Unified MPLS の機能、特徴、および設定例

目次

概要

このドキュメントでは、スケーリングを可能にするユニファイド マルチプロトコル ラベル スイッチング（MPLS）について説明します。 これは、従来セグメント化されていたインフラストラクチャで、単純なエンドツーエンド トラフィックやサービスを実現するテクノロジー ソリューションのフレームワークです。 これにより、階層型インフラストラクチャの利点を活用しながら、ネットワーク設計がより拡張可能かつ簡素になります。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

ネットワークの進化

ネットワーク パケット ベースのサービスの歴史を見ると、ネットワーク ビジネスの価値が変化しているのがわかります。 アプリケーションをできる限り円滑にするための分散接続の強化に始まり、モバイル コラボレーションをサポートするためのコラボレーション テクノロジーが登場しました。 最終的にオンデマンド クラウド サービスがアプリケーション サービスとともに導入されたことで、組織内で使用されるツールが最適化され、安定性と所有コストが改善しました。

Figure 1

このようにネットワークの価値と機能が継続的に高まった結果、ネットワークのシンプルさ、管理容易性、統合性、安定性がさらに広く必要とされるようになりました。運用形態が「島」のようなセグメントに分割され、真のエンドツーエンド パス制御が存在しないためです。 管理しやすく、何 10 万ものノードに拡張可能で、現在の高可用性/高速コンバージェンス テクノロジを使用できる単一のアーキテクチャに対するニーズが現在、大きくなっています。 これを満たすのが Unified MPLS です。これは、単一のコントロール プレーンとエンドツーエンド パスの可視性を備えた、セグメント化されたネットワークです。

最近のネットワーク要件

- 帯域幅要件の増加（ビデオ）
- より複雑になるアプリケーション（クラウドおよび仮想化）
- コンバージェンスの必要性の増加（モビリティ）

より大規模になっていくネットワークと、より複雑化するアプリケーションの要件に対して、どうすれば MPLS 運用を簡素化できますか。

さまざまなアクセス テクノロジーを使用した従来の MPLS の課題

- Traffic Engineering Fast Reroute（TE FRR）による 50 ミリ秒のコンバージェンスを実現するための複雑さ

- レイヤ 2 プロトコルでの高度なルーティング プロトコルとインタラクションの必要性
- 大規模ネットワークを複数ドメインに分割すると同時に、エンドツーエンドにサービスを提供
- 共通のエンドツーエンド コンバージェンスおよび復元メカニズム
- 複数のドメインにおよぶエンドツーエンドのトラブルシューティングとプロビジョニング

Unified MPLS の長所を次に示します。

- より少ない運用ポイント。 一般的なトランスポート プラットフォームでは、運用ポイント（operational point）を介して各ネットワーク要素でサービスを設定する必要があります。 管理システムはトポロジを把握している必要があります。Unified MPLS では、すべての MPLS アイランド（島）が統合されており、運用ポイントの数が最小化されます。
- サービスを容易にプロビジョニングできます： 疑似回線ステッチング（PW ステッチング）または InterAS メカニズムを使用しないレイヤ 3（L3）VPN、バーチャル プライベート ワイヤ サービス（VPWS）、バーチャル プライベート LAN サービス（VPLS）。 集約における MPLS の導入により、MPLS アイランドを形成するいくつかのスタティック設定が回避されます。
- エンドツーエンド MPLS トランスポートを提供。
- 内部ゲートウェイ プロトコル（IGP）エリアの分離と、小規模なルーティング テーブルを維持します。
- 高速コンバージェンス
- 設定とトラブルシューティングが容易。
- 任意のアクセス テクノロジーとの統合が可能。
- IPv6 に対応。

