EVPN 機能

この章では、ルータでレイヤ 2 イーサネット VPN（EVPN）機能を設定する方法について説明します。

EVPN の概要

イーサネット VPN（EVPN）は、MPLS ネットワークを介してイーサネット マルチポイント サービスを提供する次世代のソリューションです。EVPN は、コアでコントロールプレーン ベースの MAC ラーニングを可能にする既存の仮想プライベート LAN サービス（VPLS）とは対照的に動作します。EVPN では、EVPN インスタンスに参加している PE が MP-BGP プロトコルを使用してコントロールプレーン内でカスタマー MAC ルートを学習します。コントロー

ルプレーン MAC ラーニングは、フローごとのロード バランシングによるマルチホーミングのサポートなど、VPLS の欠点に EVPN で対処できるようにする数多くの利点をもたらします。

EVPN は、ネットワークでの次の新たなニーズに対応するソリューションをネットワーク オペレータに提供します。

- データセンター相互接続操作（DCI）
- クラウドおよびサービスの仮想化
- プロトコルの排除とネットワークの簡素化
- 同じ VPN を介した L2 サービスと L3 サービスの統合
- サービスとワークロードの柔軟な配置
- L2 および L3 VPN によるマルチテナント
- 最適な転送とワークロード モビリティ
- 高速コンバージェンス
- 効率的な帯域幅利用

EVPN の利点

EVPN には次の利点があります。

- 統合サービス：L2 および L3 VPN サービスの統合、拡張性と制御における L3VPN のような原則と運用経験、ECMP を使用したオールアクティブ マルチホーミングと PE ロード バランシング、複数の PE に対してマルチホームである CE との間で発着信するトラフィックのロードバランシングが可能。
- ネットワーク効率：フラッドと学習メカニズムの排除、デュアルホーム接続サーバへのリンクでの障害発生時の高速再ルーティング、復元力、および高速な再コンバージェンス、ブロードキャスト、不明ユニキャスト、マルチキャスト（BUM）トラフィック配信の最適化。
- サービスの柔軟性：MPLS データ プレーンのカプセル化、既存および新しいサービス タイプのサポート（E-LAN、E-Line）、ピア PE 自動検出、および冗長グループ自動感知。

EVPN のモード

次の EVPN モードがサポートされています。

- シングルホーミング：これにより、カスタマー エッジ（CE）デバイスをプロバイダー エッジ（PE）デバイス 1 台に接続できます。
- マルチホーミング：これにより、カスタマーエッジ（CE）デバイスを複数のプロバイダーエッジ（PE）デバイスに接続できます。マルチホーミングにより、冗長接続が確保されます。冗長 PE デバイスは、ネットワーク障害が発生している場合にトラフィックが中断されないようにします。次にマルチホーミングのタイプを示します。

• オールアクティブ：オールアクティブ モードでは、特定のイーサネットセグメントに接続されているすべての PE が、そのイーサネット セグメントとの間で発着信するトラフィックを転送できます。

EVPN の概念

EVPN 機能を実装するには、次の概念を理解する必要があります。

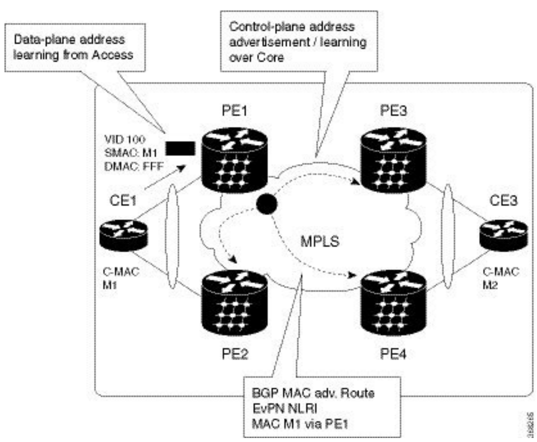
- イーサネット セグメント（ES）：イーサネット セグメントは、マルチホーム デバイスに接続する一連のイーサネット リンクです。マルチホーム デバイスまたはネットワークが 2 つ以上の PE に一連のイーサネット リンクを通じて接続されている場合に、その一連のリンクをイーサネット セグメントと呼びます。イーサネット セグメント ルートはルート タイプ 4 とも呼びます。このルートは、BUM トラフィックの指定フォワーダ（DF）の選択に使用されます。
- イーサネットセグメント識別子（ESI）：イーサネットセグメントには一意の非ゼロの識別子が割り当てられます。これをイーサネットセグメント識別子（ESI）と呼びます。ESI は、ネットワーク全体にわたってイーサネット セグメントを一意に表します。
- EVI：EVPN インスタンス（EVI）は仮想ネットワーク識別子（VNI）で表されます。EVI は、PE ルータ上の VPN を表します。EVI は IP VPN ルーティングおよび転送（VRF）と同じ役割を果たし、インポート/エクスポート ルート ターゲット（RT）が割り当てられます。ユーザ ネットワーク インターフェイス（UNI）でのサービス多重化動作に応じて、ポート上のすべてのトラフィック（すべて対 1 のバンドリング）、VLAN 上のトラフィック（1 対 1 のマッピング）、または VLAN のリスト/範囲のトラフィック（選択的バンドリング）をブリッジ ドメイン（BD）にマップできます。この BD は EVI に関連付けられ、MPLS コアに転送されます。
- EAD/ES：ES ごとのイーサネット自動検出ルートはルート タイプ 1 とも呼ばれます。このルートは、アクセス失敗のシナリオ時にトラフィックを早急に収束するために使用されます。このルートにはイーサネット タグ 0xFFFFFFFF が使用されます。
- EAD/EVI：EVI ごとのイーサネット自動検出ルートはルート タイプ 1 とも呼ばれます。このルートは、トラフィックはスイッチの 1 つにのみハッシュされるときのエイリアシングとロード バランシングに使用されます。EAD/ES ルートと区別するため、このルートにはイーサネット タグ値 0xFFFFFF を使用できません。
- エイリアシング：ルート タイプ 1 の EAD/EVI ルートを使用する所定のイーサネット セグメントで接続されているすべてのスイッチへのトラフィックのロード バランシングに使用されます。これはホストを実際に学習するスイッチとは関係なく実行されます。
- 大量撤回：ルート タイプ 1 の EAD/ES ルートを使用し、アクセス障害シナリオ時に早急に収束するために使用されます。
- DF の選択：ループの転送を防ぐために使用されます。カプセル化を解除し、所定のイーサネット セグメントにトラフィックを転送するため、単一のルータのみを使用します。

EVPN 動作

以下をアドバタイズするため、PE は起動時に EVPN ルートを交換します。

- **VPN メンバーシップ**：PE は所定のリモート PE のすべてのメンバーを検出します。マルチキャスト入力レプリケーション モデルの場合、EVI に関連付けられている PE フラッドリストの構築にこの情報が使用されます。MAC アドレスを学習した時点で BUM ラベルとユニキャスト ラベルが交換されます。
- **イーサネット セグメント到達可能性**：マルチホーミングのシナリオでは、PE がリモート PE と対応するそれらの冗長モード（オールアクティブまたはシングルアクティブ）を自動的に検出します。セグメント障害が発生した場合、PE はこの段階で使用していたルートを撤回し、リモート PE 上の MAC 大量撤回をシグナリングすることで高速コンバージェンスをトリガーします。
- **冗長グループメンバーシップ**：同じイーサネットセグメントに接続している（マルチホーミング）PE は互いに自動的に検出され、所定の EVI に対するブロードキャスト、不明ユニキャストおよびマルチキャスト（BUM）トラフィックの転送を担う指定フォワーダ（FD）を選択します。

図 *1 : EVPN* 動作



EVPN はシングルホーミング モードまたはデュアルホーミング モードで動作できます。PE 上で EVPN が有効になっており、各 PE が所定の EVPN インスタンスの他のすべてのメンバー PE を検出したときにルートタイプ 3 がアドバタイズされるシングルホーミングのシナリオを考えてみます。不明ユニキャスト（または BUM）MAC を PE で受信すると、EVPN ルート タイプ 2 として他の PE にアドバタイズされます。MAC ルートは EVPN ルート タイプ 2 を使用して他の PE にアドバタイズされます。マルチホーミングのシナリオでは、ルート タイプ 1、3、および 4 がアドバタイズされ、他の PE とそれらの冗長モード（シングルアクティブまたはオールアクティブ）を検出します。ルート タイプ 1 を使用するのは、同じ CE をホストする他の PE を自動検出するためです。この他にも、このルート タイプは CE と PE 間の破損リンクから離れている高速ルートユニキャスト トラフィックにも使用されます。ルート タイプ 4 は、指定フォワーダの選択に使用されます。たとえば、カスタマー トラフィックが PE に着信し、

ローカル イーサネット セグメント上で学習した各カスタマー MAC アドレスの到達可能性情報を EVPN MAC アドバタイズメント ルートでコアを介して配布するトポロジを考えてみます。各 EVPN MAC ルートは、カスタマー MAC アドレスと、MAC を学習したポートに関連付けられたイーサネット セグメントおよびその関連付けられた MPLS ラベルをアナウンスします。この EVPN MPLS ラベルは、アドバタイズされた MAC アドレス宛にトラフィックを送信するときにリモート PE によって後で使用されます。

EVPN ルート タイプ

EVPN ネットワーク層到達可能性情報（NLRI）は、さまざまなルート タイプを提供します。

表 *1 : EVPN* ルート タイプ

ルート タイプ	名前	使用法
1	イーサネット自動検出（AD）ルート	ES ごとの少数ルートの送信、ES に属する EVI のリストの伝送
2	MAC/IP アドバタイズメント ルート	MAC のアドバタイズ、アドレス到達可能性、IP/MAC バインディングのアドバタイズ
3	包括的なマルチキャスト イーサネット タグ ルート	マルチキャスト トンネル エンド ポイントの検出
4	イーサネット セグメント ルート	冗長グループの検出、DF の選択
5	IP プレフィックス ルート	IP プレフィックスのアドバタイズ

ルート タイプ 1：イーサネット自動検出（AD）ルート

イーサネット自動検出（AD）ルートは、EVI ごとと ESI ごとにアドバタイズされます。これらのルートは、ES ごとに送信されます。これらは ES に属している EVI のリストを伝送します。ESI フィールドは、CE がシングルホームの場合はゼロに設定されます。このルート タイプは、ロード バランシングのための MAC アドレスの大量撤回とエイリアシングに使用されます。

ルート タイプ 2：MAC/IP アドバタイズメント ルート

これらのルートは VLAN ごとのルートであるため、VNI に含まれている PE のみにこれらのルートが必要です。ホストの IP アドレスと MAC アドレスが NRLI 内のピアにアドバタイズされます。MAC アドレスのコントロール プレーン学習は不明ユニキャストのフラッディングを削減します。

ルート タイプ 3：包括的なマルチキャスト イーサネット タグ ルート

このルートは、送信元 PE からリモート PE へのブロードキャスト、不明ユニキャスト、およびマルチキャスト（BUM）トラフィック用の接続を確立します。このルートは、VLAN ごとと ESI ごとにアドバタイズされます。

ルート タイプ 4：イーサネット セグメント ルート

イーサネット セグメント ルートでは CE デバイスを 2 台のデバイスまたは PE デバイスを接続できます。ES ルートでは同じイーサネット セグメントに接続されている PE デバイスを検出できます。

ルート タイプ 5：IP プレフィックス ルート

IP プレフィックスが MAC アドバタイズメント ルートとは関係なくアドバタイズされます。EVPN IRB では、ホスト ルート /32 は RT-2 を使用してアドバタイズされ、サブネット /24 は RT-5 を使用してアドバタイズされます。

（注） EVPN IRB では、ホスト ルート /32 は RT-2 を使用してアドバタイズされ、サブネット /24 は RT-5 を使用してアドバタイズされます。

EVPN L2 ブリッジング サービスの設定

EVPN L2 ブリッジング サービスを設定するには、次のステップを実行します。

（注） 必ず、ラベル モードをプレフィックス単位から VRF ラベル モード単位に変更してください。L2FIB および VPNv4 ルート（ラベル）は同じリソースを共有しているため、リソースを枯渇させると BVI の ping は失敗します。

（注） デバイスには最大 128K の MAC アドレス エントリを含めることができます。デバイス上のブリッジ ドメインには最大 64K の MAC アドレス エントリを含めることができます。

（注） フラッディングの無効化は、EVPN ブリッジ ドメインではサポートされていません。

```
/* Configure address family session in BGP */
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router#(config)# router bgp 200
RP/0/RSP0/CPU0:router#(config-bgp)# bgp router-id 209.165.200.227
RP/0/RSP0/CPU0:router#(config-bgp)# address-family l2vpn evpn
```

```
RP/0/RSP0/CPU0:router#(config-bgp)# neighbor 10.10.10.10
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# remote-as 200
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# description MPLSFACING-PEER
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# update-source Loopback 0
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# address-family l2vpn evpn

/* Configure EVI and define the corresponding BGP route targets */

Router# configure
Router(config)# evpn
Router(config-evpn)# evi 6005
Router(config-evpn-evi)# bgp
Router(config-evpn-evi-bgp)# rd 200:50
Router(config-evpn-evi-bgp)# route-target import 100:6005
Router(config-evpn-evi-bgp)# route-target export 100:6005
Router(config-evpn-evi-bgp)# exit
Router(config-evpn-evi)# advertise-mac

/* Configure a bridge domain */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group 1
Router(config-l2vpn-bg)# bridge-domain 1-1
Router(config-l2vpn-bg-bd)# interface GigabitEthernet 0/0/0/1
Router(config-l2vpn-bg-bd-ac)# evi 6005
Router(config-l2vpn-bg-bd-ac-evi)# commit
Router(config-l2vpnbg-bd-ac-evi)# exit
```

実行コンフィギュレーション

```
router bgp 200 bgp
 router-id 209.165.200.227
 address-family l2vpn evpn
 neighbor 10.10.10.10
  remote-as 200 description MPLS-FACING-PEER
  updatesource Loopback0
  addressfamily l2vpn evpn
!

configure
evpn
 evi 6005
  bgp
   rd 200:50
   route-target import 100:6005
   route-target export 100:6005
!
  advertise-mac


configure
l2vpn
 bridge group 1
  bridge-domain 1-1
   interface GigabitEthernet 0/0/0/1

    evi 6005
!
```

EVPN MAC アドレス制限の設定

EVPN MAC アドレス制限を設定する場合、次の制限事項が適用されます。

- リモート MAC アドレスは、MAC アドレス制限が設定されているかどうかに関係なく、ハードウェアでプログラムされます。
- MAC アドレス制限のアクションは、ローカル MAC アドレスの数が設定された制限を超えた場合にのみ適用されます。MAC アドレス制限が、リモートおよびローカル MAC アドレスによって枯渇した場合、またはリモート MAC アドレスによってのみ割り当てられた場合、MAC アドレス制限のアクションは適用されません。超過したトラフィックは不明なユニキャストと見なされ、ブリッジ ドメイン全体にフラッディングされます。
- MAC アドレス制限は、デバイスが MAC アドレスをアクティブに学習していない場合にのみ、正しく変更できます。これは予期された動作です。
- MAC ラーニングが有効になっている場合は、MAC アドレス制限を最大 6 つまで設定できます。ただし、MAC ラーニングが無効になっている場合は、MAC アドレス制限を最大 5 つまで設定できます。
- **clear l2vpn mac address table** コマンドはサポートされていません。MAC アドレス テーブルは、接続回線インターフェイスまたはサブインターフェイスで **shut** または **no shutdown** が実行された場合、あるいはMAC エージング タイマーが期限切れになった場合にクリアされます。

設定例

EVPN MAC アドレス制限を設定するには、次の作業を実行します。

次の表に、設定する MAC アドレス制限のパラメータと値を示します。

パラメータ	値
MAC アドレス制限	50
MAC 制限アクション	limit, no-flood
MAC 通知	syslog および SNMP トラップ メッセージ
MAC 制限しきい値	80%

