    </rtctrlScope>
</rtctrlCtxP>
</rtctrlProfile>
    <ospfExtP annotation="" areaCost="1" areaCtrl="redistribute,summary" areaId="backbone"
    areaType="regular" descr="" multipodInternal="no" nameAlias=""/>
    <l3extRsEctx annotation="" tnFvCtxName="ctx0"/>
    <l3extLNodeP annotation="" configIssues="" descr="" name="leaf" nameAlias=""
    ownerKey="" ownerTag="" tag="yellow-green" targetDscp="unspecified">
    <l3extRsNodeL3OutAtt annotation="" configIssues="" rtrId="20.2.0.2"
    rtrIdLoopBack="no" tDn="topology/pod-1/node-104">
    <l3extLoopBackIfP addr="14.1.1.1/32" annotation="" descr="" name=""
    nameAlias=""/>
    <l3extInfraNodeP annotation="" descr="" fabricExtCtrlPeering="no"
    fabricExtIntersiteCtrlPeering="no" name="" nameAlias="" spineRole=""/>
    </l3extRsNodeL3OutAtt>
    <l3extLIIfP annotation="" descr="" name="interface" nameAlias="" ownerKey=""
    ownerTag="" tag="yellow-green">
    <ospfIfP annotation="" authKeyId="1" authType="none" descr="" name=""
    nameAlias="">
    <ospfRsIfPol annotation="" tnOspfIfPolName=""/>
    </ospfIfP>
    <l3extRsPathL3OutAtt addr="36.1.1.1/24" annotation="" autostate="disabled"
    descr="" encap="vlan-3063" encapScope="local" ifInstT="ext-svi" ipv6Dad="enabled"
    llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
    tDn="topology/pod-1/paths-104/pathep-[accBndlGrp_104_pc13]" targetDscp="unspecified"/>
    <l3extRsNdIfPol annotation="" tnNdIfPolName=""/>
    <l3extRsIngressQosDppPol annotation="" tnQosDppPolName=""/>
    <l3extRsEgressQosDppPol annotation="" tnQosDppPolName=""/>
    </l3extLIIfP>
    </l3extLNodeP>
    <l3extInstP annotation="" descr="" exceptionTag="" floodOnEncap="disabled"
    matchT="AtleastOne" name="epg" nameAlias="" prefGrMemb="exclude" prio="unspecified"
    targetDscp="unspecified">
    <l3extRsInstPToProfile annotation="" direction="export"
    tnRtctrlProfileName="rpm_with_catch_all"/>
    <l3extSubnet aggregate="" annotation="" descr="" ip="0.0.0.0/0" name=""
    nameAlias="" scope="import-security"/>
    <fvRsCustQosPol annotation="" tnQosCustomPolName=""/>
    </l3extInstP>
</l3extOut>

<rtctrlAttrP annotation="" descr="" dn="uni/tn-t9/attr-set_metric_type"
name="set_metric_type" nameAlias="">
    <rtctrlSetRtMetricType annotation="" descr="" metricType="ospf-type1" name=""
nameAlias="" type="metric-type"/>
</rtctrlAttrP>

<rtctrlSubjP annotation="" descr="" dn="uni/tn-t9/subj-catch_all_ip" name="catch_all_ip"
nameAlias="">
    <rtctrlMatchRtDest aggregate="yes" annotation="" descr="" ip="0.0.0.0/0" name=""
nameAlias=""/>
</rtctrlSubjP>

```

このルート マップでは、0.0.0.0/0 で予想されることは、すべてのルートが metricType = "ospf-type1" プロパティを使用することですが、OSPF ルートに対してのみです。

さらに、ブリッジドメイン (たとえば、209.165.201.0/27) の下に、スタティック ルートのパーベイシブ サブネット (fvSubnet) を持つルート マップを使用して、ブリッジドメインと L3Out

の関係を設定したサブネットワークがあります。ただし、上記のルートマップは結合可能ですが、上記のルートマップで 0.0.0.0/0 を、スタティックルートではなく、中継ルートにのみ適用するため、ブリッジドメインで設定されたサブネットワークには適用されません。

次に、show route-map および show ip prefix-list コマンドの出力を示します。exp-ctx-st-2555939 は、ブリッジドメインで設定されたサブネットワークの発信ルートマップの名前、および、show route-map コマンドの出力に示されているプレフィックスリストの名前です。

```
leaf4# show route-map exp-ctx-st-2555939
route-map exp-ctx-st-2555939, deny, sequence 1
  Match clauses:
    tag: 4294967295
  Set clauses:
route-map exp-ctx-st-2555939, permit, sequence 15801
  Match clauses:
    ip address prefix-lists: IPv4-st16391-2555939-exc-int-inferred-export-dst
    ipv6 address prefix-lists: IPv6-deny-all
  Set clauses:

leaf4# show ip prefix-list IPv4-st16391-2555939-exc-int-inferred-export-dst
ip prefix-list IPv4-st16391-2555939-exc-int-inferred-export-dst: 1 entries
seq 1 permit 209.165.201.0/27
```

```
leaf4#
```

この場合、ブリッジドメインサブネットワークが外に出ると、rpm_with_catch_all ルートマップポリシーが適用されないため、すべてが予期したとおりに動作します。

シナリオ 2

2 番目のシナリオでは、エクスポートルート制御用の「default-export」ルートマップを設定します。この場合、次のような設定ポストを使用して、明示的なプレフィックスリスト (Match Prefix ルール) が「default-export」ルートマップに割り当てられます。次のとおりです。

```
<l3extOut annotation="" descr="" dn="uni/tn-t9/out-L3-out" enforceRtctrl="export"
name="L3-out" nameAlias="" ownerKey="" ownerTag="" targetDscp="unspecified">
  <rtctrlProfile annotation="" descr="" name="default-export" nameAlias="" ownerKey=""
ownerTag="" type="combinable">
    <rtctrlCtxP action="permit" annotation="" descr="" name="set-rule" nameAlias=""
order="0">
      <rtctrlScope annotation="" descr="" name="" nameAlias="">
        <rtctrlRsScopeToAttrP annotation="" tnRtctrlAttrPName="set_metric_type"/>
      </rtctrlScope>
    </rtctrlCtxP>
  </rtctrlProfile>
  <ospfExtP annotation="" areaCost="1" areaCtrl="redistribute,summary" areaId="backbone"
areaType="regular" descr="" multipodInternal="no" nameAlias=""/>
  <l3extRsEctx annotation="" tnFvCtxName="ctx0"/>
  <l3extLNodeP annotation="" configIssues="" descr="" name="leaf" nameAlias=""
ownerKey="" ownerTag="" tag="yellow-green" targetDscp="unspecified">
    <l3extRsNodeL3OutAtt annotation="" configIssues="" rtrId="20.2.0.2"
rtrIdLoopBack="no" tDn="topology/pod-1/node-104">
      <l3extLoopBackIfP addr="14.1.1.1/32" annotation="" descr="" name=""
nameAlias=""/>
      <l3extInfraNodeP annotation="" descr="" fabricExtCtrlPeering="no"
fabricExtIntersiteCtrlPeering="no" name="" nameAlias="" spineRole=""/>
```



```

    </l3extRsNodeL3OutAtt>
    <l3extLIIfP annotation="" descr="" name="interface" nameAlias="" ownerKey=""
ownerTag="" tag="yellow-green">
      <ospfIfP annotation="" authKeyId="1" authType="none" descr="" name=""
nameAlias="">
        <ospfRsIfPol annotation="" tnOspfIfPolName=""/>
      </ospfIfP>
      <l3extRsPathL3OutAtt addr="36.1.1.1/24" annotation="" autostate="disabled"
descr="" encap="vlan-3063" encapScope="local" ifInstT="ext-svi" ipv6Dad="enabled"
llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
tDn="topology/pod-1/paths-104/pathep-[accBndlGrp_104_pc13]" targetDscp="unspecified"/>
      <l3extRsNdIfPol annotation="" tnNdIfPolName=""/>
      <l3extRsIngressQosDppPol annotation="" tnQosDppPolName=""/>
      <l3extRsEgressQosDppPol annotation="" tnQosDppPolName=""/>
    </l3extLIIfP>
  </l3extLNodeP>
  <l3extInstP annotation="" descr="" exceptionTag="" floodOnEncap="disabled"
matchT="AtleastOne" name="epg" nameAlias="" prefGrMemb="exclude" prio="unspecified"
targetDscp="unspecified">
    <l3extSubnet aggregate="" annotation="" descr="" ip="0.0.0.0/0" name=""
nameAlias="" scope="import-security"/>
    <fvRsCustQosPol annotation="" tnQosCustomPolName=""/>
  </l3extInstP>
</l3extOut>

```

この default-export ルート マップには、rpm_with_catch_all ルート マップと同様の情報があり、IP が 0.0.0.0/0 (ip=0.0.0.0/0) に設定されており、default-export ルートマップの設定ルールが Set Metric Type (tnRtctrlAttrPName=set_metric_type) でのみ設定されます。

前の例の状況と同様にブリッジ ドメインの下に同じサブネットを設定し、前の例と同様にブリッジ ドメインと L3Out の関係を設定します。

ただし、このシナリオでは、show route-map コマンドと show ip prefix-list コマンドの出力を次に示します。

```

leaf4# show route-map exp-ctx-st-2555939
route-map exp-ctx-st-2555939, deny, sequence 1
  Match clauses:
    tag: 4294967295
  Set clauses:
route-map exp-ctx-st-2555939, permit, sequence 8201
  Match clauses:
    ip address prefix-lists:
IPv4-st16391-2555939-exc-int-out-default-export2set-rule0pfx-only-dst
    ipv6 address prefix-lists: IPv6-deny-all
  Set clauses:
    metric-type type-1

leaf4# show ip prefix-list IPv4-st16391-2555939-exc-int-inferred-export-dst
% Policy IPv4-st16391-2555939-exc-int-inferred-export-dst not found
ifav82-leaf4# show ip prefix-list
IPv4-st16391-2555939-exc-int-out-default-export2set-rule0pfx-only-dst
ip prefix-list IPv4-st16391-2555939-exc-int-out-default-export2set-rule0pfx-only-dst: 1
entries
  seq 1 permit 209.165.201.0/27