Cisco Unified MPLS

Unified MPLS は従来の MPLS にいくつかの機能を追加して定義されたもので、拡張性、セキュリティ、シンプルさ、管理容易性が向上しています。 エンドツーエンドで MPLS サービスを提供するには、エンドツーエンド Labeled Switches Path（LSP）が必要です。 これは、MPLS サービス（MPLS VPN、MPLS L2VPN）をそのままの状態で維持し、かつ拡張性を向上することを目的としています。 このためには、一部の IGP プレフィックスを Border Gateway Protocol（BGP）に移動します（プロバイダー エッジ（PE）ルータのループバック プレフィックス）。次にこれらのプレフィックスがエンドツーエンドで配布されます。

図 2

Cisco Unified MPLS のアーキテクチャを見ていく前に、これを実現するために使用されている主な機能を理解することが重要です。

機能とコンポーネント

BGP-4 でのラベル情報の伝達（RFC 3107）

これは、ネットワーク セグメント間でプレフィックスを交換するためのスケーラブルな方法を実現するための前提条件です。 IGP（Open Shortest Path First（OSPF）、intermediate system-to-intermediate system（IS-IS）、Enhanced Interior Gateway Routing Protocol（EIGRP））を 単一

のドメインに簡単に統合できます。 ただし、IGP は数十万ものプレフィックスを伝達するように設計されていません。 その目的で選択されるプロトコルは BGP です。 これは、数百万ものエントリを含む MPLS-VPN 環境と数十万ものルートを含むインターネットをサポートする、十分に検証されたプロトコルです。 Cisco Unified MPLS では、ラベル情報交換をともなう MPLS BGP-4 を使用します（RFC3107）。 BGP がルートを配布するときには、そのルートにマッピングされる MPLS ラベルを配布することもできます。 ルートの MPLS ラベル マッピング情報は、ルートについての情報を含む BGP 更新メッセージによって伝送されます。 ネクスト ホップが変わらない場合はラベルが維持され、ネクスト ホップが変化する場合はラベルが変更されます。 Unified MPLS では、エリア境界ルータ（ABR）でネクストホップが変化します。

両方の BGP ルータで RFC 3107 を有効にすると、ルートとともに MPLS ラベルを送信できることがルータ間で相互にアドバタイズされます。 ルータ間で MPLS ラベルを送信可能であると正常にネゴシエーションされると、それらのルータからのすべての発信 BGP アップデートに MPLS ラベルが追加されます。

セグメント間でエンドツーエンド パス情報を保持するには、ラベル交換が必要です。 その結果、各セグメントがオペレータによる管理可能なサイズにまで小さくなると同時に、2 つの異なる IP スピーカー間でパスを認識するための回線情報が配布されます。

この仕組みを説明しましょう

図 3

図 3 では、Label Discovery Protocol Labeled Switches Path（LDP LSP）の 3 つのセグメントがあり、アクセス ネットワークでは LDP が無効です。 ここでの目標は、これらを結合して、集約前（Pre-Agg）ノード間で 1 つの MPLS パス（内部 BGP（iBGP）階層 LSP）にすることです。 ネットワークが単一 BGP 自律システム（AS）であるため、すべてのセッションは iBGP セッションです。 各セグメントは独自の IGP（OSPF、IS-IS、または EIGRP）および LSPP LSP パスを IGP ドメイン内で実行します。 Cisco Unified MPLS では、各セッションで設定される Pv4+ ラベルを伝達するために、セグメントを結合するルータ（ABR）は Next-Hop-Self および RFC 3107 による BGP インライン ルート リフレクタである必要があります。 これらの BGP スピーカーは、ABR と呼ばれる Cisco Unified MPLS アーキテクチャ内にあります。

ABR をインライン ルート リフレクタにするのは、なぜですか

Unified MPLS の目的の 1 つは、高い拡張性を持つエンドツーエンド インフラストラクチャを実現することです。 つまり、操作しやすいように各セグメントをシンプルに保つ必要があります。 すべてのピアリングは iBGP ピアリングであるため、ネットワーク全体のすべての iBGP スピーカー間のピアリングをフルメッシュで行う必要があります。 その結果、BGP スピーカーが何千もある場合には、まったく非実用的なネットワーク環境になります。 ABR がルート リフレクタになった場合、iBGP ピアリングの数は、AS 全体のすべての BGP スピーカー間ではなくセグメントごとの BGP スピーカー数に減ります。