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group EVPN-BG-SH
Router(config-l2vpn-bg)# bridge-domain EVPN_2701
Router(config-l2vpn-bg-bd)# mac
Router(config-l2vpn-bg-bd-mac)# limit
Router(config-l2vpn-bg-bd-mac-limit)# maximum 50
Router(config-l2vpn-bg-bd-mac-limit)# action no-flood
Router(config-l2vpn-bg-bd-mac-limit)# notification both
```

```
Router(config-l2vpn-bg-bd-mac-limit)#  exit
Router(config-l2vpn-bg-bd)#  exit
Router(config-l2vpn-bg)# exit
Router(config-l2vpn)# mac limit threshold 80
Router(config-l2vpn)# commit
```

実行コンフィギュレーション

```
l2vpn
bridge group EVPN-BG-SH
  bridge-domain EVPN_2701
   mac
    limit
     maximum 50
     action no-flood
     notification both
    !
   !
!
mac limit threshold 80
commit
```

確認

EVPN MAC アドレス制限パラメータが前述の表のように設定されていることを確認します。

```
Router# show l2vpn bridge-domain bd-name EVPN_2701 detail
Legend: pp = Partially Programmed.
Bridge group: EVPN-BG-SH, bridge-domain: EVPN_2701, id: 25, state: up, ShgId: 0, MSTi:
0
  Coupled state: disabled
  VINE state: EVPN Native
  MAC learning: enabled
  MAC withdraw: enabled
    MAC withdraw for Access PW: enabled
    MAC withdraw sent on: bridge port up
    MAC withdraw relaying (access to access): disabled
  Flooding:
    Broadcast & Multicast: enabled
    Unknown unicast: enabled
  MAC aging time: 300 s, Type: inactivity
  MAC limit: 50, Action: limit, no-flood, Notification: syslog, trap
  MAC limit reached: no, threshold: 80%
  MAC port down flush: enabled
  MAC Secure: disabled, Logging: disabled
  Split Horizon Group: none
  Dynamic ARP Inspection: disabled, Logging: disabled
  IP Source Guard: disabled, Logging: disabled
  DHCPv4 Snooping: disabled
  DHCPv4 Snooping profile: none
  IGMP Snooping: disabled
  IGMP Snooping profile: none
  MLD Snooping profile: none
  Storm Control: disabled
  Bridge MTU: 1500
  MIB cvplsConfigIndex: 26
  Filter MAC addresses:
  P2MP PW: disabled
  Create time: 21/04/2019 16:28:05 (2d23h ago)
  No status change since creation
  ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up), VNIs: 0 (0 up)
```

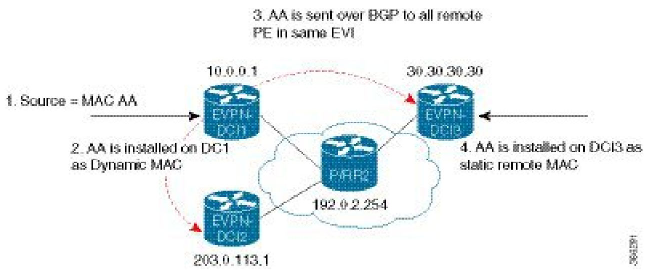
```
  List of EVPNs:
    EVPN, state: up
      evi: 6101
      XC ID 0x8000040c
     Statistics:
       packets: received 0 (unicast 0), sent 0
       bytes: received 0 (unicast 0), sent 0
       MAC move: 0
  List of ACs:
    AC: Bundle-Ether101.2701, state is up, active in RG-ID 101
      Type VLAN; Num Ranges: 1
      Rewrite Tags: [1000, 2000]
      VLAN ranges: [2701, 2701]
      MTU 9112; XC ID 0xa000060b; interworking none; MSTi 6
      MAC learning: enabled
      Flooding:
        Broadcast & Multicast: enabled
        Unknown unicast: enabled
      MAC aging time: 300 s, Type: inactivity
      MAC limit: 50, Action: limit, no-flood, Notification: syslog, trap
      MAC limit reached: no, threshold: 80%
      MAC port down flush: enabled
      MAC Secure: disabled, Logging: disabled
      Split Horizon Group: none
      Dynamic ARP Inspection: disabled, Logging: disabled
      IP Source Guard: disabled, Logging: disabled
      DHCPv4 Snooping: disabled
      DHCPv4 Snooping profile: none
      IGMP Snooping: disabled
      IGMP Snooping profile: none
      MLD Snooping profile: none
      Storm Control:
        Broadcast: enabled(160000 pps)
        Multicast: enabled(160000 pps)
        Unknown unicast: enabled(160000 pps)
      Static MAC addresses:
      Statistics:
        packets: received 0 (multicast 0, broadcast 0, unknown unicast 0, unicast 0),
sent 0
       bytes: received 0 (multicast 0, broadcast 0, unknown unicast 0, unicast 0), sent
 0
        MAC move: 0
      Storm control drop counters:
        packets: broadcast 0, multicast 0, unknown unicast 0
        bytes: broadcast 0, multicast 0, unknown unicast 0
      Dynamic ARP inspection drop counters:
        packets: 0, bytes: 0
      IP source guard drop counters:
        packets: 0, bytes: 0
  List of Access PWs:
  List of VFIs:
  List of Access VFIs:
```

EVPN ソフトウェア MAC ラーニング

あるデバイス上で学習した MAC アドレスは、VLAN 内の別のデバイス上で学習されるか、配布されるようにする必要があります。EVPN ソフトウェア MAC ラーニング機能では、あるデバイス上で学習された MAC アドレスをネットワークに接続された別のデバイスに配布できます。MAC アドレスは、BGP を使用してリモート デバイスから学習されます。

（注） デバイスには最大 128K の MAC アドレス エントリを含めることができます。デバイス上のブリッジ ドメインには最大 64K の MAC アドレス エントリを含めることができます。

図 ***2 : EVPN*** ソフトウェア ***MAC*** ラーニング



上の図は、ソフトウェア MAC ラーニングのプロセスを示しています。次に、このプロセスに関わるステップを示します。

1. トラフィックは、ブリッジ ドメイン内の 1 つのポートに着信します。
2. 送信元 MAC アドレス（AA）は PE 上で学習され、ダイナミック MAC エントリとして格納されます。
3. MAC アドレス（AA）がタイプ 2 BGP ルーtに変換され、BGP を介して同じ EVI 内のすべてのリモート PE に送信されます。
4. MAC アドレス（AA）は、リモート MAC アドレスとして PE で更新されます。

EVPN ソフトウェア MAC ラーニングの設定

次の項では、EVPN ソフトウェア MAC ラーニングの設定方法について説明します。

（注） ルータは、フロー認識型トランスポート（FAT）擬似回線をサポートしていません。

```
/* Configure bridge domain. */

RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group EVPN_SH
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain EVPN_2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface TenGigE0/0/0/1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# exit
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface BundleEther 20.2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# storm-control broadcast pps 10000 ← Enabling
 storm-control is optional
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# exit
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# evi 2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-evi)# commit
```

```
/* Configure address family session in BGP. */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router bgp 200
RP/0/RSP0/CPU0:router(config-bgp)# bgp router-id 209.165.200.227
RP/0/RSP0/CPU0:router(config-bgp)# address-family l2vpn evpn

RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 200
RP/0/RSP0/CPU0:router(config-bgp-nbr)# description MPLSFACINGPEER
RP/0/RSP0/CPU0:router(config-bgp-nbr)# update-source Loopback 0
RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family l2vpn evpn
```

EVPN ソフトウェア MAC ラーニングでサポートされているモード

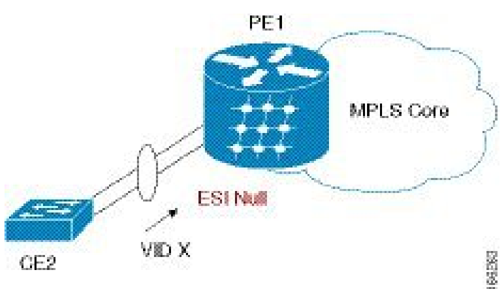
EVPN ソフトウェア MAC ラーニングでサポートされているモードは次のとおりです。

- シングル ホーム デバイス（SHD）またはシングル ホーム ネットワーク（SHN）
- デュアル ホーム デバイス（DHD）：オール アクティブ ロード バランシング

シングル ホーム デバイスまたはシングル ホーム ネットワーク モード

次の項では、EVPN ソフトウェア MAC ラーニング機能をシングル ホーム デバイスまたはシングル ホーム ネットワーク（SHD/SHN）モードで設定する方法について説明します。

図 *3:* シングル ホーム デバイスまたはシングル ホーム ネットワーク モード



上の図では、PE（PE1）はバンドルインターフェイスまたは物理インターフェイスを使用してイーサネット セグメントに接続されています。SHD/SHN にはヌル イーサネット セグメント識別子（ESI）を使用します。

シングル ホーム デバイスまたはシングル ホーム ネットワーク モードでの EVPN の設定

この項では、シングル ホーム デバイスまたはシングル ホーム ネットワーク モードで EVPN ソフトウェア MAC ラーニング機能を設定する方法について説明します。

```
/* Configure bridge domain. */

RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group EVPN_ALL_ACTIVE
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain EVPN_2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface BundleEther1.2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# evi 2001
```

```
/* Configure advertisement of MAC routes. */

RP/0/RSP0/CPU0:router(config)# evpn
RP/0/RSP0/CPU0:router(config-evpn)# evi 2001
RP/0/RSP0/CPU0:router(config-evpn-evi)# advertise-mac


/* Configure address family session in BGP. */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router#(config)# router bgp 200
RP/0/RSP0/CPU0:router#(config-bgp)# bgp router-id 09.165.200.227
RP/0/RSP0/CPU0:router#(config-bgp)# address-family l2vpn evpn
RP/0/RSP0/CPU0:router#(config-bgp)# neighbor 10.10.10.10
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# remote-as 200
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# description MPLSFACING-PEER
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# update-source Loopback 0
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# address-family l2vpn evpn
```

実行コンフィギュレーション

```
l2vpn
bridge group EVPN_ALL_ACTIVE
 bridge-domain EVPN_2001
  interface BundleEther1.2001
  evi 2001
!
evpn
 evi 2001
  advertise-mac
!
router bgp 200 bgp
 router-id 40.40.40.40
 address-family l2vpn evpn
 neighbor 10.10.10.10
  remote-as 200 description MPLS-FACING-PEER
  updatesource Loopback0
  addressfamily l2vpn evpn
```

確認

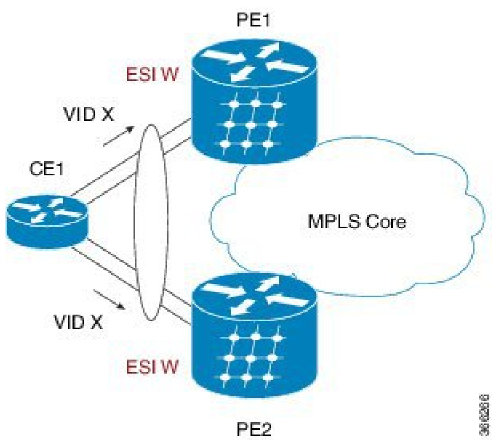
シングル ホーム デバイスの EVPN を確認します。

```
RP/0/RSP0/CPU0:router# show evpn ethernet-segment interface Te0/4/0/10 detail

Ethernet Segment Id     Interface   Nexthops
--------------------    ----------  ----------
N/A                     Te0/4/0/10  20.20.20.20
..............
 Topology :
 Operational : SH
 Configured : Single-active (AApS) (default)
```

デュアル ホーム デバイス：オールアクティブ ロード バランシング モード

次の項では、デュアル ホーム デバイス（DHD）にオールアクティブ ロード バランシング モードで EVPN ソフトウェア MAC ラーニング機能を設定する方法について説明します。

図 *4*：デュアル ホーム デバイス：オールアクティブ ロード バランシング モード



オールアクティブ ロード バランシングはフローごとのアクティブ/アクティブ（AApF）と呼ばれています。上の図では、両方の EVPN PE に同一のイーサネット セグメント識別子を使用しています。PE は、バンドル インターフェイスを使用してイーサネット セグメントに接続されています。CE では、単一のバンドルが 2 つの EVPN PE に向けて設定されます。このモードでは、学習した MAC アドレスが PE1 と PE2 の両方に格納されます。PE1 と PE2 は両方とも同じ EVI 内でトラフィックを転送できます。

デュアル ホーム デバイスでの EVPN ソフトウェア MAC ラーニングの設定：オールアクティブ モード

この項では、オールアクティブ モードのデュアル ホーム デバイスでEVPN ソフトウェア MAC ラーニング機能を設定する方法について説明します。

```
/* Configure bridge domain. */

RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group EVPN_ALL_ACTIVE
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain EVPN_2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface BundleEther1.2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# evi 2001


/* Configure advertisement of MAC routes. */

RP/0/RSP0/CPU0:router(config)# evpn
RP/0/RSP0/CPU0:router(config-evpn)# evi 2001
RP/0/RSP0/CPU0:router(config-evpn-evi)# advertise-mac
RP/0/RSP0/CPU0:router(config-evpn-evi)# exit
RP/0/RSP0/CPU0:router(config-evpn)# interface bundle-ether1
RP/0/RSP0/CPU0:router(config-evpn-ac)# ethernet-segment
RP/0/RSP0/CPU0:router(config-evpn-ac-es)# identifier type 0 01.11.00.00.00.00.00.00.01


/* Configure address family session in BGP. */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router#(config)# router bgp 200
RP/0/RSP0/CPU0:router#(config-bgp)# bgp router-id 209.165.200.227
RP/0/RSP0/CPU0:router#(config-bgp)# address-family l2vpn evpn
RP/0/RSP0/CPU0:router#(config-bgp)# neighbor 10.10.10.10
```

```
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# remote-as 200
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# description MPLSFACING-PEER
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# update-source Loopback 0
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# address-family l2vpn evpn

/* Configure Link Aggregation Control Protocol (LACP) bundle. */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether1 300
RP/0/RSP0/CPU0:router(config-if)# lacp switchover suppress-flaps 300
RP/0/RSP0/CPU0:router(config-if)# exit

/* Configure VLAN Header Rewrite.*/

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface bundle-Ether1.2001 l2transport
RP/0/RSP0/CPU0:router(config-if)# encapsulation dot1q 10
RP/0/RSP0/CPU0:router(config-if)# rewrite ingress tag pop 1 symmetric
```

実行コンフィギュレーション

```
l2vpn
bridge group EVPN_ALL_ACTIVE
 bridge-domain EVPN_2001
 interface Bundle-Ether1.2001
 !
 evi 2001
 !
!
evpn
 evi 2001
 !
 advertise-mac
 !
 interface bundle-ether1
  ethernet-segment
  identifier type 0 01.11.00.00.00.00.00.00.01
  !
 !
router bgp 200
bgp router-id  209.165.200.227
address-family l2vpn evpn
!
neighbor 10.10.10.10
 remote-as 200
 description MPLS-FACING-PEER
 update-source Loopback0
 address-family l2vpn evpn
!
interface Bundle-Ether1
lacp switchover suppress-flaps 300
load-interval 30
!
interface bundle-Ether1.2001 l2transport
 encapsulation dot1aq 2001
 rewrite ingress tag pop 1 symmetric
!
```

確認

オールアクティブ モードのデュアル ホーム デバイスの EVPN を確認します。

```
RP/0/RSP0/CPU0:router# show evpn ethernet-segment interface bundle-Ether 1 carvin$