leaf4#

```

この状況では、ブリッジドメインサブネットが発信されると、default-export ルートマップポリシーが適用されます。この状況では、そのルートマップは BD サブネットと直接接続ネットワークを含むすべてのルートに一致します。これは一貫性のない動作です。

注意事項と制約事項

- 次の2つの方法のいずれかを選択し、ルートマップの設定を行う必要があります。両方の方法を使用する場合は、二重エントリになり定義されていないルートマップになります。
 - レイヤ3アウトサイド関係にブリッジドメイン (BD) でルートを追加し、BDを設定します。
 - rtctrlSubjP マッチ プロファイルで、マッチプレフィックスを構成します。
- 2.3(x) 以降、[deny-static] 暗黙エントリはエクスポート ルート マップから削除されています。ユーザは、静的ルートのエクスポートを制御するために必要な許可と拒否を暗黙で設定する必要があります。
- L3Out ではピアごとの Route-map は OSPF および EIGRP でサポートされません。Route-map は、全体として L3Out にのみ適用できます。4.2(x) 以降、L3Out のピアごとのルートマップは BGP でサポートされます。

この問題の回避策を次に示します。

 - ネイバーの反対側からアドバタイズされないようにプレフィックスをブロックします。
 - プレフィックスを学習したくない既存 L3Out で route-map のプレフィックスをブロックし、プレフィックスを学習したい別の L3Out にネイバーを移動して、別の route-map を作成します。
- GUI と API コマンドの組み合わせを使用した route-map の作成はサポートされません。考えられる解決策として、GUI を使用してデフォルトの route-map とは異なる route-map を作成することはできますが、L3Out で GUI を通じて作成された route-map をピアごとに適用することはできません。

GUI を使用した、明示的なプレフィックス リストでルート マップ/プロファイルの設定

始める前に

- テナントと VRF を設定する必要があります。
- リーフ スイッチで VRF をイネーブルにする必要があります。

- ステップ 1** メニューバーで [テナント (Tenant)] をクリックし、[ナビゲーション (Navigation)] ペインで [Tenant_name] [ポリシー (Policies)] [プロトコル (Protocol)] [一致ルール (Match Rules)] を展開します。 > > >
- ステップ 2** [一致ルール (Match Rules)] を右クリックし、[ルート マップの一致ルールの作成 (Create Match Rule for a Route Map)] をクリックします。
- ステップ 3** [一致ルールの作成 (Create Match Rule)] ウィンドウで、ルールの名前を入力し、必要なコミュニティ条件を選択します。
- ステップ 4** 一致プレフィックスに必要な情報を入力します。
- 一致プレフィックスの情報を入力する方法は、APIC のリリースによって異なります。
- APIC リリース 4.2(3) 以前では、[一致ルールの作成 (Create Match Rule)] ウィンドウで、[一致プレフィックス (Match Prefix)] を展開し、次のアクションを実行します:
 1. **IP** フィールドで、明示的プレフィックス リストを入力します。
明示的プレフィックスは、BD サブネットまたは外部ネットワークを表記できます。
 2. (任意) [説明 (Description)] フィールドに、このポリシーの説明を入力します。
 3. **Aggregate** チェック ボックスは、集約プレフィックスが必要な場合にのみオンにします。
 4. [更新 (Update)] をクリックします。
 - APIC リリース 4.2(3) 以降では、[一致ルールの作成 (Create Match Rule)] ウィンドウで、[一致プレフィックス (Match Prefix)] 領域の [+] をクリックします。
[一致ルート宛先ルールの作成 (Create Match Route Destination Rule)] ウィンドウが表示されます。
このウィンドウで次のアクションを実行します。
 1. **IP** フィールドで、明示的プレフィックス リストを入力します。
明示的プレフィックスは、BD サブネットまたは外部ネットワークを表記できます。
 2. (任意) [説明 (Description)] フィールドに、このポリシーの説明を入力します。
 3. 集約プレフィックスが必要かどうかを決定します。
 - 集約プレフィックスが不要な場合は、[集約 (Aggregate)] をオフのままにし、[送信 (Submit)] をクリックしてに進みます。 [ステップ 5 \(366 ページ\)](#)
 - 集約プレフィックスが必要な場合に [集約 (Aggregate)] チェック ボックスをオンにします。
- [以上マスク (Greater Equal Mask)] フィールドと [以下マスク (Less Equal Mask)] フィールドが使用可能になります。
1. [以上マスク (Greater Equal Mask)] フィールドで、一致させるプレフィックス長を指定します。
有効な範囲は 0 ~ 128 です。値 0 は未指定と見なされます。

2. [以下マスク (Less Equal Mask)] フィールドで、一致させるプレフィックス長を指定します。

有効な範囲は 0 ~ 128 です。値 0 は未指定と見なされます。

APIC リリース 4.2(3) 以降の [以上マスク (Greater Equal Mask)] および [以下マスク (Less Equal Mask)] フィールドの詳細については、[一致プレフィックスの機能拡張 \(357 ページ\)](#) を参照してください。

4. [一致ルート宛先ルールの作成 (Create Match Route Destination Rule)] ウィンドウで [送信 (Submit)] をクリックします。

ステップ 5 [一致ルールの作成 (Create Match Rule)] ウィンドウで、[送信 (Submit)] をクリックします。

一致ルールは、1つ以上の一致宛先ルールと、1つ以上の一致コミュニティ条件を持つことができます。一致の種類では AND フィルタがサポートされています。これを利用すると、受け入れられるためには、一致ルール内のすべて条件がルート一致ルールと一致する必要があります。**Match Destination Rules** に複数の一致プレフィックスがある場合には、OR フィルタがサポートされます。これを利用すると、任意の一致プレフィックスがルート タイプとして受け入れられます。

ステップ 6 [L3outs] の下で、利用可能なデフォルト レイヤ 3 Out をクリックして選択します。

別のレイヤ 3 Out が必要な場合には、代わりにそれを選択することができます。

ステップ 7 [ルート制御のインポートおよびエクスポートのルート マップ (Route Map for import and export rout control)] を右クリックし、[ルート制御のインポートおよびエクスポートのルート マップの作成 (Create Route Map for import and export rout control)] をクリックします。

ステップ 8 ルート制御のインポートおよびエクスポートのルート マップの作成 (Create Route Map for import and export rout control) ダイアログボックスで、デフォルトのルート マップを使用するか、使用するルート マップの名前を入力します。

この例では、**default_export** ルート マップを使用します。

ステップ 9 **Type** フィールドで、**Match Routing Policy Only** を選択します。

一致ルーティングポリシーは、グローバルな RPC 一致宛先ルートです。このフィールドで使用できる他のオプションとしては、一致プレフィックスおよびルーティング ポリシーで、RPC ルーティング ポリシーの宛先ルートと組み合わせることができます。

ステップ 10 [コンテキスト (Contexts)] 領域で、+ アイコンを展開して [ルート制御コンテキストの作成 (Create Route Control Context)] ダイアログ ボックスを表示します。

ステップ 11 ルート制御のコンテキストの名前を入力し、各フィールドで必要なオプションを選択します。一致ルールで定義されている基準に一致するルートを拒否するには (次の手順で選択します)、アクション [拒否 (deny)] を選択します。デフォルトのアクションは **permit** です。

ステップ 12 **Match Rule** フィールドで、前に作成したルールを選択します。

ステップ 13 **Set Rule** フィールドで、**Create Set Rules for a Route Map** を選択します。

通常は、ルート マップ/プロファイルで一致させることにより、プレフィックス リストに入出力を許可しますが、それに加えて何らかの属性をこれらのルートに設定し、その属性を持つルートをさらに一致させることもできます。

ステップ 14 Create Set Rules for a Route Map ダイアログボックスで、アクションルールの名前を入力し、必要なチェック ボックスをオンにします。[完了 (Finish)] をクリックします。

ステップ 15 Create Route Control Context ダイアログボックスで、OK をクリックします。[インポートおよびエクスポート ルート制御向けのルート マップの作成 (Create Route map for import and export route control)] ダイアログ ボックスで、[送信 (Submit)] をクリックします。

これで、ルート マップ/プロファイルの作成は完了です。ルート マップは、一致アクションルールと設定アクションルールの組み合わせです。ルート マップは、ユーザの必要に応じて、エクスポート プロファイルまたはインポート プロファイルまたは再配布可能プロファイルに関連付けられます。ルート マップのプロトコルを有効にすることができます。

ルート制御プロトコル

インポート制御とエクスポート制御を使用するルーティング制御プロトコルの設定について

このトピックでは、インポート制御とエクスポート制御を使用するルーティング制御プロトコルを設定する方法の典型的な例を示します。これは、外部 BGP を使用したネットワーク接続のレイヤ 3 が設定されていると仮定します。OSPF で設定されたネットワークの外部レイヤ 3 の次のタスクを実行することもできます。

GUI を使用した、インポート制御とエクスポート制御を使用するルート制御プロトコルの設定

この例では、ネットワーク接続 BGP を使用して外部レイヤ 3 が設定されていることを前提としています。OSPF を使用するように設定されたネットワークに対してもこれらのタスクを実行することができます。

このタスクでは、インポートポリシーとエクスポートポリシーの作成手順を示します。デフォルトでは、インポート制御は適用されていないため、インポート制御を手動で割り当てる必要があります。

始める前に

- テナント、プライベートネットワーク、およびブリッジドメインが作成されていること。
- テナント ネットワークのレイヤ 3 Outside が作成されていること。

- ステップ 1** メニューバーで、[テナント (TENANTS)] > [Tenant_name] > [ネットワーキング (Networking)] > [L3Out] > [Layer3_Outside_name] の順にクリックします。
- ステップ 2** [Layer3_Outside_name] を右クリックして、[ルート制御のインポートおよびエクスポート向けルートマップの作成 (Create Route map for import and export route control)] をクリックします。
- ステップ 3** [ルート制御のインポートおよびエクスポート向けルートマップの作成 (Create Route map for import and export route control)] ダイアログボックスで、次のアクションを実行します。
- [Name] フィールドのドロップダウンリストから、適切なルートプロファイルを選択します。選択内容に応じて、特定の Outside でアドバタイズされている内容が自動的に使用されます。
 - Type** フィールドで、**Match Prefix AND Routing Policy** を選択します。
 - [コンテキスト (Contexts)] 領域で、[+] をクリックして [ルート制御コンテキストの作成 (Create Route Control Context)] ウィンドウを表示します。
- ステップ 4** [Create Route Control Context] ダイアログボックスで、次の操作を実行します。
- [Order] フィールドで、目的の順序の番号を選択します。
 - [Name] フィールドに、ルート制御プライベートネットワークの名前を入力します。
 - Match Rule** フィールドのドロップダウンリストで、**Create Match Rule For a Route Map** をクリックします。
 - Create Match Rule** ダイアログボックスの **Name** フィールドに、一致ルールの名前を入力します。[Submit] をクリックします。
必要に応じて、正規表現による一致コミュニティ条件および一致コミュニティ条件を指定します。一致コミュニティファクタでは、名前、コミュニティ、およびスコープを指定する必要があります。
 - [セットルール (Set Rule)] ドロップダウンリストから、[ルートマップのセットルールの作成 (Create Set Rules For a Route Map)] を選択します。
 - Create Set Rules For a Route Map** ダイアログボックスの **Name** フィールドに、ルールの名前を入力します。
 - 設定するルールのチェックボックスをオンにし、選択肢として表示されている適切な値を選択します。[完了 (Finish)] をクリックします。
ポリシーが作成され、アクションルールに関連付けられました。
 - [ルート制御コンテキストの作成 (Create Route Control Context)] ダイアログボックスで、[OK] をクリックします。
 - [インポートおよびエクスポート ルート制御向けのルートマップの作成 (Create Route map for import and export route control)] ダイアログボックスで、[送信 (Submit)] をクリックします。
- ステップ 5** [ナビゲーション (Navigation)] ペインで、[ルートプロファイル (Route Profile)] > [route_profile_name] > [route_control_private_network_name] の順に選択します。
[Work] ペインの [Properties] に、ルートプロファイルポリシーと関連アクションルール名が表示されます。
- ステップ 6** [ナビゲーション (Navigation)] ペインで、[Layer3_Outside_name] をクリックし、[ポリシー/メイン (Policy/Main)] タブをクリックします。
Work ウィンドウに、**Properties** が表示されます。
- ステップ 7** (任意) [ルート制御の強化 (Route Control Enforcement)] フィールドのとなりの [インポート (Import)] チェックボックスをオンにして、インポートポリシーを有効にします。

インポート制御ポリシーはデフォルトで有効になっていませんが、ユーザが有効にすることができます。インポート制御ポリシーは BGP と OSPF でサポートされていますが、EIGRP ではサポートされていません。ユーザがサポートされていないプロトコルのインポート制御ポリシーを有効にしても、自動的に無視されます。エクスポート制御ポリシーは、BGP、EIGRP、および OSPF でサポートされます。

(注) BGP が OSPF 上で確立されると、インポート制御ポリシーは BGP にのみ適用され、OSPF は無視されます。

ステップ 8 カスタマイズされたエクスポートポリシーを作成するには、[ルート制御のインポートおよびエクスポートのルートマップ (Route Map for import and export route control)] を右クリックし、[ルート制御のインポートおよびエクスポートのルートマップの作成 (Create Route Map for import and export route control)] をクリックし、次のアクションを実行します。

- a) [ルート制御のインポートおよびエクスポート向けルートマップの作成 (Create Route map for import and export route control)] ダイアログボックスで、[名前 (Name)] フィールドのドロップダウンリストから、エクスポートポリシーを選択するか、名前を入力します。
- b) [コンテキスト (Contexts)] 領域で、[+] をクリックして [ルート制御コンテキストの作成 (Create Route Control Context)] ウィンドウを表示します。
- c) [Create Route Control Context] ダイアログボックスの [Order] フィールドで、値を選択します。
- d) [Name] フィールドに、ルート制御プライベートネットワークの名前を入力します。
- e) (任意) **Match Rule** フィールドのドロップダウンリストから **Create Match Rule For a Route Map** を選択し、必要に応じて一致ルールポリシーを作成して、アタッチします。
- f) [セットルール (Set Rule)] フィールドのドロップダウンリストから、[ルートマップのセットルールの作成 (Create Set Rules For a Route Map)] を選択して、[OK] をクリックします。
または、必要に応じて既存の set アクションを選択し、**OK** をクリックします。
- g) **Create Set Rules For A Route Map** ダイアログボックスの **Name** フィールドに名前を入力します。
- h) 設定するルールのチェックボックスをオンにし、選択肢として表示されている適切な値を選択します。[完了 (Finish)] をクリックします。
[Create Route Control Context] ダイアログボックスでは、ポリシーが作成されてアクションルールに関連付けられています。
- i) **OK** をクリックします。
- j) [インポートおよびエクスポートルート制御向けのルートマップの作成 (Create Route map for import and export route control)] ダイアログボックスで、[送信 (Submit)] をクリックします。

[Work] ペインに、エクスポートポリシーが表示されます。

(注) エクスポートポリシーを有効にするには、最初に適用する必要があります。この例では、このポリシーはネットワークのすべてのサブネットに適用されます。

ステップ 9 [ナビゲーション (Navigation)] ペインで [L3Outs] > [L3Out_name] > [外部 EPG (External EPGs)] > [externalEPG_name] の順に展開して、次のアクションを実行します。

- a) **Route Control Profile** を展開します。
- b) **Name** フィールドのドロップダウンリストから、前に作成したポリシーを選択します。

- c) [方向 (Direction)] フィールドのドロップダウンリストから、[ルート エクスポート ポリシー (Route Export Policy)] を選択します。[更新 (Update)] をクリックします。

MP-BGP のインターリーク再配布

MP-BGP のインターリーク再配布の概要

このトピックでは、() を使用して () ファブリックでのインターリーク再配布を設定する方法について説明します。Cisco Application Centric Infrastructure APIC Cisco Application Policy Infrastructure Controller APIC

Cisco ACI では、レイヤ 3 Outside (L3Out) が展開されている境界リーフ ノードが、L3Out ルートを BGP IPv4/IPv6 アドレス ファミリーに再配布し、VRF 情報とともに MP-BGP VPNv4/VPNv6 アドレス ファミリーに再配布して、L3Out ルートを配布します。境界リーフ ノードからスパイン ノードを介して他のリーフ ノードに移動します。Cisco ACI ファブリック内のインターリーク再配布は、BGP IPv4/IPv6 アドレス ファミリーへの L3Out ルートのこの再配布を指します。デフォルトでは、BGP を介して学習されたルートを除き、ダイナミック ルーティング プロトコル、スタティック ルート、および L3Out インターフェイスの直接接続されたサブネットを介して学習されたルートなど、すべての L3Out ルートでインターリークが発生します。BGP を介して学習されたルートはすでに BGP IPv4/IPv6 テーブルにあり、インターリークなしで MP-BGP VPNv4/VPNv6 にエクスポートする準備ができています。

インターリーク再配布により、ユーザはルートマップを適用して L3Out ルートを選択的に BGP に再配布し、他のリーフ ノードに表示されるルートを制御したり、BGP コミュニティ、プリファレンス、メトリックなどの一部の属性をルートに設定したりできます。。この再配布により、入力境界リーフ ノードによって設定された属性に基づいて、または他のリーフ ノードがある境界リーフ ノードから別の境界リーフ ノードへのルートを優先できるように、別の境界リーフ ノードで選択的中継ルーティングを実行できます。

以前のリリースでは、OSPF および EIGRP ルートからのインターリーク再配布にルートマップを適用できました。

Cisco APIC 4.2(1) リリース以降では、スタティック ルートからのインターリーク再配布へのルートマップの適用がサポートされています。

Cisco APIC 5.1(4) リリース以降、直接サブネット (L3Out インターフェイス) からのインターリーク再配布へのルートマップの適用がサポートされています。この機能は、当初 Cisco APIC 4.2(6h) リリースで追加されましたが、5.1(4) リリースまではいずれの 5.x リリースでも使用できませんでした。

Cisco APIC 5.1(4) リリース以降では、スタティック ルートおよび直接サブネットのインターリーク再配布のために、ルートマップで拒否アクションを設定できます。この機能は、当初 Cisco APIC 4.2(6h) リリースで追加されましたが、5.1(4) リリースまではいずれの 5.x リリースでも使用できませんでした。

GUI を使用したインターリーク再配布のルート マップ の設定

インターリーク再配布のルート マップは、[テナント (Tenant)] [ポリシー (Policies)] [プロトコル (Protocol)] [ルート制御のルート マップ (Route Maps for Route Control)] で作成できます。 > > >

始める前に

テナントを作成します。

-
- ステップ 1 メニュー バーで、[テナント] をクリックします。
 - ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。
 - ステップ 3 [ナビゲーション (Navigation)] ペインで、[tenant_name Policies] [プロトコル (Protocol)] [ルート制御のルート マップ (Route Maps for Route Control)] を展開します。 > >
 - ステップ 4 [ルート制御のルート マップ (Route Maps for Route Control)] を右クリックし、[ルート制御のルート マップの作成 (Create Route Maps for Route Control)] をクリックします。[ルート制御のルート マップの作成 (Create Route Maps for Route Control)] ダイアログボックスが表示されます。
 - ステップ 5 [名前 (Name)] フィールドに、インターリーク (BGP への再配布) を制御するルート マップの名前を入力します。
 - ステップ 6 [コンテキスト (Contexts)] 領域で[+]サインをクリックして、[ルート制御コンテキスト作成 (Create Route Control Context)] ダイアログ ボックスを表示し、次のアクションを実行します。
 - a) 必要に応じて、[順序 (Order)] と [名前 (Name)] フィールドに入力します。
 - b) [アクション (Action)] フィールドで [許可 (Permit)] を選択します。
 - c) [一致ルール (Match Rule)] フィールドで、目的の一致ルールを選択するか、新しい一致ルールを作成します。
 - d) [セットルール (Set Rule)] フィールドで、目的のセットルールを選択するか、新しいセットルールを作成します。
 - e) [OK] をクリックします。作成する必要があるルート制御コンテキストごとに、この手順を繰り返します。
 - ステップ 7 [ルート マップの作成 (Create Route Map)] ダイアログ ボックスで、[送信 (Submit)] をクリックします。
-

GUI を使用したインターリーク再配布のルート マップ の適用

特定の L3Out からのインターリーク再配布をカスタマイズするルート マップは、L3Out を介して適用する必要があります。

始める前に

テナント、VRF、および L3Out を作成します。

-
- ステップ 1** メニュー バーで、**[テナント]** をクリックします。
- ステップ 2** **[Work]** ペインで、テナントの名前をダブルクリックします。
- ステップ 3** **[ナビゲーション (Navigation)]** ペインで、**[tenant_name]>[ネットワークング (Networking)]>[L3Outs]>[L3Out_name]** の順に展開します。
- ステップ 4** **[ポリシーメイン (Policy Main)]** タブをクリックして、この L3Out の **[プロパティ (Properties)]** ウィンドウにアクセスします。 >
- ステップ 5** OSPF または EIGRP ルートの場合は、次の操作を実行します。
- [インターリークのルート プロファイル (Route Profile for Interleak)]** フィールドで、ルートマップ/プロファイルを選択するか作成します。
 - [ワーク (Work)]** ペインで、**[送信 (Submit)]** をクリックし、**[変更の送信 (Submit Changes)]** をクリックします。
- ステップ 6** スタティック ルートの場合は、次の操作を実行します。
- [再配布のルート プロファイル (Route Profile for Redistribution)]** フィールドで、**[+]** アイコンをクリックします。
 - [送信元 (Source)]** フィールドで、インターリーク再配布の送信元としてスタティック ルートのスタティックを選択します。
 - [更新 (Update)]** をクリックします。
-



第 22 章

ルーティングとサブネット範囲

この章は、次の内容で構成されています。

- [L3Out EPG スコープと制御パラメータ \(373 ページ\)](#)
- [セキュリティインポートポリシー \(374 ページ\)](#)

L3Out EPG スコープと制御パラメータ

サブネットの範囲と集約コントロール

次のセクションでは、サブネットを作成するときに利用できるいくつかの範囲と集約に関するオプションについて説明します:

Export Route Control Subnet: コントロールは、ファブリック外の特定の中継ルートをアドバタイズします。これは中継ルートにのみ影響するもので、内部ルートやブリッジドメインで設定されるデフォルトのゲートウェイには影響しません。

インポートルートコントロールサブネット: このコントロールは、インポートルート制御の強制が設定されている場合、ルートを **Border Gateway Protocol (BGP)** と **Open Shortest Path First (OSPF)** でファブリックにアドバタイズすることを可能にします。

External Subnets for the External EPG (セキュリティインポートサブネットとも呼ばれる): このオプションは、ルーティング情報のファブリックへの出入りはコントロールしません。トラフィックがある外部 EPG から別の外部 EPG に、または内部 EPG に流れるようにするには、サブネットにはこのコントロールでマークを付ける必要があります。このコントロールを使用してサブネットにマークしなかった場合には、ある EPG から学習したルートが他の外部 EPG にもアドバタイズされますが、パケットはファブリックでドロップされます。パケットがドロップされるのは、APIC が許可済みリストモデルで動作するからです。そのデフォルトの動作は、契約で明示的に許可されていない限り、EPG間の全データプレーントラフィックをドロップするというものです。この許可済みリストモデルは外部 EPG とアプリケーション EPG に適用されます。このオプションが設定されているセキュリティポリシーを使用する場合には、契約とセキュリティプレフィックスを設定する必要があります。

Shared Route Control Subnet: VRF 間のリーキングの共有 L3Outs から学習されたサブネットは、他の VRF にアドバタイズされる前に、このコントロールでマークされる必要があります。APIC リリース 2.2(2e) 以降では、異なる VRF の共有 L3Outs は契約を使用して相互に通信できます。異なる VRF の共有 L3Outs 間の通信の詳細については、『Cisco APIC レイヤ 3 ネットワーク キング構成定ガイド』を参照してください。

Shared Security Import Subnet: このコントロールは、共有 L3Out 学習ルートについては、[External Subnets for the External EPG] と同じです。トラフィックがある外部 EPG から別の外部 EPG に、または別の内部 EPG に流れるようにするには、サブネットにはこのコントロールでマークを付ける必要があります。このコントロールを使用してサブネットにマークしなかった場合には、ある EPG から学習したルートが他の外部 EPG にもアドバタイズされますが、パケットはファブリックでドロップされます。このオプションが設定されているセキュリティポリシーを使用する場合には、契約とセキュリティプレフィックスを設定する必要があります。

Aggregate Export, Aggregate Import, and Aggregate Shared Routes: このオプションは、0.0.0.0/0 プレフィックスの前に 32 を追加します。現在、インポート/エクスポートルート制御サブネットに集約できるのは、0.0.0.0/0 プレフィックスのみです。0.0.0.0/0 プレフィックスを集約すると、制御プロファイルを 0.0.0.0 ネットワークに適用することはできなくなります。

Aggregate Shared Route: このオプションは、共有ルート制御サブネットとしてマークされている任意のプレフィックスに使用できます。

Route Control Profile: ACI ファブリックは、ファブリックの内部と外部にアドバタイズされるルート用に、ルートマップの set 句もサポートします。ルートマップの set ルールは、ルート制御プロファイルポリシーとアクションルールプロファイルで設定されます。

セキュリティインポートポリシー

静的 L3Out EPG

本書で説明されているポリシーでは、ACI ファブリックの内外へのルーティング情報の交換、およびルートの制御とタグ付けに使用する方法を取り扱ってきました。ファブリックは許可リストモデルで動作します。そのデフォルトの動作は、契約によって明示的に許可されていない限り、エンドポイントグループ間のすべてのデータプレーントラフィックをドロップするというものです。この許可リストモデルは外部 EPG とテナント EPG に適用されます。

中継トラフィックの場合、テナントトラフィックとは、セキュリティポリシーの設定方法と実装方法が少し異なります。

中継セキュリティポリシー

- プレフィックスフィルタリングを使用します。
- リリース 2.0(1m) 以降では、Ethertype、プロトコル、L4 ポート、および TCP フラグフィールドのサポートが利用できるようになりました。
- セキュリティインポートサブネット（プレフィックス）と外部 EPG で設定されたコントロールを使用して実装されます。

テナント EPG セキュリティ ポリシー

- プレフィックス フィルタリングは使用しないでください。
- Ethertype、プロトコル、L4 ポート、および TCP フラグ フィルタをサポートします。
- テナント EPG ↔ EPG およびテナント EPG ↔ 外部 EPG でサポートされます。

外部プレフィックス ベースの EPG 間に契約が存在しない場合、トラフィックはドロップされます。2つの外部 EPG の間のトラフィックを許可するには、契約とセキュリティプレフィックスを設定する必要があります。プレフィックス フィルタリングのみがサポートされるため、契約ではデフォルト フィルタを使用できます。

外部 L3Out 接続契約

L3Out 接続が展開されているすべてのリーフ ノードでは、L3Out 接続のプレフィックスの結合がプログラムされます。3つ以上の L3Out 接続が展開されている場合、集約ルール 0.0.0.0/0 を使用すると、契約のない L3Out 接続間でもトラフィックのフローが許可されます。

L3Out インスタンス プロファイル (instP) で、プロバイダーとコンシューマの契約の関連づけとセキュリティ インポート サブネットを設定します。

セキュリティ インポート サブネットが設定されており、集約ルール、0.0.0.0/0 がサポートされている場合、セキュリティ インポート サブネットは ACL タイプのルールに従います。セキュリティ インポート サブネットのルール 10.0.0.0/8 は、10.0.0.0 ~ 10.255.255.255 の範囲のすべてのアドレスに適合します。ルート制御サブネットで許可されているプレフィックスに対して正確なプレフィックス照合を設定する必要はありません。

3つ以上の L3Out 接続が同じ VRF 内に設定されている場合は、ルールの結合が問題となるため、セキュリティ インポート サブネットを設定するときに注意する必要があります。

同じ L3Out で入出力する中継トラフィック フローは、0.0.0.0/0 セキュリティ インポート サブネットを設定すると、ポリシーによってドロップされます。この動作は、ダイナミックまたはスタティックルーティングに当てはまります。この動作を防ぐためには、より詳細なサブネットを定義してください。

ダイナミック L3Out EPG 分類

Cisco APIC 5.2(4) リリースより前は、外部サブネットは外部 EPG の下で構成されていたため、外部サブネットの pcTag は外部 EPG の pcTag から派生していました。ルーティングが変更されると、外部サブネットは別の L3Out または外部 EPG から学習されました。pcTag は、ルーティングが変更されても変更されません。

Cisco APIC 5.2(4) リリース以降、動的 L3Out EPG 分類 (DEC) 機能が導入され、ルーティングの変更に伴う pcTag の動的な変更が可能になりました。

この機能により、管理者はサブネットまたは BGP コミュニティを照合することにより、ルートマップを使用して外部 EPG を設定することもできます。外部 EPG 設定が設定されたルートマップは、デフォルト インポートを使用して L3Out に、またはルート制御プロファイルを使用して BGP ピアに適用できます。L3Out の外部 EPG および契約設定は以前と同じままです。

ルートマップに基づいて、特定の外部 EPG および関連する契約がプレフィックスに対して決定されます。



- (注) ルートマップによる外部 EPG の選択は、L3Out で設定された外部 EPG サブネットよりも優先されます。たとえば、ルートマップ構成が 10.1.1.0/24 を外部 EPG1 に関連付け、サブネット 10.1.1.0/24 が外部 EPG2 に構成されている場合、外部 EPG1 はルートマップによる外部 EPG 決定が優先されるため、10.1.1.0/24 のハードウェアでプログラムされます。

DEC の注意事項と制限事項

- この機能は、BGP と OSPF のみをサポートします。
- DEC は、L3Out デフォルト インポート ルート マップまたは BGP ピア インポート ルート マップでのみサポートされます。
- 共有セキュリティを有効にするには、共有する共有セキュリティフラグとサブネットを使用して外部 EPG を構成します。
- DEC は次の機能をサポートしていません。
 - サイト間
 - 浮動 L3Out との統合
 - スタティックルーティング
 - EIGRP
 - セグメント ルーティング
 - 午前
 - 浮動 L3Out を使用した BGP ネクストホップ伝達
 - Cisco ACI GOLF、SR-MPLS、およびフォールバック ルートとの共存

GUI を使用したダイナミック L3Out EPG 分類の設定

この手順では、ダイナミック L3Out EPG 分類 (DEC) を構成し、BGP を使用してレイヤー 3 外部ネットワーク接続を構成していることを前提としています。OSPF を使用して設定された L3Out に対してこれらのタスクを実行することもできます。

このタスクでは、インポートポリシーとエクスポートポリシーの作成手順を示します。デフォルトでは、インポート制御は適用されていないため、インポート制御を手動で割り当てる必要があります。

始める前に

- テナント、プライベートネットワーク、およびブリッジドメインが作成されていること。

- テナント ネットワークのレイヤ 3 Outside が作成されていること。

-
- ステップ 1** メニューバーで、[テナント (Tenants)] > [すべてのテナント (ALL Tenants)] の順に選択します。
- ステップ 2** [作業 (Work)] ペインで、テナント名をダブルクリックします。
- ステップ 3** [ナビゲーション (Navigation)] ペインで、[tenant_name] > [ネットワークング (Networking)] > [L3Outs] > [L3Out_name] の順に展開します。
- ステップ 4** [Layer3_Outside_name] を右クリックして、[ルート制御のインポートおよびエクスポート向けルートマップの作成 (Create Route map for import and export route control)] をクリックします。
- ステップ 5** [ルート制御のインポートおよびエクスポート向けルートマップの作成 (Create Route map for import and export route control)] ダイアログボックスで、次のアクションを実行します。
- [名前 (Name)] フィールドから、[default-import] を選択します。
選択内容に応じて、特定の L3Out でアドバタイズされている内容が自動的に使用されます。
 - Type** フィールドで、**Match Prefix AND Routing Policy** を選択します。
 - [コンテキスト (Contexts)] 領域で、[+] をクリックして [ルート制御コンテキストの作成 (Create Route Control Context)] ウィンドウを表示します。
- ステップ 6** [Create Route Control Context] ダイアログボックスで、次の操作を実行します。
- [Order] フィールドで、目的の順序の番号を選択します。
 - [Name] フィールドに、ルート制御プライベートネットワークの名前を入力します。
 - [関連する一致したルール (Associated Matched Rules)] テーブルで、[+] をクリックします。
 - [セットルール (Set Rule)] ドロップダウンリストから、[ルートマップのセットルールの作成 (Create Set Rules For a Route Map)] を選択します。
 - [ルートマップの一致ルールの作成 (Create Match Rule for Route Map)] ダイアログボックスの [名前 (Name)] フィールドに、一致ルールの名前を入力します。
 - 必要に応じて、正規表現による一致コミュニティ条件および一致コミュニティ条件を指定します。
一致コミュニティファクタでは、名前、コミュニティ、および範囲を指定する必要があります。
 - [送信 (Submit)] をクリックします。
 - [セットルール (Set Rule)] ドロップダウンリストから、[ルートマップのセットルールの作成 (Create Set Rules For a Route Map)] を選択します。
 - [ルートマップのセットルールの作成 (Create Set Rules For a Route Map)] ダイアログボックスの [名前 (Name)] フィールドに、ルールの名前を入力します。
 - [外部 EPG の設定 (Set External EPG)] チェックボックスをオンにして、[外部 EPG (External EPG)] ドロップダウンリストで EPG を選択して、[完了 (Finish)] をクリックします。
ポリシーが作成され、アクションルールに関連付けられました。
 - [ルート制御コンテキストの作成 (Create Route Control Context)] ダイアログボックスで、[OK] をクリックします。
 - [インポートおよびエクスポート ルート制御向けのルートマップの作成 (Create Route map for import and export route control)] ダイアログボックスで、[送信 (Submit)] をクリックします。
- ステップ 7** [作業 (Work)] ペインで、[ポリシー (Policy)] > [メイン (Main)] タブを選択します。
Work ウィンドウに、**Properties** が表示されます。

ステップ 8 (任意) [ルート制御の強化 (Route Control Enforcement)] フィールドのとなりの [インポート (Import)] チェック ボックスをオンにして、インポート ポリシーを有効にして [送信 (Submit)] をクリックします。

インポート制御ポリシーはデフォルトで無効になっています。インポート制御ポリシーは BGP と OSPF でサポートされていますが、EIGRP ではサポートされていません。ユーザーがサポートされていないプロトコルのインポート制御ポリシーを有効にしても、プロトコルは自動的に無視されます。エクスポート制御ポリシーは、BGP、EIGRP、および OSPF でサポートされます。また、ネイバー インポート ルート マップごとに BGP を設定する場合は、インポート ポリシーの [インポート (Import)] チェック ボックスをオンにする必要はありません。

(注) BGP が OSPF 上で確立されると、インポート制御ポリシーは BGP にのみ適用され、OSPF は無視されます。

ステップ 9 カスタマイズされたエクスポートポリシーを作成するには、[ナビゲーション (Navigation)] ペインで、[ルート制御のインポートおよびエクスポートのルート マップ (Route Map for import and export route control)] を右クリックし、[ルート制御のインポートおよびエクスポートのルート マップの作成 (Create Route Map for import and export route control)] をクリックし、次のアクションを実行します。

- a) [ルート制御のインポートおよびエクスポート向けルート マップの作成 (Create Route map for import and export route control)] ダイアログ ボックスで、[名前 (Name)] ドロップダウン リストから、エクスポート ポリシーを選択するか、名前を入力します。
- b) [コンテキスト (Contexts)] 領域で、[+] をクリックして [ルート制御コンテキストの作成 (Create Route Control Context)] ダイアログを開きます。
- c) [ルート制御コンテキストの作成 (Create Route Control Context)] ダイアログボックスの [注文 (Order)] フィールドに、値を入力します。
- d) [Name] フィールドに、ルート制御プライベート ネットワークの名前を入力します。
- e) (任意) [関連する一致ルール (Associated Match Rules)] テーブルで、[+] をクリックし、[ルール名 (Route Name)] ドロップダウン リストから [ルート マップの一致ルールを作成 (Create Match Rule For a Route Map)] を選択し、必要に応じてフィールドに入力して、[送信 (Submit)] をクリックします。
- f) [セット ルール (Set Rule)] ドロップダウン リストから、[ルート マップのセット ルールの作成 (Create Set Rules For a Route Map)] を選択します。

または、既存のセット ルールを選択できます。

- g) [ルート マップのセット ルールの作成 (Create Set Rules For a Route Map)] を選択した場合は、[ルート マップのセット ルールの作成 (Create Set Rules For A Route Map)] ダイアログ ボックスで、[名前 (Name)] フィールドにセット ルールの名前を入力し、設定するルールのチェック ボックスをオンにして、次のように入力します。ルールに適切な値を入力し、[完了 (Finish)] をクリックします。

[Create Route Control Context] ダイアログ ボックスでは、ポリシーが作成されてアクション ルールに関連付けられています。

- h) **OK** をクリックします。
- i) [インポートおよびエクスポート ルート制御向けのルート マップの作成 (Create Route map for import and export route control)] ダイアログ ボックスで、[送信 (Submit)] をクリックします。

[Work] ペインに、エクスポート ポリシーが表示されます。

(注) エクスポート ポリシーを有効にするには、最初に適用する必要があります。この例では、このポリシーはネットワークのすべてのサブネットに適用されます。

ステップ 10 [ナビゲーション (Navigation)] ペインで *[tenant_name]* > [ネットワーク (Networking)] > [L3Outs] > *[L3Out_name]* > [外部 EPG (External EPGs)] > *[external_EPG_name]* の順に展開して、次のアクションを実行します。

- a) ルート制御プロファイル テーブルで、+ をクリックします。
 - b) [名前 (Name)] フィールドのドロップダウン リストから、前に作成したポリシーを選択します。
 - c) [方向 (Direction)] フィールドのドロップダウン リストから、[ルートエクスポートポリシー (Route Export Policy)] を選択します。
 - d) **Update** をクリックします。
 - e) [送信 (Submit)] をクリックします。
-



第 23 章

トランジット ルーティング

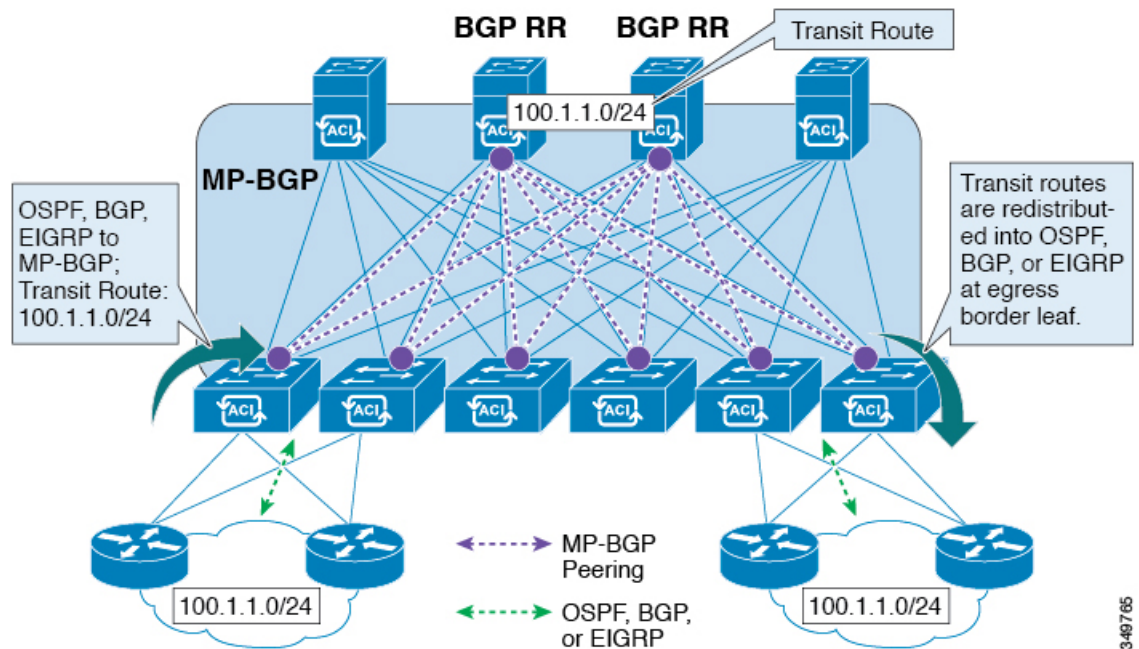
この章は、次の内容で構成されています。

- [中継 ACI ファブリックのルーティング \(381 ページ\)](#)
- [トランジット ルーティングの使用例 \(382 ページ\)](#)
- [サポートされるトランジットの組み合わせのマトリックス \(388 ページ\)](#)
- [トランジット ルーティングの注意事項 \(390 ページ\)](#)
- [トランジット ルーティングの設定 \(399 ページ\)](#)

中継 ACI ファブリックのルーティング

Cisco APIC ソフトウェアは、OSPF (NSSA) および iBGP を使用した外部レイヤ 3 接続をサポートします。ファブリックは、外部レイヤ 3 アウトサイド (I3out) 接続の外部ルータにテナントブリッジドメインのサブネットをアドバタイズします。外部ルータから学習されたルートは、他の外部ルータにアドバタイズされません。ファブリックはスタブネットワークと同じように動作し、外部レイヤ 3 ドメイン間のトラフィックの伝送に使用できます。

図 40: ファブリックでルーティング中継



中継のルーティングで1つのテナントとVRF内の複数のL3Out接続がサポートされているし、APICは別のL3Out接続を1つのL3Out接続から学習したルートを実バタイズします。外部レイヤ3ドメインは、境界リーフスイッチのファブリックとピアリングします。ファブリックはピア間のMultiprotocol-Border Gateway Protocol (MP-BGP) 中継ドメインです。

外部L3Out接続の設定は、テナントとVRFレベルで実行されます。外部ピアから学習したルートは、VRFごとに入力リーフのMP-BGPにインポートされます。L3Out接続から学習したプレフィックスは、テナントVRFが存在するリーフスイッチにのみエクスポートされます。



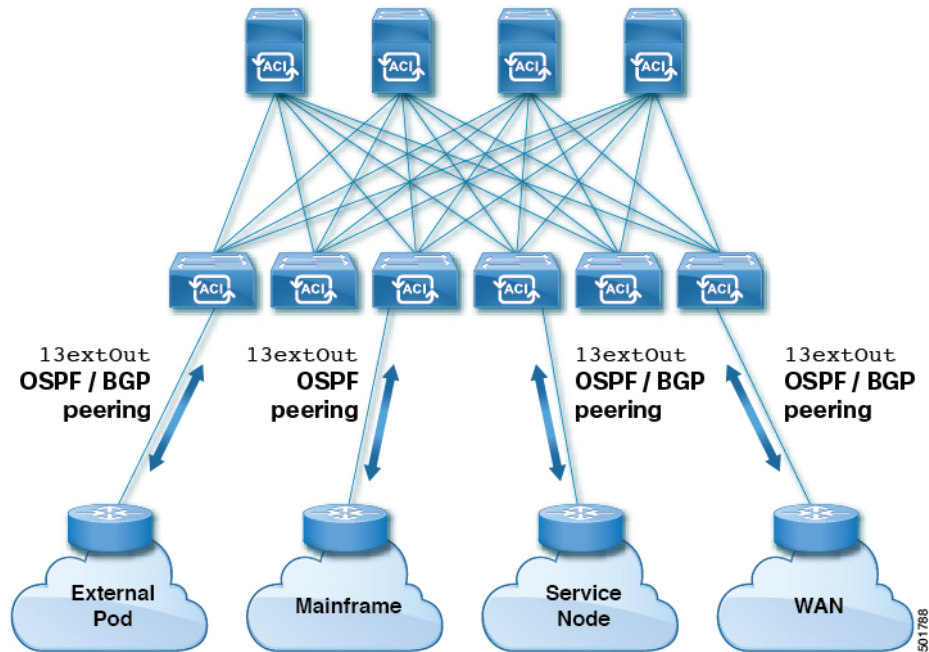
(注) 注意事項と中継ルーティングの設定のガイドラインは、次を参照してください。[中継ルーティングのガイドライン \(390 ページ\)](#)

トランジットルーティングの使用例

レイヤ3ドメイン間のトランジットルーティング

外部ポッド、メインフレーム、サービスノード、WANルータなどの複数のレイヤ3ドメインがACIファブリックとピアリングして、それらの間のトランジット機能を提供することができます。

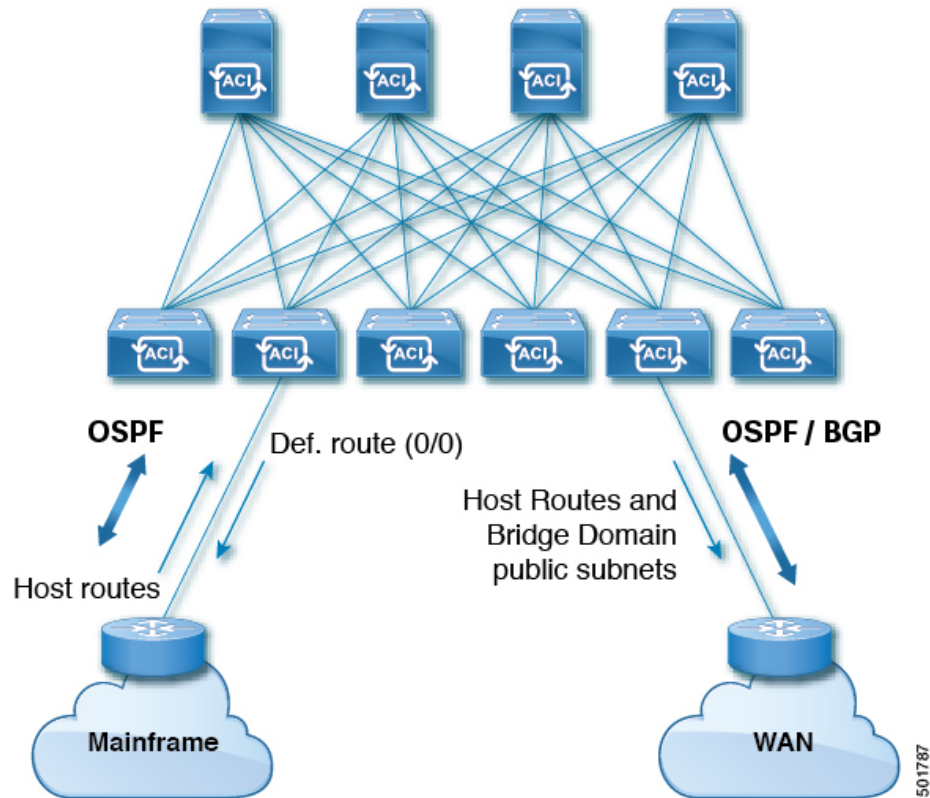
図 41: レイヤ 3 ドメイン間のトランジットルーティング



ACI ファブリックで中継されるメインフレームトラフィック

メインフレームは、論理パーティション (LPAR) および仮想 IP アドレスリング (VIPA) の要件に対応する標準 IP ルーティングプロトコルを実行する IP サーバとして機能します。

図 42: メインフレームのトランジット接続

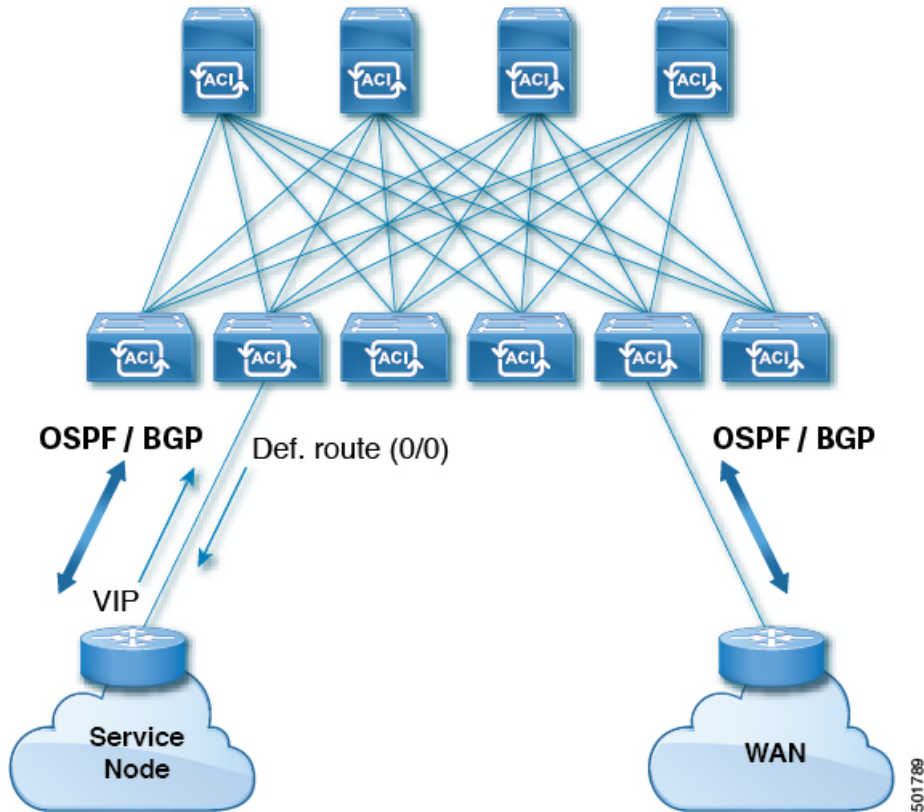


このトポロジにおいて、メインフレームは、ACI ファブリックが WAN ルータを経由して外部と接続するため、およびファブリック内の East-West トラフィックのための中継ドメインとなることを必要とします。これらは、ホストルートを手動でファブリックにプッシュして、ファブリック内、および外部インターフェイスに再配布されるようにします。

サービスノードのトランジット接続

サービスノードは ACI ファブリックとピアリングし、外部 WAN インターフェイスに再配布される仮想 IP (VIP) ルートをアドバタイズすることができます。

図 43: サービス ノードのトランジット接続

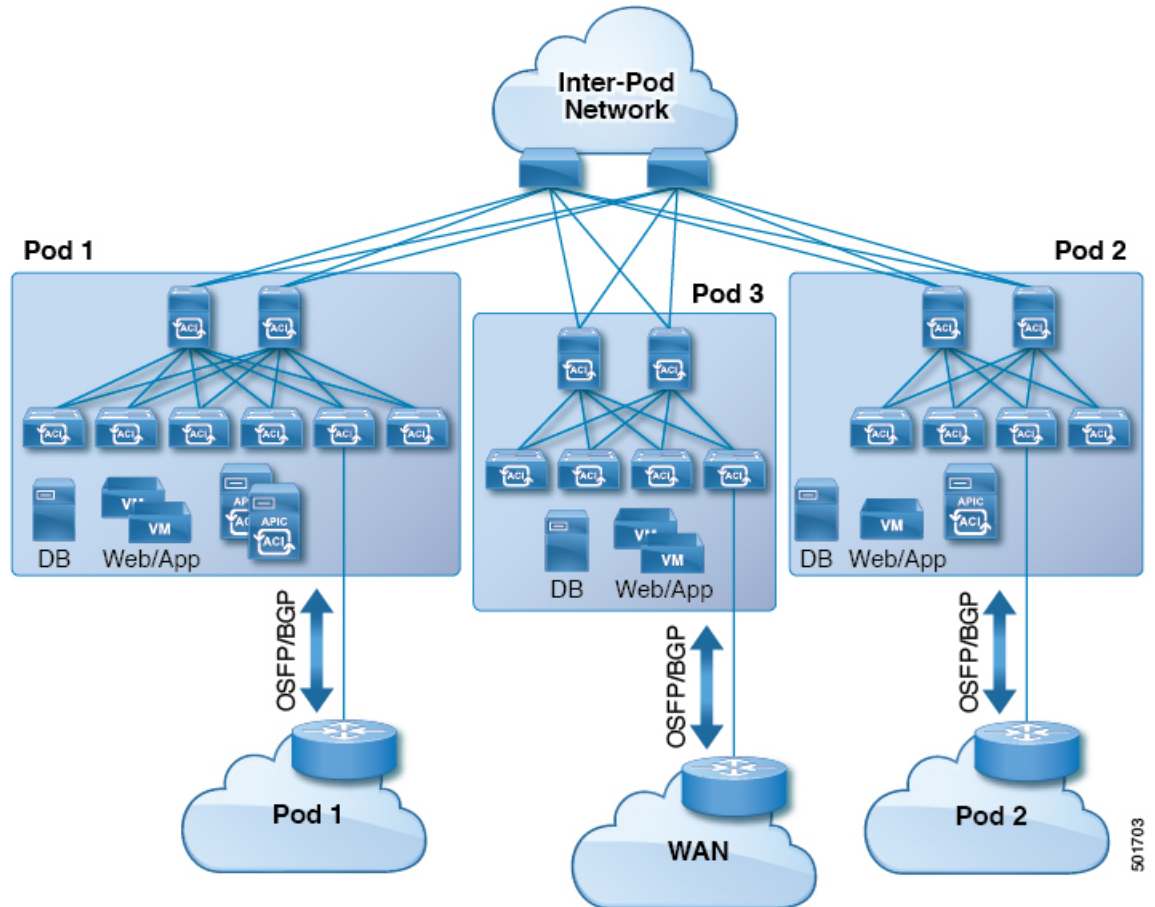


VIP は、特定のサイトやサービスの外部向けの IP アドレスです。VIP は、サービス ノードの背後にある 1 つ以上のサーバまたはノードに関連付けられています。

中継ルーティング設定でのマルチポッド

マルチポッドトポロジでは、ファブリックは、外部接続と複数のポッド間の相互接続の中継として機能します。クラウドプロバイダは、顧客データセンター内に管理対象のリソースポッドを展開できます。責任分界点は、ファブリックとのピアリングを行っている OSPF または BGP を伴う L3Out にすることができます。

図 44: 中継ルーティング設定における L3Out を伴う複数のポッド

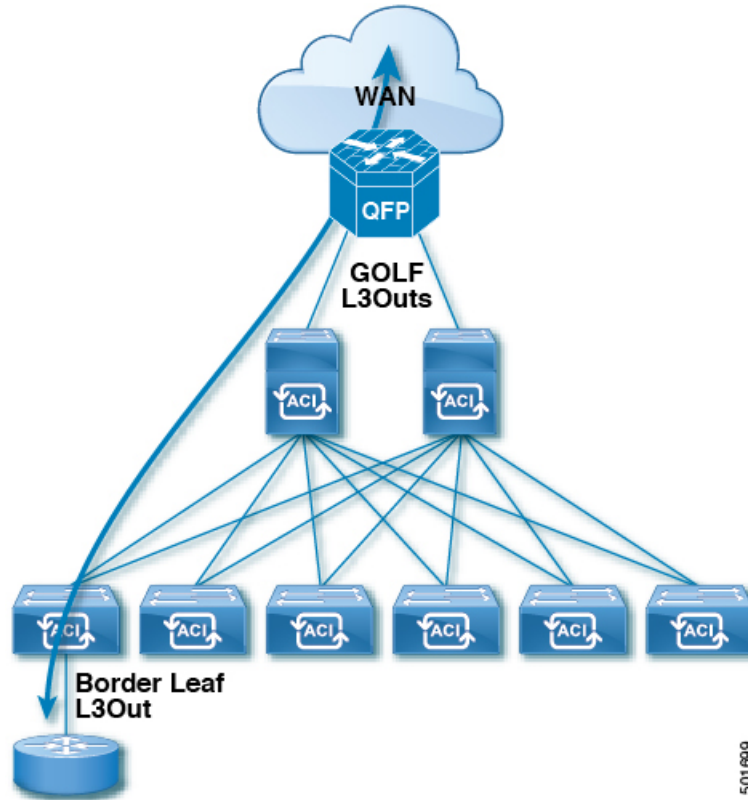


このようなシナリオでは、ポリシーは責任分界点で管理され、ACI ポリシーを設定する必要はありません。

レイヤ4～レイヤ7ルートピアリングはファブリックを中継として使用する特殊な使用例であり、ファブリックは複数ポッドに対する中継OSPFまたはBGPドメインの役目を果たします。ルートピアリングは、接続されているリーフノードとルートとを交換できるようにするため、レイヤ4～レイヤ7サービスデバイス上でOSPFまたはBGPピアリングを有効にするように設定します。ルートピアリングの一般的な使用例として、SLB VIPがOSPFおよびiBGPを介してファブリック外のクライアントにアドバタイズされる、ルートヘルスインジェクションがあります。このシナリオの詳細については、『*L4-L7 Route Peering with Transit Fabric - Configuration Walkthrough*』を参照してください。

中継ルーティング設定での GOLF

APIC、リリース 2.0 以降では、Cisco ACI は、GOLF L3Out での中継ルーティング (BGP と OSPF) をサポートしています。たとえば、次の図は、GOLF L3Out と境界リーフ L3Out を伴うファブリックで中継されるトラフィックを示しています。

図 45: 中継ルーティング設定での *GOLF L3Out* と境界リーフ *L3Out*

サポートされるトランジットの組み合わせのマトリックス

レイヤ 3 Outside 接続タイプ		OSPF	iBGP			eBGP			EIGRP v4	EIGRP v6	スタ ティッ ク ルー ト
			OSPF 上 の iBGP	スタ ティッ ク ルー ト上 の iBGP	直接接 続上の iBGP	OSPF 上 の eBGP	スタ ティッ ク ルー ト上 の eBGP	直接接 続上の eBGP			
OSPF		はい	対応*	はい	○* (APIC リリース 1.3 c でテスト)	はい	はい	はい	はい	○* (APIC リリース 1.2 g でテ スト)	○
iBGP	OSPF 上 の iBGP	○*	X	X	X	○* (APIC リリース 1.3 c でテスト)	非対 応	はい	はい	非対 応	○
	スタ ティッ ク ルー ト 上 の iBGP	はい	X	X	X	○* (APIC リリース 1.2 g でテスト)	X	○* (APIC リリース 1.2 g でテスト)	はい	非対 応	○
	直接接 続上 の iBGP	はい	X	X	X	-	X	○* (APIC リリース 1.2 g でテスト)	はい	非対 応	○

レイヤ 3 Outside 接続タイプ		OSPF	iBGP			eBGP			EIGRP v4	EIGRP v6	スタ ティッ ク ルー ト
			OSPF 上 の iBGP	スタ ティッ ク ルー ト 上 の iBGP	直接接 続上 の iBGP	OSPF 上 の eBGP	スタ ティッ ク ルー ト 上 の eBGP	直接接 続上 の eBGP			
eBGP	OSPF 上 の eBGP	はい	○* (APIC リ リー ス 1.3 c で テ ス ト)	○* (APIC リ リー ス 1.3 c で テ ス ト)	○* (APIC リ リー ス 1.3 c で テ ス ト)	はい	○* (APIC リ リー ス 1.3 c で テ ス ト)	○* (APIC リ リー ス 1.3 c で テ ス ト)	はい	非対 応	○* (APIC リ リー ス 1.3 c で テ ス ト)
	スタ ティッ ク ルー ト 上 の eBGP	はい	X	X	X	○* (APIC リ リー ス 1.2 g で テ ス ト)	○ (APIC リ リー ス 3.0 で テ ス ト)	○* (APIC リ リー ス 1.2 g で テ ス ト)	はい	非対 応	○
	直接接 続上 の eBGP	はい	はい	はい	○* (APIC リ リー ス 1.3 c で テ ス ト)	○* (APIC リ リー ス 1.3 c で テ ス ト)	○* (APIC リ リー ス 1.3 c で テ ス ト)	はい	はい	非対 応	○
EIGRPv4		はい	はい	はい	はい	はい	はい	はい	○ (APIC リ リー ス 1.3 c で テ ス ト)	非対 応	○

レイヤ 3 Outside 接続タイプ	OSPF	iBGP			eBGP			EIGRP v4	EIGRP v6	スタ ティッ ク ルー ト
		OSPF 上 の iBGP	スタ ティッ ク ルー ト上 の iBGP	直接接 続上の iBGP	OSPF 上 の eBGP	スタ ティッ ク ルー ト上 の eBGP	直接接 続上の eBGP			
EIGRPv6	○ (APIC リ リー ス 1.2 g でテ スト)	X	X	X	X	X	X	X	○ (APIC リ リー ス 1.3 c でテ スト)	○ (APIC リ リー ス 1.2 g でテ スト)
スタティック ルート	はい	はい	はい	はい	○ (APIC リ リー ス 1.3 c でテス ト)	はい	はい	はい	○ (APIC リ リー ス 1.2 g でテ スト)	○

- 接続= 接続
- * = 同じリーフ スイッチではサポートされません
- × = サポートされていないかテストされていない組み合わせ

トランジットルーティングの注意事項

中継ルーティングのガイドライン

作成し、中継ルーティング接続を維持する場合は、次のガイドラインを使用します。

トピック	注意またはガイドライン
<p>複数の VRF 間のトランジットルーティング時の ACI ファブリック iBGP への OSPF/EIGRP 再配布：ルートタグ</p>	<p>外部ルータを使用して複数の VRF 間のルーティングを行う中継ルーティングシナリオでは、デフォルトルートタグ (4294967295) 以外のエントリを使用して異なる VRF のポリシーを識別する場合に、1 つまたは複数の OSPF または EIGRP のテナント L3Out から取り消されたルートが存在する時にルーティングがループするリスクがあります。</p> <p>これは想定されている動作です。EIGRP/OSPF が ACI ファブリックにルートを再配布すると、境界リーフスイッチのデフォルトの iBGP アンチルーティングループメカニズムは、特定のデフォルトルートタグ 4294967295 を使用するか、または [VRF/ポリシー (VRF/Policy)] ページの [トランジットルートタグポリシー (Transit Route Tag Policy)] フィールドで割り当てられたものと同じタグを使用します。</p> <p>VRF ごとに異なる固有の中継ルートタグを設定すると、デフォルトのアンチルーティングループメカニズムは機能しません。この状況を回避するには、すべての VRF で [トランジットルートタグポリシー (Transit Route Tag Policy)] フィールドに同じ値を使用します。ルートマップとタグの使用に関する詳細については、「OSPF または EIGRP のバックツーバック設定」の行と、この表のルート制御プロファイルポリシーに関するその他の情報を参照してください。</p> <p>(注) ルートタグポリシーは、[ルートタグポリシーの作成 (Create Route Tag Policy)] ページで設定します。このページには、[VRF/ポリシー (VRF/Policy)] ページの [トランジットルートタグポリシー (Transit Route Tag Policy)] フィールドからアクセスします。</p> <p>[テナント (Tenants)] > [tenant_name] > [ネットワーキング (Networking)] > [VRFs] > [VRF_name] の順にクリックします。</p>

トピック	注意またはガイドライン
中継が1つのL3Outプロファイルを使用してルーティング	<p>前に APIC リリース 2.3(1f) では、ルーティングを通過、1つのL3Outプロファイル内ではサポートされていませんでした。APIC2.3(1f)のリリース、および以降では、中継が単一L3Outプロファイルで、次の制限でルーティングを設定できます。</p> <ul style="list-style-type: none"> • VRF が適用されるではない場合は、同じL3EPGを共有ルータ間のトラフィックを許可する0.0.0.0/0の外部のサブネット (l3extSubnet) を使用できます。 • 外部デフォルトサブネット (0.0.0.0/0) の場合は、VRFを適用すると、できません 同一のレイヤ3 EPG内のトラフィックの送信元と宛先の両方のプレフィックスに一致するために使用します。同一のレイヤ3 EPG内のすべてのトラフィックを一致するには、次のプレフィックスがサポートされています。 <ul style="list-style-type: none"> • IPv4 <ul style="list-style-type: none"> • 外部 EPG の 0.0.0.0/1—with 外部サブネット • 外部 EPG の 128.0.0.0/1—with 外部サブネット • 0.0.0.0/0—with インポートルート制御サブネット、集約のインポート • IPv6 <ul style="list-style-type: none"> • 0::0/1: 外部 EPG の外部のサブネットを持つ • 8000::0/1: 外部 EPG の外部のサブネットを持つ • 0:0/0: インポートルート制御のサブネットで集約のインポート • また、VzAny 契約と組み合わせると、1つのデフォルトのサブネット (0.0.0.0/0) を使用できます。次に例を示します。 <ul style="list-style-type: none"> • 使用契約とレイヤ3 EPG の提供 VzAny 消費契約 (一致する 0.0.0.0/0)、または、VzAny には、契約とレイヤ3 EPG が提供される契約 (0.0.0.0/0 に一致する) が使用された行数。 • サブネット 0.0.0.0/0—with インポート/エクスポートルート制御サブネット、集約のインポートおよび集約エクスポートを使用します。

トピック	注意またはガイドライン
ハードウェア サポートの違いを共有ルート:	<p>第2世代のスイッチの VRF 機能間で正常にルートが共有されます (N9K-93108TC-EX など、スイッチモデル名の最後やその後に「EX」や「FX」がつく Cisco Nexus N9K)。第1世代のスイッチですが、ルートを保存する物理的な3進コンテンツ対応メモリ (TCAM) にルートの解析を完全にサポートするだけの容量がないため、この設定のパケットは失敗する可能性があります。</p>
背面に戻る設定で EIGRP や OSPF	<p>Cisco APIC では、中継が、L3Out に設定されているエクスポート ルート制御ポリシーのルーティングをサポートします。ルート(プレフィックス)を通過するこれらのポリシー制御は、L3Out でルーティングプロトコルに再配送されます。これらの中継ルートは、EIGRP や OSPF に再配布されたが、これらはルーティングループを防ぐためにタグ付けされた 4294967295 です。Cisco ACI ファブリックは、OSPF または EIGRP L3Out で学習すると、このタグに一致するルートを受け入れません。ただし、次の場合、この動作をオーバーライドする必要があります。</p> <ul style="list-style-type: none"> • EIGRP や OSPF を使用して、2つの Cisco ACI ファブリックを接続します。 • EIGRP や OSPF を使用して、同じ Cisco ACI ファブリックで2つの異なる Vrf を接続します。 <p>オーバーライドが必要な場合、APIC GUI の次の場所に別のタグ ポリシーを使用して VRF を設定する必要があります。[テナント (Tenant)] > [Tenant_name] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [ルート タグ (Route Tag)] 異なるタグを適用します。</p> <p>新しいルートタグポリシーを作成するだけでなく、APIC GUI の次の場所でのこのポリシーを使用する VRF を更新します。[テナント (Tenant)] > [Tenant_name] > [ネットワーキング (Networking)] > [VRFs] > [Tenant_VRF] VRF を作成したルート タグ ポリシーを適用します。</p> <p>(注) 複数 L3Outs または同じ L3Out で複数のインターフェイスは同じリーフ スイッチに導入し、中継ルーティングに使用、(、IGP に再配布されません) IGP 内で、ルートをアドバタイズします。この状況では、ルート タグ ポリシーは適用されません。</p>

トピック	注意またはガイドライン
BD サブネットをファブリック外にアドバタイズする	<p>インポートおよびエクスポートのルート制御ポリシーは、中継ルート（他の外部ピアから学習したルート）およびスタティック ルートのみに適用されます。テナント BD サブネット上に設定されているファブリック内部のサブネットは、エクスポート ポリシー サブネットを使用して外部にアドバタイズされません。IP プレフィックス リストおよびルート マップを使用すると IP テナント サブネットは許可されますが、これらは別の設定手順を使用して実装されます。テナント サブネットをファブリックの外部にアドバタイズする場合は、次の設定手順を参照してください。</p> <ol style="list-style-type: none"> 1. [subnet properties] ウィンドウで、テナント サブネットの範囲を [Public Subnet] として設定します。 2. オプション。[subnet properties] ウィンドウで、[Subnet Control] を [ND RA Prefix] として設定します。 3. テナントブリッジドメイン (BD) を外部レイヤ 3 Outside に関連付けます (L3Out)。 4. テナント EPG と外部 EPG 間にコントラクト (プロバイダ/コンシューマ) の関連付けを作成します。 <p>BD サブネットを Public 範囲に設定し、BD をレイヤ 3 Out に関連付けると、BD サブネットプレフィックスの境界リーフに IP プレフィックスおよびルートマップの連続エントリが作成されます。</p>

トピック	注意またはガイドライン
デフォルト ルートのアドバタイズ	<p>デフォルトルートのみを必要とするファブリックへの外部接続の場合、OSPF、EIGRP、および BGP の L3Out 接続をデフォルト ルートの起点とすることがサポートされます。外部ピアからデフォルト ルートが受信されると、この文書で説明されている中継エクスポート ルート制御に従って、このルートを別のピアに再配布できます。</p> <p>デフォルト ルートは、デフォルト ルート リーク ポリシーを使用してアドバタイズすることもできます。このポリシーは、デフォルト ルートがルーティング テーブル内にあるか、または常にデフォルト ルートをアドバタイズすることがサポートされている場合、デフォルト ルートのアドバタイズをサポートします。デフォルト ルート リーク ポリシーは、L3Out 接続で設定されます。</p> <p>デフォルトルート リーク ポリシーを作成するときは、以下のガイドラインに従ってください:</p> <ul style="list-style-type: none"> • BGP の場合、Always プロパティは適用されません。 • BGP の場合、Scope プロパティを設定するときには、Outside を選択します。 • OSPF の場合、範囲の値が Context だとタイプ 5 LSA が作成されるのに対し、Outside だとタイプ 7 LSA が作成されます。選択した場合は、L3Out で設定されたエリアのタイプによって異なります。エリアタイプが場合 定期的な、範囲を設定します コンテキスト。エリアタイプが場合 NSSA、範囲を設定します 外部。 • EIGRP で、Scope プロパティを選択する場合には、Context を選択する必要があります。
MTU	<p>Cisco ACI は、IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ 3 Outside (L3Out) 接続、または Inter-Pod Network (IPN) を介した multipod 接続を設定する場合は、MTU が両側で適切に設定されていることが重要です。ACI、Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定された MTU 値は IP ヘッダーを考慮に入れています (結果として、最大パケットサイズは、ACI で 9216 バイト、NX-OS および IOS で 9000 バイトに設定されます)。ただし、IOS XR などの他のプラットフォームは、パケットヘッダーを除く MTU 値を設定します (結果として最大パケットサイズは 8986 バイトになります)。</p> <p>各プラットフォームの適切な MTU 値については、それぞれの設定ガイドを参照してください。</p> <p>CLI ベースのコマンドを使用して MTU をテストすることを強く推奨します。たとえば、Cisco NX-OS CLI で <code>ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1</code> などのコマンドを使用します。</p>

トランジットルート制御

ルートトランジットは、インポートされるレイヤ3アウトサイドネットワーク L3extOut プロファイル (l3extInstP) を通してトラフィックをインポートするために定義されます。異なるルートトランジットは、エクスポートされる別の l3extInstP を通してトラフィックをエクスポートするために定義されます。

ファブリック内の1つまたは複数のノードに複数の l3extOut ポリシーを配置できるので、プロトコルのさまざまな組み合わせがサポートされます。プロトコルの組み合わせはすべて、複数の l3extOut ポリシーを使用して1つのノードに配置することも、または複数の l3extOut ポリシーを使用して複数のノードに配置することも可能です。同じファブリック内の異なる l3extOut ポリシーに3つ以上のプロトコルを配置することもできます。

エクスポートルートマップは、プレフィックスリストの一致から構成されます。各プレフィックスリストは、VRF 内のブリッジドメイン (BD) パブリックサブネットプレフィックスと、外部にアドバタイズする必要のあるエクスポートプレフィックスから構成されます。

ルート制御ポリシーは、l3extOut ポリシーで定義され、l3extOut に関連付けられたプロパティおよび関係によって制御されます。APIC は l3extOut の enforceRtctrl プロパティを使用して、ルート制御方向を適用します。デフォルトでは、エクスポートの制御を適用し、インポートのすべてを許可します。インポートおよびエクスポートされたルート (l3extSubnets) は、l3extInstP で定義されます。すべてのルートのデフォルトスコープはインポートです。これらは、プレフィックスベースの EPG を形成するルートおよびプレフィックスです。

インポートルートマップからのすべてのインポートルートは、BGP および OSPF によってインポートを制御するために使用されます。エクスポートルートマップからのすべてのエクスポートルートは OSPF および BGP によってエクスポートを制御するために使用されます。

インポートとエクスポートのルート制御ポリシーは、異なるレベルで定義されます。IPv6 ではすべての IPv4 ポリシーレベルがサポートされます。l3extInstP および l3extSubnet MO で定義されている追加の関係でインポートを制御します。

デフォルトルートリークは、l3extOut の下の l3extDefaultRouteLeakP MO の定義によって有効になります。

OSPF のエリアごと、BGP のピアごとに l3extDefaultRouteLeakP は Virtual Routing and Forwarding (VRF) 範囲または L3extOut 範囲を有することができます。

次の設定ルールは、ルート制御を提供します。

- rtctrlSetPref
- rtctrlSetRtMetric
- rtctrlSetRtMetricType

rtctrlSetComm MO の追加構文には以下が含まれています。

- no-advertise
- no-export
- no-peer

BGP

ACI ファブリックは、外部ルータとの BGP ピアリングをサポートします。BGP ピアは `l3extOut` ポリシーに関連付けられており、`l3extOut` ごとに複数の BGP ピアを設定することができます。BGP は、`l3extOut` の下で `bgpExtP MO` を定義することにより `l3extOut` レベルで有効化できます。



- (注) `l3extOut` ポリシーにルーティングプロトコル (たとえば、関連する VRF を含む BGP) が含まれる一方で、`L3Out` インターフェイスのプロファイルには必要な BGP インターフェイス設定の詳細が含まれます。いずれも BGP の有効化に必要です。

BGP ピアには、OSPF、EIGRP、接続されたインターフェイス、スタティック ルート、またはループバック経由で到達できます。外部ルータとのピアリングには `iBGP` または `eBGP` を使用できます。ファブリック内への外部ルートの配付には `MP-BGP` が使用されるため、外部ルータからの BGP ルート属性は保持されます。BGP は `l3extOut` に関連付けられた VRF に `Ipv4` や `IPv6` アドレス ファミリーを有効にすることができます。スイッチ上で有効になるアドレス ファミリーは、`bgpPeerP` ポリシーで `l3extOut` のために定義した IP アドレス タイプによって決まります。ポリシーは省略可能です。定義しない場合はデフォルトが使用されます。ポリシーはテナントに対して定義され、名前で参照される VRF によって使用できます。

ピア ポリシーを少なくとも 1 つのピアを定義して、境界リーフ (BL) の各スイッチでプロトコルを有効にする必要があります。ピア ポリシーは 2 つの場所で定義できます。

- `l3extRsPathL3OutAtt` の下：送信元インターフェイスとして物理インターフェイスが使用されます。
- `l3extLNodeP` の下：送信元インターフェイスとしてループバック インターフェイスが使用されます。

OSPF

接続を有効にして冗長性を提供するために、さまざまなホストタイプが OSPF を必要とします。これらには、たとえばファブリック内および WAN へのレイヤ 3 中継として ACI ファブリックを使用するサービス ノード、外部ポッド、メインフレーム デバイスなどがあります。このような外部デバイスは、OSPF を実行している非境界リーフスイッチを介してファブリックとピアリングします。デフォルトルートは受信し、全域ルーティングには参加しないよう、OSPF エリアを NSSA (スタブ) エリアとして設定します。通常は、既存のルーティングの導入によって設定の変更が回避されるため、スタブ エリアの設定は必須ではありません。

`l3extOut` で `ospfExtP` 管理対象オブジェクトを設定して、OSPF を有効にします。BL スイッチ上で設定されている OSPF IP アドレス ファミリー バージョンは、OSPF インターフェイス IP アドレスに設定されているアドレス ファミリーによって決まります。



- (注) 13extOut ポリシーにルーティングプロトコル (たとえば、関連する VRF とエリア ID を含む OSPF) が含まれる一方で、レイヤ 3 外部インターフェイスのプロファイルには必要な OSPF インターフェイスの詳細が含まれます。いずれも OSPF のイネーブル化に必要です。

アドレスファミリごとに設定可能な fvRsCtxToOspfCtxPol 関係を使用して、VRF レベルで OSPF ポリシーを設定します。設定していない場合、デフォルトパラメータが使用されます。

要求されるエリアプロパティ Ipv6 を公開する ospfExtP 管理対象オブジェクトで OSPF を設定します。

サブネットの範囲と集約コントロール

次のセクションでは、サブネットを作成するときに利用できるいくつかの範囲と集約に関するオプションについて説明します:

Export Route Control Subnet: コントロールは、ファブリック外の特定の中継ルートをアドバタイズします。これは中継ルートにのみ影響するもので、内部ルートやブリッジドメインで設定されるデフォルトのゲートウェイには影響しません。

インポートルートコントロールサブネット: このコントロールは、インポートルート制御の強制が設定されている場合、ルートを Border Gateway Protocol (BGP) と Open Shortest Path First (OSPF) でファブリックにアドバタイズすることを可能にします。

External Subnets for the External EPG (セキュリティインポートサブネットとも呼ばれる): このオプションは、ルーティング情報のファブリックへの出入りはコントロールしません。トラフィックがある外部 EPG から別の外部 EPG に、または内部 EPG に流れるようにするには、サブネットにはこのコントロールでマークを付ける必要があります。このコントロールを使用してサブネットにマークしなかった場合には、ある EPG から学習したルートが他の外部 EPG にもアドバタイズされますが、パケットはファブリックでドロップされます。パケットがドロップされるのは、APIC が許可済みリストモデルで動作するからです。そのデフォルトの動作は、契約で明示的に許可されていない限り、EPG 間の全データプレーントラフィックをドロップするというものです。この許可済みリストモデルは外部 EPG とアプリケーション EPG に適用されます。このオプションが設定されているセキュリティポリシーを使用する場合には、契約とセキュリティプレフィックスを設定する必要があります。

Shared Route Control Subnet: VRF 間のリーキングの共有 L3Outs から学習されたサブネットは、他の VRF にアドバタイズされる前に、このコントロールでマークする必要があります。APIC リリース 2.2(2e) 以降では、異なる VRF の共有 L3Outs は契約を使用して相互に通信できます。異なる VRF の共有 L3Outs 間の通信の詳細については、『Cisco APIC レイヤ 3 ネットワーキング構成ガイド』を参照してください。

Shared Security Import Subnet: このコントロールは、共有 L3Out 学習ルートについては、[External Subnets for the External EPG] と同じです。トラフィックがある外部 EPG から別の外部 EPG に、または別の内部 EPG に流れるようにするには、サブネットにはこのコントロールでマークを付ける必要があります。このコントロールを使用してサブネットにマークしなかった場合に

は、ある EPG から学習したルートが他の外部 EPG にもアドバタイズされますが、パケットはファブリックでドロップされます。このオプションが設定されているセキュリティポリシーを使用する場合には、契約とセキュリティプレフィックスを設定する必要があります。

Aggregate Export, Aggregate Import, and Aggregate Shared Routes: このオプションは、0.0.0.0/0 プレフィックスの前に 32 を追加します。現在、インポート/エクスポートルート制御サブネットに集約できるのは、0.0.0.0/0 プレフィックスのみです。0.0.0.0/0 プレフィックスを集約すると、制御プロファイルを 0.0.0.0 ネットワークに適用することはできなくなります。

Aggregate Shared Route: このオプションは、共有ルート制御サブネットとしてマークされている任意のプレフィックスに使用できます。

Route Control Profile: ACI ファブリックは、ファブリックの内部と外部にアドバタイズされるルート用に、ルートマップの set 句もサポートします。ルートマップの set ルールは、ルート制御プロファイルポリシーとアクションルールプロファイルで設定されます。

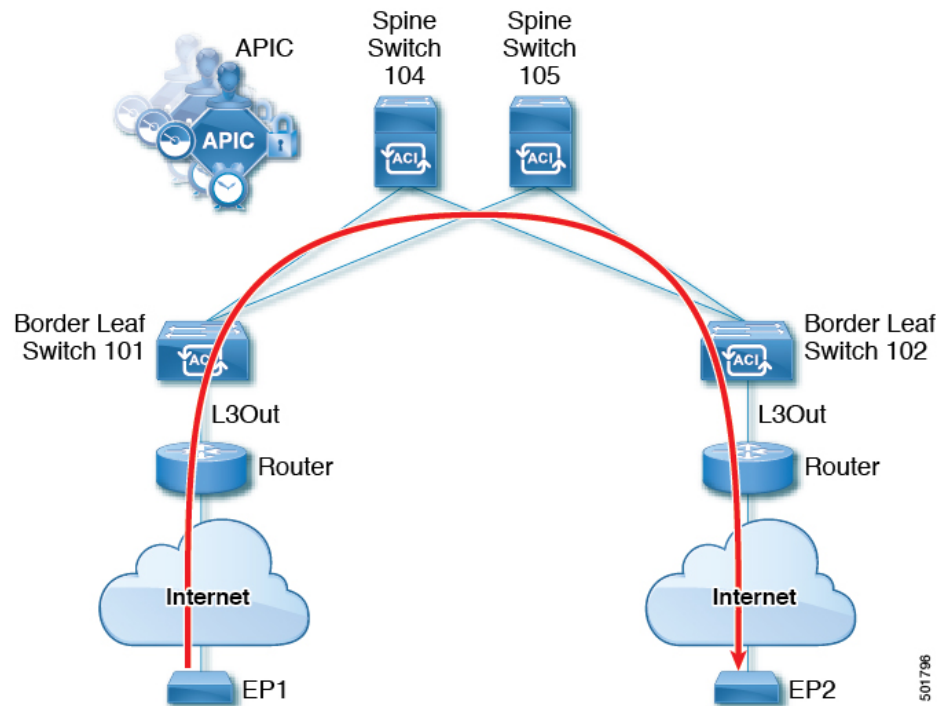
トランジットルーティングの設定

トランジットルーティングの概要

このトピックでは、Cisco APIC を使用する際のトランジットルーティングを設定する方法の一般的な例を説明します。

この章にある例では、次のトポロジを使用します。

図 46:



この章の例では、Cisco ACI ファブリックには APIC クラスタによって制御される 2 個のリーフスイッチと 2 個のスパインスイッチがあります。境界リーフスイッチ 101 と 102 には L3Out があり、2 つのルータに接続することでインターネットにも接続しています。この例の目標は、2 つの L3Out を通して、インターネット上の EP1 から EP2 へ、ファブリック内外をトラフィックが行き来できるようにすることです。

この例では、両方の L3Out に関連付けられているテナントは、t1 と、VRF がつく v1 です。

L3Out を設定する前に、ノード、ポート、機能プロファイル、AEP、レイヤ 3 ドメインを設定します。BGP ルートリフレクタとして 104 と 105 スパインスイッチを設定する必要があります。

トランジットルーティングの設定には、次のコンポーネントの定義が含まれます。

1. テナントおよび VRF
2. リーフ 101 と 102 上のノードおよびインターフェイス
3. 各 L3Out のプライマリルーティングプロトコル（境界リーフスイッチと外部ルータ間のルートの交換に使用。この例では BGP）
4. 各 L3Out のルーティングプロトコルの接続性（プライマリプロトコルへの到達可能性情報の提供。この例では、OSPF）
5. 2 個の外部 EPG
6. 1 個のルートマップ

7. 少なくとも1つのフィルタと1つのコントラクト
8. 外部 EPG とコントラクトを関連付ける



(注) トランジットルーティングの注意事項については、[中継ルーティングのガイドライン \(390 ページ\)](#) を参照してください。

次の表では、この章で使用される名前を一覧にしています。

プロパティ	ノード 101 の L3Out1 の名前	ノード 102 の L3Out2 の名前
テナント	t1	t1
VRF	v1	v1
ノード	ルータ ID 11.11.11.103 を持つ nodep1	ルータ ID 22.22.22.203 を持つ nodep2
OSPF インターフェイス	Eth/1/3 の ifp1	Eth/1/3 の ifp2
BPG ピア アドレス	15.15.15.2/24	25.25.25.2/24
外部 EPG	192.168.1.0/24 の extnw1	192.168.2.0/24 の extnw2
ルート マップ	Ctx1 を持つ rp1 とルートの宛先 192.168.1.0/24	ctx2 を持つ rp2 とルートの宛先 192.168.2.0/24
フィルタ	http-filter	http-filter
コントラクト	extnw1 によって提供される httpCtrct	extnw2 によって消費される httpCtrct

GUI を使用した中継ルーティングの設定

これらの手順は、テナントの中継ルーティングを設定する方法を示しています。この例では、2つの L3Outs を、1つの VRF 内、2つの境界リーフスイッチ上に展開します。スイッチは別々のルータに接続されています。

テナントと VRF を作成する手順を除き、これらの手順を2回繰り返して、同じテナントと VRF の下に2つの L3Out を作成します。

サンプルの名前については、[中継 ACI ファブリックのルーティング \(381 ページ\)](#) を参照してください。

始める前に

- L3Out で使用されるインターフェイス (AAEP、VLAN プール、インターフェイス セレクタ) の L3 ドメインおよびファブリック アクセス ポリシーを設定します。

- ファブリック インフラ MPBGP の BGP ルート リフレクタ ポリシーを設定します。

- ステップ 1** テナントと VRF を作成するには、メニューバーで、**Tenants > Add Tenant** を選択し、**Create Tenant** ダイアログボックスで、次のタスクを実行します:
- Name** フィールドに、テナント名を入力します。
 - In the **VRF Name** フィールドに、VRF 名を入力します。
 - Submit** をクリックします。
- (注) この手順の後の手順は 2 回実行して、中継ルーティングのための同じテナントと VRF に 2 つの L3Out を作成します。
- ステップ 2** L3Out の作成を開始するには、[ナビゲーション (Navigation)] ペインで [テナント (Tenant)] [ネットワークワーキング (Networking)] を展開し、[L3Outs] を右クリックして [L3Out の作成 (Create L3Out)] を選択します。
- [L3Out の作成 (Create L3Out)] ウィザードが表示されます。次の手順では、[L3Out の作成 (Create L3Out)] ウィザードを使用した L3Out 設定例の手順を示します。
- ステップ 3** [L3Out の作成 (Create L3Out)] ウィザードの [識別 (Identity)] ウィンドウに必要な情報を入力します。
- Name** フィールドに L3Out の名前を入力します。
 - VRF** ドロップダウンリストから VRF を選択します。
 - [**L3 ドメイン (L3 Domain)**] ドロップダウンリストで、先ほど作成した、外部ルーテッドドメインを選択します。
 - ルーテッドプロトコルのチェックボックスがある領域で、目的のプロトコル (BGP、OSPF、または EIGRP) をオンにします。
- この章の例では、**BGP** および **OSPF** を選択します。
- 選択するプロトコルに応じて、設定する必要があるプロパティに入力します。
- OSPF を有効にした場合は、OSPF の詳細を入力します。
- この章の例では、OSPF エリア **0** を使用し、**Regular area** に入力します。
- [**次 (Next)**] をクリックして [**ノードとインターフェイス (Nodes and Interfaces)**] ウィンドウに移動します。
- ステップ 4** [L3Out の作成 (Create L3Out)] ウィザードの [**ノードとインターフェイス (Nodes and Interfaces)**] ウィンドウに必要な情報を入力します。
- デフォルトの命名規則を使用するかどうかを決定します。
- [**デフォルトの使用 (Use Defaults)**] フィールドで、デフォルトのノードプロファイル名およびインターフェイスプロファイル名を使用する場合は、チェックをオンにします。
- デフォルトのノードプロファイル名は *L3Out-name_nodeProfile* です。ここで、*L3Out-name* は [識別 (Identity)] ページの [名前 (Name)] フィールドに入力した名前です。

- デフォルトのインターフェイス プロファイル名は `L3Out-name_interfaceProfile` です。ここで、`L3Out-name` は、[識別 (Identity)] ページの [名前 (Name)] フィールドに入力した名前です。

- b) [インターフェイス タイプ (Interface Types)] 領域で、[レイヤ 3 (Layer 3)] および [レイヤ 2 (Layer 2)] フィールドで必要な選択を行います。

次のオプションがあります。

• レイヤ 3 :

- **ルーテッド** : ポート チャネルへのレイヤ 3 ルートを設定するには、このオプションを選択します。

このオプションを選択すると、レイヤ 3 ルートは、このページの [レイヤ 2 (Layer 2)] フィールドで選択された物理ポートまたはダイレクト ポート チャネルのいずれかになります。

- **ルーテッド サブ** : ポート チャネルへのレイヤ 3 サブインターフェイス ルートを設定するには、このオプションを選択します。

このオプションを選択すると、レイヤ 3 サブインターフェイスのルートは、このページの [レイヤ 2 (Layer 2)] フィールドで選択された物理ポートまたはダイレクト ポート チャネルのいずれかになります。

- **SVI** : ACI リーフ スイッチとルータ間に接続性を提供する Switch Virtual Interface (SVI) を設定するにはこのオプションを選択します。

SVI は、物理ポート、直接ポート チャネル、仮想ポート チャネルのメンバーを持つことができ、このページの [レイヤ 2 (Layer 2)] フィールドで選択します。

- **フローティング SVI** : フローティング L3Out を設定するにはこのオプションを選択します。

フローティング L3Out を使用すると、仮想ルータが 1 つのリーフ スイッチの下から別のリーフ スイッチに移動できるようにする L3Out を設定できます。この機能により、VM がホスト間を移動する際に、ルーティングを維持するために複数の L3Out インターフェイスを設定する必要がなくなります。

• レイヤ 2 : (レイヤ 3 エリアで仮想 SVI を選択した場合は使用できません)

- ポート
- 仮想ポート チャネル (レイヤ 3 領域で [SVI] を選択した場合に使用可能)
- ダイレクトポートチャネル(Direct Port Channel)

- c) [ノード ID (Node ID)] フィールドのドロップダウン メニューで、L3Out のノードを選択します。

これらの例のトポロジでは、ノード 103 を使用します。

- d) **Router ID** フィールドで、ルータ ID (L3Out に接続されているルータの IPv4 または IPv6 アドレス) を入力します。

- e) (任意) 必要に応じて、ループバック アドレスに別の IP アドレスを設定できます。
- [ルータ ID (Router ID)] フィールドに入力したエントリと同じ内容が [ループバック アドレス (Loopback Address)] フィールドに自動で入力されます。これは以前のビルドでの [ループバック アドレスのルータ ID の使用 (Use Router ID for Loopback Address)] と同等です。ループバック アドレスにルータ ID を使用しない場合は、ループバック アドレスに別の IP アドレスを入力します。または、ループバック アドレスにルータ ID を使用しない場合は、このフィールドを空のままにします。
- f) [ノードとインターフェイス (Nodes and Interfaces)] ウィンドウに追加の必要な情報を入力します。このウィンドウに表示されるフィールドは、[レイヤ 3 (Layer 3)] および [レイヤ 2 (Layer 2)] 領域で選択したオプションによって異なります。
- g) [ノードとインターフェイス (Nodes and Interfaces)] ウィンドウで残りの追加の情報を入力したら、[次 (Next)] をクリックします。
- [プロトコル (Protocols)] ウィンドウが表示されます。

ステップ 5 [L3Out の作成 (Create L3Out)] ウィザードの [プロトコル (Protocols)] ウィンドウに必要な情報を入力します。

この例ではプロトコルとして BGP と OSPF を使用しているため、次の手順でこれらのフィールドに情報を提供します。

- a) [BGP ループバック ポリシー (BGP Loopback Policies)] および [BGP インターフェイス ポリシー (BGP Interface Policies)] 領域で、次の情報を入力します。
- **ピア アドレス (Peer Address)** : ピア IP アドレスを入力します
 - **EBGP Multihop TTL (EBGP マルチホップ TTL)** : 接続の存続可能時間 (TTL) を入力します。範囲は 1 ~ 255 ホップです。ゼロの場合、TTL は指定されません。デフォルトは 0 です。
 - **リモート ASN (Remote ASN)** : ネイバー自律システムを固有に識別する番号を入力します。自律システム番号は、1 ~ 4294967295 のプレーン形式で 4 バイトにすることができます。
- (注) ACI は asdot または asdot+ 形式の AS 番号をサポートしていません。
- b) [OSPF] 領域で、デフォルト OSPF ポリシー、以前に作成した OSPF ポリシー、または [OSPF インターフェイス ポリシーの作成 (Create OSPF Interface Policy)] を選択します。
- c) [次へ (Next)] をクリックします。
- [外部 EPG (External EPG)] ウィンドウが表示されます。

ステップ 6 [L3Out の作成 (Create L3Out)] ウィザードで [外部 EPG (External EPG)] ウィンドウに必要な情報を入力します。

- a) **Name** フィールドに、外部ネットワークの名前を入力します。
- b) [提供済みコントラクト (Provided Contract)] フィールドで、提供済みコントラクトの名前を入力します。
- c) [消費済みコントラクト (Consumed Contract)] フィールドで、消費済みコントラクトの名前を入力します。

- d) [すべての外部ネットワークのデフォルト EPG (Default EPG for all external network)] フィールドで、この L3Out 接続からのすべての中継ルートをアドバタイズしない場合はオフにします。
このボックスをオフにすると、[Subnets] 領域が表示されます。次の手順に従って、必要なサブネットとコントロールを指定します。
- e) [+] アイコンをクリックして [サブネット (Subnet)] を展開し、[サブネットの作成 (Create Subnet)] ダイアログ ボックスで次の操作を実行します。
- f) **IP address** フィールドに、外部ネットワークの IP アドレスとサブネット マスクを入力します。
- g) [名前 (Name)] フィールドに、サブネットの名前を入力します。
- h) **Scope** フィールドで、L3Out のプレフィックスのインポートとエクスポートを制御するための適切なチェック ボックスをオンにします。
(注) 範囲のオプションの詳細については、この **Create Subnet** パネルのオンラインヘルプを参照してください。
- i) (任意) [ルート制御サブネットのエクスポート (Export Route Control Subnet)] のチェック ボックスをオンにします。
[BGP ルート集約ポリシー (BGP Route Summarization Policy)] フィールドが使用可能になります。
- j) [**BGP ルート集約ポリシー (BGP Route Summarization Policy)**] フィールドでは、ドロップダウン リストから既存のルート集約ポリシーを選択するか、必要に応じて新しいユーザーを作成します。
ルート集約ポリシーのタイプは、L3Out に対して有効になっているルーティング プロトコルに依存します。
- k) [サブネットの作成 (Create Subnet)] ウィンドウで必要な設定が完了したら、[OK] をクリックします。
- l) (任意) より多くのサブネットを追加するにはこれを繰り返します。
- m) [完了 (Finish)] をクリックして、[L3Out の作成 (Create L3Out)] ウィザードに必要な設定の入力を完了させます。

ステップ 7 作成した L3Out に移動し、[L3Out] を右クリックして、[ルート制御のインポートおよびエクスポートのルート マップの作成 (Create Route map for import and export route control)] を選択します。

ステップ 8 [ルート制御のインポートおよびエクスポートのルート マップの作成 (Create Route map for import and export route control)] ウィンドウで、次の操作を実行します。

- a) **Name** フィールドに、ルート マップ名を入力します。
- b) **Type** を選択します。
この例では、デフォルトの **Match Prefix AND Routing Policy** のままにします。
- c) + アイコンをクリックして **Contexts** を展開し、ルート マップのルート コンテキストを作成します。
- d) プロファイル コンテキストの順序と名前を入力します。
- e) このコンテキストで実行するアクションとして **Deny** または **Permit** を選択します。
- f) (任意) **Set Rule** フィールドで、**Create Set Rules for a Route Map** を選択します。

セットルールのための名前を入力し、ルールで使用するオブジェクトをクリックし、**Finish** をクリックします。

- g) [一致ルール (Match Rule)] フィールドで、[ルート マップの一致ルールの作成 (Create Match Rules for a Route Map)] を選択します。
- h) 一致ルールの名前を入力し、ルールで一致させる対象として **正規表現コミュニティ用語の一致 (Match Regex Community Terms)**、**コミュニティ用語の一致 (Match Community Terms)**、または **一致プレフィックス (Match Prefix)** を入力します。
- i) [一致ルールの作成 (Create Match Rule)] ウィンドウのフィールドへの入力完了したら、[送信 (Submit)] をクリックします。
- j) **Create Route Control Context** ダイアログボックスで、**OK** をクリックします。
- k) [インポートおよびエクスポートルート制御向けのルート マップの作成 (Create Route map for import and export route control)] ダイアログボックスで、[送信 (Submit)] をクリックします。

ステップ 9 [ナビゲーション (Navigation)] ペインで [L3Outs] > [L3Out_name] > [外部 EPG (External EPGs)] > [externalEPG_name] の順に展開して、次のアクションを実行します。

- a) + アイコンをクリックして **Route Control Profile** を展開します。
- b) **Name** フィールドのドロップダウンリストから、前に作成したルート制御プロファイルを選択します。
- c) **Direction** フィールドで、**Route Export Policy** を選択します。
- d) **Update** をクリックします。

ステップ 10 作成した L3Out に移動し、[L3Out] を右クリックして、[ルート制御のインポートおよびエクスポートのルート マップの作成 (Create Route map for import and export route control)] を選択します。

ステップ 11 [ルート制御のインポートおよびエクスポートのルート マップの作成 (Create Route map for import and export route control)] ウィンドウで、次の操作を実行します。

(注) 受信ルートについて BGP、OSPF、または EIGRP の属性を設定するには、default-import ルート制御プロファイルを作成し、適切な set アクションと、no match のアクションを作成します。

- a) [名前 (Name)] フィールドから、[default-import] を選択します。
- b) [タイプ (Type)] フィールドでは、[ルーティング ポリシーのみ一致 (Match Routing Policy Only)] をクリックする必要があります。
- c) [インポートおよびエクスポートルート制御向けのルート マップの作成 (Create Route map for import and export route control)] ダイアログボックスで、[送信 (Submit)] をクリックします。

ステップ 12 L3Out を使用していた EPG 間の通信を有効にするには、次の手順を使用して、少なくとも 1 つのフィルタと契約を作成します:

- a) ナビゲーション ウィンドウの L3Out を使用するテナントの下で、**Contracts** を展開します。
- b) **Filters** を右クリックして **Create Filter** を選択します。
- c) **Name** フィールドに、フィルタの名前を入力します。

フィルタは基本的にはアクセス コントロール リスト (ACL) です。

- d) + アイコンをクリックして **Entries** を展開し、フィルタ エントリを追加します。
- e) エントリ の詳細を追加します。

たとえば、単純な Web フィルタの場合には、次のような条件を設定します:

- **EtherType—IP**
- **IP Protocol—tcp**
- **Destination Port Range From—Unspecified**
- **Destination Port Range To to https**

- f) **Update** をクリックします。
- g) **Create Filter** ダイアログボックスで、**Submit** をクリックします。

ステップ 13 契約を追加するには、次の手順を実行します:

- a) **Contracts** の下で、**Standard** を右クリックして、**Create Contract** を選択します。
- b) 契約の名前を入力します。
- c) +アイコンをクリックして **Subjects** を展開し、情報カテゴリを契約に追加します。
- d) 情報カテゴリの名前を入力します。
- e) [+]アイコンをクリックして [**フィルタ (Filters)**] を展開し、ドロップダウンリストから、前に作成したフィルタを選択します。
- f) **Update** をクリックします。
- g) **Create Contract Subject** ダイアログボックスで、**OK** をクリックします。
- h) **Create Contract** ダイアログボックスで、**Submit** をクリックします。

ステップ 14 次の手順で、L3Out の EPG を契約に関連付けます:

最初の L3 外部 EPG (extnw1 が契約のプロバイダとなり、2 番目の外部 EPG、extnw2) がコンシューマとなります。

- a) 契約をプロバイダとしての L3 外部 EPG に関連付けるには、テナントの下で [**ネットワーキング (Networking)**] をクリックし、[**L3Outs**] をクリックし、L3Out を展開します。
- b) [**外部 EPG (External EPGs)**] を展開し、L3 外部 EPG をクリックし、[**コントラクト (Contracts)**] タブをクリックします。
- c) +アイコンをクリックして **Provided Contracts** を展開します。
2 番目の L3 外部 EPG で、+アイコンをクリックして **Consumed Contracts** を展開します。
- d) **Name** フィールドで、前に作成した契約をリストから選択します。
- e) **Update** をクリックします。
- f) [**送信 (Submit)**] をクリックします。



第 24 章

共有サービス

この章は、次の内容で構成されています。

- [共有レイヤ 3 Out \(409 ページ\)](#)
- [レイヤ 3 アウトからレイヤ 3 アウト内部 VRF への漏洩 \(413 ページ\)](#)

共有レイヤ 3 Out

共有レイヤ 3 アウトサイド ネットワーク (L3extOut) は、外部ネットワークへのルーテッド接続を共有サービスとして提供します。L3extOut プロファイル (l3extInstP) EPG は、外部ネットワークへのルーテッド接続を提供します。これは、任意のテナント (*user*、*common*、*infra*、*mgmt.*) の共有サービスとしてプロビジョニングできます。リリース 1.2(1x) より前では、この設定は *user* テナントと *common* テナントでのみサポートされていました。任意のテナントの EPG が、l3extInstP EPG がファブリック内のどこにプロビジョニングされているかには関係なく、共有サービス コントラクトを使用してその l3extInstP EPG に接続できます。これにより、外部ネットワークへのルーテッド接続のプロビジョニングが簡単になります。複数のテナントが、外部ネットワークへのルーテッド接続用に単一の l3extInstP EPG を共有できます。l3extInstP EPG を共有すると、単一の共有 l3extInstP EPG を使用する EPG の数には関係なくスイッチ上で使用されるセッションは 1 つのみであるため、より効率的になります。



- (注) l3extInstP EPG 共有サービス コントラクトを使用するすべてのスイッチは、APIC 1.2 (1x) およびスイッチ 11.2 (1x) の各リリース以降で使用可能なハードウェアおよびソフトウェアのサポートを必要とします。詳細については、「*Cisco APIC Management, Installation, Upgrade, and Downgrade Guide*」とリリース ノート ドキュメントを参照してください。

次の図は、共有 l3extInstP EPG 用に設定された主なポリシー モデル オブジェクトを示しています。

- トラフィック中断 (フラップ) : l3instP EPG が、l3instP サブセットのスコープ プロパティを共有ルート制御 (*shared-ctrl*) または共有セキュリティ (*shared-security*) に設定して外部サブネット 0.0.0.0/0 を使用して設定されると、VRF はグローバル pcTag を使用して再配置されます。これにより、その VRF 内のすべての外部トラフィックが中断されます (VRF がグローバル pcTag を使用して再配置されるため)。
- 共有レイヤ L3extOut のプレフィックスは一意である必要があります。同じコンテキスト (VRF) の同じプレフィックスを使用した、複数の共有 L3extOut 設定は動作しません。VRF にアドバタイズする外部サブネット (外部プレフィックス) が一意であることを確認してください (同じ外部サブネットが複数の l3instP に属することはできません)。プレフィックス prefix1 を使用した L3extOut 設定 (たとえば、L3Out1) と、同様にプレフィックス prefix1 を使用した 2 番目のレイヤ 3 アウトサイド設定 (たとえば、L3Out2) が同じ VRF に属すると、動作しません (導入される pcTag は 1 つのみであるため)。L3extOut のさまざまな動作は、同じ VRF の同じリーフ スイッチに設定されている可能性があります。考えられるシナリオは次の 2 つです。
 - シナリオ 1 には、SVI インターフェイスおよび 2 個のサブネット (10.10.10.0/24 および 0.0.0.0/0) が定義された L3extOut があります。レイヤ 3 アウトサイドネットワークの入力トラフィックに一致するプレフィックス 10.10.10.0/24 がある場合、入力トラフィックは外部 EPG pcTag を使用します。レイヤ 3 アウトサイドネットワーク上の入力トラフィックに一致するデフォルトプレフィックス 0.0.0.0/0 がある場合、入力トラフィックは外部ブリッジ pcTag を使用します。
 - シナリオ 2 には、2 個のサブネット (10.10.10.0/24 および 0.0.0.0/0) が定義されたルーテッドまたは routed-sub-interface を使用する L3extOut があります。レイヤ 3 アウトサイドネットワークの入力トラフィックに一致するプレフィックス 10.10.10.0/24 がある場合、入力トラフィックは外部 EPG pcTag を使用します。レイヤ 3 アウトサイドネットワーク上の入力トラフィックに一致するデフォルトプレフィックス 0.0.0.0/0 がある場合、入力トラフィックは VRF pcTag を使用します。
- これらの説明した動作の結果として、SVI インターフェイスを使用して L3extOut-A および L3extOut-B で同じ VRF および同じリーフ スイッチが設定されている場合、次のユース ケースが考えられます。

ケース 1 は L3extOut -A 用です。この外部ネットワーク EPG には 2 個のサブネットが定義されています。10.10.10.0/24 & 0.0.0.0/1。L3extOut-A の入力トラフィックに一致するプレフィックス 10.10.10.0/24 がある場合、L3extOut-A に関連付けられている外部 EPG pcTag & コントラクトを使用します。L3extOut-A の出力トラフィックに特定的一致がなく、最大のプレフィックス一致が 0.0.0.0/1 の場合、外部ブリッジドメイン (BD) pcTag & コントラクト-A を使用します。

ケース 2 は L3extOut-B です。この外部ネットワーク EPG には定義された 1 個のサブネット: 0.0.0.0/0 があります。L3extOut-B の入力トラフィックに一致するプレフィックス 10.10.10.0/24 (L3extOut-A で定義) がある場合、L3extOut-A に関連付けられている L3extOut-A およびコントラクト A の外部 EPG pcTag を使用します。L3extOut-B に関連付けられているコントラクト-B は使用しません。

- 許可されないトラフィック：無効な設定で、共有ルート制御 (`shared-rtctrl`) に対する外部サブネットの範囲が、共有セキュリティ (`shared-security`) に設定されているサブネットのサブセットとして設定されている場合、トラフィックは許可されません。たとえば、以下の設定は許可されません。

- `shared rtctrl` : 10.1.1.0/24, 10.1.2.0/24
- `shared security` : 10.1.0.0/16

この場合、10.1.1.0/24 および 10.1.2.0/24 の各プレフィックスがドロップルールを使用してインストールされているため、宛先 IP 10.1.1.1 を使用して非境界リーフの入力トラフィックはドロップされます。トラフィックは許可されません。そのようなトラフィックは、`shared-rtctrl` プレフィックスを `shared-security` プレフィックスとしても使用するように設定を修正することで、有効にすることができます。

- 不注意によるトラフィックフロー：次の設定シナリオを避けることで、不注意によるトラフィックフローを予防します。

- ケース 1 設定の詳細：

- VRF1 を持つレイヤ 3 アウトサイド ネットワーク設定 (たとえば、名前付き `L3extOut-1`) は `provider1` と呼ばれます。
- VRF2 を持つ二番目のレイヤ 3 アウトサイド ネットワーク設定 (たとえば、名前付き `L3extOut-2`) は `provider2` と呼ばれます。
- `L3extOut-1` VRF1 は、インターネット `0.0.0.0/0` にデフォルト ルートをアドバタイズし、これは `shared-rtctrl` および `shared-security` の両方を有効にします。
- `L3extOut-2` VRF2 は特定のサブネットを DNS および NTP `192.0.0.0/8` にアドバタイズし、`shared-rtctrl` を有効にします。
- `L3extOut-2` VRF2 に特定の `192.1.0.0/16` があり、`shared-security` を有効にします。
- バリエーション A : EPG トラフィックが複数の VRF に向かいます。
 - EPG1 と `L3extOut-1` の間の通信は `allow_all` コントラクトによって制御されます。
 - EPG1 と `L3extOut-2` の間の通信は `allow_all` コントラクトによって制御されます。

結果 : EPG1 から `L3extOut-2` へのトラフィックも `192.2.x.x` に向かいます。