なぜ Next-Hop-Self を使用するのですか

BGP の機能の基礎となっているのは、再帰的なルーティング ルックアップです。 これが行われる理由は、基盤となる IGP 内の拡張性を提供するためです。 再帰ルックアップのために、BGP は各 BGP ルート エントリに付加されたネクストホップを使用します。 たとえばソース ノードから宛先ノードにパケットを送信する必要が生じ、パケットが BGP ルータに達した場合、BGP ルータは自身の BGP ルーティング テーブルでルーティング ルックアップを行います。 宛先ノードへのルートが検出され、次のステップとしてネクストホップが検出されます。 基盤となる IGP でこのネクストホップが既知である必要があります。 最後のステップとして、そのネクストホップ

に付加されている IP と MPLS ラベル情報に基づき、BGP ルータがパケットを転送します。

各セグメント内で、ネクストホップだけが IGP で既知である必要があるようにするには、BGP エントリに付加されたネクストホップが近接（または遠隔）セグメントではなく、そのネットワーク セグメント内にある必要があります。 Next-Hop-Self 機能を使用して BGP ネクストホップを書き換える場合は、ネクストホップがローカル セグメント内にあることを確認してください。

まとめ

図 4

図 4 は、L3 VPN プレフィックス「A」とラベル交換が機能する方法、および両方の PE 間のトラフィック フローに関するエンドツーエンド パス情報を示す MPLS ラベル スタックが作成される方法を示しています。

ネットワークは、3 つの独立した IGP/LDP ドメインに分割されています。 ルータでのルーティングと転送テーブルのサイズが小さくなり、安定性が増し、コンバージェンスが高速になります。 LDP は、ドメインにおけるドメイン内 LSP の構築に使用されます。 RFC 3107 BGP IPv4+ ラベルは、ドメイン間のラベル配布プロトコルとして、ドメイン間の階層 BGP LSP の構築に使用されます。 BGP3107 は、Unified MPLS アーキテクチャの転送ラベル スタックに追加のラベルを挿入します。

ドメイン内 - LDP LSP

ドメイン間 - BGP 階層型 LSP

図 5：

VPN プレフィクス「A」が PE 31 によって PE11 にアドバタイズされます。L3VPN サービス ラベル 30、およびエンドツーエンド ドメイン間階層 BGP LSP を介した PE 31 のループバックとしてネクストホップが使用されます。 ここで、PE11 から PE31 への VPN プレフィクス「A」の転送パスに注目してください。

- PE11 では、PE31 との BGP セッションを介してプレフィックス A がネクストホップ PE31 として認識され、BGP ラベル 100 で P1 を介して PE31 が再帰的に到達可能です。 IPv4 とラベル情報を送信するために RFC 3107 機能が有効になっているため、PE11 が P1 から IPv4+ ラベル情報を BGP 更新として受信しました。
- P1 はドメイン内 LDP LSP を介して PE11 から到達可能であり、BGP ラベルの上に別の LDP ラベルを追加します。 最終的に、3 つのラベル付きでパケットが PE11 から送出されます。 たとえば 30 L3VPN サービス ラベル、100 BGP ラベル、および 200 LDP IGP ラベルです。
- LDP 最上位ラベルは引き続きドメイン内 LDP LSP でスワップし、パケットは Penultimate Hop Popping（PHP）後に 2 つのラベル付きで P1 に到達します。
- P1 は Next-Hop Self 機能でインライン ルート リフレクタ（RR）として設定され、2 つの IGP ドメインまたは LDP LSP を結合します。
- P1 では、PE31 のネクストホップが P2 に変更され、IPv4+ ラベル（RFC3107）付きで BGP 経由で更新が受信されます。 ネクストホップが変更されたため BGP ラベルが新しいラベルとスワップされ、IGP ラベルが最上位にプッシュされます。
- 3 つのラベル付きでパケットが P1 ノードから送出され、サービス ラベル 30 は無変更のまま