Ethernet Segment Id        Interface  Nexthops
-------- ----------        --------   --------
0100.211b.fce5.df00.0b00   BE11       10.10.10.10
 209.165.201.1
Topology :
 Operational : MHN
 Configured : All-active (AApF) (default)
 Primary Services : Auto-selection
 Secondary Services: Auto-selection
 Service Carving Results:
 Forwarders : 4003
 Elected : 2002
 EVI E : 2000, 2002, 36002, 36004, 36006, 36008
 ........
 Not Elected : 2001
 EVI NE : 2001, 36001, 36003, 36005, 36007, 36009

 MAC Flushing mode : Invalid

Peering timer : 3 sec [not running]
 Recovery timer : 30 sec [not running]
 Local SHG label : 34251
 Remote SHG labels : 1
  38216 : nexthop 209.165.201.1
```

EVPN ソフトウェア MAC ラーニングの確認

パケット ドロップ統計情報を確認します。

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain bd-name EVPN_2001 details

Bridge group: EVPN_ALL_ACTIVE, bridge-domain: EVPN_2001, id: 1110,
state: up, ShgId: 0, MSTi: 0
 List of EVPNs:
 EVPN, state: up
 evi: 2001
 XC ID 0x80000458
 Statistics:
 packets: received 28907734874 (unicast 9697466652), sent
76882059953
 bytes: received 5550285095808 (unicast 1861913597184), sent
14799781851396
 MAC move: 0
 List of ACs:
 AC: TenGigE0/0/0/1, state is up
 Type VLAN; Num Ranges: 1
...
 Statistics:
 packets: received 0 (multicast 0, broadcast 0, unknown
unicast 0, unicast 0), sent 45573594908
 bytes: received 0 (multicast 0, broadcast 0, unknown unicast
0, unicast 0), sent 8750130222336
 MAC move: 0
 ........
```

VPN-ID と MAC アドレス フィルタを使用して EVPN ID を確認します。

```
RP/0/RSP0/CPU0:router# show evpn evi vpn-id 2001 neighbor
```

```
Neighbor IP    vpn-id
-----------   --------
209.165.200.225   2001
209.165.201.30   2001
```

BGP L2VPN EVPN の概要を確認します。

```
RP/0/RSP0/CPU0:router# show bgp l2vpn evpn summary
...
Neighbor        Spk    AS     MsgRcvd  MsgSent   TblVer    InQ   OutQ   Up/Down   St/PfxRcd
209.165.200.225  0     200     216739  229871   200781341   0     0      3d00h    348032
209.165.201.30   0     200     6462962 4208831  200781341  10     0      2d22h    35750
```

ライン カードの L2FIB テーブルへの MAC の更新を確認します。

```
RP/0/RSP0/CPU0:router# show l2vpn mac mac all location 0/6/cPU0

Topo ID Producer Next Hop(s)     Mac Address    IP Address
------- -------- -----------     -------------- ----------
1112    0/6/CPU0 Te0/0/0/1 00a3.0001.0001
```

ルート スイッチ プロセッサ（RSP）の L2FIB テーブルへの MAC の更新を確認します。

```
RP/0/RSP0/CPU0:router# show l2vpn mac mac all location 0/6/cPU0

Topo ID  Producer Next Hop(s)     Mac Address    IP Address
-------  -------- -----------     -------------- ----------
1112     0/6/CPU0 0/0/0/1 00a3.0001.0001
```

MAC アドレスの概要情報を確認します。

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain EVPN_ALL_ACTIVE:EVPN_2001
mac-address location 0/6/CPU0

.....
Mac Address     Type      Learned from/Filtered on   LC learned   Resync Age/Last Change
Mapped to
0000.2001.5555  dynamic    Te0/0/0/2           N/A          11 Jan 14:37:22
N/A <-- local dynamic
00bb.2001.0001 dynamic     Te0/0/0/2           N/A          11 Jan 14:37:22
N/A
0000.2001.1111 EVPN        BD id: 1110                 N/A          N/A
N/A <-- remote static
00a9.2002.0001 EVPN        BD id: 1110                 N/A          N/A
N/A
```

VPN-ID と MAC アドレス フィルタを使用して EVPN ID を確認します。

```
RP/0/RSP0/CPU0:router# show evpn evi vpn-id 2001 mac

EVI    MAC address      IP address         Nexthop       Label
----   --------------   -----------        -------       ------
2001   00a9.2002.0001   ::                 10.10.10.10   34226      <-- Remote MAC
2001   00a9.2002.0001   ::                 209.165.201.30  34202
```

```
2001   0000.2001.5555  20.1.5.55        TenGigE0/0/0/2 34203    <-- local MAC


RP/0/RSP0/CPU0:router# RP/0/RSP0/CPU0:router# show evpn evi vpn-id 2001 mac 00a9.2002.0001
 detail

EVI     MAC address      IP address  Nexthop      Label
----    --------------   ----------  -------      -----
2001    00a9.2002.0001   ::          10.10.10.10  34226

2001    00a9.2002.0001   ::          209.165.201.30  34202

 Ethernet Tag : 0
 Multi-paths Resolved : True <--- aliasing to two remote PE with All-Active load balancing


 Static : No
 Local Ethernet Segment : N/A
 Remote Ethernet Segment : 0100.211b.fce5.df00.0b00
 Local Sequence Number : N/A
 Remote Sequence Number : 0
 Local Encapsulation : N/A
 Remote Encapsulation : MPLS
```

EVPN に関連付けられている BGP ルートをブリッジドメインフィルタを使用して確認します。

```
RP/0/RSP0/CPU0:router# show bgp l2vpn evpn bridge-domain EVPN_2001 route-type 2

*> [2][0][48][00bb.2001.0001][0]/104
                        0.0.0.0          0 i <------ locally learnt MAC
*>i[2][0][48][00a9.2002.00be][0]/104
                        10.10.10.10 100    0 i <----- remotely learnt MAC
* i 209.165.201.30 100 0 i
```

EVPN アウト オブ サービス

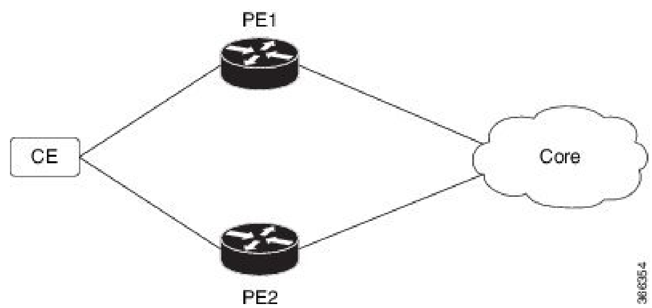
EVPN アウト オブ サービス機能では、Link Aggregation Control Protocol（LACP）を設定したイーサネット セグメントに含まれているバンドル インターフェイスの状態を制御することができます。この機能を使用すると、ノードをアウト オブ サービス（OOS）に移行させることができます。プロバイダー エッジ（PE）のすべてのバンドルを手動でシャットダウンする必要はありません。

cost-out コマンドを使用してノード上のイーサネット VPN（EVPN）のイーサネット セグメントに属するすべてのバンドル インターフェイスをダウンさせます。イーサネット A-D のイーサネット セグメント（ES EAD）ルートは、バンドルをシャット ダウンする前に撤回されます。PE は接続されているカスタマーエッジ（CE）デバイスにシグナリングし、対応するバンドル メンバーをダウンさせます。こうすることで、トラフィックを中断させることなく、トラフィックをこの PE ノードからそらします。CE からイーサネット セグメントへのトラフィックは、マルチホーミング環境内のピア PE へと方向付けられます。

（注） EVPN のコストアウトは、手動で設定された ESI でのみサポートされます。

次に、CE が PE1 と PE2 に接続されているトポロジを示します。PE1 に cost-out コマンドを設定すると、イーサネットセグメント上のすべてのバンドルインターフェイスがダウンします。また、CE 上の対応するバンドル メンバーもダウンします。したがって、このイーサネット セグメントのトラフィックは CE から PE2 へと送信されるようになります。

図 *5: EVPN* アウト オブ サービス



ノードをサービス状態に戻すには、no cost-out コマンドを使用します。これにより、PE 上の EPVN イーサネット セグメントに属するすべてのバンドル インターフェイスと CE 上の対応するバンドル メンバーが起動します。

ノードがコストアウト状態にある場合に新しいバンドル イーサネット セグメントを追加するとそのバンドルがダウンします。同様に、バンドル イーサネット セグメントを削除するとそのバンドルは起動します。

リロード時に指定した時間が経過した後にノードをサービス状態に戻すには、startup-cost-in コマンドを使用します。EPVN が初期化された時点でノードがコストアウトになり、設定時間までコストアウト状態が維持されます。タイマー実行中に evpn no startup-cost-in コマンドを実行すると、タイマーが停止し、ノードがコストイン状態になります。

「cost-out」設定は「startup-cost-in」タイマーよりも常に優先されます。そのため、両方の設定でリロードすると、コストアウト状態は「cost-out」設定で制御されます。タイマーは関係ありません。同様に、起動タイマーでリロードし、タイマーが実行している間に「cost-out」を設定するとタイマーが停止し、OOS 状態は「cost-out」設定のみで制御されます。

startup-cost-in timer が実行している間に何らかのプロシージャを実行すると、ノードはコストアウト状態を維持し、タイマーが再起動します。

EVPN アウト オブ サービスの設定

この項では、EVPN アウト オブ サービスを設定する方法について説明します。

```
/* Configuring node cost-out on a PE */

Router# configure
Router(config)# evpn
```

```
Router(config-evpn)# cost-out
Router(config-evpn)commit

/* Bringing up the node into service */

Router# configure
Router(config)# evpn
Router(config-evpn)# no cost-out
Router(config-evpn)commit

/* Configuring the timer to bring up the node into service after the specified time on
reload */

Router# configure
Router(config)# evpn
Router(config-evpn)# startup-cost-in 6000
Router(config-evpn)commit
```

実行コンフィギュレーション

```
configure
evpn
 cost-out
!

configure
evpn
 startup-cost-in 6000
!
```

確認

EVPN アウト オブ サービスの設定を確認します。

```
/* Verify the node cost-out configuration */

Router# show evpn summary
Fri Apr  7 07:45:22.311 IST
Global Information
-----------------------------
Number of EVIs                : 2
Number of Local EAD Entries   : 0
Number of Remote EAD Entries  : 0
Number of Local MAC Routes    : 0
Number of Local MAC Routes    : 5
          MAC                 : 5
          MAC-IPv4            : 0
          MAC-IPv6            : 0
Number of Local ES:Global MAC : 12
Number of Remote MAC Routes   : 7
          MAC                 : 7
          MAC-IPv4            : 0
          MAC-IPv6            : 0
Number of Local IMCAST Routes : 56
Number of Remote IMCAST Routes: 56
Number of Internal Labels     : 5
Number of ES Entries          : 9
Number of Neighbor Entries    : 1
EVPN Router ID                : 192.168.0.1
BGP Router ID                 : ::
```

```
BGP ASN                        : 100
PBB BSA MAC address            : 0207.1fee.be00
Global peering timer           :      3 seconds
Global recovery timer          :     30 seconds
EVPN cost-out                  : TRUE
      startup-cost-in timer    : Not configured


/* Verify the no cost-out configuration */

Router# show evpn summary
Fri Apr  7 07:45:22.311 IST
Global Information
-----------------------------
Number of EVIs                 : 2
Number of Local EAD Entries    : 0
Number of Remote EAD Entries   : 0
Number of Local MAC Routes     : 0
Number of Local MAC Routes     : 5
          MAC                  : 5
          MAC-IPv4             : 0
          MAC-IPv6             : 0
Number of Local ES:Global MAC  : 12
Number of Remote MAC Routes    : 7
          MAC                  : 7
          MAC-IPv4             : 0
          MAC-IPv6             : 0
Number of Local IMCAST Routes  : 56
Number of Remote IMCAST Routes: 56
Number of Internal Labels      : 5
Number of ES Entries           : 9
Number of Neighbor Entries     : 1
EVPN Router ID                 : 192.168.0.1
BGP Router ID                  : ::
BGP ASN                        : 100
PBB BSA MAC address            : 0207.1fee.be00
Global peering timer           :      3 seconds
Global recovery timer          :     30 seconds
EVPN cost-out                  : FALSE
      startup-cost-in timer    : Not configured


/* Verify the startup-cost-in timer configuration */

Router# show evpn summary
Fri Apr  7 07:45:22.311 IST
Global Information
-----------------------------
Number of EVIs                 : 2
Number of Local EAD Entries    : 0
Number of Remote EAD Entries   : 0
Number of Local MAC Routes     : 0
Number of Local MAC Routes     : 5
          MAC                  : 5
          MAC-IPv4             : 0
          MAC-IPv6             : 0
Number of Local ES:Global MAC  : 12
Number of Remote MAC Routes    : 7
          MAC                  : 7
          MAC-IPv4             : 0
          MAC-IPv6             : 0
Number of Local IMCAST Routes  : 56
Number of Remote IMCAST Routes: 56
Number of Internal Labels      : 5
```

```
Number of ES Entries          : 9
Number of Neighbor Entries    : 1
EVPN Router ID                : 192.168.0.1
BGP Router ID                 : ::
BGP ASN                       : 100
PBB BSA MAC address           : 0207.1fee.be00
Global peering timer          :      3 seconds
Global recovery timer         :     30 seconds
EVPN node cost-out            : TRUE
        startup-cost-in timer : 6000
```

EVPN 対応 CFM のサポート

イーサネット接続障害管理（CFM）はサービス レベル OAM プロトコルの 1 つで、VLAN ごとにエンドツーエンドのイーサネット サービスをモニタリングおよびトラブルシューティングするためのツールとなります。これには、予防的な接続モニタリング、障害検証、および障害分離の機能が含まれています。CFM は EVPN ネットワークに導入できます。EVPN ネットワークで CFM を使用して、ノード間の接続をモニタできます。

制約事項

EVPN 対応 CFM は、次の制限の下でサポートされています。

- アクティブ-アクティブ マルチホーミングのシナリオでは、マルチホーム CE デバイスとそれらに接続している PE デバイスとの間の接続をモニタする場合、CFM は CE と PE 間の個別のリンク間でのみ使用できます。CE デバイスと PE デバイス間のバンドルで CFM の使用を試みると、シーケンス番号エラーが発生し、統計情報が不正確になります。
- ループバックおよびリンクトレースの結果に副作用が生じる可能性があります。ループバックまたはリンクトレースのいずれかで同じインスタンスに対して複数の結果が報告されたり、同じ 2 つのエンドポイント間にあるループバックとリンクトレースの連続するインスタンスで異なる結果が生じたりする場合があります。

イーサネット セグメント単位の EVPN 複数サービス

イーサネット セグメント単位の EVPN 複数サービス機能を使用すると、単一のイーサネット セグメント（ES）で複数のサービスを設定できます。複数の ES で複数のサービスを設定する代わりに、1 つの ES で複数のサービスを設定できます。

単一のイーサネット バンドルで次のサービスを設定できます。サブインターフェイスごとにサービスを 1 つずつ設定できます。

- フレキシブル クロスコネクト（FXC） サービス。VLAN 非認識型、VLAN 認識型、およびローカル スイッチング モードをサポートしています。

  詳細については、『*L2VPN and Ethernet Services Configuration Guide for Cisco NCS 540 Series Routers*』の「*Configure Point-to-Point Layer 2 Services*」の章を参照してください。

- EVPN-VPWS Xconnect サービス

詳細については、『*L2VPN and Ethernet Services Configuration Guide for Cisco NCS 540 Series Routers*』の「*EVPN Virtual Private Wire Service (VPWS)*」の章を参照してください。

- EVPN Integrated Routing and Bridging（IRB）

  詳細については、『*L2VPN and Ethernet Services Configuration Guide for Cisco NCS 540 Series Routers*』の「*Configure EVPN IRB*」の章を参照してください。

- ネイティブ EVPN

  詳細については、『*L2VPN and Ethernet Services Configuration Guide for Cisco NCS 540 Series Routers*』の「*EVPN Features*」の章を参照してください。

これらのサービスはすべて、オールアクティブのマルチホーミングのシナリオでのみサポートされます。

イーサネット セグメント単位の EVPN 複数サービスの設定

イーサネット バンドル インターフェイス 22001 を介して 2 つのプロバイダー エッジ（PE）デバイスに接続しているカスタマー エッジ（CE）デバイスを考えてみます。バンドル イーサネット サブインターフェイスで複数のサービスを設定します。

設定例

Bundle-Ether22001 ES を考慮し、サブインターフェイスで複数のサービスを設定します。