- バリエーション B : EPG は 2 番目の共有レイヤ 3 アウトサイド ネットワークの `allow_all` コントラクトに従います。
 - EPG1 と `L3extOut-1` の間の通信は `allow_all` コントラクトによって制御されます。
 - EPG1 と `L3extOut-2` の間の通信は `allow_icmp` コントラクトによって制御されます。

結果：EPG1 ~ L3extOut-2 から 192.2.x.x へのトラフィックは *allow_all* コントラクトに従います。

• ケース 2 設定の詳細：

- L3extOut プロファイル (l3instP) は、1 つの共有プレフィックスとその他の非共有プレフィックスを持っています。
- src = non-shared で到達するトラフィックは、EPG に向かうことが許可されません。

- **バリエーション A**：意図しないトラフィックが EPG を通過します。

L3extOut (l3instP) EPG のトラフィックがこれらのプレフィックスを持つ L3extOut に向かいます。

- 192.0.0.0/8 = import-security, shared-rtctrl

- 192.1.0.0/16 = shared-security

- EPG には 1.1.0.0/16 = shared があります

結果：192.2.x.x からのトラフィックも EPG に向かいます。

- **バリエーション B**：意図しないトラフィックが EPG を通過します。共有 L3extOut に到達したトラフィックは EPG を通過できます。

- 共有 L3extOut VRF には、pcTag = prov vrf を持つ EPG と *allow_all* に設定されているコントラクトがあります。

- EPG は <subnet> = shared となっています。

結果：レイヤ3アウトに到達するトラフィックは EPG を通過することができます。

レイヤ3アウトからレイヤ3アウト内部 VRF への漏洩

Cisco APIC リリース 2.2(2e) から、2 つの異なる VRF に 2 個のレイヤ3アウトがある場合、VRF 内部の漏洩がサポートされています。

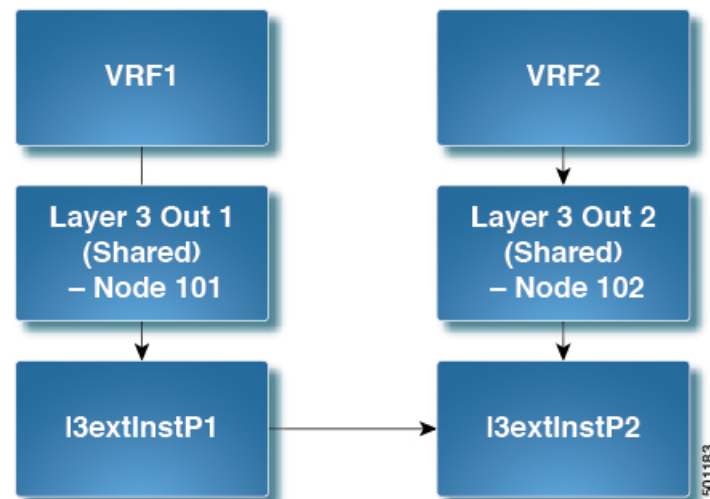
この機能を稼働するには、次の条件を満たす必要があります。

- 2 個のレイヤ3アウト間にはコントラクトが必要です。
- レイヤ3アウトの接続したり移行したりするサブネットのルートは、コントラクトを適用し (L3Out-L3Out および L3Out-EPG)、VRF 間の動的または静的ルートを漏洩させることなく漏洩します。
- 動的または静的ルートは、コントラクトを適用し (L3Out-L3Out および L3Out-EPG)、VRF 間で直接接続したり移行したりするルートをアドバタイズすることなく漏洩します。

- 異なる VRF の共有のレイヤ 3 アウトは相互に通信できます。
- ブリッジ ドメインに必要な関連付けられた L3Out はありません。VRF 間共有 L3Out を使用する場合は、テナント共通の L3Out にユーザ テナント ブリッジ ドメインを関連付ける必要はありません。テナント固有の L3Out がある場合、それぞれのテナントのブリッジ ドメインに関連付けられます。
- 2 個のレイヤ 3 アウトは異なる 2 個の VRF に存在し、正常にルートを交換できます。
- この強化は、アプリケーション EPG およびレイヤ 3 アウト内部 VRF 間の通信と同じです。唯一の違いは、アプリケーション EPG ではなく別のレイヤ 3 アウトが存在します。したがってこの状況では、コントラクトは 2 個のレイヤ 3 アウト間で記録されます。

次の図では、共有サブネットによる 2 個のレイヤ 3 アウトが存在します。両方の VRF でレイヤ 3 外部インスタンス プロファイル (l3extInstP) 間のコントラクトがあります。この場合、VRF 1 の共有レイヤ 3 アウトは VRF 2 の共有レイヤ 3 と通信できます。

図 48: 2 個の VRF 間で通信する共有レイヤ 3 アウト



拡張 GUI を使用した共有レイヤ 3 Out VRF 間リーキングの設定

始める前に

コンシューマとプロバイダーによって使用される契約ラベルがすでに作成されています。

- ステップ 1 メニュー バーで **Tenants > Add Tenant** を選択します。
- ステップ 2 **Create Tenant** ダイアログボックスに、プロバイダーのテナント名を入力します。
- ステップ 3 **[VRF 名 (VRF Name)]** フィールドに、プロバイダの VRF 名を入力し、**[送信 (Submit)]** をクリックしてテナントを作成します。
- ステップ 4 **[ナビゲーション (Navigation)]** ペインの新しいテナント名の下で、**[L3Outs]** に移動します。

- ステップ 5** [L3Outs] を右クリックし、[L3Out の作成 (Create L3Out)] を選択します。
[L3Out の作成 (Create L3Out)] ウィザードが表示されます。
- ステップ 6** [VRF の作成 (Create VRF)] ダイアログ ボックスで、次の操作を実行します。
- Name** フィールドに、L3Out の名前を入力します。
 - [VRF] フィールドで、前に作成した VRF を選択します。
 - [L3 ドメイン (L3 Domain)] フィールドで、L3 ドメインを選択します。
 - プロトコルに適切な選択を行い、[次へ (Next)] をクリックします。
- ステップ 7** [外部 EPG (External EPG)] ウィンドウが表示されるまで、次のウィンドウで必要な選択を行います。
[識別 (Identity)] ウィンドウで選択したプロトコルに応じて、[ノードとインターフェイス (Nodes and Interfaces)] ウィンドウと [プロトコル (Protocols)] ウィンドウが表示される場合があります。[L3Out の作成 (Create L3Out)] ウィザードの最後のウィンドウは、[外部 EPG (External EPG)] ウィンドウです。
- ステップ 8** [外部 EPG (External EPG)] ウィンドウで次のアクションを実行します。
- Name** フィールドに、外部ネットワーク名を入力します。
 - [すべての外部ネットワークのデフォルト EPG (Default EPG for all external network)] チェックボックスをオフにします。
[サブネット (Subnets)] フィールドが表示されます。
 - [サブネットの作成 (Create Subnet)] ウィンドウにアクセスするには、[+] をクリックします。
 - [サブネットの作成 (Create Subnet)] ダイアログ ボックスの [IP アドレス (IP Address)] フィールドに、マッチングを行う IP アドレスを入力します。OK をクリックします。
 - [L3Out の作成 (Create L3Out)] ウィザードで [完了 (Finish)] をクリックします。
- ステップ 9** [ナビゲーション (Navigation)] ペインで、作成した [L3Out_name] [外部 EPG (External EPGs)] [ExternalEPG_name] に移動します。 >>
- ステップ 10** **Work** ウィンドウの、外部ネットワークの **Properties** の下で、**Resolved VRF** フィールドに解決された VRF が表示されていることを確認します。
- ステップ 11** 外部サブネットの IP アドレスをダブルクリックして、[サブネット (Subnet)] ダイアログ ボックスを開きます。
- ステップ 12** **Scope** フィールドで、必要なチェック ボックスをオンにして、**Submit** をクリックします。
このシナリオで、次のチェック ボックスをオンにします。
- [外部 EPG の外部サブネット (External Subnets for the External EPG)]
 - 共有ルートコントロールサブネット
 - 共有セキュリティインポートサブネット
- ステップ 13** 以前に作成した [L3 Outside] に移動します。
- ステップ 14** [プロバイダラベル (Provider Label)] フィールドに、このタスクを開始するための前提条件として作成したプロバイダ名を入力します。Submit をクリックします。
- ステップ 15** メニュー バーで、**Tenants > Add Tenant** をクリックします。

- ステップ 16 [テナントの作成 (Create Tenant)] ダイアログボックスで、L3 コンシューマのためのテナント名を入力します。
- ステップ 17 VRF Name フィールドに、コンシューマの VRF 名を入力します。
- ステップ 18 [ナビゲーション (Navigation)] ペインの新しいテナント名の下で、コンシューマの [L3Outs] に移動します。
- ステップ 19 [L3Outs] を右クリックし、[L3Out の作成 (Create L3Out)] を選択します。
[L3Out の作成 (Create L3Out)] ウィザードが表示されます。
- ステップ 20 [VRF の作成 (Create VRF)] ダイアログボックスで、次の操作を実行します。
- Name フィールドに、L3Out の名前を入力します。
 - [VRF] フィールドで、ドロップダウンメニューから、コンシューマのために作成された VRF を選択します。
 - Consumer Label フィールドに、コンシューマ ラベルの名前を入力します。
 - [L3 ドメイン (L3 Domain)] フィールドで、L3 ドメインを選択します。
 - プロトコルに適切な選択を行い、[次へ (Next)] をクリックします。
- ステップ 21 [外部 EPG (External EPG)] ウィンドウが表示されるまで、次のウィンドウで必要な選択を行います。
[識別 (Identity)] ウィンドウで選択したプロトコルに応じて、[ノードとインターフェイス (Nodes and Interfaces)] ウィンドウと [プロトコル (Protocols)] ウィンドウが表示される場合があります。[L3Out の作成 (Create L3Out)] ウィザードの最後のウィンドウは、[外部 EPG (External EPG)] ウィンドウです。
- ステップ 22 [外部 EPG (External EPG)] ウィンドウで次のアクションを実行します。
- Name フィールドに、外部ネットワーク名を入力します。
 - [すべての外部ネットワークのデフォルト EPG (Default EPG for all external network)] チェックボックスをオフにします。
[サブネット (Subnets)] フィールドが表示されます。
 - [サブネットの作成 (Create Subnet)] ウィンドウにアクセスするには、[+] をクリックします。
 - [サブネットの作成 (Create Subnet)] ダイアログボックスの [IP アドレス (IP Address)] フィールドに、マッチングを行う IP アドレスを入力します。OK をクリックします。
 - Scope フィールドで、必要なチェックボックスをオンにして、OK をクリックします。
このシナリオでは、Shared Route Control Subnet と Shared Security Import Subnet のチェックボックスをオンにします。
 - [L3Out の作成 (Create L3Out)] ウィザードで [完了 (Finish)] をクリックします。

これで、共有レイヤ 3 Out VRF 間リーキングの設定は完了です。



第 25 章

L3Out の QoS

この章は、次の内容で構成されています。

- [L3Out QoS \(417 ページ\)](#)
- [L3Out QoS ガイドラインと制約事項 \(417 ページ\)](#)
- [GUI を使用して L3Out に QoS ディレクトリを設定する \(419 ページ\)](#)
- [GUI を使用した L3Outs の QoS コントラクトの設定 \(419 ページ\)](#)

L3Out QoS

L3Out QoS は、外部 EPG レベルで適用されるコントラクトを使用して設定できます。リリース 4.0(1) 以降、L3Out QoS は L3Out インターフェイスで直接設定することもできます。



- (注) Cisco APICリリース 4.0(1) 以降を実行している場合は、L3Out に直接適用されるカスタム QoS ポリシーを使用して L3Out の QoS を設定することを推奨します。

パケットは入力 DSCP または CoS 値を使用して分類されるため、カスタム QoS ポリシーを使用して着信トラフィックを Cisco ACIQoS キューに分類できます。カスタム QoS ポリシーには、DSCP/CoS 値をユーザキューまたは新しい DSCP/CoS 値 (マーキングの場合) にマッピングするテーブルが含まれます。特定の DSCP/CoS 値のマッピングがない場合、ユーザキューは入力 L3Out インターフェイスの QoS 優先度設定によって選択されます (設定されている場合)。

L3Out QoS ガイドラインと制約事項

L3Out の QoS 設定には次の注意事項が適用されます。

- カスタム QoS ポリシーは、Cisco Application Centric Infrastructure (ACI) ファブリックの外部から送信された (L3Out から受信した) レイヤ 3 マルチキャストトラフィックではサポートされません。

- L3Out が存在する境界リーフ スイッチに適用するコントラクトを使用して QoS ポリシーを設定するには、VRF テーブルが出力モードである必要があります (ポリシー制御適用の方向は「出力」にする必要があります)。

リリース 4.0(1) 以降、カスタム QoS 設定は L3Out で直接設定でき、境界リーフからのトラフィックに適用できます。そのため、VRF テーブルは出力モードである必要はありません。

- 適用する QoS ポリシーを有効にするには、VRF ポリシー制御適用設定を「適用」にする必要があります。
- L3Out とその他の EPG 間の通信を制御する契約を設定する際に、契約またはサブジェクトに QoS クラスまたはターゲット DSCP を含めます。



(注) 外部 EPG ではなく、契約の QoS クラスまたはターゲット DSCP のみ設定します (l3extInstP)。

- 契約のサブジェクトを作成する際は、QoS 優先度レベルを選択する必要があります。[Unspecified] を選択することはできません。



(注) カスタム QoS ポリシーは QoS クラスが [未指定 (Unspecified)] に設定されている場合でも DSCP/CoS 値を設定するため、カスタム QoS ポリシーは例外となります。QoS レベルが指定されていない場合、レベルはデフォルトで 3 として扱われます。未指定はサポートされず、無効です。

- リリース 4.0(1) 以降、QoS で、グローバル ポリシー、EPG、L3out、カスタム QoS、および契約で設定された新しいレベル 4、5、6 をサポートします。次の制限が適用されます。
 - 厳密な優先順位を設定できるクラスの数、5 つまで増加できます。
 - 非 EX および非 FX スイッチでは、3 つの新しいクラスはサポートされません。
 - 非 EX または非 FX スイッチと、EX または FX スイッチの間でトラフィックが流れる場合、トラフィックは QoS レベル 3 を使用します。
 - 新しいクラスで FEX と通信するため、トラフィックは値 0 のレイヤ 2 Cos を伝送します。
- リリース 4.0(1) 以降、QoS クラスを設定したり、L3Out インターフェイスに適用するカスタム QoS ポリシーを作成できるようになりました。

GUI を使用して L3Out に QoS ディレクトリを設定する

この章では L3Out で QoS ディレクトリを設定する方法について説明します。これは、リリース 4.0(1) 以降の L3Out QoS の推奨設定方法です。Cisco APIC

ステップ 1 メインメニューバーから [テナント (Tenants)] > [*<tenant-name>*] を選択します。

ステップ 2 左側の [ナビゲーション (Navigation)] ペインで、[テナント (Tenant) *<tenant-name>*] [ネットワーク (Networking)] [L3Outs] [*<routed-network-name>*] [論理ノードプロファイル (Logical Node Profiles)] [*<node-profile-name>*] [論理インターフェイスプロファイル (Logical Interface Profiles)] [*<interface-profile-name>*] を展開します。 >>> >> >>

存在しない場合は、新しいネットワーク、ノードプロファイル、およびインターフェイスプロファイルを作成する必要があります。

ステップ 3 メインウィンドウペインで、L3Out のカスタム QoS を設定します。

[QoS 優先順位 (QoS Priority)] ドロップダウンリストを使用して、標準 QoS レベルの優先順位を設定できます。または、[カスタム QoS ポリシー (Custom QoS Policy)] ドロップダウンから既存のカスタム QoS ポリシーを設定するか、新しいカスタム QoS ポリシーを作成できます。

GUI を使用した L3Outs の QoS コントラクトの設定

この項では、コントラクトを使用して L3Out の QoS を設定する方法について説明します。



(注) リリース 4.0(1) 以降では、L3Out QoS 用にカスタム QoS ポリシーを使用することを推奨しています。 [GUI を使用して L3Out に QoS ディレクトリを設定する \(419 ページ\)](#) で説明しています。

この項で説明するコントラクトを使用した QoS 分類の設定は、L3Out で直接設定された QoS ポリシーよりも優先されます。

ステップ 1 L3Out により使用される境界リーフスイッチに適用される QoS をサポートするために、L3Out を利用していたテナントの VRF インスタンスを設定します。

- メインメニューバーから [テナント (Tenants)] > [*<tenant-name>*] を選択します。
- Navigation** ウィンドウで、**Networking** を展開し、**VRFs** を右クリックし、**Create VRF** を選択します。
- VRF の名前を入力します。
- Policy Control Enforcement Preference** フィールドで、**Enforced** を選択します。
- [Policy Control Enforcement Dirction] で [Egress] を選択します

QoS 分類がコントラクトで実行される場合は、VRF の適用を強制を [出力 (Egress)] に設定する必要があります。

- f) L3Out の要件に従って VRF を設定します。

ステップ 2 L3Out を使用する EPG の間の通信を可能にするためにフィルタを設定するときには、QoS クラスまたはターゲット DSCP を含めて、L3Out を通して入力されるトラフィックにおける QoS の優先順位を適用します。

- a) [Navigation] ウィンドウの L3Out を使用するテナントで、**Contracts** を展開し、**Filters** を右クリックし、**Create Filter** を選択します。
- b) **Name** フィールドに、ファイルの名前を入力します。
- c) [Entries] フィールドで、[+] をクリックしてフィルタ エントリを追加します。
- d) エントリの詳細を追加し、**Update** をクリックし、**Submit** をクリックします。
- e) 以前に作成したフィルタを展開し、フィルタ エントリをクリックします。
- f) **Match DSCP** フィールドを、そのエントリに必要な DSCP レベルに設定します。たとえば **EF** にします。

ステップ 3 契約を追加します。

- a) **Contracts** の下で、**Standard** を右クリックして、**Create Contract** を選択します。
- b) 契約の名前を入力します。
- c) **QoS Class** フィールドで、この契約で管理されるトラフィックの QoS 優先順位を選択します。または、**Target DSCP** の値を選択することもできます。

この項で説明するコントラクトを使用した QoS 分類の設定は、L3Out で直接設定された QoS ポリシーよりも優先されます。

- d) [Subjects] の [+] アイコンをクリックして、情報カテゴリを契約に追加します。
- e) 情報カテゴリの名前を入力します。
- f) [QoS Priority] フィールドで、必要な優先度レベルを選択します。[Unspecified] を選択することはできません。
- g) [Filter Chain] の下で、[Filters] の [+] アイコンをクリックし、先ほど作成したフィルタをドロップダウンリストから選択します。
- h) **Update** をクリックします。
- i) **Create Contract Subject** ダイアログボックスで、**OK** をクリックします。



第 26 章

IP SLAs

この章は、次の内容で構成されています。

- [ACI IP SLA について \(421 ページ\)](#)
- [IP SLA のガイドラインと制約事項 \(431 ページ\)](#)
- [スタティック ルートの ACI IP SLA の設定および関連付け \(432 ページ\)](#)
- [ACI IP SLA モニタリング情報の確認 \(438 ページ\)](#)

ACI IP SLA について

多くの企業ではビジネスのほとんどをオンラインで行い、サービスの損失は企業の収益性に影響を及ぼすことがあります。今では、インターネット サービス プロバイダ (ISP) や内部 IT 部門でさえも、定義済みのサービス レベル、サービス レベル契約 (SLA) を提供して、お客様に一定の予測可能性を提供しています。

IPSLA トラッキングは、ネットワークの一般的な要件です。IPSLA トラッキングにより、ネットワーク管理者はネットワークパフォーマンスに関する情報をリアルタイムで収集できます。Cisco ACI IP SLA では、ICMP および TCP プロブを使用して IP アドレスを追跡できます。トラッキング設定はルートテーブルに影響を与える可能性があり、トラッキング結果がネガティブになったときにルートを削除し、結果が再びポジティブになったときにルートをテーブルに戻すことができます。

ACI IP SLA は、次のものに使用できます。

- スタティック ルート :
 - ACI 4.1 の新機能
 - ルートテーブルからのスタティック ルートの自動削除または追加
 - ICMP および TCP プロブを使用してルートを追跡する
- ポリシーベース リダイレクト (PBR) トラッキング :
 - ACI 3.1 以降で使用可能
 - ネクスト ホップの自動削除または追加

- ICMP プローブと TCP プローブ、または L2Ping を使用した組み合わせを使用して、ネクストホップ IP アドレスを追跡します。
- ネクストホップの到達可能性に基づいて PBR ノードにトラフィックをリダイレクトする

PBR トラッキングの詳細については、『*Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*』の「ポリシーベース リダイレクトの設定」を参照してください。



(注) いずれの機能でも、設定、APIの使用、スクリプトの実行など、プローブの結果に基づいてネットワーク アクションを実行できます。

ACI IP SLA でサポートされるトポロジ

次の ACI ファブリック トポロジは IP SLA をサポートします。

- シングルファブリック : IP SLA トラッキングは、L3out と EPG/BD の両方を介して到達可能な IP アドレスでサポートされます。
- マルチポッド
 - 異なるポッドで単一のオブジェクト トラッキング ポリシーを定義できます。
 - ワークロードは、あるポッドから別のポッドに移動できます。IPSLA ポリシーは引き続きアクセス可能性情報をチェックし、エンドポイントが移動したかどうかを検出します。
 - エンドポイントが別のポッドに移動すると、IPSLA トラッキングも他のポッドに移動されるため、トラッキング情報は IP ネットワークを通過しません。
- リモート リーフ
 - ACI メイン データ センターおよびリモート リーフ スイッチ全体で単一オブジェクト トラッキング ポリシーを定義できます。
 - リモート リーフ スイッチの IP SLA プローブは、IP ネットワークを使用せずに IP アドレスをローカルに追跡します。
 - ワークロードは、1つのローカルリーフからリモートリーフに移動できます。IPSLA ポリシーは引き続きアクセス可能性情報をチェックし、エンドポイントが移動したかどうかを検出します。
 - IP SLA ポリシーは、エンドポイントの場所に基づいてリモート リーフ スイッチまたは ACI メイン データ センターに移動し、ローカル トラッキングを行うため、トラッキング トラフィックは IP ネットワークを通過しません。

Cisco ACI IP SLA のオペレーション

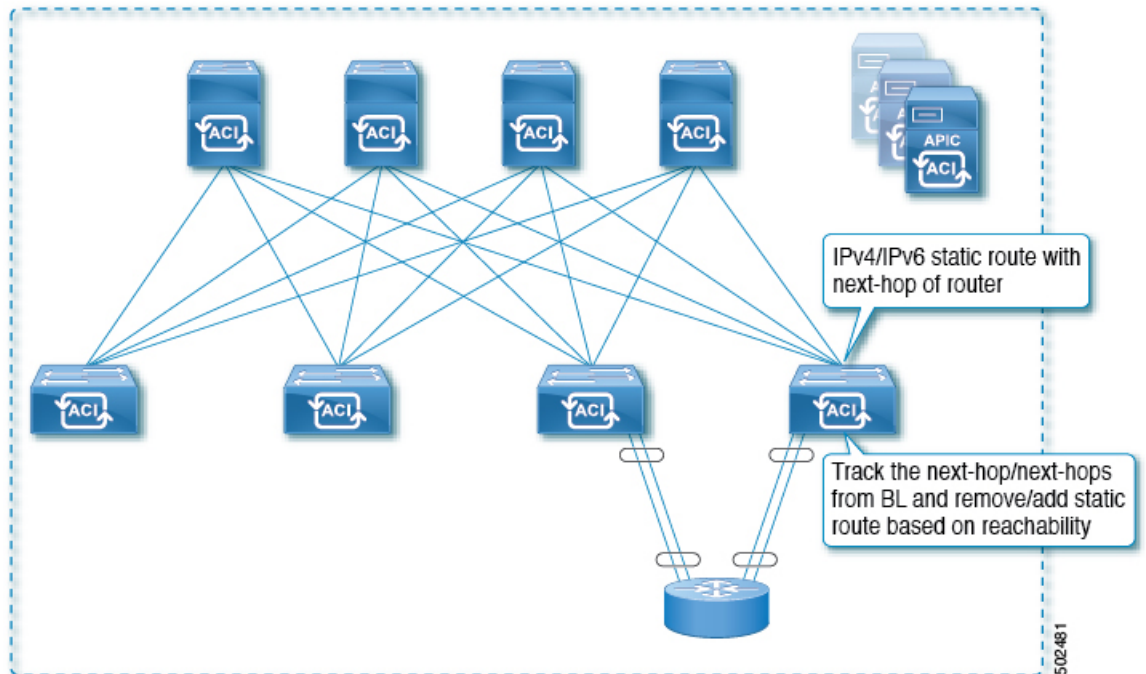
Cisco ACI IP SLA は、ACI ファブリック上でモニタリング機能を提供し、SLA プロブをデータセンター ネットワーク全体および外部ネットワークで実行できるようにします。これは、モニタリング中に使用されるプロブ タイプを定義する IP SLA モニタリング ポリシーを設定することによって実現されます。モニタリング ポリシーは、「トラック メンバー」と呼ばれるモニタリングプロブプロファイルに関連付けられます。設定が完了すると、IP アドレス、関連付けられたモニタリング ポリシー、およびスコープ (ブリッジドメインまたは L3Out) によって、エンドポイントまたはネクストホップを定義します。1つ以上のトラックメンバーを「トラックリスト」に割り当てることができます。トラックリストは、しきい値を設定します。これを超えると、トラックリストが使用可能 (アップ) か使用不可 (ダウン) かが決まります。

次の4つの例は、スタティックルートでサポートされる ACI IP SLA の使用例を示しています。

例 1 : ネクストホップのトラッキングによるスタティック ルートの可用性

次の図は、ネットワーク トポロジと、ルータのスタティック ルートの可用性を追跡する動作を示しています。

図 49: ネクストホップのトラッキングによるスタティック ルートの可用性



この使用ケースでは :

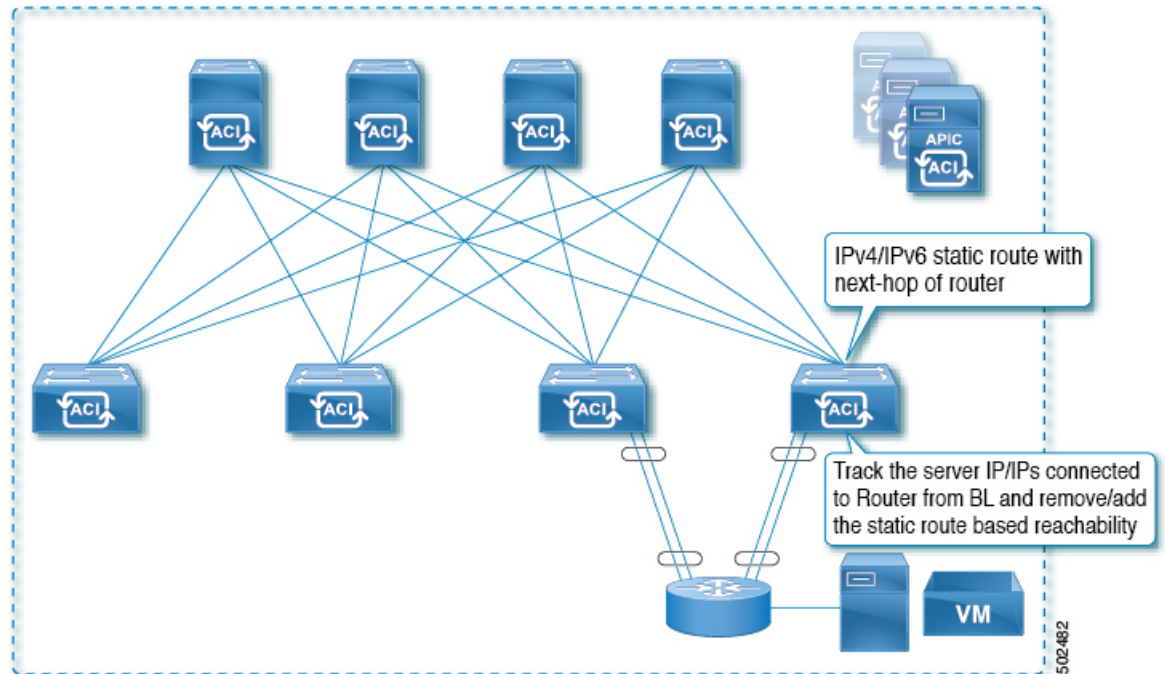
- ネクストホップは直接または間接のいずれかになります。つまり、ネクストホップはルータのループバック IP アドレスになります。
- ネクストホップには、物理インターフェイス、サブインターフェイス、ポートチャネル (PC)、PC サブインターフェイス、vPC、またはスイッチ仮想インターフェイス (SVI) を介してアクセスできます。

- スタティックルートはL3out外部ネットワークの下で設定され、ネクストホップのアクセス可能性に基づいてルートテーブルから削除または追加できます。

例 2 : L3Out を介した IP アドレスのトラッキングによるスタティック ルートの可用性

次の図は、L3Out 外部ルートを通じてサーバのスタティックルートの可用性を追跡するためのネットワーク トポロジと動作を示しています。

図 50 : L3Out を介した IP アドレスの追跡によるスタティック ルートの可用性



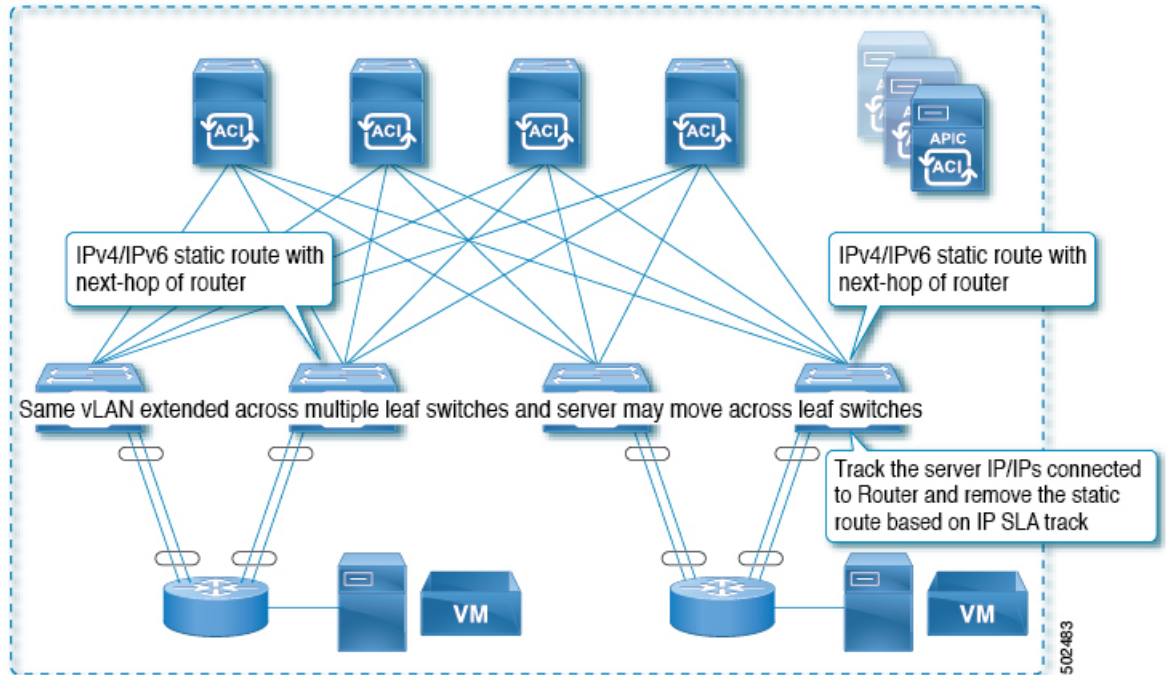
この使用ケースでは :

- ACI ファブリック（境界リーフ）からルータに接続されているサーバの IP アドレスを追跡し、サーバのアクセス可能性に基づいてスタティックルートを削除または追加します。
- L3Out は、ポート チャネル（PC）、PC サブインターフェイス、vPC、スイッチ仮想インターフェイス（SVI）、L3 インターフェイス、または L3 サブインターフェイスを経由できます。
- スタティック ルートは L3Out で設定され、IP アドレスのアクセス可能性に基づいて削除または追加されます。

例 3 : L3Out を介した IP アドレスのトラッキングによるスタティック ルートの削除

次の図は、L3Out 外部ルートを通じてサーバのスタティックルートの可用性を追跡するためのネットワーク トポロジと動作を示しています。L3Out/VRFからアクセスできない場合、ルートは削除されます。

図 51: L3Out を介した IP アドレスのトラッキングによるスタティック ルートの削除



この使用ケースでは：

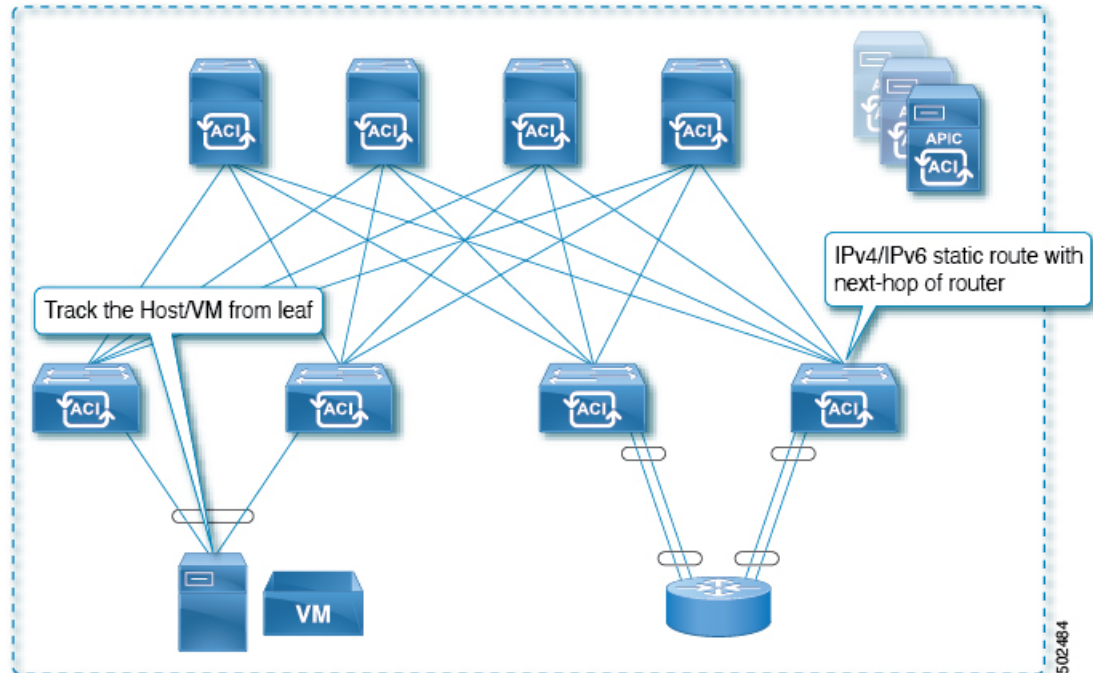
- L3Out は VLAN/SVI を介して設定され、その SVI は複数のリーフに拡張されます。
- L3Out を介してアクセス可能なサーバの IP アドレスは、リーフ間を移動できます。
- サーバの IP アドレスを追跡し、L3Out/VRF からアクセスできない場合は、ルート テーブルからスタティック ルートを削除します。
- サーバが再びアクセス可能になると、スタティック ルートがルート テーブルに戻されます。

例 4 : ACI ファブリックの IP アドレスのトラッキングによるスタティック ルートの削除

前の例で示したように、ルートの IP SLA のプローブ IP は通常、ルートのネクストホップまたはルート経由で到達可能な外部 IP アドレスですが、エンドポイントが IP SLA の対象となるルートの背後に存在しない場合でも、プローブ IP として ACI BD でエンドポイント IP アドレスを使用することもできます。これは、ACI 内の特定のエンドポイントだけがスタティック ルートを使用する場合に役立ちます。このようなエンドポイントが存在しない場合、ルートは使用されません。

次の図は、ネットワーク トポロジと、ACI ファブリックの IP アドレスを追跡する動作を示しています。

図 52: ACI ファブリックでの IP アドレスの追跡によるスタティック ルートの可用性



この使用ケースでは：

- EPG/BD 経路で接続されているエンドポイントの IP 到達可能性を追跡します。
- エンドポイントのアクセス可能性に基づいて、スタティック ルートが L3Out で削除または追加されます。
- エンドポイントがファブリック内のある場所から別の場所に移動しても、同じ BD からエンドポイントへの IP 到達可能性がある限り、IP SLA モニタリングはそれをアクセス可能と見なし、スタティック ルートの有効性に影響を与えません。

IP SLA モニタリングポリシー

IP Service Level Agreements (SLA) は、継続的で信頼性のある予測可能な方法でトラフィックを生成する、アクティブトラフィック モニタリングを使用し、ネットワークのパフォーマンスを測定するために分析を行います。IP SLA モニタリング ポリシー動作による測定統計情報を、トラブルシューティング、問題分析、ネットワーク トポロジの設計に使用できます。

Cisco ACI では、IP SLA モニタリング ポリシーは次のものに関連付けられます。

- サービスリダイレクトポリシー：サービスリダイレクトポリシー下のすべての宛先は、モニタリングポリシーで設定された設定とパラメータに基づいてモニタされます。
- スタティックルート：IP SLA モニタリングポリシーをトラックリストまたはトラックメンバーに追加し、スタティックルートに関連付けることで、ルートのネクストホップセグメントの可用性をモニタリングできます。

IP SLA モニタリング ポリシーは、プローブの頻度とタイプを識別します。

ACI IP SLA モニタリング動作プローブ タイプ

ACI IP SLA を使用して、コア、分散、エッジといったネットワークの任意の領域間のパフォーマンスをモニタできます。モニタリングは、物理的なプローブを展開しなくても、時間と場所を問わず実行できます。ACI IP SLA は、生成されたトラフィックを使用して、スイッチなどの 2 つのネットワーク デバイス間のネットワーク パフォーマンスを測定します。IP SLA 動作のタイプは次のとおりです。

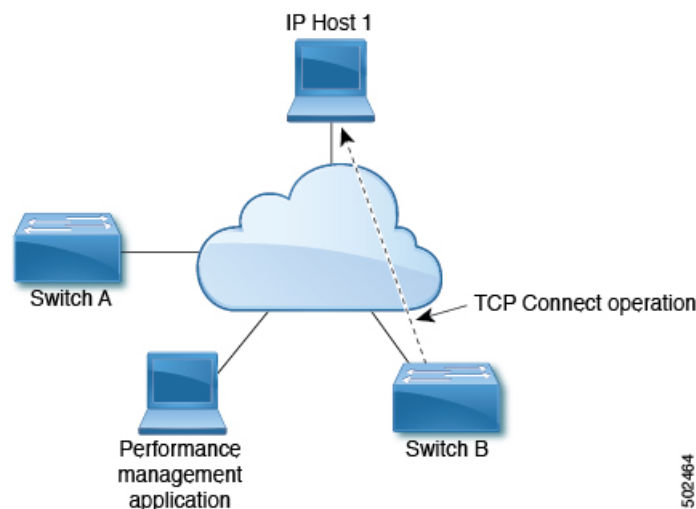
- ICMP : エコー プローブ
- TCP : プローブの接続

TCP 接続動作

IP SLA TCP 接続動作は、シスコ スイッチと IP デバイス間の TCP プローブの実行に要する応答時間を測定します。TCP は、信頼性の高い全二重データ伝送を行うトランスポート層 (レイヤ 4) インターネットプロトコルです。宛先デバイスは、IP を使用する任意のデバイスになります。

次の図では、設定されたスタティックルートに基づいて、スイッチ B が送信元 IP SLA デバイスとして設定されています。TCP 接続動作は、IP SLA モニタリング ポリシー (スタティックルートに関連付けられている) で、宛先デバイスを IP ホスト 1 として設定されます。

図 53: TCP 接続の動作例



接続応答時間は、スイッチ B から IP ホスト 1 に TCP 要求メッセージを送信してから、IP ホスト 1 からの応答を受信するまでの時間を測定して算出されます。

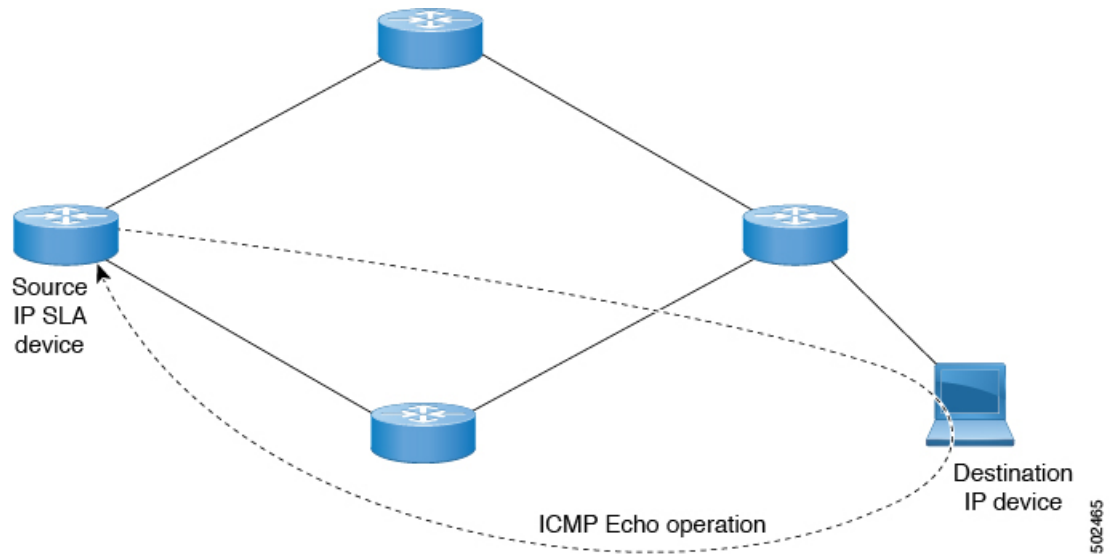
ICMP エコー動作

Internet Control Message Protocol (ICMP) エコー動作は、IPv4 または IPv6 を使用する 2 台のデバイス間のエンドツーエンド応答時間を測定します。応答時間は、ICMP エコー要求メッセー

ジを宛先に送信して応答を受信するまでの時間を測定して算出します。ICMP エコーは、ネットワーク接続問題のトラブルシューティングに役立ちます。ICMP エコー動作の結果を表示および分析することで、ネットワーク IP 接続の実況状況を判断できます。

次の図では、ICMP エコー動作は ping ベースのプロブを使用して送信元 IP SLA デバイスと宛先 IP デバイスの間の応答時間を測定します。多くのお客様が、応答時間の測定に IP SLA ICMP ベース動作、社内 ping テスト、または ping ベース専用プロブを使用しています。

図 54: ICMP エコー動作の例



IP SLA ICMP エコー動作と ICMP ping テストは同じ IETF 仕様に準拠しているため、どちらの方法でも同じ応答時間が得られます。

IP SLA トラック メンバー

IP SLA トラック メンバーは、以下を識別します。

- 追跡対象の IP アドレス
- IP SLA モニタリング ポリシー (プロブの頻度とタイプ)
- スコープ (ブリッジ ドメインまたは L3Out)

IP SLA トラック リスト

IP SLA トラック リストは、モニタ対象のネットワーク セグメントを表す 1 つ以上の IP SLA トラック メンバーを集約します。トラック リストは、スタティック ルートを使用可能または使用不可と見なすために必要なトラック メンバーのパーセンテージまたは重みを決定します。しきい値のパーセンテージまたは重みに基づいてトラック リストが稼働している場合、スタティック ルートはルーティング テーブルに残ります。トラック リストがダウンしている場合、

スタティック ルートは、トラック リストが回復するまでルーティング テーブルから削除されます。

次に、しきい値パーセンテージ オプションを使用して、トラック リストに 4 つのトラック メンバーを設定する例を示します。

しきい値の設定：

- 「Percentage Up」パラメータを 100（パーセント）に設定します。
- 「Percentage Down」パラメータを 50（パーセント）に設定します。

このトラック リストでは、4 つのトラック メンバーのそれぞれに 25% が割り当てられます。トラック リストが到達不能（ダウン）になるには、4 つのトラック メンバーのうち 2 つが到達不能（50%）である必要があります。トラック リストが到達可能（アップ）に戻るには、4 つのトラック メンバーすべてが到達可能（100%）である必要があります。



-
- (注) トラッキング リストがスタティック ルートに関連付けられ、トラッキング リストが到達不能（ダウン）になると、トラッキング リストが再び到達可能になるまで、スタティック ルートはルーティング テーブルから削除されます。
-

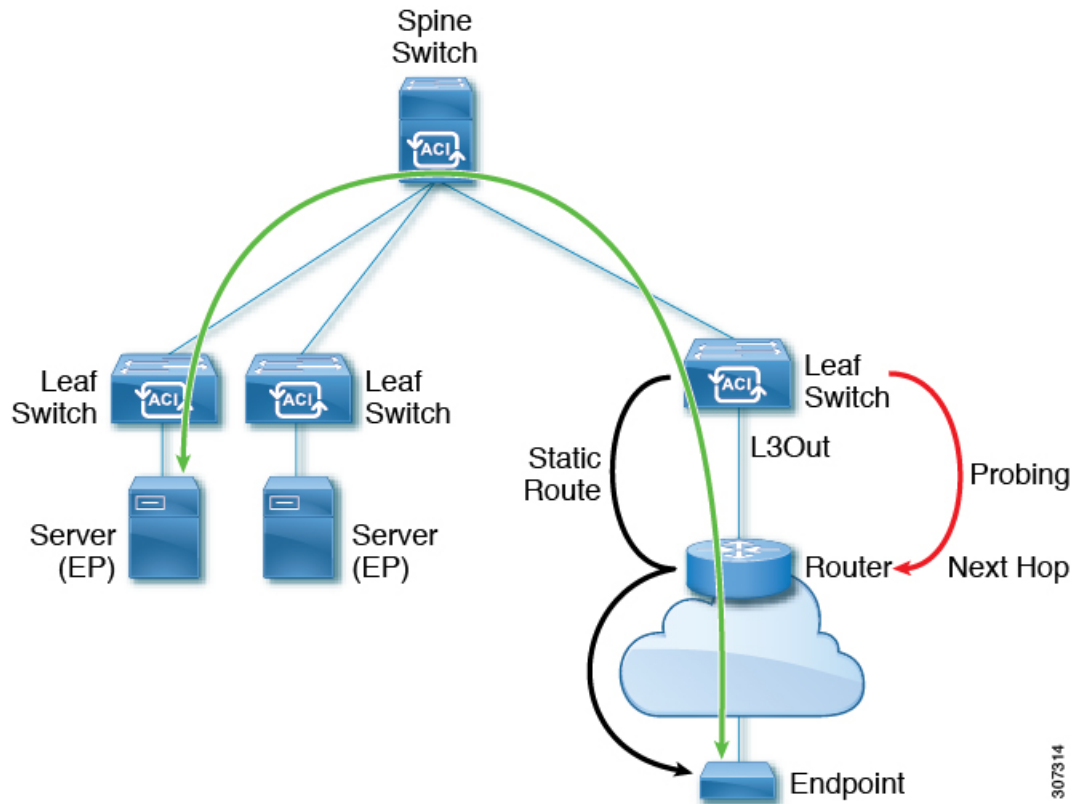
IP SLA 設定コンポーネントの関連付けの例

ACI IP SLA は、トラック メンバーとトラック リストに基づいて、送信するプローブのタイプと送信先を特定します。設定を計画すると、タスクを簡単かつ迅速に行うことができます。このセクションでは、IP SLA の設定方法を説明する例を使用します。

Cisco ACI IP SLA L3Out Example

次の図は、ACI ファブリック内で外部エンドポイントを含む特定の設定済みスタティック ルートのモニタリング/プローブを提供する Cisco ACI IP SLA を示しています。

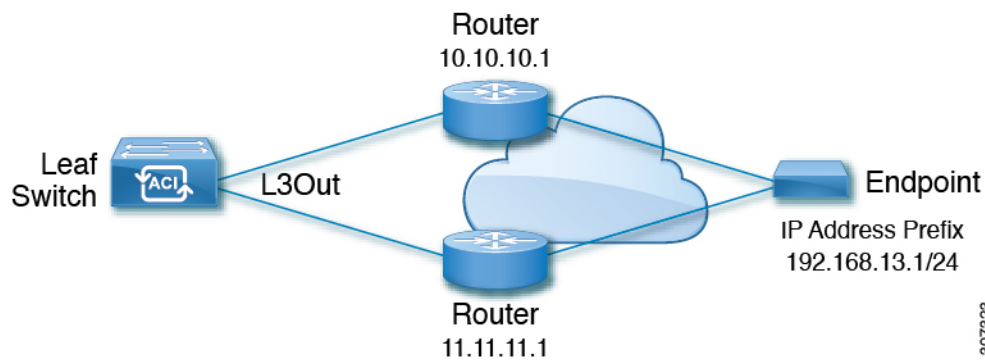
図 55: 例 : ACI L3Out IP SLA



307314

次の図は、エンドポイントプレフィックス 192.168.13.1/24 のスタティック ルートを示しています。また、L3Out リーフ スイッチとコンシューマ エンドポイント間のスタティック ルートにあるルータのペアも示します。

図 56: スタティックルートの例



307323

上の図に基づいて ACI IP SLA を設定するには、ルータをモニタして、コンシューマ エンドポイントへの接続を確認する必要があります。これを行うには、スタティックルート、トラックメンバ、およびトラック リストを作成します。

- ネクスト ホップ 10.10.10.1 および 11.11.11.1 の 192.168.13.1/24 のスタティック ルート

- トラックメンバー1 (TM-1) には、ルータの IP アドレス 10.10.10.1 が含まれています (これはネクストホッププローブです)。
- トラックメンバー2 (TM-2) には、ルータの IP アドレス 11.11.11.1 が含まれています (これはネクストホッププローブです)。
- TM-1 および TM-2 を含むトラックリスト1 (TL-1) (スタティックルートに関連付けられたトラックリスト)。トラックリストには、設定されたプレフィックスエンドポイントに到達できるネクストホップのリストが含まれます。トラックリストが到達可能か到達不能かを決定するしきい値も設定されます)。
- TM-1 を含むトラックリスト2 (TL-2) (スタティックルートに含まれるネクストホップエントリに関連付けられる)
- TM-2 を含むトラックリスト3 (TL-3) (スタティックルートに含まれるネクストホップエントリに関連付けられる)

汎用スタティックルートの場合、TL-1 をスタティックルートに関連付け、TL-2 を 10.10.10.1 ネクストホップに関連付け、TL-3 を 11.11.11.1 ネクストホップに関連付けることができます。特定のスタティックルートのペア (両方とも 192.168.13.1/24) では、一方の TL-2 と他方の TL-3 を関連付けることができます。また、ルータのネクストホップに TL-2 と TL-3 が関連付けられている必要があります。

これらのオプションを使用すると、1台のルータで障害が発生しても、障害発生時にバックアップルートを提供できます。トラックメンバーとトラックリストの詳細については、次のセクションを参照してください。

IP SLA のガイドラインと制約事項

IP サービス レベル合意事項を計画および設定する場合は、次のガイドラインと制限事項を考慮してください。

- IP SLA は、IPv4 アドレスと IPv6 アドレスの両方をサポートします。
- IP SLA は、-EX および -FX シャーシを含むすべての Cisco Nexus 第 2 世代スイッチでサポートされます。
- Cisco Application Policy Infrastructure Controller (APIC) リリース 4.1(1) 以降、IP SLA モニタポリシーは IP SLA ポート値を検証します。検証のため、TCP が IP SLA タイプとして設定されている場合、Cisco APIC は以前のリリースで許可されていた IP SLA ポート値 0 を受け入れなくなります。IP SLA ポート値が 0 である以前のリリースの IP SLA モニタポリシーは、Cisco APIC がリリース 4.1(1) 以降にアップグレードされると無効になります。これにより、設定のインポートまたはスナップショットのロールバックが失敗します。

回避策は、Cisco APIC をアップグレードする前にゼロ以外の IP SLA ポート値を設定し、IP SLA ポートの変更後に取得されたスナップショットと設定のエクスポートを使用することです。

- IP SLA でリモート リーフ スイッチをサポートする場合は、グローバル GIPo を有効にする必要があります。
 1. メニュー バーで、[システム (System)] > [システム設定 (System Settings)] を選択します。
 2. [システム設定 (System Settings)] ナビゲーション ウィンドウで [システム グローバル GIPo (System Global GIPo)] をクリックします。
 3. [システム グローバル GIPo ポリシー (System Global GIPo Policy)] 作業ウィンドウで [有効化 (Enabled)] をクリックします。
 4. [ポリシー使用警告 (Policy Usage Warning)] ダイアログで、GIPo ポリシーを使用する可能性があるノードとポリシーを確認し、必要に応じて [変更の送信 (Submit Changes)] をクリックします。
- [ファブリック (Fabric)]、[インベントリ (Inventory)]、[ポッド番号 (Pod number)]、[リーフ ノード名 (LeafNode name)]、[プロトコル (Protocols)]、[IP SLA]、[ICMP エコー操作 (ICMP Echo Operations)]、または [TCP 接続操作 (TCP Connect Operations)] で表示される統計情報は、5 分間隔でのみ収集できます。間隔のデフォルトは [15 分] ですが、[5 分] に設定する必要があります。
- IP SLA ポリシーは、vPod 経由で接続されたエンドポイントではサポートされません。
- IP SLA は、シングルポッド、およびリモートリーフ スイッチでサポートされます。Cisco ACI マルチポッド
- 追跡対象の宛先 IP アドレスが接続されている場合、IP SLA はサポートされません。Cisco ACI マルチサイト

検証済み IP SLA 番号の詳細については、Cisco APIC のドキュメント ページで該当する『Cisco APIC の検証済みスケーラビリティ ガイド』を参照してください。 <https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>

スタティック ルートの ACI IP SLA の設定および関連付け

ここでは、次の IP SLA ポリシーおよびプロファイルを設定および関連付けるために必要なタスクについて説明します。

- IP SLA モニターリング ポリシー
- IP SLA トラック メンバー
- IP SLA トラック リスト

前のコンポーネントは、スタティック ルートまたはネクスト ホップ プロファイルに適用されます。

GUI を使用した IP SLA モニタリング ポリシーの設定

GUI を使用して () が特定の SLA タイプのモニタリング プローブを送信できるようにするには、次の手順を実行します。Cisco Application Policy Infrastructure Controller APIC Cisco APIC

ステップ 1 メニューバーで [テナント (Tenant)] > [tenant_name] をクリックします。[ナビゲーション (Navigation)] ペインで、[ポリシー (Policies)] > [プロトコル (Protocol)] > [IP SLA] をクリックします。

ステップ 2 IP SLA Monitoring Policies を右クリックして、**Create IP SLA Monitoring Policy** をクリックします。

ステップ 3 Create IP SLA Monitoring Policy ダイアログボックスで、次の操作を実行します:

- a) [名前 (Name)] フィールドに、IP SLA モニタリング ポリシーの一意の名前を入力します。
- b) **SLA Type** フィールドで、SLA タイプを選択します。

SLA タイプは、[TCP]、[ICMP]、[L2Ping]、または [HTTP] です。[ICMP] がデフォルト値です。

(注) [L2Ping] は、レイヤ 1/レイヤ 2 ポリシーベース リダイレクト (PBR) トラッキングでのみサポートされます。

- c) SLA タイプに [HTTP] を選択した場合は、[HTTP バージョン (HTTP Version)] ボタンにバージョンを選択します。
- d) SLA タイプに [HTTP] を選択した場合は、[HTTP URI] フィールドに、サービス ノード トラッキングに使用する HTTP URI を入力します。

URI は「/index.html」のように「/」で始まる必要があります。

- e) SLA タイプに [TCP] を選択した場合は、[宛先 ポート (Destination Port)] フィールドにポート番号を入力します。
- f) [SLA 頻度 (SLA Frequency)] フィールドに、パケットを追跡するために設定された頻度を決定する値を秒単位で入力します。

範囲は、1 ~ 300 です。デフォルト値は 60 です。HTTP トラッキングの最小頻度は 5 秒です。

- g) [検出乗数 (Detect Multiplier)] フィールドに、失敗が検出されたか、またはトラックがダウンしていることを示す、失敗したプローブの数を行に入力します。

デフォルトでは、3 つのプローブが連続して検出されなかった場合に障害が検出されます。[検出乗数 (Detect Multiplier)] フィールドの値を変更すると、行で検出されなかったプローブの数が変更されます。これにより、障害が検出されたタイミング、またはトラックがダウンしていると思われるタイミングが決まります。

[SLA 頻度 (SLA Frequency)] のエントリと組み合わせて使用すると、障害が検出されるタイミングを決定できます。たとえば、これらのフィールドに次のエントリを入力したとします。

- SLA 頻度 (秒) (SLA Frequency (sec)) : 5
- 検出乗数 (Detect Multiplier) : 30

この例のシナリオでは、約 150 秒で障害が検出されます (5 秒 x 30)。

- h) [TCP] 以外の SLA タイプを選択した場合は、[データ サイズ (バイト) の要求 (Request Data Size (bytes))] フィールドに、IP SLA 動作の要求パケットのペイロードに含まれるプロトコル データのサイズをバイト単位で入力します。
 - i) [サービスのタイプ (Type of Service)] フィールドに、IP SLA 動作の IPv4 ヘッダーのタイプ オブ サービス (ToS) を入力します。
 - j) [処理タイムアウト (ミリ秒) (Operarion Timeout (milliseconds))] フィールドに、要求パケットの応答に対する IP SLA 処理の待機時間をミリ秒単位で指定します。
 - k) **Threshold (milliseconds)** フィールドに、IP SLA 動作によって作成されるネットワーク モニタリング統計情報を計算するための上限しきい値を入力します。
 - l) [トラフィック クラス値 (Traffic Class Value)] フィールドに、IPv6 ネットワークの IP SLA 動作の IPv6 ヘッダーのトラフィック クラス バイトを入力します。
 - m) [送信 (Submit)] をクリックします。
- IP SLA モニタリング ポリシーが設定されます。

GUI を使用した IP SLA ट्रック メンバーの設定

このタスクを使用して、IP SLA ट्रック リストに追加された番号の 1 つである IP SLA ट्रック メンバーを作成します。トラッキング リストはスタティック ルートに適用され、定義されたネクスト ホップ間のパフォーマンスをモニタします。

始める前に

IP SLA モニタリング ポリシーを作成し、スタティック ルートでこのトラック メンバーが表すネクスト ホップの宛先 IP アドレスを知っている必要があります。

APIC GUI を使用して IP SLA ट्रック メンバーを設定するには、次の手順を実行します。

- ステップ 1** メニュー バーで、[テナント (Tenants)] > [tenant-name] をクリックします。
- ステップ 2** [ナビゲーション (Navigation)] ペインで、[ポリシー (Policies)] を展開した後で、[プロトコル (Protocol)] を展開します。
- ステップ 3** [IP SLA] を展開し、[トラック メンバー (Track Members)] を右クリックして [トラック メンバーの作成 (Create Track Member)] を選択します。
- ステップ 4** 次のパラメータを設定します。
 - a) [名前 (Name)] フィールドに、トラック メンバーの一意の名前を入力します。
 - b) [宛先 IP (Destination IP)] フィールドに、この設定が表すネクスト ホップの IP アドレスを入力します。
 - c) [トラックメンバーの範囲 (Scope of Track Member)] ドロップダウン リストで、このトラック メンバーが属する既存のブリッジ ドメインまたは外部ネットワークを選択します。
 - d) [IP SLA ポリシー (IP SLA Policy)] フィールドで、既存のを選択するか、モニタリング中に使用されるプローブを定義する新しい IP SLA モニタリング ポリシーを作成します。

ステップ 5 [送信 (Submit)] をクリックします。`

次のタスク

上記の手順を繰り返して、モニタするスタティック ルートに必要な数のトラック メンバーを作成します。すべてのトラック メンバーを設定したら、トラック リストを作成して追加します。

GUI を使用した IP SLA トラック リストの設定

このタスクを使用して、スタティック ルートのネクスト ホップを表すトラック メンバーのグループを定義する IP SLA トラック リストを作成します。トラッキング リストはスタティック ルートに適用され、定義されたネクスト ホップ間のパフォーマンスをモニタします。

始める前に

1 つ以上の IP SLA トラック メンバーを作成しておく必要があります。

APIC GUI を使用して IP SLA トラック リストを設定するには、次の手順を実行します。

ステップ 1 メニュー バーで、[テナント (Tenants)] > [tenant-name] をクリックします。

ステップ 2 [ナビゲーション (Navigation)] ペインで、[ポリシー (Policies)] を展開した後で、[プロトコル (Protocol)] を展開します。

ステップ 3 [IP SLA] を展開し、[トラック リスト (Track Lists)] を右クリックして [トラック リストの作成 (Create Track List)] を選択します。

[テナントの作成 (Create Tenant)] ダイアログ ボックスが表示されます。

ステップ 4 次のパラメータを設定します。

- [名前 (Name)] フィールドに、トラック リストの一意の名前を入力します。
- ルートの可用性をアップまたはダウンしているトラック メンバーのパーセンテージに基づいて設定する場合は、[トラック リストのタイプ (Type of Track List)] フィールドで、[しきい値パーセンテージ (Threshold percentage)] を選択します。ルートの可用性が各トラック メンバーに割り当てられた重み値に基づいている場合は、[しきい値の重み (Threshold weight)] を選択します。
- メンバー リストを追跡する [トラック メンバー関係のトラック リスト (Track list to track member relation)] テーブルで、テーブル ヘッドの [+] アイコンをクリックして、トラック メンバーをリストに追加します。既存のトラック メンバーを選択し、[トラック リストのタイプ (Type of Track List)] が [しきい値の重み (Threshold weight)] の場合は、重み値を割り当てます。

ステップ 5 [送信 (Submit)] をクリックします。`

次のタスク

スタティック ルートまたはネクスト ホップ IP アドレスにトラック リストを関連付けます。

GUI を使用したスタティック ルートとトラック リストの関連付け

このタスクを使用して、トラック リストを設定済みのスタティック ルートに関連付け、システムが一連のネクスト ホップのパフォーマンスをモニタできるようにします。



(注) 次のタスクは、スタティック ルートのネクスト ホップ設定がすでに存在することを前提としています。

始める前に

スタティック ルートが設定されたルーテッドネットワークが使用可能である必要があります。設定済みのトラック リストも使用できる必要があります。

APIC GUI を使用して IP SLA トラック リストをスタティック ルートに関連付けるには、次の手順を実行します。

- ステップ 1 メニュー バーで、[テナント (Tenants)] > [tenant-name] をクリックします。
- ステップ 2 [ナビゲーション (Navigation)] ペインで、[ネットワークング (Networking)]、[L3Outs] の順に展開します。
- ステップ 3 設定済みのルーテッド ネットワーク (名前)、[論理ノードプロファイル (Logical Node Profiles)]、設定済みの論理ノードプロファイル (名前)、および [設定済みノード (Configured Nodes)] を展開します。
- ステップ 4 設定済みのノード (名前) をクリックします。
[ノード関連付け (Node Association)] 作業ペインが表示されます。
- ステップ 5 [スタティック ルート (Static Routes)] テーブルで、トラック リストを追加するルート エントリをダブルクリックします。
[スタティック ルート (Static Route)] ダイアログ ボックスが表示されます。
- ステップ 6 [トラック ポリシー (Track Policy)] ドロップダウン リストで、このスタティック ルートに関連付ける IP SLA トラック リストを選択または作成します。
- ステップ 7 [送信 (Submit)] をクリックします。
- ステップ 8 [ポリシー使用の警告 (Policy Usage Warning)] ダイアログが表示されます。
- ステップ 9 この変更がこのスタティック ルートを使用する他のノードまたはポリシーに影響を与えないことを確認し、[変更の送信 (Submit Changes)] をクリックします。

GUI を使用した、トラック リストとネクストホップ プロファイルの関連付け

このタスクを使用して、トラック リストを設定済みのスタティック ルートのネクストホップ プロファイルに関連付けると、システムがネクストホップのパフォーマンスをモニタできるようにします。

始める前に

スタティック ルートとネクストホップ プロファイルが設定されたルーテッド ネットワークが使用可能である必要があります。

APIC GUI を使用して IP SLA トラック リストをネクストホップ プロファイルに関連付けるには、次の手順を実行します。

-
- ステップ 1 メニュー バーで、[テナント (Tenants)] > [tenant-name] をクリックします。
 - ステップ 2 [ナビゲーション (Navigation)] ペインで、[ネットワークング (Networking)]、[L3Outs] の順に展開します。
 - ステップ 3 設定済みのルーテッド ネットワーク (名前)、[論理ノード プロファイル (Logical Node Profiles)]、設定済みの論理ノード プロファイル (名前)、および [設定済みノード (Configured Nodes)] を展開します。
 - ステップ 4 設定済みのノード (名前) をクリックします。
[ノード関連付け (Node Association)] 作業ペインが表示されます。
 - ステップ 5 [スタティック ルート (Static Routes)] テーブルで、トラック リストを追加するルート エントリをダブルクリックします。
[スタティック ルート (Static Route)] ダイアログ ボックスが表示されます。
 - ステップ 6 [ネクストホップ アドレス (Next Hop Addresses)] テーブルで、トラック リストを追加するネクストホップ エントリをダブルクリックします。
[ネクストホップ プロファイル (Next Hop Profile)] ダイアログが表示されます。
 - ステップ 7 [トラック ポリシー (Track Policy)] ドロップダウン リストで、このスタティック ルートに関連付ける IP SLA トラック リストを選択または作成します。
(注) IP SLA ポリシーをネクストホップ プロファイルに追加すると、トラック メンバーとトラック リストが自動的に作成され、プロファイルに関連付けられます。
 - ステップ 8 [送信 (Submit)] をクリックします。
 - ステップ 9 [ポリシー使用の警告 (Policy Usage Warning)] ダイアログが表示されます。
 - ステップ 10 この変更がこのスタティック ルートを使用する他のノードまたはポリシーに影響を与えないことを確認し、[変更の送信 (Submit Changes)] をクリックします。
-

ACI IP SLA モニタリング情報の確認

ここでは、IP SLA 統計情報、トラックリスト、トラックメンバー、および関連するスタティック ルートを表示するために必要なタスクについて説明します。

- GUI を使用した ACI IP SLA プローブ統計情報の表示
- CLI を使用したトラック リストおよびトラック メンバー ステータスの表示

GUI を使用した IP SLA プローブ統計情報の確認

ACI IP SLA は、次のリアルタイム統計情報を生成します。

ICMP

- ICMP エコー ラウンドトリップ時間 (ミリ秒)
- 失敗した ICMP エコー プローブ (パケット) の数
- 成功した ICMP エコー プローブ (パケット) の数
- 伝送した ICMP エコー プローブ (パケット) の数

[TCP]

- 失敗した TCP 接続プローブ (パケット) の数
- 成功した TCP 接続プローブ (パケット) の数
- 伝送した TCP 接続プローブ (パケット) の数
- TCP 接続ラウンドトリップ時間 (ミリ秒)

このタスクを使用して、現在スタティック ルートまたはネクスト ホップをモニタしている IP SLA トラック リストまたはメンバーの統計情報を表示します。

始める前に

統計情報を表示する前に、IP SLA トラック リストを作成し、スタティック ルートに関連付ける必要があります。

-
- ステップ 1** メニュー バーで、[テナント (Tenants)] > [tenant-name] をクリックします。
 - ステップ 2** [ナビゲーション (Navigation)] セクションで、[ポリシー (Policies)] を展開した後で、[プロトコル (Protocol)] を展開します。
 - ステップ 3** [IP SLA] を展開し、[トラック メンバー (Track Members)] または [トラック リスト (Track Lists)] を展開します。
 - ステップ 4** 表示する既存のトラック メンバーまたはトラック リストをクリックします。
 - ステップ 5** [Stats] タブをクリックします。

- ステップ 6** [統計情報の選択 (Select Stats)] アイコンをクリックして、表示するプローブ統計タイプを選択します。
- ステップ 7** プローブ統計タイプを選択し (選択した統計タイプは青色で強調表示されます)、矢印アイコンで [使用可能 (Available)] から [選択済み (Selected)] に移動します。反対の矢印アイコンを使用して、プローブ統計タイプを [選択済み (Selected)] から [使用可能 (Available)] に戻すことができます。
- ステップ 8** 表示するプローブ統計タイプの選択が終了したら、[送信 (Submit)] をクリックします。
-

次のタスク

このタスクで選択された統計情報は、グラフの上の凡例に表示されます。カウンタが累積し始めると、選択したプローブ統計タイプを表す線がグラフに表示されます。



第 27 章

HSRP

この章は、次の項で構成されています。

- [HSRP について \(441 ページ\)](#)
- [Cisco APIC と HSRP について \(442 ページ\)](#)
- [HSRP のバージョン \(443 ページ\)](#)
- [注意事項と制約事項 \(444 ページ\)](#)
- [デフォルトの HSRP 設定 \(445 ページ\)](#)
- [GUI を使用した HSRP の設定 \(446 ページ\)](#)

HSRP について

HSRP はファーストホップ冗長プロトコル (FHRP) であり、ファーストホップ IP ルータの透過的なフェールオーバーを可能にします。HSRP は、デフォルト ルータの IP アドレスを指定して設定された、イーサネット ネットワーク上の IP ホストにファーストホップルーティングの冗長性を提供します。ルータ グループでは HSRP を使用して、アクティブ ルータおよびスタンバイルータを選択します。ルータ グループでは、アクティブルータはパケットをルーティングするルータであり、スタンバイルータはアクティブルータに障害が発生したときや、プリセット条件に達したときに使用されるルータです。

大部分のホストの実装では、ダイナミックなルータ ディスカバリ メカニズムをサポートしていませんが、デフォルトのルータを設定することはできます。すべてのホスト上でダイナミックなルータ ディスカバリ メカニズムを実行するのは、管理上のオーバーヘッド、処理上のオーバーヘッド、セキュリティ上の問題など、さまざまな理由で現実的ではありません。HSRP は、そうしたホストにフェールオーバー サービスを提供します。

HSRP を使用するとき、ホストのデフォルト ルータとして HSRP 仮想 IP アドレスを設定します (実際のルータ IP アドレスの代わりに)。仮想 IP アドレスは、HSRP が動作するルータのグループで共有される IPv4 または IPv6 アドレスです。

ネットワーク セグメントに HSRP を設定する場合は、HSRP グループ用の仮想 MAC アドレスと仮想 IP アドレスを設定します。グループの各 HSRP 対応インターフェイス上で、同じ仮想アドレスを指定します。各インターフェイス上で、実アドレスとして機能する固有の IP アドレスおよび MAC アドレスも設定します。HSRP はこれらのインターフェイスのうちの 1 つを

アクティブ ルータにするために選択します。アクティブ ルータは、グループの仮想 MAC アドレス宛ての packets を受信してルーティングします。

指定されたアクティブ ルータで障害が発生すると、HSRP によって検出されます。その時点で、選択されたスタンバイ ルータが HSRP グループの MAC アドレスおよび IP アドレスの制御を行うこととなります。HSRP はこの時点で、新しいスタンバイ ルータの選択も行います。

HSRP ではプライオリティ指示子を使用して、デフォルトのアクティブ ルータにする HSRP 設定インターフェイスを決定します。アクティブ ルータとしてインターフェイスを設定するには、グループ内の他のすべての HSRP 設定インターフェイスよりも高いプライオリティを与えます。デフォルトのプライオリティは 100 なので、それよりもプライオリティが高いインターフェイスを 1 つ設定すると、そのインターフェイスがデフォルトのアクティブ ルータになります。

HSRP が動作するインターフェイスは、マルチキャストユーザデータグラムプロトコル (UDP) ベースの hello メッセージを送受信して、障害を検出し、アクティブおよびスタンバイ ルータを指定します。アクティブ ルータが設定された時間内に hello メッセージを送信できなかった場合は、最高のプライオリティのスタンバイ ルータがアクティブ ルータになります。アクティブ ルータとスタンバイ ルータ間の packet フォワーディング機能の移動は、ネットワーク上のすべてのホストに対して完全に透過的です。

1 つのインターフェイス上で複数の HSRP グループを設定できます。仮想ルータは物理的には存在しませんが、相互にバックアップするように設定されたインターフェイスにとって、共通のデフォルトルータになります。アクティブ ルータの IP アドレスを使用して、LAN 上でホストを設定する必要はありません。代わりに、仮想ルータの IP アドレス (仮想 IP アドレス) をホストのデフォルトルータとして設定します。アクティブ ルータが設定時間内に hello メッセージを送信できなかった場合は、スタンバイ ルータが引き継いで仮想アドレスに応答し、アクティブ ルータになってアクティブ ルータの役割を引き受けます。ホストの観点からは、仮想ルータは同じままです。



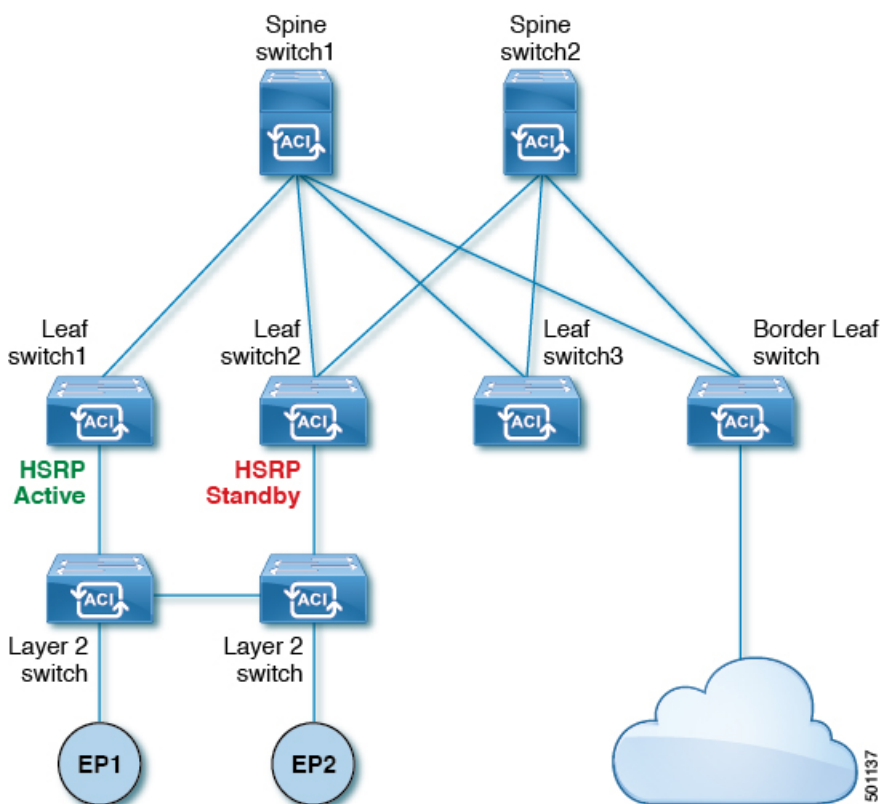
- (注) ルーテッドポートで受信した HSRP 仮想 IP アドレス宛の packets は、ローカルルータ上で終端します。そのルータがアクティブ HSRP ルータであるのかスタンバイ HSRP ルータであるのかは関係ありません。このプロセスには ping トラフィックと Telnet トラフィックが含まれます。レイヤ 2 (VLAN) インターフェイスで受信した HSRP 仮想 IP アドレス宛の packets は、アクティブ ルータ上で終端します。

Cisco APIC と HSRP について

Cisco ACI の HSRP は、ルーテッドインターフェイスまたはサブインターフェイスでのみサポートされます。したがって HSRP は、レイヤ 3 Out でのみ設定できます。レイヤ 2 接続は、HSRP を実行している ACI リーフスイッチ間のレイヤ 2 スイッチなどの外部デバイスから提供される必要があります。HSRP は外部レイヤ 2 接続上で Hello メッセージを交換するリーフスイッチ上で動作するからです。HSRP の hello メッセージは、スパインスイッチではパススルーされません。

次に示すのは、Cisco APIC での HSRP の導入のトポロジの例です。

図 57: HSRP の配置トポロジ



HSRP のバージョン

Cisco APICは、デフォルトで HSRP バージョン 1 をサポートします。HSRP バージョン 2 を使用するようにインターフェイスを設定できます。

HSRP バージョン 2 では、HSRP バージョン 1 から次のように拡張されています。

- グループ番号の範囲が拡大されました。HSRP バージョン 1 がサポートするグループ番号は 0 ~ 255 です。HSRP バージョン 2 がサポートするグループ番号は 0 ~ 4095 です。
- IPv4 では、HSRP バージョン 1 で使用する IP マルチキャストアドレス 224.0.0.2 の代わりに、IPv4 マルチキャストアドレス 224.0.0.102 または IPv6 マルチキャストアドレス FF02::66 を使用して hello パケットを送信します。
- IPv4 では 0000.0C9F.F000 ~ 0000.0C9F.FFFF、IPv6 アドレスでは 0005.73A0.0000 ~ 0005.73A0.0FFF の MAC アドレス範囲を使用します。HSRP バージョン 1 で使用する MAC アドレス範囲は、0000.0C07.AC00 ~ 0000.0C07.ACFF です。

注意事項と制約事項

次の注意事項と制約事項に従ってください。

- HSRP 状態は、HSRP IPv4 および IPv6 の両方で同じである必要があります。フェールオーバー後に同じ状態になるようにするには、プライオリティとプリエンプションを設定する必要があります。
- 現在、1 個の IPv4 と 1 個の IPv6 グループのみが Cisco ACI の同じサブインターフェイスでサポートされています。デュアルスタックが設定されている場合でも、仮想 MAC は IPv4 および IPv6 HSRP の設定で同じである必要があります。
- HSRP ピアに接続しているネットワークが純粋なレイヤ 2 ネットワークである場合、BFD IPv4 および IPv6 がサポートされています。リーフスイッチでは、別のルータの MAC アドレスを設定する必要があります。BFD セッションは、リーフ インターフェイスで異なる MAC アドレスを設定する場合にのみアクティブになります。
- ユーザーは、デュアルスタック設定の IPv4 および IPv6 HSRP グループに同じ MAC アドレスを設定する必要があります。
- HSRP VIP はインターフェイス IP と同じサブネット内にある必要があります。
- HSRP 設定のインターフェイス遅延を設定することをお勧めします。
- HSRP は、ルーテッドインターフェイスまたはサブインターフェイスでのみサポートされます。HSRP は、VLAN インターフェイスおよびスイッチ済み仮想インターフェイス (SVI) ではサポートされていません。したがって、HSRP の VPC サポートは使用できません。
- HSRP のオブジェクト トラッキングはサポートされていません。
- SNMP の HSRP 管理情報ベース (MIB) はサポートされません。
- HSRP では、複数グループの最適化 (MGO) はサポートされていません。
- ICMP IPv4 および IPv6 のリダイレクトはサポートされていません。
- Cold Standby および Non-Stop Forwarding (NSF) は、Cisco ACI 環境で再起動できないためサポートされていません。
- HSRP はリーフスイッチでのみサポートされているため、拡張ホールドダウンタイマーのサポートはありません。HSRP はスパインスイッチでサポートされていません。
- APIC 内では、HSRP のバージョン変更はサポートされていません。設定を削除し、新しいバージョンを再設定する必要があります。
- HSRP バージョン 2 は HSRP バージョン 1 と相互運用できません。どちらのバージョンも相互に排他的なので、インターフェイスはバージョン 1 およびバージョン 2 の両方を運用できません。しかし、同一ルータの異なる物理インターフェイス上であれば、異なるバージョンを実行できます。

- ルートセグメンテーションは、HSRP がインターフェイスでアクティブな場合、Cisco Nexus 93128TX、Cisco Nexus 9396PX、および Cisco Nexus 9396TX リーフスイッチでプログラムされています。したがって、インターフェイスでルートパケットに実施する DMAC=router MAC チェックはありません。この制限は、Cisco Nexus 93180LC EX、Cisco Nexus 93180YC-EX、Cisco Nexus 93108TC EX リーフスイッチには適用されません。
- HSRP 設定は、基本的な GUI モードではサポートされていません。APIC リリース 3.0 (1) 以降、基本的な GUI モードが廃止されました。
- ファブリックからレイヤ 3 アウトトラフィックは、状態に関係なく HSRP リーフスイッチ全体で常にロードバランスします。HSRP リーフスイッチが複数のポッドにわたる場合、ファブリックからアウトトラフィックは同じポッドで常にリーフスイッチを使用します。
- この制限は、以前の Cisco Nexus 93128TX、Cisco Nexus 9396PX と Cisco Nexus 9396TX スイッチの一部に適用されます。HSRP を使用すると、レイヤ 2 の外部デバイスのフラッピングを防ぐため、ルーテッドインターフェイスまたはルーテッドサブインターフェイスの MAC アドレスを 1 個変更する必要があります。これは、インターフェイス論理プロファイルの下で論理インターフェイスごとに Cisco APIC が同じ MAC アドレス (00:22:BD:F8:19:FF) を割り当てるためです。

デフォルトの HSRP 設定

パラメータ	デフォルト値
Version	1
Delay	0
Reload Delay	0
Interface Control	No 使用-焼き込みアドレス (BIA)
Group ID	0
Group Af	IPv4
IP Obtain Mode	admin
プライオリティ	100
Hello Interval	3000 ミリ秒
Hold Interval	10000 ミリ秒
Group Control	プリエンプションは無効
Preempt Delay	0

パラメータ	デフォルト値
Authentication Type	プレーンテキスト
Authentication Key Timeout	0
VMAC	導出方法 (HSRP グループ Id)

GUI を使用した HSRP の設定

リーフスイッチが設定されている場合、HSRP が有効になっています。

始める前に

- テナントと VRF が設定されています。
- VLAN プールは、適切な VLAN 範囲が定義され、レイヤ 3 ドメインが作成されて VLAN プールに接続されている状態で設定される必要があります。
- エンティティプロファイルの接続も、レイヤ 3 ドメインに関連付けられている必要があります。
- リーフスイッチのインターフェイスプロファイルは必要に応じて設定する必要があります。

ステップ 1 メニューバーで、>[テナント]>[Tenant-name] をクリックします。[ナビゲーション (Navigation)] ページで、[ネットワーキング (Networking)] > L3Outs > L3Out_name > [論理ノードプロファイル (Logical Node Profiles)] > [論理インターフェイスプロファイル (Logical Interface Profile)] をクリックします。

ここで、HSRP インターフェイスプロファイルが作成されます。

ステップ 2 論理インターフェイスプロファイルを選択し、**Create HSRP Interface Profile** をクリックします。

ステップ 3 **Create HSRPInterface Profile** ダイアログボックスで、次の操作を実行します。

- Version** フィールドで、該当するバージョンを選択します。
- HSRP Interface Policy** フィールドで、ドロップダウンから **Create HSRP Interface Policy** を選択します。
- Create HSRP Interface Policy** ダイアログボックスの **Name** フィールドに、ポリシーの名前を入力します。
- Control** フィールドで、該当するコントロールを選択します。
- Delay** フィールドと **Reload Delay** フィールドで、該当する値を設定します。**Submit** をクリックします。

HSRP インターフェイスポリシーが作成され、インターフェイスプロファイルに関連付けられます。

ステップ 4 **Create HSRP Interface Profile** ダイアログボックスで、**HSRP Interface Groups** を展開します。

ステップ 5 **Create HSRP Group Profile** ダイアログボックスで、次の操作を実行します。

- Name** フィールドに、HSRP インターフェイスのグループ名を入力します。

- b) **Group ID** フィールドで、適切な ID を選択します
使用可能な値は、HSRP バージョン 1 または 2 のバージョンのいずれがインターフェイス プロファイルに選択されたかに応じて異なります。
- c) **IP** フィールドに、IP アドレスを入力します。
この IP アドレスはインターフェイスと同じサブネット内になければなりません。
- d) **MAC Address** フィールドに、Mac アドレスを入力します。
(注) このフィールドを空白のままにすると、HSRP 仮想 MAC アドレスはグループ ID に基づいて自動的に計算されます。
- e) [グループ名 (Group Name)] フィールドにグループ名を入力します。
これは、HSRP MGO 機能の HSRP により、プロトコルで使用する名前です。
- f) **Group Type** フィールドで、該当するタイプを選択します。
- g) **IP Obtain Mode** フィールドで、該当するモードを選択します。
- h) **HSRP Interface Policy** フィールドで、ドロップダウンから **Create HSRP Interface Policy** を選択します。

ステップ 6 Create HSRP Group Policy ダイアログボックスで、次の操作を実行します。

- a) **Name** フィールドに、HSRP グループポリシーの名前を入力します。
- b) **Key or Password** フィールドが自動的に設定されます。
認証タイプのデフォルト値はシンプルで、キーは、「cisco」です。これはユーザーが新規ポリシーを作成するときに、デフォルトで選択されます。
- c) **Type** フィールドで、必要とするセキュリティのレベルを選択します。
- d) **Priority** フィールドで、アクティブ ルータとスタンバイ ルータを定義する優先度を選択します。
- e) 残りのフィールドで、該当する値を選択し、**Submit** をクリックします。
HSRP グループ ポリシーが作成されます。
- f) **Secondary Virtual IPs** フィールドに自動記入することにより、セカンダリ バーチャル IP を作成します。
これは、セカンダリ バーチャル IP で各サブインターフェイスで HSRP を有効にするために使用できます。また、ここで指定する IP アドレスは、インターフェイスのサブネットになければなりません。
- g) **OK** をクリックします。

ステップ 7 Create HSRP Interface Profile ダイアログボックスで、**Submit** をクリックします。
これで HSRP の設定は完了です。

ステップ 8 [ナビゲーション] ペインで、作成した HSRP インターフェイスとグループ ポリシーを確認するには、[ネットワーク (Networking)] > [プロトコル ポリシー (Protocol Policies)] > [HSRP] をクリックします。



CHAPTER 28

Cisco ACI GOLF

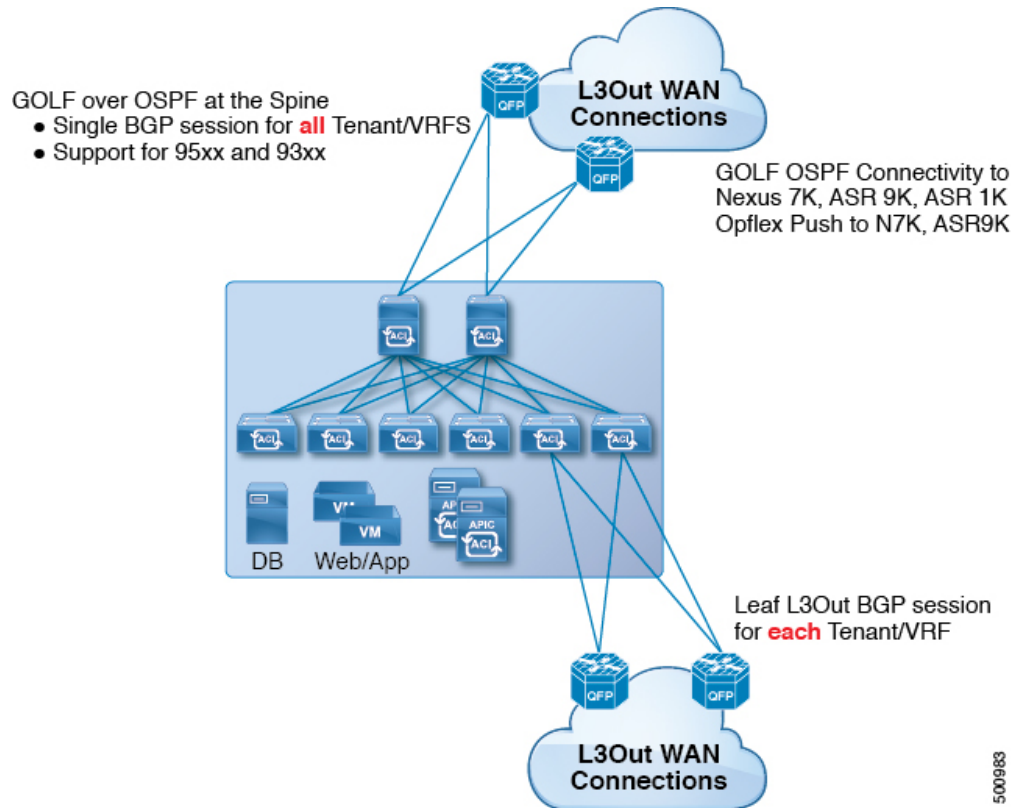
- [Cisco ACI GOLF, on page 449](#)
- [DCIG への BGP EVPN タイプ 2 ホスト ルートの分散化, on page 456](#)

Cisco ACI GOLF

Cisco ACI GOLF

Cisco ACI GOLF 機能 (ファブリック WAN のレイヤ 3 EVPN サービス機能とも呼ばれる) では、より効率的かつスケーラブルな ACI ファブリック WAN 接続が可能になります。スパインスイッチに接続されている WAN に OSPF 経由で BGP EVPN プロトコルが使用されます。

図 58 : Cisco ACI GOLF のトポロジ



すべてのテナント WAN 接続が、WAN ルータが接続されたスパインスイッチ上で単一のセッションを使用します。データセンター相互接続ゲートウェイ (DCIG) へのテナント BGP セッションのこの集約では、テナント BGP セッションの数と、それらすべてに必要な設定の量を低減することによって、コントロールプレーンのスケールが向上します。ネットワークは、スパインファブリックポートに設定されたレイヤ3サブインターフェイスを使用して拡張されます。GOLFを使用した、共有サービスを伴うトランジットルーティングはサポートされていません。

スパインスイッチでの GOLF 物理接続のためのレイヤ3外部外側ネットワーク (L3extOut) は、*infra* テナントの下で指定され、次のものを含みます:

- LNodeP (*infra* テナントの L3Out では、L3extInstP は必要ありません)。
- *infra* テナントの GOLF 用の L3extOut のプロバイダラベル。
- OSPF プロトコルポリシー
- BGP プロトコルポリシー

すべての通常テナントが、上記で定義した物理接続を使用します。通常のテナントで定義した L3extOut では、次が必要です:

- サブネットとコントラクトを持つ `l3extInstP` (EPG)。サブネットの範囲を使用して、ルート制御ポリシーとセキュリティポリシーのインポートまたはエクスポートを制御します。ブリッジドメインサブネットは外部的にアダプタイズするように設定される必要があります。アプリケーション EPG および GOLF L3Out EPG と同じ VRF に存在する必要があります。
- アプリケーション EPG と GOLF L3Out EPG の間の通信は、(契約優先グループではなく) 明示的な契約によって制御されます。
- `l3extConsLbl` コンシューマ ラベル。これは `infra` テナントの GOLF 用の L3Out の同じプロバイダラベルと一致している必要があります。ラベルを一致させることにより、他のテナント内のアプリケーション EPG が `LNodeP` 外部 L3Out EPG を利用することが可能になります。
- `infra` テナント内のマッピングプロバイダ `L3extOut` の BGP EVPN セッションは、この L3Out で定義されたテナント ルートをアダプタイズします。

注意事項と制約事項

次に示す GOLF のガイドラインおよび制限事項に従ってください。

- GOLF ルータは、トラフィックを受け入れるために少なくとも 1 つのルートを Cisco ACI にアダプタイズする必要があります。Cisco ACI が外部ルータからルートを受信するまで、リーフスイッチと外部ルータの間にトンネルは作成されません。
- すべての Cisco Nexus 9000 シリーズ ACI モードのスイッチと、すべての Cisco Nexus 9500 プラットフォーム ACI モード スイッチライン カードおよびファブリック モジュールが GOLF をサポートします。Cisco APIC、リリース 3.1(x) 以降では、これに N9K-C9364C スイッチが含まれます。
- 現時点では、ファブリック全体のスパインスイッチインターフェイスに展開できるのは、単一の GOLF プロバイダ ポリシーだけです。
- APIC リリース 2.0(2) までは、GOLF はマルチポッドでサポートされていません。リリース 2.0 (2) では、同じファブリックでの 2 つの機能を、スイッチ名の末尾に「EX」のない Cisco Nexus N9000K スイッチ上でのみサポートしています。たとえば N9K-9312TX です。2.1(1) リリース以降では、2 つの機能を、マルチポッドおよび EVPN トポロジで使用されているすべてのスイッチでともに展開できるようになりました。
- スパインスイッチで GOLF を設定する場合、コントロールプレーンがコンバージするまでは、別のスパインスイッチで GOLF の設定を行わないでください。
- スパインスイッチは複数のプロバイダの GOLF 外側ネットワーク (GOLF L3Outs) に追加できますが、GOLF L3Out ごとのプロバイダ ラベルは異なっている必要があります。また、この例では、OSPF エリアも `L3extOut` ごとに異なっていて、異なるループバックアドレスを使用する必要があります。
- `infra` テナント内のマッピングプロバイダ `L3out` の BGPEVPN セッションは、この `L3extOut` で定義されたテナント ルートをアダプタイズします。

- 3つの GOLF Outs を展開する場合、1つだけが GOLF, and 0/0 エクスポート集約のプロバイダ/コンシューマラベルを持っているなら、APICはすべてのルートをエクスポートします。これは、テナントのリーフスイッチ上の既存の L3extOut と同じです。
- スパインスイッチとデータセンター相互接続 (DCI) ルータ間に直接ピアリングがある場合、リーフスイッチから ASR へのトランジットルートには、リーフスイッチの PTEP として次のホップが存在することになります。この場合、その ACI ポッドの TEP 範囲に対して ASR の静的ルートを定義します。また、DCI が同じポッドにデュアルホーム接続されている場合は、静的ルートの優先順位 (管理距離) は、他のリンクを通じて受信するルートと同じである必要があります。
- デフォルトの bgpPeerPfxPol ポリシーは、ルートを 20,000 に制限します。ACI WAN インターコネクト ピアの場合には、必要に応じてこれを増やしてください。
- 1つのスパインスイッチ上に2つの L3extOut が存在し、そのうちの一方のプロバイダラベルが prov1 で DCI 1 とピアリングしており、もう一方の L3extOut のプロバイダラベルが prov2 で DCI 2 とピアリングしているという、展開シナリオを考えます。テナント VRF に、プロバイダラベルのいずれか一方 (prov1 または prov2) をポイントしているコンシューマラベルがある場合、テナントルートは DCI 1 と DCI 2 の両方に送信されます。
- GOLF OpFlex Vrf を集約する場合、ACI ファブリックまたは GOLF OpFlex VRF とシステム内のその他の VRF 間の GOLF デバイスでは、ルートのリーキングは発生しません。VRF リーキングのためには、(GOLF ルータではなく) 外部デバイスを使用する必要があります。



(注) Cisco ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ 3 Outside (L3Out) 接続、または Inter-Pod Network (IPN) を介したマルチポッド接続を設定する場合は、インターフェイス MTU がリンクの両端で適切に設定されていることが推奨されます。Cisco ACI、Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定可能な MTU 値はイーサネットヘッダー (一致する IP MTU、14-18 イーサネットヘッダーサイズを除く) を考慮していません。また、IOS XR などの他のプラットフォームには、設定された MTU 値にイーサネットヘッダーが含まれています。設定された値が 9000 の場合、Cisco ACI、Cisco NX-OS Cisco IOS の最大 IP パケットサイズは 9000 バイトになりますが、IOS-XR のタグなしインターフェイスの最大 IP パケットサイズは 8986 バイトになります。

各プラットフォームの適切な MTU 値については、それぞれの設定ガイドを参照してください。

CLI ベースのコマンドを使用して MTU をテストすることを強く推奨します。たとえば、Cisco NX-OS CLI で ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1 などのコマンドを使用します。

Multi-Site サイト間の共有 GOLF 接続を使用する

複数のサイトで共有 APIC ゴルフ接続

トポロジでは、複数のサイト、APIC サイトの拡大 Vrf は、ゴルフ接続を共有している場合、リスクのクロス VRF トラフィックの問題を回避する次のガイドラインに従います。

スパインスイッチと、DCI の間でルートターゲットの設定

ゴルフ Vrf の EVPN ルート ターゲット (RTs) を設定する 2 つの方法があります: 手動 RT と自動 RT. ルート ターゲットは、ACI 背表紙と OpFlex を介して DCIs の間で同期されます。ゴルフ Vrf の自動 RT は、形式に組み込まれて Fabric ID: - ASN : [FabricID] VNID

2 つのサイトには、次の図のように導入の Vrf がある、Vrf 間のトラフィックを混在させることができます。

サイト 1	サイト 2
ASN: 100、ファブリック ID: 1	ASN: 100、ファブリック ID: 1
VRF A : VNID 1000 インポート/エクスポートルートターゲット : 100 : [1] 1000	VRF A : VNID 2000 インポート/エクスポートルートターゲット : 100 : [1] 2000
VRF B : VNID 2000 インポート/エクスポートルートターゲット : 100 : [1] 2000	VRF B : VNID 1000 インポート/エクスポートルートターゲット : 100 : [1] 1000

Dci のために必要なルート マップ

トンネルは、中継ルートは、[DCI を介してリークとサイト間では作成されません、ため、コントロールプレーンの手間をも削減する必要があります。もう 1 つのサイトでゴルフ スパインに、DCI への 1 つのサイトでゴルフ スパインから送信される EVPN タイプ 5 およびタイプ 2 ルートを送信できませんする必要があります。これが発生スパイン スイッチに dci のために次のタイプの BGP セッションが必要がある場合。

Site1: IBGP--DCI--EBGP--サイト 2

Site1: EBGP--DCI--IBGP--サイト 2

Site1:--DCI--EBGP EBGP--サイト 2

Site1: IBGP RR クライアント--DCI (RR)---IBGP サイト 2

Dci のためにこの問題を避けるためには、ルートマップは、インバウンドおよびアウトバウンドのピア ポリシーのさまざまな BGP コミュニティで使用されます。

ルートを 1 つのサイト、もう 1 つのサイト フィルタ着信ピア ポリシーでコミュニティに基づくルートでゴルフ スパインへのアウトバウンドピア ポリシー ゴルフ スパインから受信しま

す。別のアウトバウンドピアポリシーは、WANへコミュニティを取り除き。すべてのルートマップは、ピアのレベルでです。

GUI を使用した ACI GOLF の設定

次に、任意のテナントネットワークが使用できるインフラ GOLF サービスを設定する手順について説明します。

ステップ 1 メニューバーで、をクリックして **テナント**、] をクリックし、 **インフラ** を選択、テナントインフラ。

ステップ 2 [ナビゲーション (Navigation)] ペインで、[ネットワーク キング (Networking)] オプションを展開し、次のアクションを行います。

- [L3Outs] を右クリックし、[L3Out の作成 (Create L3Out)] をクリックして、[L3Out の作成 (Create L3Out)] ウィザードを開きます。
- [名前 (Name)]、[VRF]、および [L3 ドメイン (L3 Domain)] フィールドに必要な情報を入力します。
- [用途: (Use For:)] フィールドで、[Golf] を選択します。

[プロバイダラベル (Provider Label)] フィールドと [ルートターゲット (Route Target)] フィールドが表示されます。

- [プロバイダラベル (Provider Label)] フィールドに、プロバイダラベル (たとえば、**golf**) を入力します。
- ルートターゲット** フィールドで、自動または明示的なポリシーを持つ BGP ルートターゲットをフィルタリングポリシーを使用するかどうかを選択します。

- **自動** -自動 BGP ルートターゲット Vrf でフィルタリングは、これに関連付けられている実装は、外部設定をルーティングします。
- **明示的な** -ルートターゲットの明示的にフィルタリングの実装では、この設定の外部ルーティングに関連付けられている Vrf に BGP ルートターゲットポリシーが設定されています。

(注) 明示的なルートターゲットポリシーが設定されている、**BGP ルートターゲットプロファイル** テーブルで、**BGP ページ** の **VRF ウィザードの作成** します。選択した場合、**自動** オプションで **ルートターゲット** フィールドで明示ルートターゲットポリシーの設定、**VRF ウィザードの作成** BGP ルーティングの中断を引き起こす可能性があります。

- 残りのフィールドはそのままにして (BGP を選択するなど)、[次へ (Next)] をクリックします。

[ノードとインターフェイス (Nodes and Interfaces)] ウィンドウが表示されます。

ステップ 3 [L3Out の作成 (Create L3Out)] ウィザードの [ノードとインターフェイス (Nodes and Interfaces)] ウィンドウに必要な情報を入力します。

- [**ノード ID**] ドロップダウンリストで、スパインスイッチノード ID を選択します。
- [Router ID] フィールドに、ルータ ID を入力します。
- (任意) 必要に応じて、ループバックアドレスに別の IP アドレスを設定できます。

[ルータ ID (Router ID)] フィールドに入力したエントリと同じ内容が [ループバックアドレス (Loopback Address)] フィールドに自動で入力されます。これは以前のビルドでの [ループバックアドレスのルータ ID の使用 (Use Router ID for Loopback Address)] と同等です。ループバックアドレスにルート ID を使用しない場合は、ループバックアドレスに別の IP アドレスを入力します。ループバックアドレスにルータ ID を使用しない場合は、このフィールドを空のままにします。

- d) [外部コントロールピア (External Control Peering)] フィールドはオンのままにします。
- e) [ノードとインターフェイス (Nodes and Interfaces)] ウィンドウに追加の必要な情報を入力します。
このウィンドウに表示されるフィールドは、[レイヤ 3 (Layer 3)] および [レイヤ 2 (Layer 2)] 領域で選択したオプションによって異なります。
- f) [ノードとインターフェイス (Nodes and Interfaces)] ウィンドウで残りの追加の情報を入力したら、[次 (Next)] をクリックします。

[プロトコル (Protocols)] ウィンドウが表示されます。

ステップ 4 [L3Out の作成 (Create L3Out)] ウィザードの [プロトコル (Protocols)] ウィンドウに必要な情報を入力します。

- a) [BGP ループバック ポリシー (BGP Loopback Policies)] および [BGP インターフェイス ポリシー (BGP Interface Policies)] 領域で、次の情報を入力します。
 - **ピアアドレス (Peer Address)** : ピア IP アドレスを入力します
 - **EBGP Multihop TTL (EBGP マルチホップ TTL)** : 接続の存続可能時間 (TTL) を入力します。範囲は 1 - 255 ホップです。ゼロの場合、TTL は指定されません。デフォルトは 0 です。
 - **リモート ASN (Remote ASN)** : ネイバー自律システムを固有に識別する番号を入力します。自律システム番号は、プレーン形式の 1 - 4294967295 の 4 バイトにすることができます。
(注) ACI は asdot または asdot+ 形式の自律システム番号をサポートしません。

- b) [OSPF] 領域で、デフォルト OSPF ポリシー、以前に作成した OSPF ポリシー、または [OSPF インターフェイス ポリシーの作成 (Create OSPF Interface Policy)] を選択します。
- c) [次へ (Next)] をクリックします。

[外部 EPG (External EPG)] ウィンドウが表示されます。

ステップ 5 [L3Out の作成 (Create L3Out)] ウィザードで [外部 EPG (External EPG)] ウィンドウに必要な情報を入力します。

- a) **Name** フィールドに、外部ネットワークの名前を入力します。
- b) [提供済みコントラクト (Provided Contract)] フィールドで、提供済みコントラクトの名前を入力します。
- c) [消費済みコントラクト (Consumed Contract)] フィールドで、消費済みコントラクトの名前を入力します。
- d) [すべてのサブネットを許可 (Allow All Subnet)] フィールドで、この L3Out 接続からのすべての中継ルートをアドバタイズしない場合はオフにします。

このボックスをオフにすると、[Subnets] 領域が表示されます。次の手順に従って、必要なサブネットとコントロールを指定します。

- e) [完了 (Finish)] をクリックして、[L3Out の作成 (Create L3Out)] ウィザードに必要な設定の入力を完了させます。

ステップ 6 テナントの [ナビゲーション (Navigation)] ペインで、*tenant_name* > [ネットワーキング (Networking)] > **L3Outs** を展開し、次のアクションを行います。

- a) [L3Outs] を右クリックし、[L3Out の作成 (Create L3Out)] をクリックしてウィザードを開きます。
- b) [名前 (Name)]、[VRF]、および [L3 ドメイン (L3 Domain)] フィールドに必要な情報を入力します。
- c) [GOLF の使用 (Use for GOLF)] フィールドの横にあるボックスをオンにします。
- d) [ラベル (Label)] フィールドで、[コンシューマ (Consumer)] を選択します。
- e) [コンシューマ ラベル] を割り当てます。この例では、(以前に作成した) *golf* を使用します。
- f) [次へ (Next)] をクリックし、[完了 (Finish)] をクリックします。

DCIG への BGP EVPN タイプ 2 ホスト ルートの分散化

DCIG への BGP EVPN タイプ 2 のホスト ルートの配信

APIC ではリリース 2.0(1f) まで、ファブリック コントロールプレーンは EVPN ホスト ルートを直接送信してはいませんでしたが、Data Center Interconnect Gateway (DCIG) にルーティングしている BGP EVPN タイプ 5 (IP プレフィックス) 形式のパブリック ドメイン (BD) サブネットをアダプタイズしていました。これにより、最適ではないトラフィックの転送となる可能性があります。転送を改善するため APIC リリース 2.1 x では、ファブリック スパインを有効にして、パブリック BD サブネットとともに DCIG に EVPN タイプ 2 (MAC-IP) ホスト ルートを使用してホスト ルートをアダプタイズできます。

そのためには、次の手順を実行する必要があります。

1. BGP アドレス ファミリ コンテキスト ポリシーを設定する際に、ホスト ルート リークを有効にします。
2. GOLF セットアップで BGP EVPN へのホスト ルートをリークする場合：
 1. GOLF が有効になっている場合にホスト ルートを有効にするには、インフラストラクチャ テナント以外に、BGP アドレス ファミリ コンテキスト ポリシーがアプリケーション テナント (アプリケーション テナントはコンシューマ テナントであり、エンドポイントを BGP EVPN にリークします) で設定されている必要があります。
 2. 単一ポッド ファブリックについては、ホスト ルート機能は必要ありません。ホスト ルート機能は、マルチポッド ファブリック セットアップで最適ではない転送を避けるために必要です。ただし、単一ポッド ファブリック がセットアップされる場合、エンドポイントから BGP EVPN にリークするため、ファブリック 外部接続 ポリシーを設定

し ETEP IP アドレスを提供する必要があります。そうしないと、ホストルートは、BGP EVPN にはリークされません。

3. VRF のプロパティを設定する場合：
 1. IPv4 および IPv6 の各アドレス ファミリの BGP コンテキストに BGP アドレス ファミリ コンテキスト ポリシーを追加します。
 2. VRF からインポートまたはエクスポート可能なルートを特定する BGP ルートターゲット プロファイルを設定します。

GUI を使用して DCIG への BGP EVPN タイプ 2 のホストルートを分散する

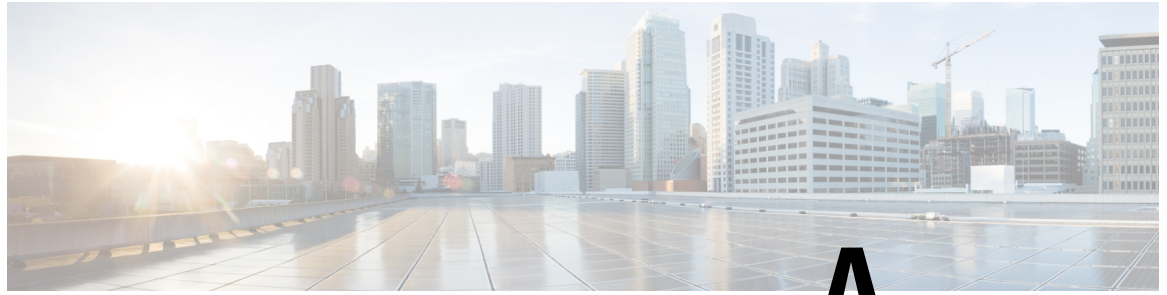
次の手順で BGP EVPN タイプ 2 のホストルートの分散を有効にします。

始める前に

インフラテナントでの ACI の WAN 相互接続サービスをすでに設定しており、サービスを使用するテナントを設定している

-
- ステップ 1 メニューバーで [テナント (Tenants)] > [インフラ (infra)] をクリックします。
 - ステップ 2 [ナビゲーション (Navigation)] ペインで、[ポリシー (Policies)] > [プロトコル (Protocol)] > [BGP] をクリックします。
 - ステップ 3 **BGP Address Family Context** を右クリックし、**Create BGP Address Family Context Policy** を選択し、次の手順を実行します:
 - a) ポリシーの名前を入力し、必要に応じて説明を追加します。
 - b) **Enable Host Route Leak** チェック ボックスをクリックします。
 - c) **Submit** をクリックします。
 - ステップ 4 [テナント (Tenants)] > [tenant-name] (BGP アドレス ファミリ コンテキスト ポリシーを使用するテナント) をクリックし、[ネットワーキング (Networking)] を展開します。
 - ステップ 5 **VRF** を展開し、分散するホストルートを含む VRF をクリックします。
 - ステップ 6 VRF のプロパティを設定するときには、**BGP Address Family Context Policy** を IPv4 と IPv6 の **BGP Context Per Address Families** に追加します。
 - ステップ 7 [送信 (Submit)] をクリックします。
-

GUI を使用して DCIG への BGP EVPN タイプ 2 のホストルートを分散する



付録 **A**

レイヤ3 ネットワーキングの注意事項

- [レイヤ3 ネットワーキングの注意事項 \(459 ページ\)](#)

レイヤ3 ネットワーキングの注意事項

レイヤ3 外部接続を作成し、維持する際には、次のガイドラインを使用してください。

トピック	注意またはガイドライン
vPC ペアの境界リーフ スイッチが、誤った VNID を持つ BGP パケットをピア上で学習したエンドポイントに転送する問題	<p>設定に次の条件が存在する場合：</p> <ul style="list-style-type: none">• 2つのリーフ スイッチが vPC ペアの一部である• L3Out の背後に接続されている2つのリーフ スイッチの場合、宛先エンドポイントは2番目（ピア）の境界リーフ スイッチに接続され、エンドポイントはそのリーフ スイッチで学習されたピアです。 <p>ピアが学習したエンドポイント宛ての BGP パケットを受信する入力リーフ スイッチでエンドポイントが学習した場合、L3Out の背後にある最初のレイヤ3 スイッチ間で中継 BGP 接続が確立できないという問題が発生する可能性があります。および vPC ペアの2番目のリーフ スイッチ上のピア上で学習されたエンドポイント。これは、ポート 179 を持つ中継 BGP パケットが VRF VNID ではなくブリッジ ドメイン VNID を使用して誤って転送されるために発生します。</p> <p>この問題を解決するには、エンドポイントをファブリック内の他の非ピアリーフ スイッチに移動して、リーフ スイッチで学習されないようにします。</p>

トピック	注意またはガイドライン
境界リーフ スイッチおよび GIR (メンテナンス) モード	<p>境界リーフ スイッチに静的ルートがあり、GIR (Graceful Insertion and Removal) モード、またはメンテナンスモードがある場合、境界リーフ スイッチからのルートは ACI ファブリックにあるルーティング テーブルから削除されない可能性があり、ルーティングの問題が発生します。</p> <p>この問題を回避するには、次のいずれかを実行します。</p> <ul style="list-style-type: none"> • その他の境界リーフ スイッチで同じ管理ディスタンスを持つ同じ静的ルートを設定するか、 • 静的ルートの次のホップへの到達性を追跡するため IP SLA または BFD を使用します
L3Out 集約統計情報は出力ドロップ カウンタをサポートしません	<p>[テナント (Tenants)] [tenant_name] [ネットワーキング (Networking)] [L3Out] [L3Out_name] [統計情報 (Stats)] を介して、[統計情報の選択 (Select Stats)] ウィンドウにアクセスすると、L3Out 集約統計情報が出力ドロップ カウンタをサポートしていないことがわかります。 >>>>これは、EPG VLAN からの出力ドロップを記録する ASIC に現在ハードウェア テーブルがないため、これらのカウンタに統計情報が入力されないためです。 EPG VLAN の入力ドロップだけがあります。</p>
CLI による更新	<p>API または GUI で作成され CLI を通して更新されたレイヤ3 外部ネットワークについては、プロトコルは API または GUI を通して外部ネットワークでグローバルに有効にする必要があり、CLI を介してさらに更新を行う前に、すべての参加ノードのノードプロファイルは API または GUI を通して追加される必要があります。</p>
同じノード上のレイヤ3 ネットワークのループバック	<p>同じノードで2つのレイヤ3 の外部ネットワークを設定するときに、ループバックはレイヤ3 ネットワークに別々に設定されます。</p>
入力ベース ポリシーの適用	<p>Cisco APIC リリース 1.2(1)以降、入力ベース ポリシーの適用により、出入力両方向でレイヤ3 アウトサイド (L3Out) トラフィックにポリシー適用を定義できます。デフォルトでは入力になっています。リリース 1.2(1)以降にアップグレード中、既存の L3Out 設定が出力に設定され、動作が既存の設定と一致します。特別なアップグレードのシーケンスは必要ありません。アップグレード後、グローバルプロパティ値を入力に変更します。変更されると、システムがルールとプレフィックス エントリを再プログラミングします。規則は出力リーフから削除され、入力リーフ上に既存の規則がない場合は、入力リーフ上にインストールされます。既存の設定がない場合、Actrl プレフィックス エントリが入力リーフ上にインストールされます。ダイレクト サーバリターン (DSR) および属性 EPG には入力ベースのポリシー適用が必要です。vzAny と禁止コントラクトは、入力ベースのポリシー適用を契約無視します。入力には中継規則が適用されます。</p>

トピック	注意またはガイドライン
L3Outs によるブリッジ ドメイン	テナントのブリッジドメインには、共通テナントでプロビジョニングされている <code>l3extOut</code> によってアドバタイズされたパブリック サブネットを含めることができます。
OSPF と EIGRP のブリッジ ドメイン ルート アドバタイズメント	<p>OSPF と EIGRP の両方があるノード上の同じ VRF で有効であり、ブリッジドメインのサブネットがいずれか1つの L3Out からアドバタイズされる場合、他の L3Out で有効になっているプロトコルからも同様にアドバタイズされます。</p> <p>OSPF と EIGRP では、ブリッジドメインルートアドバタイズメントは VRF ごとに行われ、L3Out ごとには行われません。同じ VRF とノードで（複数エリアの）複数の OSPF L3Out が有効になっている場合、これと同じ動作が想定されます。この場合、ブリッジドメインのルートがいずれかの領域で有効になっていれば、すべての領域からアドバタイズされます。</p>
BGP 最大プレフィックス制限	Cisco APIC リリース 1.2 (1x) 以降、BGP <code>l3extOut</code> 接続のテナントポリシーは、最大プレフィックス制限を使用して設定できます。これにより、ピアから受信されるルートプレフィックスの数をモニタし、制限することができます。最大プレフィックス制限を超えると、ログエントリが記録され、さらにプレフィックスが拒否されます。カウントが一定の間隔でしきい値を下回る場合、接続を再起動することができますが、そうしない場合接続がシャットダウンします。一度に1つのオプションだけを使用できます。デフォルト設定では20,000プレフィックスに制限され、その後は新しいプレフィックスは拒否されます。拒否オプションが導入されると、APIC でエラーが発生する前に BGP は設定されている制限よりも1つ多くプレフィックスを受け入れます。

トピック	注意またはガイドライン
MTU	<ul style="list-style-type: none"> • Cisco ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ3 Outside (L3Out) 接続、または Inter-Pod Network (IPN) を介したマルチポッド接続を設定する場合は、インターフェイス MTU がリンクの両端で適切に設定されていることが推奨されます。Cisco ACI、Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定可能な MTU 値はイーサネットヘッダー (一致する IP MTU、14-18 イーサネットヘッダーサイズを除く) を考慮していません。また、IOS XR などの他のプラットフォームには、設定された MTU 値にイーサネットヘッダーが含まれています。設定された値が 9000 の場合、Cisco ACI、Cisco NX-OS Cisco IOS の最大 IP パケットサイズは 9000 バイトになりますが、IOS-XR のタグなしインターフェイスの最大 IP パケットサイズは 8986 バイトになります。 • 物理インターフェイスの MTU 設定は次のように異なります。Cisco ACI <ul style="list-style-type: none"> • サブインターフェイスの場合、物理インターフェイスの MTU は固定され、リーフスイッチの前面パネルポートでは 9216 に設定されます。 • SVI の場合、物理インターフェイス MTU はファブリック MTU ポリシーに基づいて設定されます。たとえば、ファブリック MTU ポリシーが 9000 に設定されている場合、SVI の物理インターフェイスは 9000 に設定されます。
L3Outs の QoS	<p>L3Out 用の QoS ポリシーを設定し、L3Out が存在する BL スイッチで適用されるポリシーを有効にするには、次の注意事項に従ってください。</p> <ul style="list-style-type: none"> • VRF ポリシー制御の適用方向を 出力 に設定する必要があります。 • VRF ポリシー制御適用の優先度設定を 有効 に設定する必要があります。 • L3Out を使用して EPG 間の通信を制御するコントラクトを設定する際に、コントラクトまたはコントラクトの件名に QoS クラスまたはターゲット DSCP を含めます。
ICMP 設定	<p>ICMP リダイレクトおよび ICMP 到達不能は、スイッチ CPU がこれらのパケットを生成しないように、デフォルトで無効になっています。Cisco ACI</p>



付録 **B**

NX-OS スタイル CLI を使用したタスクの実行

- [Part I : レイヤ 3 の設定 \(463 ページ\)](#)
- [パートII : 外部ルーティング \(L3Out\) の設定 \(493 ページ\)](#)

Part I : レイヤ 3 の設定

NX-OS スタイルの CLI を使用した共通パーベイシブ ゲートウェイの設定

NX-OS スタイルの CLI を使用した共通パーベイシブ ゲートウェイの設定

始める前に

- テナント、VRF、およびブリッジ ドメインが作成されていること。

共通パーベイシブ ゲートウェイを設定します。

例 :

