ASR 1000によるOverlay Transport Virtualizationの設定

内容

はじめに

このドキュメントでは、ASR1000およびCatalyst 8300/8500シリーズルータでサポートされるOverlay Transport Virtualization(OTV)ネットワークトポロジについて説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ASR1000、IOS® XEバージョン16.10.1a以降
- Catalyst 8300、IOS® XEバージョン17.5.1a以降
- Catalyst 8500、IOS® XEバージョン17.6.1a以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

ASR1000は、Cisco IOS® XEリリース3.5以降でOTVをサポートしています。Catalyst 8300シリーズルータはIOS® XE17.5.1aから、Catalyst 8500シリーズルートはIOS® XEバージョン17.6.1aから、それぞれサポートが開始されています。

OTVは、トランスポートネットワーク全体でMACアドレスベースのルーティングとIPカプセル化フォワーディング(MAC-in-IP)を使用してリモートネットワークサイト間にレイヤ2接続を提供し、クラスタや仮想化などのレイヤ2隣接関係を必要とするアプリケーションをサポートします。OTVは、オーバーレイコントロールプレーンプロトコルを使用して、オーバーレイネットワーク全体にMACルーティング情報を学習し、伝播します。OTVコントロールプレーンプロトコルは、Intermediate-System-to-Intermediate-System(IS-IS)メッセージを使用して、リモートサイトとの隣接関係を構築し、MACルートアップデートをリモートサイトに送信します。OTVは、リモートOTVデバイスを自動検出することで、オーバーレイネットワーク上のリモートサイトとのレイヤ2隣接関係を構築します。

レイヤ2拡張に関するOTVの利点は次のとおりです。

- MPLS要件なし
- メッシュ用の複雑なEthernet over Multiprotocol Label Switching(EoMPLS)設定なし
- レイヤ2拡張のための複雑な仮想プライベートLANサービス(VPLS)の導入が不要
- ネイティブのスパニングツリー分離
  - ブリッジデータプロトコルユニット(BPDU)フィルタを明示的に設定する必要はありません
  - 特定のデータセンターへのスパニングツリー問題のデフォルトの分離
- ネイティブの未知のユニキャストフラッディング分離
  - 不明なユニキャストMACパケットは転送されない
  - MAC単位の未知のユニキャスト転送のサポートが許可される
- OTV ARPキャッシングによるアドレス解決プロトコル(ARP)の最適化
  - 不要なWANトラフィックを削減する
- ファーストホップ冗長プロトコル(FHRP)分離のプロビジョニングの簡素化
- サイトの簡単な追加
- シンプルな冗長構成
- 一時的なサービスが必要な場合に、移行のために「アプライアンスを導入」する機能

要件

以降の項目は、OTVの導入を設計する際に留意すべき主要なルールです。 これらのルールに従えば、設計と導入が合理化されます。

- 設定されたすべてのOTVオーバーレイインターフェイスに対して、1つのインターフェイスだけを使用してOTVカプセル化トラフィックを送信できます。これは結合インターフェイスと呼ばれます
- OTVサイトVLAN用のデータセンターL2サービスインスタンスと、設定されたすべてのOTVオーバーレイインターフェイス用のデータセンター間で拡張されるVLANを設定するために使用できるインターフェイスは1つだけです
- ポートチャネルは、インターフェイスの冗長性とVSSまたはVPCスイッチへの接続に使用でき、接続用に「1つのみ」のインターフェイスとしてサポートされます。
- すべてのOTVルータは、Joinインターフェイスを介して到達可能である必要があります
- データセンターをポイントするOTVルータにスパニングツリーを設定する必要がある
- データセンターのマルチキャストトラフィックを正しく転送するには、IGMPスヌーピングとクエリを設定する必要があります
- 特定のデータセンターは、1台または2台のOTVルータで構成できます。2台のルータを使用して、VLAN番号に基づいて奇数/偶数の方法でVLAN転送を分散します。 データセンター内の各OTVルータは、互いのバックアップとして機能します。
- マルチホームペアは、同じOTVサイトIDで設定する必要がある
- ASR1000/Catalyst 8300/Catalyst 8500とNexus 7000は同じOTVネットワークに参加可能
    - Nexus 7000はOTVフラグメンテーションまたは暗号化をサポートしないため、これらの機能は「ハイブリッド」展開では使用できません。