```
/* Configure attachment circuits */
Router# configure
Router(config)# interface Bundle-Ether22001.12 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 12
Router(config-l2vpn-subif)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether22001.13 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 13
Router(config-l2vpn-subif)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether22001.14 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 14
Router(config-l2vpn-subif)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether22001.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 1
Router(config-l2vpn-subif)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether22001.2 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 2
Router(config-l2vpn-subif)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether22001.3 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 3
Router(config-l2vpn-subif)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether22001.4 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 4
Router(config-l2vpn-subif)# exit
```

```
Router(config-l2vpn)# exit

/*Configure VLAN Unaware FXC Service */
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-unaware fxc_mh1
Router(config-l2vpn-fxs-vu)# interface Bundle-Ether22001.1
Router(config-l2vpn-fxs-vu)# interface Bundle-Ether22001.2
Router(config-l2vpn-fxs-vu)# interface Bundle-Ether22001.3
Router(config-l2vpn-fxs-vu)# neighbor evpn evi 21006 target 22016
Router(config-l2vpn-fxs-vu)# commit

/* Configure VLAN Aware FXC Service */
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-aware evi 24001
Router(config-l2vpn-fxs-vu)# interface Bundle-Ether22001.12
Router(config-l2vpn-fxs-vu)# interface Bundle-Ether22001.13
Router(config-l2vpn-fxs-vu)# interface Bundle-Ether22001.14
Router(config-l2vpn-fxs-vu)# commit

/* Configure Local Switching - Local switching is supported only on VLAN-aware FXC */
PE1
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-aware evi 31400
Router(config-l2vpn-fxs)# interface Bundle-Ether22001.1400
Router(config-l2vpn-fxs)# interface Bundle-Ether23001.1400
Router(config-l2vpn-fxs)# commit
Router(config-l2vpn-fxs)# exit
PE2
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-aware evi 31401
Router(config-l2vpn-fxs)# interface Bundle-Ether22001.1401
Router(config-l2vpn-fxs)# interface Bundle-Ether23001.1401
Router(config-l2vpn-fxs)# commit
Router(config-l2vpn-fxs)# exit

/* Configure EVPN-VPWS xconnect service and native EVPN with IRB */

Router# configure
Router(config)# interface Bundle-Ether22001.11 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 11
Router(config-l2vpn-subif)# rewrite ingress tag pop 2 symmetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit

Router# configure
Router(config)# interface Bundle-Ether22001.21 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q  21
Router(config-l2vpn-subif)# rewrite ingress tag pop 2 symmetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit

Router# configure
Route(config)# l2vpn
Router(config-l2vpn)# xconnect group xg22001
Router(config-l2vpn-xc)# p2p evpn-vpws-mclag-22001
Router(config-l2vpn-xc-p2p)# interface Bundle-Ether22001.11
Router(config-l2vpn-xc-p2p)# neighbor evpn evi 22101 target 220101 source 220301
Router(config-l2vpn-xc-p2p)# commit
Router(config-l2vpn-xc-p2p)# exit

Router # configure
```

```
Router (config)# l2vpn
Router (config-l2vpn)# bridge group native_evpn1
Router (config-l2vpn-bg)#  bridge-domain bd21
Router (config-l2vpn-bg-bd)# interface Bundle-Ether22001.21
Router (config-l2vpn-bg-bd-ac)# routed interface BVI21
Router (config-l2vpn-bg-bd-bvi)# evi 22021
Router (config-l2vpn-bg-bd-bvi)# commit
Router (config-l2vpn-bg-bd-bvi)# exit

/* Configure Native EVPN */
Router # configure
Router (config)# evpn
Router (config-evpn)# interface Bundle-Ether22001
Router (config-evpn-ac)# ethernet-segment identifier type 0 ff.ff.ff.ff.ff.ff.ff.ff.ee
Router (config-evpn-ac-es)# bgp route-target 2200.0001.0001
Router (config-evpn-ac-es)# exit
Router (config-evpn)# evi 24001
Router (config-evpn-evi)# bgp
Router (config-evpn-evi-bgp)# route-target import 64:24001
Router (config-evpn-evi-bgp)# route-target export 64:24001
Router (config-evpn-evi-bgp)# exit
Router (config-evpn-evi)# exit
Router (config-evpn)# evi 21006
Router (config-evpn-evi)# bgp
Router (config-evpn-evi-bgp)# route-target route-target 64:10000
Router (config-evpn-evi-bgp)# exit
Router (config-evpn-evi)# exit
Router (config-evpn)# evi 22101
Router (config-evpn-evi)# bgp
Router (config-evpn-evi-bgp)# route-target import 64:22101
Router (config-evpn-evi-bgp)# route-target export 64:22101
Router (config-evpn-evi-bgp)# exit
Router (config-evpn-evi)# exit
Router (config-evpn)# evi 22021
Router (config-evpn-evi)# bgp
Router (config-evpn-evi-bgp)# route-target import 64: 22021
Router (config-evpn-evi-bgp)# route-target export 64: 22021
Router (config-evpn-evi-bgp)# exit
Router (config-evpn-evi)# exit
Router (config-evpn-evi)# advertise-mac
Router (config-evpn-evi)# exit
Router (config-evpn)# evi 22022
Router (config-evpn-evi)# bgp
Router (config-evpn-evi-bgp)# route-target import 64: 22022
Router (config-evpn-evi-bgp)# route-target export 64: 22022
Router (config-evpn-evi-bgp)# exit
Router (config-evpn-evi)# advertise-mac
Router (config-evpn-evi)# commit
Router (config-evpn-evi)# exit
```

実行コンフィギュレーション

```
/* Configure attachment circuits */
interface Bundle-Ether22001.12 l2transport
encapsulation dot1q 1 second-dot1q 12
!
interface Bundle-Ether22001.13 l2transport
encapsulation dot1q 1 second-dot1q 13
!
interface Bundle-Ether22001.14 l2transport
```

```
encapsulation dot1q 1 second-dot1q 14
!
interface Bundle-Ether22001.1 l2transport
 encapsulation dot1q 1 second-dot1q 1
!
interface Bundle-Ether22001.2 l2transport
encapsulation dot1q 1 second-dot1q 2
!
interface Bundle-Ether22001.3 l2transport
encapsulation dot1q 1 second-dot1q 3
!
interface Bundle-Ether22001.4 l2transport
encapsulation dot1q 1 second-dot1q 4

/*Configure VLAN Unaware FXC Service */
flexible-xconnect-service vlan-unaware fxc_mh1
  interface Bundle-Ether22001.1
  interface Bundle-Ether22001.2
  interface Bundle-Ether22001.3
 neighbor evpn evi 21006 target 22016
!
/*Configure VLAN Aware FXC Service */
l2vpn
 flexible-xconnect-service vlan-aware evi 24001
   interface Bundle-Ether22001.12
   interface Bundle-Ether22001.13
   interface Bundle-Ether22001.14

/* Configure Local Switching */
flexible-xconnect-service vlan-aware evi 31400
 interface Bundle-Ether22001.1400
 interface Bundle-Ether23001.1400
!
flexible-xconnect-service vlan-aware evi 31401
 interface Bundle-Ether22001.1401
 interface Bundle-Ether23001.1401
!

/* Configure EVPN-VPWS xconnect service and native EVPN with IRB */
interface Bundle-Ether22001.11 l2transport
  encapsulation dot1q 1 second-dot1q 11
  rewrite ingress tag pop 2 symmetric
 !
interface Bundle-Ether22001.21 l2transport
  encapsulation dot1q 1 second-dot1q  21
  rewrite ingress tag pop 2 symmetric
 !
!
l2vpn
xconnect group xg22001
p2p evpn-vpws-mclag-22001
 interface Bundle-Ether22001.11
 neighbor evpn evi 22101 target 220101 source 220301
!
bridge group native_evpn1
   bridge-domain bd21
   interface Bundle-Ether22001.21
    routed interface BVI21
     evi 22021
  !
/* Configure Native EVPN */
Evpn
 interface Bundle-Ether22001
  ethernet-segment   identifier type 0 ff.ff.ff.ff.ff.ff.ff.ff.ee
```

```
 bgp route-target 2200.0001.0001
 !
 evi 24001
  bgp
   route-target import 64:24001
   route-target export 64:24001
  !
  evi 21006
   bgp
     route-target 64:100006
  !
   evi 22101
    bgp
      route-target import 64:22101
      route-target export 64:22101
     !
  evi 22021
   bgp
     route-target import 64:22021
     route-target export 64:22021
    !
   advertise-mac
 !
 evi 22022
  bgp
   route-target import 64:22022
   route-target export 64:22022
  !
   advertise-mac
 !
```

確認

各サービスがサブインターフェイスで設定されているかどうかを確認します。

```
Router# show l2vpn xconnect summary
Number of groups: 6
Number of xconnects: 505  Up: 505  Down: 0  Unresolved: 0 Partially-programmed: 0
AC-PW: 505  AC-AC: 0  PW-PW: 0 Monitor-Session-PW: 0
Number of Admin Down segments: 0
Number of MP2MP xconnects: 0
 Up 0 Down 0
Advertised: 0 Non-Advertised: 0


Router# show l2vpn xconnect-service summary
Number of flexible xconnect services: 74
 Up: 74

Router# show l2vpn flexible-xconnect-service name fxc_mh1
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed
Flexible XConnect Service  Segment
Name    ST  Type  Description  ST
------------------------ ---------------------------- -----------------------------
fxc_mh1 UP  AC:   BE22001.1    UP
            AC:   BE22001.2    UP
            AC:   BE22001.3    UP
----------------------------------------------------------------------------------------

Router# show l2vpn flexible-xconnect-service evi 24001
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed
```

```
Flexible XConnect Service  Segment
Name      ST  Type  Description  ST
------------------------ ----------------------------- -----------------------------
evi:24001 UP  AC:   BE22001.11    UP
              AC:   BE22001.12    UP
              AC:   BE22001.13    UP
              AC:   BE22001.14    UP
----------------------------------------------------------------------------------------


Router# show l2vpn xconnect group xg22001 xc-name evpn-vpws-mclag-22001
Fri Sep 1 17:28:58.259 UTC
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed
XConnect                                Segment 1           Segment 2
Group     Name                    ST     Description ST      Description
 ST
------------------------ ---------------------------- ----------------------------------
xg22001  evpn-vpws-mclag-22001   UP    BE22001.101  UP      EVPN 22101, 220101,64.1.1.6
 UP
----------------------------------------------------------------------------------------
```

関連コマンド

- evpn
- evi
- ethernet-segment
- advertise-mac
- show evpn ethernet-segment
- show evpn evi
- show evpn summary
- show l2vpn xconnect summary
- show l2vpn flexible-xconnect-service
- show l2vpn xconnect group

EVPN MPLS と VPLS のシームレスな統合

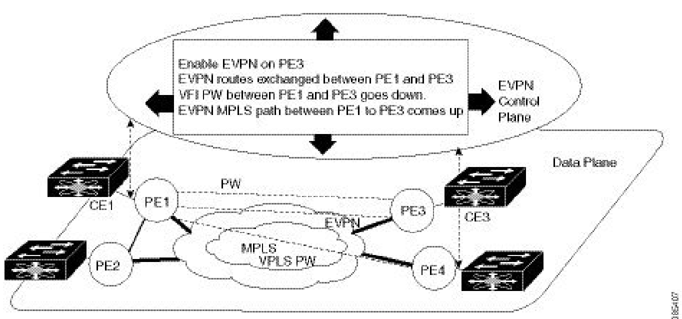
EVPN MPLS と VPLS のシームレスな統合により、同じ VPN インスタンスに対して EVPN と VPLS を実行する PE ノードの共存が可能になります。VPLS またはレガシー ネットワークを、サービスの中断なしで次世代の EVPN ネットワークにアップグレードできます。選択したすべての VPLS プロバイダーエッジ（PE）ノードに、EVPN サービスを同時に導入できます。ただし、トラフィックの中断を回避するため、既存の VPLS 対応 PE で EVPN サービスを 1 つずつプロビジョニングします。

シームレスな統合による VPLS ネットワークの EVPN ネットワークへの移行

EVPN ネットワークでは、VPN インスタンスは EVPN インスタンス ID（EVI）によって識別されます。他の L2VPN テクノロジーと同様に、EVPN インスタンスもルートターゲットおよびルート識別子に関連付けられています。MAC をデータ プレーンで学習する（「フラッディングと学習の技術」を使用して学習する）従来の VPLS とは異なり、EVPN ではコントロール プレーンを使用して MAC を学習し伝播します。EVPN では、MAC ルートは MP BGP プロトコルによって伝送されます。EVPN 対応 PE では、PE のルート ターゲット（RT）が一致した場合にのみ、PE が MAC ルートをラベルとともにそれぞれの EVPN 転送テーブルにインポートします。EVPN PE ルータは、同じ VPN インスタンスで VPLS および EVPN L2 ブリッジングを実行する機能を備えています。EVPN と BGP-AD PW の両方が VPN インスタンスで設定されている場合、EVPN PE は、BGP VPLS 自動検出（AD）ルートと、BGP EVPN 包括マルチキャスト ルート（タイプ 3）を、特定の VPN インスタンスにアドバタイズします。ルート タイプ 3 は入力複製マルチキャスト ルートと呼ばれ、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（BUM）トラフィックの送信に使用されます。その他のリモート PE は、送信側の PE RT が設定済みの RT と一致する場合にのみ、同じ VPN インスタンスに対してタイプ 3 ルートをインポートします。したがって、これらのルート交換の最後に、EVPN 対応 PE は、VPN インスタンスにある他のすべての PE とそれらの関連機能を検出します。PE が自身の BUM トラフィックを他の PE に送信するために使用するタイプ 3 ルートでは、同じ RT を持つ PE が BUM トラフィックを受信することが保証されます。EVPN は、タイプ 2 ルートを使用してカスタマー MAC アドレスをアドバタイズします。

EVPN MPLS と VPLS のシームレスな統合により、ネットワーク サービスを中断することなく、VPLS PE ルータを EVPN に 1 つずつアップグレードすることができます。PE1、PE2、PE3、および PE4 が VPLS PW を使用してフルメッシュ ネットワークで相互接続されている次のトポロジを考えてみます。

図 *6 : EVPN MPLS* と *VPLS* のシームレスな統合



EVPN サービスは、一度に 1 つの PE ノードずつ、ネットワークに導入できます。VPLS サービスの VPN インスタンスで EVPN を有効にすることによって、VPLS から EVPN への移行が PE1 で開始されます。EVPN が有効になるとすぐに、PE1 は他の PE ノードへの EVPN 包括マルチキャスト ルートのアドバタイズを開始します。PE1 は他の PE ノードからの包含マルチキャスト ルートを受信しないため、PE1 と他の PE ノード間の VPLS 擬似回線はアクティブなままです。PE1 は、VPLS 疑似回線を使用してトラフィックの転送を維持します。同時に、PE1 は EVPN ルート タイプ 2 を使用して CE1 から学習したすべての MAC アドレスをアドバタイズし

ます。2 番目のステップでは、EVPN が PE3 で有効になっています。PE3 は、他の PE ノードへの包含マルチキャストルートのアドバタイズを開始します。PE1 と PE3 の両方が EVPN ルートを介して互いを検出します。その結果、PE1 と PE3 は両者間の擬似回線をシャットダウンします。EVPN サービスが、PE1 と PE3 の間で VPLS サービスの代わりとなります。この段階では、PE1 は PE2 と PE4 を使用して VPLS サービスを実行し続け、同じ VPN インスタンスで PE3 を使用して EVPN サービスを開始します。このことを、EVPN と VPLS のシームレスな統合と呼びます。VPLS から EVPN への移行は残りの PE ノードに対して続けられます。最終的に、4 つすべての PE ノードが EVPN サービスで有効になります。VPLS サービスがネットワーク内の EVPN サービスに完全に置き換えられます。すべての VPLS 擬似回線がシャットダウンされます。

既存の VPLS ネットワークでの EVPN の設定

既存の VPLS ネットワークで EVPN を設定するには、次の作業を実行します。

- L2VPN EVPN アドレスファミリの設定
- EVPN コンフィギュレーション モードで、EVI と対応する BGP ルートターゲットを設定します。
- ブリッジドメインでの EVI の設定

さまざまな VPLS ベース ネットワークを EVPN に移行する方法については、L2VPN ブリッジドメインでの EVI の設定 （32 ページ）を参照してください。

L2 EVPN アドレスファミリの設定

BGP と参加ネイバーの両方で EVPN アドレス ファミリを有効にするには、次の作業を実行します。

設定例