```
apicl#configure
apicl(config)#tenant demo
apicl(config-tenant)#bridge-domain test
apicl(config-tenant-bd)#l2-unknown-unicast flood
apicl(config-tenant-bd)#arp flooding
apicl(config-tenant-bd)#exit

apicl(config-tenant)#interface bridge-domain test
apicl(config-tenant-interface)#multi-site-mac-address 12:34:56:78:9a:bc
apicl(config-tenant-interface)#mac-address 00:CC:CC:CC:C1:01 (Should be unique for each ACI fabric)
```

```
apic1(config-tenant-interface)#ip address 192.168.10.1/24 multi-site
apic1(config-tenant-interface)#ip address 192.168.10.254/24 (Should be unique for each ACI fabric)
```

NX-OS Style CLI を使用した IP エージングの設定

NX-OS スタイル CLI を使用した IP エージング ポリシーの設定

このセクションでは、CLI を使用した IP エージング ポリシーを有効および無効にする方法を説明します。

ステップ 1 IP エージング ポリシーを有効にするには：

例：

```
ifc1(config)# endpoint ip aging
```

ステップ 2 IP エージング ポリシーを無効にするには：

例：

```
ifav9-ifc1(config)# no endpoint ip aging
```

次のタスク

エンドポイントの IP アドレスをトラッキングするために使用される間隔を指定するには、エンドポイント保持ポリシーを作成します。

NX-OS スタイル CLI を使用したブリッジ ドメイン上のスタティック ルートの設定

NX-OS スタイル CLI を使用したブリッジ ドメイン上のスタティック ルートの設定

パーベイシブブリッジドメイン (BD) でスタティック ルートを設定するには、NX-OS スタイルの次の CLI コマンドを使用します：

始める前に

テナント、VRF、BD および EPG が設定されています。

- スタティック ルートのサブネットを作成するには、epg (fvAEPg で fvSubnet オブジェクト)、普及 BD (fvBD) 自体 BD しないに関連付けられているように構成されます。
- サブネットマスクが/32 にする必要があります (128/for IPv6) 1 つの IP アドレスまたは 1 つのエンドポイントをポイントします。これは、EPG に関連付けられている普及 BD で含まれています。

手順の概要

1. **configure**
2. **tenant** *tenant-name*
3. **application** *ap-name*
4. **epg** *epg-name*
5. **endpoint** *ipA.B.C.D/LEN next-hop A.B.C.D* [*scope scope*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure 例： apic1# configure	コンフィギュレーション モードに入ります。
ステップ 2	tenant <i>tenant-name</i> 例： apic1(config)# tenant t1	テナントを作成するか、テナント設定モードに入ります。
ステップ 3	application <i>ap-name</i> 例： apic1(config-tenant)# application ap1	アプリケーションプロファイルを作成するか、アプリケーションプロファイル モードに入ります。
ステップ 4	epg <i>epg-name</i> 例： apic1(config-tenant-app)# epg ep1 <> <A.B.C.D> [scope <scope>]	EPG を作成するか、EPG 設定モードに入ります。
ステップ 5	endpoint <i>ipA.B.C.D/LEN next-hop A.B.C.D</i> [<i>scope scope</i>] 例： apic1(config-tenant-app-epg)# endpoint ip 125.12.1.1/32 next-hop 26.0.14.101	EPG の背後にエンドポイントを作成します。サブネットマスクは /32 で (IPv6 の場合は /128)、1 つの IP アドレスまたは 1 つのエンドポイントをポイントしている必要があります。

例

次の例は、EPG の背後にあるエンドポイントを設定するコマンドを示しています。

```
apic1# config
  apic1(config)# tenant t1
  apic1(config-tenant)# application ap1
  apic1(config-tenant-app)# epg ep1
  apic1(config-tenant-app-epg)# endpoint ip 125.12.1.1/32 next-hop 26.0.14.101
```

NX-OS Style CLI を使用した VRF ごとのデータプレーン IP ラーニングの設定

NX-OS-Style CLI を使用したデータプレーン IP ラーニングの設定

このセクションでは、NX-OS-Style CLI を使用してデータプレーン IP ラーニングを無効にする方法について説明します。

特定の VRF のデータプレーン IP ラーニングを無効にするには：

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# config
```

ステップ 2 特定のテナントのテナント モードに入ります。

例：

```
apic1(config)# tenant name
```

ステップ 3 VRF のコンテキスト モードに入ります。

例：

```
apic1(config-tenant)# vrf context name
```

ステップ 4 VRF のデータプレーン IP ラーニングを無効にします。

例：

```
apic1(config-tenant-vrf)# ipdataplanelearning disabled
```

NX-OS Style CLI を使用した IPv6 ネイバー探索の設定

NX-OS スタイル CLI を使用したブリッジ ドメイン上の IPv6 ネイバー検索によるテナント、VRF、ブリッジ ドメインの設定

ステップ 1 IPv6 ネイバー検索インターフェイス ポリシーを設定し、ブリッジ ドメインに割り当てます。

a) IPv6 ネイバー検索インターフェイス ポリシーを作成します。

例：

```
apic1(config)# tenant ExampleCorp  
apic1(config-tenant)# template ipv6 nd policy NDPol001  
apic1(config-tenant-template-ipv6-nd)# ipv6 nd mtu 1500
```

b) VRF およびブリッジ ドメインを作成します：

例 :

```
apicl(config-tenant)# vrf context pvnl
apicl(config-tenant-vrf)# exit
apicl(config-tenant)# bridge-domain bd1
apicl(config-tenant-bd)# vrf member pvnl
apicl(config-tenant-bd)# exit
```

- c) IPv6 ネイバー探索ポリシーをブリッジ ドメインに割り当てます。

例 :

```
apicl(config-tenant)# interface bridge-domain bd1
apicl(config-tenant-interface)# ipv6 nd policy NDPol001
apicl(config-tenant-interface)#exit
```

ステップ 2 サブネット上で IPV6 ブリッジ ドメイン サブネットおよびネイバー探索プレフィックス ポリシーを作成します。

例 :

```
apicl(config-tenant)# interface bridge-domain bd1
apicl(config-tenant-interface)# ipv6 address 34::1/64
apicl(config-tenant-interface)# ipv6 address 33::1/64
apicl(config-tenant-interface)# ipv6 nd prefix 34::1/64 1000 1000
apicl(config-tenant-interface)# ipv6 nd prefix 33::1/64 4294967295 4294967295
```

NX-OS スタイル CLI を使用したレイヤ 3 インターフェイス上の RA による IPv6 ネイバー探索インターフェイス ポリシーの設定

この例では、IPv6 ネイバー探索インターフェイス ポリシーを設定し、レイヤ 3 インターフェイスに割り当てます。次に、IPv6 レイヤ 3 アウトインターフェイス、ネイバー探索プレフィックス ポリシーを設定し、インターフェイスにネイバー探索ポリシーを関連付けます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure 例 : apicl# configure	コンフィギュレーション モードに入ります。
ステップ 2	tenant tenant_name 例 : apicl(config)# tenant ExampleCorp apicl(config-tenant)#	テナントを作成し、テナントモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	template ipv6 nd policy <i>policy_name</i> 例 : <pre>apic1(config-tenant)# template ipv6 nd policy NDPo1001</pre>	IPv6 ND ポリシーを作成します。
ステップ 4	ipv6 nd mtu <i>mtu value</i> 例 : <pre>apic1(config-tenant-template-ipv6-nd)# ipv6 nd mtu 1500 apic1(config-tenant-template-ipv6)# exit apic1(config-tenant-template)# exit apic1(config-tenant)#</pre>	IPv6 ND ポリシーに MTU 値を割り当てます。
ステップ 5	vrf context <i>VRF_name</i> 例 : <pre>apic1(config-tenant)# vrf context pvn1 apic1(config-tenant-vrf)# exit</pre>	VRF を作成します。
ステップ 6	l3out <i>VRF_name</i> 例 : <pre>apic1(config-tenant)# l3out l3extOut001</pre>	レイヤ 3 アウトを作成します。
ステップ 7	vrf member <i>VRF_name</i> 例 : <pre>apic1(config-tenant-l3out)# vrf member pvn1 apic1(config-tenant-l3out)# exit</pre>	VRF をレイヤ 3 アウトインターフェイスに関連付けます。
ステップ 8	external-l3 epg instp l3out <i>l3extOut001</i> 例 : <pre>apic1(config-tenant)# external-l3 epg instp l3out l3extOut001 apic1(config-tenant-l3ext-epg)# vrf member pvn1 apic1(config-tenant-l3ext-epg)# exit</pre>	レイヤ 3 アウトおよび VRF をレイヤ 3 インターフェイスに割り当てます。
ステップ 9	leaf <i>2011</i> 例 :	リーフ スイッチ モードを開始します。

	コマンドまたはアクション	目的
	<code>apicl(config)# leaf 2011</code>	
ステップ 10	vrf context tenant ExampleCorp vrf pvn1 l3out l3extOut001 例 : <code>apicl(config-leaf)# vrf context tenant ExampleCorp vrf pvn1 l3out l3extOut001</code> <code>apicl(config-leaf-vrf)# exit</code>	VRF をリーフ スイッチに関連付けます。
ステップ 11	int eth 1/1 例 : <code>apicl(config-leaf)# int eth 1/1</code> <code>apicl(config-leaf-if)#</code>	インターフェイス モードに入ります。
ステップ 12	vrf member tenant ExampleCorp vrf pvn1 l3out l3extOut001 例 : <code>apicl(config-leaf-if)# vrf member tenant ExampleCorp vrf pvn1 l3out l3extOut001</code>	インターフェイスで関連付けられているテナント、VRF、レイヤ 3 Out を指定します。
ステップ 13	ipv6 address 2001:20:21:22::2/64 preferred 例 : <code>apicl(config-leaf-if)# ipv6 address 2001:20:21:22::2/64 preferred</code>	プライマリまたは優先 IPv6 アドレスを指定します。
ステップ 14	ipv6 nd prefix 2001:20:21:22::2/64 1000 1000 例 : <code>apicl(config-leaf-if)# ipv6 nd prefix 2001:20:21:22::2/64 1000 1000</code>	レイヤ 3 インターフェイス下で IPv6 ND プレフィックス ポリシーを設定します。
ステップ 15	inherit ipv6 nd NDPol001 例 : <code>apicl(config-leaf-if)# inherit ipv6 nd NDPol001</code> <code>apicl(config-leaf-if)# exit</code> <code>apicl(config-leaf)# exit</code>	レイヤ 3 インターフェイス下で ND ポリシーを設定します。

設定が完了します。

NX-OS Style CLI を使用した Microsoft NLB の設定

NX-OS Style CLI を使用したユニキャストモードでのMicrosoft NLB の設定

このタスクは、ブリッジドメインのすべてのポートに Microsoft NLB がフラッドするように設定します。

始める前に

これらの手順を進める前に次の使用可能な情報を準備してください。

- Microsoft NLB クラスタ VIP
- Microsoft NLB クラスタ MAC アドレス

手順の概要

1. **configure**
2. **tenant** *tenant-name*
3. **application** *app-profile-name*
4. **epg** *epg-name*
5. **[no] endpoint {ip | ipv6} ip-address epnlb mode mode-uc mac mac-address**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure 例： apicl# configure	コンフィギュレーションモードに入ります。
ステップ 2	tenant <i>tenant-name</i> 例： apicl (config)# tenant <i>tenant1</i>	存在しない場合はテナントを作成します。または、テナント コンフィギュレーションモードを開始します。
ステップ 3	application <i>app-profile-name</i> 例： apicl (config-tenant)# application <i>appl</i>	存在しない場合はアプリケーションプロファイルを作成します。または、アプリケーションプロファイル コンフィギュレーションモードを開始します。
ステップ 4	epg <i>epg-name</i> 例： apicl (config-tenant-app)# epg <i>epg1</i>	存在しない場合はEPGを作成します。または、EPG コンフィギュレーションモードを開始します。
ステップ 5	[no] endpoint {ip ipv6} ip-address epnlb mode mode-uc mac mac-address	Microsoft NLB をユニキャストモードで設定します。

	コマンドまたはアクション	目的
	例 : <pre>apic1 (config-tenant-app-epg)# endpoint ip 192.0.2.2/32 eplb mode mode-uc mac 03:BF:01:02:03:04</pre>	<ul style="list-style-type: none"> • <i>ip-address</i> はMicrosoft NLB クラスタ VIP です。 • <i>mac-address</i> は Microsoft NLB クラスタ MAC アドレスです。

NX-OS Style CLI を使用したマルチキャストモードでのMicrosoft NLB の設定

このタスクは、ブリッジドメインの特定のポートでのみ Microsoft NLB がフラッドするように設定します。

始める前に

これらの手順を進める前に次の使用可能な情報を準備してください。

- Microsoft NLB クラスタ VIP
- Microsoft NLB クラスタ MAC アドレス

手順の概要

1. **configure**
2. **tenant** *tenant-name*
3. **application** *app-profile-name*
4. **epg** *epg-name*
5. **[no] endpoint** {**ip** | **ipv6**} *ip-address* **eplb mode mode-mcast--static mac** *mac-address*
6. **[no] nld static-group** *mac-address* **leaf** *leaf-num* **interface** {**ethernet** *slot/port* | **port-channel** *port-channel-name*} **vlan** *portEncapVlan*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure 例 : <pre>apic1# configure</pre>	コンフィギュレーション モードに入ります。
ステップ 2	tenant <i>tenant-name</i> 例 : <pre>apic1 (config)# tenant tenant1</pre>	存在しない場合はテナントを作成します。または、テナント コンフィギュレーション モードを開始します。
ステップ 3	application <i>app-profile-name</i> 例 : <pre>apic1 (config-tenant)# application app1</pre>	存在しない場合はアプリケーションプロファイルを作成します。または、アプリケーションプロファイル コンフィギュレーション モードを開始します。
ステップ 4	epg <i>epg-name</i> 例 :	存在しない場合はEPGを作成します。または、EPG コンフィギュレーション モードを開始します。

NX-OS Style CLI を使用した IGMP モードでの Microsoft NLB の設定

	コマンドまたはアクション	目的
	<code>apicl (config-tenant-app) # epg epg1</code>	
ステップ 5	<p>[no] endpoint {ip ipv6} ip-address eplb mode mode-mcast--static mac mac-address</p> <p>例 :</p> <pre>apicl (config-tenant-app-epg) # endpoint ip 192.0.2.2/32 eplb mode mode-mcast--static mac 03:BF:01:02:03:04</pre>	<p>スタティック マルチキャスト モードで Microsoft NLB を設定します。</p> <ul style="list-style-type: none"> • <i>ip-address</i> は Microsoft NLB クラスタ VIP です。 • <i>mac-address</i> は Microsoft NLB クラスタ MAC アドレスです。
ステップ 6	<p>[no] nld static-group mac-address leaf leaf-num interface {ethernet slot/port port-channel port-channel-name} vlan portEncapVlan</p> <p>例 :</p> <pre>apicl (config-tenant-app-epg) # nld static-group 03:BF:01:02:03:04 leaf 102 interface ethernet 1/12 vlan 19</pre>	<p>Microsoft NLB マルチキャスト VMAC を、Microsoft NLB サーバが接続されている EPG ポートに追加します。</p> <ul style="list-style-type: none"> • <i>mac-address</i> は、入力した Microsoft NLB クラスタの MAC アドレスです。 ステップ 5 (472 ページ) • <i>leaf-num</i> は、追加または削除するインターフェイスを含む リーフ スイッチです。 • <i>port-channel-name</i> は、<i>port-channel</i> オプションを使用する場合のポートチャネルの名前です。 • <i>portEncapVlan</i> は、アプリケーション EPG のスタティック メンバのカプセル化 VLAN です。

NX-OS Style CLI を使用した IGMP モードでの Microsoft NLB の設定

このタスクは、ブリッジドメインの特定のポートでのみ Microsoft NLB がフラッドするように設定します。

始める前に

これらの手順を進める前に次の使用可能な情報を準備してください。

- Microsoft NLB クラスタ VIP
- Microsoft NLB クラスタ MAC アドレス

手順の概要

1. **configure**
2. **tenant** *tenant-name*
3. **application** *app-profile-name*
4. **epg** *epg-name*
5. **[no] endpoint {ip | ipv6} ip-address eplb mode mode-mcast-igmp group multicast-IP-address**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure 例： apic1# configure	コンフィギュレーション モードに入ります。
ステップ 2	tenant tenant-name 例： apic1 (config)# tenant tenant1	存在しない場合はテナントを作成します。または、テナント コンフィギュレーション モードを開始します。
ステップ 3	application app-profile-name 例： apic1 (config-tenant)# application app1	存在しない場合はアプリケーションプロファイルを作成します。または、アプリケーションプロファイル コンフィギュレーション モードを開始します。
ステップ 4	epg epg-name 例： apic1 (config-tenant-app)# epg epg1	存在しない場合は EPG を作成します。または、EPG コンフィギュレーション モードを開始します。
ステップ 5	[no] endpoint {ip ipv6} ip-address eplnb mode mode-mcast-igmp group multicast-IP-address 例： apic1 (config-tenant-app-epg)# endpoint ip 192.0.2.2/32 eplnb mode mode-mcast-igmp group 1.3.5.7	Microsoft NLB を IGMP モードで設定します。 <ul style="list-style-type: none"> • <i>ip-address</i> は Microsoft NLB クラスタ VIP です。 • <i>multicast-IP-address</i> は、NLB エンドポイントグループのマルチキャスト IP です。

NX-OS Style CLI を使用した IGMP スヌーピングの設定

NX-OS スタイル CLI を使用した IGMP スヌーピング ポリシーの設定とブリッジ ドメインへの割り当て

始める前に

- IGMP スヌーピングのポリシーを消費するテナントを作成します。
- IGMP スヌーピング ポリシーを接続するテナントのブリッジ ドメインを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	デフォルト値に基づいてスヌーピングポリシーを作成します。 例：	例の NX-OS スタイル CLI シーケンス： <ul style="list-style-type: none"> • デフォルト値を持つ <code>cookieCut1</code> という名前の IGMP スヌーピング ポリシーを作成します。

	コマンドまたはアクション	目的
	<pre> apicl(config-tenant)# template ip igmp snooping policy cookieCut1 apicl(config-tenant-template-ip-igmp-snooping)# show run all # Command: show running -config all tenant foo template ip igmp snooping policy cookieCut1 # Time: Thu Oct 13 18:26:03 2016 tenant t_10 template ip igmp snooping policy cookieCut1 ip igmp snooping no ip igmp snooping fast-leave ip igmp snooping last-member-query-interval 1 no ip igmp snooping querier ip igmp snooping query-interval 125 ip igmp snooping query-max-response-time 10 ip igmp snooping stqrtup-query-count 2 ip igmp snooping startup-query-interval 31 no description exit exit apicl(config-tenant-template-ip-igmp-snooping)# </pre>	<ul style="list-style-type: none"> • ポリシー cookieCut1 のデフォルト IGMP スヌーピングの値が表示されます。
ステップ 2	<p>必要に応じてスヌーピングポリシーを変更します。</p> <p>例 :</p> <pre> apicl(config-tenant-template-ip-igmp-snooping)# ip igmp snooping query-interval 300 apicl(config-tenant-template-ip-igmp-snooping)# show run all # Command: show running -config all tenant foo template ip igmp snooping policy cookieCut1 #Time: Thu Oct 13 18:26:03 2016 tenant foo template ip igmp snooping policy cookieCut1 ip igmp snooping no ip igmp snooping fast-leave ip igmp snooping last-member-query-interval 1 no ip igmp snooping querier ip igmp snooping query-interval 300 ip igmp snooping query-max-response-time 10 ip igmp snooping stqrtup-query-count 2 ip igmp snooping startup-query-interval 31 no description exit exit apicl(config-tenant-template-ip-igmp-snooping)# exit apicl(config--tenant)# </pre>	<p>例の NX-OS スタイル CLI シーケンス :</p> <ul style="list-style-type: none"> • cookieCut1 という名前の IGMP スヌーピングポリシーのクエリ間隔値のカスタム値を指定します。 • ポリシー cookieCut1 の変更された IGMP スヌーピング値を確認します。
ステップ 3	<p>必要に応じてスヌーピングポリシーを変更します。</p> <p>例 :</p>	<p>例の NX-OS スタイル CLI シーケンス :</p>

	コマンドまたはアクション	目的
	<pre> apic1(config-tenant-template-ip-igmp-snooping)# ip igmp snooping ? <CR> fast-leave Enable IP IGMP Snooping fast leave processing last-member-query-interval Change the IP IGMP snooping last member query interval param querier Enable IP IGMP Snooping querier processing query-interval Change the IP IGMP snooping query interval param query-max-response-time Change the IP IGMP snooping max query response time startup-query-count Change the IP IGMP snooping number of initial queries to send startup-query-interval Change the IP IGMP snooping time for sending initial queries version Change the IP IGMP snooping version param apic1(config-tenant-template-ip-igmp-snooping)# ip igmp snooping version ? v2 version-2 v3 version-3 apic1(config-tenant)# show run # Command: show running-config tenant tenant1 # Time: Mon Jun 1 01:53:53 2020 tenant tenant1 <snipped> interface bridge-domain amit_bd ip address 10.175.31.30/24 secondary ip address 100.175.31.1/32 secondary snooping-querier ip igmp snooping policy igmp_snoop_policy exit template ip igmp snooping policy igmp_snoop_policy ip igmp snooping fast-leave ip igmp snooping last-member-query-interval 2 ip igmp snooping querier v3 ip igmp snooping query-interval 100 ip igmp snooping startup-query-count 5 ip igmp snooping version v3 exit exit </pre>	<ul style="list-style-type: none"> IGMP スヌーピング ポリシーのクエリバージョンのカスタム値を指定します。 ポリシーの変更された IGMP スヌーピングバージョンを確認します。
ステップ 4	<p>ブリッジドメインにポリシーを割り当てます。</p> <p>例 :</p> <pre> apic1(config-tenant)# int bridge-domain bd3 apic1(config-tenant-interface)# ip igmp snooping policy cookieCut1 </pre>	<p>例の NX-OS スタイル CLI シーケンス :</p> <ul style="list-style-type: none"> ブリッジドメインの BD3 に移動します。IGMP スヌーピング ポリシーのクエリ間隔値は cookieCut1 という名前です。 ポリシー cookieCut1 の変更された IGMP スヌーピングの値を持つ IGMP スヌーピングのポリシーを割り当てます。

次のタスク

複数のブリッジ ドメインに IGMP スヌーピングのポリシーを割り当てることができます。

NX-OS スタイル CLI によりスタティック ポートで IGMP スヌーピングおよびマルチキャストの有効化

EPG に静的に割り当てられたポートで IGMP スヌーピングおよびマルチキャストをイネーブルにできます。それらのポートで有効な IGMP スヌーピングおよびマルチキャストトラフィックへのアクセスを許可または拒否するアクセスユーザーのグループを作成および割り当てることができます。

このタスクで説明されている手順には、次のエンティティの事前設定を前提とします。

- テナント : tenant_A
- アプリケーション : application_A
- EPG : epg_A
- ブリッジ ドメイン : bridge_domain_A
- vrf : vrf_A -- a member of bridge_domain_A
- VLAN ドメイン : vd_A (300 ~ 310 の範囲で設定される)

- リーフ スイッチ : 101 およびインターフェイス 1/10

スイッチ 101 のターゲット インターフェイス 1/10 が VLAN 305 に関連付けられており、tenant_A、application_A、epg_A に静的にリンクされています。

- リーフ スイッチ : 101 およびインターフェイス 1/11

スイッチ 101 のターゲット インターフェイス 1/11 が VLAN 309 に関連付けられており、tenant_A、application_A、epg_A に静的にリンクされています。

始める前に

EPG に IGMP スヌーピングおよびマルチキャストを有効にする前に、次のタスクを実行します。

- この機能を有効にして静的に EPG に割り当てるインターフェイスを特定する



(注) スタティック ポートの割り当てに関する詳細は、『Cisco APIC レイヤ 2 ネットワーキング設定ガイド』の「NX-OS スタイル CLI を使用した APIC で特定のポートの EPG を展開する」を参照してください。

- IGMP スヌーピング マルチキャスト トラフィックの受信者の IP アドレスを特定します。

手順

	コマンドまたはアクション	目的
ステップ 1	<p>ターゲットインターフェイスで IGMP スヌーピングおよびレイヤ 2 マルチキャストリングを有効にします</p> <p>例 :</p> <pre> apic1# conf t apic1(config)# tenant tenant_A apic1(config-tenant)# application application_A apic1(config-tenant-app)# epg epg_A apic1(config-tenant-app-epg)# ip igmp snooping static-group 225.1.1.1 leaf 101 interface ethernet 1/10 vlan 305 apic1(config-tenant-app-epg)# end apic1# conf t apic1(config)# tenant tenant_A; application application_A; epg epg_A apic1(config-tenant-app-epg)# ip igmp snooping static-group 227.1.1.1 leaf 101 interface ethernet 1/11 vlan 309 apic1(config-tenant-app-epg)# exit apic1(config-tenant-app)# exit </pre>	<p>例のシーケンスでは次を有効にします。</p> <ul style="list-style-type: none"> 静的にリンクされているターゲットインターフェイス 1/10 の IGMP スヌーピング、そしてマルチキャスト IP アドレス、225.1.1.1 に関連付けます 静的にリンクされているターゲットインターフェイス 1/11 の IGMP スヌーピング、そしてマルチキャスト IP アドレス、227.1.1.1 に関連付けます

NX-OS スタイル CLI を使用した IGMP スヌーピングおよびマルチキャストグループへのアクセスの有効化

EPG に静的に割り当てられたポートで IGMP スヌーピングおよびマルチキャストを有効にした後、それらのポートで有効な IGMP スヌーピングおよびマルチキャストトラフィックへのアクセスを許可または拒否するユーザーのアクセスグループを作成および割り当てできます。

このタスクで説明されている手順には、次のエンティティの事前設定を前提とします。

- テナント : tenant_A
- アプリケーション : application_A
- EPG : epg_A
- ブリッジドメイン : bridge_domain_A
- vrf : vrf_A -- a member of bridge_domain_A
- VLAN ドメイン : vd_A (300 ~ 310 の範囲で設定される)
- リーフスイッチ : 101 およびインターフェイス 1/10
 スイッチ 101 のターゲットインターフェイス 1/10 が VLAN 305 に関連付けられており、tenant_A、application_A、epg_A に静的にリンクされています。
- リーフスイッチ : 101 およびインターフェイス 1/11

スイッチ 101 のターゲット インターフェイス 1/11 が VLAN 309 に関連付けられており、enant_A、application_A、epg_A に静的にリンクされています。



(注) スタティック ポートの割り当てに関する詳細は、『Cisco APIC レイヤ 2 ネットワーキング設定ガイド』の「NX-OS スタイル CLI を使用した APIC で特定のポートの EPG を展開する」を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	<p>route-map 「アクセス グループ」を定義します。</p> <p>例 :</p> <pre>apicl# conf t apicl(config)# tenant tenant_A; application application_A; epg epg_A apicl(config-tenant)# route-map fooBroker permit apicl(config-tenant-rtmap)# match ip multicast group 225.1.1.1/24 apicl(config-tenant-rtmap)# exit apicl(config-tenant)# route-map fooBroker deny apicl(config-tenant-rtmap)# match ip multicast group 227.1.1.1/24 apicl(config-tenant-rtmap)# exit</pre>	<p>例のシーケンスを設定します。</p> <ul style="list-style-type: none"> マルチキャストグループ 225.1.1.1/24 にリンクされる Route-map-access グループ「foobroker」のアクセスが許可されています。 マルチキャストグループ 227.1.1.1/24 にリンクされる Route-map-access グループ「foobroker」のアクセスが拒否されています。
ステップ 2	<p>ルート マップ設定を確認します。</p> <p>例 :</p> <pre>apicl(config-tenant)# show running-config tenant test route-map fooBroker # Command: show running-config tenant test route-map fooBroker # Time: Mon Aug 29 14:34:30 2016 tenant test route-map fooBroker permit 10 match ip multicast group 225.1.1.1/24 exit route-map fooBroker deny 20 match ip multicast group 227.1.1.1/24 exit exit</pre>	
ステップ 3	<p>アクセス グループ接続パスを指定します。</p> <p>例 :</p> <pre>apicl(config-tenant)# application application_A apicl(config-tenant-app)# epg epg_A apicl(config-tenant-app-epg)# ip igmp snooping access-group route-map fooBroker leaf 101 interface ethernet 1/10 vlan 305 apicl(config-tenant-app-epg)# ip igmp snooping access-group route-map newBroker leaf 101 interface ethernet 1/10 vlan 305</pre>	<p>例のシーケンスを設定します。</p> <ul style="list-style-type: none"> リーフ スイッチ 101、インターフェイス 1/10、VLAN 305 で接続されている Route-map-access グループ「foobroker」。 リーフ スイッチ 101、インターフェイス 1/10、VLAN 305 で接続されている Route-map-access グループ「newbroker」。

	コマンドまたはアクション	目的
ステップ 4	<p>アクセスグループ接続を確認します。</p> <p>例 :</p> <pre> apic1(config-tenant-app-epg)# show run # Command: show running-config tenant tenant_A application application_A epg epg_A # Time: Mon Aug 29 14:43:02 2016 tenant tenant_A application application_A epg epg_A bridge-domain member bridge_domain_A ip igmp snooping access-group route-map fooBroker leaf 101 interface ethernet 1/10 vlan 305 ip igmp snooping access-group route-map fooBroker leaf 101 interface ethernet 1/11 vlan 309 ip igmp snooping access-group route-map newBroker leaf 101 interface ethernet 1/10 vlan 305 ip igmp snooping static-group 225.1.1.1 leaf 101 interface ethernet 1/10 vlan 305 ip igmp snooping static-group 225.1.1.1 leaf 101 interface ethernet 1/11 vlan 309 exit exit exit </pre>	

NX-OS Style CLI を使用した MLD スヌーピングの設定

NX-OS Style CLI を使用したブリッジ ドメインに対する MLD スヌーピング ポリシーの設定と割り当て

始める前に

- MLD スヌーピングのポリシーを消費するテナントを作成します。
- MLD スヌーピング ポリシーを接続するテナントのブリッジ ドメインを作成します。

手順の概要

1. **configure terminal**
2. **tenant *tenant-name***
3. **template ipv6 mld snooping policy *policy-name***
4. **[no] ipv6 mld snooping**
5. **[no] ipv6 mld snooping fast-leave**
6. **[no] ipv6 mld snooping querier**
7. **ipv6 mld snooping last-member-query-interval *parameter***
8. **ipv6 mld snooping query-interval *parameter***

9. **ipv6 mld snooping query-max-response-time** *parameter*
10. **ipv6 mld snooping startup-query-count** *parameter*
11. **ipv6 mld snooping startup-query-interval** *parameter*
12. **exit**
13. **interface bridge-domain** *bridge-domain-name*
14. **ipv6 address** *sub-bits/prefix-length snooping-querier*
15. **ipv6 mld snooping policy** *policy-name*
16. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： apic1# configure terminal apic1(config)#	コンフィギュレーション モードに入ります。
ステップ 2	tenant <i>tenant-name</i> 例： apic1(config)# tenant tn1 apic1(config-tenant)#	テナントを作成するか、テナント設定モードに入ります。
ステップ 3	template ipv6 mld snooping policy <i>policy-name</i> 例： apic1(config-tenant)# template ipv6 mld snooping policy mldPolicy1 apic1(config-tenant-template-ip-mld-snooping)#	MLD スヌーピング ポリシーを作成します。例の NX-OS スタイルの CLI シーケンスは、mldPolicy1 という名前の MLD スヌーピング ポリシーを作成します。
ステップ 4	[no] ipv6 mld snooping 例： apic1(config-tenant-template-ip-mld-snooping)# ipv6 mld snooping apic1(config-tenant-template-ip-mld-snooping)# no ipv6 mld snooping	MLD スヌープポリシーの管理状態を有効または無効にします。デフォルトのステートはディセーブルです。
ステップ 5	[no] ipv6 mld snooping fast-leave 例： apic1(config-tenant-template-ip-mld-snooping)# ipv6 mld snooping fast-leave apic1(config-tenant-template-ip-mld-snooping)# no ipv6 mld snooping fast-leave	IPv6 MLD スヌーピングファストリーブ処理を有効または無効にします。
ステップ 6	[no] ipv6 mld snooping querier 例：	IPv6 MLD スヌーピングクエリア処理を有効または無効にします。有効にするクエリア オプションを

	コマンドまたはアクション	目的
	<pre>apicl (config-tenant-template-ip-mld-snooping) # ipv6 mld snooping querier apicl (config-tenant-template-ip-mld-snooping) # no ipv6 mld snooping querier</pre>	<p>割り当て済みのポリシーで効果的に有効にするには、ステップ 14 (482 ページ) で説明されているように、ポリシーを適用するブリッジドメインに割り当てられるサブネットでもクエリア オプションを有効にする必要があります。</p>
ステップ 7	<p>ipv6 mld snooping last-member-query-interval <i>parameter</i></p> <p>例 :</p> <pre>apicl (config-tenant-template-ip-mld-snooping) # ipv6 mld snooping last-member-query-interval 25</pre>	<p>IPv6 MLD スヌーピングの最終メンバークエリー間隔パラメータを変更します。NX-OS スタイルの CLI シーケンスの例では、IPv6 MLD スヌーピングの最後のメンバーのクエリー間隔パラメータが 25 秒に変更されます。有効なオプションは 1 ~ 25 です。デフォルト値は 1 秒です。</p>
ステップ 8	<p>ipv6 mld snooping query-interval <i>parameter</i></p> <p>例 :</p> <pre>apicl (config-tenant-template-ip-mld-snooping) # ipv6 mld snooping query-interval 300</pre>	<p>IPv6 MLD スヌーピングクエリー間隔パラメータを変更します。NX-OS スタイルの CLI シーケンス例では、IPv6 MLD スヌーピングクエリー間隔パラメータを 300 秒に変更します。有効なオプションは 1 ~ 18000 です。デフォルト値は 125 秒です。</p>
ステップ 9	<p>ipv6 mld snooping query-max-response-time <i>parameter</i></p> <p>例 :</p> <pre>apicl (config-tenant-template-ip-mld-snooping) # ipv6 mld snooping query-max-response-time 25</pre>	<p>IPv6 MLD スヌーピングの最大クエリー応答時間を変更します。NX-OS スタイルの CLI シーケンスの例では、IPv6 MLD スヌーピングの最大クエリー応答時間が 25 秒に変更されます。有効なオプションは 1 ~ 25 です。デフォルトは 10 秒です。</p>
ステップ 10	<p>ipv6 mld snooping startup-query-count <i>parameter</i></p> <p>例 :</p> <pre>apicl (config-tenant-template-ip-mld-snooping) # ipv6 mld snooping startup-query-count 10</pre>	<p>送信する初期クエリーの IPv6 MLD スヌーピング数を変更します。NX-OS スタイルの CLI シーケンスの例では、最初のクエリーの IPv6 MLD スヌーピング数を 10 に変更します。有効なオプションは 1 ~ 10 です。デフォルトは 2 です。</p>
ステップ 11	<p>ipv6 mld snooping startup-query-interval <i>parameter</i></p> <p>例 :</p> <pre>apicl (config-tenant-template-ip-mld-snooping) # ipv6 mld snooping startup-query-interval 300</pre>	<p>初期クエリーを送信するための IPv6 MLD スヌーピング時間を変更します。NX-OS スタイルの CLI シーケンスの例では、最初のクエリーを送信するための IPv6 MLD スヌーピング時間が 300 秒に変更されます。有効なオプションは 1 ~ 18000 です。デフォルト値は 31 秒です。</p>
ステップ 12	<p>exit</p> <p>例 :</p> <pre>apicl (config-tenant-template-ip-mld-snooping) # exit apicl (config-tenant) #</pre>	<p>設定モードに戻ります。</p>

NX-OS Style CLI を使用した IP マルチキャストの設定

	コマンドまたはアクション	目的
ステップ 13	interface bridge-domain <i>bridge-domain-name</i> 例 : <pre>apic1(config-tenant)# interface bridge-domain bd1 apic1(config-tenant-interface)#</pre>	インターフェイスブリッジドメインを設定します。例の NX-OS スタイルの CLI シーケンスは、bd1 という名前のインターフェイスブリッジドメインを設定します。
ステップ 14	ipv6 address <i>sub-bits/prefix-length</i> snooping-querier 例 : <pre>apic1(config-tenant-interface)# ipv6 address 2000::5/64 snooping-querier</pre>	ブリッジドメインをスイッチクエリアとして設定します。これにより、ポリシーが適用されるブリッジドメインに割り当てられたサブネットワークでクエリアオプションが有効になります。
ステップ 15	ipv6 mld snooping policy <i>policy-name</i> 例 : <pre>apic1(config-tenant-interface)# ipv6 mld snooping policy mldPolicy1</pre>	ブリッジドメインを MLD スヌーピングポリシーに関連付けます。例の NX-OS スタイルの CLI シーケンスは、mldPolicy1 という名前の MLD スヌーピングポリシーにブリッジドメインに関連付けます。
ステップ 16	exit 例 : <pre>apic1(config-tenant-interface)# exit apic1(config-tenant)#</pre>	設定モードに戻ります。

NX-OS Style CLI を使用した IP マルチキャストの設定

NX-OS スタイルの CLI を使用したレイヤ 3 マルチキャストの設定

ステップ 1 コンフィギュレーションモードを開始します。

例 :

```
apic1# configure
```

ステップ 2 テナントの設定モード、VRF の設定モードは、および PIM オプションの設定モードに入ります。

例 :

```
apic1(config)# tenant tenant1
apic1(config-tenant)# vrf context tenant1_vrf
apic1(config-tenant-vrf)# ip pim
apic1(config-tenant-vrf)# ip pim fast-convergence
apic1(config-tenant-vrf)# ip pim bsr forward
```

ステップ 3 IGMP を設定し、VRF に適切な IGMP オプションを設定します。

例 :


```
apicl(config-tenant-vrf)# ip igmp
apicl(config-tenant-vrf)# exit
apicl(config-tenant)# interface bridge-domain tenant1_bd
apicl(config-tenant-interface)# ip multicast
apicl(config-tenant-interface)# ip igmp allow-v3-asm
apicl(config-tenant-interface)# ip igmp fast-leave
apicl(config-tenant-interface)# ip igmp inherit interface-policy igmp_intpoll1
apicl(config-tenant-interface)# exit
```

ステップ4 テナントの L3 Out モードに入り、PIM を有効にし、リーフ インターフェイス モードに入ります。このインターフェイスの PIM を設定します。

例 :

```
apicl(config-tenant)# l3out tenant1_l3out
apicl(config-tenant-l3out)# ip pim
apicl(config-tenant-l3out)# exit
apicl(config-tenant)# exit
apicl(config)#
apicl(config)# leaf 101
apicl(config-leaf)# interface ethernet 1/125
apicl(config-leaf-if) ip pim inherit interface-policy pim_intpoll1
```

ステップ5 IGMP コマンドを使用して、インターフェイスの IGMP を設定します。

例 :

```
apicl(config-leaf-if)# ip igmp fast-leave
apicl(config-leaf-if)# ip igmp inherit interface-policy igmp_intpoll1
apicl(config-leaf-if)# exit
apicl(config-leaf)# exit
```

ステップ6 ファブリック RP を設定します。

例 :

```
apicl(config)# tenant tenant1
apicl(config-tenant)# vrf context tenant1_vrf
apicl(config-tenant-vrf)# ip pim fabric-rp-address 20.1.15.1 route-map intervrf-ctx2
apicl(config-tenant-vrf)# ip pim fabric-rp-address 20.1.15.2 route-map intervrf-ctx1
apicl(config-tenant-vrf)# exit
```

ステップ7 Inter-VRF マルチキャストを設定します。

例 :

```
apicl(config-tenant)# vrf context tenant1_vrf
apicl(config-tenant-vrf)# ip pim inter-vrf-src ctx2 route-map intervrf-ctx2
apicl(config-tenant-vrf)# route-map intervrf-ctx2 permit 1
apicl(config-tenant-vrf)# match ip multicast group 226.20.0.0/24
apicl(config-tenant-vrf)# exit
apicl(config-tenant)# exit
apicl(config)#
```

これにより、APIC のレイヤ3 マルチキャストの設定を完了します。

NX-OS Style CLI を使用したレイヤ 3 IPv6 の設定

始める前に

- 目的の VRF、ブリッジドメイン、IPv6 アドレスを持つレイヤ 3 Out インターフェイスは、PIM6 が有効になるように設定する必要があります。レイヤ 3 Out の場合、IPv6 マルチキャストが機能するために、論理ノードプロファイルのノードに IPv6 ループバック アドレスが設定されます。
- 基本的なユニキャスト ネットワークを設定する必要があります。

ステップ 1 VRF で PIM6 を有効にし、ランデブー ポイント (RP) を設定します。

例 :

```
apic1(config)# tenant tenant1
apic1(config-tenant)# vrf context tenant1_vrf
apic1(config-tenant-vrf)# ipv6 pim
apic1(config-tenant-vrf)# ipv6 rp-address 2018::100:100:100:100 route-map ipv6_pim_routemap
```

ステップ 2 PIM6 インターフェイス ポリシーを設定し、レイヤ 3 Out に適用します。

例 :

```
apic1(config-tenant)# l3out tenant1_l3out
apic1(config-tenant-l3out)# ipv6 pim
apic1(config-tenant-l3out)# exit
apic1(config-tenant)# exit
apic1(config)#
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/125
apic1(config-leaf-if) ipv6 pim inherit interface-policy pim6_intpoll1
```

ステップ 3 BD で PIM6 を有効にします。

例 :

```
apic1(config-tenant)# interface bridge-domain tenant1_bd
apic1(config-tenant-interface)# ipv6 multicast
apic1(config-tenant)# exit
apic1(config)#
```

PIM6 を使用したレイヤ 3 IPv6 マルチキャストが有効になります。

NX-OS スタイルの CLI を使用したマルチキャスト フィルタリングの構成

ブリッジドメイン レベルでマルチキャスト フィルタリングを設定します。このトピックの手順を使用して、ブリッジドメイン レベルで送信元フィルタリングまたは受信者フィルタリング、あるいはその両方を設定します。

始める前に

- マルチキャストフィルタリングを設定するブリッジドメインはすでに作成されています。
- ブリッジドメインは PIM 対応ブリッジドメインです。
- レイヤ 3 マルチキャストは VRF レベルで有効になります。

ステップ 1 コンフィギュレーション モードを開始します。

```
apicl# configure
apicl(config)#
```

ステップ 2 テナントにアクセスし、PIM を有効にします。

```
apicl(config)# tenant tenant-name
apicl(config-tenant)# vrf context VRF-name
apicl(config-tenant-vrf)# ip pim
apicl(config-tenant-vrf)# exit
apicl(config-tenant)#
```

例 :

```
apicl(config)# tenant t1
apicl(config-tenant)# vrf context v1
apicl(config-tenant-vrf)# ip pim
apicl(config-tenant-vrf)# exit
apicl(config-tenant)#
```

ステップ 3 マルチキャストフィルタリングを構成するブリッジドメインにアクセスします。

```
apicl(config-tenant)# bridge-domain BD-name
apicl(config-tenant-bd)#
```

例 :

```
apicl(config-tenant)# bridge-domain bd1
apicl(config-tenant-bd)#
```

ステップ 4 マルチキャスト [送信元] または [受信者] のフィルタリングを有効にするかどうかを決定します。

(注) 送信元フィルタリングと受信先フィルタリングの両方を同じブリッジドメインで有効にできません。

- このブリッジドメインでマルチキャスト送信元フィルタリングを有効にする場合は、次の例のように入力します。

```
apicl(config-tenant-bd)# src-filter source-route-map-policy
```

次に例を示します。

```
apic1(config-tenant-bd) # src-filter routemap-Mcast-src
```

- このブリッジドメインでマルチキャスト送信元フィルタリングを有効にする場合は、次の例のように入力します。

```
apic1(config-tenant-bd) # dst-filter destination-route-map-policy
```

次に例を示します。

```
apic1(config-tenant-bd) # dst-filter routemap-Mcast-dst
```

ステップ 5 IPv4 のマルチキャストを有効にします。

```
apic1(config-tenant-bd) # mcast-allow
apic1(config-tenant-bd) #
```

ステップ 6 VRF にブリッジドメインを関連付けます。

```
apic1(config-tenant-bd) # vrf member VRF-name
apic1(config-tenant-bd) # exit
apic1(config-tenant) #
```

例：

```
apic1(config-tenant-bd) # vrf member v1
apic1(config-tenant-bd) # exit
apic1(config-tenant) #
```

ステップ 7 ブリッジドメインでマルチキャストを有効にします。

```
apic1(config-tenant) # interface bridge-domain BD-name
apic1(config-tenant-interface) # ip multicast
apic1(config-tenant-interface) # exit
apic1(config-tenant) #
```

例：

```
apic1(config-tenant) # interface bridge-domain bd1
apic1(config-tenant-interface) # ip multicast
apic1(config-tenant-interface) # exit
apic1(config-tenant) #
```

ステップ 8 ルートマップを設定します。

```
apic1(config-tenant) # route-map destination-route-map-policy <permit/deny> sequence_number
apic1(config-tenant-rtmap) # match ip multicast <source/group> IP_address_subnet <source/group>
IP_address_subnet
apic1(config-tenant-rtmap) # exit
apic1(config-tenant) # exit
```

```
apicl(config)#
```

例 :

```
apicl(config-tenant)# route-map routemap-Mcast-src permit 1
apicl(config-tenant-rtmap)# match ip multicast source 10.10.1.1/24 group 192.1.1.1/32
apicl(config-tenant-rtmap)# exit
apicl(config-tenant)# route-map routemap-Mcast-dst permit 1
apicl(config-tenant-rtmap)# match ip multicast group 192.2.2.2/32
apicl(config-tenant-rtmap)# exit
apicl(config-tenant)# exit
apicl(config)#
```

NX-OS Style CLI を使用したマルチポッドの設定

NX-OS CLI を使用したマルチポッド ファブリックのセットアップ

始める前に

- ノードグループポリシーと L3Out ポリシーがすでに作成されています。

ステップ 1 次の例に示すように、マルチポッドを設定します。

例 :

```
ifav4-ifc1# show run system
# Command: show running-config system
# Time: Mon Aug 1 21:32:03 2016
system cluster-size 3
system switch-id FOX2016G9DW 204 ifav4-spine4 pod 2
system switch-id SAL1748H56D 201 ifav4-spine1 pod 1
system switch-id SAL1803L25H 102 ifav4-leaf2 pod 1
system switch-id SAL1819RXP4 101 ifav4-leaf1 pod 1
system switch-id SAL1931LA3B 203 ifav4-spine2 pod 2
system switch-id SAL1934MNY0 103 ifav4-leaf3 pod 1
system switch-id SAL1934MNY3 104 ifav4-leaf4 pod 1
system switch-id SAL1938P7A6 202 ifav4-spine3 pod 1
system switch-id SAL1938PHBB 105 ifav4-leaf5 pod 2
system switch-id SAL1942R857 106 ifav4-leaf6 pod 2
system pod 1 tep-pool 10.0.0.0/16
system pod 2 tep-pool 10.1.0.0/16
ifav4-ifc1#
```

ステップ 2 次の例のよ、VLAN ドメインを設定します。

例 :

```
ifav4-ifc1# show running-config vlan-domain l3Dom
# Command: show running-config vlan-domain l3Dom
# Time: Mon Aug 1 21:32:31 2016
vlan-domain l3Dom
vlan 4
```

```
exit
ifav4-ifc1#
```

ステップ 3 次の例のよ、ファブリックの外部接続を設定します。

例 :

```
ifav4-ifc1# show running-config fabric-external
# Command: show running-config fabric-external
# Time: Mon Aug 1 21:34:17 2016
fabric-external 1
  bgp evpn peering
  pod 1
    interpod data hardware-proxy 100.11.1.1/32
    bgp evpn peering
    exit
  pod 2
    interpod data hardware-proxy 200.11.1.1/32
    bgp evpn peering
    exit
  route-map interpod-import
    ip prefix-list default permit 0.0.0.0/0
    exit
  route-target extended 5:16
  exit
ifav4-ifc1#
```

ステップ 4 スパイン スイッチ インターフェイスと次の例のよの OSPF 設定を構成します。

例 :

```
# Command: show running-config spine
# Time: Mon Aug 1 21:34:41 2016
spine 201
  vrf context tenant infra vrf overlay-1
    router-id 201.201.201.201
    exit
  interface ethernet 1/1
    vlan-domain member l3Dom
    exit
  interface ethernet 1/1.4
    vrf member tenant infra vrf overlay-1
    ip address 201.1.1.1/30
    ip router ospf default area 1.1.1.1
    ip ospf cost 1
    exit
  interface ethernet 1/2
    vlan-domain member l3Dom
    exit
  interface ethernet 1/2.4
    vrf member tenant infra vrf overlay-1
    ip address 201.2.1.1/30
    ip router ospf default area 1.1.1.1
    ip ospf cost 1
    exit
  router ospf default
    vrf member tenant infra vrf overlay-1
    area 1.1.1.1 loopback 201.201.201.201
    area 1.1.1.1 interpod peering
    exit
  exit
exit
spine 202
  vrf context tenant infra vrf overlay-1
    router-id 202.202.202.202
```

```
    exit
interface ethernet 1/2
  vlan-domain member l3Dom
  exit
interface ethernet 1/2.4
  vrf member tenant infra vrf overlay-1
  ip address 202.1.1.1/30
  ip router ospf default area 1.1.1.1
  exit
router ospf default
  vrf member tenant infra vrf overlay-1
  area 1.1.1.1 loopback 202.202.202.202
  area 1.1.1.1 interpod peering
  exit
  exit
exit
spine 203
  vrf context tenant infra vrf overlay-1
  router-id 203.203.203.203
  exit
interface ethernet 1/1
  vlan-domain member l3Dom
  exit
interface ethernet 1/1.4
  vrf member tenant infra vrf overlay-1
  ip address 203.1.1.1/30
  ip router ospf default area 0.0.0.0
  ip ospf cost 1
  exit
interface ethernet 1/2
  vlan-domain member l3Dom
  exit
interface ethernet 1/2.4
  vrf member tenant infra vrf overlay-1
  ip address 203.2.1.1/30
  ip router ospf default area 0.0.0.0
  ip ospf cost 1
  exit
router ospf default
  vrf member tenant infra vrf overlay-1
  area 0.0.0.0 loopback 203.203.203.203
  area 0.0.0.0 interpod peering
  exit
  exit
exit
spine 204
  vrf context tenant infra vrf overlay-1
  router-id 204.204.204.204
  exit
interface ethernet 1/31
  vlan-domain member l3Dom
  exit
interface ethernet 1/31.4
  vrf member tenant infra vrf overlay-1
  ip address 204.1.1.1/30
  ip router ospf default area 0.0.0.0
  ip ospf cost 1
  exit
router ospf default
  vrf member tenant infra vrf overlay-1
  area 0.0.0.0 loopback 204.204.204.204
  area 0.0.0.0 interpod peering
  exit
  exit
exit
```

```
exit
ifav4-ifc1#
```

NX-OS Style CLI を使用したリモート リーフ スイッチの設定

NX-OS スタイル CLI を使用したリモート リーフ スイッチの設定

この例では、リーフ スイッチがメインのファブリック ポッドと通信できるようにするため、スパイン スイッチとリモート リーフ スイッチを設定しています。

始める前に

- IPN ルータとリモート リーフ スイッチはアクティブで設定されています。 [WAN ルータとリモート リーフ スイッチ設定の注意事項 \(144 ページ\)](#) を参照してください。
- リモート リーフ スイッチは、13.1.x 以降 (aci n9000 dk9.13.1.x.x.bin) のスイッチ イメージを実行しています。
- リモート リーフ スイッチを追加する予定のポッドが作成され、設定されています。

ステップ 1 ポッド 2 のリモート ロケーション 5 で TEP プールを定義します。

ネットワーク マスクは /24 以下である必要があります。

次の新しいコマンドを使用します : **system remote-leaf-site site-id pod pod-id tep-pool ip-address-and-netmask**

例 :

```
apic1(config)# system remote-leaf-site 5 pod 2 tep-pool 192.0.0.0/16
```

ステップ 2 ポッド 2 の、リモート リーフ サイト 5 にリモート リーフ スイッチを追加します。

次のコマンドを使用します : **system switch-id serial-number node-id leaf-switch-namepod pod-id remote-leaf-site remote-leaf-site-id node-type remote-leaf-wan**

例 :

```
apic1(config)# system switch-id FDO210805SKD 109 ifav4-leaf9 pod 2
remote-leaf-site 5 node-type remote-leaf-wan
```

ステップ 3 VLAN 4 を含む VLAN で VLAN ドメインを設定します。

例 :

```
apic1(config)# vlan-domain ospfDom
apic1(config-vlan)# vlan 4-5
apic1(config-vlan)# exit
```

ステップ 4 インフラ テナントに 2 つの L3Out を設定します。1 つはリモート リーフ 接続のためで、もう 1 つはマルチポッド IPN のためです。

例 :


```
apicl(config)# tenant infra
apicl(config-tenant)# l3out rl-wan
apicl(config-tenant-l3out)# vrf member overlay-1
apicl(config-tenant-l3out)# exit
apicl(config-tenant)# l3out ipn-multipodInternal
apicl(config-tenant-l3out)# vrf member overlay-1
apicl(config-tenant-l3out)# exit
apicl(config-tenant)# exit
apicl(config)#
```

ステップ 5 L3Out が使用する、スパイン スイッチ インターフェイスとサブインターフェイスを設定します。

例 :

```
apicl(config)# spine 201
apicl(config-spine)# vrf context tenant infra vrf overlay-1 l3out rl-wan-test
apicl(config-spine-vrf)# exit
apicl(config-spine)# vrf context tenant infra vrf overlay-1 l3out ipn-multipodInternal
apicl(config-spine-vrf)# exit
apicl(config-spine)#
apicl(config-spine)# interface ethernet 8/36
apicl(config-spine-if)# vlan-domain member ospfDom
apicl(config-spine-if)# exit
apicl(config-spine)# router ospf default
apicl(config-spine-ospf)# vrf member tenant infra vrf overlay-1
apicl(config-spine-ospf-vrf)# area 5 l3out rl-wan-test
apicl(config-spine-ospf-vrf)# exit
apicl(config-spine-ospf)# exit
apicl(config-spine)#
apicl(config-spine)# interface ethernet 8/36.4
apicl(config-spine-if)# vrf member tenant infra vrf overlay-1 l3out rl-wan-test
apicl(config-spine-if)# ip router ospf default area 5
apicl(config-spine-if)# exit
apicl(config-spine)# router ospf multipod-internal
apicl(config-spine-ospf)# vrf member tenant infra vrf overlay-1
apicl(config-spine-ospf-vrf)# area 5 l3out ipn-multipodInternal
apicl(config-spine-ospf-vrf)# exit
apicl(config-spine-ospf)# exit
apicl(config-spine)#
apicl(config-spine)# interface ethernet 8/36.5
apicl(config-spine-if)# vrf member tenant infra vrf overlay-1 l3out ipn-multipodInternal
apicl(config-spine-if)# ip router ospf multipod-internal area 5
apicl(config-spine-if)# exit
apicl(config-spine)# exit
apicl(config)#
```

ステップ 6 メインのファブリック ポッドと通信するために使用するリモートのリーフ スイッチ インターフェイスとサブインターフェイスを設定します。

例 :

```
(config)# leaf 101
apicl(config-leaf)# vrf context tenant infra vrf overlay-1 l3out rl-wan-test
apicl(config-leaf-vrf)# exit
apicl(config-leaf)#
apicl(config-leaf)# interface ethernet 1/49
apicl(config-leaf-if)# vlan-domain member ospfDom
apicl(config-leaf-if)# exit
apicl(config-leaf)# router ospf default
apicl(config-leaf-ospf)# vrf member tenant infra vrf overlay-1
apicl(config-leaf-ospf-vrf)# area 5 l3out rl-wan-test
apicl(config-leaf-ospf-vrf)# exit
```

```

apic1(config-leaf-ospf)# exit
apic1(config-leaf)#
apic1(config-leaf)# interface ethernet 1/49.4
apic1(config-leaf-if)# vrf member tenant infra vrf overlay-1 l3out rl-wan-test
apic1(config-leaf-if)# ip router ospf default area 5
apic1(config-leaf-if)# exit