規定された規則に従わない特定のバックツーバック接続設計がサポートされています。 これらの設定はサポートされていますが、推奨されません。 詳細については、後述の「特殊なユニキャストトポロジ」のセクションを参照してください。

OTVの参加インターフェイスとL2アクセスインターフェイスを設定する際に、現在のOTVソフトウェアに「1つのみ」のインターフェイス制限があることを十分に強調することはできません。ポートチャネルインターフェイスは冗長性のために使用できます。 ポートチャネルのVPC内のNexus 7000への接続はサポートされています。 単一のスイッチへの基本的なポートチャネル接続もサポートされています。

OTV実装タイプ

OTVでは、単一のJoinインターフェイスと単一のL2インターフェイスが必要です。 各OTVルータでは、これらのそれぞれ1つのみをサポートできます。 また、OTVでは、マルチホームOTVルータがローカルネットワークを介して相互に通信できるように、サイトVLANを設定する必要があります。 シングルホームのOTVルータでも、OTVサイトVLANが設定されている必要があります。 また、各サイトまたはデータセンターには、一意のサイト識別子を設定する必要があります。 デュアルホームOTVルータは、同じサイトIDを使用し、同じVLANで通信できる必要があります。

以降の設定では、OTVに必要な基本的な設定が提供されますが、ユニキャストまたはマルチキャ

ストコアの設定を追加する必要があるため、完全ではありません。 これについては、このドキュメントの後続のセクションで詳しく説明します。

```
otv site bridge-domain 100
otv site-identifier 0000.0000.1111
!
interface Overlay1
  no ip address
  otv join-interface GigabitEthernet0/0/0
  service instance 99 ethernet
    encapsulation dot1q 99
    bridge-domain 99
  !
  service instance 90 ethernet
    encapsulation dot1q 90
    bridge-domain 90
!
interface GigabitEthernet1/0/1
  no ip address
  negotiation auto
  service instance 100 ethernet
    encapsulation dot1q 100
    bridge-domain 100
  !
  service instance 99 ethernet
    encapsulation dot1q 99
    bridge-domain 99
  !
  service instance 98 ethernet
    encapsulation dot1q 98 second-dot1q 1098
    rewrite ingress tag trans 2-to-1 dot1q 90 symmetric
    bridge-domain 90
```

サービスインスタンス設定は、OTVを使用するすべてのL2インターフェイス設定に使用されます。

L2インターフェイスの各サービスインスタンスは、特定のシングルまたはダブルタグ付きカプセル化に関連付けられている必要があります。

次に、これらの各サービスインスタンスをブリッジドメインに関連付ける必要があります。

そのブリッジドメインは、オーバーレイインターフェイスに設定されたサービスインスタンスで使用されます。

ブリッジドメインは、オーバーレイサービスインスタンスをL2インターフェイスサービスインスタンスにリンクする接着剤です。

オーバーレイインターフェイスでのトラフィックのカプセル化は、L2インターフェイスでの書き換え入力後のトラフィックのカプセル化と一致する必要があります。

この例では、Gig1/0/1サービスインスタンス99に入るトラフィックは、単一の802.1Q VLANが99で、ブリッジドメインが99です。オーバーレイインターフェイスのブリッジドメイン99に対応