```
Router# configure
Router(config)#router bgp 65530
Router(config-bgp)#nsr
Router(config-bgp)#bgp graceful-restart
Router(config-bgp)#bgp router-id 200.0.1.1
Router(config-bgp)#address-family l2vpn evpn
Router(config-bgp-af)#exit
Router(config-bgp)#neighbor 200.0.4.1
Router(config-bgp-nbr)#remote-as 65530
Router(config-bgp-nbr)#update-source Loopback0
Router(config-bgp-nbr)#address-family l2vpn evpn
Router(config-bgp-nbr-af)#commit
```

実行コンフィギュレーション

```
configure
 router bgp 65530
```

```
 nsr
 bgp graceful-restart
 bgp router-id 200.0.1.1
 address-family l2vpn evpn
 !
 neighbor 200.0.4.1
  remote-as 65530
  update-source Loopback0
  address-family l2vpn evpn
  !
!
```

EVPN コンフィギュレーション モードでの EVI と対応する BGP ルート ターゲットの設定

EVI を設定し、対応する BGP ルート ターゲットを定義するには、次の作業を実行します。また、advertise-mac を設定します。設定しないと MAC ルート（タイプ 2）がアドバタイズされません。

設定例

```
Router# configure
Router(config)#evpn
Router(config-evpn)#evi i
Router(config-evpn-evi-bgp)#bgp
Router(config-evpn-evi-bgp)#table-policy spp-basic-6
Router(config-evpn-evi-bgp)#route-target import 100:6005
Router(config-evpn-evi-bgp)#route-target export 100:6005
Router(config-evpn-evi-bgp)#exit
Router(config-evpn-evi)#advertise-mac
Router(config-evpn-evi)#commit
```

実行コンフィギュレーション

```
configure
 evpn
  evi
   bgp
    table-policy spp-basic-6
    route-target import 100:6005
    route-target export 100:6005
    !
   advertise-mac
   !
  !
 !
```

ブリッジ ドメインでの EVI の設定

対応する L2VPN ブリッジ ドメインで EVI を設定するには、次の作業を実行します。

設定例

```
Router# configure
Router(config)#l2vpn
Router(config-l2vpn)#bridge group bg1
Router(config-l2vpn-bg)#bridge-domain bd1
Router(config-l2vpn-bg-bd)#interface GigabitEthernet0/0/0/0
Router(config-l2vpn-bg-bd-ac)#exit
Router(config-l2vpn-bg-bd)#evi 1
Router(config-l2vpn-bg-bd-evi)#exit
Router(config-l2vpn-bg-bd)#vfi v1
Router(config-l2vpn-bg-bd-vfi)#neighbor 10.1.1.2 pw-id 1000
Router(config-l2vpn-bg-bd-vfi-pw)#mpls static label local 20001 remote 10001
Router(config-l2vpn-bg-bd-vfi-pw)#commit
```

実行コンフィギュレーション

```
configure
 l2vpn
  bridge group bg1
   bridge-domain bd1
    interface GigabitEthernet0/0/0/0
    !
    evi 1
    !
   vfi v1
    neighbor 10.1.1.2 pw-id 1000
     mpls static label local 20001 remote 10001
     !
    !
    evi 1
 !
```

L2VPN ブリッジ ドメインでの EVI の設定

次の例は、さまざまな VPLS ベース ネットワークの L2VPN ブリッジドメインでの EVI 設定を示しています。

MPLS スタティック ラベルをベースとする VPLS

```
l2vpn
 bridge group bg1
  bridge-domain bd-1-1
   interface GigabitEthernet0/0/0/0
   !
   vfi vfi-1-1
    neighbor 200.0.2.1 pw-id 1200001
     mpls static label local 20001 remote 10001
    !
    neighbor 200.0.3.1 pw-id 1300001
     mpls static label local 30001 remote 10001
    !
    neighbor 200.0.4.1 pw-id 1400001
     mpls static label local 40001 remote 10001
    !
```

```
  !
  evi 1
!
```

自動検出 BGP および BGP シグナリングをベースとする VPLS

```
l2vpn
bridge group bg1
bridge-domain bd-1-2
   interface GigabitEthernet0/0/0/2
   !
   vfi vfi-1-2
    vpn-id 2
    autodiscovery bgp
     rd 101:2
     route-target 65530:200
     signaling-protocol bgp
      ve-id 11
      ve-range 16
     !
    !
   evi 2
  !
```

ターゲット LDP をベースとする VPLS

```
bridge-domain bd-1-4
   interface GigabitEthernet0/0/0/4
   !
   vfi vfi-1-4
    neighbor 200.0.2.1 pw-id 1200004
    !
    neighbor 200.0.3.1 pw-id 1300004
    !
    neighbor 200.0.4.1 pw-id 1400004
    !
   evi 3
   !
```

EVPN 設定の確認

EVPN の設定と MAC のアドバタイズメントを確認するには、次のコマンドを使用します。EVPN のステータス、AC のステータス、および VFI のステータスを確認します。

- show l2vpn bridge-domain
- show evpn summary
- show bgp rt l2vpn evpn
- show evpn evi
- show l2route evpn mac all

```
Router#show l2vpn bridge-domain bd-name bd-1-1
Mon Feb 20 21:03:40.244 EST
```

```
Legend: pp = Partially Programmed.
Bridge group: bg1, bridge-domain: bd-1-1, id: 0, state: up, ShgId: 0, MSTi: 0
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 1 (1 up), VFIs: 1, PWs: 3 (2 up), PBBs: 0 (0 up), VNIs: 0 (0 up)
  List of EVPNs:
    EVPN, state: up
  List of ACs:
    Gi0/2/0/0.1, state: up, Static MAC addresses: 0, MSTi: 2
  List of Access PWs:
  List of VFIs:
    VFI vfi-1-1 (up)
      Neighbor 200.0.2.1 pw-id 1200001, state: up, Static MAC addresses: 0
      Neighbor 200.0.3.1 pw-id 1300001, state: down, Static MAC addresses: 0
      Neighbor 200.0.4.1 pw-id 1400001, state: up, Static MAC addresses: 0
  List of Access VFIs:
 When PEs are evpn enabled, pseudowires that are associated with that BD will be brought
 down. The VPLS BD pseudowires are always up.
```

EVI の設定済みのローカルおよびリモート MAC ルートのうちアドバタイズされたものの数を確認します。

```
Router#show evpn summary
Mon Feb 20 21:05:16.755 EST
-----------------------------
Global Information
-----------------------------
Number of EVIs                      : 6
Number of Local EAD Entries         : 0
Number of Remote EAD Entries        : 0
Number of Local MAC Routes          : 4
          MAC                       : 4
          MAC-IPv4                  : 0
          MAC-IPv6                  : 0
Number of Local ES:Global MAC       : 1
Number of Remote MAC Routes         : 0
          MAC                       : 0
          MAC-IPv4                  : 0
          MAC-IPv6                  : 0
Number of Remote SOO MAC Routes     : 0
Number of Local IMCAST Routes       : 4
Number of Remote IMCAST Routes      : 4
Number of Internal Labels           : 0
Number of ES Entries                : 1
Number of Neighbor Entries          : 4
EVPN Router ID                      : 200.0.1.1
BGP ASN                             : 65530
PBB BSA MAC address                 : 0026.982b.c1e5
Global peering timer                :      3 seconds
Global recovery timer               :     30 seconds
```

EVPN ルートターゲットを確認します。

```
Router#show bgp rt l2vpn evpn
Mon Feb 20 21:06:18.882 EST
EXTCOMM         IMP/EXP
RT:65530:1               1 / 1
RT:65530:2               1 / 1
RT:65530:3               1 / 1
RT:65530:4               1 / 1
Processed 4 entries
```

```
Locally learnt MAC routes can be viewed by forwarding table
show l2vpn forwarding bridge-domain mac-address location 0/0/cpu0
To Resynchronize MAC table from the Network Processors, use the command...
    l2vpn resynchronize forwarding mac-address-table location <r/s/i>

Mac Address    Type    Learned from/Filtered on    LC learned Resync Age/Last Change
Mapped to
-------------- ------- --------------------------- ---------- ----------------------
0033.0000.0001 dynamic Gi0/2/0/0.1                 N/A        20 Feb 21:06:59     N/A

0033.0000.0002 dynamic Gi0/2/0/0.2                 N/A        20 Feb 21:06:59     N/A

0033.0000.0003 dynamic Gi0/2/0/0.3                 N/A        20 Feb 21:04:29     N/A

0033.0000.0004 dynamic Gi0/2/0/0.4                 N/A        20 Feb 21:06:59     N/A

The remote routes learned via evpn enabled BD
show l2vpn forwarding bridge-domain mac-address location 0/0$
To Resynchronize MAC table from the Network Processors, use the command...
    l2vpn resynchronize forwarding mac-address-table location <r/s/i>

Mac Address    Type    Learned from/Filtered on    LC learned Resync Age/Last Change
Mapped to
-------------- ------- --------------------------- ---------- ----------------------
0033.0000.0001 EVPN    BD id: 0                    N/A        N/A                 N/A

0033.0000.0002 EVPN    BD id: 1                    N/A        N/A                 N/A

0033.0000.0003 EVPN    BD id: 2                    N/A        N/A                 N/A

0033.0000.0004 EVPN    BD id: 3                    N/A        N/A                 N/A
```

特定の VPN インスタンスに関係のある EVPN MAC ルートを確認します。

```
Router#show evpn evi vpn-id 1 mac
Mon Feb 20 21:36:23.574 EST

EVI        MAC address    IP address                       Nexthop
   Label
---------- -------------- ----------------------------------------
---------------------------------
1      0033.0000.0001      ::                         200.0.1.1
45106
```

L2 ルーティングを確認します。

```
Router#show l2route evpn mac all
Mon Feb 20 21:39:43.953 EST
Topo ID  Mac Address    Prod   Next Hop(s)
-------- -------------- ------ ----------------------------------------
0        0033.0000.0001 L2VPN  200.0.1.1/45106/ME
1        0033.0000.0002 L2VPN  200.0.1.1/45108/ME
2        0033.0000.0003 L2VPN  200.0.1.1/45110/ME
3        0033.0000.0004 L2VPN  200.0.1.1/45112/ME
```

EVPN ルート タイプ 2 ルートを確認します。

```
Router#show bgp l2vpn evpn route-type 2
Mon Feb 20 21:43:23.616 EST
```

```
BGP router identifier 200.0.3.1, local AS number 65530
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 21
BGP NSR Initial initsync version 1 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 200.0.1.1:1
*>i[2][0][48][0033.0000.0001][0]/104
                      200.0.1.1                     100      0 i
Route Distinguisher: 200.0.1.1:2
*>i[2][0][48][0033.0000.0002][0]/104
                      200.0.1.1                     100      0 i
Route Distinguisher: 200.0.1.1:3
*>i[2][0][48][0033.0000.0003][0]/104
                      200.0.1.1                     100      0 i
Route Distinguisher: 200.0.1.1:4
*>i[2][0][48][0033.0000.0004][0]/104
                      200.0.1.1                     100      0 i
Route Distinguisher: 200.0.3.1:1 (default for vrf bd-1-1)
*>i[2][0][48][0033.0000.0001][0]/104
                      200.0.1.1                     100      0 i
Route Distinguisher: 200.0.3.1:2 (default for vrf bd-1-2)
*>i[2][0][48][0033.0000.0002][0]/104
                      200.0.1.1                     100      0 i
Route Distinguisher: 200.0.3.1:3 (default for vrf bd-1-3)
*>i[2][0][48][0033.0000.0003][0]/104
                      200.0.1.1                     100      0 i
Route Distinguisher: 200.0.3.1:4 (default for vrf bd-1-4)
*>i[2][0][48][0033.0000.0004][0]/104
                      200.0.1.1                     100      0 i

Processed 8 prefixes, 8 paths
```

包含マルチキャスト ルートとルート タイプ 3 ルートを確認します。

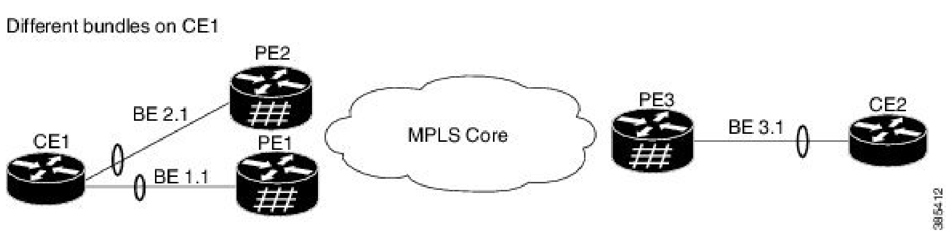
```
Router#show bgp l2vpn evpn route-type 3
Mon Feb 20 21:43:33.970 EST
BGP router identifier 200.0.3.1, local AS number 65530
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 21
BGP NSR Initial initsync version 1 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 200.0.1.1:1
*>i[3][0][32][200.0.1.1]/80
                      200.0.1.1                     100      0 i
Route Distinguisher: 200.0.1.1:2
*>i[3][0][32][200.0.1.1]/80
```