```

例

次の例は、ダウンロード可能な設定を示しています:

```

apic1# configure
apic1(config)# system remote-leaf-site 5 pod 2 tep-pool 192.0.0.0/16
apic1(config)# system switch-id FDO210805SKD 109 ifav4-leaf9 pod 2
remote-leaf-site 5 node-type remote-leaf-wan
apic1(config)# vlan-domain ospfDom
apic1(config-vlan)# vlan 4-5
apic1(config-vlan)# exit
apic1(config)# tenant infra
apic1(config-tenant)# l3out rl-wan-test
apic1(config-tenant-l3out)# vrf member overlay-1
apic1(config-tenant-l3out)# exit
apic1(config-tenant)# l3out ipn-multipodInternal
apic1(config-tenant-l3out)# vrf member overlay-1
apic1(config-tenant-l3out)# exit
apic1(config-tenant)# exit
apic1(config)#
apic1(config)# spine 201
apic1(config-spine)# vrf context tenant infra vrf overlay-1 l3out rl-wan-test
apic1(config-spine-vrf)# exit
apic1(config-spine)# vrf context tenant infra vrf overlay-1 l3out ipn-multipodInternal
apic1(config-spine-vrf)# exit
apic1(config-spine)#
apic1(config-spine)# interface ethernet 8/36
apic1(config-spine-if)# vlan-domain member ospfDom
apic1(config-spine-if)# exit
apic1(config-spine)# router ospf default
apic1(config-spine-ospf)# vrf member tenant infra vrf overlay-1
apic1(config-spine-ospf-vrf)# area 5 l3out rl-wan-test
apic1(config-spine-ospf-vrf)# exit
apic1(config-spine-ospf)# exit
apic1(config-spine)#
apic1(config-spine)# interface ethernet 8/36.4
apic1(config-spine-if)# vrf member tenant infra vrf overlay-1 l3out rl-wan-test
apic1(config-spine-if)# ip router ospf default area 5
apic1(config-spine-if)# exit
apic1(config-spine)# router ospf multipod-internal
apic1(config-spine-ospf)# vrf member tenant infra vrf overlay-1
apic1(config-spine-ospf-vrf)# area 5 l3out ipn-multipodInternal
apic1(config-spine-ospf-vrf)# exit
apic1(config-spine-ospf)# exit
apic1(config-spine)#
apic1(config-spine)# interface ethernet 8/36.5
apic1(config-spine-if)# vrf member tenant infra vrf overlay-1 l3out ipn-multipodInternal
apic1(config-spine-if)# ip router ospf multipod-internal area 5
apic1(config-spine-if)# exit
apic1(config-spine)# exit
apic1(config)#
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant infra vrf overlay-1 l3out rl-wan-test

```

```
apicl(config-leaf-vrf)# exit
apicl(config-leaf)#
apicl(config-leaf)# interface ethernet 1/49
apicl(config-leaf-if)# vlan-domain member ospfDom
apicl(config-leaf-if)# exit
apicl(config-leaf)# router ospf default
apicl(config-leaf-ospf)# vrf member tenant infra vrf overlay-1
apicl(config-leaf-ospf-vrf)# area 5 l3out rl-wan-test
apicl(config-leaf-ospf-vrf)# exit
apicl(config-leaf-ospf)# exit
apicl(config-leaf)#
apicl(config-leaf)# interface ethernet 1/49.4
apicl(config-leaf-if)# vrf member tenant infra vrf overlay-1 l3out rl-wan-test
apicl(config-leaf-if)# ip router ospf default area 5
apicl(config-leaf-if)# exit
```

パートII：外部ルーティング（L3Out）の設定

外部ネットワークへのルーテッド接続

NX-OS Style CLI を使用した MP-BGP ルート リフレクタの設定

ACI ファブリックの MP-BGP ルート リフレクタの設定

ACI ファブリック内のルートを配布するために、MP-BGP プロセスを最初に実行し、スパインスイッチを BGP ルート リフレクタとして設定する必要があります。

次に、MP-BGP ルート リフレクタの設定例を示します。



(注) この例では、BGP ファブリック ASN は 100 です。スパインスイッチ 104 と 105 が MP-BGP ルート リフレクタとして選択されます。

```
apicl(config)# bgp-fabric
apicl(config-bgp-fabric)# asn 100
apicl(config-bgp-fabric)# route-reflector spine 104,105
```

L3Out のノードとインターフェイス

NX-OS Style CLI を使用したレイヤ 3 ルーテッド ポート チャネルとサブインターフェイス ポート チャネルの設定

ポート チャネルの NX-OS は、CLI を使用してをルーテッド レイヤ 3 の設定

この手順では、レイヤ 3 ルーテッドポート チャネルを設定します。

手順の概要

1. **configure**
2. **leaf** *node-id*
3. **interface port-channel** *channel-name*
4. **no switchport**
5. **vrf member** *vrf-name* **tenant** *tenant-name*
6. **vlan-domain member** *vlan-domain-name*
7. **ip address** *ip-address/subnet-mask*
8. **ipv6 address** *sub-bits/prefix-length* **preferred**
9. **ipv6 link-local** *ipv6-link-local-address*
10. **mac-address** *mac-address*
11. **mtu** *mtu-value*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure 例： apic1# configure	グローバル コンフィギュレーション モードを開始します。
ステップ 2	leaf <i>node-id</i> 例： apic1(config)# leaf 101	リーフ スイッチまたはリーフ スイッチの設定を指定します。 <i>Node-id</i> は形式 <i>node-id1-node-id2</i> の単一ノード ID または ID の範囲となる可能性があり、設定が適用されます。
ステップ 3	interface port-channel <i>channel-name</i> 例： apic1(config-leaf)# interface port-channel po1	指定したポート チャネルのインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	no switchport 例： apic1(config-leaf-if)# no switchport	レイヤ 3 インターフェイスを可能になります。
ステップ 5	vrf member <i>vrf-name</i> tenant <i>tenant-name</i> 例： apic1(config-leaf-if)# vrf member v1 tenant t1	この仮想ルーティングおよび転送 (VRF) インスタンスと L3 ポリシー、外部には、このポートチャネルを関連付けます場所。 <ul style="list-style-type: none"> • <i>Vrf-name</i> は VRF 名です。32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。 • テナント名 は、テナント名です。32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。

	コマンドまたはアクション	目的
ステップ 6	vlan-domain member <i>vlan-domain-name</i> 例： apicl(config-leaf-if)# vlan-domain member dom1	以前に設定された VLAN ドメインには、ポートチャンネルのテンプレートを関連付けます。
ステップ 7	ip address <i>ip-address/subnet-mask</i> 例： apicl(config-leaf-if)# ip address 10.1.1.1/24	指定したインターフェイスの IP アドレスとサブネットマスクを設定します。
ステップ 8	ipv6 address <i>sub-bits/prefix-length preferred</i> 例： apicl(config-leaf-if)# ipv6 address 2001::1/64 preferred	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。場所： <ul style="list-style-type: none">• <i>sub-bits</i> 引数は、<i>prefix-name</i> 引数で指定された一般的なプレフィックスによって提供されるプレフィックスに連結する、アドレスのサブプレフィックス ビットおよびホストビットです。<i>sub-bits</i> 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。• <i>Prefix-length</i> は IPv6 プレフィックスの長さです。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
ステップ 9	ipv6 link-local <i>ipv6-link-local-address</i> 例： apicl(config-leaf-if)# ipv6 link-local fe80::1	インターフェイスに IPv6 リンクローカルアドレスを設定します。
ステップ 10	mac-address <i>mac-address</i> 例： apicl(config-leaf-if)# mac-address 00:44:55:66:55::01	インターフェイス MAC アドレスを手動で設定します。
ステップ 11	mtu <i>mtu-value</i> 例： apicl(config-leaf-if)# mtu 1500	このサービス クラスの MTU を設定します

例

この例では、基本レイヤ 3 ポート チャンネルを設定する方法を示します。

NX-OS CLI を使用したレイヤ3 サブインターフェイス ポート チャンネルの設定

```

apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface port-channel po1
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member v1 tenant t1
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# ip address 10.1.1.1/24
apic1(config-leaf-if)# ipv6 address 2001::1/64 preferred
apic1(config-leaf-if)# ipv6 link-local fe80::1
apic1(config-leaf-if)# mac-address 00:44:55:66:55::01
apic1(config-leaf-if)# mtu 1500

```

NX-OS CLI を使用したレイヤ3 サブインターフェイス ポート チャンネルの設定

この手順では、レイヤ3 サブインターフェイス ポート チャンネルを設定します。

手順の概要

1. **configure**
2. **leaf** *node-id*
3. **vrf member** *vrf-name* **tenant** *tenant-name*
4. **vlan-domain member** *vlan-domain-name*
5. **ip address** *ip-address* / *subnet-mask*
6. **ipv6 address** *sub-bits* / *prefix-length* **preferred**
7. **ipv6 link-local** *ipv6-link-local-address*
8. **mac-address** *mac-address*
9. **mtu** *mtu-value*
10. **exit**
11. **interface port-channel** *channel-name*
12. **vlan-domain member** *vlan-domain-name*
13. **exit**
14. **interface port-channel** *channel-name.number*
15. **vrf member** *vrf-name* **tenant** *tenant-name*
16. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure 例： apic1# configure	グローバル コンフィギュレーション モードを開始します。
ステップ 2	leaf <i>node-id</i> 例： apic1(config)# leaf 101	リーフ スイッチまたはリーフ スイッチの設定を指定します。 <i>Node-id</i> は形式 <i>node-id1-node-id2</i> の単一ノード ID または ID の範囲となる可能性があり、設定が適用されます。

	コマンドまたはアクション	目的
ステップ 3	vrf member vrf-name tenant tenant-name 例 : <pre>apicl(config-leaf-if)# vrf member v1 tenant t1</pre>	この仮想ルーティングおよび転送 (VRF) インスタンスと L3 アウトサイドポリシーにポート チャンネルを関連付けます。場所 : <ul style="list-style-type: none"> • <i>Vrf-name</i> は VRF 名です。32 文字以内の英数字のストリング (大文字と小文字を区別) で指定します。 • テナント名 は、テナント名です。32 文字以内の英数字のストリング (大文字と小文字を区別) で指定します。
ステップ 4	vlan-domain member vlan-domain-name 例 : <pre>apicl(config-leaf-if)# vlan-domain member dom1</pre>	以前に設定された VLAN ドメインには、ポートチャンネルのテンプレートを関連付けます。
ステップ 5	ip address ip-address / subnet-mask 例 : <pre>apicl(config-leaf-if)# ip address 10.1.1.1/24</pre>	指定したインターフェイスの IP アドレスとサブネット マスクを設定します。
ステップ 6	ipv6 address sub-bits / prefix-length preferred 例 : <pre>apicl(config-leaf-if)# ipv6 address 2001::1/64 preferred</pre>	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。場所 : <ul style="list-style-type: none"> • <i>sub-bits</i> 引数は、<i>prefix-name</i> 引数で指定された一般的なプレフィックスによって提供されるプレフィックスに連結する、アドレスのサブプレフィックス ビットおよびホスト ビットです。<i>sub-bits</i> 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。 • <i>Prefix-length</i> は IPv6 プレフィックスの長さです。プレフィックス (アドレスのネットワーク部分) を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
ステップ 7	ipv6 link-local ipv6-link-local-address 例 : <pre>apicl(config-leaf-if)# ipv6 link-local fe80::1</pre>	インターフェイスに IPv6 リンクローカルアドレスを設定します。
ステップ 8	mac-address mac-address 例 :	インターフェイス MAC アドレスを手動で設定します。

	コマンドまたはアクション	目的
	<code>apic1(config-leaf-if)# mac-address 00:44:55:66:55::01</code>	
ステップ 9	mtu <i>mtu-value</i> 例： <code>apic1(config-leaf-if)# mtu 1500</code>	このサービス クラスの MTU を設定します
ステップ 10	<code>exit</code> 例： <code>apic1(config-leaf-if)# exit</code>	設定モードに戻ります。
ステップ 11	interface port-channel <i>channel-name</i> 例： <code>apic1(config-leaf)# interface port-channel po1</code>	指定したポート チャネルのインターフェイス コンフィギュレーション モードを開始します。
ステップ 12	vlan-domain member <i>vlan-domain-name</i> 例： <code>apic1(config-leaf-if)# vlan-domain member dom1</code>	以前に設定された VLAN ドメインには、ポート チャネルのテンプレートを関連付けます。
ステップ 13	<code>exit</code> 例： <code>apic1(config-leaf-if)# exit</code>	設定モードに戻ります。
ステップ 14	interface port-channel <i>channel-name.number</i> 例： <code>apic1(config-leaf)# interface port-channel po1.2001</code>	指定したサブインターフェイス ポート チャネルのインターフェイス設定モードを開始します。
ステップ 15	vrf member <i>vrf-name tenant tenant-name</i> 例： <code>apic1(config-leaf-if)# vrf member v1 tenant t1</code>	この仮想ルーティングおよび転送 (VRF) インスタンスと L3 アウトサイド ポリシーにポート チャネルを関連付けます。場所： <ul style="list-style-type: none">• <i>Vrf-name</i> は VRF 名です。32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。• テナント名 は、テナント名です。32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。
ステップ 16	<code>exit</code> 例： <code>apic1(config-leaf-if)# exit</code>	設定モードに戻ります。

例

この例では、基本的なレイヤ 3 サブインターフェイス ポートチャネルを設定する方法を示します。

```

apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface vlan 2001
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member v1 tenant t1
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# ip address 10.1.1.1/24
apic1(config-leaf-if)# ipv6 address 2001::1/64 preferred
apic1(config-leaf-if)# ipv6 link-local fe80::1
apic1(config-leaf-if)# mac-address 00:44:55:66:55::01
apic1(config-leaf-if)# mtu 1500
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface port-channel po1
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface port-channel po1.2001
apic1(config-leaf-if)# vrf member v1 tenant t1
apic1(config-leaf-if)# exit

```

NX-OS CLI を使用したレイヤ 3 ポート チャネルにポートを追加する

この手順では、以前に設定したレイヤ 3 ポート チャネルにポートを追加します。

手順の概要

1. **configure**
2. **leaf node-id**
3. **interface Ethernet slot/port**
4. **channel-group** チャネル名

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure 例： apic1# configure	グローバル コンフィギュレーション モードを開始します。
ステップ 2	leaf node-id 例： apic1(config)# leaf 101	リーフ スイッチまたはリーフ スイッチの設定を指定します。 <i>Node-id</i> は形式 <i>node-id1-node-id2</i> の単一ノード ID または ID の範囲となる可能性があり、設定が適用されます。

NX-OS Style CLI を使用したスイッチ仮想インターフェイスの設定

	コマンドまたはアクション	目的
ステップ 3	interface Ethernet <i>slot/port</i> 例： apicl(config-leaf)# interface Ethernet 1/1-2	設定するインターフェイスのインターフェイスコンフィギュレーションモードを開始します。
ステップ 4	channel-group チャンネル名 例： apicl(config-leaf-if)# channel-group p01	チャンネルグループでポートを設定します。

例

この例では、ポートをレイヤ 3 にポートチャンネルを追加する方法を示します。

```
apicl# configure
apicl(config)# leaf 101
apicl(config-leaf)# interface Ethernet 1/1-2
apicl(config-leaf-if)# channel-group p01
```

NX-OS Style CLI を使用したスイッチ仮想インターフェイスの設定

NX-OS スタイル CLI を使用して、SVI インターフェイスのカプセル化スコープの設定

SVI インターフェイスカプセル化のスコープ設定を次の例表示する手順では、名前付きのレイヤ 3 アウト設定です。

手順の概要

1. コンフィギュレーションモードを開始します。
2. スイッチモードを開始します。
3. VLAN インターフェイスを作成します。
4. カプセル化の範囲を指定します。
5. インターフェイスモードを終了します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	コンフィギュレーションモードを開始します。 例： apicl# configure	コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 2	スイッチ モードを開始します。 例： apic1(config)# leaf 104	スイッチ モードを開始します。
ステップ 3	VLAN インターフェイスを作成します。 例： apic1(config-leaf)# interface vlan 2001	VLAN インターフェイスを作成します。VLAN の範囲は 1 ~ 4094 です。
ステップ 4	カプセル化の範囲を指定します。 例： apic1(config-leaf-if)# encap scope vrf context	カプセル化の範囲を指定します。
ステップ 5	インターフェイス モードを終了します。 例： apic1(config-leaf-if)# exit	インターフェイス モードを終了します。

NX-OS スタイル CLI を使用した SVI 自動状態の設定

始める前に

- テナントと VRF が設定されています。
- レイヤ 3 アウトが設定されており、レイヤ 3 アウトの論理ノードプロファイルと論理インターフェイスプロファイルが設定されています。

手順の概要

1. コンフィギュレーション モードを開始します。
2. スイッチ モードを開始します。
3. VLAN インターフェイスを作成します。
4. SVI 自動状態を有効にします。
5. インターフェイス モードを終了します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	コンフィギュレーション モードを開始します。 例： apic1# configure	コンフィギュレーション モードを開始します。
ステップ 2	スイッチ モードを開始します。 例：	スイッチ モードを開始します。

	コマンドまたはアクション	目的
	apicl(config)# leaf 104	
ステップ 3	VLAN インターフェイスを作成します。 例： apicl(config-leaf)# interface vlan 2001	VLAN インターフェイスを作成します。VLAN の範囲は 1 ~ 4094 です。
ステップ 4	SVI 自動状態を有効にします。 例： apicl(config-leaf-if)# autostate	SVI 自動状態を有効にします。 デフォルトで、SVI 自動状態の値は有効ではありません。
ステップ 5	インターフェイス モードを終了します。 例： apicl(config-leaf-if)# exit	インターフェイス モードを終了します。

NX-OS Style CLI を使用したルーティング プロトコルの設定

NX-OS Style CLI を使用した BFD サポート付き BGP 外部ルーテッド ネットワークの設定

NX-OS スタイルの CLI を使用した BGP 外部ルーテッド ネットワークの設定

ここでは、NX-OS CLI を使用して BGP 外部ルーテッド ネットワークを設定する方法を示します。

例：

```

apicl(config-leaf)# template route-profile damp_rp tenant t1
This template will be available on all leaves where tenant t1 has a VRF deployment
apicl(config-leaf-template-route-profile)# set dampening 15 750 2000 60
apicl(config-leaf-template-route-profile)# exit
apicl(config-leaf)#
apicl(config-leaf)# router bgp 100
apicl(config-bgp)# vrf member tenant t1 vrf ctx3
apicl(config-leaf-bgp-vrf)# neighbor 32.0.1.0/24 13out 13out-bgp
apicl(config-leaf-bgp-vrf-neighbor)# update-source ethernet 1/16.401
apicl(config-leaf-bgp-vrf-neighbor)# address-family ipv4 unicast
apicl(config-leaf-bgp-vrf-neighbor-af)# weight 400
apicl(config-leaf-bgp-vrf-neighbor-af)# exit
apicl(config-leaf-bgp-vrf-neighbor)# remote-as 65001
apicl(config-leaf-bgp-vrf-neighbor)# private-as-control remove-exclusive
apicl(config-leaf-bgp-vrf-neighbor)# private-as-control remove-exclusive-all
apicl(config-leaf-bgp-vrf-neighbor)# private-as-control remove-exclusive-all-replace-as
apicl(config-leaf-bgp-vrf-neighbor)# exit
apicl(config-leaf-bgp-vrf)# address-family ipv4 unicast
apicl(config-leaf-bgp-vrf-af)# inherit bgp dampening damp_rp
This template will be inherited on all leaves where VRF ctx3 has been deployed
apicl(config-leaf-bgp-vrf-af)# exit
apicl(config-leaf-bgp-vrf)# address-family ipv6 unicast
apicl(config-leaf-bgp-vrf-af)# inherit bgp dampening damp_rp
This template will be inherited on all leaves where VRF ctx3 has been deployed

```

```
apicl(config-leaf-bgp-vrf-af)# exit
```

NX-OS スタイルの CLI を使用した BGP 最大パスの設定

始める前に

次のフィールドの許容値については、Cisco APIC ドキュメンテーション ページの『Verified Scalability Guide for Cisco APIC』を参照してください。<https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>

適切なテナントと BGP 外部ルーテッド ネットワークが作成され、使用可能になっています。

BGP にログインして、次のコマンドを使用します:

- eBGP パスのマルチパスを設定するためのコマンド:

```
maximum-paths <value>
no maximum-paths <value>
```

- iBGP パスのマルチパスを設定するためのコマンド:

```
maximum-paths ibgp <value>
no maximum-paths ibgp <value>
```

例:

```
apicl(config)# leaf 101
apicl(config-leaf)# template bgp address-family newAf tenant t1
This template will be available on all nodes where tenant t1 has a VRF deployment
apicl(config-bgp-af)# maximum-paths ?
<1-64> Number of parallel paths
ibgp  Configure multipath for IBGP paths
apicl(config-bgp-af)# maximum-paths 10
apicl(config-bgp-af)# maximum-paths ibgp 8
apicl(config-bgp-af)# end
apicl#
```

NX-OS スタイルの CLI を使用した AS パスのプリペンド

このセクションでは、NX-OS スタイル コマンドライン インターフェイス (CLI) を使用して、AS パスのプリペンド機能を実現する方法について説明します。

始める前に

構成済みのテナント

手順の概要

1. 境界ゲートウェイ プロトコル (BGP) ルートの自動システムパス (AS パス) を変更するには、set as-path コマンドを使用します。set as-path コマンドは、

```
apicl(config-leaf-vrf-template-route-profile)# set
as-path {'prepend as-num [ ,... as-num ] | prepend-last-as num}
```

 の形式で実行します。

手順の詳細

境界ゲートウェイプロトコル (BGP) ルートの自動システムパス (AS パス) を変更するには、`set as-path` コマンドを使用します。`set as-path` コマンドは、`apic1(config-leaf-vrf-template-route-profile)# set as-path {'prepend as-num [,... as-num] | prepend-last-as num}` の形式で実行します。

例 :

```
apic1(config)# leaf 103
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# template route-profile rp1
apic1(config-leaf-vrf-template-route-profile)# set as-path ?
prepend Prepend to the AS-Path
prepend-last-as Prepend last AS to the as-path
apic1(config-leaf-vrf-template-route-profile)# set as-path prepend 100, 101, 102, 103
apic1(config-leaf-vrf-template-route-profile)# set as-path prepend-last-as 8
apic1(config-leaf-vrf-template-route-profile)# exit
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# exit
```

次のタスク

AS パスのプリペンドを無効にするには、示されているコマンドの `no` 形式を使用します:

```
apic1(config-leaf-vrf-template-route-profile)# [no] set
as-path { prepend as-num [ ,... as-num ] | prepend-last-as num}
```

NX-OS Style CLI を使用した BGP ネイバー シャットダウンの設定

NX-OS Style CLI を使用した BGP ネイバー シャットダウンの設定

次の手順では、NX-OS CLI を使用して BGP ネイバー シャットダウン機能を使用する方法について説明します。

ステップ 1 L3Out のノードとインターフェイスを設定します。

この例では設定 VRF `v1` ノード 103 (border リーフ スイッチ) と呼ばれるで `nodep1`、ルータ ID を `11.11.11.103`。インターフェイスの設定も `eth1/3` ルーテッドインターフェイス (レイヤ 3 のポート)、IP アドレスとして `12.12.12.3/24` とレイヤ 3 ドメイン `dom1`。

例 :

```
apic1(config)# leaf 103
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# router-id 11.11.11.103
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# vlan-domain member dom1
```

```

apicl(config-leaf-if)# no switchport
apicl(config-leaf-if)# vrf member tenant t1 vrf v1
apicl(config-leaf-if)# ip address 12.12.12.3/24
apicl(config-leaf-if)# exit
apicl(config-leaf)# exit

```

ステップ2 BGP ルーティング プロトコルを設定します。

この例では、15.15.15.2 および ASN 100 の BGP ピア アドレスを使用して、プライマリのルーティング プロトコルとして BGP を設定します。

例：

```

apicl(config)# leaf 103
apicl(config-leaf)# router bgp 100
apicl(config-leaf-bgp)# vrf member tenant t1 vrf v1
apicl(config-leaf-bgp-vrf)# neighbor 15.15.15.2

```

ステップ3 BGP ネイバーシャットダウン機能を使用します。

例：

```

apicl(config-leaf-bgp-vrf-neighbor)# shutdown
apicl(config-leaf-bgp-vrf)# exit
apicl(config-leaf-bgp)# exit
apicl(config-leaf)# exit

```

NX-OS スタイル CLI を使用してノード BGP タイマー ポリシーあたりの VRF あたりを設定する

手順の概要

1. タイマー ポリシーを作成する前に、BGP ASN およびルート リフレクタを設定します。
2. タイマー ポリシーを作成します。
3. 設定された BGP ポリシーを表示します。
4. ノードで特定のポリシーを参照します。
5. 特定の BGP のタイマー ポリシーのノードが表示されます。

手順の詳細

	コマンドまたはアクション	目的
ステップ1	<p>タイマー ポリシーを作成する前に、BGP ASN およびルート リフレクタを設定します。</p> <p>例：</p> <pre> apicl(config)# apicl(config)# bgp-fabric apicl(config-bgp-fabric)# route-reflector spine 102 apicl(config-bgp-fabric)# asn 42 apicl(config-bgp-fabric)# exit apicl(config)# exit apicl# </pre>	

	コマンドまたはアクション	目的
ステップ 2	<p>タイマー ポリシーを作成します。</p> <p>例 :</p> <pre> apicl# config apicl(config)# leaf 101 apicl(config-leaf)# template bgp timers pol7 tenant tn1 This template will be available on all nodes where tenant tn1 has a VRF deployment apicl(config-bgp-timers)# timers bgp 120 240 apicl(config-bgp-timers)# graceful-restart stalepath-time 500 apicl(config-bgp-timers)# maxas-limit 300 apicl(config-bgp-timers)# exit apicl(config-leaf)# exit apicl(config)# exit apicl# </pre>	特定の値は、例としてのみ提供されます。
ステップ 3	<p>設定された BGP ポリシーを表示します。</p> <p>例 :</p> <pre> apicl# show run leaf 101 template bgp timers pol7 # Command: show running-config leaf 101 template bgp timers pol7 leaf 101 template bgp timers pol7 tenant tn1 timers bgp 120 240 graceful-restart stalepath-time 500 maxas-limit 300 exit exit </pre>	
ステップ 4	<p>ノードで特定のポリシーを参照します。</p> <p>例 :</p> <pre> apicl# config apicl(config)# leaf 101 apicl(config-leaf)# router bgp 42 apicl(config-leaf-bgp)# vrf member tenant tn1 vrf ctx1 apicl(config-leaf-bgp-vrf)# inherit node-only bgp timer pol7 apicl(config-leaf-bgp-vrf)# exit apicl(config-leaf-bgp)# exit apicl(config-leaf)# exit apicl(config)# exit apicl# </pre>	
ステップ 5	<p>特定の BGP のタイマー ポリシーのノードが表示されます。</p> <p>例 :</p> <pre> apicl# show run leaf 101 router bgp 42 vrf member </pre>	

	コマンドまたはアクション	目的
	<pre> tenant tn1 vrf ctx1 # Command: show running-config leaf 101 router bgp 42 vrf member tenant tn1 vrf ctx1 leaf 101 router bgp 42 vrf member tenant tn1 vrf ctx1 inherit node-only bgp timer pol7 exit exit exit exit apicl# </pre>	

NX-OS スタイルの CLI を使用したセカンダリ IP アドレスでの双方向フォワーディング検出の設定

この手順では、NX-OS スタイルの CLI を使用して、セカンダリ IP アドレスに双方向転送検出 (BFD) を設定します。この例ではノード 103 (border リーフ スイッチ) で、ルータ ID を 11.11.11.103 で VRF v1 を構成します。また、インターフェイス eth1/3 をルーテッドインターフェイス (レイヤ 3 のポート) として構成し、IP アドレス 12.12.12.3/24 をプライマリ アドレスとして、6.11.1.224/24 をレイヤー 3 ドメイン dom1 のセカンダリ アドレスとして構成します。BFD は 99.99.99.14/32 で有効になっており、セカンダリ サブネット 6.11.1.0/24 を使用して到達可能です。

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apicl# configure terminal
```

ステップ 2 リーフ スイッチ 103 の構成モードを開始します。

例：

```
apicl(config)# leaf 103
```

ステップ 3 VRF インスタンスの構成モードを開始します。

例：

```
apicl(config-leaf)# vrf context tenant t1 vrf v1
```

ステップ 4 セカンダリ IP アドレスを構成します。

例：

```

apicl(config-leaf-vrf)# router-id 1.1.24.24
apicl(config-leaf-vrf)# exit
apicl(config-leaf)# interface ethernet 1/3
apicl(config-leaf-if)# vlan-domain member dom1
apicl(config-leaf-if)# no switchport
apicl(config-leaf-if)# vrf member tenant t1 vrf v1
apicl(config-leaf-if)# ip address 12.12.12.3/24
apicl(config-leaf-if)# ip address 6.11.1.224/24 secondary
apicl(config-leaf-if)# exit
apicl(config-leaf)# exit

```

ステップ 5 BFD を有効にします。

例 :

```
apic1(config-leaf)# vrf context tenant t1 vrf v1 l3out Routed
apic1(config-leaf-vrf)#router-id 1.1.24.24
apic1(config-leaf-vrf)#ip route 95.95.95.95/32 12.12.12.4 bfd
apic1(config-leaf-vrf)#ip route 99.99.99.14/32 6.11.1.100 bfd
```

NX-OS スタイル CLI を使用したリーフスイッチでの BFD のグローバルな設定

ステップ 1 NX-OS CLI を使用して BFD IPV4 グローバル設定 (bfdIpv4InstPol) を設定するには :

例 :

```
apic1# configure
apic1(config)# template bfd ip bfd_ipv4_global_policy
apic1(config-bfd)# [no] echo-address 1.2.3.4
apic1(config-bfd)# [no] slow-timer 2500
apic1(config-bfd)# [no] min-tx 100
apic1(config-bfd)# [no] min-rx 70
apic1(config-bfd)# [no] multiplier 3
apic1(config-bfd)# [no] echo-rx-interval 500
apic1(config-bfd)# exit
```

ステップ 2 NX-OS CLI を使用して BFD IPV6 グローバル設定 (bfdIpv6InstPol) を設定するには :

例 :

```
apic1# configure
apic1(config)# template bfd ipv6 bfd_ipv6_global_policy
apic1(config-bfd)# [no] echo-address 34::1/64
apic1(config-bfd)# [no] slow-timer 2500
apic1(config-bfd)# [no] min-tx 100
apic1(config-bfd)# [no] min-rx 70
apic1(config-bfd)# [no] multiplier 3
apic1(config-bfd)# [no] echo-rx-interval 500
apic1(config-bfd)# exit
```

ステップ 3 NX-OS CLI を使用してアクセス リーフ ポリシー グループ (infraAccNodePGrp) を設定し、以前に作成した BFD グローバル ポリシーを継承するには:

例 :

```
apic1# configure
apic1(config)# template leaf-policy-group test_leaf_policy_group
apic1(config-leaf-policy-group)# [no] inherit bfd ip bfd_ipv4_global_policy
apic1(config-leaf-policy-group)# [no] inherit bfd ipv6 bfd_ipv6_global_policy
apic1(config-leaf-policy-group)# exit
```

ステップ 4 NX-OS CLI を使用して以前に作成したリーフ ポリシー グループを リーフに関連付けるには:

例 :

```
apic1(config)# leaf-profile test_leaf_profile
apic1(config-leaf-profile)# leaf-group test_leaf_group
apic1(config-leaf-group)# leaf-policy-group test_leaf_policy_group
```

```
apicl(config-leaf-group)# leaf 101-102
apicl(config-leaf-group)# exit
```

NX-OS スタイル CLI を使用したスパインスイッチ上の BFD のグローバル設定

次の手順を使用して、NX-OS スタイル CLI を使用してスパインスイッチの BFD をグローバルに設定します。

ステップ 1 NX-OS CLI を使用して BFD IPV4 グローバル設定 (bfdIpv4InstPol) を設定するには :

例 :

```
apicl# configure
apicl(config)# template bfd ip bfd_ipv4_global_policy
apicl(config-bfd)# [no] echo-address 1.2.3.4
apicl(config-bfd)# [no] slow-timer 2500
apicl(config-bfd)# [no] min-tx 100
apicl(config-bfd)# [no] min-rx 70
apicl(config-bfd)# [no] multiplier 3
apicl(config-bfd)# [no] echo-rx-interval 500
apicl(config-bfd)# exit
```

ステップ 2 NX-OS CLI を使用して BFD IPV6 グローバル設定 (bfdIpv6InstPol) を設定するには :

例 :

```
apicl# configure
apicl(config)# template bfd ipv6 bfd_ipv6_global_policy
apicl(config-bfd)# [no] echo-address 34::1/64
apicl(config-bfd)# [no] slow-timer 2500
apicl(config-bfd)# [no] min-tx 100
apicl(config-bfd)# [no] min-rx 70
apicl(config-bfd)# [no] multiplier 3
apicl(config-bfd)# [no] echo-rx-interval 500
apicl(config-bfd)# exit
```

ステップ 3 NX-OS CLI を使用してスパイン ポリシー グループを設定し以前作成した BFD グローバル ポリシーを継承するには :

例 :

```
apicl# configure
apicl(config)# template spine-policy-group test_spine_policy_group
apicl(config-spine-policy-group)# [no] inherit bfd ip bfd_ipv4_global_policy
apicl(config-spine-policy-group)# [no] inherit bfd ipv6 bfd_ipv6_global_policy
apicl(config-spine-policy-group)# exit
```

ステップ 4 NX-OS を使用して以前作成したスパイン ポリシー グループをスパイン スイッチに関連付けるには :

例 :

```
apicl# configure
apicl(config)# spine-profile test_spine_profile
apicl(config-spine-profile)# spine-group test_spine_group
apicl(config-spine-group)# spine-policy-group test_spine_policy_group
```

NX-OS スタイルの CLI を使用して BFD インターフェイスのオーバーライドを設定する

```
apic1(config-spine-group)# spine 103-104
apic1(config-leaf-group)# exit
```

NX-OS スタイルの CLI を使用して BFD インターフェイスのオーバーライドを設定する

ステップ 1 NX-OS CLI を使用して BFD インターフェイス ポリシー (bfdIfPol) を設定するには:

例 :

```
apic1# configure
apic1(config)# tenant t0
apic1(config-tenant)# vrf context v0
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# exit
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t0 vrf v0
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface Ethernet 1/18
apic1(config-leaf-if)# vrf member tenant t0 vrf v0
apic1(config-leaf-if)# exit
apic1(config-leaf)# template bfd bfdIfPol1 tenant t0
apic1(config-template-bfd-pol)# [no] echo-mode enable
apic1(config-template-bfd-pol)# [no] echo-rx-interval 500
apic1(config-template-bfd-pol)# [no] min-rx 70
apic1(config-template-bfd-pol)# [no] min-tx 100
apic1(config-template-bfd-pol)# [no] multiplier 5
apic1(config-template-bfd-pol)# [no] optimize subinterface
apic1(config-template-bfd-pol)# exit
```

ステップ 2 NX-OS CLI を使用して、以前に作成した BFD インターフェイス ポリシーを、IPv4 アドレスを持つ L3 インターフェイスに継承させるには:

例 :

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface Ethernet 1/15
apic1(config-leaf-if)# bfd ip tenant mode
apic1(config-leaf-if)# bfd ip inherit interface-policy bfdPol1
apic1(config-leaf-if)# bfd ip authentication keyed-sha1 key 10 key password
```

ステップ 3 NX-OS CLI を使用して、以前に作成した BFD インターフェイス ポリシーを、IPv6 アドレスを持つ L3 インターフェイスに継承させるには:

例 :

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface Ethernet 1/15
apic1(config-leaf-if)# ipv6 address 2001::10:1/64 preferred
apic1(config-leaf-if)# bfd ipv6 tenant mode
apic1(config-leaf-if)# bfd ipv6 inherit interface-policy bfdPol1
apic1(config-leaf-if)# bfd ipv6 authentication keyed-sha1 key 10 key password
```

ステップ 4 NX-OS CLI を使用して、IPv4 アドレスを持つ VLAN インターフェイス上の BFD を設定するには:

例 :

```
apicl# configure
apicl(config)# leaf 101
apicl(config-leaf)# interface vlan 15
apicl(config-leaf-if)# vrf member tenant t0 vrf v0
apicl(config-leaf-if)# bfd ip tenant mode
apicl(config-leaf-if)# bfd ip inherit interface-policy bfdPoll
apicl(config-leaf-if)# bfd ip authentication keyed-shal key 10 key password
```

ステップ 5 NX-OS CLI を使用して、IPv6 アドレスを持つ VLAN インターフェイス上の BFD を設定するには:

例 :

```
apicl# configure
apicl(config)# leaf 101
apicl(config-leaf)# interface vlan 15
apicl(config-leaf-if)# ipv6 address 2001::10:1/64 preferred
apicl(config-leaf-if)# vrf member tenant t0 vrf v0
apicl(config-leaf-if)# bfd ipv6 tenant mode
apicl(config-leaf-if)# bfd ipv6 inherit interface-policy bfdPoll
apicl(config-leaf-if)# bfd ipv6 authentication keyed-shal key 10 key password
```

NX-OS スタイルの CLI を使用した BFD コンシューマ プロトコルの設定

ステップ 1 NX-OS は、CLI を使用して、BGP コンシューマ プロトコルを BFD をイネーブルにします。

例 :

```
apicl# configure
apicl(config)# bgp-fabric
apicl(config-bgp-fabric)# asn 200
apicl(config-bgp-fabric)# exit
apicl(config)# leaf 101
apicl(config-leaf)# router bgp 200
apicl(config-bgp)# vrf member tenant t0 vrf v0
apicl(config-leaf-bgp-vrf)# neighbor 1.2.3.4
apicl(config-leaf-bgp-vrf-neighbor)# [no] bfd enable
```

ステップ 2 NX-OS は、CLI を使用して、EIGRP コンシューマ プロトコルを BFD をイネーブルにします。

例 :

```
apicl(config-leaf-if)# [no] ip bfd eigrp enable
```

ステップ 3 NX-OS は、CLI を使用して、OSPF コンシューマ プロトコルを BFD をイネーブルにします。

例 :

```
apicl(config-leaf-if)# [no] ip ospf bfd enable
```

```
apicl# configure
apicl(config)# spine 103
apicl(config-spine)# interface ethernet 5/3.4
apicl(config-spine-if)# [no] ip ospf bfd enable
```

ステップ 4 NX-OS は、CLI を使用して、スタティック ルート コンシューマ プロトコルを BFD をイネーブルにします。

例 :

```
apic1(config-leaf-vrf)# [no] ip route 10.0.0.1/16 10.0.0.5 bfd

apic1(config)# spine 103
apic1(config-spine)# vrf context tenant infra vrf overlay-1
apic1(config-spine-vrf)# [no] ip route 21.1.1.1/32 32.1.1.1 bfd
```

ステップ 5 NX-OS は、CLI を使用して、IS-IS コンシューマ プロトコルを BFD をイネーブルにします。

例 :

```
apic1(config)# leaf 101
apic1(config-spine)# interface ethernet 1/49
apic1(config-spine-if)# isis bfd enabled
apic1(config-spine-if)# exit
apic1(config-spine)# exit

apic1(config)# spine 103
apic1(config-spine)# interface ethernet 5/2
apic1(config-spine-if)# isis bfd enabled
apic1(config-spine-if)# exit
apic1(config-spine)# exit
```

NX-OS Style CLI を使用した OSPF 外部ルーテッド ネットワークの設定

NX-OS CLI を使用したテナントの OSPF 外部ルーテッド ネットワークの作成

外部ルーテッド ネットワーク接続の設定には、次のステップがあります。

1. テナントの下に VRF を作成します。
2. 外部ルーテッド ネットワークに接続された境界リーフ スイッチの VRF の L3 ネットワーキング構成を設定します。この設定には、インターフェイス、ルーティング プロトコル (BGP、OSPF、EIGRP)、プロトコル パラメータ、ルートマップが含まれています。
3. テナントの下に外部 L3 EPG を作成してポリシーを設定し、これらの EPG を境界リーフ スイッチに導入します。ACI ファブリック内で同じポリシーを共有する VRF の外部ルーテッド サブネットが、1 つの「外部 L3 EPG」または 1 つの「プレフィクス EPG」を形成します。

設定は、2 つのモードで実現されます。

- テナント モード : VRF の作成および外部 L3 EPG 設定
- リーフ モード : L3 ネットワーキング構成と外部 L3 EPG の導入

次の手順は、テナントの OSPF 外部ルーテッドネットワークを作成するためのものです。テナントの OSPF 外部ルーテッドネットワークを作成するには、テナントを選択してからテナント用の VRF を作成する必要があります。



(注) この項の例では、テナント「exampleCorp」の「OnlineStore」アプリケーションの「web」epg に外部ルーテッド接続を提供する方法について説明します。

ステップ1 VLAN ドメインを設定します。

例：

```
apicl(config)# vlan-domain dom_exampleCorp
apicl(config-vlan)# vlan 5-1000
apicl(config-vlan)# exit
```

ステップ2 テナント VRF を設定し、VRF のポリシーの適用を有効にします。

例：

```
apicl(config)# tenant exampleCorp
apicl(config-tenant)# vrf context
exampleCorp_v1
apicl(config-tenant-vrf)# contract enforce
apicl(config-tenant-vrf)# exit
```

ステップ3 テナント BD を設定し、ゲートウェイ IP を「public」としてマークします。エントリ「scope public」は、このゲートウェイアドレスを外部 L3 ネットワークのルーティングプロトコルによるアドバタイズに使用できるようにします。

例：

```
apicl(config-tenant)# bridge-domain exampleCorp_b1
apicl(config-tenant-bd)# vrf member exampleCorp_v1
apicl(config-tenant-bd)# exit
apicl(config-tenant)# interface bridge-domain exampleCorp_b1
apicl(config-tenant-interface)# ip address 172.1.1.1/24 scope public
apicl(config-tenant-interface)# exit
```

ステップ4 リーフの VRF を設定します。

例：

```
apicl(config)# leaf 101
apicl(config-leaf)# vrf context tenant exampleCorp vrf exampleCorp_v1
```

ステップ5 OSPF エリアを設定し、ルートマップを追加します。

例：

```
apicl(config-leaf)# router ospf default
apicl(config-leaf-ospf)# vrf member tenant exampleCorp vrf exampleCorp_v1
apicl(config-leaf-ospf-vrf)# area 0.0.0.1 route-map map100 out
apicl(config-leaf-ospf-vrf)# exit
apicl(config-leaf-ospf)# exit
```

ステップ 6 VRF をインターフェイス (この例ではサブインターフェイス) に割り当て、OSPF エリアを有効にします。

例 :

(注) サブインターフェイスの構成では、メインインターフェイス (この例では、ethernet 1/11) は、「no switchport」によって L3 ポートに変換し、サブインターフェイスが使用するカプセル化 VLAN を含む vlan ドメイン (この例では dom_exampleCorp) を割り当てる必要があります。サブインターフェイス ethernet1/11.500 で、500 はカプセル化 VLAN です。

```
apic1(config-leaf)# interface ethernet 1/11
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vlan-domain member dom_exampleCorp
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface ethernet 1/11.500
apic1(config-leaf-if)# vrf member tenant exampleCorp vrf exampleCorp_v1
apic1(config-leaf-if)# ip address 157.10.1.1/24
apic1(config-leaf-if)# ip router ospf default area 0.0.0.1
```

ステップ 7 外部 L3 EPG ポリシーを設定します。これは、外部サブネットを特定し、epg 「web」と接続する契約を消費するために一致させるサブネットが含まれます。

例 :

```
apic1(config)# tenant t100
apic1(config-tenant)# external-l3 epg l3epg100
apic1(config-tenant-l3ext-epg)# vrf member v100
apic1(config-tenant-l3ext-epg)# match ip 145.10.1.0/24
apic1(config-tenant-l3ext-epg)# contract consumer web
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)#exit
```

ステップ 8 リーフスイッチの外部 L3 EPG を導入します。

例 :

```
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t100 vrf v100
apic1(config-leaf-vrf)# external-l3 epg l3epg100
```

NX-OS Style CLI を使用した EIGRP 外部ルーテッドネットワークの設定

NX-OS スタイルの CLI を使用した EIGRP の設定

ステップ 1 ファブリックの Application Policy Infrastructure Controller (APIC) に SSH 接続します。

例 :

```
# ssh admin@node_name
```

ステップ 2 設定モードを開始します。

例 :

```
apic1# configure
```


ステップ3 テナントの設定モードを入力します。

例：

```
apic1(config)# tenant tenant1
```

ステップ4 テナントでレイヤ3 Outside を設定します：

例：

```
apic1(config-tenant)# show run
# Command: show running-config tenant tenant1
# Time: Tue Feb 16 09:44:09 2016
tenant tenant1
  vrf context l3out
  exit
  l3out l3out-L1
    vrf member l3out
  exit
  l3out l3out-L3
    vrf member l3out
  exit
  external-l3 epg tenant1 l3out l3out-L3
    vrf member l3out
    match ip 0.0.0.0/0
    match ip 3.100.0.0/16
    match ipv6 43:101::/48
    contract consumer default
  exit
  external-l3 epg tenant1 l3out l3out-L1
    vrf member l3out
    match ipv6 23:101::/48
    match ipv6 13:101::/48
    contract provider default
  exit
exit
```

ステップ5 リーフで EIGRP の VRF を設定します：

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant tenant1 vrf l3out l3out l3out-L1
apic1(config-leaf-vrf)# show run
# Command: show running-config leaf 101 vrf context tenant tenant1 vrf l3out l3out l3out-L1
# Time: Tue Feb 16 09:44:45 2016
leaf 101
  vrf context tenant tenant1 vrf l3out l3out l3out-L1
    router-id 3.1.1.1
    route-map l3out-L1_in
      scope global
      ip prefix-list tenant1 permit 1:102::/48
      match prefix-list tenant1
    exit
  exit
  route-map l3out-L1_out
    scope global
    ip prefix-list tenant1 permit 3.102.10.0/23
    ip prefix-list tenant1 permit 3.102.100.0/31
    ip prefix-list tenant1 permit 3.102.20.0/24
    ip prefix-list tenant1 permit 3.102.30.0/25
    ip prefix-list tenant1 permit 3.102.40.0/26
    ip prefix-list tenant1 permit 3.102.50.0/27
    ip prefix-list tenant1 permit 3.102.60.0/28
    ip prefix-list tenant1 permit 3.102.70.0/29
```

```

ip prefix-list tenant1 permit 3.102.80.0/30
ip prefix-list tenant1 permit 3.102.90.0/32
<OUTPUT TRUNCATED>
ip prefix-list tenant1 permit ::/0
match prefix-list tenant1
  exit
exit
route-map l3out-L1_shared
  scope global
  exit
exit
exit

```

ステップ6 EIGRP インターフェイス ポリシーを設定します:

例:

```

apicl(config-leaf)# template eigrp interface-policy tenant1 tenant tenant1
This template will be available on all leaves where tenant tenant1 has a VRF deployment
apicl(config-template-eigrp-if-pol)# show run
# Command: show running-config leaf 101 template eigrp interface-policy tenant1 tenant tenant1
# Time: Tue Feb 16 09:45:50 2016
leaf 101
  template eigrp interface-policy tenant1 tenant tenant1
  ip hello-interval eigrp default 10
  ip hold-interval eigrp default 30
  ip throughput-delay eigrp default 20 tens-of-micro
  ip bandwidth eigrp default 20
  exit
exit

```

ステップ7 EIGRP の VRF ポリシーを設定します:

例:

```

apicl(config-leaf)# template eigrp vrf-policy tenant1 tenant tenant1
This template will be available on all leaves where tenant tenant1 has a VRF deployment
apicl(config-template-eigrp-vrf-pol)# show run
# Command: show running-config leaf 101 template eigrp vrf-policy tenant1 tenant tenant1
# Time: Tue Feb 16 09:46:31 2016
leaf 101
  template eigrp vrf-policy tenant1 tenant tenant1
  metric version 64bit
  exit
exit

```

ステップ8 EIGRP VLAN インターフェイスを設定し、インターフェイスで EIGRP を有効にします:

例:

```

apicl(config-leaf)# interface vlan 1013
apicl(config-leaf-if)# show run
# Command: show running-config leaf 101 interface vlan 1013
# Time: Tue Feb 16 09:46:59 2016
leaf 101
  interface vlan 1013
  vrf member tenant tenant1 vrf l3out
  ip address 101.13.1.2/24
  ip router eigrp default
  ipv6 address 101:13::1/112 preferred
  ipv6 router eigrp default
  ipv6 link-local fe80::101:13:1:2
  inherit eigrp ip interface-policy tenant1
  inherit eigrp ipv6 interface-policy tenant1
  exit

```

```

exit
apic1(config-leaf-if)# ip summary-address ?
  eigrp  Configure route summarization for EIGRP
apic1(config-leaf-if)# ip summary-address eigrp default 11.11.0.0/16 ?
  <CR>
apic1(config-leaf-if)# ip summary-address eigrp default 11.11.0.0/16
apic1(config-leaf-if)# ip summary-address eigrp default 11:11:1::/48
apic1(config-leaf-if)# show run
# Command: show running-config leaf 101 interface vlan 1013
# Time: Tue Feb 16 09:47:34 2016
leaf 101
  interface vlan 1013
    vrf member tenant tenant1 vrf l3out
    ip address 101.13.1.2/24
    ip router eigrp default
    ip summary-address eigrp default 11.11.0.0/16
    ip summary-address eigrp default 11:11:1::/48
    ipv6 address 101:13::1:2/112 preferred
    ipv6 router eigrp default
    ipv6 link-local fe80::101:13:1:2
    inherit eigrp ip interface-policy tenant1
    inherit eigrp ipv6 interface-policy tenant1
  exit
exit

```

ステップ9 物理インターフェイスに VLAN を適用します:

例:

```

apic1(config-leaf)# interface ethernet 1/5
apic1(config-leaf-if)# show run
# Command: show running-config leaf 101 interface ethernet 1 / 5
# Time: Tue Feb 16 09:48:05 2016
leaf 101
  interface ethernet 1/5
    vlan-domain member cli
    switchport trunk allowed vlan 1213 tenant tenant13 external-svi l3out l3out-L1
    switchport trunk allowed vlan 1613 tenant tenant17 external-svi l3out l3out-L1
    switchport trunk allowed vlan 1013 tenant tenant1 external-svi l3out l3out-L1
    switchport trunk allowed vlan 666 tenant ten_v6_cli external-svi l3out l3out_cli_L1
    switchport trunk allowed vlan 1513 tenant tenant16 external-svi l3out l3out-L1
    switchport trunk allowed vlan 1313 tenant tenant14 external-svi l3out l3out-L1
    switchport trunk allowed vlan 1413 tenant tenant15 external-svi l3out l3out-L1
    switchport trunk allowed vlan 1113 tenant tenant12 external-svi l3out l3out-L1
    switchport trunk allowed vlan 712 tenant mgmt external-svi l3out inband_l1
    switchport trunk allowed vlan 1913 tenant tenant10 external-svi l3out l3out-L1
    switchport trunk allowed vlan 300 tenant tenant1 external-svi l3out l3out-L1
  exit
exit

```

ステップ10 ルータ EIGRP を有効にします:

例:

```

apic1(config-eigrp-vrf)# show run
# Command: show running-config leaf 101 router eigrp default vrf member tenant tenant1 vrf l3out
# Time: Tue Feb 16 09:49:05 2016
leaf 101
  router eigrp default
  exit
  router eigrp default
  exit
  router eigrp default
  exit

```

```

router eigrp default
  vrf member tenant tenant1 vrf l3out
  autonomous-system 1001 l3out l3out-L1
  address-family ipv6 unicast
    inherit eigrp vrf-policy tenant1
  exit
  address-family ipv4 unicast
    inherit eigrp vrf-policy tenant1
  exit
exit
exit

```

NX-OS スタイル CLI を使用したルート集約の設定

NX-OS スタイル CLI を使用した BGP、OSPF、および EIGRP のルート集約の設定

ステップ 1 NX-OS CLI を使用して次のように BGP ルート集約を設定します:

- a) 次のように BGP を有効にします:

例 :

```

apic1(config)# pod 1
apic1(config-pod)# bgp fabric
apic1(config-pod-bgp)# asn 10
apic1(config-pod)# exit
apic1(config)# leaf 101
apic1(config-leaf)# router bgp 10

```

- b) 次のように 要約ルートを設定します:

例 :

```

apic1(config-bgp)# vrf member tenant common vrf vrf1
apic1(config-leaf-bgp-vrf)# aggregate-address 10.0.0.0/8

```

ステップ 2 NX-OS CLI を使用して次のように OSPF 外部集約を設定します。

例 :

```

apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant common vrf vrf1
apic1(config-leaf-ospf-vrf)# summary-address 10.0.0.0/8

```

ステップ 3 NX-OS CLI を使用して次のように OSPF エリア間集約を設定します。

```

apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant common vrf vrf1
apic1(config-leaf-ospf-vrf)# area 0.0.0.2 range 10.0.0.0/8 cost 20

```

ステップ 4 NX-OS CLI を使用して次のように EIGRP 集約を設定します。

例 :

```
apicl(config)# leaf 101
apicl(config-leaf)# interface ethernet 1/31 (Or interface vlan <vlan-id>)
apicl(config-leaf-if)# ip summary-address eigrp default 10.0.0.0/8
```

(注) EIGRP を設定するルート集約ポリシーはありません。EIGRP の集約を有効にするために必要なだけの設定では、サマリー サブネット、InstP です。

NX-OS スタイルの CLI を使用したルート マップとルート プロファイルによるルート制御の構成

NX-OS Style CLI を使用した BGP ピアごとのルート制御の設定

次の手順では、NX-OS CLI を使用して BGP ピア単位のルート制御を設定する方法について説明します。

ステップ 1 ルート グループ テンプレートを作成し、ルート グループに IP プレフィックスを追加します。

この例では、テナント t1 のルート グループ match-rule1 を作成し、IP プレフィックス 200.3.2.0/24 をルート グループに追加します。

例：

```
apicl(config)# leaf 103
apicl(config-leaf)# template route group match-rule1 tenant t1
apicl(config-route-group)# ip prefix permit 200.3.2.0/24
apicl(config-route-group)# exit
apicl(config-leaf)#
```

ステップ 2 ノードのテナント VRF モードを開始します。

この例では、テナント t1 の VRF v1 のテナント VRF モードを開始します。

例：

```
apicl(config-leaf)# vrf context tenant t1 vrf v1
```

ステップ 3 ルートマップを作成し、ルートマップコンフィギュレーションモードを開始します。すでに作成されているルート グループとマッチし、マッチ モードを開始してルートプロファイルを設定します。

この例では、ルートマップ rp1 を作成し、ルート グループ match-rule1 を順序番号 0 で照合します。

例：

```
apicl(config-leaf-vrf)# route-map rp1
apicl(config-leaf-vrf-route-map)# match route group match-rule1 order 0
apicl(config-leaf-vrf-route-map-match)# exit
apicl(config-leaf-vrf-route-map)# exit
apicl(config-leaf-vrf)# exit
```

ステップ 4 BGP ルーティング プロトコルを設定します。

この例では、15.15.15.2 および ASN 100 の BGP ピア アドレスを使用して、プライマリのルーティング プロトコルとして BGP を設定します。

例：

```
apic1(config)# leaf 103
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 15.15.15.2
```

ステップ 5 BGP ピアごとのルート制御機能を設定します。

ここで、

- **in** は、ルート インポート ポリシー（ファブリックに許可されるルート）です。
- **out** は、ルート エクスポート ポリシー（外部ネットワークからアドバタイズされるルート）です。

例：

```
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp1 in
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# exit
```

NX-OS スタイル CLI を使用して、明示的なプレフィックス リストでルート マップ/プロファイルの設定

始める前に

- テナントと VRF は、NX-OS CLI を介して設定する必要があります。
- NX-OS CLI を介してリーフ スイッチで VRF をイネーブルにする必要があります。

手順の概要

1. **configure**
2. **leaf** *node-id*
3. **template route group** *group-name* **tenant** *tenant-name*
4. **ip prefix permit** *prefix/masklen* [**le**{32 | 128 }]
5. **community-list** [**standard** | **expanded**] *community-list-name* *expression*
6. **exit**
7. **vrf context** **tenant** *tenant-name* **vrf** *vrf-name* [**l3out** {**BGP** | **EIGRP** | **OSPF** | **STATIC** }]
8. **template route-profile** *profile-name* [*route-control-context-name* *order-value*]
9. **set** *attribute value*
10. **exit**
11. **route-map** *map-name*
12. **match route group** *group-name* [**order number**] [**deny**]

13. **inherit route-profile** *profile-name*
14. **exit**
15. **exit**
16. **exit**
17. **router bgp** *fabric-asn*
18. **tl v1 vrf member tenant vrf**
19. **neighbor** *IP-address-of-neighbor*
20. **route-map** *map-name* {**in** | **out** }

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure 例： apicl# configure	コンフィギュレーション モードに入ります。
ステップ 2	leaf node-id 例： apicl(config)# leaf 101	設定するリーフを指定します。
ステップ 3	template route group group-name tenant tenant-name 例： apicl(config-leaf)# template route group g1 tenant exampleCorp	ルート グループ テンプレートを作成します。 (注) ルート グループ (マッチルール) は、1つ以上の IP プレフィックスと 1つ以上の マッチコミュニティタームを持つことができます。マッチタイプ全体では、AND フィルタがサポートされているため、ルート マッチルールが受け入れられるようにするために、ルート グループ内のすべての条件がマッチしている必要があります。ルート グループに複数の IP プレフィックスがある場合は、OR フィルタがサポートされます。マッチする場合は、いずれかのプレフィックスがルート タイプとして受け入れられます。
ステップ 4	ip prefix permit prefix/masklen [le{32 128 }] 例： apicl(config-route-group)# ip prefix permit 15.15.15.0/24	ルート グループに IP プレフィックスを追加します。 (注) IP プレフィックスは、BD サブネットまたは外部ネットワークを示すことができます。集約プレフィックスが必要な場合は、IPv4 にはオプションの le 32 を、IPv6 には le 128 を使用してください。

	コマンドまたはアクション	目的
ステップ 5	community-list [standard expanded] <i>community-list-name expression</i> 例 : <pre>apic1(config-route-group)# community-list standard com1 65535:20</pre>	これは任意のコマンドです。コミュニティも IP プレフィックスと照合する必要がある場合は、コミュニティのマッチ基準を追加します。
ステップ 6	exit 例 : <pre>apic1(config-route-group)# exit apic1(config-leaf)#</pre>	テンプレート モードを終了します。
ステップ 7	vrf context tenant <i>tenant-name</i> vrf <i>vrf-name</i> [l3out { BGP EIGRP OSPF STATIC }] 例 : <pre>apic1(config-leaf)# vrf context tenant exampleCorp vrf v1</pre>	ノードのテナント VRF モードを開始します。 (注) オプションの l3out 文字列を入力する場合、L3Out は NX-OS CLI で設定した L3Out である必要があります。
ステップ 8	template route-profile <i>profile-name</i> [<i>route-control-context-name order-value</i>] 例 : <pre>apic1(config-leaf-vrf)# template route-profile rp1 ctx1 1</pre>	マッチするルートに適用する必要があるセットアクションを含むテンプレートを作成します。
ステップ 9	set attribute value 例 : <pre>apic1(config-leaf-vrf-template-route-profile)# set metric 128</pre>	必要な属性 (アクションの設定) をテンプレートに追加します。
ステップ 10	exit 例 : <pre>apic1(config-leaf-vrf-template-route-profile)# exit apic1(config-leaf-vrf)#</pre>	テンプレート モードを終了します。
ステップ 11	route-map <i>map-name</i> 例 : <pre>apic1(config-leaf-vrf)# route-map bgpMap</pre>	ルートマップを作成し、ルートマップ コンフィギュレーション モードを開始します。
ステップ 12	match route group <i>group-name</i> [order number] [deny] 例 : <pre>apic1(config-leaf-vrf-route-map)# match route group g1 order 1</pre>	すでに作成されているルートグループとマッチし、マッチ モードを開始してルートプロファイルを設定します。さらに、ルートグループで定義されているマッチ基準にマッチするルートを拒否する必要がある場合は、キーワード [Deny] を選択します。デフォルトの設定は [Permit] です。

	コマンドまたはアクション	目的
ステップ 13	inherit route-profile <i>profile-name</i> 例 : <pre>apicl(config-leaf-vrf-route-map-match)# inherit route-profile rp1</pre>	ルートプロファイルを継承します(アクションを設定します)。 (注) これらのアクションは、マッチしたルートに適用されます。または、ルートプロファイルを継承する代わりに、インラインで設定されたアクションを設定することもできます。
ステップ 14	exit 例 : <pre>apicl(config-leaf-vrf-route-map-match)# exit apicl(config-leaf-vrf-route-map)#</pre>	一致モードを終了します。
ステップ 15	exit 例 : <pre>apicl(config-leaf-vrf-route-map)# exit apicl(config-leaf-vrf)#</pre>	ルートマップコンフィギュレーションモードを終了します。
ステップ 16	exit 例 : <pre>apicl(config-leaf-vrf)# exit apicl(config-leaf)#</pre>	VRF コンフィギュレーションモードを終了します。
ステップ 17	router bgp <i>fabric-asn</i> 例 : <pre>apicl(config-leaf)# router bgp 100</pre>	リーフ ノードを設定します。
ステップ 18	tl vl vrf member tenant vrf 例 : <pre>apicl(config-leaf-bgp)# vrf member tenant t1 vrf v1</pre>	BGP ポリシーの BGP の VRF メンバーシップとテナントを設定します。
ステップ 19	neighbor <i>IP-address-of-neighbor</i> 例 : <pre>apicl(config-leaf-bgp-vrf)# neighbor 15.15.15.2</pre>	BGP ネイバーを設定します。
ステップ 20	route-map <i>map-name</i> { in out } 例 : <pre>apicl(config-leaf-bgp-vrf-neighbor)# route-map bgpMap out</pre>	BGP ネイバのルート マップを設定します。

NX-OS スタイルの CLI を使用した、インポート制御とエクスポート制御を使用するルート制御プロトコルの設定

この例では、ネットワーク接続 BGP を使用して外部レイヤ 3 が設定されていることを前提としています。OSPF を使用するように設定されたネットワークに対してもこれらのタスクを実行することができます。

ここでは、NX-OS CLI を使用してルート マップを作成する方法を説明します。

始める前に

- テナント、プライベートネットワーク、およびブリッジドメインが作成されていること。
- レイヤ 3 Outside テナント ネットワークが設定されていること。

ステップ 1 一致コミュニティ、一致プレフィックス リストを使用したインポートルート制御

例：

```
apic1# configure
apic1(config)# leaf 101
    # Create community-list
apic1(config-leaf)# template community-list standard CL_1 65536:20 tenant exampleCorp
apic1(config-leaf)# vrf context tenant exampleCorp vrf v1

    #Create Route-map and use it for BGP import control.
apic1(config-leaf-vrf)# route-map bgpMap
    # Match prefix-list and set route-profile actions for the match.
apic1(config-leaf-vrf-route-map)# ip prefix-list list1 permit 13.13.13.0/24
apic1(config-leaf-vrf-route-map)# ip prefix-list list1 permit 14.14.14.0/24
apic1(config-leaf-vrf-route-map)# match prefix-list list1
apic1(config-leaf-vrf-route-map-match)# set tag 200
apic1(config-leaf-vrf-route-map-match)# set local-preference 64
apic1(config-leaf)# router bgp 100
apic1(config-bgp)# vrf member tenant exampleCorp vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 3.3.3.3
apic1(config-leaf-bgp-vrf-neighbor)# route-map bgpMap in
```

ステップ 2 一致 BD、デフォルトのエクスポートルート プロファイルを使用したエクスポートルート制御

例：

```
# Create custom and "default-export" route-profiles
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant exampleCorp vrf v1
apic1(config-leaf-vrf)# template route-profile default-export
apic1(config-leaf-vrf-template-route-profile)# set metric 256
apic1(config-leaf-vrf)# template route-profile bd-rtctrl
apic1(config-leaf-vrf-template-route-profile)# set metric 128

#Create a Route-map and match on BD, prefix-list
apic1(config-leaf-vrf)# route-map bgpMap
apic1(config-leaf-vrf-route-map)# match bridge-domain bd1
apic1(config-leaf-vrf-route-map-match)#exit
apic1(config-leaf-vrf-route-map)# match prefix-list p1
apic1(config-leaf-vrf-route-map-match)#exit
```

```
apicl(config-leaf-vrf-route-map)# match bridge-domain bd2
apicl(config-leaf-vrf-route-map-match)# inherit route-profile bd-rtctrl
```

- (注) この場合、bd1 のパブリック サブネットとプレフィックスリスト p1 を照合するプレフィックスが、ルート プロファイルの「default-export」を使用してエクスポートされ、bd2 のパブリック サブネットはルート プロファイルの「bd-rtctrl」を使用してエクスポートされます。

NX-OS Style CLI を使用したインターリーク再配布の設定

次の手順では、NX-OS スタイルの CLI を使用してインターリーク再配布を設定する方法について説明します。

始める前に

テナント、VRF および L3Out を作成します。

ステップ 1 境界リーフ ノードのインターリーク再配布のルート マップを設定します。

例：

次の例では、[テナント (tenant)][CLI_TEST] および [VRF][VRF1] の IP プレフィックスリスト [CLI_PFX1] を使用してルート マップ [CLI_RP] を設定します。

```
apicl# conf t
apicl(config)# leaf 101
apicl(config-leaf)# vrf context tenant CLI_TEST vrf VRF1
apicl(config-leaf-vrf)# route-map CLI_RP
apicl(config-leaf-vrf-route-map)# ip prefix-list CLI_PFX1 permit 192.168.1.0/24
apicl(config-leaf-vrf-route-map)# match prefix-list CLI_PFX1 [deny]
```

ステップ 2 設定されたルート マップを使用して、インターリーク再配布を設定します。

例：

次に、設定されたルート マップ [CLI_RP] を使用して OSPF ルートの再配布を設定する例を示します。

```
apicl# conf t
apicl(config)# leaf 101
apicl(config-leaf)# router bgp 65001
apicl(config-leaf-bgp)# vrf member tenant CLI_TEST vrf VRF1
apicl(config-leaf-bgp-vrf)# redistribute ospf route-map CLI_RP
```

NX-OS スタイル CLI を使用したトランジットルーティングの設定

NX-OS スタイル CLI を使用したトランジットルーティングの設定

次の手順では、テナントのトランジットルーティングを設定する方法を説明します。この例では、別々にルータに接続された2つの境界リーフスイッチ上の1個のVRFで、2個のL3Outsを展開します。

始める前に

- ノード、ポート、機能プロファイル、AEP、レイヤ3ドメインを設定します。
- 使用してVLANドメイン設定、**vlan** ドメイン ドメイン および **vlan** *vlan* 範囲 コマンド。
- BGP ルート リフレクタ ポリシーを設定し、ファブリック内でルーテッドを伝達します。

ステップ1 テナントおよびVRFを設定します。

この例ではVRF v1でテナント t1を設定します。VRFはまだ展開されていません。

例：

```
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# vrf context v1
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# exit
```

ステップ2 ノードおよびインターフェイスを設定します。

この例では、2つの境界リーフスイッチでテナント t1 の2つのL3Outsを設定します。

- 最初のL3Outはノード101上にあり、nodep1という名前です。ノード101はルータID 11.11.11.103で設定されます。ルーテッドインターフェイス ifp1 が eth1/3 にあり、IPアドレス 12.12.12.3/24 です。
- 2番目のL3Outがノード102上にあり、nodep2という名前です。ノード102はルータID 22.22.22.203で設定されます。ルーテッドインターフェイス ifp2 が eth1/3 に存在し、IPアドレスは 23.23.23.1/24 です。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# router-id 11.11.11.103
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member tenant t1 vrf v1
apic1(config-leaf-if)# ip address 12.12.12.3/24
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)# leaf 102
```

```
apicl(config-leaf)# vrf context tenant t1 vrf v1
apicl(config-leaf-vrf)# router-id 22.22.22.203
apicl(config-leaf-vrf)# exit
apicl(config-leaf)# interface ethernet 1/3
apicl(config-leaf-if)# vlan-domain member dom1
apicl(config-leaf-if)# no switchport
apicl(config-leaf-if)# vrf member tenant t1 vrf v1
apicl(config-leaf-if)# ip address 23.23.23.3/24
apicl(config-leaf-if)# exit
apicl(config-leaf)# exit
```

ステップ3 両方のリーフスイッチのルーティングプロトコルを設定します。

この例では、両方の境界リーフスイッチに対して、ASN 100 でプライマリ ルーティングプロトコルとして BGP を設定します。BGP ピア 15.15.15.2 を持つノード 101 と BGP ピア 25.25.25.2 を持つノード102を設定します。

例：

```
apicl(config)# leaf 101
apicl(config-leaf)# router bgp 100
apicl(config-leaf-bgp)# vrf member tenant t1 vrf v1
apicl(config-leaf-bgp-vrf)# neighbor 15.15.15.2
apicl(config-leaf-bgp-vrf-neighbor)# exit
apicl(config-leaf-bgp-vrf)# exit
apicl(config-leaf-bgp)# exit
apicl(config-leaf)# exit
apicl(config)# leaf 102
apicl(config-leaf)# router bgp 100
apicl(config-leaf-bgp)# vrf member tenant t1 vrf v1
apicl(config-leaf-bgp-vrf)# neighbor 25.25.25.2
apicl(config-leaf-bgp-vrf-neighbor)# exit
apicl(config-leaf-bgp-vrf)# exit
apicl(config-leaf-bgp)# exit
apicl(config-leaf)# exit
```

ステップ4 接続ルーティングプロトコルを設定します。

この例では、定期的なエリア ID 0.0.0.0 で両方の L3Outs に対して通信プロトコルとして OSPF を設定します。

例：

```
apicl(config)# leaf 101
apicl(config-leaf)# router ospf default
apicl(config-leaf-ospf)# vrf member tenant t1 vrf v1
apicl(config-leaf-ospf-vrf)# area 0.0.0.0 loopback 40.40.40.1
apicl(config-leaf-ospf-vrf)# exit
apicl(config-leaf-ospf)# exit
apicl(config-leaf)# exit
apicl(config)# leaf 102
apicl(config-leaf)# router ospf default
apicl(config-leaf-ospf)# vrf member tenant t1 vrf v1
apicl(config-leaf-ospf-vrf)# area 0.0.0.0 loopback 60.60.60.1
apicl(config-leaf-ospf-vrf)# exit
apicl(config-leaf-ospf)# exit
apicl(config-leaf)# exit
```

ステップ5 外部 EPG を設定します。

この例では、ネットワーク 192.168.1.0/24 をノード 101 上の外部ネットワーク extnw1 として、ネットワーク 192.168.2.0/24 をノード 102 上の外部ネットワーク extnw2 として設定します。

例 :

```

apic1(config)# tenant t1
apic1(config-tenant)# external-l3 epg extnw1
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# match ip 192.168.1.0/24
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# external-l3 epg extnw2
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# match ip 192.168.2.0/24
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# exit
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# external-l3 epg extnw1
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# exit
apic1(config)# leaf 102
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# external-l3 epg extnw2
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# exit

```

ステップ 6 オプション。ルート マップを設定します。

この例では、インバウンドおよびアウトバウンド方向で各 BGP ピアのルート マップを設定します。

例 :

例 :

```

apic1(config)# leaf 101
apic1(config-leaf)# template route group match-rule1 tenant t1
apic1(config-route-group)# ip prefix permit 192.168.1.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# template route group match-rule2 tenant t1
apic1(config-route-group)# ip prefix permit 192.168.2.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# route-map rp1
apic1(config-leaf-vrf-route-map)# match route group match-rule1 order 0
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# route-map rp2
apic1(config-leaf-vrf-route-map)# match route group match-rule2 order 0
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 15.15.15.2
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp1 in
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp2 out
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# exit

apic1(config)# leaf 102
apic1(config-leaf)# template route group match-rule1 tenant t1
apic1(config-route-group)# ip prefix permit 192.168.1.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# template route group match-rule2 tenant t1
apic1(config-route-group)# ip prefix permit 192.168.2.0/24
apic1(config-route-group)# exit

```

```

apicl(config-leaf)# vrf context tenant t1 vrf v1
apicl(config-leaf-vrf)# route-map rp1
apicl(config-leaf-vrf-route-map)# match route group match-rule2 order 0
apicl(config-leaf-vrf-route-map-match)# exit
apicl(config-leaf-vrf-route-map)# exit
apicl(config-leaf-vrf)# route-map rp2
apicl(config-leaf-vrf-route-map)# match route group match-rule1 order 0
apicl(config-leaf-vrf-route-map-match)# exit
apicl(config-leaf-vrf-route-map)# exit
apicl(config-leaf-vrf)# exit
apicl(config-leaf)# router bgp 100
apicl(config-leaf-bgp)# vrf member tenant t1 vrf v1
apicl(config-leaf-bgp-vrf)# neighbor 25.25.25.2
apicl(config-leaf-bgp-vrf-neighbor)# route-map rp2 in
apicl(config-leaf-bgp-vrf-neighbor)# route-map rp1 out
apicl(config-leaf-bgp-vrf-neighbor)# exit
apicl(config-leaf-bgp-vrf)# exit
apicl(config-leaf-bgp)# exit
apicl(config-leaf)# exit

```

ステップ7 フィルタ（アクセスリスト）およびコントラクトを作成し、EPG が通信できるようにします。

例：