です。 つまり、30 L3VPN サービス ラベル、101 BGP ラベル、201 LDP ラベルです。
- LDP 最上位ラベルがドメイン内 LDP LSP でスワップし、パケットは PHP 後に 2 つのラベル付きで P2 に到達します。
- P2 では、PE31 のネクスト ホップが再び変更され、IGP を介して到達可能になります。 PHP 用に PE31 から暗黙的 NULL BGP ラベルが受信されるため、BGP ラベルが削除されます。
- パケットは 2 つのラベル付きで出発します。 たとえば 30 L3VPN サービス ラベルと 110 LDP ラベルです。
- PE31 では、LDP ラベルの PHP 後に 1 つのラベル付きで、サービス ラベル 30 に基づいてパケットが到達します。 ラベルが付いていないパケットは Virtual Routing and Forwarding（VRF）の下で CE31 宛先に転送されます。

MPLS ラベル スタックを見ると、MPLS スイッチング環境において、以前のプレフィックスおよびラベルの交換に基づく送信元/宛先デバイス間のパケット切り替えを確認できます。

図 6

BGP プレフィックス非依存コンバージェンス（BGP PIC）

これは、BGP 障害シナリオで使用されているシスコのテクノロジーです。 BGP 再コンバージェンスでは、従来の損失時間（秒）なしでネットワークを収束できます。 BGP PIC を使用すると、ほとんどの障害シナリオで再コンバージョンの時間を 100 ミリ秒未満に短縮できます。

これを実現する方法

従来は、BGP が障害を検出すると、それぞれの BGP エントリに対してベスト パスを再計算します。 ルーティング テーブルに数千におよぶルート エントリがある場合、かなりの時間がかかることがあります。 さらに、この BGP ルータは、ネットワーク トポロジの変更とベスト パスの変更を通知するために、各ネイバーにすべての新しいベスト パスを配布する必要があります。 最後のステップとして、それぞれの受信側 BGP スピーカーはベスト パス計算を実行して新しいベスト パスを検出する必要があります。

最初の BGP スピーカーが何らかの問題を検出するたびに、ベスト パス計算が開始され、隣接するすべての BGP スピーカーが独自の再計算を完了するまではトラフィック フローが失われることがあります。

図 7

IP および MPLS VPN 向け BGP PIC 機能により、ネットワーク障害後のコンバージェンスが向上します。 このコンバージェンスは、コアの障害とエッジの障害の両方に適用され、IP および MPLS ネットワークの両方で使用可能です。 IP および MPLS VPN 向け BGP PIC 機能は、障害が検出された場合、即座にバックアップ/代替パスに引き継いで高速フェールオーバーできるように、ルーティング情報ベース（RIB）、転送情報ベース（FIB）、および Cisco Express Forwarding（CEF）にバックアップ/代替パスを作成し、保存します。

ネクストホップ情報の 1 回の書き換えによって、トラフィック フローが復元されます。 またネットワーク BGP コンバージェンスはバックグラウンドで発生しますが、トラフィック フローは影響を受けません。 この書き換えは 50 ミリ秒以内で完了します。 このテクノロジーを使用すると、ネットワーク収束は数秒から 50 ミリ秒に短縮され、IGP コンバージェンスも行われます。

BGP 追加パス

BGP 追加パス（Add-Path）は、BGP エントリが BGP スピーカー間で通信される方法を改善します。 特定の BGP スピーカーで、特定の宛先へのエントリが複数ある場合、その BGP スピーカーはその宛先のベスト パスであるエントリのみをネイバーに送信します。 その結果、同じ宛先への複数パスのアドバタイズメントを可能にするプロビジョンは行われません。

BGP 追加パスは、ベスト パス以外の複数パスを可能にする BGP 機能です。 以前のパスを暗黙的に新しいパスに置き換えることなく、同じ宛先への複数パスが可能になります。 BGP のこの拡張機能は、BGP ルート リフレクタが使用される場合の BGP PIC を支援するうえで特に重要です。これにより、1 つの AS 内の複数の BGP スピーカーが、ルート リフレクタに基づく「ベスト BGP パス」以外の複数の BGP パスにアクセスできるようになります。