```
                      200.0.1.1                     100      0 i
Route Distinguisher: 200.0.1.1:3
*>i[3][0][32][200.0.1.1]/80
                      200.0.1.1                     100      0 i
Route Distinguisher: 200.0.1.1:4
*>i[3][0][32][200.0.1.1]/80
                      200.0.1.1                     100      0 i
Route Distinguisher: 200.0.3.1:1 (default for vrf bd-1-1)
*>i[3][0][32][200.0.1.1]/80
                      200.0.1.1                     100      0 i
*> [3][0][32][200.0.3.1]/80
                      0.0.0.0                                0 i
Route Distinguisher: 200.0.3.1:2 (default for vrf bd-1-2)
*>i[3][0][32][200.0.1.1]/80
                      200.0.1.1                     100      0 i
*> [3][0][32][200.0.3.1]/80
                      0.0.0.0                                0 i
Route Distinguisher: 200.0.3.1:3 (default for vrf bd-1-3)
*>i[3][0][32][200.0.1.1]/80
                      200.0.1.1                     100      0 i
*> [3][0][32][200.0.3.1]/80
                      0.0.0.0                                0 i
Route Distinguisher: 200.0.3.1:4 (default for vrf bd-1-4)
*>i[3][0][32][200.0.1.1]/80
                      200.0.1.1                     100      0 i
*> [3][0][32][200.0.3.1]/80
                      0.0.0.0                                0 i
```

EVPN シングルアクティブ マルチホーミング

EVPN シングルアクティブ マルチホーミング機能はシングルアクティブ冗長モードをサポートしています。シングルアクティブ モードでは、PE ノードは EVPN サービス インスタンス（EVI）に基づいて、イーサネット セグメントとの間で発着信するイーサネット セグメント ロード バランス トラフィックにローカルに接続されます。EVPN サービス インスタンス内では、1 つの PE のみがイーサネット セグメントとの間で発着信するトラフィックを転送します。

図 *7: EVPN*：シングルアクティブ マルチホーミング



ここには、CE1 が PE1 と PE2 のマルチホームであるトポロジが示されています。PE1 と PE2 は MPLS コアを通じて PE3 に接続しています。CE3 はイーサネット インターフェイス バンドルを通じて PE3 に接続されています。PE1 と PE2 はタイプ 4 ルートをアドバタイズしてから、指定フォワーダ（DF）の選択を実行します。非 DF はシングルアクティブ モードの両方向のトラフィックをブロックします。

CE1 から CE2 へのトラフィック フローを考えてみます。CE1 は PE1 と PE2 の両方に Address Resolution Protocol（ARP）ブロードキャスト要求を送信します。PE1 が EVI の指定フォワーダである場合、PE1 は CE1 から ARP 要求を転送します。PE2 は CE1 からのトラフィックをド

ロップします。その後で、すべてのユニキャスト トラフィックが PE1 を通じて送信されます。PE2 はスタンバイになるか、またはブロックされます。トラフィックはこのパスを介して送信されません。PE1 は PE3 に MAC をアドバタイズします。PE3 は常に PE1 を通じてトラフィックを送受信します。PE3 はイーサネット インターフェイス バンドルを介してトラフィックを CE2 に送信します。

EVPN シングルアクティブ マルチホーミングの設定

EVPN シングルアクティブ マルチホーミング機能を設定するには、PE1 と PE2 上で次のタスクを実行します。

EVPN イーサネット セグメントの設定

EVPN イーサネット セグメントを設定するには、次のタスクを実行します。

```
Router# configure
Router(config)# evpn
Router(config-evpn)# timers
Router(config-evpn-timers)# peering 15
Router(config-evpn-timers)# recovery 30
Router(config-evpn-timers)# exit
Router(config-evpn)# interface Bundle-Ether1
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 40.00.00.00.00.00.00.00.01
Router(config-evpn-ac-es)# load-balancing-mode single-active
Router(config-evpn-ac-es)# bgp route-target 4000.0000.0001
Router(config-evpn-ac-es)# service-carving manual primary 100 secondary 200
Router(config-evpn-ac-es-man)# exit
Router(config-evpn-ac-es)# exit
Router(config-evpn-ac)# mac-flush mvrp
Router(config-evpn-ac)# timers
Router(config-evpn-ac-timers)# peering 15
Router(config-evpn-ac-timers)# recovery 30
Router(config-evpn-ac-timers)# commit
Router(config-evpn-ac-timers)# exit
```

実行コンフィギュレーション

```
configure
evpn
 timers
  peering 15
  recovery 30
!
  interface Bundle-Ether1
   ethernet-segment
    identifier type 0 40.00.00.00.00.00.00.00.01
    load-balancing-mode single-active
    bgp route-target 4000.0000.0001
    service-carving manual primary 100 secondary 200
!
   mac-flush mvrp
    timers
     peering 15
     recovery 30
!
```

EVPN サービス インスタンス（EVI）パラメータの設定

EVPN サービス インスタンス（EVI）パラメータを定義するには、このタスクを実行します。

```
Router# configure
Router(config)# evpn
Router(config-evpn)# evi 6005
Router(config-evpn-evi)# bgp
Router(config-evpn-evi-bgp)# rd 200:50
Router(config-evpn-evi-bgp)# route-target import 100:6005
Router(config-evpn-evi-bgp)# route-target export 100:6005
Router(config-evpn-evi-bgp)# exit
Router(config-evpn-evi)# advertise-mac
Router(config-evpn-evi)# commit
Router(config-evpn-evi)# exit
```

実行コンフィギュレーション

```
configure
evpn
 evi 6005
  bgp
   rd 200:50
   route-target import 100:6005
   route-target export 100:6005
!
  advertise-mac

!
```

レイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスを定義するには、次のタスクを実行します。

```
Router# configure
Router(config)# interface bundle-ether2.1 l2transport
Router(config-subif-l2)# no shutdown
Router(config-subif-l2)# encapsulation dot1q 1
Router(config-subif-l2)# rewrite ingress tag pop 1 symmetric
Router(config-subif-l2)#commit
Router(config-subif-l2)#exit
```

実行コンフィギュレーション

```
configure
interface bundle-ether2.1 l2transport
 no shutdown
 encapsulation dot1q 1
 rewrite ingress tag pop 1 symmetric
!
```

ブリッジ ドメインの設定

次のステップを実行して PE1 と PE2 上にブリッジ ドメインを設定します。

```
Router# configure
```

```
Router(config)# l2vpn
Router(config-l2vpn)# bridge group 6005
Router(config-l2vpn-bg)# bridge-domain 6005
Router(config-l2vpn-bg-bd)# interface Bundle-Ether2.1
Router(config-l2vpn-bg-bd-ac)# evi 6005
Router(config-l2vpnbg-bd-evi)# commit
Router(config-l2vpnbg-bd-evi)# exit
```

実行コンフィギュレーション

```
configure
l2vpn
 bridge group 6005
  bridge-domain 6005
   interface Bundle-Ether2.1
    evi 6005
!
```

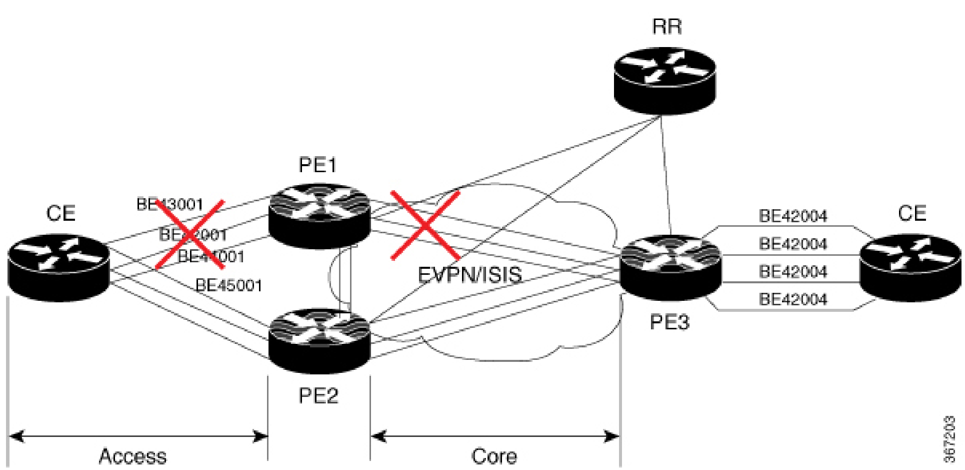
EVPN コア分離保護

EVPN コア分離保護機能を使用すると、コア内のリンク障害をモニタして検出することができます。プロバイダー エッジ（PE）デバイスでコア リンク障害が検出されると、EVPN は、PE のイーサネット セグメント（ES）を停止します。ES は、カスタマー エッジ（CE）デバイスに接続しているアクセス インターフェイスに関連付けられています。

EVPN は、ICCP のコア分離の検出を置き換えるものです。この新機能により、EVPN 環境で ICCP を使用する必要がなくなります。

CE が PE1 および PE2 に接続されているトポロジを考えてみます。PE1、PE2、および PE3 では、MPLS コア ネットワーク上で EVPN が実行されています。コア インターフェイスにはギガビット イーサネットまたはバンドル インターフェイスを使用できます。

図 8 : EVPN コア分離保護



PE1 のコア リンクがダウンすると、EVPN はリンク障害を検出し、アクセス ネットワークをダウンさせてコア ネットワークから PE1 ノードを分離します。これにより、CE は PE1 にトラフィックを送信できなくなります。BGP セッションもダウンしているため、BGP は、障害が

発生したPEによってアドバタイズされたすべてのルートを無効にします。これにより、リモート PE2 および PE3 は、L2FIB 内のネクストホップ パスリストと MAC ルートを更新します。PE2はすべてのトラフィックの転送者になるため、コア ネットワークからPE1を分離します。

すべてのコア インターフェイスと BGP セッションがアップすると、PE1 はイーサネット A-D イーサネットセグメント（ES-EAD）ルートを再度アドバタイズし、サービスカービングをトリガーして、コア ネットワークの一部になります。

EVPN コア分離保護の設定

EVPN グループの配下にコア インターフェイスを設定し、そのグループを、CE に接続された接続回線（AC）であるイーサネット セグメントに関連付けます。すべてのコアインターフェイスがダウンすると、EVPNは、関連付けられているアクセスインターフェイスをダウンさせます。これにより、CE デバイスは自身のバンドル内でこれらのリンクを使用できなくなります。グループの一部であるすべてのインターフェイスがダウンすると、EVPNはバンドルをダウンさせ 、ES-EAD ルートを取り消します。

制約事項

- EVPN の配下には最大 24 のグループを作成できます。
- グループの下には最大 12 のコア インターフェイスを追加できます。
- コア インターフェイスはグループ間で再利用できます。コア インターフェイスは、バンドル インターフェイスにすることができます。
- EVPNグループにはコア インターフェイスのみを含める必要があります。 EVPNグループの配下にアクセス インターフェイスを追加しないでください。
- アクセス インターフェイスは、バンドル インターフェイスにしかなれません。
- EVPN コアに面するインターフェイスは、物理インターフェイスまたはバンドル メイン インターフェイスのみにする必要があります。サブインターフェイスはサポートされていません。

```
Router# configure
Router(config)# evpn
Router(config-evpn)# group 42001
Router(config-evpn-group)# core interface GigabitEthernet0/2/0/1
Router(config-evpn-group)# core interface GigabitEthernet0/2/0/3
Router(config-evpn-group)#exit
!
Router(config-evpn)# group 43001
Router(config-evpn-group)# core interface GigabitEthernet0/2/0/2
Router(config-evpn-group)# core interface GigabitEthernet0/2/0/4
Router(config-evpn-group)#exit
!
Router# configure
Router(config)# evpn
Router(config-evpn)# interface bundle-Ether 42001
Router(config-evpn-ac)# core-isolation-group 42001
Router(config-evpn-ac)# exit
```

```
!
Router(config-evpn)# interface bundle-Ether 43001
Router(config-evpn-ac)# core-isolation-group 43001
Router(config-evpn-ac)# commit
```

実行コンフィギュレーション

```
configure
 evpn
  group 42001
   core interface GigabitEthernet0/2/0/1
   core interface GigabitEthernet0/2/0/3
   !
  group 43001
   core interface GigabitEthernet0/2/0/2
   core interface GigabitEthernet0/2/0/4
   !
 !
configure
 evpn
  interface bundle-Ether 42001
   core-isolation-group 42001
   !
  interface bundle-Ether 43001
   core-isolation-group 43001
   !
  !
```

確認

show evpn group コマンドは、evpn グループの完全なリストと、それらに関連付けられているコア インターフェイスおよびアクセス インターフェイスを表示します。各インターフェイスのステータス（アップまたはダウン）も表示されます。アクセスインターフェイスがアップ状態になるには、コア インターフェイスが少なくとも 1 つアップ状態である必要があります。

```
Router# show evpn group /* Lists specific group with core-interfaces and access interface
 status */
EVPN Group: 42001
  State: Ready
  Core Interfaces:
     Bundle-Ethernet110: down
     Bundle-Ethernet111: down
     GigabethEthernet0/2/0/1: up
     GigabethEthernet0/2/0/3: up
     GigabethEthernet0/4/0/8: up
     GigabethEthernet0/4/0/9: up
     GigabethEthernet0/4/0/10: up
  Access Interfaces:
     Bundle-Ether42001: up

EVPN Group: 43001
  State: Ready
  Core Interfaces:
     Bundle-Ethernet110: down
     GigabethEthernet0/2/0/2: up
     GigabethEthernet0/2/0/4: up
     GigabethEthernet0/4/0/9: up
```

```
Access Interfaces:
   Bundle-Ether43001: up
```

EVPN ルーティング ポリシー

EVPN ルーティング ポリシー機能では、アドレスファミリ L2VPN EVPN のルート ポリシー サポートを提供します。この機能は、EVPN ルート フィルタリング機能をルーティング ポリシー言語（RPL）に追加します。フィルタリングはさまざまな EVPN 属性に基づきます。

ピアから受け入れるか、ピアにアドバタイズされる、または1個のルーティング プロトコルから別のプロトコルへ再配布されるときに、ルートを検査し、フィルタリングして、属性を変更するように、ルーティング ポリシーがルータに指示します。

この機能により、より粒度が高いルートポリシーの定義を提供するルートポリシー一致基準の EVPN ルートタイプ 1 ～ 5 の EVPN ネットワーク層到達可能性情報（NLRI）属性を使用してルートポリシーを設定できます。たとえば、ルートポリシーを特定の EVPN ルートタイプのみに適用したり、任意の組み合わせの EVPN NLRI 属性に適用できます。この機能は、ルートポリシーを有効にして EVPN NLRI 属性でフィルタリングすることで、ソリューションの設定および展開に柔軟性をもたらします。

この機能を実装するには、次の概念を理解する必要があります。

- ルーティング ポリシー言語
- ルーティング ポリシー言語の構造
- ルーティング ポリシー言語コンポーネント
- ルーティング ポリシー言語使用方法
- ポリシー定義
- パラメータ化
- ポリシー適用のセマンティック
- ポリシー ステートメント
- 接続点

これらの概念については「ルーティング ポリシーの実装」を参照してください。

現在、この機能は接続ポイント「イン」または「アウト」の BGP ネイバーでのみサポートされています。ルート ポリシーは BGP ネイバーのインバウンドまたはアウトバウンドのみに適用できます。

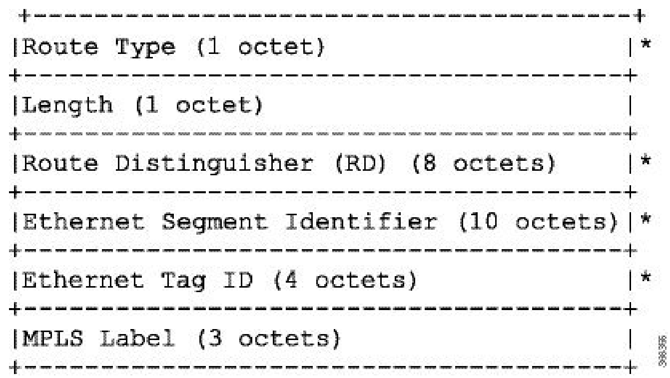
EVPN ルート タイプ

EVPN NLRI には次のさまざまなルート タイプがあります。

ルート タイプ 1：イーサネット自動検出（AD）ルート

イーサネット（AD）ルートは、EVI ごととイーサネットセグメント識別子（ESI）ごとにアドバタイズされます。これらのルートは、イーサネットセグメント（ES）ごとに送信されます。これらは ES に属している EVI のリストを伝送します。ESI フィールドは、CE がシングルホームの場合はゼロに設定されます。

イーサネット A-D ルート タイプ固有の EVPN NLRI は次のフィールドで構成されます。



NLRI の形式：**ルートタイプ 1**：

`[Type][Len][RD][ESI][ETag][MPLS Label]`

ネット属性：`[Type][RD][ESI][ETag]`

パス属性：`[MPLS Label]`

例