```

apicl(config)# tenant t1
apicl(config-tenant)# access-list http-filter
apicl(config-tenant-acl)# match ip
apicl(config-tenant-acl)# match tcp dest 80
apicl(config-tenant-acl)# exit
apicl(config-tenant)# contract httpCtrct
apicl(config-tenant-contract)# scope vrf
apicl(config-tenant-contract)# subject subj1
apicl(config-tenant-contract-subj)# access-group http-filter both
apicl(config-tenant-contract-subj)# exit
apicl(config-tenant-contract)# exit
apicl(config-tenant)# exit

```

ステップ8 契約を設定し、Epg に関連付けます。

例：

```

apicl(config)# tenant t1
apicl(config-tenant)# external-l3 epg extnw1
apicl(config-tenant-l3ext-epg)# vrf member v1
apicl(config-tenant-l3ext-epg)# contract provider httpCtrct
apicl(config-tenant-l3ext-epg)# exit
apicl(config-tenant)# external-l3 epg extnw2
apicl(config-tenant-l3ext-epg)# vrf member v1
apicl(config-tenant-l3ext-epg)# contract consumer httpCtrct
apicl(config-tenant-l3ext-epg)# exit
apicl(config-tenant)# exit
apicl(config)#

```

例：中継ルーティング

この例では、中継ルーティングのマージされた設定を提供します。設定は別々のルータに接続されている2個の障壁リーフスイッチで、2つのL3Outsを持つ単一のテナントとVRFのためにあります。

```

apicl# configure
apicl(config)# tenant t1

```

```
apic1(config-tenant)# vrf context v1
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# exit

apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# router-id 11.11.11.103
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member tenant t1 vrf v1
apic1(config-leaf-if)# ip address 12.12.12.3/24
apic1(config-leaf-if)# exit
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 15.15.15.2
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant t1 vrf v1
apic1(config-leaf-ospf-vrf)# area 0.0.0.0 loopback 40.40.40.1
apic1(config-leaf-ospf-vrf)# exit
apic1(config-leaf-ospf)# exit
apic1(config-leaf)# exit

apic1(config)# leaf 102
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# router-id 22.22.22.203
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member tenant t1 vrf v1
apic1(config-leaf-if)# ip address 23.23.23.3/24
apic1(config-leaf-if)# exit
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 25.25.25.2/24
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant t1 vrf v1
apic1(config-leaf-ospf-vrf)# area 0.0.0.0 loopback 60.60.60.3
apic1(config-leaf-ospf-vrf)# exit
apic1(config-leaf-ospf)# exit
apic1(config-leaf)# exit

apic1(config)# tenant t1
apic1(config-tenant)# external-l3 epg extnw1
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# match ip 192.168.1.0/24
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# external-l3 epg extnw2
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# match ip 192.168.2.0/24
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# exit

apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# external-l3 epg extnw1
```



```
apicl(config-leaf-vrf)# exit
apicl(config-leaf)# exit
apicl(config)# leaf 102
apicl(config-leaf)# vrf context tenant t1 vrf v1
apicl(config-leaf-vrf)# external-l3 epg extnw2
apicl(config-leaf-vrf)# exit
apicl(config-leaf)# exit

apicl(config)# leaf 101
apicl(config-leaf)# template route group match-rule1 tenant t1
apicl(config-route-group)# ip prefix permit 192.168.1.0/24
apicl(config-route-group)# exit
apicl(config-leaf)# template route group match-rule2 tenant t1
apicl(config-route-group)# ip prefix permit 192.168.2.0/24
apicl(config-route-group)# exit
apicl(config-leaf)# vrf context tenant t1 vrf v1
apicl(config-leaf-vrf)# route-map rp1
apicl(config-leaf-vrf-route-map)# match route group match-rule1 order 0
apicl(config-leaf-vrf-route-map-match)# exit
apicl(config-leaf-vrf-route-map)# exit
apicl(config-leaf-vrf)# route-map rp2
apicl(config-leaf-vrf-route-map)# match route group match-rule2 order 0
apicl(config-leaf-vrf-route-map-match)# exit
apicl(config-leaf-vrf-route-map)# exit
apicl(config-leaf-vrf)# exit
apicl(config-leaf)# router bgp 100
apicl(config-leaf-bgp)# vrf member tenant t1 vrf v1
apicl(config-leaf-bgp-vrf)# neighbor 15.15.15.2
apicl(config-leaf-bgp-vrf-neighbor)# route-map rp1 in
apicl(config-leaf-bgp-vrf-neighbor)# route-map rp2 out
apicl(config-leaf-bgp-vrf-neighbor)# exit
apicl(config-leaf-bgp-vrf)# exit
apicl(config-leaf-bgp)# exit
apicl(config-leaf)# exit

apicl(config)# leaf 102
apicl(config-leaf)# template route group match-rule1 tenant t1
apicl(config-route-group)# ip prefix permit 192.168.1.0/24
apicl(config-route-group)# exit
apicl(config-leaf)# template route group match-rule2 tenant t1
apicl(config-route-group)# ip prefix permit 192.168.2.0/24
apicl(config-route-group)# exit
apicl(config-leaf)# vrf context tenant t1 vrf v1
apicl(config-leaf-vrf)# route-map rp1
apicl(config-leaf-vrf-route-map)# match route group match-rule1 order 0
apicl(config-leaf-vrf-route-map-match)# exit
apicl(config-leaf-vrf-route-map)# exit
apicl(config-leaf-vrf)# route-map rp2
apicl(config-leaf-vrf-route-map)# match route group match-rule2 order 0
apicl(config-leaf-vrf-route-map-match)# exit
apicl(config-leaf-vrf-route-map)# exit
apicl(config-leaf-vrf)# exit
apicl(config-leaf)# router bgp 100
apicl(config-leaf-bgp)# vrf member tenant t1 vrf v1
apicl(config-leaf-bgp-vrf)# neighbor 25.25.25.2
apicl(config-leaf-bgp-vrf-neighbor)# route-map rp2 in
apicl(config-leaf-bgp-vrf-neighbor)# route-map rp1 out
apicl(config-leaf-bgp-vrf-neighbor)# exit
apicl(config-leaf-bgp-vrf)# exit
apicl(config-leaf-bgp)# exit
apicl(config-leaf)# exit

apicl(config)# tenant t1
apicl(config-tenant)# access-list http-filter
```

```

apic1(config-tenant-acl)# match ip
apic1(config-tenant-acl)# match tcp dest 80
apic1(config-tenant-acl)# exit
apic1(config-tenant)# contract httpCtct
apic1(config-tenant-contract)# scope vrf
apic1(config-tenant-contract)# subject http-subj
apic1(config-tenant-contract-subj)# access-group http-filter both
apic1(config-tenant-contract-subj)# exit
apic1(config-tenant-contract)# exit
apic1(config-tenant)# exit

apic1(config)# tenant t1
apic1(config-tenant)# external-l3 epg extnw1
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# contract provider httpCtct
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# external-l3 epg extnw2
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# contract consumer httpCtct
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# exit
apic1(config)#

```

NX-OS Style CLI を使用した共有サービスの設定

NX-OS スタイル CLI を使用して共有 レイヤ 3 VRF 内リークを設定する - 名前が付けられた例

手順の概要

1. コンフィギュレーションモードを開始します。
2. プロバイダー レイヤ 3 を設定します。
3. レイヤ 3 Out コンシューマを設定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<p>コンフィギュレーションモードを開始します。</p> <p>例 :</p> <pre>apic1# configure</pre>	
ステップ 2	<p>プロバイダー レイヤ 3 を設定します。</p> <p>例 :</p> <pre>apic1(config)# tenant t1_provider apic1(config-tenant)# external-l3 epg l3extInstP-1 l3out T0-o1-L3OUT-1 apic1(config-tenant-l3ext-epg)# vrf member VRF1 apic1(config-tenant-l3ext-epg)# match ip 192.168.2.0/24 shared apic1(config-tenant-l3ext-epg)# contract provider vzBrCP-1 apic1(config-tenant-l3ext-epg)# exit</pre>	

	コマンドまたはアクション	目的
	<pre> apicl(config-tenant)# exit apicl(config)# leaf 101 apicl(config-leaf)# vrf context tenant t1_provider vrf VRF1 l3out T0-o1-L3OUT-1 apicl(config-leaf-vrf)# route-map T0-o1-L3OUT-1_shared apicl(config-leaf-vrf-route-map)# ip prefix-list l3extInstP-1 permit 192.168.2.0/24 apicl(config-leaf-vrf-route-map)# match prefix-list l3extInstP-1 apicl(config-leaf-vrf-route-map-match)# exit apicl(config-leaf-vrf-route-map)# exit apicl(config-leaf-vrf)# exit apicl(config-leaf)# exit </pre>	
ステップ 3	<p>レイヤ 3 Out コンシューマを設定します。</p> <p>例 :</p> <pre> apicl(config)# tenant t1_consumer apicl(config-tenant)# external-l3 epg l3extInstP-2 l3out T0-o1-L3OUT-1 apicl(config-tenant-l3ext-epg)# vrf member VRF2 apicl(config-tenant-l3ext-epg)# match ip 199.16.2.0/24 shared apicl(config-tenant-l3ext-epg)# contract consumer vzBrCP-1 imported apicl(config-tenant-l3ext-epg)# exit apicl(config-tenant)# exit apicl(config)# leaf 101 apicl(config-leaf)# vrf context tenant t1_consumer vrf VRF2 l3out T0-o1-L3OUT-1 apicl(config-leaf-vrf)# route-map T0-o1-L3OUT-1_shared apicl(config-leaf-vrf-route-map)# ip prefix-list l3extInstP-2 permit 199.16.2.0/24 apicl(config-leaf-vrf-route-map)# match prefix-list l3extInstP-2 apicl(config-leaf-vrf-route-map-match)# exit apicl(config-leaf-vrf-route-map)# exit apicl(config-leaf-vrf)# exit apicl(config-leaf)# exit apicl(config)# </pre>	

NX-OS Style CLI を使用した共有レイヤ 3 VRF 間リークの設定 : 名前を付けた例

手順の概要

1. コンフィギュレーション モードを開始します。
2. プロバイダ テナントおよび VRF の設定
3. コンシューマ テナントおよび VRF の設定
4. コントラクトの設定
5. プロバイダ外部レイヤ 3 EPG の設定
6. プロバイダ エクスポート マップの設定

7. コンシューマ外部レイヤ 3 EPG の設定
8. コンシューマ エクスポート マップの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<p>コンフィギュレーション モードを開始します。</p> <p>例 :</p> <pre>apicl# configure</pre>	
ステップ 2	<p>プロバイダ テナントおよび VRF の設定</p> <p>例 :</p> <pre>apicl(config)# tenant t1_provider apicl(config-tenant)# vrf context VRF1 apicl(config-tenant-vrf)# exit apicl(config-tenant)# exit</pre>	
ステップ 3	<p>コンシューマ テナントおよび VRF の設定</p> <p>例 :</p> <pre>apicl(config)# tenant t1_consumer apicl(config-tenant)# vrf context VRF2 apicl(config-tenant-vrf)# exit apicl(config-tenant)# exit</pre>	
ステップ 4	<p>コントラクトの設定</p> <p>例 :</p> <pre>apicl(config)# tenant t1_provider apicl(config-tenant)# contract vzBrCP-1 type permit apicl(config-tenant-contract)# scope exportable apicl(config-tenant-contract)# export to tenant t1_consumer apicl(config-tenant-contract)# exit</pre>	
ステップ 5	<p>プロバイダ外部レイヤ 3 EPG の設定</p> <p>例 :</p> <pre>apicl(config-tenant)# external-l3 epg l3extInstP-1 apicl(config-tenant-l3ext-epg)# vrf member VRF1 apicl(config-tenant-l3ext-epg)# match ip 192.168.2.0/24 shared apicl(config-tenant-l3ext-epg)# contract provider vzBrCP-1 apicl(config-tenant-l3ext-epg)# exit apicl(config-tenant)# exit</pre>	
ステップ 6	<p>プロバイダ エクスポート マップの設定</p> <p>例 :</p> <pre>apicl(config)# leaf 101 apicl(config-leaf)# vrf context tenant t1_provider</pre>	

	コマンドまたはアクション	目的
	<pre> vrf VRF1 apic1(config-leaf-vrf) # route-map map1 apic1(config-leaf-vrf-route-map) # ip prefix-list p1 permit 192.168.2.0/24 apic1(config-leaf-vrf-route-map) # match prefix-list p1 apic1(config-leaf-vrf-route-map-match) # exit apic1(config-leaf-vrf-route-map) # exit apic1(config-leaf-vrf) # export map map1 apic1(config-leaf-vrf) # exit apic1(config-leaf) # exit </pre>	
ステップ 7	<p>コンシューマ外部レイヤ 3 EPG の設定</p> <p>例 :</p> <pre> apic1(config) # tenant t1_consumer apic1(config-tenant) # external-13 epg l3extInstP-2 apic1(config-tenant-l3ext-epg) # vrf member VRF2 apic1(config-tenant-l3ext-epg) # match ip 199.16.2.0/24 shared apic1(config-tenant-l3ext-epg) # contract consumer vzBrCP-1 imported apic1(config-tenant-l3ext-epg) # exit apic1(config-tenant) # exit </pre>	
ステップ 8	<p>コンシューマ エクスポート マップの設定</p> <p>例 :</p> <pre> apic1(config) # leaf 101 apic1(config-leaf) # vrf context tenant t1_consumer vrf VRF2 apic1(config-leaf-vrf) # route-map map2 apic1(config-leaf-vrf-route-map) # ip prefix-list p2 permit 199.16.2.0/24 apic1(config-leaf-vrf-route-map) # match prefix-list p2 apic1(config-leaf-vrf-route-map-match) # exit apic1(config-leaf-vrf-route-map) # exit apic1(config-leaf-vrf) # export map map2 apic1(config-leaf-vrf) # exit apic1(config-leaf) # exit apic1(config) # </pre>	

NX-OS スタイルの CLI を使用した L3Out の QoS の設定

CLI を使用した L3Out での QoS の直接設定

この章では L3Out で QoS ディレクトリを設定する方法について説明します。これは、リリース 4.0(1)以降の L3Out QoS の推奨設定方法です。Cisco APIC

次のオブジェクトの内の 1 つで L3Out の QoS を設定できます。

- Switch Virtual Interface (SVI)
- サブインターフェイス

- 外部ルーテッド

ステップ1 L3Out SVI に QoS プライオリティを設定します。

例：

```
interface vlan 19
  vrf member tenant DT vrf dt-vrf
  ip address 107.2.1.252/24
  description 'SVI19'
  service-policy type qos VrfQos006 // for custom QoS attachment
  set qos-class level6 // for set QoS priority
  exit
```

ステップ2 サブインターフェイスに QoS プライオリティを設定します。

例：

```
interface ethernet 1/48.10
  vrf member tenant DT vrf inter-tenant-ctx2 l3out L4_E48_inter_tenant
  ip address 210.2.0.254/16
  service-policy type qos vrfQos002
  set qos-class level5
```

ステップ3 外部ルーテッドに QoS プライオリティを設定します。

例：

```
interface ethernet 1/37
  no switchport
  vrf member tenant DT vrf dt-vrf l3out L2E37
  ip address 30.1.1.1/24
  service-policy type qos vrfQos002
  set qos-class level5
  exit
```

CLI を使用した L3Out の QoS コントラクトの設定

この項では、コントラクトを使用して L3Out の QoS を設定する方法について説明します。



(注) リリース 4.0(1) 以降では、L3Out QoS 用にカスタム QoS ポリシーを使用することを推奨しています。CLI を使用した L3Out での QoS の直接設定 (535 ページ) で説明しています。

ステップ1 L3Out で QoS 優先順位の適用をサポートするために、出力モードの VRF を設定し、ポリシー適用を有効化します。

```
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# vrf context v1
apic1(config-tenant-vrf)# contract enforce egress
apic1(config-tenant-vrf)# exit
```

```
apicl(config-tenant)# exit
apicl(config)#
```

ステップ2 QoS を設定します。

フィルタ (access-list) を作成するとき、ターゲット DSCP レベルの **match dscp** コマンドを含みます。コントラクトを設定するとき、L3Out でのトラフィック出力の QoS クラスを含めます。または、ターゲット DSCP の値を定義することもできます。QoS ポリシーは、コントラクトまたはサブジェクトのいずれかでサポートされます。

L3out インターフェイスでの QoS またはカスタム QoS では VRF の適用は入力である必要があります。VRF の適用を出力にする必要があるのは、QoS 分類が EPG と L3out の間、または L3out から L3out へのトラフィックのコントラクトで実行される場合に限りです。

- (注) QoS 分類がコントラクトで設定され、VRF の適用が出力である場合、コントラクト QoS 分類は L3out インターフェイス QoS またはカスタム QoS 分類をオーバーライドします。

```
apicl(config)# tenant t1
apicl(config-tenant)# access-list http-filter
apicl(config-tenant-acl)# match ip
apicl(config-tenant-acl)# match tcp dest 80
apicl(config-tenant-acl)# match dscp EF
apicl(config-tenant-acl)# exit
apicl(config-tenant)# contract httpCtrct
apicl(config-tenant-contract)# scope vrf
apicl(config-tenant-contract)# qos-class level1
apicl(config-tenant-contract)# subject http-subject
apicl(config-tenant-contract-subj)# access-group http-filter both
apicl(config-tenant-contract-subj)# exit
apicl(config-tenant-contract)# exit
apicl(config-tenant)# exit
apicl(config)#
```

NX-OS Style CLI を使用した ACI IP SLA の設定

NX-OS Style CLI を使用した IP SLA モニタリング ポリシーの設定

NX-OS スタイル CLI を使用して特定の SLA タイプのモニタリングプローブを送信するように Cisco Application Policy Infrastructure Controller (APIC) を設定するには、次の手順を実行します。

始める前に

テナントが設定されていることを確認します。

ステップ1 コンフィギュレーション モードを開始します。

例 :

```
apicl# configure
```

NX-OS Style CLI を使用した IP-SLA トラック メンバーの設定

ステップ 2 テナントを作成してテナント コンフィギュレーション モードを開始するか、既存のテナントのテナント コンフィギュレーション モードを開始します。

例 :

```
apic1(config)# tenant t1
```

ステップ 3 IP SLA モニタリング ポリシーを作成し、IP SLA ポリシー コンフィギュレーション モードを開始します。

例 :

```
apic1(config-tenant)# ipsla-pol ipsla-policy-3
```

ステップ 4 モニタリング頻度を秒単位で設定します。これはプローブの送信間隔です。

例 :

```
apic1(config-ipsla-pol)# sla-frequency 40
```

ステップ 5 モニタリング プローブ タイプを設定します。

タイプに指定できる値は次のとおりです。

- icmp
- l2ping
- tcp sla-port number

スタティック ルートの IP SLA には ICMP と TCP のみが有効です。

例 :

```
apic1(config-ipsla-pol)# sla-type tcp sla-port 90
```

次のタスク

作成した IP SLA モニタリング ポリシーを表示するには、次のように入力します。

```
show running-config all tenant tenant-name ipsla-pol
```

次の出力が表示されます。

```
# Command: show running-config all tenant 99 ipsla-pol
# Time: Tue Mar 19 19:01:06 2019
tenant t1
  ipsla-pol ipsla-policy-3
    sla-detectmultiplier 3
    sla-frequency 40
    sla-type tcp sla-port 90
      sla-port 90
    exit
  exit
exit
```

NX-OS Style CLI を使用した IP-SLA トラック メンバーの設定

NX-OS スタイルの CLI を使用して IP SLA トラック メンバーを設定するには、次の手順を実行します。

始める前に

テナントおよびテナントの下の IP SLA モニタリング ポリシーが設定されていることを確認します。

ステップ 1 **configure**

コンフィギュレーション モードに入ります。

例 :

```
apicl# configure
```

ステップ 2 **tenant tenant-name**

テナントを作成するか、テナント設定モードに入ります。

例 :

```
apicl(config)# tenant t1
```

ステップ 3 **name ipv4-or-ipv6-address name track-member dst-IPAddr l3-out**

宛先 IP アドレスを持つトラック メンバーを作成し、トラック メンバー コンフィギュレーション モードを開始します。

例 :

```
apicl(config-tenant)# )# track-member tm-1 dst-IPAddr 10.10.10.1 l3-out ext-l3-1
```

ステップ 4 **ipsla-monpol name**

トラック メンバーに IP SLA モニタリング ポリシーを割り当てます。

例 :

```
apicl(config-track-member)# ipsla-monpol ipsla-policy-3
```

例

次の例は、IP SLA トラック メンバーを設定するコマンドを示しています。

```
apicl# configure
apicl(config)# tenant t1
apicl(config-tenant)# )# track-member tm-1 dst-IPAddr 10.10.10.1 l3-out ext-l3-1
apicl(config-track-member)# ipsla-monpol ipsla-policy-3
```

次のタスク

作成したトラック メンバー設定を表示するには、次のように入力します。

```
show running-config all tenant tenant-name track-member name
```

次の出力が表示されます。

```
# Command: show running-config all tenant 99 track-member tm-1
# Time: Tue Mar 19 19:01:06 2019
```

```
tenant t1
  track-member tm-1 10.10.10.1 13-out ext-13-1
    ipsla-monpol slaICMPProbe
  exit
exit
```

NX-OS Style CLI を使用した IP-SLA トラック リストの設定

NX-OS スタイルの CLI を使用して IP SLA トラック リストを設定するには、次の手順を実行します。

始める前に

テナント、IP SLA モニタリング ポリシー、およびテナント下の少なくとも 1 つのトラック メンバーが設定されていることを確認します。

ステップ 1 **configure**

コンフィギュレーション モードに入ります。

例：

```
apic1# configure
```

ステップ 2 **tenant tenant-name**

テナントを作成するか、テナント設定モードに入ります。

例：

```
apic1(config)# tenant t1
```

ステップ 3 **track-list name { percentage [percentage-down | percentage-up] number | weight [weight-down | weight-up number] }**

パーセンテージまたは重みしきい値の設定でトラックリストを作成し、トラック リストコンフィギュレーション モードを開始します。

例：

```
apic1(config-tenant)# )# track-list t1-1 percentage percentage-down 50 percentage-up 100
```

ステップ 4 **track-member name**

既存のトラック メンバーをトラック リストに割り当てます。

例：

```
apic1(config-track-list)# track-member tm-1
```

例

次の例は、IP SLA トラック リストを設定するコマンドを示しています。

```
apic1# configure
  apic1(config)# tenant t1
```

```
apicl(config-tenant)# )# track-list t1-1 percentage percentage-down 50 percentage-up
100
apicl(config-track-list)# track-member tml
```

次のタスク

作成したトラック メンバー設定を表示するには、次のように入力します。

```
show running-config all tenant tenant-name track-member name
```

次の出力が表示されます。

```
# Command: show running-config all tenant 99 track-list t1-1
# Time: Tue Mar 19 19:01:06 2019
tenant t1
  track-list t1-1 percentage percentage-down 50 percentage-up 100
  track-member tm-1 weight 10
  exit
exit
```

NX-OS Style CLI を使用したスタティック ルートとトラック リストの関連付け

NX-OS スタイル CLI を使用して IP SLA トラック リストをスタティック ルートに関連付けるには、次の手順を実行します。

始める前に

テナント、VRF およびテナントの下にあるトラック リストが設定されていることを確認してください。

ステップ 1 configure

コンフィギュレーション モードに入ります。

例 :

```
apicl# configure
```

ステップ 2 leaf id または leaf-name

リーフ スイッチを選択し、リーフ スイッチ コンフィギュレーション モードを開始します。

例 :

```
apicl(config)# leaf 102
```

ステップ 3 vrf context tenant name vrf name

VRF コンテキストを選択し、VRF コンフィギュレーション モードを開始します。

例 :

```
apicl(config-leaf)# )# vrf context tenant 99 vrf default
```

ステップ 4 ip route ip-address next-hop-ip-address route-prefix bfd ip-trackList name

既存のトラック リストをスタティック ルートに割り当てます。

例 :

```
apic1(config-leaf-vrf)# ip route 10.10.10.1/4 20.20.20.8 10 bfd ip-trackList tl-1
```

例

次に、IP SLA トラック リストをスタティック ルートに関連付けるコマンドの例を示します。

```
apic1# configure
apic1(config)# leaf 102
apic1(config-leaf)# )# vrf context tenant 99 vrf default
apic1(config-leaf-vrf)# ip route 10.10.10.1/4 20.20.20.8 10 bfd ip-trackList tl-1
```

NX-OS Style CLI を使用したトラック リストとネクストホップ プロファイルの関連付け

NX-OS スタイルの CLI を使用して IP SLA トラック リストをネクストホップ プロファイルに関連付けるには、次の手順を実行します。

始める前に

テナント、VRF およびテナントの下にあるトラック リストが設定されていることを確認してください。

ステップ 1 **configure**

コンフィギュレーション モードに入ります。

例：

```
apic1# configure
```

ステップ 2 **leaf id** または **leaf-name**

リーフ スイッチを選択し、リーフ スイッチ コンフィギュレーション モードを開始します。

例：

```
apic1(config)# leaf 102
```

ステップ 3 **vrf context tenant name vrf name**

VRF コンテキストを選択し、VRF コンフィギュレーション モードを開始します。

例：

```
apic1(config-leaf)# )# vrf context tenant 99 vrf default
```

ステップ 4 **ip route ip-address next-hop-ip-address route-prefix bfd nh-ip-trackList name**

既存のトラック リストをネクストホップに割り当てます。

例：

```
apic1(config-leaf-vrf)# ip route 10.10.10.1/4 20.20.20.8 10 bfd nh-trackList tl-1
```

例

次に、IP SLA トラック リストをネクスト ホップ プロファイルに関連付けるコマンドの例を示します。

```
apicl# configure
  apicl(config)# leaf 102
  apicl(config-leaf)# vrf context tenant 99 vrf default
  apicl(config-leaf-vrf)# ip route 10.10.10.1/4 20.20.20.8 10 bfd nh-ip-trackList
t1-1
```

CLI を使用したトラック リストおよびトラック メンバー ステータスの表示

IP SLA トラック リストおよびトラック メンバー ステータスを表示できます。

手順

	コマンドまたはアクション	目的
ステップ 1	show track brief 例 : switch# show track brief	すべてのトラック リストおよびトラック メンバーのステータスを表示します。

例

```
switch# show track brief
TrackId  Type      Instance  Parameter      State  Last Change
97       IP SLA    2034     reachability   up     2019-03-20T14:08:34.127-07:00
98       IP SLA    2160     reachability   up     2019-03-20T14:08:34.252-07:00
99       List      ---      percentage      up     2019-03-20T14:08:45.494-07:00
100      List      ---      percentage      down   2019-03-20T14:08:45.039-07:00
101      List      ---      percentage      down   2019-03-20T14:08:45.040-07:00
102      List      ---      percentage      up     2019-03-20T14:08:45.495-07:00
103      IP SLA    2040     reachability   up     2019-03-20T14:08:45.493-07:00
104      IP SLA    2887     reachability   down   2019-03-20T14:08:45.104-07:00
105      IP SLA    2821     reachability   up     2019-03-20T14:08:45.494-07:00
1        List      ---      percentage      up     2019-03-20T14:08:39.224-07:00
2        List      ---      weight          down   2019-03-20T14:08:33.521-07:00
3        IP SLA    2412     reachability   up     2019-03-20T14:08:33.983-07:00
26       IP SLA    2320     reachability   up     2019-03-20T14:08:33.988-07:00
27       IP SLA    2567     reachability   up     2019-03-20T14:08:33.987-07:00
28       IP SLA    2598     reachability   up     2019-03-20T14:08:33.990-07:00
29       IP SLA    2940     reachability   up     2019-03-20T14:08:33.986-07:00
30       IP SLA    2505     reachability   up     2019-03-20T14:08:38.915-07:00
31       IP SLA    2908     reachability   up     2019-03-20T14:08:33.990-07:00
32       IP SLA    2722     reachability   up     2019-03-20T14:08:33.992-07:00
33       IP SLA    2753     reachability   up     2019-03-20T14:08:38.941-07:00
34       IP SLA    2257     reachability   up     2019-03-20T14:08:33.993-07:00
```

CLI を使用したトラック リストとトラック メンバーの詳細の表示

IP SLA トラック リストおよびトラック メンバーの詳細を表示できます。

手順

	コマンドまたはアクション	目的
ステップ 1	show track [<i>number</i>] more 例 : switch# show track more	すべてのトラック リストおよびトラック メンバーの詳細を表示します。

例

```

switch# show track | more
Track 4
  IP SLA 2758
  reachability is down
  1 changes, last change 2019-03-12T21:41:34.729+00:00
  Tracked by:
    Track List 3
    Track List 5

Track 3
  List Threshold percentage
  Threshold percentage is down
  1 changes, last change 2019-03-12T21:41:34.700+00:00
  Threshold percentage up 1% down 0%
  Tracked List Members:
    Object 4 (50)% down
    Object 6 (50)% down
  Attached to:
    Route prefix 172.16.13.0/24

Track 5
  List Threshold percentage
  Threshold percentage is down
  1 changes, last change 2019-03-12T21:41:34.710+00:00
  Threshold percentage up 1% down 0%
  Tracked List Members:
    Object 4 (100)% down
  Attached to:
    Nexthop Addr 12.12.12.2/32

Track 6
  IP SLA 2788
  reachability is down
  1 changes, last change 2019-03-14T21:34:26.398+00:00
  Tracked by:
    Track List 3
    Track List 7

Track 20
  List Threshold percentage
  Threshold percentage is up
  4 changes, last change 2019-02-21T14:04:21.920-08:00
  Threshold percentage up 100% down 32%
  Tracked List Members:
    Object 4 (20)% up
    Object 5 (20)% up
    Object 6 (20)% up
    Object 3 (20)% up
    Object 9 (20)% up
  Attached to:

```

```
Route prefix 88.88.88.0/24
Route prefix 5000:8:1:14::/64
Route prefix 5000:8:1:2::/64
Route prefix 5000:8:1:1::/64
```

この例では、Track 4 は IP SLA ID と [Tracked by :] フィールドのトラック リストによって識別されるトラック メンバーです。

Track 3 は、しきい値情報と [トラック リストメンバー (Track List Members)] フィールドのトラック メンバーによって識別されるトラック リストです。

トラック 20 は、現在到達可能 (アップ) で、関連付けられているスタティック ルートを示すトラック リストです。

NX-OS Style CLI を使用した HSRP の設定

NX-OS スタイル CLI での Cisco APIC を使用してインラインパラメータで HSRP の設定

リーフ スイッチが設定されている場合、HSRP が有効になっています。

始める前に

- テナントと VRF が設定されています。
- VLAN プールは、適切な VLAN 範囲が定義され、レイヤ 3 ドメインが作成されて VLAN プールに接続されている状態で設定される必要があります。
- エンティティ プロファイルの接続も、レイヤ 3 ドメインに関連付けられている必要があります。
- リーフ スイッチのインターフェイス プロファイルは必要に応じて設定する必要があります。

手順の概要

1. **configure**
2. インラインパラメータを作成することにより、HSRP を設定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure 例 : apic1# configure	コンフィギュレーション モードに入ります。
ステップ 2	インラインパラメータを作成することにより、HSRP を設定します。 例 :	

コマンドまたはアクション	目的
<pre> apicl (config) # leaf 101 apicl (config-leaf) # interface ethernet 1/17 apicl (config-leaf-if) # hsrp version 1 apicl (config-leaf-if) # hsrp use-bia apicl (config-leaf-if) # hsrp delay minimum 30 apicl (config-leaf-if) # hsrp delay reload 30 apicl (config-leaf-if) # hsrp 10 ipv4 apicl (config-if-hsrp) # ip 182.16.1.2 apicl (config-if-hsrp) # ip 182.16.1.3 secondary apicl (config-if-hsrp) # ip 182.16.1.4 secondary apicl (config-if-hsrp) # mac-address 5000.1000.1060 apicl (config-if-hsrp) # timers 5 18 apicl (config-if-hsrp) # priority 100 apicl (config-if-hsrp) # preempt apicl (config-if-hsrp) # preempt delay minimum 60 apicl (config-if-hsrp) # preempt delay reload 60 apicl (config-if-hsrp) # preempt delay sync 60 apicl (config-if-hsrp) # authentication none apicl (config-if-hsrp) # authentication simple apicl (config-if-hsrp) # authentication md5 apicl (config-if-hsrp) # authentication-key <mypassword> apicl (config-if-hsrp) # authentication-key-timeout <timeout> </pre>	

NX-OS スタイル CLI のテンプレートとポリシーを使用した Cisco APIC の HSRP の設定

リーフ スイッチが設定されている場合、HSRP が有効になっています。

始める前に

- テナントと VRF が設定されています。
- VLAN プールは、適切な VLAN 範囲が定義され、レイヤ 3 ドメインが作成されて VLAN プールに接続されている状態で設定される必要があります。
- エンティティプロファイルの接続も、レイヤ 3 ドメインに関連付けられている必要があります。
- リーフ スイッチのインターフェイス プロファイルは必要に応じて設定する必要があります。

手順の概要

1. **configure**
2. HSRP ポリシー テンプレートを設定します。
3. 設定されているポリシー テンプレートを使用します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure 例： <pre>apic1# configure</pre>	コンフィギュレーション モードに入ります。
ステップ 2	HSRP ポリシー テンプレートを設定します。 例： <pre>apic1(config)# leaf 101 apic1(config-leaf)# template hsrp interface-policy hsrp-intfPol1 tenant t9 apic1(config-template-hsrp-if-pol)# hsrp use-bia apic1(config-template-hsrp-if-pol)# hsrp delay minimum 30 apic1(config-template-hsrp-if-pol)# hsrp delay reload 30 apic1(config)# leaf 101 apic1(config-leaf)# template hsrp group-policy hsrp-groupPol1 tenant t9 apic1(config-template-hsrp-group-pol)# timers 5 18 apic1(config-template-hsrp-group-pol)# priority 100 apic1(config-template-hsrp-group-pol)# preempt apic1(config-template-hsrp-group-pol)# preempt delay minimum 60 apic1(config-template-hsrp-group-pol)# preempt delay reload 60 apic1(config-template-hsrp-group-pol)# preempt delay sync 60</pre>	
ステップ 3	設定されているポリシー テンプレートを使用します。 例： <pre>apic1(config)# leaf 101 apic1(config-leaf)# interface ethernet 1/17 apic1(config-leaf-if)# hsrp version 1 apic1(config-leaf-if)# inherit hsrp interface-policy hsrp-intfPol1 apic1(config-leaf-if)# hsrp 10 ipv4 apic1(config-if-hsrp)# ip 182.16.1.2 apic1(config-if-hsrp)# ip 182.16.1.3 secondary apic1(config-if-hsrp)# ip 182.16.1.4 secondary apic1(config-if-hsrp)# mac-address 5000.1000.1060 apic1(config-if-hsrp)# inherit hsrp group-policy hsrp-groupPol1</pre>	

NX-OS Style CLI を使用した Cisco ACI GOLF の設定

NX-OS スタイル CLI を使用した推奨される共有 GOLF 設定

マルチサイトで管理されている複数の APIC サイト間で、DCI による GOLF 接続を共有する場合、ルートマップと BGP を設定し VRF 間のトラフィックの問題を避けるために次の手順を使用します。

ステップ 1 インバウンドルート マップ

例 :

```
Inbound peer policy to attach community:
```

```
route-map multi-site-in permit 10
```

```
set community 1:1 additive
```

ステップ 2 アウトバウンド ピア ポリシーを設定し、インバウンド ピア ポリシーのコミュニティに基づいてルートをフィルタします。

例 :

```
ip community-list standard test-com permit 1:1
```

```
route-map multi-site-out deny 10
```

```
match community test-com exact-match
```

```
route-map multi-site-out permit 11
```

ステップ 3 アウトバウンド ピア ポリシーを設定し、WAN へのコミュニティをフィルタします。

例 :

```
ip community-list standard test-com permit 1:1
```

```
route-map multi-site-wan-out permit 11
```

```
set comm-list test-com delete
```

ステップ 4 BGP を設定します。

例 :

```
router bgp 1
```

```
address-family l2vpn evpn
```

```
neighbor 11.11.11.11 remote-as 1
```

```
update-source loopback0
```

```
address-family l2vpn evpn
```

```
send-community both
```

```
route-map multi-site-in in
```

```
neighbor 13.0.0.2 remote-as 2
```

```
address-family l2vpn evpn

send-community both

route-map multi-site-out out
```

NX-OS スタイル CLI を使用した Cisco ACI GOLF 設定の例:

次の例を設定する CLI コマンドの show GOLF サービスで、OSPF over スパイン スイッチに接続されている WAN ルータの BGP EVPN プロトコルを使用します。

設定、BGP EVPN のテナント インフラ

次の例を設定する方法を示しています、インフラ VLAN ドメイン、VRF、インターフェイスの IP アドレッシングを含む、BGP EVPN および OSPF のテナントします。

```
configure
vlan-domain evpn-dom dynamic
exit
spine 111
# Configure Tenant Infra VRF overlay-1 on the spine.
vrf context tenant infra vrf overlay-1
router-id 10.10.3.3
exit

interface ethernet 1/33
vlan-domain member golf_dom
exit
interface ethernet 1/33.4
vrf member tenant infra vrf overlay-1
mtu 1500
ip address 5.0.0.1/24
ip router ospf default area 0.0.0.150
exit
interface ethernet 1/34
vlan-domain member golf_dom
exit
interface ethernet 1/34.4
vrf member tenant infra vrf overlay-1
mtu 1500
ip address 2.0.0.1/24
ip router ospf default area 0.0.0.200
exit

router ospf default
vrf member tenant infra vrf overlay-1
area 0.0.0.150 loopback 10.10.5.3
area 0.0.0.200 loopback 10.10.4.3
exit
exit
```

スパイン ノード上の BGP の設定

次の例では、BGP EVPN をサポートする BGP を設定する方法を示します。

```
Configure
```

```

spine 111
router bgp 100
  vrf member tenant infra vrf overlay- 1
    neighbor 10.10.4.1 evpn
      label golf_aci
      update-source loopback 10.10.4.3
      remote-as 100
    exit
    neighbor 10.10.5.1 evpn
      label golf_aci2
      update-source loopback 10.10.5.3
      remote-as 100
    exit
  exit
exit

```

BGP EVPN のテナントの設定

次の例では、BGPEVPN、BGPEVPNセッションで提供されるゲートウェイサブネットを含むのテナントを設定する方法を示します。

```

configure
tenant sky
  vrf context vrf_sky
  exit
  bridge-domain bd_sky
  vrf member vrf_sky
  exit
  interface bridge-domain bd_sky
  ip address 59.10.1.1/24
  exit
  bridge-domain bd_sky2
  vrf member vrf_sky
  exit
  interface bridge-domain bd_sky2
  ip address 59.11.1.1/24
  exit
exit

```

BGP EVPN ルート ターゲット、ルート マップと、テナントのプレフィックス EPG の設定

次の例では、BGP EVPN を介してブリッジ ドメイン サブネットをアドバタイズするルートマップを設定する方法を示します。

```

configure
spine 111
  vrf context tenant sky vrf vrf_sky
  address-family ipv4 unicast
  route-target export 100:1
  route-target import 100:1
  exit

  route-map rmap
  ip prefix-list p1 permit 11.10.10.0/24
  match bridge-domain bd_sky
  exit
  match prefix-list p1
  exit

  evpn export map rmap label golf_aci

```

```

route-map rmap2
 match bridge-domain bd_sky
   exit
 match prefix-list p1
   exit
 exit

evpn export map rmap label golf_aci2

external-l3 epg l3_sky
 vrf member vrf_sky
 match ip 80.10.1.0/24
 exit

```

NX-OS スタイル CLI を使用して DCIG への配布の BGP EVPN タイプ 2 のホスト ルートの有効化

手順

	コマンドまたはアクション	目的
ステップ 1	<p>BGP アドレス ファミリ configuration mode(設定モード、コンフィギュレーションモード)で、次のコマンドを DCIG に配布 EVPN タイプ 2 のホスト ルートを設定します。</p> <p>例 :</p> <pre> apic1(config)# leaf 101 apic1(config-leaf)# template bgp address-family bgpAf1 tenant bgp_t1 apic1(config-bgp-af)# distance 250 240 230 apic1(config-bgp-af)# host-rt-enable apic1(config-bgp-af)# exit </pre>	<p>このテンプレートは、テナント bgp_t1 は VRF の導入を持つすべてのノードで利用可能になります。配布 EVPN タイプ 2 のホスト ルートを無効にするには、次のように入力します。、 no ホスト-rt-enable コマンド。</p>



付録 C

REST API を使用してタスクを実行する

- Part I : レイヤ 3 の設定 (553 ページ)
- パートII : 外部ルーティング (L3Out) の設定 (578 ページ)

Part I : レイヤ 3 の設定

REST API を使用した共通パーベイシブ ゲートウェイの設定

REST API を使用した共通パーベイシブ ゲートウェイの設定

始める前に

- テナント、VRF、およびブリッジ ドメインが作成されていること。

共通パーベイシブ ゲートウェイを設定します。

次の REST API XML の例では、太字のテキストは一般的なパーベイシブ ゲートウェイの設定に関連しています。

例 :

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/.xml -->
<polUni>
  <fvTenant name="test">
    <fvCtx name="test"/>

    <fvBD name="test" vmac="12:34:56:78:9a:bc">
      <fvRsCtx tnFvCtxName="test"/>
      <!-- Primary address -->
      <fvSubnet ip="192.168.15.254/24" preferred="yes"/>
      <!-- Virtual address -->
      <fvSubnet ip="192.168.15.1/24" virtual="yes"/>
    </fvBD>

    <fvAp name="test">
```

```

<fvAEPg name="web">
  <fvRsBd tnFvBDName="test"/>
  <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/3]" encap="vlan-1002"/>
</fvAEPg>
</fvAp>
</fvTenant>
</polUni>

```

REST API を使用した IP エージングの設定

REST API を使用した IP エージングの設定

このセクションでは、REST API を使用した IP エージング ポリシーを有効および無効にする方法を説明します。

ステップ 1 IP エージング ポリシーを有効にするには：

例：

```

<epIpAgingP adminSt="enabled" descr="" dn="uni/infra/ipAgingP-default" name="default" ownerKey=""
ownerTag=""/>

```

ステップ 2 IP エージング ポリシーを無効にするには：

例：

```

<epIpAgingP adminSt="disabled" descr="" dn="uni/infra/ipAgingP-default" name="default" ownerKey=""
ownerTag=""/>

```

次のタスク

エンドポイントの IP アドレスをトラッキングするために使用される間隔を指定するには、次の例のように XML で `post` を送信することによって、エンドポイント保持ポリシーを作成します。

```

<fvEpRetPol bounceAgeIntvl="630" bounceTrig="protocol"
holdIntvl="350" lcOwn="local" localEpAgeIntvl="900" moveFreq="256"
name="EndpointPol1" remoteEpAgeIntvl="350"/>

```

REST API を使用したブリッジ ドメインのスタティック ルートの設定

REST API を使用してブリッジ ドメインでのスタティック ルートの設定

- スタティック ルートのサブネットを作成するには、`epg` (`fvAEPg` で `fvSubnet` オブジェクト)、普及 BD (`fvBD`) 自体 BD しないに関連付けられているように構成されます。

- サブネットマスクが/32にする必要があります (128/for IPv6) 1つの IP アドレスまたは1つのエンドポイントをポイントします。これは、パーベイスブ BD に関連付けられている EPG に含まれます。

始める前に

テナント、VRF、BD、および EPG が作成されています。

普及ゲートウェイで使用される BD のスタティック ルートを設定するには、次の例など post を入力します。

例：

```
<fvAEPg name="ep1">
  <fvRsBd tnFvBDName="bd1"/>
    <fvSubnet ip="2002:0db8:85a3:0000:0000:8a2e:0370:7344/128" ctrl="no-default-gateway"
  >
    <fvEpReachability>
      <ipNexthopEpP nhAddr="2001:0db8:85a3:0000:0000:8a2e:0370:7343/128" />
    </fvEpReachability>
  </fvSubnet>
</fvAEPg>
```

REST API を使用した IPv6 ネイバー 探索の設定

REST API を使用したブリッジドメインの IPv6 ネイバー探索対応のテナント、VRF、およびブリッジドメインの作成

ネイバー探索インターフェイス ポリシーとネイバー探索プレフィックス ポリシーが適用された、テナント、VRF、ブリッジドメインを作成します。

例：

```
<fvTenant descr="" dn="uni/tn-ExampleCorp" name="ExampleCorp" ownerKey="" ownerTag="">
  <ndIfPol name="NDPol001" ctrl="managed-cfg" descr="" hopLimit="64" mtu="1500" nsIntvl="1000"
  nsRetries="3" ownerKey="" ownerTag="" raIntvl="600" raLifetime="1800" reachableTime="0"
  retransTimer="0"/>
  <fvCtx descr="" knwMcastAct="permit" name="pvn1" ownerKey="" ownerTag="" pcEnfPref="enforced">
  </fvCtx>
  <fvBD arpFlood="no" descr="" mac="00:22:BD:F8:19:FF" multiDstPktAct="bd-flood" name="bd1"
  ownerKey="" ownerTag="" unicastRoute="yes" unkMacUcastAct="proxy" unkMcastAct="flood">
    <fvRsBDToNDP tnNdIfPolName="NDPol001"/>
    <fvRsCtx tnFvCtxName="pvn1"/>
    <fvSubnet ctrl="nd" descr="" ip="34::1/64" name="" preferred="no" scope="private">
      <fvRsNdPfxPol tnNdPfxPolName="NDPfxPol001"/>
    </fvSubnet>
    <fvSubnet ctrl="nd" descr="" ip="33::1/64" name="" preferred="no" scope="private">
      <fvRsNdPfxPol tnNdPfxPolName="NDPfxPol002"/>
    </fvSubnet>
  </fvBD>
  <ndPfxPol ctrl="auto-cfg,on-link" descr="" lifetime="1000" name="NDPfxPol001" ownerKey=""
```

```
ownerTag="" prefLifetime="1000"/>
  <ndPfxPol ctrl="auto-cfg,on-link" descr="" lifetime="4294967295" name="NDPfxPol002" ownerKey=""
ownerTag="" prefLifetime="4294967295"/>
</fvTenant>
```

(注) 外部ルーテッドを設定するときにはパブリックサブネットがある場合は、ブリッジドメインを外部設定と関連付ける必要があります。

REST API を使用したレイヤ 3 インターフェイス上の RA による IPv6 ネイバー探索インターフェイス ポリシーの設定

IPv6 ネイバー検索インターフェイス ポリシーを設定し、レイヤ 3 インターフェイスに関連付けます。

次の例では、非 VPC セットアップの設定が表示されます。

例 :

```
<fvTenant dn="uni/tn-ExampleCorp" name="ExampleCorp">
  <ndIfPol name="NDPol001" ctrl="managed-cfg" hopLimit="64" mtu="1500" nsIntvl="1000" nsRetries="3"
raIntvl="600" raLifetime="1800" reachableTime="0" retransTimer="0"/>
  <fvCtx name="pvn1" pcEnfPref="enforced">
    </fvCtx>
  <l3extOut enforceRtctrl="export" name="l3extOut001">
    <l3extRsEctx tnFvCtxName="pvn1"/>
    <l3extLNodeP name="lnodeP001">
      <l3extRsNodeL3OutAtt rtrId="11.11.205.1" rtrIdLoopBack="yes" tDn="topology/pod-2/node-2011"/>

      <l3extLIfP name="lifP001">
        <l3extRsPathL3OutAtt addr="2001:20:21:22::2/64" ifInstT="l3-port" llAddr="::"
mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit" tDn="topology/pod-2/paths-2011/pathep-[eth1/1]">

          <ndPfxP>
            <ndRsPfxPToNdPfxPol tnNdPfxPolName="NDPfxPol001"/>
          </ndPfxP>
        </l3extRsPathL3OutAtt>
        <l3extRsNdIfPol tnNdIfPolName="NDPol001"/>
      </l3extLIfP>
    </l3extLNodeP>
    <l3extInstP name="instp"/>
  </l3extOut>
  <ndPfxPol ctrl="auto-cfg,on-link" descr="" lifetime="1000" name="NDPfxPol001" ownerKey="" ownerTag=""
prefLifetime="1000"/>
</fvTenant>
```

- (注) VPC ポートについては、ndPfxP が l3extRsNodeL3OutAtt ではなく l3extMember の子である必要があります。次のコードスニペットは、VPC のセットアップでの設定を示します。

```
<l3extLNodeP name="lnodeP001">
<l3extRsNodeL3OutAtt rtrId="11.11.205.1" rtrIdLoopBack="yes" tDn="topology/pod-2/node-2011"/>
<l3extRsNodeL3OutAtt rtrId="12.12.205.1" rtrIdLoopBack="yes" tDn="topology/pod-2/node-2012"/>

  <l3extLIfP name="lifP002">
    <l3extRsPathL3OutAtt addr="0.0.0.0" encap="vlan-205" ifInstT="ext-svi" llAddr="::"
mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
tDn="topology/pod-2/protopaths-2011-2012/pathep-[vpc7]" >
      <l3extMember addr="2001:20:25:1::1/64" descr="" llAddr="::" name="" nameAlias=""
side="A">
        <ndPfxP >
          <ndRsPfxPToNdPfxPol tnNdPfxPolName="NDPfxPol001"/>
        </ndPfxP>
      </l3extMember>
      <l3extMember addr="2001:20:25:1::2/64" descr="" llAddr="::" name="" nameAlias=""
side="B">
        <ndPfxP >
          <ndRsPfxPToNdPfxPol tnNdPfxPolName="NDPfxPol001"/>
        </ndPfxP>
      </l3extMember>
    </l3extRsPathL3OutAtt>
    <l3extRsNdIfPol tnNdIfPolName="NDPol001"/> </l3extLIfP>
  </l3extLNodeP>
```

REST API を使用したネイバー探索重複アドレス検出の設定

ステップ 1 サブネットの ipv6Dad エントリの値を **disabled** に変更することによって、サブネットのネイバー探索重複アドレス検出プロセスを無効にします。

次の例は、2001:DB8:A::11/64 サブネットのネイバー探索重複アドレス検出エントリを **disabled** に設定する方法を示しています。

- (注) 次の REST API の例では、読みやすくなるように、長い行を \ 文字で分割しています。

例 :

```
<l3extRsPathL3OutAtt addr="2001:DB8:A::2/64" autostate="enabled" \
childAction="" descr="" encap="vlan-1035" encapScope="local" \
ifInstT="ext-svi" ipv6Dad="enabled" llAddr=": : " \
mac="00:22:BD:F8:19:DD" mtu="inherit" \
rn="rspathL3OutAtt-[topology/pod-1/paths-105/pathep-[eth1/1]]" \
status="" tDn="topology/pod-1/paths-105/pathep-[eth1/1]" >
  <l3extIp addr="2001:DB8:A::11/64" childAction="" descr="" \
    ipv6Dad="disabled" name="" nameAlias="" \
    rn="addr-[2001:DB8:A::11/64]" status=""/>
</l3extRsPathL3OutAtt>
</l3extLIfP>
</l3extLNodeP>
```

ステップ 2 リーフ スイッチで **show ipv6 int** コマンドを入力して、設定がリーフ スイッチに正しくプッシュされたか確認してください。例：

```
swtb23-leaf5# show ipv6 int vrf icmpv6:v1
IPv6 Interface Status for VRF "icmpv6:v1"(9)

vlan2, Interface status: protocol-up/link-up/admin-up, iod: 73
if_mode: ext
  IPv6 address:
    2001:DB8:A::2/64 [VALID] [PREFERRED]
    2001:DB8:A::11/64 [VALID] [dad-disabled]
  IPv6 subnet: 2001:DB8:A::/64
  IPv6 link-local address: fe80::863d:c6ff:fe9f:eb8b/10 (Default) [VALID]
```

REST API を使用した Microsoft NLB の設定

REST API を使用したユニキャスト モードでの Microsoft NLB の設定

Microsoft NLB をユニキャスト モードで設定するには、次の例のように XML で POST を送信します。

例：

```
https://apic-ip-address/api/node/mo/uni/.xml
<polUni>
  <fvTenant name="tn2" >
    <fvCtx name="ctx1"/>
    <fvBD name="bd2">
      <fvRsCtx tnFvCtxName="ctx1" />
    </fvBD>
    <fvAp name = "ap1">
      <fvAEPg name = "ep1">
        <fvRsBd tnFvBDName = "bd2"/>
        <fvSubnet ip="10.0.1.1/32" scope="public" ctrl="no-default-gateway">
          <fvEpNlb mac="12:21:21:35" mode="mode-uc"/>
        </fvSubnet>
      </fvAEPg>
    </fvAp>
  </fvTenant>
</polUni>
```

REST API を使用したマルチキャスト モードでの Microsoft NLB の設定

Microsoft NLB をマルチキャスト モードで設定するには、次の例のように XML で POST を送信します。

例：

```

https://apic-ip-address/api/node/mo/uni/.xml
<polUni>
  <fvTenant name="tn2" >
    <fvCtx name="ctx1"/>
    <fvBD name="bd2">
      <fvRsCtx tnFvCtxName="ctx1" />
    </fvBD>
    <fvAp name = "ap1">
      <fvAEPg name = "ep1">
        <fvRsBd tnFvBDName = "bd2"/>
        <fvSubnet ip="2001:0db8:85a3:0000:0000:8a2e:0370:7344/128" scope="public"
ctrl="no-default-gateway">
          <fvEpNlb mac="03:21:21:35" mode="mode-mcast--static"/>
        </fvSubnet>
        <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/6]" encap="vlan-911" >
          <fvNlbStaticGroup mac = "03:21:21:35" />
        </fvRsPathAtt>
      </fvAEPg>
    </fvAp>
  </fvTenant>
</polUni>

```

REST API を使用した IGMP モードでの Microsoft NLB の設定

Microsoft NLB を IGMP モードで設定するには、次の例のように XML で POST を送信します。

例 :

```

https://apic-ip-address/api/node/mo/uni/.xml
<polUni>
  <fvTenant name="tn2" >
    <fvCtx name="ctx1"/>
    <fvBD name="bd2">
      <fvRsCtx tnFvCtxName="ctx1" />
    </fvBD>
    <fvAp name = "ap1">
      <fvAEPg name = "ep1">
        <fvRsBd tnFvBDName = "bd2"/>
        <fvSubnet ip="10.0.1.3/32" scope="public" ctrl="no-default-gateway">
          <fvEpNlb group = "224.132.18.17" mode="mode-mcast-igmp" />
        </fvSubnet>
      </fvAEPg>
    </fvAp>
  </fvTenant>
</polUni>

```

REST API を使用した IGMP スヌーピングの設定

REST API を使用したブリッジドメインへの IGMP スヌーピング ポリシーの設定と割り当て

手順の概要

1. IGMP スヌーピング ポリシーを設定してブリッジドメインに割り当てるには、次の例のように XML で POST を送信します。

手順の詳細

IGMP スヌーピング ポリシーを設定してブリッジドメインに割り当てるには、次の例のように XML で POST を送信します。

例：

```
https://apic-ip-address/api/node/mo/uni/.xml
<fvTenant name="mcast_tenant1">
<!-- Create an IGMP snooping template, and provide the options -->
<igmpSnoopPol name="igmp_snp_bd_21"
ver="v2"
adminSt="enabled"
lastMbrIntvl="1"
queryIntvl="125"
rspIntvl="10"
startQueryCnt="2"
startQueryIntvl="31"
/>
<fvCtx name="ip_video"/>
<fvBD name="bd_21">
<fvRsCtx tnFvCtxName="ip_video"/>
<!-- Bind IGMP snooping to a BD -->
<fvRsIgmpsn tnIgmpSnoopPolName="igmp_snp_bd_21"/>
</fvBD></fvTenant>
```

この例では、次のプロパティで IGMP スヌーピング ポリシー、`igmp_snp_bd_12` を作成および設定し、IGMP ポリシー、`igmp_snp_bd_12` をブリッジドメイン `bd_21` にバインドします。

- 管理状態が有効です。
- 最後のメンバクエリ間隔は、デフォルトでは、1 秒です。
- クエリ間隔は、デフォルトでは 125 です。
- クエリの応答間隔はデフォルトでは 10 秒です。
- クエリの開始カウントは、デフォルトでは 2 メッセージです。
- クエリの開始間隔は 31 秒です。
- クエリアバージョンを v2 に設定する。

REST API を使用した静的ポートでの IGMP スヌーピングとマルチキャストの有効化

EPG に静的に割り当てられているポートで、IGMP スヌーピングおよびマルチキャスト処理を有効にできます。それらのポートで有効な IGMP スヌープおよびマルチキャストトラフィックへのアクセスを許可または拒否するアクセスユーザーのグループを作成および割り当てることができます。

手順の概要

1. スタティック ポートでアプリケーション EPG を設定するには、それらのポートを IGMP スヌーピングおよびマルチキャストトラフィックを受信し処理するように有効にして、グループをアクセスに割り当てるかトラフィックへのアクセスを拒否するように割り当て、次の例のように XML で POST を送信します。

手順の詳細

スタティック ポートでアプリケーション EPG を設定するには、それらのポートを IGMP スヌーピングおよびマルチキャストトラフィックを受信し処理するように有効にして、グループをアクセスに割り当てるかトラフィックへのアクセスを拒否するように割り当て、次の例のように XML で POST を送信します。

次の例では、IGMP スヌーピングが VLAN 202 上の leaf 102 インターフェイス 1/10 で有効になっています。マルチキャスト IP アドレス 224.1.1.1 および 225.1.1.1 がこのポートに関連付けられます。

例：

```
https://apic-ip-address/api/node/mo/uni/.xml
<fvTenant name="tenant_A">
  <fvAp name="application">
    <fvAEPg name="epg_A">
      <fvRsPathAtt encap="vlan-202" instrImedcycy="immediate" mode="regular"
tDn="topology/pod-1/paths-102/pathep-[eth1/10]">
        <!-- IGMP snooping static group case -->
        <igmpSnoopStaticGroup group="224.1.1.1" source="0.0.0.0"/>
        <igmpSnoopStaticGroup group="225.1.1.1" source="2.2.2.2"/>
      </fvRsPathAtt>
    </fvAEPg>
  </fvAp>
</fvTenant>
```

IGMP スヌーピングを REST API を使用するマルチキャストグループのアクセスを有効化

IGMP を有効にした後にスヌーピングおよび、EPG に静的に割り当てられているポートでマルチキャストすることができますし、作成を許可または IGMP スヌーピングへのアクセスを拒否するユーザのアクセスのグループを割り当てるおよびマルチキャストトラフィックは、これらのポートで有効になっています。

アクセスグループを定義する F23broker 、送信 XML で post このような次の例のよ。

例は、設定アクセスグループ `F23broker` `tenant_A`、`Rmap_A`、`application_A`、リーフ 102、1/10、インターフェイス VLAN 202 で、`epg_A` に関連付けられている。`Rmap_A`、アクセスグループとの関連付けによって `F23broker` マルチキャストアドレス 226.1.1.1/24 で受信したマルチキャストトラフィックへのアクセスがあり、マルチキャストアドレス 227.1.1.1/24 で受信したトラフィックへのアクセスは拒否されます。

例：

```
<!-- api/node/mo/uni/.xml --><fvTenant name="tenant_A"><pimRouteMapPol name="Rmap_A"><pimRouteMapEntry
action="permit" grp="226.1.1.1/24" order="10"/><pimRouteMapEntry action="deny" grp="227.1.1.1/24" order="20"/>
</pimRouteMapPol><fvAp name="application_A"><fvAEPg name="epg_A"><fvRsPathAtt encap="vlan-202"
instrImedcyc="immediate" mode="regular" tDn="topology/pod-1/paths-102/pathep-[eth1/10]"><!-- IGMP snooping
access group case --><igmpSnoopAccessGroup name="F23broker"><igmpRsSnoopAccessGroupFilterRMap
tnPimRouteMapPolName="Rmap_A"/></igmpSnoopAccessGroup></fvRsPathAtt></fvAEPg></fvAp></fvTenant>
```

REST API を使用した MLD スヌーピングの設定

REST API を使用した MLD スヌーピングポリシーの設定とブリッジドメインへの割り当て

MLD スヌーピングポリシーを設定してブリッジドメインに割り当てるには、次の例のように XML で POST を送信します。

例：

```
https://apic-ip-address/api/node/mo/uni/.xml
<fvTenant name="mldsn">
  <mldSnoopPol adminSt="enabled" ctrl="fast-leave,querier" name="mldsn-it-fabric-querier-policy"
queryIntvl="125"
  rspIntvl="10" startQueryCnt="2" startQueryIntvl="31" status=""/>
  <fvBD name="mldsn-bd3">
    <fvRsMldsn status="" tnMldSnoopPolName="mldsn-it-policy"/>
  </fvBD>
</fvTenant>
```

この例では、MLD スヌーピングポリシー [mldsn] を作成して次のプロパティを設定し、MLD ポリシー [mldsn-it-fabric-querier-policy] をブリッジドメイン [mldsn-bd3] にバインドします。

- 高速脱退処理が有効になっています
- クエリア処理が有効になっています
- クエリ間隔は 125 に設定されています
- 最大クエリ レスポンス タイムは 10 に設定されています
- 送信する初期クエリの数は 2 に設定されます
- 初期クエリの送信時間は 31 に設定されます

REST API を使用した IP マルチキャストの設定

REST API を使用したレイヤ 3 マルチキャストの設定

ステップ 1 テナントと VRF を設定し、VRF のマルチキャストを有効にします。

例：

```
<fvTenant dn="uni/tn-PIM_Tenant" name="PIM_Tenant">
  <fvCtx knwMcastAct="permit" name="ctx1">
    <pimCtxP mtu="1500">
      </pimCtxP>
    </fvCtx>
  </fvTenant>
```

ステップ 2 L3 アウトを設定し、L3 アウト上のマルチキャスト（PIM、IGMP）を有効にします。

例：

```
<l3extOut enforceRtctrl="export" name="l3out-pim_l3out1">
  <l3extRsEctx tnFvCtxName="ctx1"/>
  <l3extLNodeP configIssues="" name="bLeaf-CTX1-101">
    <l3extRsNodeL3OutAtt rtrId="200.0.0.1" rtrIdLoopBack="yes" tDn="topology/pod-1/node-101"/>

    <l3extLIIfP name="if-PIM_Tenant-CTX1" tag="yellow-green">
      <igmpIfP/>
      <pimIfP>
        <pimRsIfPol tDn="uni/tn-PIM_Tenant/pimifpol-pim_poll1"/>
      </pimIfP>
      <l3extRsPathL3OutAtt addr="131.1.1.1/24" ifInstT="l3-port" mode="regular" mtu="1500"
tDn="topology/pod-1/paths-101/pathep-[eth1/46]"/>
    </l3extLIIfP>
  </l3extLNodeP>
  <l3extRsL3DomAtt tDn="uni/l3dom-l3outDom"/>
  <l3extInstP name="l3out-PIM_Tenant-CTX1-1topo" >
    </l3extInstP>
  <pimExtP enabledAf="ipv4-mcast" name="pim"/>
</l3extOut>
```

ステップ 3 テナントで BD を設定して、BD のマルチキャストおよび IGMP を有効にします。

例：

```
<fvTenant dn="uni/tn-PIM_Tenant" name="PIM_Tenant">
  <fvBD arpFlood="yes" mcastAllow="yes" multiDstPktAct="bd-flood" name="bd2" type="regular"
unicastRoute="yes" unkMacUcastAct="flood" unkMcastAct="flood">
    <igmpIfP/>
    <fvRsBDToOut tnL3extOutName="l3out-pim_l3out1"/>
    <fvRsCtx tnFvCtxName="ctx1"/>
    <fvRsIgmpsn/>
    <fvSubnet ctrl="" ip="41.1.1.254/24" preferred="no" scope="private" virtual="no"/>
  </fvBD>
</fvTenant>
```

ステップ 4 IGMP ポリシーを設定し、それを BD に割り当てます。

例：

```
<fvTenant dn="uni/tn-PIM_Tenant" name="PIM_Tenant">
  <igmpIfPol grpTimeout="260" lastMbrCnt="2" lastMbrRespTime="1" name="igmp_pol"
querierTimeout="255" queryIntvl="125" robustFac="2" rspIntvl="10" startQueryCnt="2">
</igmpIfPol>
</fvTenant>
```

```

startQueryIntvl="125" ver="v2">
  </igmpIfPol>
  <fvBD arpFlood="yes" mcastAllow="yes" name="bd2">
    <igmpIfP>
      <igmpRsIfPol tDn="uni/tn-PIM_Tenant/igmpIfPol-igmp_pol"/>
    </igmpIfP>
  </fvBD>
</fvTenant>

```

ステップ 5 VRF のルート マップ、PIM、および RP ポリシーを設定します。

(注) REST API を使用してファブリック RP を設定する場合、最初にスタティック RP を設定します。

例 :

スタティック RP を設定しています :

```

<fvTenant dn="uni/tn-PIM_Tenant" name="PIM_Tenant">
  <pimRouteMapPol name="rootMap">
    <pimRouteMapEntry action="permit" grp="224.0.0.0/4" order="10" rp="0.0.0.0" src="0.0.0.0/0"/>
  </pimRouteMapPol>
  <fvCtx knwMcastAct="permit" name="ctx1">
    <pimCtxP ctrl="" mtu="1500">
      <pimStaticRPPol>
        <pimStaticRPEntryPol rpIp="131.1.1.2">
          <pimRPGrpRangePol>
            <rtmcRsFilterToRtMapPol tDn="uni/tn-PIM_Tenant/rtmap-rootMap"/>
          </pimRPGrpRangePol>
        </pimStaticRPEntryPol>
      </pimStaticRPPol>
    </pimCtxP>
  </fvCtx>
</fvTenant>

```

ファブリック RP を設定しています :

```

<fvTenant name="t0">
  <pimRouteMapPol name="fabricrp-rtmap">
    <pimRouteMapEntry grp="226.20.0.0/24" order="1" />
  </pimRouteMapPol>
  <fvCtx name="ctx1">
    <pimCtxP ctrl="">
      <pimFabricRPPol status="">
        <pimStaticRPEntryPol rpIp="6.6.6.6">
          <pimRPGrpRangePol>
            <rtmcRsFilterToRtMapPol tDn="uni/tn-t0/rtmap-fabricrp-rtmap" />
          </pimRPGrpRangePol>
        </pimStaticRPEntryPol>
      </pimFabricRPPol>
    </pimCtxP>
  </fvCtx>
</fvTenant>

```

ステップ 6 PIM インターフェイス ポリシーを設定し、それを L3 アウトに適用します。

例 :

```

<fvTenant dn="uni/tn-PIM_Tenant" name="PIM_Tenant">
  <pimIfPol authKey="" authT="none" ctrl="" drDelay="60" drPrio="1" helloItvl="30000" itvl="60"
name="pim_poll"/>
  <l3extOut enforceRtctrl="export" name="l3out-pim_l3out1" targetDscp="unspecified">
    <l3extRsEctx tnFvCtxName="ctx1"/>
  </l3extOut>
</fvTenant>

```

```

<l3extLNodeP name="bLeaf-CTX1-101">
  <l3extRsNodeL3OutAtt rtrId="200.0.0.1" rtrIdLoopBack="yes" tDn="topology/pod-1/node-101"/>

  <l3extLIIfP name="if-SIRI_VPC_src_rcv-CTX1" tag="yellow-green">
    <pimIfP>
      <pimRsIfPol tDn="uni/tn-tn-PIM_Tenant/pimifpol-pim_poll1"/>
    </pimIfP>
  </l3extLIIfP>
</l3extLNodeP>
</l3extOut>
</fvTenant>

```

ステップ 7 Inter-VRF マルチキャストを設定します。

例 :

```

<fvTenant name="t0">
  <pimRouteMapPol name="intervrf" status="">
    <pimRouteMapEntry grp="225.0.0.0/24" order="1" status=""/>
    <pimRouteMapEntry grp="226.0.0.0/24" order="2" status=""/>
    <pimRouteMapEntry grp="228.0.0.0/24" order="3" status="deleted"/>
  </pimRouteMapPol>
  <fvCtx name="ctx1">
    <pimCtxP ctrl="">
      <pimInterVRFPol status="">
        <pimInterVRFEntryPol srcVrfDn="uni/tn-t0/ctx-stig_r_ctx" >
          <rtDmcsRsFilterToRtMapPol tDn="uni/tn-t0/rtmap-intervrf" />
        </pimInterVRFEntryPol>
      </pimInterVRFPol>
    </pimCtxP>
  </fvCtx>
</fvTenant>

```

REST API を使用したレイヤ 3 IPv6 マルチキャストの設定

始める前に

- 目的の VRF、ブリッジドメイン、IPv6 アドレスを持つレイヤ 3 Out インターフェイスは、PIM6 が有効になるように設定する必要があります。レイヤ 3 Out の場合、IPv6 マルチキャストが機能するために、論理ノードプロファイルのノードに IPv6 ループバック アドレスが設定されます。
- 基本的なユニキャスト ネットワークを設定する必要があります。

ステップ 1 VRF で PIM6 を有効にします。

例 :

```

<fvTenant name="t0">
  <fvCtx name="ctx1" pcEnfPref="unenforced" >
    <pimIPv6CtxP ctrl="" mtu="1500" />
  </fvCtx>
</fvTenant>

```

ステップ 2 レイヤ 3 Out で PIM6 を有効にします。

例 :

```
<fvTenant dn="uni/tn-t0" name="t0">
  <l3extOut enforceRtctrl="export" name="bl_l3out_1">
    <pimExtP enabledAf="ipv6-mcast" name="pim"/>
  </l3extOut>
</fvTenant>
```

ステップ3 BD で PIM6 を有効にします。

例 :

```
<fvTenant name="t0" >
  <fvBD name="BD_VPC5" ipv6McastAllow="yes" >
    <fvRsCtx tnFvCtxName="ctx1" />
    <fvSubnet ip="124:1::ffff:ffff:ffff:0/64" scope="public"/>
  </fvBD>
</fvTenant>
```

ステップ4 スタティック ランデブー ポイントの設定

例 :

```
<fvTenant name="t0">
  <pimRouteMapPol dn="uni/tn-t0/rtmap-static_101_ipv6" name="static_101_ipv6">
    <pimRouteMapEntry action="permit" grp="ff00::/8" order="1" rp="2001:0:2001:2001:1:1:1:1/128"
src="::"/>
  </pimRouteMapPol>
  <fvCtx name="ctx1" pcEnfPref="unenforced">
    <pimIPV6CtxP ctrl="" mtu="1500">
      <pimStaticRPPol>
        <pimStaticRPEntryPol rpIp="2001:0:2001:2001:1:1:1:1">
          <pimRPGrpRangePol>
            <rtdmcRsFilterToRtMapPol tDn="uni/tn-t0/rtmap-static_101_ipv6"/>
          </pimRPGrpRangePol>
        </pimStaticRPEntryPol>
      </pimStaticRPPol>
    </pimIPV6CtxP>
  </fvCtx>
</fvTenant>
```

ステップ5 PIM6 インターフェイス ポリシーを設定し、レイヤ 3 Out に適用します。

例 :

```
<fvTenant dn="uni/tn-t0" name="t0">
  <l3extOut enforceRtctrl="export" name="bl_l3out_1">
    <l3extLNodeP annotation="" configIssues="" descr="" name="common_np1" nameAlias="" ownerKey=""
ownerTag="" tag="yellow-green" targetDscp="unspecified">
      <l3extLIIFP annotation="" descr="" name="common_intpl_v6" nameAlias="" ownerKey="" ownerTag=""
prio="unspecified" tag="yellow-green">
        <pimIPV6IfP annotation="" descr="" name="" nameAlias="">
          <pimRsV6IfPol annotation="" tDn="uni/tn-common/pimifpol-pimv6_policy"/>
        </pimIPV6IfP>
      </l3extLIIFP>
    </l3extLNodeP>
  </l3extOut>
</fvTenant>
```

PIM6 を使用したレイヤ 3 IPv6 マルチキャストが有効になります。

REST API を使用したマルチキャスト フィルタリングの設定

ブリッジ ドメイン レベルでマルチキャスト フィルタリングを設定します。このトピックの手順を使用して、ブリッジ ドメイン レベルで送信元フィルタリングまたは受信者フィルタリング、あるいはその両方を設定します。

始める前に

- マルチキャストフィルタリングを設定するブリッジドメインはすでに作成されています。
- ブリッジドメインは PIM 対応ブリッジドメインです。
- レイヤ 3 マルチキャストは VRF レベルで有効になります。

ステップ 1 ブリッジドメインでマルチキャストソースフィルタリングを有効にする場合は、次の例のように XML で POST を送信します。

例：

```
<fvBD dn="uni/tn-filter/BD-BD1520" ipv6McastAllow="no" mcastAllow="yes">
  <pimBDP annotation="" descr="" name="" nameAlias="" ownerKey="" ownerTag="">
    <pimBDFilterPol annotation="" descr="" name="" nameAlias="">
      <pimBDSrcFilterPol annotation="" descr="" name="" nameAlias="">
        <rtDmcRsFilterToRtMapPol tDn="uni/tn-filter/rtmap-test_src_filter"/>
      </pimBDSrcFilterPol>
    </pimBDFilterPol>
  </pimBDP>
</fvBD>
```