IGP 高速コンバージェンス用のループフリー代替および rLFA

ループフリー代替（LFA）と呼ばれる新たなテクノロジーによって、リンクまたはノードの障害後に 50 ミリ秒以内の復元を実現する操作が大幅に簡素化されます。 LFA によってリンクステート ルーティング プロトコル（IS-IS および OSPF）が強化され、ループフリー手法で代替ルーティング パスが検出されます。 LFA では各ルータでバックアップ パスを事前定義することができ、隣接関係（ネットワーク ノードまたはリンク）に障害があった場合、そのパスが使用されます。 リンクまたはノードの障害時に 50 ミリ秒以内の復元を可能にするには、MPLS TE FRR を導入できます。 ただし、これを使用するには TE トンネルのセットアップ/管理用に別のプロトコル（Resource Reservation Protocol（RSVP））を追加する必要があります。 帯域幅管理のためにこれが必要になる可能性がありますが、保護および復元操作では帯域幅管理は必要ありません。したがって、単にリンクとノードを保護するだけであれば、RSVP TE の追加によるオーバーヘッドは高いと考えられます。

LFA は、このようなシナリオで RSVP TE を導入する必要のないシンプルかつ簡単な手法を提供します。 これらの手法により、現在の大規模ネットワークで相互接続されたルータは、オペレータが設定を行わなくても、リンク/ノード障害時に 50 ミリ秒で復元できます。

図 8

LFA-FRR は、IP、MPLS、Ethernet Over MPLS（EoMPLS）、Inverse Multiplexing over ATM（IMA）over MPLS、Circuit Emulation Service over Packet Switched Network（CESoPSN）over MPLS、および Structure-Agnostic Time Division Multiplexing over Packet（SAToP）over MPLS networks でのユニキャスト トラフィックのローカル保護を実現する機能です。 ただし、いくつかのトポロジ（リング トポロジなど）では、LFA-FRR 単体では提供されない保護が必要です。 このような状況ではリモート LFA-FRR 機能が役立ちます。

リモート LFA-FRR は、LFA-FRR の基本動作を任意のトポロジに拡張します。 障害が発生したノードのトラフィックを、2 ホップ以上離れたリモート LFA に転送します。 図 9 では、C1 と C2 の間のリンクが A1 に到達できない場合、C2 は、ダイレクトされた LDP セッションを介して、A1 に到達可能な C5 にパケットを転送します。

図 9

リモート LFA-FRR では、ノードは動的に LFA ノードを計算します。（直接接続されていない

）代替ノードが特定されると、ノードは代替ノードへのダイレクトされた Label Distribution Protocol（LDP）セッションを自動的に確立します。 ダイレクトされた LDP セッションは、特定の転送エラー訂正（FEC）用にラベルを交換します。

リンクに障害が発生すると、ノードはラベル スタック構成を使用してトラフィックをリモート LFA ノードにトンネリングし、トラフィックを宛先に転送します。 ラベル交換とリモート LFA ノードへのトンネリングはすべて動的に行われ、プロビジョニングは必要ありません。 ラベル交換とトンネリングはすべて動的に行われるため、手動でプロビジョニングする必要はありません。

ドメイン内 LSP では、リング トポロジでのユニキャスト MPLS トラフィックにリモート LFA FRR が使用されます。 リモート LFA FRR は IGP ルーティング テーブル内のすべてのプレフィックスに関するバックアップ パスを事前計算するため、障害発生時にノードは迅速にバックアップ パスに切り替えられます。 これによって、約 50 ミリ秒での復元が可能になります。

Cisco Unified MPLS アーキテクチャ例

これまでのすべてのツールと機能をネットワーク環境内で 1 つにまとめると、Cisco Unified MPLS ネットワーキング環境が形成されます。 大規模サービス プロバイダでは、この例のようなアーキテクチャを使用します。