```
route-policy evpn-policy
  if rd in (1.1.1.1:0) [and/or evpn-route-type is 1] [and/or esi in
(0a1.a2a3.a4a5.a6a7.a8a9)] [and/or etag is 4294967295] then
    set ..
  endif
end-policy
!
route-policy evpn-policy
  if rd  in (1.1.1.2:0) [and/or evpn-route-type is 1] [and/or esi in
(00a1.a2a3.a4a5.a6a7.a8a9)] [and/or etag is 4294967295] then
    set ..
  endif
end-policy
```

ルート タイプ 2：MAC/IP アドバタイズメント ルート

ホストの IP アドレスと MAC アドレスが NLRI 内のピアにアドバタイズされます。MAC アドレスのコントロール プレーン学習は不明ユニキャストのフラッディングを削減します。

MAC/IP アドバタイズメント ルート タイプ固有の EVPN NLRI は次のフィールドで構成されます。

```
+---------------------------------------+
|Route Type (1 octet)                   |*
+---------------------------------------+
|Length (1 octet)                       |
+---------------------------------------+
|RD (8 octets)                          |*
+---------------------------------------+
|Ethernet Segment Identifier (10 octets)|
+---------------------------------------+
|Ethernet Tag ID (4 octets)             |*
+---------------------------------------+
|MAC Address Length (1 octet)           |*
+---------------------------------------+
|MAC Address (6 octets)                 |*
+---------------------------------------+
|IP Address Length (1 octet)            |*
+---------------------------------------+
|IP Address (0, 4, or 16 octets)        |*
+---------------------------------------+
|MPLS Label1 (3 octets)                 |
+---------------------------------------+
|MPLS Label2 (0 or 3 octets)            |
+---------------------------------------+
```

NLRI の形式：ルートタイプ **2**：

`[Type][Len][RD][ESI][ETag][MAC Addr Len][MAC Addr][IP Addr Len][IP Addr][MPLS Label1][MPLS Label2]`

ネット属性：`[Type][RD][ETag][MAC Addr Len][MAC Addr][IP Addr Len][IP Addr]`

パス属性：`[ESI], [MPLS Label1], [MPLS Label2]`

例

```
route-policy evpn-policy
  if rd in (1.1.1.2:0) [and/or evpn-route-type is 2] [and/or esi in
(0000.0000.0000.0000.0000)] [and/or etag is 0] [and/or macaddress in (0013.aabb.ccdd)]
[and/or destination in (1.2.3.4/32)] then
    set ..
  endif
end-policy
```

ルート タイプ 3：包括的なマルチキャスト イーサネット タグ ルート

このルートは、送信元 PE からリモート PE へのブロードキャスト、不明ユニキャスト、およびマルチキャスト（BUM）トラフィック用の接続を確立します。このルートは、VLAN ごとと ESI ごとにアドバタイズされます。

包括的マルチキャスト イーサネット タグ ルート タイプ固有の EVPN NLRI は次のフィールドで構成されます。

```
+---------------------------------------+
|  Route Type (1 octet)                 |*
+---------------------------------------+
|  Length (1 octet)                     |
+---------------------------------------+
|  RD (8 octets)                        |*
+---------------------------------------+
|  Ethernet Tag ID (4 octets)           |*
+---------------------------------------+
|  IP Address Length (1 octet)          |*
+---------------------------------------+
|  Originating Router's IP Address      |*
| (4 or 16 octets)                      |
+---------------------------------------+
```

308357

NLRI の形式：ルートタイプ 3：

`[Type][Len][RD][ETag][IP Addr Len][Originating Router's IP Addr]`

ネット属性：`[Type][RD][ETag][IP Addr Len][Originating Router's IP Addr]`

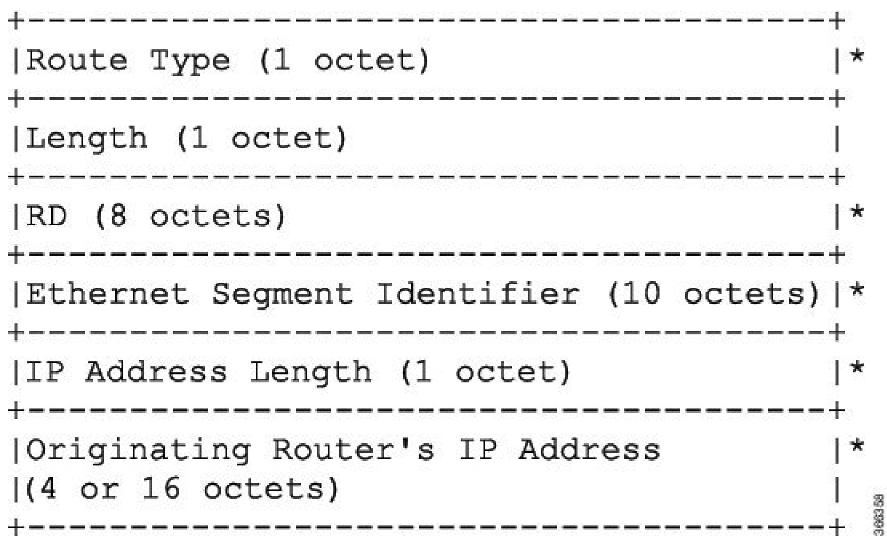
例

```
route-policy evpn-policy
  if rd  in (1.1.1.1:300) [and/or evpn-route-type is 3] [and/or etag is 0] [and/or
evpn-originator in (1.1.1.1)] then
    set ..
  endif
end-policy
```

ルート タイプ 4：イーサネット セグメント ルート

イーサネット セグメント ルートでは CE デバイスを 2 台のデバイスまたは PE デバイスを接続できます。ES ルートでは同じイーサネット セグメントに接続されている PE デバイスを検出できます。

イーサネットセグメントルートタイプ固有のEVPNNLRIは次のフィールドで構成されます。



NLRI の形式：**ルートタイプ 4**：

```
[Type][Len][RD][ESI][IP Addr Len][Originating Router's IP Addr]
```

ネット属性：`[Type][RD][ESI][IP Addr Len][Originating Router's IP Addr]`

例

```
route-policy evpn-policy
  if rd  in (1.1.1.1:0) [and/or evpn-route-type is 4] [and/or esi in
(00a1.a2a3.a4a5.a6a7.a8a9)] [and/or evpn-originator in (1.1.1.1)] then
    set ..
  endif
end-policy
```

ルート タイプ 5：IP プレフィックス ルート

IP プレフィックス ルート タイプ固有の EVPN NLRI は次のフィールドで構成されます。

```
+---------------------------------------+
|Route Type (1 octet)                   |*
+---------------------------------------+
|Length (1 octet)                       |
+---------------------------------------+
|RD   (8 octets)                        |*
+---------------------------------------+
|Ethernet Segment Identifier (10 octets)|
+---------------------------------------+
|Ethernet Tag ID (4 octets)             |*
+---------------------------------------+
|IP Address Length (1 octet)            |*
+---------------------------------------+
|IP Address (4 or 16 octets)            |*
+---------------------------------------+
|GW IP Address (4 or 16 octets)         |
+---------------------------------------+
|MPLS Label (3 octets)                  |
+---------------------------------------+
```

NLRI の形式：**ルートタイプ 5**：

`[Type][Len][RD][ESI][ETag][IP Addr Len][IP Addr][GW IP Addr][Label]`

ネット属性：`[Type][RD][ETag][IP Addr Len][IP Addr]`

パス属性：`[ESI], [GW IP Addr], [Label]`

例

```
route-policy evpn-policy
  if rd in (30.30.30.30:1) [and/or evpn-route-type is 5] [and/or esi in
(0000.0000.0000.0000.0000)] [and/or etag is 0] [and/or destination in (12.2.0.0/16)]
[and/or evpn-gateway in (0.0.0.0)] then
    set ..
  endif
end-policy
```

EVPN RPL 属性

ルート識別子

ルート識別子（rd）属性は、8 オクテットで構成されます。rd は EVPN ルートのタイプそれぞれに指定できます。この属性は、ルートポリシーでは必須ではありません。

例

```
rd in (1.2.3.4:0)
```

EVPN ルート タイプ

EVPN ルート タイプ属性は、1 オクテットで構成されます。これによって EVPN ルート タイプが指定されます。EVPN ルート タイプ属性は、特定の EPVN NLRI プレフィックス形式を識別するために使用されます。これは、すべての EVPN ルート タイプのネット属性の 1 つです。

例

```
evpn-route-type is 3
```

```
The following are the various EVPN route types that can be used:
1 - ethernet-ad
2 - mac-advertisement
3 - inclusive-multicast
4 - ethernet-segment
5 - ip-advertisement
```

IP プレフィックス

IP プレフィックス属性は、それぞれ 4 つの部分（アドレス、マスク長、最小一致長、最大一致長）がある IPv4 または IPv6 プレフィックス一致指定を保持しています。アドレスは必須ですが、他の 3 つの部分は任意です。EVPN ルート タイプ 2 での IP プレフィックスの指定により、IPv4 または IPv6 のいずれかのホスト IP アドレスを表します（/32 または /128）。EVPN ルート タイプ 5 の IP プレフィックスでの指定により、IPv4 または IPv6 のサブネットを表します。これは、EVPN ルート 2 と 5 のネット属性の 1 つです。

例

```
destination in (128.47.10.2/32)
destination in (128.47.0.0/16)
destination in (128:47::1/128)
destination in (128:47::0/112)
```

esi

イーサネット セグメント識別子（ESI）属性は、10 オクテットで構成されます。これは EVPN ルート タイプ 1 と 4 のネット属性であり、EVPN ルート タイプ 2 と 5 のパス属性です。

例

```
esi in (ffff.ffff.ffff.ffff.fff0)
```

etag

イーサネット タグ属性は 4 オクテットで構成されます。イーサネット タグは、特定のブロードキャスト ドメイン（VLAN など）を識別します。EVPN インスタンスは 1 つまたは複数のブ

ロード キャスト ドメインで構成されます。これは EVPN ルート タイプ 1、2、3、および 5 のネット属性です。

例

```
etag in (10000)
```

mac

MAC 属性は 6 オクテットで構成されます。これは、EVPN ルート 2 のネット属性です。

例

```
mac in (0206.acb1.e806)
```

evpn-originator

evpn-originator 属性は、発信元ルータの IP アドレス（4 または 16 オクテット）を指定します。これは、EVPN ルート 3 と 4 のネット属性です。

例

```
evpn-originator in (1.2.3.4)
```

evpn-gateway

evpn-gateway 属性は、ゲートウェイの IP アドレスを指定します。ゲートウェイ IP アドレスは 32 ビットまたは 128 ビットのフィールド（IPv4 または IPv6）であり、IP プレフィックスに応じてオーバーレイ ネクストホップをエンコードします。ゲートウェイ IP アドレス フィールドは、オーバーレイ ネクストホップとして使用しない場合はゼロに設定できます。これは、EVPN ルート 5 のパス属性です。

例

```
evpn-gateway in (1.2.3.4)
```

EVPN RPL 属性セット

このコンテキストでは、セットという用語を、順序付けのない固有のエレメントの集合を意味する数学的な概念で使用されます。ポリシー言語は、セットをマッチング用の値のグループに対するコンテナとして提供します。セットは、条件式で使用されます。セットの要素はカンマで区切ります。ヌル（空）のセットは許可されます。

prefix-set

prefix-set は、それぞれ 4 つの部分（アドレス、マスク長、最小一致長、最大一致長）がある IPv4 または IPv6 プレフィックス一致指定を保持しています。アドレスは必須ですが、他の 3 つの部分は任意です。prefix-set は 1 つまたは複数の IP プレフィックスを指定します。

例

```
prefix-set ip_prefix_set
14.2.0.0/16,
54.0.0.0/16,
12.12.12.0/24,
50:50::1:0/112
end-set
```

mac-set

mac-set は 1 つまたは複数の MAC プレフィックスを指定します。

例

```
mac-set mac_address_set
1234.2345.6789,
2345.3456.7890
end-set
```

esi-set

esi-set は、1 つまたは複数の ESI を指定します。

例

```
esi-set evpn_esi_set
1234.2345.3456.4567.5678,
1234.2345.3456.4567.5670
end-set
```

etag-set

etag-set は、1 つまたは複数のイーサネット タグを指定します。

例

```
etag-set evpn_etag_set
10000,
20000
end-set
```

EVPN RPL 機能の設定

次の項では、mac-set、esi-set、evpn-gateway、および evpn-originator を設定する方法について説明します。

```
/* Configuring a mac-set and refering it in a route-policy (Attach point - neighbor-in)
 */
Router# configure
Router(config)# mac-set demo_mac_set
Router(config-mac)# 1234.ffff.aaa3,
Router(config-mac)# 2323.4444.ffff
Router(config-mac)# end-set
Router(config)# !
Router(config)# route-policy policy_use_pass_mac_set
Router(config-rpl)# if mac in demo_mac_set then
Router(config-rpl-if)# set med 200
Router(config-rpl-if)# else
Router(config-rpl-else)# set med 1000
Router(config-rpl-else)# endif
Router(config-rpl)# end-policy
Router(config)# commit
Router(config)# router bgp 100
Router(config-bgp)# address-family ipv4 unicast
Router(config-bgp-af)# !
Router(config-bgp-af)# neighbor 10.0.0.10
Router(config-bgp-nbr)# remote-as 8
Router(config-bgp-nbr)# address-family ipv4 unicast
Router(config-bgp-nbr-af)# route-policy policy_use_pass_mac_set in
Router(config-bgp-nbr-af)# commit

/* Configuring a esi-set and refering it in a route-policy (Attach point - neighbor-in)
 */
Router# configure
Router(config)# esi-set demo_esi
Router(config-esi)# ad34.1233.1222.ffff.44ff,
Router(config-esi)# ad34.1233.1222.ffff.6666
Router(config-esi)# end-set
Router(config)# !
Router(config)# route-policy use_esi
Router(config-rpl)# if esi in demo_esi then
Router(config-rpl-if)# set local-preference 100
Router(config-rpl-if)# else
Router(config-rpl-else)# set local-preference 300
Router(config-rpl-else)# endif
Router(config-rpl)# end-policy
Router(config)# commit

/* Configuring evpn-gateway/evpn-originator in a route-policy (Attach point - neighbor-in
 and out) */
Router# configure
Router(config)# route-policy gateway_demo
Router(config-rpl)# if evpn-gateway in (10.0.0.0/32) then
Router(config-rpl-if)# pass
Router(config-rpl-if)# endif
Router(config-rpl)# end-policy
Router(config)# commit
Router(config)# route-policy originator_demo
Router(config-rpl)# if evpn-originator in (10.0.0.1/32) then
Router(config-rpl-if)# set local-preference 100
Router(config-rpl-if)# else
```

```
Router(config-rpl-else)# set med 200
Router(config-rpl-else)# endif
Router(config-rpl)# end-policy
Router(config)# commit
Router(config)# router bgp 100
Router(config-bgp)# address-family ipv4 unicast
Router(config-bgp-af)# !
Router(config-bgp-af)# neighbor 10.0.0.10
Router(config-bgp-nbr)# remote-as 8
Router(config-bgp-nbr)# address-family ipv4 unicast
Router(config-bgp-nbr-af)# route-policy gateway_demo in
Router(config-bgp-nbr-af)# route-policy originator_demo out
Router(config-bgp-nbr-af)# commit
```

実行コンフィギュレーション

```
/* Configuring a mac-set and refering it in a route-policy (Attach point - neighbor-in)
 */
mac-set demo_mac_set
  1234.ffff.aaa3,
  2323.4444.ffff
end-set
!
route-policy policy_use_pass_mac_set
  if mac in demo_mac_set then
    set med 200
  else
    set med 1000
  endif
end-policy
!
router bgp 100
 address-family ipv4 unicast
 !
 neighbor 10.0.0.10
  remote-as 8
  address-family ipv4 unicast
  route-policy policy_use_pass_mac_set in
  !
 !
!
end