ステップ 2 ブリッジドメインでマルチキャストレシーバフィルタリングを有効にする場合は、次の例のように XML で POST を送信します。

例：

```
<fvBD dn="uni/tn-filter/BD-BD1520" ipv6McastAllow="no" mcastAllow="yes">
  <pimBDP annotation="" descr="" name="" nameAlias="" ownerKey="" ownerTag="">
    <pimBDFilterPol annotation="" descr="" name="" nameAlias="">
      <pimBDDestFilterPol annotation="" descr="" name="" nameAlias="">
        <rtDmcRsFilterToRtMapPol tDn="uni/tn-filter/rtmap-Recv_filter"/>
      </pimBDDestFilterPol>
    </pimBDFilterPol>
  </pimBDP>
</fvBD>
```

- (注) また、次の例のように XML で POST を送信することで、同じブリッジドメインで送信元と受信者の両方のフィルタリングを有効にすることもできます。

```
<fvBD dn="uni/tn-filter/BD-BD1520" ipv6McastAllow="no" mcastAllow="yes">
  <pimBDP annotation="" descr="" name="" nameAlias="" ownerKey="" ownerTag="">
    <pimBDFilterPol annotation="" descr="" name="" nameAlias="">
      <pimBDSrcFilterPol annotation="" descr="" name="" nameAlias="">
        <rtmcRsFilterToRtMapPol tDn="uni/tn-filter/rtnmap-test_src_filter"/>
      </pimBDSrcFilterPol>
      <pimBDDestFilterPol annotation="" descr="" name="" nameAlias="">
        <rtmcRsFilterToRtMapPol tDn="uni/tn-filter/rtnmap-Recv_filter"/>
      </pimBDDestFilterPol>
    </pimBDFilterPol>
  </pimBDP>
</fvBD>
```

REST API を使用したマルチポッドの設定

REST API を使用したマルチポッド ファブリックのセットアップ

ステップ 1 Cisco APIC へのログイン :

例 :

```
http://<apic-name/ip>:80/api/aaaLogin.xml
```

```
data: <aaaUser name="admin" pwd="ins3965!" />
```

ステップ 2 TEP プールの設定 :

例 :

```
http://<apic-name/ip>:80/api/policymgr/mo/uni/controller.xml
```

```
<fabricSetupPol status=''>
  <fabricSetupP podId="1" tepPool="10.0.0.0/16" />
  <fabricSetupP podId="2" tepPool="10.1.0.0/16" status='' />
</fabricSetupPol>
```

ステップ 3 ノード ID ポリシーの設定 :

例 :

```
http://<apic-name/ip>:80/api/node/mo/uni/controller.xml
```

```
<fabricNodeIdentPol>
<fabricNodeIdentP serial="SAL1819RXP4" name="ifav4-leaf1" nodeId="101" podId="1"/>
<fabricNodeIdentP serial="SAL1803L25H" name="ifav4-leaf2" nodeId="102" podId="1"/>
<fabricNodeIdentP serial="SAL1934MNY0" name="ifav4-leaf3" nodeId="103" podId="1"/>
<fabricNodeIdentP serial="SAL1934MNY3" name="ifav4-leaf4" nodeId="104" podId="1"/>
<fabricNodeIdentP serial="SAL1748H56D" name="ifav4-spine1" nodeId="201" podId="1"/>
<fabricNodeIdentP serial="SAL1938P7A6" name="ifav4-spine3" nodeId="202" podId="1"/>
<fabricNodeIdentP serial="SAL1938PHBB" name="ifav4-leaf5" nodeId="105" podId="2"/>
<fabricNodeIdentP serial="SAL1942R857" name="ifav4-leaf6" nodeId="106" podId="2"/>
<fabricNodeIdentP serial="SAL1931LA3B" name="ifav4-spine2" nodeId="203" podId="2"/>
```

```
<fabricNodeIdentP serial="FGE173400A9" name="ifav4-spine4" nodeId="204" podId="2"/>
</fabricNodeIdentPol>
```

ステップ 4 インフラ L3Out および外部接続プロファイルの設定 :

例 :

```
http://<apic-name/ip>:80/api/node/mo/uni.xml
```

```
<polUni>

<fvTenant descr="" dn="uni/tn-infra" name="infra" ownerKey="" ownerTag="">

  <l3extOut descr="" enforceRtctrl="export" name="multipod" ownerKey="" ownerTag=""
targetDscp="unspecified" status=''>
    <ospfExtP areaId='0' areaType='regular' status=''/>
    <l3extRsEctx tnFvCtxName="overlay-1"/>
    <l3extProvLbl descr="" name="prov_mpl" ownerKey="" ownerTag="" tag="yellow-green"/>

    <l3extLNodeP name="bSpine">
      <l3extRsNodeL3OutAtt rtrId="201.201.201.201" rtrIdLoopBack="no" tDn="topology/pod-1/node-201">

        <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
        <l3extLoopBackIfP addr="201::201/128" descr="" name=""/>
        <l3extLoopBackIfP addr="201.201.201.201/32" descr="" name=""/>
      </l3extRsNodeL3OutAtt>

      <l3extRsNodeL3OutAtt rtrId="202.202.202.202" rtrIdLoopBack="no" tDn="topology/pod-1/node-202">

        <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
        <l3extLoopBackIfP addr="202::202/128" descr="" name=""/>
        <l3extLoopBackIfP addr="202.202.202.202/32" descr="" name=""/>
      </l3extRsNodeL3OutAtt>

      <l3extRsNodeL3OutAtt rtrId="203.203.203.203" rtrIdLoopBack="no" tDn="topology/pod-2/node-203">

        <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
        <l3extLoopBackIfP addr="203::203/128" descr="" name=""/>
        <l3extLoopBackIfP addr="203.203.203.203/32" descr="" name=""/>
      </l3extRsNodeL3OutAtt>

      <l3extRsNodeL3OutAtt rtrId="204.204.204.204" rtrIdLoopBack="no" tDn="topology/pod-2/node-204">

        <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
        <l3extLoopBackIfP addr="204::204/128" descr="" name=""/>
        <l3extLoopBackIfP addr="204.204.204.204/32" descr="" name=""/>
      </l3extRsNodeL3OutAtt>

    <l3extLIfP name='portIf'>
      <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-1/paths-201/pathep-[eth1/1]"
encap='vlan-4' ifInstT='sub-interface' addr="201.1.1.1/30" />
      <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-1/paths-201/pathep-[eth1/2]"
encap='vlan-4' ifInstT='sub-interface' addr="201.2.1.1/30" />
      <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-1/paths-202/pathep-[eth1/2]"
encap='vlan-4' ifInstT='sub-interface' addr="202.1.1.1/30" />
      <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-2/paths-203/pathep-[eth1/1]"
encap='vlan-4' ifInstT='sub-interface' addr="203.1.1.1/30" />
      <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-2/paths-203/pathep-[eth1/2]"
encap='vlan-4' ifInstT='sub-interface' addr="203.2.1.1/30" />
      <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-2/paths-204/pathep-[eth4/31]"
encap='vlan-4' ifInstT='sub-interface' addr="204.1.1.1/30" />

    <ospfIfP>
      <ospfRsIfPol tnOspfIfPolName='ospfIfPol' />
  </l3extOut>
</fvTenant>
```

```

        </ospfIfP>

    </l3extLIfP>
</l3extLNodeP>

    <l3extInstP descr="" matchT="AtleastOne" name="instp1" prio="unspecified"
targetDscp="unspecified">
        <fvRsCustQosPol tnQosCustomPolName=""/>
    </l3extInstP>
</l3extOut>

<fvFabricExtConnP descr="" id="1" name="Fabric_Ext_Conn_Pol1" rt="extended:as2-nn4:5:16" status='>

    <fvPodConnP descr="" id="1" name="">
        <fvIp addr="100.11.1.1/32"/>
    </fvPodConnP>
    <fvPodConnP descr="" id="2" name="">
        <fvIp addr="200.11.1.1/32"/>
    </fvPodConnP>
    <fvPeeringP descr="" name="" ownerKey="" ownerTag="" type="automatic_with_full_mesh"/>
    <l3extFabricExtRoutingP descr="" name="ext_routing_prof_1" ownerKey="" ownerTag="">
        <l3extSubnet aggregate="" descr="" ip="100.0.0.0/8" name="" scope="import-security"/>
        <l3extSubnet aggregate="" descr="" ip="200.0.0.0/8" name="" scope="import-security"/>
        <l3extSubnet aggregate="" descr="" ip="201.1.0.0/16" name="" scope="import-security"/>
        <l3extSubnet aggregate="" descr="" ip="201.2.0.0/16" name="" scope="import-security"/>
        <l3extSubnet aggregate="" descr="" ip="202.1.0.0/16" name="" scope="import-security"/>
        <l3extSubnet aggregate="" descr="" ip="203.1.0.0/16" name="" scope="import-security"/>
        <l3extSubnet aggregate="" descr="" ip="203.2.0.0/16" name="" scope="import-security"/>
        <l3extSubnet aggregate="" descr="" ip="204.1.0.0/16" name="" scope="import-security"/>
    </l3extFabricExtRoutingP>
</fvFabricExtConnP>
</fvTenant>
</polUni>

```

REST API を使用したリモート リーフ スイッチの設定

REST API を使用したリモート リーフ スイッチの設定

Cisco APIC を有効にして IPN ルータとリモートリーフ スイッチを検出し接続するには、このトピックの手順を実行します。

この例では、マルチポッド トポロジで、ポッドにリモートリーフ スイッチが接続されていることを前提としています。VRF オーバーレイ 1 とともに、インフラ テナントに設定されている 2 個の L3Outs が含まれます。

- 1 個は VLAN 4 に設定され、リモートリーフ スイッチとスパイン スイッチ両方が WAN ルータに接続されている必要があります。
- 1 個はマルチポッド内部 L3Out が VLAN5 で設定されており、一緒に展開する場合はマルチポッドとリモートリーフ機能に必要です。

ステップ 1 ポッドに接続されるように 2 個のリモートリーフ スイッチに TEP プールを定義するには、次の例のように XML で POST を送信します。

例 :

```
<fabricSetupPol>
  <fabricSetupP tepPool="10.0.0.0/16" podId="1" >
    <fabricExtSetupP tepPool="30.0.128.0/20" extPoolId="1"/>
  </fabricSetupP>
  <fabricSetupP tepPool="10.1.0.0/16" podId="2" >
    <fabricExtSetupP tepPool="30.1.128.0/20" extPoolId="1"/>
  </fabricSetupP>
</fabricSetupPol>
```

ステップ 2 ノードのアイデンティティポリシーを定義するには、次の例のように XML で POST を送信します。

例 :

```
<fabricNodeIdentPol>
  <fabricNodeIdentP serial="SAL17267Z7W" name="leaf1" nodeId="101" podId="1"
  extPoolId="1" nodeType="remote-leaf-wan"/>
  <fabricNodeIdentP serial="SAL17267Z7X" name="leaf2" nodeId="102" podId="1"
  extPoolId="1" nodeType="remote-leaf-wan"/>
  <fabricNodeIdentP serial="SAL17267Z7Y" name="leaf3" nodeId="201" podId="1"
  extPoolId="1" nodeType="remote-leaf-wan"/>
  <fabricNodeIdentP serial="SAL17267Z7Z" name="leaf4" nodeId="201" podId="1"
  extPoolId="1" nodeType="remote-leaf-wan"/>
</fabricNodeIdentPol>
```

ステップ 3 ファブリック外部接続プロファイルを設定するには、次の例のように XML で POST を送信します。

例 :

```
<?xml version="1.0" encoding="UTF-8"?>
<imdata totalCount="1">
  <fvFabricExtConnP dn="uni/tn-infra/fabricExtConnP-1" id="1" name="Fabric_Ext_Conn_Pol1"
  rt="extended:as2-nn4:5:16" siteId="0">
    <l3extFabricExtRoutingP name="test">
      <l3extSubnet ip="150.1.0.0/16" scope="import-security"/>
    </l3extFabricExtRoutingP>
    <l3extFabricExtRoutingP name="ext_routing_prof_1">
      <l3extSubnet ip="204.1.0.0/16" scope="import-security"/>
      <l3extSubnet ip="209.2.0.0/16" scope="import-security"/>
      <l3extSubnet ip="202.1.0.0/16" scope="import-security"/>
      <l3extSubnet ip="207.1.0.0/16" scope="import-security"/>
      <l3extSubnet ip="200.0.0.0/8" scope="import-security"/>
      <l3extSubnet ip="201.2.0.0/16" scope="import-security"/>
      <l3extSubnet ip="210.2.0.0/16" scope="import-security"/>
      <l3extSubnet ip="209.1.0.0/16" scope="import-security"/>
      <l3extSubnet ip="203.2.0.0/16" scope="import-security"/>
      <l3extSubnet ip="208.1.0.0/16" scope="import-security"/>
      <l3extSubnet ip="207.2.0.0/16" scope="import-security"/>
      <l3extSubnet ip="100.0.0.0/8" scope="import-security"/>
      <l3extSubnet ip="201.1.0.0/16" scope="import-security"/>
      <l3extSubnet ip="210.1.0.0/16" scope="import-security"/>
      <l3extSubnet ip="203.1.0.0/16" scope="import-security"/>
      <l3extSubnet ip="208.2.0.0/16" scope="import-security"/>
    </l3extFabricExtRoutingP>
    <fvPodConnP id="1">
      <fvIp addr="100.11.1.1/32"/>
    </fvPodConnP>
    <fvPodConnP id="2">
      <fvIp addr="200.11.1.1/32"/>
    </fvPodConnP>
    <fvPeeringP type="automatic_with_full_mesh"/>
  </fvFabricExtConnP>
</imdata>
```

ステップ 4 VLAN 4 で L3Out を設定するには、リモートリーフスイッチとスパインスイッチ両方が WAN ルータに接続され、次の例のように XML を入力する必要があります。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<polUni>
<fvTenant name="infra">
  <l3extOut name="rleaf-wan-test">
    <ospfExtP areaId="0.0.0.5"/>
    <bgpExtP/>
    <l3extRsEctx tnFvCtxName="overlay-1"/>
    <l3extRsL3DomAtt tDn="uni/l3dom-l3extDom1"/>
    <l3extProvLbl descr="" name="prov_mpl" ownerKey="" ownerTag="" tag="yellow-green"/>
    <l3extLNodeP name="rleaf-101">
      <l3extRsNodeL3OutAtt rtrId="202.202.202.202" tDn="topology/pod-1/node-101">
        </l3extRsNodeL3OutAtt>
        <l3extLIfP name="portIf">
          <l3extRsPathL3OutAtt ifInstT="sub-interface" tDn="topology/pod-1/paths-101/pathep-[eth1/49]"
            addr="202.1.1.2/30" mac="AA:11:22:33:44:66" encap='vlan-4'/>
          <ospfIfP>
            <ospfRsIfPol tnOspfIfPolName='ospfIfPol'/>
          </ospfIfP>
        </l3extLIfP>
      </l3extLNodeP>
    <l3extLNodeP name="rlSpine-201">
      <l3extRsNodeL3OutAtt rtrId="201.201.201.201" rtrIdLoopBack="no" tDn="topology/pod-1/node-201">
        <!--
        <l3extLoopBackIfP addr="201::201/128" descr="" name=""/>
        <l3extLoopBackIfP addr="201.201.201.201/32" descr="" name=""/>
        -->
        <l3extLoopBackIfP addr=":" />
      </l3extRsNodeL3OutAtt>
      <l3extLIfP name="portIf">
        <l3extRsPathL3OutAtt ifInstT="sub-interface" tDn="topology/pod-1/paths-201/pathep-[eth8/36]"
          addr="201.1.1.1/30" mac="00:11:22:33:77:55" encap='vlan-4'/>
        <ospfIfP>
          <ospfRsIfPol tnOspfIfPolName='ospfIfPol'/>
        </ospfIfP>
      </l3extLIfP>
    </l3extLNodeP>
    <l3extInstP descr="" matchT="AtleastOne" name="instp1" prio="unspecified" targetDscp="unspecified">
      <fvRsCustQosPol tnQosCustomPolName=""/>
    </l3extInstP>
  </l3extOut>
  <ospfIfPol name="ospfIfPol" nwT="bcast"/>
</fvTenant>
</polUni>
```

ステップ 5 リリース 4.1(2) 以前で、VLAN-5 でマルチポッド L3Out を設定するには、マルチポッドとリモートリーフトポロジの両方と、次の例のように XML を送信する必要があります。

(注) リリース 4.1(2) 以降を実行している新しいリモートリーフスイッチを導入し、それらのリモートリーフスイッチで直接トラフィック転送をイネーブルにする場合は、この情報を入力しないでください。この場合、マルチポッドに VLAN-5 を使用して OSPF インスタンスを設定する必要はありません。詳細については、「[ダイレクトトラフィックフォワーディングについて \(159 ページ\)](#)」を参照してください。

例：

```

<?xml version="1.0" encoding="UTF-8"?>
<polUni>

  <fvTenant name="infra" >
    <l3extOut name="ipn-multipodInternal">
      <ospfExtP areaCtrl="inherit-ipsec,redistribute,summary" areaId="0.0.0.5" multipodInternal="yes"
/>
      <l3extRsEctx tnFvCtxName="overlay-1" />
      <l3extLNodeP name="bLeaf">
        <l3extRsNodeL3OutAtt rtrId="202.202.202.202" rtrIdLoopBack="no" tDn="topology/pod-2/node-202">

          <l3extLoopBackIfP addr="202.202.202.212"/>
        </l3extRsNodeL3OutAtt>
        <l3extRsNodeL3OutAtt rtrId="102.102.102.102" rtrIdLoopBack="no" tDn="topology/pod-1/node-102">

          <l3extLoopBackIfP addr="102.102.102.112"/>
        </l3extRsNodeL3OutAtt>
        <l3extLIfP name="portIf">
          <ospfIfP authKeyId="1" authType="none">
            <ospfRsIfPol tnOspfIfPolName="ospfIfPol" />
          </ospfIfP>
          <l3extRsPathL3OutAtt addr="10.0.254.233/30" encap="vlan-5" ifInstT="sub-interface"
tDn="topology/pod-2/paths-202/pathep-[eth5/2]"/>
          <l3extRsPathL3OutAtt addr="10.0.255.229/30" encap="vlan-5" ifInstT="sub-interface"
tDn="topology/pod-1/paths-102/pathep-[eth5/2]"/>
        </l3extLIfP>
      </l3extLNodeP>
      <l3extInstP matchT="AtleastOne" name="ipnInstP" />
    </l3extOut>
  </fvTenant>
</polUni>

```

REST API を使用した SR-MPLS ハンドオフの設定

REST API を使用した SR-MPLS インフラ L3Out の設定

- SR-MPLS インフラ L3Out は、境界リーフスイッチで設定され、SR-MPLS ハンドオフに必要なアンダーレイ BGP-LU およびオーバーレイ MP-BGP/EVPN セッションを設定するために使用されます。
- SR-MPLS インフラ L3Out は、ポッドまたはリモートリーフスイッチサイトにスコープされます。
- 1つの SR-MPLS インフラ L3Out 内の境界リーフスイッチまたはリモートリーフスイッチは、1つ以上のルーティングドメイン内の1つ以上のプロバイダーエッジ (PE) ルータに接続できます。
- ポッドまたはリモートリーフスイッチサイトには、1つ以上の SR-MPLS インフラ L3Out を設定できます。
- 各 SR-MPLS インフラ L3Out には、一意のプロバイダーラベルと1つのプロバイダーラベルのみが必要です。各 SR-MPLS インフラ L3Out は、プロバイダーラベルによって識別されます。

SR-MPLS インフラ L3Out を設定する場合は、次の項目を設定します。

• ノード

- リーフスイッチのみが SR-MPLS インフラ L3Out のノードとして設定できます（境界リーフスイッチおよびリモートリーフスイッチ）。
- 各 SR-MPLS インフラ L3Out は、1つのポッドからの境界リーフスイッチまたは同じサイトからのリモートリーフスイッチを持つことができます。
- 各境界リーフスイッチまたはリモートリーフスイッチは、複数の SR-MPLS ドメインに接続する場合、複数の SR-MPLS インフラ L3Out で設定できます。
- また、ノードの下にループバックインターフェイスを設定し、ループバックインターフェイスの下にノード SID ポリシーを設定します。

• インターフェイス

- サポートされるインターフェイスのタイプは次のとおりです。
 - ルーテッドインターフェイスまたはサブインターフェイス
 - ルーテッドポートチャネルまたはポートチャネルサブインターフェイス
- サブインターフェイスでは、任意の VLAN タグがサポートされます。
- また、SR-MPLS infra L3Out のインターフェイスエリアの下にアンダーレイ BGP ピアポリシーを設定します。

• QoS ルール

- MPLS 入力ルールと MPLS 出力ルールは、SR-MPLS インフラ L3Out の MPLS QoS ポリシーを使用して設定できます。
- MPLS QoS ポリシーを作成しない場合、入力 MPLS トラフィックにはデフォルトの QoS レベルが割り当てられます。

また、SR-MPLS インフラ L3Out を使用してアンダーレイとオーバーレイを設定します。

- アンダーレイ：インターフェイス設定の一部としての BGP ピア IP (BGPLU ピア) 設定。
- オーバーレイ：論理ノードプロファイル設定の一部としての MP-BGPEVPN リモート IPv4 アドレス (MP-BGP EVPN ピア) 設定。

始める前に

- [注意事項と制約事項 \(189 ページ\)](#) で提供されている SR-MPLS ガイドラインと制約事項を確認します。特に、[SR-MPLS インフラ L3Out のガイドラインと制約事項 \(190 ページ\)](#) で提供されているガイドラインと制約事項を確認してください。
- (任意) 必要に応じて、の手順を使用して MPLS カスタム QoS ポリシーを設定します。[REST API を使用した SR-MPLS カスタム QoS ポリシー \(577 ページ\)](#)

- ユーザテナント VRF は SR-MPLS インフラ L3Out にマッピングされ、テナントブリッジドメインサブネットを DC-PE ルータにアドバタイズし、DC-PE から受信した MPLS VPN ルートをインポートします。
- 各 VRF の SR-MPLS VRF L3Out でルーティングポリシーとセキュリティポリシーを指定する必要があります。これらのポリシーは、1つ以上の SR-MPLS インフラ L3Out をポイントします。
- VRF ごとに1つの SR-MPLS VRF L3Out がサポートされます。
- 1つの SR-MPLS VRF L3Out で複数のコンシューマラベルを設定でき、各コンシューマラベルで1つの SR-MPLS インフラ L3Out を識別できます。コンシューマラベルは、特定のポッドまたはリモートリーフスイッチの特定の MPLS ドメインである1つの SR-MPLS VRF L3Out との間のトラフィックのエントリポイントと出口ポイントを識別します。

始める前に

- [注意事項と制約事項 \(189 ページ\)](#) で提供されている SR-MPLS ガイドラインと制約事項を確認します。特に、[SR-MPLS VRF L3Out のガイドラインと制約事項 \(190 ページ\)](#) で提供されているガイドラインと制約事項を確認してください。
- [REST API を使用した SR-MPLS インフラ L3Out の設定 \(573 ページ\)](#) の手順に従って、SR-MPLS インフラ L3Out を設定します。

次のような情報が表示されます。

```
<polUni>
<fvTenant name="t1">
  <fvCtx name="v1">
    <!-- specify bgp evpn route-target -->
    <bgpRtTargetP af="ipv4-ucast">
      <bgpRtTarget rt="route-target:as4-nn2:100:1259" type="import"/>
      <bgpRtTarget rt="route-target:as4-nn2:100:1259" type="export"/>
    </bgpRtTargetP>
  </fvCtx>

  <!-- MPLS L3out -->
  <l3extOut name="out1" mplsEnabled="yes">
    <l3extRsEctx tnFvCtxName="v1" />

    <!-- MPLS consumer label -->
    <l3extConsLbl name="mpls1">
      <!-- route profile association -->
      <l3extRsLblToProfile tDn="uni/tn-t1/prof-rp1" direction="export" />
      <!-- InstP association -->
      <l3extRsLblToInstP tDn="uni/tn-t1/out-out1/instP-epgMpls1" />
    </l3extConsLbl>

    <!-- External-EPG -->
    <l3extInstP name="epgMpls1">
      <fvRsProv tnVzBrCPName="cp1"/>
      <l3extSubnet ip="55.1.1.1/28"/>
    </l3extInstP>
  </bgpExtP/>
```

```
</l3extOut>

<!-- route control profile -->
<rtctrlProfile descr="" name="rpl" type="global" status="">
  <rtctrlCtxP action="permit" descr="" name="ctx1" order="0">
    <rtctrlRsCtxPToSubjP status="" tnRtctrlSubjPName="subj1"/>
  </rtctrlCtxP>
</rtctrlProfile>
<rtctrlSubjP descr="" name="subj1" status="" >
  <rtctrlMatchRtDest ip="101.1.1.1/32"/>
  <rtctrlMatchRtDest ip="102.1.1.0/24" aggregate="yes"/>
</rtctrlSubjP>

<!-- Filter and Contract (global) -->
<vzBrCP name="cpl" scope="global">
  <vzSubj name="allow-all">
    <vzRsSubjFiltAtt action="permit" tnVzFilterName="default" />
  </vzSubj>
</vzBrCP>
</fvTenant>
</polUni>
```

REST API を使用した SR-MPLS カスタム QoS ポリシー

SR MPLS カスタム QoS ポリシーは、MPLS QoS 出力 ポリシーで定義された着信 MPLS EXP 値に基づいて、SR-MPLS ネットワークから送信されるパケットのプライオリティを定義します。これらのパケットは、ACI ファブリック内にあります。また、MPLS QoS 出力ポリシーで定義された IPv4 DSCP 値に基づく MPLS インターフェイスを介して ACI ファブリックから離れるパケットの CoS 値および MPLS EXP 値をマーキングします。

カスタム出力ポリシーが定義されていない場合、デフォルトの QoS レベル (Level13) がファブリック内のパケットに割り当てられます。カスタム出力ポリシーが定義されていない場合、デフォルトの EXP 値 (0) がファブリックから離れるパケットにマーキングされます。

ステップ 1 SR-MPLS QoS ポリシーの作成

次のPOSTで、

- *customqos1* を、作成する SR-MPLS QoS ポリシーの名前に置き換えます。
- *qosMplsIngressRule* の場合：
 - *from = "2" to = "3"* を、ポリシーに一致させる EXP 範囲に置き換えます。
 - *prio = "level5"* を ACI ファブリック内にあるパケットの ACI QoS レベルに置き換えます。
 - *target = "CS5"* は、パケットが一致したときに設定する DSCP 値に置き換えます。
 - *targetCos = "4"* を、パケットが一致したときにパケットに設定する CoS 値に置き換えます。
- *qosMplsEgressRule* の場合：
 - *from = "CS2" to = "CS4"* を、ポリシーを照合する DSCP 範囲に置き換えます。

- targetExp = "5" を、パケットがファブリックを離れるときに設定する EXP 値に置き換えます。
- targetCos = "3" を、パケットがファブリックを離れるときに設定する CoS 値に置き換えます。

```
<polUni>
  <fvTenant name="infra">
    <qosMplsCustomPol descr="" dn="uni/tn-infra/qosmplscustom-customqos1" name="customqos1" status=""
  >
    <qosMplsIngressRule from="2" to="3" prio="level5" target="CS5" targetCos="4" status="" />
    <qosMplsEgressRule from="CS2" to="CS4" targetExp="5" targetCos="3" status="" />
  </qosMplsCustomPol>
</fvTenant>
</polUni>
```

ステップ2 SR-MPLS QoS ポリシーの作成

次の POST で、customqos1 を前の手順で作成した SR-MPLS QoS ポリシーの名前に置き換えます。

```
<polUni>
  <fvTenant name="infra">
    <l3extOut name="mplsOut" status="" descr="bl">
      <l3extLNodeP name="mplsLNP" status=""
        <l3extRsLNodePMplsCustQosPol tDn="uni/tn-infra/qosmplscustom-customqos1"/>
      </l3extLNodeP>
    </l3extOut>
  </fvTenant>
</polUni>
```

パートII：外部ルーティング（L3Out）の設定

外部ネットワークへのルーテッド接続

REST API を使用した MP-BGP ルート リフレクタの設定

REST API を使用した MP-BGP ルート リフレクタの設定

ステップ1 スパイン スイッチをルート リフレクタとしてマークします。

例：

POST <https://apic-ip-address/api/policymgr/mo/uni/fabric.xml>

```
<bgpInstPol name="default">
  <bgpAsP asn="1" />
  <bgpRRP>
    <bgpRRNodePEp id="\<spine_id1\>"/>
    <bgpRRNodePEp id="\<spine_id2\>"/>
  </bgpRRP>
</bgpInstPol>
```

ステップ2 次のポストを使用してポッドセレクタをセットアップします。

例 :

FuncP セットアップの場合 :

```
POST https://apic-ip-address/api/policymgr/mo/uni.xml

<fabricFuncP>
  <fabricPodPGrp name="bgpRRPodGrp">
    <fabricRsPodPGrpBGPRRP tnBgpInstPolName="default" />
  </fabricPodPGrp>
</fabricFuncP>
```

例 :

PodP セットアップの場合 :

```
POST https://apic-ip-address/api/policymgr/mo/uni.xml

<fabricPodP name="default">
  <fabricPodS name="default" type="ALL">
    <fabricRsPodPGrp tDn="uni/fabric/funcprof/podpgrp-bgpRRPodGrp"/>
  </fabricPodS>
</fabricPodP>
```

REST API を使用したループ防止のための BGP ドメインパス機能の設定

始める前に

[ループ防止のための BGP ドメインパス機能について \(223 ページ\)](#) に記載されている情報を使用して、BGP ドメインパス機能に精通します。

ステップ 1 ループ防止に BGP ドメインパス機能を使用する場合は、グローバル `DomainIdBase` を設定します。

```
<polUni>
  <fabricInst>
    <bgpInstPol name="default">
      <bgpDomainIdBase domainIdBase="12346" />
    </bgpInstPol>
  </fabricInst>
</polUni>
```

ステップ 2 適切な L3Out で `send-domain-path` を有効にします。

```
<bgpPeerP addr="22.22.3.5" addrTCtrl="af-uicast" allowedSelfAsCnt="3" ttl="2"
  ctrlExt="send-domain-path" ctrl="send-ext-com">
</bgpPeerP>
```

L3Out のノードとインターフェイス

REST API を使用したレイヤ 3 ルーテッド ポート チャネルとサブインターフェイス ポート チャネルの設定

REST API を使用したレイヤ 3 ルーテッド ポート チャネルの設定

始める前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが ACI ファブリックに登録され、使用可能であること。
- ポートチャネルは、L3Out インターフェイスにポートチャネルが使用される場合に設定されます。



(注) 次の REST API 例では、長い 1 行のテキストは \ で分けて読みやすくします。

REST API を使用して以前作成したポートチャネルにレイヤ 3 ルートを設定するには、次のように XML で post を送信します。

例 :

```
<polUni>
<fvTenant name=pep9>
  <l3extOut descr="" dn="uni/tn-pep9/out-routAccounting" enforceRtctrl="export" \
name="routAccounting" nameAlias="" ownerKey="" ownerTag="" \
targetDscp="unspecified">
    <l3extRsL3DomAtt tDn="uni/l3dom-Dom1"/>
    <l3extRsEctx tnFvCtxName="ctx9"/>
    <l3extLNodeP configIssues="" descr="" name="node101" nameAlias="" ownerKey="" \
ownerTag="" tag="yellow-green" targetDscp="unspecified">
      <l3extRsNodeL3OutAtt rtrId="10.1.0.101" rtrIdLoopBack="yes" \
tDn="topology/pod-1/node-101">
        <l3extInfraNodeP descr="" fabricExtCtrlPeering="no" \
fabricExtIntersiteCtrlPeering="no" name="" nameAlias="" spineRole=""/>
      </l3extRsNodeL3OutAtt>
    <l3extLIIfP descr="" name="lifpl7" nameAlias="" ownerKey="" ownerTag="" \
tag="yellow-green">
      <ospfIfP authKeyId="1" authType="none" descr="" name="" nameAlias="">
        <ospfRsIfPol tnOspfIfPolName=""/>
      </ospfIfP>
    <l3extRsPathL3OutAtt addr="10.1.5.3/24" autostate="disabled" descr="" \
encap="unknown" encapScope="local" ifInstT="l3-port" llAddr="::" \
mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit" \
tDn="topology/pod-1/paths-101/pathep-[pol17_PolGrp]" \
targetDscp="unspecified"/>
  </l3extOut>
</fvTenant>
</polUni>
```

```

        <l3extRsNdIfPol tnNdIfPolName=""/>
        <l3extRsIngressQosDppPol tnQosDppPolName=""/>
        <l3extRsEgressQosDppPol tnQosDppPolName=""/>
    </l3extLIfP>
</l3extLNodeP>
<l3extInstP descr="" floodOnEncap="disabled" matchT="AtleastOne" \
name="accountingInst" nameAlias="" prefGrMemb="exclude" prio="unspecified" \
targetDscp="unspecified">
    <fvRsProv matchT="AtleastOne" prio="unspecified" tnVzBrCPName="webCtrct"/>
    <l3extSubnet aggregate="export-rtctrl,import-rtctrl" descr="" ip="0.0.0.0/0" \
name="" nameAlias="" scope="export-rtctrl,import-rtctrl,import-security"/>
    <l3extSubnet aggregate="export-rtctrl,import-rtctrl" descr="" ip="::/0" \
name="" nameAlias="" scope="export-rtctrl,import-rtctrl,import-security"/>
    <fvRsCustQosPol tnQosCustomPolName=""/>
</l3extInstP>
<l3extConsLbl descr="" name="golf" nameAlias="" owner="infra" ownerKey="" \
ownerTag="" tag="yellow-green"/>
</l3extOut>
</fvTenant>
</polUni>

```

REST API を使用して、レイヤ3 サブインターフェイス ポート チャネルの設定

始める前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが ACI ファブリックに登録され、使用可能であること。
- ポートチャネルは、「REST API を使用したポートチャネルの設定」の手順を使用して設定されます。



(注) 次の REST API 例では、1 つ以上の行のテキストはで区分するが、\ 読みやすさを改善する文字。

REST API を使用して、以前に作成したポートチャネルをレイヤ3 サブインターフェイス ルートを設定するには、次のようには、XML で post を送信します。

例 :

```

<polUni>
<fvTenant name=pep9>
  <l3extOut descr="" dn="uni/tn-pep9/out-routAccounting" enforceRtctrl="export" \
name="routAccounting" nameAlias="" ownerKey="" ownerTag="" targetDscp="unspecified">
    <l3extRsL3DomAtt tDn="uni/l3dom-Dom1"/>
    <l3extRsEctx tnFvCtxName="ctx9"/>
    <l3extLNodeP configIssues="" descr="" name="node101" nameAlias="" ownerKey="" \
ownerTag="" tag="yellow-green" targetDscp="unspecified">

```

```

<l3extRsNodeL3OutAtt rtrId="10.1.0.101" rtrIdLoopBack="yes" \
  tDn="topology/pod-1/node-101">
  <l3extInfraNodeP descr="" fabricExtCtrlPeering="no" \
    fabricExtIntersiteCtrlPeering="no" name="" nameAlias="" spineRole=""/>
</l3extRsNodeL3OutAtt>
<l3extLIfP descr="" name="lifp27" nameAlias="" ownerKey="" ownerTag="" \
  tag="yellow-green">
  <ospfIfP authKeyId="1" authType="none" descr="" name="" nameAlias="">
    <ospfRsIfPol tnOspfIfPolName=""/>
  </ospfIfP>
  <l3extRsPathL3OutAtt addr="11.1.5.3/24" autostate="disabled" descr="" \
    encap="vlan-2001" encapScope="local" ifInstT="sub-interface" \
    llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit" \
    tDn="topology/pod-1/paths-101/pathep-[po27_PolGrp]" \
    targetDscp="unspecified"/>
  <l3extRsNdIfPol tnNdIfPolName=""/>
  <l3extRsIngressQosDppPol tnQosDppPolName=""/>
  <l3extRsEgressQosDppPol tnQosDppPolName=""/>
</l3extLIfP>
</l3extLNodeP>
<l3extInstP descr="" floodOnEncap="disabled" matchT="AtleastOne" \
  name="accountingInst" nameAlias="" prefGrMemb="exclude" prio="unspecified" \
  targetDscp="unspecified">
  <fvRsProv matchT="AtleastOne" prio="unspecified" tnVzBrCPName="webCtrct"/>
  <l3extSubnet aggregate="export-rtctrl,import-rtctrl" descr="" ip="0.0.0.0/0" \
    name="" nameAlias="" scope="export-rtctrl,import-rtctrl,import-security"/>
  <l3extSubnet aggregate="export-rtctrl,import-rtctrl" descr="" ip="::/0" \
    name="" nameAlias="" scope="export-rtctrl,import-rtctrl,import-security"/>
  <fvRsCustQosPol tnQosCustomPolName=""/>
</l3extInstP>
<l3extConsLbl descr="" name="golf" nameAlias="" owner="infra" ownerKey="" \
  ownerTag="" tag="yellow-green"/>
</l3extOut>
</fvTenant>
</polUni>

```

REST API を使用したスイッチ仮想インターフェイスの設定

REST API を使用して、SVI インターフェイスのカプセル化スコープの設定

始める前に

インターフェイス セレクタが設定されます。

SVI インターフェイスのカプセル化の範囲を設定します。

例 :

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- /api/node/mo/.xml -->
<polUni>
  <fvTenant name="coke">
    <l3extOut descr="" dn="uni/tn-coke/out-l3out1" enforceRtctrl="export" name="l3out1" nameAlias=""
      ownerKey="" ownerTag="" targetDscp="unspecified">
      <l3extRsL3DomAtt tDn="uni/l3dom-Dom1"/>
      <l3extRsEctx tnFvCtxName="vrf0"/>
      <l3extLNodeP configIssues="" descr="" name="__ui_node_101" nameAlias="" ownerKey="" ownerTag=""

```

```

tag="yellow-green" targetDscp="unspecified">
  <l3extRsNodeL3OutAtt rtrId="1.1.1.1" rtrIdLoopBack="no" tDn="topology/pod-1/node-101"/>
  <l3extLIIfP descr="" name="int1_11" nameAlias="" ownerKey="" ownerTag="" tag="yellow-green">
    <l3extRsPathL3OutAtt addr="1.2.3.4/24" descr="" encap="vlan-2001" encapScope="ctx"
ifInstT="ext-svi" llAddr="0.0.0.0" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
tDn="topology/pod-1/paths-101/pathep-[eth1/5]" targetDscp="unspecified"/>
    <l3extRsNdIfPol tnNdIfPolName=""/>
    <l3extRsIngressQosDppPol tnQosDppPolName=""/>
    <l3extRsEgressQosDppPol tnQosDppPolName=""/>
  </l3extLIIfP>
</l3extLNodeP>
  <l3extInstP descr="" matchT="AtleastOne" name="epg1" nameAlias="" prefGrMemb="exclude"
prio="unspecified" targetDscp="unspecified">
    <l3extSubnet aggregate="" descr="" ip="101.10.10.1/24" name="" nameAlias=""
scope="import-security"/>
    <fvRsCustQosPol tnQosCustomPolName=""/>
  </l3extInstP>
</l3extOut>
</fvTenant>
</polUni>

```

REST API を使用した SVI 自動状態の設定

始める前に

- テナントと VRF が設定されています。
- レイヤ3アウトが設定されており、レイヤ3アウトの論理ノードプロファイルと論理インターフェイス プロファイルが設定されています。

SVI の自動状態の値を有効にします。

例 :

```

<fvTenant name="t1" >
  <l3extOut name="out1">
    <l3extLNodeP name="__ui_node_101" >
      <l3extLIIfP descr="" name="__ui_eth1_10_vlan_99_af_ipv4" >
        <l3extRsPathL3OutAtt addr="19.1.1.1/24" autostate="enabled" descr="" encap="vlan-100"
encapScope="local" ifInstT="ext-svi" llAddr=":" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
tDn="topology/pod-1/paths-101/pathep-[eth1/10]" targetDscp="unspecified" />
      </l3extLIIfP>
    </l3extLNodeP>
  </l3extOut>
</fvTenant>

```

自動状態を無効にするには、上記の例では無効に値を変更する必要があります。例 : autostate="disabled".

REST API を使用したルーティング プロトコルの設定

REST API を使用した BFD サポート付き BGP 外部ルーテッド ネットワークの設定

REST API を使用した BGP 外部ルーテッド ネットワークの設定

始める前に

外部ルーテッド ネットワークを設定するテナントがすでに作成されていること。

ここでは、REST API を使用して BGP 外部ルーテッド ネットワークを設定する方法を示します。

例：

例：

```
<l3extOut descr="" dn="uni/tn-t1/out-l3out-bgp" enforceRtctrl="export" name="l3out-bgp" ownerKey=""
ownerTag="" targetDscp="unspecified">
  <l3extRsEctx tnFvCtxName="ctx3"/>
  <l3extLNodeP configIssues="" descr="" name="l3extLNodeP_1" ownerKey="" ownerTag="" tag="yellow-green"
targetDscp="unspecified">
    <l3extRsNodeL3OutAtt rtrId="1.1.1.1" rtrIdLoopBack="no" tDn="topology/pod-1/node-101"/>
    <l3extLIIfP descr="" name="l3extLIIf_2" ownerKey="" ownerTag="" tag="yellow-green">
      <l3extRsNdIfPol tnNdIfPolName=""/>
      <l3extRsIngressQosDppPol tnQosDppPolName=""/>
      <l3extRsEgressQosDppPol tnQosDppPolName=""/>
      <l3extRsPathL3OutAtt addr="3001::31:0:1:2/120" descr="" encap="vlan-3001" encapScope="local"
ifInstT="sub-interface" llAddr=":" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
tDn="topology/pod-1/paths-101/pathep-[eth1/8]" targetDscp="unspecified">
        <bgpPeerP addr="3001::31:0:1:0/120" allowedSelfAsCnt="3" ctrl="send-com,send-ext-com" descr=""
name="" peerCtrl="" privateASctrl="remove-all,remove-exclusive,replace-as" ttl="1" weight="1000">
          <bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
          <bgpAsP asn="3001" descr="" name=""/>
        </bgpPeerP>
      </l3extRsPathL3OutAtt>
    </l3extLIIfP>
  <l3extLIIfP descr="" name="l3extLIIf_1" ownerKey="" ownerTag="" tag="yellow-green">
    <l3extRsNdIfPol tnNdIfPolName=""/>
    <l3extRsIngressQosDppPol tnQosDppPolName=""/>
    <l3extRsEgressQosDppPol tnQosDppPolName=""/>
    <l3extRsPathL3OutAtt addr="31.0.1.2/24" descr="" encap="vlan-3001" encapScope="local"
ifInstT="sub-interface" llAddr=":" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
tDn="topology/pod-1/paths-101/pathep-[eth1/8]" targetDscp="unspecified">
      <bgpPeerP addr="31.0.1.0/24" allowedSelfAsCnt="3" ctrl="send-com,send-ext-com" descr="" name=""
peerCtrl="" privateASctrl="remove-all,remove-exclusive,replace-as" ttl="1" weight="100">
        <bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
        <bgpLocalAsnP asnPropagate="none" descr="" localAsn="200" name=""/>
        <bgpAsP asn="3001" descr="" name=""/>
      </bgpPeerP>
    </l3extRsPathL3OutAtt>
  </l3extLIIfP>
</l3extLNodeP>
<l3extRsL3DomAtt tDn="uni/l3dom-l3-dom"/>
<l3extRsDampeningPol af="ipv6-ucast" tnRtctrlProfileName="damp_rp"/>
<l3extRsDampeningPol af="ipv4-ucast" tnRtctrlProfileName="damp_rp"/>
```

```

<l3extInstP descr="" matchT="AtleastOne" name="l3extInstP_1" prio="unspecified"
targetDscp="unspecified">
  <l3extSubnet aggregate="" descr="" ip="130.130.130.0/24" name="" scope="import-rtctrl"></l3extSubnet>

  <l3extSubnet aggregate="" descr="" ip="130.130.131.0/24" name="" scope="import-rtctrl"/>
  <l3extSubnet aggregate="" descr="" ip="120.120.120.120/32" name=""
scope="export-rtctrl,import-security"/>
  <l3extSubnet aggregate="" descr="" ip="3001::130:130:130:100/120" name="" scope="import-rtctrl"/>

</l3extInstP>
<bgpExtP descr=""/>
</l3extOut>
<rtctrlProfile descr="" dn="uni/tn-t1/prof-damp_rp" name="damp_rp" ownerKey="" ownerTag=""
type="combinable">
  <rtctrlCtxP descr="" name="ipv4_rpc" order="0">
    <rtctrlScope descr="" name="">
      <rtctrlRsScopeToAttrP tnRtctrlAttrPName="act_rule"/>
    </rtctrlScope>
  </rtctrlCtxP>
</rtctrlProfile>
<rtctrlAttrP descr="" dn="uni/tn-t1/attr-act_rule" name="act_rule">
  <rtctrlSetDamp descr="" halfLife="15" maxSuppressTime="60" name="" reuse="750" suppress="2000"
type="dampening-pol"/>
</rtctrlAttrP>

```

REST API を使用した BGP パスの設定

次のフィールドの許容値については、Cisco APIC ドキュメンテーション ページの 『Verified Scalability Guide for Cisco APIC』 を参照してください。 <https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>

さらに多くのパスを設定できるようにする 2 つのプロパティは、bgpCtxAfPol オブジェクトの maxEcmp と maxEcmpIbgp です。これら 2 つのプロパティを設定した後、実装の残り部分に反映されます。ECMP ポリシーは VRF レベルで適用されます。

次の例では、REST API を使用して BGP 最長パス機能を設定する方法の情報を提供します。

```

<fvTenant descr="" dn="uni/tn-t1" name="t1">
  <fvCtx name="v1">
    <fvRsCtxToBgpCtxAfPol af="ipv4-ucast" tnBgpCtxAfPolName="bgpCtxPol1"/>
  </fvCtx>
  <bgpCtxAfPol name="bgpCtxPol1" maxEcmp="64" maxEcmpIbgp="64"/>
</fvTenant>

```

REST API を使用した AS パス プリペンドの設定

次の例では、REST API を使用した AS パス プリペンド機能を設定する方法の情報を提供します。

```

<?xml version="1.0" encoding="UTF-8"?>
<fvTenant name="coke">
  <rtctrlAttrP name="attrp1">
    <rtctrlSetASPath criteria="prepend">
      <rtctrlSetASPathASN asn="100" order="1"/>
      <rtctrlSetASPathASN asn="200" order="10"/>
    </rtctrlSetASPath>
  </rtctrlAttrP>
</fvTenant>

```

```

        <rtctrlSetASPathASN asn="300" order="5"/>
        <rtctrlSetASPath/>
        <rtctrlSetASPath criteria="prepend-last-as" lastnum="9" />
    </rtctrlAttrP>

    <l3extOut name="out1">
        <rtctrlProfile name="rp1">
            <rtctrlCtxP name="ctxp1" order="1">
                <rtctrlScope>
                    <rtctrlRsScopeToAttrP tnRtctrlAttrPName="attrp1"/>
                </rtctrlScope>
            </rtctrlCtxP>
        </rtctrlProfile>
    </l3extOut>
</fvTenant>

```

REST API を使用した自律システム オーバーライド対応のネットワークのルーティング BGP 外部の設定

手順の概要

1. 自律型オーバーライドを有効にして、BGP 外部ルーテッド ネットワークを設定します。

手順の詳細

自律型オーバーライドを有効にして、BGP 外部ルーテッド ネットワークを設定します。

(注) 太字で表示されているコードの行に設定の BGP AS オーバーライド部分が表示されます。この機能は Cisco APIC リリース 3.1(2m) で導入されました。

例 :

```

<fvTenant name="coke">

    <fvCtx name="coke" status="">
        <bgpRtTargetP af="ipv4-ucast">
            <bgpRtTarget type="import" rt="route-target:as4-nn2:1234:1300" />
            <bgpRtTarget type="export" rt="route-target:as4-nn2:1234:1300" />
        </bgpRtTargetP>
        <bgpRtTargetP af="ipv6-ucast">
            <bgpRtTarget type="import" rt="route-target:as4-nn2:1234:1300" />
            <bgpRtTarget type="export" rt="route-target:as4-nn2:1234:1300" />
        </bgpRtTargetP>
    </fvCtx>

    <fvBD name="cokeBD">
        <!-- Association from Bridge Doamin to Private Network -->
        <fvRsCtx tnFvCtxName="coke" />
        <fvRsBDToOut tnL3extOutName="routAccounting" />
        <!-- Subnet behind the bridge domain-->
        <fvSubnet ip="20.1.1.1/16" scope="public"/>
        <fvSubnet ip="2000:1::1/64" scope="public"/>
    </fvBD>

    <fvBD name="cokeBD2">
        <!-- Association from Bridge Doamin to Private Network -->
        <fvRsCtx tnFvCtxName="coke" />
        <fvRsBDToOut tnL3extOutName="routAccounting" />
        <!-- Subnet behind the bridge domain-->
    </fvBD>

```



```

    <fvSubnet ip="30.1.1.1/16" scope="public"/>

</fvBD>
<vzBrCP name="webCtrct" scope="global">
  <vzSubj name="http">
    <vzRsSubjFiltAtt tnVzFilterName="default"/>
  </vzSubj>
</vzBrCP>

<!-- GOLF L3Out -->
<l3extOut name="routAccounting">
  <l3extConsLbl name="golf_transit" owner="infra" status=""/>
  <bgpExtP/>
  <l3extInstP name="accountingInst">
    <!--
    <l3extSubnet ip="192.2.2.0/24" scope="import-security,import-rtctrl" />
    <l3extSubnet ip="192.3.2.0/24" scope="export-rtctrl"/>
    <l3extSubnet ip="192.5.2.0/24" scope="export-rtctrl"/>
    <l3extSubnet ip="64:ff9b::c007:200/120" scope="export-rtctrl" />
    -->
    <l3extSubnet ip="0.0.0.0/0"
      scope="export-rtctrl,import-security"
      aggregate="export-rtctrl"

    />
    <fvRsProv tnVzBrCPName="webCtrct"/>
  </l3extInstP>

  <l3extRsEctx tnFvCtxName="coke"/>
</l3extOut>

<fvAp name="cokeAp">
  <fvAEPg name="cokeEPg" >
    <fvRsBd tnFvBDName="cokeBD" />
    <fvRsPathAtt tDn="topology/pod-1/paths-103/pathep-[eth1/20]" encap="vlan-100"
instrImedcy="immediate" mode="regular"/>
    <fvRsCons tnVzBrCPName="webCtrct"/>
  </fvAEPg>
  <fvAEPg name="cokeEPg2" >
    <fvRsBd tnFvBDName="cokeBD2" />
    <fvRsPathAtt tDn="topology/pod-1/paths-103/pathep-[eth1/20]" encap="vlan-110"
instrImedcy="immediate" mode="regular"/>
    <fvRsCons tnVzBrCPName="webCtrct"/>
  </fvAEPg>
</fvAp>

<!-- Non GOLF L3Out-->
<l3extOut name="NonGolfOut">
  <bgpExtP/>
  <l3extLNodeP name="bLeaf">
    <!--
    <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="20.1.13.1"/>
    -->
    <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="20.1.13.1">
    <l3extLoopBackIfP addr="1.1.1.1"/>

    <ipRouteP ip="2.2.2.2/32" >
      <ipNextHopP nhAddr="20.1.12.3"/>
    </ipRouteP>

  </l3extRsNodeL3OutAtt>
  <l3extLIIfP name='portIfv4'>
    <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/17]" encap='vlan-1010'

```

REST API を使用した BGP ネイバー シャットダウンおよびソフトリセットの設定

```

ifInstT='sub-interface' addr="20.1.12.2/24">
    </l3extRsPathL3OutAtt>
    </l3extLIIfP>
    <l3extLIIfP name='portIfV6'>
        <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/17]" encap='vlan-1010'
ifInstT='sub-interface' addr="64:ff9b::1401:302/120">
        <bgpPeerP addr="64:ff9b::1401:d03" ctrl="send-com,send-ext-com" />
    </l3extRsPathL3OutAtt>
    </l3extLIIfP>
    <bgpPeerP addr="2.2.2.2" ctrl="as-override,disable-peer-as-check, send-com,send-ext-com"
status=""/>
</l3extLNodeP>
<!--
<bgpPeerP addr="2.2.2.2" ctrl="send-com,send-ext-com" status=""/>
-->
<l3extInstP name="accountingInst">
    <l3extSubnet ip="192.10.0.0/16" scope="import-security,import-rtctrl" />
    <l3extSubnet ip="192.3.3.0/24" scope="import-security,import-rtctrl" />
    <l3extSubnet ip="192.4.2.0/24" scope="import-security,import-rtctrl" />
    <l3extSubnet ip="64:ff9b::c007:200/120" scope="import-security,import-rtctrl" />
    <l3extSubnet ip="192.2.2.0/24" scope="export-rtctrl" />
    <l3extSubnet ip="0.0.0.0/0"
        scope="export-rtctrl,import-rtctrl,import-security"
        aggregate="export-rtctrl,import-rtctrl"
    />
</l3extInstP>
<l3extRsEctx tnFvCtxName="coke"/>
</l3extOut>
</fvTenant>

```

REST API を使用した BGP ネイバー シャットダウンおよびソフトリセットの設定

REST API を使用した BGP ネイバー シャットダウンの設定

次の手順では、REST API を使用して BGP ネイバー シャットダウン機能を使用する方法について説明します。

ステップ 1 ノードおよびインターフェイスを設定します。

この例では、ノードプロファイル、nodep1、ルータ ID 11.11.11.103 を持つノード 103（境界リーフスイッチ）上で、VRF v1 を設定します。また、IP アドレス 12.12.12.1/24 およびレイヤ 3 ドメイン dom1 で、ルーテッドインターフェイス（レイヤ 3 ポート）としてインターフェイス eth1/3 を設定します。

例：

```

<l3extOut name="l3out1">
    <l3extRsEctx tnFvCtxName="v1"/>
    <l3extLNodeP name="nodep1">
        <l3extRsNodeL3OutAtt rtrId="11.11.11.103" tDn="topology/pod-1/node-103"/>
        <l3extLIIfP name="ifp1"/>
        <l3extRsPathL3OutAtt addr="12.12.12.3/24" ifInstT="l3-port"
tDn="topology/pod-1/paths-103/pathep-[eth1/3]"/>
    </l3extLIIfP>

```

```

    </l3extLNodeP>
    <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
</l3extOut>

```

ステップ 2 BGP ルーティング プロトコルを設定し、BGP ネイバー シャットダウン機能を設定します。

この例では、IP アドレス、15.15.15.2、ASN 100 を持つ BGP ピアで、プライマリ ルーティング プロトコルとして BGP を設定します。

adminSt 変数は、次のいずれかに設定できます。

- **enabled** : BGP ネイバー シャットダウン機能をイネーブルにします。
- **disabled** : BGP ネイバー シャットダウン機能を無効にします。

次の例では、BGP ネイバー シャットダウン機能がイネーブルになっています。

例 :

```

<l3extOut name="l3out1">
  <l3extLNodeP name="nodep1">
    <bgpPeerP addr="15.15.15.2"> adminSt="enabled"
      <bgpAsP asn="100"/>
    </bgpPeerP>
  </l3extLNodeP>
  <bgpExtP/>
</l3extOut>

```

REST API を使用した BGP ネイバー ソフトリセットの設定

次の手順では、REST API を使用して BGP ネイバー ソフトリセット機能を使用する方法について説明します。

ステップ 1 ノードおよびインターフェイスを設定します。

この例では、ノードプロファイル、nodep1、ルータ ID 11.11.11.103 を持つノード 103（境界リーフスイッチ）上で、VRF v1 を設定します。また、IP アドレス 12.12.12.1/24 およびレイヤ 3 ドメイン dom1 で、ルーテッドインターフェイス（レイヤ 3 ポート）としてインターフェイス eth1/3 を設定します。

例 :

```

<l3extOut name="l3out1">
  <l3extRsEctx tnFvCtxName="v1"/>
  <l3extLNodeP name="nodep1">
    <l3extRsNodeL3OutAtt rtrId="11.11.11.103" tDn="topology/pod-1/node-103"/>
    <l3extLIIfP name="ifp1"/>
    <l3extRsPathL3OutAtt addr="12.12.12.3/24" ifInstT="l3-port"
tDn="topology/pod-1/paths-103/pathep-[eth1/3]"/>
  </l3extLIIfP>
  </l3extLNodeP>
  <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
</l3extOut>

```

ステップ 2 BGP ルーティング プロトコルを設定し、BGP ネイバー ソフトリセット機能を設定します。

REST API を使用した VRF ごと、ノード BGP ごとのタイマーの設定

この例では、IP アドレス、15.15.15.2、ASN 100 を持つ BGP ピアで、プライマリ ルーティング プロトコルとして BGP を設定します。

dir 変数は、次のいずれかに設定できます。

- **in** : ソフト ダイナミック インバウンド リセットを有効にします。
- **out** : ソフト アウトバウンド リセットを有効にします。

次の例では、ソフト ダイナミック インバウンド リセットが有効になっています。

例 :

```
<l3extOut name="l3out1">
  <l3extLNodeP name="nodep1">
    <bgpPeerP addr="15.15.15.2">
      <bgpAsP asn="100"/>
      <bgpPeerEntryClearPeerLTask>
        <attributes>
          <mode>soft</mode>
          <dir>in</dir>
          <adminSt>start</adminSt>
        </attributes>
        <children/>
      </bgpPeerEntryClearPeerLTask>
    </bgpPeerP>
  </l3extLNodeP>
  <bgpExtP/>
</l3extOut>
```

REST API を使用した VRF ごと、ノード BGP ごとのタイマーの設定

次の例では、ノード内の VRF ごと、ノード BGP ごとのタイマーの設定方法を示します。

bgpProtP (l3extLNodeP の下) を設定します。bgpProtP の下で、目的とする関係 (bgpRsBgpNodeCtxPol) を設定します。これは、BGP コンテキスト ポリシー (bgpCtxPol) に対するものです。

node1 でノード固有の BGP タイマー ポリシーを設定し、node2 を、ノード固有ではない BGP タイマー ポリシーで設定します。

例 :

POST https://apic-ip-address/mo.xml

```
<fvTenant name="tn1" >
  <bgpCtxPol name="pol1" staleIntvl="25" />
  <bgpCtxPol name="pol2" staleIntvl="35" />
  <fvCtx name="ctx1" >
    <fvRsBgpCtxPol tnBgpCtxPolName="pol1"/>
  </fvCtx>
  <l3extout name="out1" >
    <l3extRsEctx toFvCtxName="ctx1" />
    <l3extLNodeP name="node1" >
      <bgpProtP name="protp1" >
        <bgpRsBgpNodeCtxPol tnBgpCtxPolName="pol2" />
      </bgpProtP>
    </l3extLNodeP>
  </l3extout>
</fvTenant>
```

```
</l3extLNodeP>
<l3extLNodeP name="node2" >
</l3extLNodeP>
```

この例では、node1 は BGP タイマー値をポリシー pol2 から取得し、node2 は BGP タイマー値を pol1 から取得します。タイマー値は bgpDom に適用されますが、これは VRF tn1:ctx1 に対応しています。これは、「VRF ごと、ノード BGP ごとのタイマーの値」のセクションで説明したアルゴリズムに従って選択された、BGP タイマー ポリシーに基づきます。

削除するノード BGP タイマーが REST API を使用してごとの VRF あたり

次の例では、ノード内で既存の VRF ごとの各ノード BGP タイマーを削除する方法を示します。

node1 で特定の BGP タイマー ポリシーのノードを削除します。

例：

POST https://apic-ip-address/mo.xml

```
<fvTenant name="tn1" >
  <bgpCtxPol name="pol1" staleIntvl="25" />
  <bgpCtxPol name="pol2" staleIntvl="35" />
  <fvCtx name="ctx1" >
    <fvRsBgpCtxPol tnBgpCtxPolName="pol1"/>
  </fvCtx>
  <l3extout name="out1" >
    <l3extRsEctx toFvCtxName="ctx1" />
    <l3extLNodeP name="node1" >
      <bgpProtP name="protpl" status="deleted" >
        <bgpRsBgpNodeCtxPol tnBgpCtxPolName="pol2" />
      </bgpProtP>
    </l3extLNodeP>
    <l3extLNodeP name="node2" >
    </l3extLNodeP>
```

上の例のコードフレーズ <bgpProtP name="protpl" status="deleted" > は、BGP タイマー ポリシーを削除します。削除後、node1 が node1 が関連付けられている VRF の BGP タイマー ポリシーのデフォルト設定になります。上の例では pol1 です。

REST API を使用したセカンダリ IP アドレスでの双方向フォワーディング検出の構成

次の例では、REST API を使用して、セカンダリ IP アドレスに Bidirectional Forwarding Detection (BFD) を構成します。

```
<l3extLIIfP
dn="uni/tn-sec-ip-bfd/out-secip-bfd-l3out/lnodep-secip-bfd-l3out_nodeProfile/
lifp-secip-bfd-l3out_interfaceProfile" name="secip-bfd-l3out_interfaceProfile"
prio="unspecified" tag="yellow-green" userdom=":all:">
  <l3extRsPathL3OutAtt addr="50.50.50.200/24" autostate="disabled"
encap="vlan-2" encapScope="local" ifInstT="ext-svi" ipv6Dad="enabled"
isMultiPodDirect="no" llAddr=":" mac="00:22:BD:F8:19:FF" mode="regular"
mtu="inherit" tDn="topology/pod-1/paths-101/pathep-[eth1/3]"
```

グローバル REST API を使用して BFD の設定

```

        targetDscp="unspecified" userdom=":all:")>
        <l3extIp addr="9.9.9.1/24" ipv6Dad="enabled" userdom=":all:"/>
        <l3extIp addr="6.6.6.1/24" ipv6Dad="enabled" userdom=":all:"/>
    </l3extRsPathL3OutAtt>
    <l3extRsNdIfPol userdom="all"/>
    <l3extRsLIfPCustQosPol userdom="all"/>
    <l3extRsIngressQosDppPol userdom="all"/>
    <l3extRsEgressQosDppPol userdom="all"/>
    <l3extRsArpIfPol userdom="all"/>
</l3extLIfP>
<ipRouteP aggregate="no"
  dn="uni/tn-sec-ip-bfd/out-secip-bfd-l3out/lnodep-secip-bfd-l3out_nodeProfile/
  rsnodeL3OutAtt-[topology/pod-1/node-101]/rt-[6.0.0.1/24]"
  fromPfxLen="0" ip="6.0.0.1/24" pref="1" rtCtrl="bfd" toPfxLen="0" userdom=":all:">
  <ipNextHopP nhAddr="6.6.6.2" pref="unspecified" type="prefix" userdom=":all:"/>
</ipRouteP>

```

グローバル REST API を使用して BFD の設定

次の REST API は、(BFD) を双方向フォワーディング検出のグローバル コンフィギュレーションを示します。

例：

```

<polUni>
  <infraInfra>
    <bfdIpv4InstPol name="default" echoSrcAddr="1.2.3.4" slowIntvl="1000" minTxIntvl="150"
    minRxIntvl="250" detectMult="5" echoRxIntvl="200"/>
    <bfdIpv6InstPol name="default" echoSrcAddr="34::1/64" slowIntvl="1000" minTxIntvl="150"
    minRxIntvl="250" detectMult="5" echoRxIntvl="200"/>
  </infraInfra>
</polUni>

```

REST API を使用した BFD インターフェイスのオーバーライドの設定

次の REST API は、(BFD) を双方向フォワーディング検出のインターフェイスのオーバーライド コンフィギュレーションを示します。

例：

```

<fvTenant name="ExampleCorp">
  <bfdIfPol name="bfdIfPol" minTxIntvl="400" minRxIntvl="400" detectMult="5" echoRxIntvl="400"
  echoAdminSt="disabled"/>
  <l3extOut name="l3-out">
    <l3extLNodeP name="leaf1">
      <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="2.2.2.2"/>
      <l3extLIfP name="portIpv4">
        <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/11]" ifInstT='l3-port'
        addr="10.0.0.1/24" mtu="1500"/>
        <bfdIfP type="sha1" key="password">
          <bfdRsIfPol tnBfdIfPolName='bfdIfPol'/>
        </bfdIfP>
      </l3extLIfP>
    </l3extLNodeP>
  </l3extOut>
</fvTenant>

```

```

    </l3extOut>
  </fvTenant>

```

REST API を使用した BFD コンシューマ プロトコルの設定

ステップ 1 次の例では、双方向の転送検出 (BFD) のインターフェイス設定を示します。

例 :

```

<fvTenant name="ExampleCorp">
  <bfdIfPol name="bfdIfPol" minTxIntvl="400" minRxIntvl="400" detectMult="5" echoRxIntvl="400"
  echoAdminSt="disabled"/>
  <l3extOut name="l3-out">
    <l3extLNodeP name="leaf1">
      <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="2.2.2.2"/>
      <l3extLIfP name='portIpv4'>
        <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/11]" ifInstT='l3-port'
        addr="10.0.0.1/24" mtu="1500"/>
        <bfdIfP type="sha1" key="password">
          <bfdRsIfPol tnBfdIfPolName='bfdIfPol' />
        </bfdIfP>
      </l3extLIfP>
    </l3extLNodeP>
  </l3extOut>
</fvTenant>

```

ステップ 2 次の例では、OSPF および EIGRP で BFD を有効にするためのインターフェイス設定を示します。

例 :

リーフ スイッチ上の BFD

```

<fvTenant name="ExampleCorp">
  <ospfIfPol name="ospf_intf_pol" cost="10" ctrl="bfd"/>
  <eigrpIfPol ctrl="nh-self,split-horizon,bfd" dn="uni/tn-Coke/eigrpIfPol-eigrp_if_default"
</fvTenant>

```

例 :

スパイン スイッチ上の BFD

```

<l3extLNodeP name="bSpine">
  <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-103" rtrId="192.3.1.8">
    <l3extLoopBackIfP addr="10.10.3.1" />
    <l3extInfraNodeP fabricExtCtrlPeering="false" />
  </l3extRsNodeL3OutAtt>
  <l3extLIfP name='portIf'>
    <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-103/pathep-[eth5/10]" encap='vlan-4'
    ifInstT='sub-interface' addr="20.3.10.1/24"/>
    <ospfIfP>
      <ospfRsIfPol tnOspfIfPolName='ospf_intf_pol' />
    </ospfIfP>
    <bfdIfP name="test" type="sha1" key="hello" status="created,modified">
      <bfdRsIfPol tnBfdIfPolName='default' status="created,modified"/>
    </bfdIfP>
  </l3extLIfP>
</l3extLNodeP>

```

```

    </l3extLIIfP>
  </l3extLNodeP>

```

ステップ3 次の例では、BGP 上の BFD を有効にするためのインターフェイス設定を示します。

例：

```

<fvTenant name="ExampleCorp">
  <l3extOut name="l3-out">
    <l3extLNodeP name="leaf1">
      <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="2.2.2.2"/>
      <l3extLIIfP name='portIpv4'>
        <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/11]" ifInstT='l3-port'
          addr="10.0.0.1/24" mtu="1500">
          <bgpPeerP addr="4.4.4.4/24" allowedSelfAsCnt="3" ctrl="bfd" descr="" name=""
            peerCtrl="" ttl="1">
            <bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
            <bgpAsP asn="3" descr="" name=""/>
          </bgpPeerP>
        </l3extRsPathL3OutAtt>
      </l3extLIIfP>
    </l3extLNodeP>
  </l3extOut>
</fvTenant>

```

ステップ4 次の例では、スタティック ルートで BFD を有効にするためのインターフェイス設定を示します。

例：

リーフ スイッチ上の BFD

```

<fvTenant name="ExampleCorp">
  <l3extOut name="l3-out">
    <l3extLNodeP name="leaf1">
      <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="2.2.2.2">
        <ipRouteP ip="192.168.3.4" rtCtrl="bfd">
          <ipNextHopP nhAddr="192.168.62.2"/>
        </ipRouteP>
      </l3extRsNodeL3OutAtt>
      <l3extLIIfP name='portIpv4'>
        <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/3]" ifInstT='l3-port'
          addr="10.10.10.2/24" mtu="1500" status="created,modified" />
      </l3extLIIfP>
    </l3extLNodeP>
  </l3extOut>
</fvTenant>

```

例：

スパイン スイッチ上の BFD

```

<l3extLNodeP name="bSpine">
  <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-103" rtrId="192.3.1.8">
    <ipRouteP ip="0.0.0.0" rtCtrl="bfd">
      <ipNextHopP nhAddr="192.168.62.2"/>
    </ipRouteP>
  </l3extRsNodeL3OutAtt>

```



```

    <l3extLIfP name='portIf'>
      <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-103/pathep-[eth5/10]" encap='vlan-4'
ifInstT='sub-interface' addr="20.3.10.1/24"/>

      <bfdIfP name="test" type="sha1" key="hello" status="created,modified">
        <bfdRsIfPol tnBfdIfPolName='default' status="created,modified"/>
      </bfdIfP>
    </l3extLIfP>

  </l3extLNodeP>

```

ステップ 5 次の例では、IS-IS で BFD を有効にするためのインターフェイス設定を示します。

例 :

```

<fabricInst>
  <l3IfPol name="testL3IfPol" bfdIsis="enabled"/>
  <fabricLeafP name="LeNode" >
    <fabricRsLePortP tDn="uni/fabric/leportp-leaf_profile" />
    <fabricLeafS name="spsw" type="range">
    <fabricNodeBlk name="node101" to_"102" from_"101" />
    </fabricLeafS>
  </fabricLeafP>

  <fabricSpineP name="SpNode" >
    <fabricRsSpPortP tDn="uni/fabric/spportp-spine_profile" />
    <fabricSpineS name="spsw" type="range">
      <fabricNodeBlk name="node103" to_"103" from_"103" />
    </fabricSpineS>
  </fabricSpineP>

  <fabricLePortP name="leaf_profile">
    <fabricLFPortS name="leafIf" type="range">
    <fabricPortBlk name="spBlk" fromCard="1" fromPort="49" toCard="1" toPort="49" />
    <fabricRsLePortPGrp tDn="uni/fabric/funcprof/leportgrp-LeTestPGrp" />
  </fabricLFPortS>
  </fabricLePortP>

  <fabricSpPortP name="spine_profile">
    <fabricSFPortS name="spineIf" type="range">
      <fabricPortBlk name="spBlk" fromCard="5" fromPort="1" toCard="5" toPort="2" />
      <fabricRsSpPortPGrp tDn="uni/fabric/funcprof/spportgrp-SpTestPGrp" />
    </fabricSFPortS>
  </fabricSpPortP>

  <fabricFuncP>
    <fabricLePortPGrp name = "LeTestPGrp">
    <fabricRsL3IfPol tnL3IfPolName="testL3IfPol"/>
    </fabricLePortPGrp>

    <fabricSpPortPGrp name = "SpTestPGrp">
    <fabricRsL3IfPol tnL3IfPolName="testL3IfPol"/>
    </fabricSpPortPGrp>

  </fabricFuncP>
</fabricInst>

```

REST API を使用した OSPF 外部ルーテッドネットワークの設定

REST API を使用した管理テナントの OSPF 外部ルーテッドネットワークの作成

- ルータ ID と論理インターフェイスプロファイルの IP アドレスが異なっていて重複していないことを確認します。
- 次の手順は、管理テナントの OSPF 外部ルーテッドネットワークを作成するためのものです。テナントの OSPF 外部ルーテッドネットワークを作成するには、テナントを選択し、テナント用の VRF を作成する必要があります。
- 詳細については、『*Cisco APIC and Transit Routing*』を参照してください。

管理テナントの OSPF 外部ルーテッドネットワークを作成します。

例：

POST: <https://apic-ip-address/api/mo/uni/tn-mgmt.xml>

```
<fvTenant name="mgmt">
  <fvBD name="bd1">
    <fvRsBDToOut tnL3extOutName="RtdOut" />
    <fvSubnet ip="1.1.1.1/16" />
    <fvSubnet ip="1.2.1.1/16" />
    <fvSubnet ip="40.1.1.1/24" scope="public" />
    <fvRsCtx tnFvCtxName="inb" />
  </fvBD>
  <fvCtx name="inb" />

  <l3extOut name="RtdOut">
    <l3extRsL3DomAtt tDn="uni/l3dom-extdom"/>
    <l3extInstP name="extMgmt">
      </l3extInstP>
    <l3extLNodeP name="borderLeaf">
      <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="10.10.10.10"/>
      <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-102" rtrId="10.10.10.11"/>
      <l3extLIIfP name='portProfile'>
        <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/40]" ifInstT='l3-port'
addr="192.168.62.1/24"/>
        <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-102/pathep-[eth1/40]" ifInstT='l3-port'
addr="192.168.62.5/24"/>
        <ospfIfP/>
      </l3extLIIfP>
    </l3extLNodeP>
    <l3extRsEctx tnFvCtxName="inb"/>
    <ospfExtP areaId="57" />
  </l3extOut>
</fvTenant>
```