図 10

- コアと集約は、個別の IGP/LDP ドメインとして編成されます。
- ドメイン間階層型 LSP は RFC 3107、BGP IPv4+ ラベルに基づいており、集約前ノードに拡張されています。
- LDP に基づくドメイン内 LSP。
- 無線アクセス ネットワーク内部ゲートウェイ プロトコル（RAN IGP）をドメイン間 iBGP に配布することで、アクセス ネットワーク内でドメイン間コア/集約 LSP が拡張され、必要なラベル付き iBGP プレフィクス（MPC（モバイル パケット コア）ゲートウェイ）を（BGP コミュニティを介して）RAN IGP に配布します。

Unified MPLS の設定例

ここでは、Unified MPLS の単純な例を示します。

コア エリア境界ルータ - Cisco IOS? XR

集約前およびセル サイト ゲートウェイ ルータ - Cisco IOS

図 11

200:200 MPC コミュニティ
300:300 集約コミュニティ

コア IGP ドメイン	ISIS レベル 2
集約 IGP ドメイン	ISIS レベル 1

アクセス IGP ドメイン OSPF 0 エリア

コア エリア境界ルータ設定

図 12

```
! IGP Configuration
router isis core-agg
net 49.0100.1010.0001.0001.00
address-family ipv4 unicast
metric-style wide
propagate level 1 into level 2 route-policy drop-all  ! Disable L1 to L2 redistribution
!
interface Loopback0
ipv4 address 10.10.10.1 255.255.255.255
passive
!
interface TenGigE0/0/0/0
!
interface TenGigE0/0/0/1
circuit-type level-2-only                    ! Core facing ISIS L2 Link

!
interface TenGigE0/0/0/2
circuit-type level-1                         ! Aggregation facingis ISIS L1 Link

  !
route-policy drop-all
drop
end-policy

! BGP Configuration

router bgp 100
bgp router-id 10.10.10.1
address-family ipv4 unicast
allocate-label all                           ! Send labels with BGP routes
!
session-group infra
remote-as 100
cluster-id 1001
update-source Loopback0
!
neighbor-group agg
use session-group infra
address-family ipv4 labeled-unicast
  route-reflector-client

   route-policy BGP_Egress_Filter out        ! BGP Community based Egress filtering

   next-hop-self
!
neighbor-group mpc
use session-group infra
address-family ipv4 labeled-unicast
  route-reflector-client
   next-hop-self
!
```

```
neighbor-group core
use session-group infra
address-family ipv4 labeled-unicast
  next-hop-self

community-set Allowed-Comm
200:200,
 300:300,
!
route-policy BGP_Egress_Filter
if community matches-any Allowed-Comm then
  pass
```

集約前の設定

図 13

```
interface Loopback0
ipv4 address 10.10.9.9 255.255.255.255
!
interface Loopback1
ipv4 address 10.10.99.9 255.255.255.255

! Pre-Agg IGP Configuration

router isis core-agg
net 49.0100.1010.0001.9007.00
is-type level-1                                  !  ISIS L1 router
metric-style wide
passive-interface Loopback0                      !  Core-agg IGP loopback0

!RAN Access IGP Configuration

router ospf 1
router-id 10.10.99.9
redistribute bgp 100 subnets route-map BGP_to_RAN     !  iBGP to RAN IGP redistribution
network 10.9.9.2 0.0.0.1 area 0
network 10.9.9.4 0.0.0.1 area 0
network 10.10.99.9 0.0.0.0 area 0
distribute-list route-map Redist_from_BGP in          !  Inbound filtering to prefer
     labeled BGP learnt prefixes

ip community-list standard MPC_Comm permit 200:200
!
route-map BGP_to_RAN permit 10                        ! Only redistribute prefixes
     marked with MPC community
 match community MPC_Comm
 set tag 1000
route-map Redist_from_BGP deny 10
match tag 1000
!
route-map Redist_from_BGP permit 20


! BGP Configuration
router bgp 100
bgp router-id 10.10.9.10
bgp cluster-id 909
neighbor csr peer-group
neighbor csr remote-as 100
```

```
neighbor csr update-source Loopback100                ! Cell Site - Routers RAN IGP
     loopback100 as source
neighbor abr peer-group
neighbor abr remote-as 100
neighbor abr update-source Loopback0                  ! Core POP ABRs - core-agg IGP
     loopback0 as source
neighbor 10.10.10.1 peer-group abr
neighbor 10.10.10.2 peer-group abr
neighbor 10.10.13.1 peer-group csr
!
address-family ipv4
bgp redistribute-internal
network 10.10.9.10 mask 255.255.255.255 route-map AGG_Comm   ! Advertise with
     Aggregation Community (100:100)
redistribute ospf 1                                   !  Redistribute RAN IGP prefixes
neighbor abr send-community
neighbor abr next-hop-self

 neighbor abr send-label                              !  Send labels with BGP routes
neighbor 10.10.10.1 activate
neighbor 10.10.10.2 activate
exit-address-family
!
route-map AGG_Comm permit 10
set community 300:300
```