/* Configuring a esi-set and refering it in a route-policy (Attach point - neighbor-in)
 */
Wed Oct 26 11:52:23.720 IST
esi-set demo_esi
  ad34.1233.1222.ffff.44ff,
  ad34.1233.1222.ffff.6666
end-set
!
route-policy use_esi
  if esi in demo_esi then
    set local-preference 100
  else
    set local-preference 300
  endif
end-policy
```

EVPN ルート ポリシーの例

```
route-policy ex_2
  if rd in (2.2.18.2:1004) and evpn-route-type is 1 then
    drop
  elseif rd in (2.2.18.2:1009) and evpn-route-type is 1 then
    drop
  else
    pass
  endif
end-policy
!
route-policy ex_3
  if evpn-route-type is 5 then
    set extcommunity bandwidth (100:9999)
  else
    pass
  endif
end-policy
!
route-policy samp
end-policy
!
route-policy samp1
  if rd in (30.0.101.2:0) then
    pass
  endif
end-policy
!
route-policy samp2
  if rd in (30.0.101.2:0, 1:1) then
    pass
  endif
end-policy
!
route-policy samp3
  if rd in (*:*) then
    pass
  endif
end-policy
!
route-policy samp4
  if rd in (30.0.101.2:*) then
    pass
  endif
end-policy
!
route-policy samp5
  if evpn-route-type is 1 then
    pass
  endif
end-policy
!
route-policy samp6
  if evpn-route-type is 2 or evpn-route-type is 5 then
    pass
  endif
end-policy
!
route-policy samp7
  if evpn-route-type is 4 or evpn-route-type is 3 then
    pass
```

```
  endif
end-policy
!
route-policy samp8
  if evpn-route-type is 1 or evpn-route-type is 2 or evpn-route-type is 3 then
    pass
  endif
end-policy
!
route-policy samp9
  if evpn-route-type is 1 or evpn-route-type is 2 or evpn-route-type is 3 or
evpn-route-type is 4 then
    pass
  endif
end-policy
!
route-policy test1
  if evpn-route-type is 2 then
    set next-hop 10.2.3.4
  else
    pass
  endif
end-policy
!
route-policy test2
  if evpn-route-type is 2 then
    set next-hop 10.10.10.10
  else
    drop
  endif
end-policy
!
route-policy test3
  if evpn-route-type is 1 then
    set tag 9988
  else
    pass
  endif
end-policy
!
route-policy samp21
  if mac in (6000.6000.6000) then
    pass
  endif
end-policy
!
route-policy samp22
  if extcommunity rt matches-any (100:1001) then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp23
  if evpn-route-type is 1 and esi in (aaaa.bbbb.cccc.dddd.eeee) then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp24
  if evpn-route-type is 5 and extcommunity rt matches-any (100:1001) then
```

```
    pass
  else
    drop
  endif
end-policy
!
route-policy samp25
  if evpn-route-type is 2 and esi in (1234.1234.1234.1234.1236) then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp26
  if etag in (20000) then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp27
  if destination in (99.99.99.1) and etag in (20000) then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp31
  if evpn-route-type is 1 or evpn-route-type is 2 or evpn-route-type is 3 or
evpn-route-type is 4 or evpn-route-type is 5 then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp33
  if esi in evpn_esi_set1 then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp34
  if destination in (90:1:1::9/128) then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp35
  if destination in evpn_prefix_set1 then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp36
```

```
  if evpn-route-type is 3 and evpn-originator in (80:1:1::3) then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp37
  if evpn-gateway in (10:10::10) then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp38
  if mac in evpn_mac_set1 then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp39
  if mac in (6000.6000.6002) then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp41
  if evpn-gateway in (10.10.10.10, 10:10::10) then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp42
  if evpn-originator in (24.162.160.1/32, 70:1:1::1/128) then
    pass
  else
    drop
  endif
end-policy
!
route-policy example
  if rd in (62300:1903) and evpn-route-type is 1 then
    drop
  elseif rd in (62300:19032) and evpn-route-type is 1 then
    drop
  else
    pass
  endif
end-policy
!
route-policy samp100
  if evpn-route-type is 4 or evpn-route-type is 5 then
    drop
  else
    pass
  endif
end-policy
```

```
!
route-policy samp101
  if evpn-route-type is 4 then
    drop
  else
    pass
  endif
end-policy
!
route-policy samp102
  if evpn-route-type is 4 then
    drop
  elseif evpn-route-type is 5 then
    drop
  else
    pass
  endif
end-policy
!
route-policy samp103
  if evpn-route-type is 2 and destination in evpn_prefix_set1 then
    drop
  else
    pass
  endif
end-policy
!
route-policy samp104
  if evpn-route-type is 1 and etag in evpn_etag_set1 then
    drop
  elseif evpn-route-type is 2 and mac in evpn_mac_set1 then
    drop
  elseif evpn-route-type is 5 and esi in evpn_esi_set1 then
    drop
  else
    pass
  endif
end-policy
!
```

EVPN ELAN での CFM

接続障害管理（CFM）はサービスレベルの Operations and Maintenance（OAM）プロトコルの 1 つで、VLAN ごとにエンドツーエンドのイーサネット サービスをモニタリングおよびトラブルシューティングするためのツールとなります。これには、予防的な接続モニタリング、障害検証、および障害分離の機能が含まれています。Cisco IOS XR ソフトウェア リリース 6.6.1 では、シングルホーム EVPN エミュレート ローカル エリア ネットワーク（ELAN）サービスに対応した CFM サポートが導入されています。この機能は、ユーザの ELAN サービスをユーザのサービスレベル契約（SLA）に照らしてモニタするのに役立ちます。これにより、復元力が高く、市場ごとの運用の複雑さが軽減された、高速のレイヤ 2 およびレイヤ 3 サービスが提供されます。

シングルホーム EVPN ELAN サービス対応の CFM は、CFM の連続性チェック、ITU-T Y.1731 準拠の遅延測定メッセージ（DMM）、および合成損失測定（SLM）の機能をサポートしています。この機能は、物理インターフェイス、サブインターフェイス、バンドルインターフェイスなどの接続回線（AI）で使用できます。

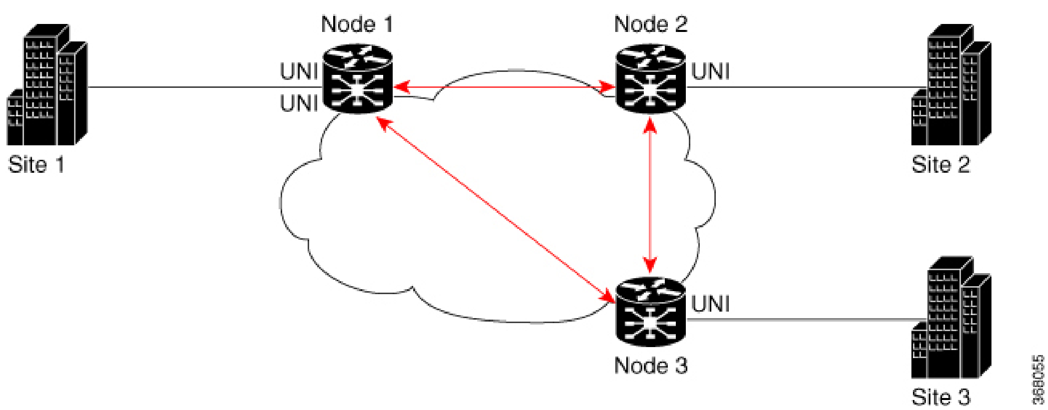
EVPN ELAN での CFM の制約事項

EVPN ELAN での CFM には、次の制限が適用されます。

- シングルホーム EVPN ELAN のみをサポートします。
- アップの MEP のみをサポートします。
- 10 秒以上の CFM タイマー値のみをサポートします。
- ベース ノードごとに最大 20 の EVPN ELAN サービスのみをサポートします。
- EVPN サービスごとに最大 200 のサイトのみをサポートします。
- 損失測定はサポートしていません。
- VPLS を介した CFM はサポートしていません。

EVPN ELAN での CFM の設定

図 *9 : EVPN ELAN* での *CFM* : フル メッシュ トポロジ



このトポロジのノード 1、2、および 3 は、Cisco NCS 5500 シリーズ ルータまたは Cisco NCS 540 シリーズ ルータにすることができます。

EVPN ELAN での CFM の設定には、主に次の作業が伴います。

- CFM サービス連続性チェックの有効化
- MEP クロスチェックの設定
- インターフェイスの CFM のイネーブル化
- SLA プロファイルの設定

EVPN ELAN での CFM の設定例 : フル メッシュ トポロジ

```
/* Enabling CFM continuity check */
Router# ethernet cfm
```

```
Router(config-cfm# domain bd-domain level 1 id null
Router(config-cfm-dmn)# service bd-domain bridge group bg-elan bridge-domain bd-elan id
 icc-based MC MCMC
Router(config-cfm-dmn-svc)# continuity-check interval 1m
/* Configuring MEP cross-check */
Router(config-cfm-dmn-svc)# mep crosscheck
Router(config-cfm-dmn-svc)# mep-id 1112
Router(config-cfm-dmn-svc)# mep-id 1113
Router(config-cfm-dmn-svc)# commit
```

ノード2とノード3について前述の設定を繰り返し、それぞれの mep-id 値を設定します。ノード 2 では、ノード 1 およびノード 3 のそれぞれの mep-id 値（この例ではそれぞれ 1111 および 1113）を使用して MEP クロスチェックを設定します。ノード 3 では、ノード 1 およびノード 2 のそれぞれの mep-id 値（この例ではそれぞれ 1111 および 1112）を使用して MEP クロスチェックを設定します。

```
/* Enabling CFM on the interface */
Router(config)# interface gigabitEthernet 0/0/0/0.100 l2transport
Router(config-subif)# description bg-elan
Router(config-subif)# encapsulation dot1q 100
Router(config-subif)# rewrite ingress tag pop 1 symmetric
Router(config-subif)# mtu 9100
Router(config-subif)# ethernet cfm
Router(config-if-cfm)# mep domain bd-domain service bd-service mep-id 1111
Router(config-if-cfm-mep)# commit
```

ノード 2 とノード 3 について前述の設定を繰り返し、それぞれの *mep-id* 値を設定する必要があります（この例では、ノード 2 の場合は 1112、ノード 3 の場合は 1113）。

```
/* Configuring SLA profile */
Router(config)# ethernet sla
Router(config-sla)# profile test-profile1 type cfm-delay-measurement
Router(config-sla-prof)# probe
Router(config-sla-prof-pb)# send burst every 10 seconds packet count 50 interval 100
milliseconds
Router(config-sla-prof-pb)# exit
Router(config-sla-prof)# schedule
Router(config-sla-prof-schedule)# every 3 minutes for 120 seconds
Router(config-sla-prof-schedule)# exit
Router(config-sla-prof)# statistics
Router(config-sla-prof-stat)# measure round-trip-delay
Router(config-sla-prof-stat-cfg)# buckets size 1 probes
Router(config-sla-prof-stat-cfg)# buckets archive 2
Router(config-sla-prof-stat-cfg)# commit
```

同様に、もう 1 つの sla プロファイル *test-profile2* を設定し、1 秒ごとにパケットを送信するようにプローブ設定を設定します。

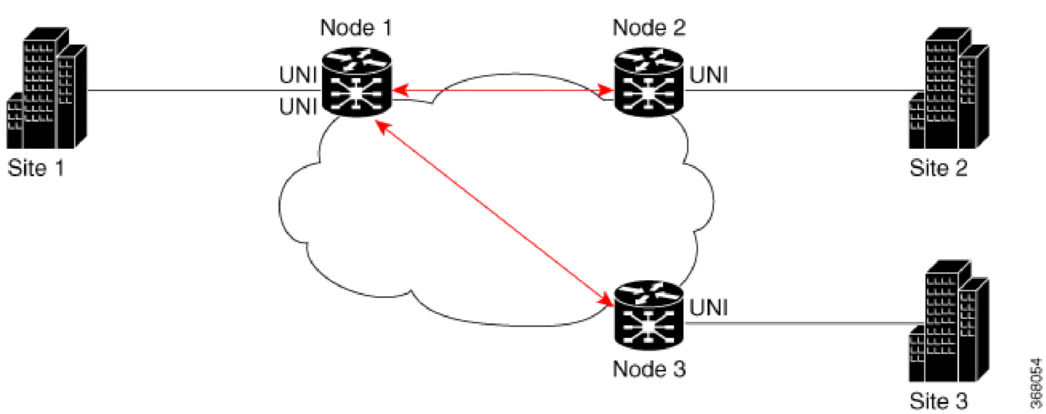
EVPN ELAN での CFM の実行コンフィギュレーション：フル メッシュ トポロジ

ここでは、ノード 1 の実行コンフィギュレーションを示します。

```
ethernet cfm
 domain bd-domain level 1 id null
  service bd-domain bridge group bg-elan bridge-domain bd-elan id icc-based MC MCMC
   continuity-check interval 1m
   mep crosscheck
```

```
    mep-id 1112
    mep-id 1113
   !
  !
 !
!

interface GigabitEthernet0/0/0/0.100 l2transport
 description bg-elan
 encapsulation dot1q 100
 rewrite ingress tag pop 1 symmetric
 mtu 9100
 ethernet cfm
  mep domain bd-domain service bd-service mep-id 1111
 !

ethernet sla
 profile test-profile1 type cfm-delay-measurement
  probe
   send burst every 10 seconds packet count 50 interval 100 milliseconds
  !
  schedule
   every 3 minutes for 120 seconds
  !
  statistics
   measure round-trip-delay
    buckets size 1 probes
    buckets archive 2

profile test-profile2 type cfm-delay-measurement
  probe
   send packet every 1 seconds
  !
  schedule
   every 3 minutes for 120 seconds
  !
  statistics
   measure round-trip-delay
    buckets size 1 probes
    buckets archive 5
```

図 *10 : EVPN ELAN* での *CFM* : ハブ アンド スポーク トポロジ



EVPN ELAN での CFM の設定例：ハブ アンド スポーク トポロジ

ハブ アンド スポーク トポロジの CFM 設定は前述のフル メッシュ トポロジの設定と同じです。ただし、インターフェイスでSLAプロファイル設定について次の追加手順を実行します。

```
/* 1112 and 1113 in this example, are the mep-id values of node 2 and node 3 */
Router(config)#interface gigabitEthernet 0/0/0/0.100 l2transport
Router(config-subif)# ethernet cfm
Router(config-if-cfm)# mep domain bd-domain service bd-service mep-id 1111
Router(config-if-cfm-mep)# sla operation profile test-profile1 target mep-id 1112
Router(config-if-cfm-mep)# sla operation profile test-profile2 target mep-id 1112
Router(config-if-cfm-mep)# sla operation profile test-profile1 target mep-id 1113
Router(config-if-cfm-mep)# sla operation profile test-profile2 target mep-id 1113
Router(config-if-cfm-mep)# commit
```

EVPN ELAN での CFM の実行コンフィギュレーション：ハブ アンド スポーク トポロジ

ここでは、ノード 1 の実行コンフィギュレーションを示します。

```
interface GigabitEthernet0/0/0/0.100 l2transport
 description bg-elan
 encapsulation dot1q 100
 rewrite ingress tag pop 1 symmetric
 mtu 9100
 ethernet cfm
  mep domain bd-domain service bd-service mep-id 1111
   sla operation profile test-profile1 target mep-id 1112
   sla operation profile test-profile2 target mep-id 1112
   sla operation profile test-profile1 target mep-id 1113
   sla operation profile test-profile2 target mep-id 1113
 !
```

関連項目

EVPN ELAN での CFM （58 ページ）

関連コマンド

- continuity-check
- ethernet cfm
- mep crosscheck
- mep domain
- sla operation