REST API を使用した EIGRP 外部ルーテッドネットワークの設定

REST API を使用した EIGRP の設定

ステップ 1 EIGRP コンテキスト ポリシーを設定します。

例 :

```
<polUni>
  <fvTenant name="cisco_6">
    <eigrpCtxAfPol actIntvl="3" descr="" dn="uni/tn-cisco_6/eigrpCtxAfP-eigrp_default_pol"
extDist="170"
    intDist="90" maxPaths="8" metricStyle="narrow" name="eigrp_default_pol" ownerKey=""
ownerTag=""/>
  </fvTenant>
</polUni>
```

ステップ 2 EIGRP インターフェイス ポリシーを設定します。

例 :

```
<polUni>
  <fvTenant name="cisco_6">
    <eigrpIfPol bw="10" ctrl="nh-self,split-horizon" delay="10" delayUnit="tens-of-micro" descr=""
dn="uni/tn-cisco_6/eigrpIfPol-eigrp_if_default"
    helloIntvl="5" holdIntvl="15" name="eigrp_if_default" ownerKey="" ownerTag=""/>
  </fvTenant>
</polUni>
```

ステップ 3 EIGRP VRF を設定します。

例 :

IPv4 :

```
<polUni>
  <fvTenant name="cisco_6">
    <fvCtx name="dev">
      <fvRsCtxToEigrpCtxAfPol tnEigrpCtxAfPolName="eigrp_ctx_pol_v4" af="1"/>
    </fvCtx>
  </fvTenant>
</polUni>
```

IPv6

```
<polUni>
  <fvTenant name="cisco_6">
    <fvCtx name="dev">
      <fvRsCtxToEigrpCtxAfPol tnEigrpCtxAfPolName="eigrp_ctx_pol_v6" af="ipv6-ucast"/>
    </fvCtx>
  </fvTenant>
</polUni>
```

ステップ 4 外部の EIGRP Layer3 を設定します。

例 :

IPv4

```
<polUni>
  <fvTenant name="cisco_6">
    <l3extOut name="ext">
      <eigrpExtP asn="4001"/>
    </l3extOut>
  </fvTenant>
</polUni>
```

```

    <l3extLNodeP name="node1">
      <l3extLIIfP name="intf_v4">
        <l3extRsPathL3OutAtt addr="201.1.1.1/24" ifInstT="l3-port"
          tDn="topology/pod-1/paths-101/pathep-[eth1/4]"/>
        <eigrpIfP name="eigrp_ifp_v4">
          <eigrpRsIfPol tnEigrpIfPolName="eigrp_if_pol_v4"/>
        </eigrpIfP>
      </l3extLIIfP>
    </l3extLNodeP>
  </l3extOut>
</fvTenant>
</polUni>

```

IPv6

```

<polUni>
  <fvTenant name="cisco_6">
    <l3extOut name="ext">
      <eigrpExtP asn="4001"/>
      <l3extLNodeP name="node1">
        <l3extLIIfP name="intf_v6">
          <l3extRsPathL3OutAtt addr="2001::1/64" ifInstT="l3-port"
            tDn="topology/pod-1/paths-101/pathep-[eth1/4]"/>
          <eigrpIfP name="eigrp_ifp_v6">
            <eigrpRsIfPol tnEigrpIfPolName="eigrp_if_pol_v6"/>
          </eigrpIfP>
        </l3extLIIfP>
      </l3extLNodeP>
    </l3extOut>
  </fvTenant>
</polUni>

```

IPv4 および IPv6

```

<polUni>
  <fvTenant name="cisco_6">
    <l3extOut name="ext">
      <eigrpExtP asn="4001"/>
      <l3extLNodeP name="node1">
        <l3extLIIfP name="intf_v4">
          <l3extRsPathL3OutAtt addr="201.1.1.1/24" ifInstT="l3-port"
            tDn="topology/pod-1/paths-101/pathep-[eth1/4]"/>
          <eigrpIfP name="eigrp_ifp_v4">
            <eigrpRsIfPol tnEigrpIfPolName="eigrp_if_pol_v4"/>
          </eigrpIfP>
        </l3extLIIfP>

        <l3extLIIfP name="intf_v6">
          <l3extRsPathL3OutAtt addr="2001::1/64" ifInstT="l3-port"
            tDn="topology/pod-1/paths-101/pathep-[eth1/4]"/>
          <eigrpIfP name="eigrp_ifp_v6">
            <eigrpRsIfPol tnEigrpIfPolName="eigrp_if_pol_v6"/>
          </eigrpIfP>
        </l3extLIIfP>
      </l3extLNodeP>
    </l3extOut>
  </fvTenant>
</polUni>

```

ステップ 5 (任意) インターフェイス ポリシー ノブを設定します。

例 :

```

<polUni>
  <fvTenant name="cisco_6">

```

```

    <eigrpIfPol bw="1000000" ctrl="nh-self,split-horizon" delay="10"
      delayUnit="tens-of-micro" helloIntvl="5" holdIntvl="15" name="default"/>
  </fvTenant>
</polUni>

```

Bandwidth (bw) 属性は (bw) 属性は kbps で定義されています。DelayUnit 属性は、「1万マイクロ」または「ピコ」です。

REST API を使用したルート集約の設定

BGP、OSPF、および REST API を使用して EIGRP のルート集約の設定

ステップ 1 次のように、REST API を使用して BGP ルート集約を設定します。

例：

```

<fvTenant name="common">
  <fvCtx name="vrf1"/>
  <bgpRtSummPol name="bgp_rt_summ" ctrl='as-set' />
  <l3extOut name="l3_ext_pol" >
    <l3extLNodeP name="bLeaf">
      <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="20.10.1.1"/>
      <l3extLIIfP name='portIf'>
        <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/31]" ifInstT='l3-port'
          addr="10.20.1.3/24"/>
      </l3extLIIfP>
    </l3extLNodeP>
    <bgpExtP />
    <l3extInstP name="InstP" >
      <l3extSubnet ip="10.0.0.0/8" scope="export-rtctrl">
        <l3extRsSubnetToRtSumm tDn="uni/tn-common/bgprtsum-bgp_rt_summ"/>
        <l3extRsSubnetToProfile tnRtctrlProfileName="rtctrlprof"/>
      </l3extSubnet>
    </l3extInstP>
    <l3extRsEctx tnFvCtxName="vrf1"/>
  </l3extOut>
</fvTenant>

```

ステップ 2 次の REST API を使用して、OSPF のエリア間および外部の集約を設定します。

例：

```

<?xml version="1.0" encoding="utf-8"?>
<fvTenant name="t20">
  <!--Ospf Inter External route summarization Policy-->
  <ospfRtSummPol cost="unspecified" interAreaEnabled="no" name="ospfext"/>
  <!--Ospf Inter Area route summarization Policy-->
  <ospfRtSummPol cost="16777215" interAreaEnabled="yes" name="interArea"/>
  <fvCtx name="ctx0" pcEnfDir="ingress" pcEnfPref="enforced"/>
  <!-- L3OUT backbone Area-->
  <l3extOut enforceRtctrl="export" name="l3_1" ownerKey="" ownerTag="" targetDscp="unspecified">
    <l3extRsEctx tnFvCtxName="ctx0"/>
    <l3extLNodeP name="node-101">
      <l3extRsNodeL3OutAtt rtrId="20.1.3.2" rtrIdLoopBack="no" tDn="topology/pod-1/node-101"/>
    </l3extLNodeP>
  </l3extOut>

```

```

    <l3extLIfP name="intf-1">
      <l3extRsPathL3OutAtt addr="20.1.5.2/24" encap="vlan-1001" ifInstT="sub-interface"
tDn="topology/pod-1/paths-101/pathep-[eth1/33]"/>
    </l3extLIfP>
  </l3extLNodeP>
  <l3extInstP name="l3InstP1">
    <fvRsProv tnVzBrCPName="default"/>
    <!--Ospf External Area route summarization-->
    <l3extSubnet aggregate="" ip="193.0.0.0/8" name="" scope="export-rtctrl">
      <l3extRsSubnetToRtSumm tDn="uni/tn-t20/ospfrtsumm-ospfext"/>
    </l3extSubnet>
  </l3extInstP>
  <ospfExtP areaCost="1" areaCtrl="redistribute,summary" areaId="backbone" areaType="regular"/>
</l3extOut>
<!-- L3OUT Regular Area-->
<l3extOut enforceRtctrl="export" name="l3_2">
  <l3extRsEctx tnFvCtxName="ctx0"/>
  <l3extLNodeP name="node-101">
    <l3extRsNodeL3OutAtt rtrId="20.1.3.2" rtrIdLoopBack="no" tDn="topology/pod-1/node-101"/>
    <l3extLIfP name="intf-2">
      <l3extRsPathL3OutAtt addr="20.1.2.2/24" encap="vlan-1014" ifInstT="sub-interface"
tDn="topology/pod-1/paths-101/pathep-[eth1/11]"/>
    </l3extLIfP>
  </l3extLNodeP>
  <l3extInstP matchT="AtleastOne" name="l3InstP2">
    <fvRsCons tnVzBrCPName="default"/>
    <!--Ospf Inter Area route summarization-->
    <l3extSubnet aggregate="" ip="197.0.0.0/8" name="" scope="export-rtctrl">
      <l3extRsSubnetToRtSumm tDn="uni/tn-t20/ospfrtsumm-interArea"/>
    </l3extSubnet>
  </l3extInstP>
  <ospfExtP areaCost="1" areaCtrl="redistribute,summary" areaId="0.0.0.57" areaType="regular"/>
</l3extOut>
</fvTenant>

```

ステップ 3 次の REST API を使用して EIGRP の集約を設定します。

例：

```

<fvTenant name="exampleCorp">
  <l3extOut name="out1">
    <l3extInstP name="eigrpSummInstp" >
      <l3extSubnet aggregate="" descr="" ip="197.0.0.0/8" name="" scope="export-rtctrl">
        <l3extRsSubnetToRtSumm/>
      </l3extSubnet>
    </l3extInstP>
  </l3extOut>
  <eigrpRtSummPol name="pol1" />

```

(注) EIGRP を設定するルート集約ポリシーはありません。EIGRP の集約を有効にするために必要なだけの設定では、サマリー サブネット、InstP です。

REST API を使用したルート マップおよびルート プロファイルによるルート制御の設定

REST API を使用した BGP ピアごとのルート制御の設定

次の手順では、REST API を使用して BGP ピア単位のルート制御を設定する方法について説明します。

BGP ピアごとのルート制御機能を設定します。

ここで、

- **direction="import"** は、ルート インポート ポリシー（ファブリックに許可されるルート）です。
- **direction="export"** は、ルート エクスポート ポリシー（外部ネットワークからアドバタイズされるルート）です。

例：

```
<polUni>
  <fvTenant name="t1">
    <fvCtx name="v1"/>
    <l3extOut name="l3out1">
      <l3extRsEctx tnFvCtxName="v1"/>
      <l3extLNodeP name="nodep1">
        <l3extRsNodeL3OutAtt rtrId="11.11.11.103" tDn="topology/pod-1/node-103"/>
        <l3extLIIfP name="ifp1">
          <l3extRsPathL3OutAtt addr="12.12.12.3/24" ifInstT="l3-port"
tDn="topology/pod-1/paths-103/pathep-[eth1/3]"/>
        </l3extLIIfP>
        <bgpPeerP addr="15.15.15.2">
          <bgpAsP asn="100"/>
          <bgpRsPeerToProfile direction="export" tnRtctrlProfileName="rp1"/>
        </bgpPeerP>
      </l3extLNodeP>
      <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
      <bgpExtP/>
      <ospfExtP areaId="0.0.0.0" areaType="regular"/>
      <l3extInstP name="extnw1" >
        <l3extSubnet ip="20.20.20.0/24" scope="import-security"/>
      </l3extInstP>
    </l3extOut>
    <rtctrlProfile name="rp1">
      <rtctrlCtxP name="ctxp1" action="permit" order="0">
        <rtctrlScope>
          <rtctrlRsScopeToAttrP tnRtctrlAttrPName="attrp1"/>
        </rtctrlScope>
        <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule1"/>
      </rtctrlCtxP>
    </rtctrlProfile>
    <rtctrlSubjP name="match-rule1">
      <rtctrlMatchRtDest ip="200.3.2.0/24"/>
    </rtctrlSubjP>
    <rtctrlAttrP name="attrp1">
      <rtctrlSetASPath criteria="prepend">
        <rtctrlSetASPathASN asn="100" order="2"/>
      </rtctrlSetASPath>
    </rtctrlAttrP>
  </fvTenant>
</polUni>
```

```

        <rtctrlSetASPathASN asn="200" order="1"/>
      </rtctrlSetASPath>
    </rtctrlAttrP>
  </fvTenant>
</polUni>

```

REST API を使用して、明示的なプレフィックスリストでルートマップ/プロファイルの設定

始める前に

- テナントと VRF を設定する必要があります。

明示的なプレフィックスリストを使用してルートマップ/プロファイルを設定します。

(注) 以下の太字のエントリは、APIC リリース 4.2(3) 以降で使用可能な一致プレフィックスの拡張機能です。これらのフィールドの詳細については、[一致プレフィックスの機能拡張 \(357 ページ\)](#) を参照してください。

例 :

```

<?xml version="1.0" encoding="UTF-8"?>
<fvTenant name="PM" status="">
  <rtctrlAttrP name="set_dest">
    <rtctrlSetComm community="regular:as2-nn2:5:24" />
  </rtctrlAttrP>
  <rtctrlSubjP name="allow_dest">
    <rtctrlMatchRtDest ip="192.169.0.0/24" aggregate="yes" fromPfxLen="26" toPfxLen="30" />
    <rtctrlMatchCommTerm name="term1">
      <rtctrlMatchCommFactor community="regular:as2-nn2:5:24" status="" />
      <rtctrlMatchCommFactor community="regular:as2-nn2:5:25" status="" />
    </rtctrlMatchCommTerm>
    <rtctrlMatchCommRegexTerm commType="regular" regex="200:*" status="" />
  </rtctrlSubjP>
  <rtctrlSubjP name="deny_dest">
    <rtctrlMatchRtDest ip="192.168.0.0/24" />
  </rtctrlSubjP>
  <fvCtx name="ctx" />
  <l3extOut name="L3Out_1" enforceRtctrl="import,export" status="">
    <l3extRsEctx tnFvCtxName="ctx" />
    <l3extLNodeP name="bLeaf">
      <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="1.2.3.4" />
      <l3extLIIfP name="portIf">
        <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/25]"
ifInstT="sub-interface" encap="vlan-1503" addr="10.11.12.11/24" />
        <ospfIfP />
      </l3extLIIfP>
      <bgpPeerP addr="5.16.57.18/32" ctrl="send-com" />
      <bgpPeerP addr="6.16.57.18/32" ctrl="send-com" />
    </l3extLNodeP>
  </l3extOut>
  <bgpExtP />
  <ospfExtP areaId="0.0.0.59" areaType="nssa" status="" />
  <l3extInstP name="l3extInstP_1" status="">
    <l3extSubnet ip="17.11.1.11/24" scope="import-security" />
  </l3extInstP>

```



```

<rtctrlProfile name="default-export" type="global" status="">
  <rtctrlCtxP name="ctx_deny" action="deny" order="1">
    <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="deny_dest" status="" />
  </rtctrlCtxP>
  <rtctrlCtxP name="ctx_allow" order="2">
    <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="allow_dest" status="" />
  </rtctrlCtxP>
  <rtctrlScope name="scope" status="">
    <rtctrlRsScopeToAttrP tnRtctrlAttrPName="set_dest" status="" />
  </rtctrlScope>
</rtctrlProfile>
</l3extOut>
<fvBD name="testBD">
  <fvRsBDToOut tnL3extOutName="L3Out_1" />
  <fvRsCtx tnFvCtxName="ctx" />
  <fvSubnet ip="40.1.1.12/24" scope="public" />
  <fvSubnet ip="40.1.1.2/24" scope="private" />
  <fvSubnet ip="2003::4/64" scope="public" />
</fvBD>
</fvTenant>

```

REST API を使用した、インポート制御とエクスポート制御によるルーティング制御プロトコルの設定

この例では、ネットワーク接続 BGP を使用して外部レイヤ 3 が設定されていることを前提としています。OSPF を使用してネットワークを次のタスクを実行することもできます。

始める前に

- テナント、プライベートネットワーク、およびブリッジドメインが作成されていること。
- レイヤ 3 Outside テナント ネットワークが設定されていること。

インポート制御とエクスポート制御を使用するルート制御プロトコルを設定します。

例：

```

<l3extOut descr="" dn="uni/tn-Ten_ND/out-L3Out1" enforceRtctrl="export" name="L3Out1" ownerKey=""
ownerTag="" targetDscp="unspecified">
  <l3extLNodeP descr="" name="LNodeP1" ownerKey="" ownerTag="" tag="yellow-green"
targetDscp="unspecified">
    <l3extRsNodeL3OutAtt rtrId="1.2.3.4" rtrIdLoopBack="yes" tDn="topology/pod-1/node-101">
      <l3extLoopBackIfP addr="2000::3" descr="" name="" />
    </l3extRsNodeL3OutAtt>
    <l3extLIfP descr="" name="IFP1" ownerKey="" ownerTag="" tag="yellow-green">
      <ospfIfP authKeyId="1" authType="none" descr="" name="">
        <ospfRsIfPol tnOspfIfPolName="" />
      </ospfIfP>
      <l3extRsNdIfPol tnNdIfPolName="" />
      <l3extRsPathL3OutAtt addr="10.11.12.10/24" descr="" encaps="unknown" ifInstT="l3-port"
llAddr="::" mac="00:22:BD:F8:19:FF" mtu="1500" tDn="topology/pod-1/paths-101/pathep-[eth1/17]"
targetDscp="unspecified"/>
    </l3extLIfP>
  </l3extLNodeP>
</l3extOut>

```

```

</l3extLNodeP>
<l3extRsEctx tnFvCtxName="PVN1"/>
<l3extInstP descr="" matchT="AtleastOne" name="InstP1" prio="unspecified"
targetDscp="unspecified">
  <fvRsCustQosPol tnQosCustomPolName=""/>
  <l3extSubnet aggregate="" descr="" ip="192.168.1.0/24" name="" scope=""/>
</l3extInstP>
<ospfExtP areaCost="1" areaCtrl="redistribute,summary" areaId="0.0.0.1" areaType="nssa"
descr=""/>
<rtctrlProfile descr="" name="default-export" ownerKey="" ownerTag="">
  <rtctrlCtxP descr="" name="routecontrolpvtnw" order="3">
    <rtctrlScope descr="" name="">
      <rtctrlRsScopeToAttrP tnRtctrlAttrPName="actionruleprofile2"/>
    </rtctrlScope>
  </rtctrlCtxP>
</rtctrlProfile>
</l3extOut>

```

REST API を使用したインターリーク再配布の設定

次の手順では、REST API を使用してインターリーク再配布を設定する方法について説明します。

始める前に

テナント、VRF、および L3Out を作成します。

ステップ 1 インターリーク再配布のルートマップを設定します。

例：

次の例では、2つのコンテキスト（`ROUTES_A` および `ROUTES_ALL`）を使用してルートマップ `INTERLEAK_RP` を設定します。最初のコンテキスト `ROUTES_A` は、IP プレフィックスリスト `10.0.0.0/24` le 32 と一致し、`set rule COM_A` を介してコミュニティ属性を設定します。2 番目のコンテキストは、すべてのルートと一致します。

```

POST: https://<APIC IP>/api/mo/uni.xml
BODY:
<fvTenant dn="uni/tn-SAMPLE">
  <!-- route map with two contexts (ROUTES_A and ROUTES_ALL)-->
  <rtctrlProfile type="global" name="INTERLEAK_RP">
    <rtctrlCtxP name="ROUTES_A" order="0" action="permit">
      <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="PFX_10-0-0-0_24"/>
    <rtctrlScope>
      <rtctrlRsScopeToAttrP tnRtctrlAttrPName="COM_A"/>
    </rtctrlScope>
  </rtctrlCtxP>
  <rtctrlCtxP name="ROUTES_ALL" order="9" action="permit">
    <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="ALL_PREFIX"/>
  </rtctrlCtxP>
</rtctrlProfile>

  <!-- match rule with an IP prefix-list -->
  <rtctrlSubjP name="ALL_PREFIX">
    <rtctrlMatchRtDest ip="0.0.0.0/0" aggregate="yes"/>
  </rtctrlSubjP>

```

```

<!-- match rule with an IP prefix-list -->
<rtctrlSubjP name="PFX_10-0-0-0_24">
  <rtctrlMatchRtDest ip="10.0.0.0/24" aggregate="yes"/>
</rtctrlSubjP>

<!-- setu rule for community attribute -->
<rtctrlAttrP name="COM_A">
  <rtctrlSetComm type="community" setCriteria="append" community="regular:as2-nn2:100:200"/>
</rtctrlAttrP>
</fvTenant>

```

ステップ2 設定されたルートマップを L3Out に適用します。

次の例では、ステップ1のルートマップを L3Out l3out1 に適用して、特定の L3Out からのルートのインターリーク再配布をカスタマイズします。

L3extRsInterleakPol は、特定の L3Out によって使用されるダイナミック ルーティング プロトコル (OSPF/EIGRP) ルートに適用されます。L3extRsRedistributePol は、src 属性 (static) で指定されたスタティック ルートに適用されます。

例：

```

POST: https://<APIC IP>/api/mo/uni.xml
BODY:
<fvTenant dn="uni/tn-SAMPLE">
  <l3extOut name="l3out1">
    <!-- interleak redistribution for OSPF/EIGRP routes -->
    <l3extRsInterleakPol tnRtctrlProfileName="INTERLEAK_RP"/>
    <!-- interleak redistribution for static routes -->
    <l3extRsRedistributePol tnRtctrlProfileName="INTERLEAK_RP" src="static"/>
  </l3extOut>
</fvTenant>

```

REST API を使用したトランジットルーティングの設定

REST API を使用したトランジットルーティングの設定

次の手順では、テナントのトランジットルーティングを設定する方法を説明します。この例では、別のルータにそれぞれ接続された2つの境界リーフスイッチで、1つのVRF内に2つのL3Outを展開します。

始める前に

- ノード、ポート、AEP、機能プロファイル、レイヤ3ドメインを設定します。
- 外部ルーテッドドメインを作成し、L3Outのインターフェイスに関連付けます。
- ファブリック内でルートを伝播させるために、BGPルートリフレクタポリシーを設定します。

ステップ1 テナントおよびVRFを設定します。

この例ではテナント `t1` および VRF `v1` を設定します。VRF はまだ展開されていません。

例 :

```
<fvTenant name="t1">
  <fvCtx name="v1"/>
</fvTenant>
```

ステップ 2 ノードおよびインターフェイスを設定します。

この例では、2つの境界リーフスイッチで、テナント `t1` と VRF `v1` に2つの L3Outs を設定します。VRF は、レイヤ3ドメイン `dom1` です。

- 最初の L3Out はノード 101 上にあり、`nodep1` という名前です。ノード 101 はルータ ID `11.11.11.103` で設定されます。ルーテッドインターフェイス `ifp1` が `eth1/3` にあり、IP アドレス `12.12.12.3/24` です。
- 2番目の L3Out がノード 102 上にあり、`nodep2` という名前です。ノード 102 はルータ ID `22.22.22.203` に設定されています。IP アドレス、`23.23.23.1/24` を持つ `eth1/3` でルーテッドインターフェイス `ifp2` があります。

例 :

```
<l3extOut name="l3out1">
  <l3extRsEctx tnFvCtxName="v1"/>
  <l3extLNodeP name="nodep1">
    <l3extRsNodeL3OutAtt rtrId="11.11.11.103" tDn="topology/pod-1/node-101"/>
    <l3extLIIfP name="ifp1"/>
    <l3extRsPathL3OutAtt addr="12.12.12.3/24" ifInstT="l3-port"
tDn="topology/pod-1/paths-101/pathep-[eth1/3]"/>
  </l3extLIIfP>
</l3extLNodeP>
  <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
</l3extOut>

<l3extOut name="l3out2">
  <l3extRsEctx tnFvCtxName="v1"/>
  <l3extLNodeP name="nodep2">
    <l3extRsNodeL3OutAtt rtrId="22.22.22.203" tDn="topology/pod-1/node-102"/>
    <l3extLIIfP name="ifp2"/>
    <l3extRsPathL3OutAtt addr="23.23.23.3/24" ifInstT="l3-port"
tDn="topology/pod-1/paths-102/pathep-[eth1/3]"/>
  </l3extLIIfP>
</l3extLNodeP>
  <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
</l3extOut>
```

ステップ 3 両方の境界リーフスイッチのルーティングプロトコルを設定します。

この例では、両方の境界リーフスイッチに対して、ASN 100 でプライマリ ルーティングプロトコルとして BGP を設定します。BGP ピア `15.15.15.2` を持つノード 101 と BGP ピア `25.25.25.2` を持つノード 102 を設定します。

例 :

```
<l3extOut name="l3out1">
  <l3extLNodeP name="nodep1">
    <bgpPeerP addr="15.15.15.2/24"
  <bgpAsP asn="100"/>
  </bgpPeerP>
</l3extLNodeP>
```

```

</l3extOut>

<l3extOut name="l3out2">
  <l3extLNodeP name="nodep2">
    <bgpPeerP addr="25.25.25.2/24"
      <bgpAsP asn="100"/>
    </bgpPeerP>
  </l3extLNodeP>
</l3extOut>

```

ステップ4 接続ルーティング プロトコルを設定します。

この例では、定期的なエリア ID 0.0.0.0 で両方の L3Outs に対して通信プロトコルとして OSPF を設定します。

例：

```

<l3extOut name="l3out1">
  <ospfExtP areaId="0.0.0.0" areaType="regular"/>
  <l3extLNodeP name="nodep1">
    <l3extLIIfP name="ifp1">
      <ospfIfP/>
    </l3extLIIfP>
  </l3extLNodeP>
</l3extOut>
<l3extOut name="l3out2">
  <ospfExtP areaId="0.0.0.0" areaType="regular"/>
  <l3extLNodeP name="nodep2">
    <l3extLIIfP name="ifp2">
      <ospfIfP/>
    </l3extLIIfP>
  </l3extLNodeP>
</l3extOut>

```

ステップ5 外部 EPG を設定します。

この例では、ノード 101 上の外部ネットワーク extnw1 としてネットワーク 192.168.1.0/24 と、ノード 102 上の外部ネットワーク extnw2 として 192.168.2.0/24 を設定します。また、ルート制御プロファイル rp1 および rp2 と外部 EPG を関連付けます。

例：

```

<l3extOut name="l3out1">
  <l3extInstP name="extnw1">
    <l3extSubnet ip="192.168.1.0/24" scope="import-security"/>
    <l3extRsInstPToProfile direction="export" tnRtctrlProfileName="rp1"/>
  </l3extInstP>
</l3extOut>
<l3extOut name="l3out2">
  <l3extInstP name="extnw2">
    <l3extSubnet ip="192.168.2.0/24" scope="import-security"/>
    <l3extRsInstPToProfile direction="export" tnRtctrlProfileName="rp2"/>
  </l3extInstP>
</l3extOut>

```

ステップ6 オプション。ルート マップを設定します。

この例では、インバウンドおよびアウトバウンド方向で各 BGP ピアのルートマップを設定します。L3out1 では、ルート マップ rp1 が 192.168.1.0/24 のインポート宛先に一致するルートに適用され、ルート マップ rp2 が 192.168.2.0/24 のエクスポート宛先に一致するルートに適用されます。L3out2 では、ルート マップの方向を反転します。

例 :

```
<fvTenant name="t1">
  <rtctrlSubjP name="match-rule1">
    <rtctrlMatchRtDest ip="192.168.1.0/24" />
  </rtctrlSubjP>
  <rtctrlSubjP name="match-rule2">
    <rtctrlMatchRtDest ip="192.168.2.0/24" />
  </rtctrlSubjP>
  <l3extOut name="l3out1">
    <rtctrlProfile name="rp1">
      <rtctrlCtxP name="ctxp1" action="permit" order="0">
        <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule1" />
      </rtctrlCtxP>
    </rtctrlProfile>
    <rtctrlProfile name="rp2">
      <rtctrlCtxP name="ctxp1" action="permit" order="0">
        <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule2" />
      </rtctrlCtxP>
    </rtctrlProfile>
    <l3extInstP name="extnw1">
      <l3extRsInstPToProfile direction="import" tnRtctrlProfileName="rp1" />
      <l3extRsInstPToProfile direction="export" tnRtctrlProfileName="rp2" />
    </l3extInstP>
  </l3extOut>
  <l3extOut name="l3out2">
    <rtctrlProfile name="rp1">
      <rtctrlCtxP name="ctxp1" action="permit" order="0">
        <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule1" />
      </rtctrlCtxP>
    </rtctrlProfile>
    <rtctrlProfile name="rp2">
      <rtctrlCtxP name="ctxp1" action="permit" order="0">
        <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule2" />
      </rtctrlCtxP>
    </rtctrlProfile>
    <l3extInstP name="extnw2">
      <l3extRsInstPToProfile direction="import" tnRtctrlProfileName="rp2" />
      <l3extRsInstPToProfile direction="export" tnRtctrlProfileName="rp1" />
    </l3extInstP>
  </l3extOut>
</fvTenant>
```

ステップ7 フィルタおよびコントラクトを作成し、EPG が通信できるようにします。

この例では、フィルタ `http-filter` とコントラクト `httpCtrct` を設定します。外部 EPG およびアプリケーション EPG は、それぞれプロバイダおよびコンシューマとして、すでにコントラクト `httpCtrct` と関連付けられています。

例 :

```
<vzFilter name="http-filter">
  <vzEntry name="http-e" etherT="ip" prot="tcp"/>
</vzFilter>
<vzBrCP name="httpCtrct" scope="context">
  <vzSubj name="subj1">
    <vzRsSubjFiltAtt tnVzFilterName="http-filter"/>
  </vzSubj>
</vzBrCP>
```

ステップ8 コントラクトと外部 EPG を関連付けます。

この例では、外部 EPG extnw1 をプロバイダとして、外部 EPG extnw2 をコントラクト httpCtrct のコンシューマとして関連付けます。

```
<l3extOut name="l3out1">
  <l3extInstP name="extnw1">
    <fvRsProv tnVzBrCPName="httpCtrct"/>
  </l3extInstP>
</l3extOut>
<l3extOut name="l3out2">
  <l3extInstP name="extnw2">
    <fvRsCons tnVzBrCPName="httpCtrct"/>
  </l3extInstP>
</l3extOut>
```

REST API の例: 中継ルーティング

次の例では、REST API を使用して、2つの境界リーフスイッチで2つの L3Outs を設定します。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/.xml -->
<polUni>
  <fvTenant name="t1">
    <fvCtx name="v1"/>
    <l3extOut name="l3out1">
      <l3extRsEctx tnFvCtxName="v1"/>
      <l3extLNodeP name="nodep1">
        <bgpPeerP addr="15.15.15.2/24">
          <bgpAsP asn="100"/>
        </bgpPeerP>
        <l3extRsNodeL3OutAtt rtrId="11.11.11.103" tDn="topology/pod-1/node-101"/>
      </l3extLNodeP>
      <l3extLIIfP name="ifp1">
        <l3extRsPathL3OutAtt addr="12.12.12.3/24" ifInstT="l3-port"
tDn="topology/pod-1/paths-101/pathep-[eth1/3]" />
        <ospfIfP/>
      </l3extLIIfP>
    </l3extLNodeP>
    <l3extInstP name="extnw1">
      <l3extSubnet ip="192.168.1.0/24" scope="import-security"/>
      <l3extRsInstPToProfile direction="import" tnRtctrlProfileName="rp1"/>
      <l3extRsInstPToProfile direction="export" tnRtctrlProfileName="rp2"/>
      <fvRsProv tnVzBrCPName="httpCtrct"/>
    </l3extInstP>
    <bgpExtP/>
    <ospfExtP areaId="0.0.0.0" areaType="regular"/>
    <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
    <rtctrlProfile name="rp1">
      <rtctrlCtxP name="ctxp1" action="permit" order="0">
        <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule1"/>
      </rtctrlCtxP>
    </rtctrlProfile>
    <rtctrlProfile name="rp2">
      <rtctrlCtxP name="ctxp1" action="permit" order="0">
        <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule2"/>
      </rtctrlCtxP>
    </rtctrlProfile>
  </l3extOut>
  <l3extOut name="l3out2">
    <l3extRsEctx tnFvCtxName="v1"/>
```

```

    <l3extLNodeP name="nodep2">
      <bgpPeerP addr="25.25.25.2/24">
        <bgpAsP asn="100"/>
      </bgpPeerP>
      <l3extRsNodeL3OutAtt rtrId="22.22.22.203" tDn="topology/pod-1/node-102"
/>

      <l3extLIIfP name="ifp2">
        <l3extRsPathL3OutAtt addr="23.23.23.3/24" ifInstT="l3-port"
tDn="topology/pod-1/paths-102/pathep-[eth1/3]" />
        <ospfIfP/>
      </l3extLIIfP>
    </l3extLNodeP>
    <l3extInstP name="extnw2">
      <l3extSubnet ip="192.168.2.0/24" scope="import-security"/>
      <l3extRsInstPToProfile direction="import" tnRtctrlProfileName="rp2"/>
      <l3extRsInstPToProfile direction="export" tnRtctrlProfileName="rp1"/>
      <fvRsCons tnVzBrCPName="httpCtrct"/>
    </l3extInstP>
    <bgpExtP/>
    <ospfExtP areaId="0.0.0.0" areaType="regular"/>
    <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
    <rtctrlProfile name="rp1">
      <rtctrlCtxP name="ctxp1" action="permit" order="0">
        <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule1"/>
      </rtctrlCtxP>
    </rtctrlProfile>
    <rtctrlProfile name="rp2">
      <rtctrlCtxP name="ctxp1" action="permit" order="0">
        <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule2"/>
      </rtctrlCtxP>
    </rtctrlProfile>
  </l3extOut>
  <rtctrlSubjP name="match-rule1">
    <rtctrlMatchRtDest ip="192.168.1.0/24"/>
  </rtctrlSubjP>
  <rtctrlSubjP name="match-rule2">
    <rtctrlMatchRtDest ip="192.168.2.0/24"/>
  </rtctrlSubjP>
  <vzFilter name="http-filter">
    <vzEntry name="http-e" etherT="ip" prot="tcp"/>
  </vzFilter>
  <vzBrCP name="httpCtrct" scope="context">
    <vzSubj name="subj1">
      <vzRsSubjFiltAtt tnVzFilterName="http-filter"/>
    </vzSubj>
  </vzBrCP>
</fvTenant>
</polUni>

```

共有 L3Out

REST API を使用した共有サービスの設定

共有設定の 2 つのレイヤ REST API を使用して 2 つの Vrf に 3 が記録されます。

2 つの方法が表示されますが、2 つの Vrf にレイヤ 3 が記録されるを共有する次の REST API の設定例は次の通信します。

ステップ1 プロバイダー レイヤ 3 を設定します。

例：

```
<tenant name="t1_provider">
<fvCtx name="VRF1">
<l3extOut name="T0-o1-L3OUT-1">
  <l3extRsEctx tnFvCtxName="o1"/>
  <ospfExtP areaId='60'/>
  <l3extInstP name="l3extInstP-1">
    <fvRsProv tnVzBrCPName="vzBrCP-1">
      </fvRsProv>
    <l3extSubnet ip="192.168.2.0/24" scope="shared-rtctrl, shared-security" aggregate=""/>
    </l3extInstP>
  </l3extOut>
</tenant>
```

ステップ2 レイヤ 3 Out コンシューマを設定します。

例：

```
<tenant name="t1_consumer">
<fvCtx name="VRF2">
<l3extOut name="T0-o1-L3OUT-1">
  <l3extRsEctx tnFvCtxName="o1"/>
  <ospfExtP areaId='70'/>
  <l3extInstP name="l3extInstP-2">
    <fvRsCons tnVzBrCPName="vzBrCP-1">
      </fvRsCons>
    <l3extSubnet ip="199.16.2.0/24" scope="shared-rtctrl, shared-security"
aggregate=""/>
    </l3extInstP>
  </l3extOut>
</tenant>
```

REST API を使用した L3Out の QoS の設定

REST API を使用した L3Out での QoS ディレクトリの設定

この章では L3Out で QoS ディレクトリを設定する方法について説明します。これは、リリース 4.0(1) 以降の L3Out QoS の推奨設定方法です。Cisco APIC

次のオブジェクトの内の 1 つで L3Out の QoS を設定できます。

- Switch Virtual Interface (SVI)
- サブインターフェイス
- 外部ルーテッド

ステップ1 L3Out SVI に QoS プライオリティを設定します。

例：

REST API を使用した L3Out の QoS コントラクトの設定

```
<l3extLifP descr="" dn="uni/tn-DT/out-L3_4_2_24_SVI17/lnodep-L3_4_E2_24/lifp-L3_4_E2_24_SVI_19"
  name="L3_4_E2_24_SVI_19" prio="level6" tag="yellow-green">
  <l3extRsPathL3OutAtt addr="0.0.0.0" autostate="disabled" descr="SVI19" encap="vlan-19"
    encapScope="local" ifInstT="ext-svi" ipv6Dad="enabled" llAddr="::"
    mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
    tDn="topology/pod-1/protpaths-103-104/pathep-[V_L3_l4_2-24]"
    targetDscp="unspecified">
    <l3extMember addr="107.2.1.253/24" ipv6Dad="enabled" llAddr="::" side="B"/>
    <l3extMember addr="107.2.1.252/24" ipv6Dad="enabled" llAddr="::" side="A"/>
  </l3extRsPathL3OutAtt>
  <l3extRsLifPCustQosPol tnQosCustomPolName="VrfQos006"/>
</l3extLifP>
```

ステップ 2 サブインターフェイスに QoS プライオリティを設定します。

例 :

```
<l3extLifP dn="uni/tn-DT/out-L4E48_inter_tenant/lnodep-L4E48_inter_tenant/lifp-L4E48"
  name="L4E48" prio="level4" tag="yellow-green">
  <l3extRsPathL3OutAtt addr="210.1.0.254/16" autostate="disabled" encap="vlan-20"
    encapScope="local" ifInstT="sub-interface" ipv6Dad="enabled" llAddr="::"
    mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
    tDn="topology/pod-1/paths-104/pathep-[eth1/48]" targetDscp="unspecified"/>

  <l3extRsNdIfPol annotation="" tnNdIfPolName=""/>
  <l3extRsLifPCustQosPol annotation="" tnQosCustomPolName=" vrfQos002"/>
</l3extLifP>
```

ステップ 3 外部ルーテッドに QoS プライオリティを設定します。

例 :

```
<l3extLifP dn="uni/tn-DT/out-L2E37/lnodep-L2E37/lifp-L2E37OUT"
  name="L2E37OUT" prio="level5" tag="yellow-green">
  <l3extRsPathL3OutAtt addr="30.1.1.1/24" autostate="disabled" encap="unknown"
    encapScope="local" ifInstT="l3-port" ipv6Dad="enabled"
    llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular"
    mtu="inherit" targetDscp="unspecified"
    tDn="topology/pod-1/paths-102/pathep-[eth1/37]"/>
  <l3extRsNdIfPol annotation="" tnNdIfPolName=""/>
  <l3extRsLifPCustQosPol tnQosCustomPolName="vrfQos002"/>
</l3extLifP>
```

REST API を使用した L3Out の QoS コントラクトの設定

この項では、コントラクトを使用して L3Out の QoS を設定する方法について説明します。



- (注) リリース 4.0(1) 以降では、L3Out QoS 用にカスタム QoS ポリシーを使用することを推奨しています。[REST API を使用した L3Out での QoS ディレクトリの設定 \(611 ページ\)](#) で説明しています。

ステップ 1 テナント、VRF、ブリッジドメインを設定する場合、ポリシー適用が有効になっている状態で、出力モードに VRF を設定します (pcEnfDir="egress)。次の例のように XML で post を送信します。

例 :

```
<fvTenant name="t1">
  <fvCtx name="v1" pcEnfPref="enforced" pcEnfDir="egress"/>
  <fvBD name="bd1">
    <fvRsCtx tnFvCtxName="v1"/>
    <fvSubnet ip="44.44.44.1/24" scope="public"/>
    <fvRsBDToOut tnL3extOutName="l3out1"/>
  </fvBD>/>
</fvTenant>
```

ステップ 2 通信のため L3Out に参加して EPG を有効にする契約を作成するときは、優先順位の QoS を設定します。

この例のコントラクトには、L3Out で出力されるトラフィックの level1 の QoS 優先順位を含みますまたは、ターゲットの DSCP 値を定義する可能性があります。QoS ポリシーは、契約またはサブジェクトのいずれかでサポートされます。

フィルタに matchDscp = 「Ef」条件があるため、このタグを持つトラフィックがコントラクト件名で指定されたキューを通して L3out プロセスにより受信できます。

- (注) L3out インターフェイスでの QOS またはカスタム QOS では VRF の適用は入力とします。VRF の適用を出力にする必要があるのは、QOS 分類が EPG と L3out の間、または L3out から L3out へのトラフィックの契約で実行される場合に限りです。
- (注) QOS 分類が契約で設定され、VRF の適用が出力である場合、契約 QOS 分類は L3out インターフェイス QOS またはカスタム QOS 分類をオーバーライドするため、これか新しいもののいずれかを設定する必要があります。

例 :

```
<vzFilter name="http-filter">
  <vzEntry name="http-e" etherT="ip" prot="tcp" matchDscp="EF"/>
</vzFilter>
<vzBrCP name="httpCtrct" prio="level1" scope="context">
  <vzSubj name="subj1">
    <vzRsSubjFiltAtt tnVzFilterName="http-filter"/>
  </vzSubj>
</vzBrCP>
```

REST API を使用した SR-MPLS カスタム QoS ポリシー

SR MPLS カスタム QoS ポリシーは、MPLS QoS 出力ポリシーで定義された着信 MPLS EXP 値に基づいて、SR-MPLS ネットワークから送信されるパケットのプライオリティを定義します。これらのパケットは、ACI ファブリック内にあります。また、MPLS QoS 出力ポリシーで定義された IPv4 DSCP 値に基づく MPLS インターフェイスを介して ACI ファブリックから離れるパケットの CoS 値および MPLS EXP 値をマーキングします。

カスタム出力ポリシーが定義されていない場合、デフォルトの QoS レベル (Level13) がファブリック内のパケットに割り当てられます。カスタム出力ポリシーが定義されていない場合、デフォルトの EXP 値 (0) がファブリックから離れるパケットにマーキングされます。

ステップ1 SR-MPLS QoS ポリシーの作成

次のPOSTで、

- *customqos1*を、作成する SR-MPLS QoS ポリシーの名前に置き換えます。
- *qosMplsIngressRule*の場合：
 - *from = "2" to = "3"*を、ポリシーに一致させる EXP 範囲に置き換えます。
 - *prio = "level5"*を ACI ファブリック内にあるパケットの ACI QoS レベルに置き換えます。
 - *target = "CS5"* は、パケットが一致したときに設定する DSCP 値に置き換えます。
 - *targetCos = "4"* を、パケットが一致したときにパケットに設定する CoS 値に置き換えます。
- *qosMplsEgressRule* の場合：
 - *from = "CS2" to = "CS4"* を、ポリシーを照合する DSCP 範囲に置き換えます。
 - *targetExp = "5"* を、パケットがファブリックを離れるときに設定する EXP 値に置き換えます。
 - *targetCos = "3"* を、パケットがファブリックを離れるときに設定する CoS 値に置き換えます。

```
<polUni>
  <fvTenant name="infra">
    <qosMplsCustomPol descr="" dn="uni/tn-infra/qosmplscustom-customqos1" name="customqos1" status=""
  >
      <qosMplsIngressRule from="2" to="3" prio="level5" target="CS5" targetCos="4" status="" />
      <qosMplsEgressRule from="CS2" to="CS4" targetExp="5" targetCos="3" status="" />
    </qosMplsCustomPol>
  </fvTenant>
</polUni>
```

ステップ2 SR-MPLS QoS ポリシーの作成

次の POST で、*customqos1* を前の手順で作成した SR-MPLS QoS ポリシーの名前に置き換えます。

```
<polUni>
  <fvTenant name="infra">
    <l3extOut name="mplsOut" status="" descr="b1">
      <l3extLNodeP name="mplsLNP" status="">
        <l3extRsLNodePMplsCustQosPol tDn="uni/tn-infra/qosmplscustom-customqos1"/>
      </l3extLNodeP>
    </l3extOut>
  </fvTenant>
</polUni>
```

REST API を使用した ACI IP SLA の設定

REST API を使用した IP SLA モニタリング ポリシーの設定

REST API を使用して特定の SLA タイプのモニタリング プローブを送信できるようにするには、次の手順を実行します。Cisco APIC

IP SLA モニタリング ポリシーの設定

例：

```
<?xml version="1.0" encoding="utf-8"?>
<imdata totalCount="1">
  <fvIPSLAMonitoringPol annotation="" descr=""
dn="uni/tn-t8/ipslaMonitoringPol-ICMP-Probe"
  name="ICMP-Probe" nameAlias="" ownerKey="" ownerTag="" slaDetectMultiplier="3"
slaFrequency="5"
  slaPort="0" slaType="icmp"/>
</imdata>
```

REST API を使用した IP-SLA ट्रック メンバーの設定

REST API を使用して IP SLA ट्रック メンバーを設定するには、次の手順を実行します。

IP SLA ट्रック メンバーを設定します。

例：

```
<?xml version="1.0" encoding="utf-8"?>
<imdata totalCount="1">
  <fvTrackMember annotation="" descr="" dn="uni/tn-t8/trackmember-TM_pc_sub"
dstIpAddr="52.52.52.1" name="TM_pc_sub" nameAlias="" ownerKey="" ownerTag=""
scopeDn="uni/tn-t8/out-t8_13">
  <fvRsIpslaMonPol annotation="" tDn="uni/tn-t8/ipslaMonitoringPol-TCP-Telnet"/>
</fvTrackMember>
</imdata>
```

REST API を使用した IP-SLA ट्रック リストの設定

REST API を使用して IP SLA ट्रック リストを設定するには、次の手順を実行します。

IP SLA ट्रック リストを設定します。

例：

```
<?xml version="1.0" encoding="utf-8"?>
<imdata totalCount="1">
  <fvTrackList annotation="" descr="" dn="uni/tn-t8/tracklist-T8_pc_sub1"
name="T8_pc_sub1" nameAlias="" ownerKey="" ownerTag="" percentageDown="0"
</fvTrackList>
</imdata>
```

REST API を使用したスタティック ルートとトラック リストの関連付け

```

percentageUp="1" type="weight" weightDown="5" weightUp="10">
  <fvRsOtmListMember annotation="" tDn="uni/tn-t8/trackmember-TM_pc_sub"
    weight="10"/>
</fvTrackList>
</imdata>

```

REST API を使用したスタティック ルートとトラック リストの関連付け

REST API を使用して IP SLA トラック リストをスタティック ルートに関連付けるには、次の手順を実行します。

IP SLA トラック リストをスタティック ルートに関連付けます。

例 :

```

<?xml version="1.0" encoding="utf-8"?>
<imdata totalCount="1">
  <ipRouteP aggregate="no" annotation="" descr=""
dn="uni/tn-t8/out-t8_l3/lnodep-t8_l3_vpc1/rsnodeL3OutAtt-[topology/pod-2/node-108]/rt-[88.88.88.2/24]"

  ip="88.88.88.2/24" name="" nameAlias="" pref="1" rtCtrl="">
    <ipRsRouteTrack annotation="" tDn="uni/tn-t8/tracklist-T8_TL1_Static"/>
    <ipNexthopP annotation="" descr="" name="" nameAlias="" nhAddr="23.23.2.3"
      pref="1" type="prefix"/>
  </ipRouteP>
</imdata>

```

REST API を使用して ネクスト ホップ プロファイルのトラック リストに関連付けをする

REST API を使用して IP SLA トラック リストをネクスト ホップ プロファイルに関連付けるには、次の手順を実行します。

IP SLA トラック リストをネクスト ホップ プロファイルに関連付けます。

例 :

```

<?xml version="1.0" encoding="utf-8"?>
<imdata totalCount="1">
  <ipRouteP aggregate="no" annotation="" descr=""
dn="uni/tn-t8/out-t8_l3/lnodep-t8_l3_vpc1/rsnodeL3OutAtt-[topology/pod-2/node-109]/rt-[86.86.86.2/24]"

  ip="86.86.86.2/24" name="" nameAlias="" pref="1" rtCtrl="">
    <ipNexthopP annotation="" descr="" name="" nameAlias="" nhAddr="25.25.25.3"
      pref="1" type="prefix">
      <ipRsNexthopRouteTrack annotation=""
tDn="uni/tn-t8/tracklist-ctx0_25.25.25.3"/>
      <ipRsNHTrackMember annotation=""
tDn="uni/tn-t8/trackmember-ctx0_25.25.25.3"/>
    </ipNexthopP>
  </ipRouteP>
</imdata>

```

```
</ipRouteP>  
</imdata>
```

REST API を使用した HSRP の設定

REST API を使用した APIC 内の HSRP の設定

リーフ スイッチが設定されている場合、HSRP が有効になっています。

始める前に

- テナントおよび VRF を設定する必要があります。
- VLAN プールは、適切な VLAN 範囲が定義され、レイヤ 3 ドメインが作成されて VLAN プールに接続されている状態で設定される必要があります。
- エンティティプロファイルの接続も、レイヤ 3 ドメインに関連付けられている必要があります。
- リーフ スイッチのインターフェイス プロファイルは必要に応じて設定する必要があります。

ステップ 1 ポート セレクタを作成します。

例：

```
<polUni>  
  <infraInfra dn="uni/infra">  
    <infraNodeP name="TenantNode_101">  
      <infraLeafS name="leafselector" type="range">  
        <infraNodeBlk name="nodeblk" from_"101" to_"101">  
          </infraNodeBlk>  
        </infraLeafS>  
      <infraRsAccPortP tDn="uni/infra/accportprof-TenantPorts_101"/>  
    </infraNodeP>  
    <infraAccPortP name="TenantPorts_101">  
      <infraHPortS name="portselector" type="range">  
        <infraPortBlk name="portblk" fromCard="1" toCard="1" fromPort="41" toPort="41">  
          </infraPortBlk>  
        <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-TenantPortGrp_101"/>  
      </infraHPortS>  
    </infraAccPortP>  
    <infraFuncP>  
      <infraAccPortGrp name="TenantPortGrp_101">  
        <infraRsAttEntP tDn="uni/infra/attentp-AttEntityProfTenant"/>  
        <infraRsHIfPol tnFabricHIfPolName="default"/>  
      </infraAccPortGrp>  
    </infraFuncP>  
  </infraInfra>  
</polUni>
```

ステップ 2 テナント ポリシーを作成します。

例 :

```
<polUni>
  <fvTenant name="t9" dn="uni/tn-t9" descr="">
    <fvCtx name="t9_ctx1" pcEnfPref="unenforced">
      </fvCtx>
    <fvBD name="t9_bd1" unkMacUcastAct="flood" arpFlood="yes">
      <fvRsCtx tnFvCtxName="t9_ctx1"/>
      <fvSubnet ip="101.9.1.1/24" scope="shared"/>
    </fvBD>
    <l3extOut dn="uni/tn-t9/out-l3extOut1" enforceRtctrl="export" name="l3extOut1">
      <l3extLNodeP name="Node101">
        <l3extRsNodeL3OutAtt rtrId="210.210.121.121" rtrIdLoopBack="no" tDn="topology/pod-1/node-101"/>
      </l3extLNodeP>
      <l3extRsEctx tnFvCtxName="t9_ctx1"/>
      <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
      <l3extInstP matchT="AtleastOne" name="extEpg" prio="unspecified" targetDscp="unspecified">
        <l3extSubnet aggregate="" descr="" ip="176.21.21.21/21" name="" scope="import-security"/>
      </l3extInstP>
    </l3extOut>
  </fvTenant>
</polUni>
```

ステップ3 LLDP インターフェイス ポリシーを作成します。 .

例 :

```
<polUni>
  <fvTenant name="t9" dn="uni/tn-t9" descr="">
    <hsrpIfPol name="hsrpIfPol" ctrl="bfd" delay="4" reloadDelay="11"/>
  </fvTenant>
</polUni>
```

ステップ4 HSRP グループ ポリシーを作成します。 .

例 :

```
<polUni>
  <fvTenant name="t9" dn="uni/tn-t9" descr="">
    <hsrpIfPol name="hsrpIfPol" ctrl="bfd" delay="4" reloadDelay="11"/>
  </fvTenant>
</polUni>
```

ステップ5 HSRP インターフェイス プロファイルおよび HSRP グループ プロファイルを作成します。

例 :

```
<polUni>
  <fvTenant name="t9" dn="uni/tn-t9" descr="">
    <l3extOut dn="uni/tn-t9/out-l3extOut1" enforceRtctrl="export" name="l3extOut1">
      <l3extLNodeP name="Node101">
        <l3extLIfP name="eth1-41-v6" ownerKey="" ownerTag="" tag="yellow-green">
          <hsrpIfP name="eth1-41-v6" version="v2">
            <hsrpRsIfPol tnHsrpIfPolName="hsrpIfPol"/>
            <hsrpGroupP descr="" name="HSRPV6-2" groupId="330" groupAf="ipv6" ip="fe80::3"
mac="00:00:0C:18:AC:01" ipObtainMode="admin">
              <hsrpRsGroupPol tnHsrpGroupPolName="G1"/>
            </hsrpGroupP>
          </hsrpIfP>
          <l3extRsPathL3OutAtt addr="2002::100/64" descr="" encap="unknown" encapScope="local"
ifInstT="l3-port" llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
tDn="topology/pod-1/paths-101/pathep-[eth1/41]" targetDscp="unspecified">
            <l3extIp addr="2004::100/64"/>
          </l3extRsPathL3OutAtt>
        </l3extLNodeP>
      </l3extOut>
    </fvTenant>
  </polUni>
```



```

    </l3extRsPathL3OutAtt>
  </l3extLIfP>
  <l3extLIfP name="eth1-41-v4" ownerKey="" ownerTag="" tag="yellow-green">
    <hsrpIfP name="eth1-41-v4" version="v1">
      <hsrpRsIfPol tnHsrpIfPolName="hsrpIfPol"/>
      <hsrpGroupP descr="" name="HSRPV4-2" groupId="51" groupAf="ipv4" ip="177.21.21.21"
mac="00:00:0C:18:AC:01" ipObtainMode="admin">
        <hsrpRsGroupPol tnHsrpGroupPolName="G1"/>
      </hsrpGroupP>
    </hsrpIfP>
  </l3extRsPathL3OutAtt addr="177.21.21.11/24" descr="" encap="unknown" encapScope="local"
ifInstT="l3-port" llAddr=":" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
tDn="topology/pod-1/paths-101/pathep-[eth1/41]" targetDscp="unspecified">
    <l3extIp addr="177.21.23.11/24"/>
  </l3extRsPathL3OutAtt>
</l3extLIfP>
</l3extLNodeP>
</l3extOut>
</fvTenant>
</polUni>

```

REST API を使用した Cisco ACI GOLF の設定

REST API を使用した GOLF の設定

手順の概要

1. 次の例では、REST API を使用して GOLF のノードおよびスパイン スイッチ インターフェイスを展開する方法を示しています。
2. 次の XML で、スパイン スイッチ インターフェイスと GOLF サービスのインフラ テナント プロバイダを設定します。次の XML 構造を POST メッセージの本文に含めます。
3. 次の XML で、GOLF サービスのインフラ部分のテナント コンシューマを設定します。次の XML 構造を POST メッセージの本文に含めます。

手順の詳細

ステップ 1 次の例では、REST API を使用して GOLF のノードおよびスパイン スイッチ インターフェイスを展開する方法を示しています。

例：

```

POST
https://192.0.20.123/api/mo/uni/golf.xml

```

ステップ 2 次の XML で、スパイン スイッチ インターフェイスと GOLF サービスのインフラ テナント プロバイダを設定します。次の XML 構造を POST メッセージの本文に含めます。

例：

```

<l3extOut descr="" dn="uni/tn-infra/out-golf" enforceRtctrl="export,import"
name="golf"
ownerKey="" ownerTag="" targetDscp="unspecified">

```

```

</l3extRsEctx tnFvCtxName="overlay-1"/>
<l3extProvLbl descr="" name="golf"
  ownerKey="" ownerTag="" tag="yellow-green"/>
<l3extLNodeP configIssues="" descr=""
  name="bLeaf" ownerKey="" ownerTag=""
  tag="yellow-green" targetDscp="unspecified">
<l3extRsNodeL3OutAtt rtrId="10.10.3.3" rtrIdLoopBack="no"
  tDn="topology/pod-1/node-111">
  <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
  <l3extLoopBackIfP addr="10.10.3.3" descr="" name=""/>
</l3extRsNodeL3OutAtt>
<l3extRsNodeL3OutAtt rtrId="10.10.3.4" rtrIdLoopBack="no"
  tDn="topology/pod-1/node-112">
<l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
<l3extLoopBackIfP addr="10.10.3.4" descr="" name=""/>
</l3extRsNodeL3OutAtt>
<l3extLIfP descr="" name="portIf-spine1-3"
  ownerKey="" ownerTag="" tag="yellow-green">
  <ospfIfP authKeyId="1" authType="none" descr="" name="">
    <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
  </ospfIfP>
  <l3extRsNdIfPol tnNdIfPolName=""/>
  <l3extRsIngressQosDppPol tnQosDppPolName=""/>
  <l3extRsEgressQosDppPol tnQosDppPolName=""/>
  <l3extRsPathL3OutAtt addr="7.2.1.1/24" descr=""
    encap="vlan-4"
    encapScope="local"
    ifInstT="sub-interface"
    llAddr="::" mac="00:22:BD:F8:19:FF"
    mode="regular"
    mtu="1500"
    tDn="topology/pod-1/paths-111/pathep-[eth1/12]"
    targetDscp="unspecified"/>
</l3extLIfP>
<l3extLIfP descr="" name="portIf-spine2-1"
  ownerKey=""
  ownerTag=""
  tag="yellow-green">
  <ospfIfP authKeyId="1"
    authType="none"
    descr=""
    name="">
    <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
  </ospfIfP>
  <l3extRsNdIfPol tnNdIfPolName=""/>
  <l3extRsIngressQosDppPol tnQosDppPolName=""/>
  <l3extRsEgressQosDppPol tnQosDppPolName=""/>
  <l3extRsPathL3OutAtt addr="7.1.0.1/24" descr=""
    encap="vlan-4"
    encapScope="local"
    ifInstT="sub-interface"
    llAddr="::" mac="00:22:BD:F8:19:FF"
    mode="regular"
    mtu="9000"
    tDn="topology/pod-1/paths-112/pathep-[eth1/11]"
    targetDscp="unspecified"/>
</l3extLIfP>
<l3extLIfP descr="" name="portif-spine2-2"
  ownerKey=""
  ownerTag=""
  tag="yellow-green">
  <ospfIfP authKeyId="1"
    authType="none" descr=""
    name="">

```

```

        <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
    </ospfIfP>
    <l3extRsNdIfPol tnNdIfPolName=""/>
    <l3extRsIngressQosDppPol tnQosDppPolName=""/>
    <l3extRsEgressQosDppPol tnQosDppPolName=""/>
    <l3extRsPathL3OutAtt addr="7.2.2.1/24" descr=""
        encap="vlan-4"
        encapScope="local"
        ifInstT="sub-interface"
            llAddr="::" mac="00:22:BD:F8:19:FF"
            mode="regular"
            mtu="1500"
            tDn="topology/pod-1/paths-112/pathep-[eth1/12]"
            targetDscp="unspecified"/>
    </l3extLIIfP>
    <l3extLIIfP descr="" name="portIf-spine1-2"
        ownerKey="" ownerTag="" tag="yellow-green">
        <ospfIfP authKeyId="1" authType="none" descr="" name="">
            <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
        </ospfIfP>
        <l3extRsNdIfPol tnNdIfPolName=""/>
        <l3extRsIngressQosDppPol tnQosDppPolName=""/>
        <l3extRsEgressQosDppPol tnQosDppPolName=""/>
        <l3extRsPathL3OutAtt addr="9.0.0.1/24" descr=""
            encap="vlan-4"
            encapScope="local"
            ifInstT="sub-interface"
                llAddr="::" mac="00:22:BD:F8:19:FF"
                mode="regular"
                mtu="9000"
                tDn="topology/pod-1/paths-111/pathep-[eth1/11]"
                targetDscp="unspecified"/>
    </l3extLIIfP>
    <l3extLIIfP descr="" name="portIf-spine1-1"
        ownerKey="" ownerTag="" tag="yellow-green">
        <ospfIfP authKeyId="1" authType="none" descr="" name="">
            <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
        </ospfIfP>
        <l3extRsNdIfPol tnNdIfPolName=""/>
        <l3extRsIngressQosDppPol tnQosDppPolName=""/>
        <l3extRsEgressQosDppPol tnQosDppPolName=""/>
        <l3extRsPathL3OutAtt addr="7.0.0.1/24" descr=""
            encap="vlan-4"
            encapScope="local"
            ifInstT="sub-interface"
                llAddr="::" mac="00:22:BD:F8:19:FF"
                mode="regular"
                mtu="1500"
                tDn="topology/pod-1/paths-111/pathep-[eth1/10]"
                targetDscp="unspecified"/>
    </l3extLIIfP>
    <bgpInfraPeerP addr="10.10.3.2"
        allowedSelfAsCnt="3"
        ctrl="send-com,send-ext-com"
        descr="" name="" peerCtrl=""
        peerT="wan"
        privateASctrl="" ttl="2" weight="0">
        <bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
        <bgpAsP asn="150" descr="" name="aspn"/>
    </bgpInfraPeerP>
    <bgpInfraPeerP addr="10.10.4.1"
        allowedSelfAsCnt="3"
        ctrl="send-com,send-ext-com" descr="" name="" peerCtrl=""
        peerT="wan"

```

```

        privateASctrl="" ttl="1" weight="0">
        <bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
        <bgpAsP asn="100" descr="" name=""/>
    </bgpInfraPeerP>
    <bgpInfraPeerP addr="10.10.3.1"
        allowedSelfAsCnt="3"
        ctrl="send-com,send-ext-com" descr="" name="" peerCtrl=""
        peerT="wan"
        privateASctrl="" ttl="1" weight="0">
        <bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
        <bgpAsP asn="100" descr="" name=""/>
    </bgpInfraPeerP>
</l3extLNodeP>
<bgpRtTargetInstrP descr="" name="" ownerKey="" ownerTag="" rtTargetT="explicit"/>
<l3extRsL3DomAtt tDn="uni/l3dom-l3dom"/>
<l3extInstP descr="" matchT="AtleastOne" name="golfInstP"
    prio="unspecified"
    targetDscp="unspecified">
    <fvRsCustQosPol tnQosCustomPolName=""/>
</l3extInstP>
<bgpExtP descr=""/>
<ospfExtP areaCost="1"
    areaCtrl="redistribute,summary"
    areaId="0.0.0.1"
    areaType="regular" descr=""/>
</l3extOut>

```

ステップ 3 次の XML で、GOLF サービスのインフラ部分のテナント コンシューマを設定します。次の XML 構造を POST メッセージの本文に含めます。

例 :

```

<fvTenant descr="" dn="uni/tn-pep6" name="pep6" ownerKey="" ownerTag="">
  <vzBrCP descr="" name="webCtrct"
    ownerKey="" ownerTag="" prio="unspecified"
    scope="global" targetDscp="unspecified">
    <vzSubj consMatchT="AtleastOne" descr=""
      name="http" prio="unspecified" provMatchT="AtleastOne"
      revFltPorts="yes" targetDscp="unspecified">
      <vzRsSubjFiltAtt directives="" tnVzFilterName="default"/>
    </vzSubj>
  </vzBrCP>
  <vzBrCP descr="" name="webCtrct-pod2"
    ownerKey="" ownerTag="" prio="unspecified"
    scope="global" targetDscp="unspecified">
    <vzSubj consMatchT="AtleastOne" descr=""
      name="http" prio="unspecified"
      provMatchT="AtleastOne" revFltPorts="yes"
      targetDscp="unspecified">
      <vzRsSubjFiltAtt directives=""
        tnVzFilterName="default"/>
    </vzSubj>
  </vzBrCP>
  <fvCtx descr="" knwMcastAct="permit"
    name="ctx6" ownerKey="" ownerTag=""
    pcEnfDir="ingress" pcEnfPref="enforced">
    <bgpRtTargetP af="ipv6-ucast"
      descr="" name="" ownerKey="" ownerTag="">
      <bgpRtTarget descr="" name="" ownerKey="" ownerTag=""
        rt="route-target:as4-nn2:100:1256"
        type="export"/>
      <bgpRtTarget descr="" name="" ownerKey="" ownerTag=""
        rt="route-target:as4-nn2:100:1256"

```

```

        type="import"/>
    </bgpRtTargetP>
    <bgpRtTargetP af="ipv4-ucast"
        descr="" name="" ownerKey="" ownerTag="">
        <bgpRtTarget descr="" name="" ownerKey="" ownerTag=""
            rt="route-target:as4-nn2:100:1256"
            type="export"/>
        <bgpRtTarget descr="" name="" ownerKey="" ownerTag=""
            rt="route-target:as4-nn2:100:1256"
            type="import"/>
    </bgpRtTargetP>
    <fvRsCtxToExtRouteTagPol tnL3extRouteTagPolName=""/>
    <fvRsBgpCtxPol tnBgpCtxPolName=""/>
    <vzAny descr="" matchT="AtleastOne" name=""/>
    <fvRsOspfCtxPol tnOspfCtxPolName=""/>
    <fvRsCtxToEpRet tnFvEpRetPolName=""/>
    <l3extGlobalCtxName descr="" name="dci-pep6"/>
</fvCtx>
<fvBD arpFlood="no" descr="" epMoveDetectMode=""
    ipLearning="yes"
    limitIpLearnToSubnets="no"
    llAddr="::" mac="00:22:BD:F8:19:FF"
    mcastAllow="no"
    multiDstPktAct="bd-flood"
    name="bd107" ownerKey="" ownerTag="" type="regular"
    unicastRoute="yes"
    unkMacUcastAct="proxy"
    unkMcastAct="flood"
    vmac="not-applicable">
    <fvRsBDToNdP tnNdIfPolName=""/>
    <fvRsBDToOut tnL3extOutName="routAccounting-pod2"/>
    <fvRsCtx tnFvCtxName="ctx6"/>
    <fvRsIgmprsn tnIgmprsnPolName=""/>
    <fvSubnet ctrl="" descr="" ip="27.6.1.1/24"
        name="" preferred="no"
        scope="public"
        virtual="no"/>
    <fvSubnet ctrl="nd" descr="" ip="2001:27:6:1::1/64"
        name="" preferred="no"
        scope="public"
        virtual="no">
        <fvRsNdPfxPol tnNdPfxPolName=""/>
    </fvSubnet>
    <fvRsBdToEpRet resolveAct="resolve" tnFvEpRetPolName=""/>
</fvBD>
<fvBD arpFlood="no" descr="" epMoveDetectMode=""
    ipLearning="yes"
    limitIpLearnToSubnets="no"
    llAddr="::" mac="00:22:BD:F8:19:FF"
    mcastAllow="no"
    multiDstPktAct="bd-flood"
    name="bd103" ownerKey="" ownerTag="" type="regular"
    unicastRoute="yes"
    unkMacUcastAct="proxy"
    unkMcastAct="flood"
    vmac="not-applicable">
    <fvRsBDToNdP tnNdIfPolName=""/>
    <fvRsBDToOut tnL3extOutName="routAccounting"/>
    <fvRsCtx tnFvCtxName="ctx6"/>
    <fvRsIgmprsn tnIgmprsnPolName=""/>
    <fvSubnet ctrl="" descr="" ip="23.6.1.1/24"
        name="" preferred="no"
        scope="public"
        virtual="no"/>

```

```

    <fvSubnet ctrl="nd" descr="" ip="2001:23:6:1::1/64"
      name="" preferred="no"
      scope="public" virtual="no">
      <fvRsNdPfxPol tnNdPfxPolName=""/>
    </fvSubnet>
    <fvRsBdToEpRet resolveAct="resolve" tnFvEpRetPolName=""/>
  </fvBD>
</vnsSvcCont/>
<fvRsTenantMonPol tnMonEPGPolName=""/>
<fvAp descr="" name="AP1"
  ownerKey="" ownerTag="" prio="unspecified">
  <fvAEPg descr=""
    isAttrBasedEPg="no"
    matchT="AtleastOne"
    name="epg107"
    pcEnfPref="unenforced" prio="unspecified">
    <fvRsCons prio="unspecified"
      tnVzBrCPName="webCtrct-pod2"/>
    <fvRsPathAtt descr=""
      encap="vlan-1256"
      instrImedcy="immediate"
      mode="regular" primaryEncap="unknown"
      tDn="topology/pod-2/paths-107/pathep-[eth1/48]"/>
    <fvRsDomAtt classPref="encap" delimiter=""
      encap="unknown"
      instrImedcy="immediate"
      primaryEncap="unknown"
      resImedcy="lazy" tDn="uni/phys-phys"/>
    <fvRsCustQosPol tnQosCustomPolName=""/>
    <fvRsBd tnFvBDName="bd107"/>
    <fvRsProv matchT="AtleastOne"
      prio="unspecified"
      tnVzBrCPName="default"/>
  </fvAEPg>
  <fvAEPg descr=""
    isAttrBasedEPg="no"
    matchT="AtleastOne"
    name="epg103"
    pcEnfPref="unenforced" prio="unspecified">
    <fvRsCons prio="unspecified" tnVzBrCPName="default"/>
    <fvRsCons prio="unspecified" tnVzBrCPName="webCtrct"/>
    <fvRsPathAtt descr="" encap="vlan-1256"
      instrImedcy="immediate"
      mode="regular" primaryEncap="unknown"
      tDn="topology/pod-1/paths-103/pathep-[eth1/48]"/>
    <fvRsDomAtt classPref="encap" delimiter=""
      encap="unknown"
      instrImedcy="immediate"
      primaryEncap="unknown"
      resImedcy="lazy" tDn="uni/phys-phys"/>
    <fvRsCustQosPol tnQosCustomPolName=""/>
    <fvRsBd tnFvBDName="bd103"/>
  </fvAEPg>
</fvAp>
<l3extOut descr=""
  enforceRtctrl="export"
  name="routAccounting-pod2"
  ownerKey="" ownerTag="" targetDscp="unspecified">
  <l3extRsEctx tnFvCtxName="ctx6"/>
  <l3extInstP descr=""
    matchT="AtleastOne"
    name="accountingInst-pod2"
    prio="unspecified" targetDscp="unspecified">
  <l3extSubnet aggregate="export-rtctrl,import-rtctrl"

```

```

        descr="" ip="::/0" name=""
        scope="export-rtctrl,import-rtctrl,import-security"/>
<l3extSubnet aggregate="export-rtctrl,import-rtctrl"
  descr=""
  ip="0.0.0.0/0" name=""
  scope="export-rtctrl,import-rtctrl,import-security"/>
<fvRsCustQosPol tnQosCustomPolName=""/>
<fvRsProv matchT="AtleastOne"
  prio="unspecified" tnVzBrCPName="webCtrct-pod2"/>
</l3extInstP>
<l3extConsLbl descr=""
  name="golf2"
  owner="infra"
  ownerKey="" ownerTag="" tag="yellow-green"/>
</l3extOut>
<l3extOut descr=""
  enforceRtctrl="export"
  name="routAccounting"
  ownerKey="" ownerTag="" targetDscp="unspecified">
<l3extRsEctx tnFvCtxName="ctx6"/>
<l3extInstP descr=""
  matchT="AtleastOne"
  name="accountingInst"
  prio="unspecified" targetDscp="unspecified">
<l3extSubnet aggregate="export-rtctrl,import-rtctrl" descr=""
  ip="0.0.0.0/0" name=""
  scope="export-rtctrl,import-rtctrl,import-security"/>
<fvRsCustQosPol tnQosCustomPolName=""/>
<fvRsProv matchT="AtleastOne" prio="unspecified" tnVzBrCPName="webCtrct"/>
</l3extInstP>
<l3extConsLbl descr=""
  name="golf"
  owner="infra"
  ownerKey="" ownerTag="" tag="yellow-green"/>
</l3extOut>
</fvTenant>

```

REST API を使用した DCIG への BGP EVPN タイプ 2 ホスト ルート配信の有効化

次のように REST API を使用して、BGP EVPN タイプ 2 ホスト ルートの配信を有効にします。

始める前に

EVPN サービスを設定する必要があります。

ステップ 1 次の例のように、XML が含まれている POST で、ホスト ルート リーク ポリシーを設定します。

例 :

```
<bgpCtxAfPol descr="" ctrl="host-rt-leak" name="bgpCtxPol_0 status=""/>
```

ステップ 2 次の例のように、XML が含まれている POST を使用してアドレス ファミリの一方または両方の VRF BGP アドレス ファミリ コンテキスト ポリシーに、ポリシーを適用します。

例 :

```
<fvCtx name="vni-10001">  
<fvRsCtxToBgpCtxAfPol af="ipv4-ucast" tnBgpCtxAfPolName="bgpCtxPol_0"/>  
<fvRsCtxToBgpCtxAfPol af="ipv6-ucast" tnBgpCtxAfPolName="bgpCtxPol_0"/>  
</fvCtx>
```

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。

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。