セル サイト ゲートウェイ (CSG) 設定

図 14

```
interface Loopback0
ip address 10.10.13.2 255.255.255.255

! IGP Configuration
router ospf 1
router-id 10.10.13.2
network 10.9.10.0 0.0.0.1 area 0
network 10.13.0.0 0.0.255.255 area 0
network 10.10.13.3 0.0.0.0 area 0
```

MTG 設定

図 15

```
Interface lookback0
ip address 10.10.11.1 255.255.255.255

! IGP Configuration
router isis core-agg
is-type level-2-only                          !  ISIS L2 router
net 49.0100.1010.0001.1001.00
address-family ipv4 unicast
metric-style wide

! BGP Configuration
router bgp 100
```

```
bgp router-id 10.10.11.1
address-family ipv4 unicast
network 10.10.11.1/32 route-policy MPC_Comm   ! Advertise Loopback-0 with MPC Community
allocate-label all                            ! Send labels with BGP routes
!
session-group infra

remote-as 100
update-source Loopback0
!
neighbor-group abr
use session-group infra
address-family ipv4 labeled-unicast
  next-hop-self
!
neighbor 10.10.6.1
use neighbor-group abr
!
neighbor 10.10.12.1
use neighbor-group abr

community-set MPC_Comm
200:200
end-set
!
route-policy MPC_Comm
set community MPC_Comm
end-policy
```

確認

モバイル パケット ゲートウェイ *(MPG)* のループバック プレフィックスは 10.10.11.1/32 であるため、このプレフィックスに注目します。 ここでパケットが CSG から MPG にどのように転送されるか見てください。

MPC プレフィクス 10.10.11.1 はルート タグ 1000 で集約前から CSG ルータに認識されており、送信 LDP ラベル 31 のラベル付きパケットとしてこれを転送できます (内部ドメイン LDP LSP) 。 OSPF での再配布中に、集約前ノードでルート タグ 1000 を使って MPC コミュニティ 200:200 がマッピングされました。

CSG ノード出力

```
CSG#sh mpls forwarding-table 10.10.11.1 detail
Local     Outgoing   Prefix          Bytes Label  Outgoing   Next Hop
Label     Label      or Tunnel Id     Switched     interface
34         31         10.10.11.1/32   0            Vl40       10.13.1.0
      MAC/Encaps=14/18, MRU=1500, Label Stack{31}
```

集約前ノード出力

集約前ノードでは、コミュニティに基づくフィルタリングによって BGP から RAN アクセス OSPF プロセスに MPC プレフィックスが再配布され、OSPF プロセスが BGP に再配布されます。 エンドツーエンド IP 到達可能性を実現すると同時に、各セグメントで必要なルートを最小限に抑えるためには、このような再配布の制御が必要です。

10.10.11.1/32 プレフィクスは、付加されている MPC 200:200 コミュニティによって階層型 BGP 100 を介して認識されます。 コア エリア境界ルータ（ABR）から受信した 16020 BGP 3107 ラベルおよび LDP ラベル 22 が、ネクストホップ再帰ルックアップ後のドメイン内転送用に最上部に追加されます。

```
Pre-AGG1#sh ip route 10.10.11.1
Routing entry for 10.10.11.1/32
Known via "bgp 100", distance 200, metric 0, type internal
Redistributing via ospf 1
Advertised by ospf 1 subnets tag 1000 route-map BGP_TO_RAN
Routing Descriptor Blocks:
* 10.10.10.2, from 10.10.10.2, 1d17h ago
    Route metric is 0, traffic share count is 1
    AS Hops 0
    MPLS label: 16020

Pre-AGG1#sh bgp ipv4 unicast 10.10.11.1
BGP routing table entry for 10.10.11.1/32, version 116586
Paths: (2 available, best #2, table default)
Not advertised to any peer
Local
  <SNIP>
Local
  10.10.10.2 (metric 30) from 10.10.10.2 (10.10.10.2)
    Origin IGP, metric 0, localpref 100, valid, internal, best
    Community: 200:200
    Originator: 10.10.11.1, Cluster list: 0.0.3.233, 0.0.2.89
    mpls labels in/out nolabel/16020

Pre-AGG1#sh bgp ipv4 unicast labels
  Network          Next Hop     In label/Out label
  10.10.11.1/32 10.10.10.1   nolabel/16021
                  10.10.10.2   nolabel/16020

Pre-AGG1#sh mpls forwarding-table 10.10.10.2 detail
Local     Outgoing  Prefix           Bytes Label   Outgoing   Next Hop
Label     Label     or Tunnel Id     Switched     interface
79         22         10.10.10.2/32 76109369     Vl10       10.9.9.1
      MAC/Encaps=14/18, MRU=1500, Label Stack{22}

Pre-AGG#sh mpls forwarding-table 10.10.11.1 detail
Local     Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label     Label     or Tunnel Id     Switched     interface
530       16020     10.10.11.1/32 20924900800   Vl10       10.9.9.1
      MAC/Encaps=14/22, MRU=1496, Label Stack{22 16020}
```

コア ABR ノード出力

ドメイン内 IGP（ISIS-L2）を介して MPLS 転送テーブルごとにプレフィックス 10.10.11.1 が認識されます。 これは LDP LSP を介して到達可能です。

```
ABR-Core2#sh ip route 10.10.11.1
Routing entry for 10.10.11.1/32
Known via "isis core-agg", distance 115, metric 20, type level-2
Installed Sep 12 21:13:03.673 for 2w3d
Routing Descriptor Blocks
  10.10.1.0, from 10.10.11.1, via TenGigE0/0/0/0, Backup
    Route metric is 0
  10.10.2.3, from 10.10.11.1, via TenGigE0/0/0/3, Protected
```

```
    Route metric is 20
No advertising protos.
```

セグメント化されたエリア間のプレフィックス配布については、ラベル（RFC 3107）付きの BGP が使用されます。 中央のインフラストラクチャに関連するアドレスと PE のループバックが、IGP のセグメント化エリア内に残っている必要があります。

異なるエリアを接続する BGP ルータは、BGP ルート リフレクタとして機能する ABR です。 これらのデバイスでは Next-Hop-Self 機能を使用することで、IGP 内の自律システム全体のすべてのネクストホップではなく、PE と中央インフラストラクチャの IP アドレスだけが必要になります。 BGP クラスタ ID に基づいてループ検出が行われます。

ネットワーク復元性を実装するには、BGP 追加パス機能を備えた BGP PIC を BGP および LFA（IGP 付き）とともに使用する必要があります。 これらの機能は、これまでの例では使用されていません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- シームレス MPLS アーキテクチャ
- Cisco Unified MPLS ホワイト ペーパー
- Cisco Carrier Packet Transport（CPT）システム
- テクニカル サポートとドキュメント – Cisco Systems