するサービスインスタンスも、単一の802.1Q VLANが99に設定されています。このケースは最も単純です。

この例では、Gig1/0/1サービスインスタンス98に入るトラフィックは、99および1098のダブル802.1Q VLANとブリッジドメイン90を持ちます。オーバーレイインターフェイス上のブリッジドメイン90を持つ対応するサービスインスタンスは、90の単一の802.1Q VLAN用に設定されます。明らかに、これらは同じではありません。 rewrite ingressコマンドは、トラフィックが入力インターフェイスを通過するときにタグが正しく変換されることを保証します。 L2インターフェイスに入るトラフィックでは、98/1098 802.1Q VLANが90の単一のVLANに置き換えられます。symmetricキーワードにより、L2インターフェイスから出るトラフィックでは、90の単一の802.1Q VLANが98/1098に置き換えられます。

OTVによって拡張される複数の802.1Q VLANを持つサービスインスタンスでは、rewrite ingressコマンドを使用する必要があります。 OTVカプセル化では、単一のVLAN IDのみがサポートされます。 そのため、L2インターフェイス上のダブルVLAN設定は、オーバーレイインターフェイスサービスインスタンス上の単一のタグに書き換える必要があります。 これにより、あいまいなVLAN設定はサポートされなくなります。

タグの書き換えの詳細については、次のドキュメントを参照してください。
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/command/ce-cr-book/ce-m1.html

この例では、OTVサイトのブリッジドメインは100です。

- OTVサイトブリッジドメインは、L2インターフェイスでのみ設定されます。
- OTVサイトのブリッジドメインをオーバーレイインターフェイスで設定しないでください。設定すると、OTVの展開が不安定になります。
- OTVサイトVLANは、OTVルータにのみ接続する必要があり、他のデータセンター/ユーザトラフィックを伝送しない。
- OTVサイトVLANは、OTV拡張VLANと同じ物理インターフェイス上に存在する必要がある

マルチホーム

データセンターは、単一のOTVホストまたは最大2台の冗長ホスト（マルチホームとも呼ばれる）に接続できます。 マルチホームは、復元力とロードバランシングに使用されます。サイトに複数のエッジデバイスが存在し、両方が同じオーバーレイネットワークに参加している場合、そのサイトはマルチホームであると見なされます。OTVマルチホームは、VLAN番号に基づいて、奇数/偶数の方法で同じサイトに属する2つのOTVルータ間でVLANを分割します。一方のエッジデバイスがすべての奇数VLANのAEDとして選択され、もう一方のOTVルータがすべての偶数VLANのAEDとして選択されます。各AEDは、他のルータ上でアクティブになっているVLANのスタンバイでもあります。いずれかのAEDでリンクまたはノード障害が発生した場合、スタンバイAEDがすべてのVLANでアクティブになります。

マルチホームを実行するために2台のASR1000が同じデータセンターに接続されている場合、2台のASR1000間に専用リンクは必要ありません。OTVは、内部インターフェイスを通じて伝播されたOTVサイトVLANと、結合インターフェイスを通じて通信を行い、偶数および奇数のVLANを担当するルータを判別します。

ASR1000とNexus 7000を同じデータセンター内に混在させることはできません。また、OTVを

両方のルータで他方のバックアップとして設定することはできません。特定のデータセンターのマルチホームは、対応するプラットフォーム（ASR1000またはNexus 7000）でサポートされます。ASR1000を1つのデータセンターに、Nexus 7000を別のデータセンターに配置できます。これら2つのプラットフォーム間の相互運用性がテストされ、サポートされています。 マルチホーム対応のデータセンターもあれば、シングルホーム対応のデータセンターもあります。

マルチホームASR1000ルータペアは、同じバージョンのCisco IOS® XEソフトウェアを実行する必要があります。

マルチホームを使用する場合は、OTVルータでスパニングツリーを有効にすることを強くお勧めします。これにより、OTVルータはトポロジ変更通知(TCN)を送信し、隣接するL2スイッチデバイス（スパニングツリー内の他のスイッチも含む）は経過時間タイマーをデフォルトから15秒に短縮します。 これにより、マルチホームペア間で障害または回復が発生した場合に、速度コンバージェンスが大幅に増加します。グローバルコンフィギュレーションに後続の行を追加することで、すべての設定済みサービスインスタンス（OTVに接続しているかどうかに関係なく）に対してスパニングツリーを有効にできます。

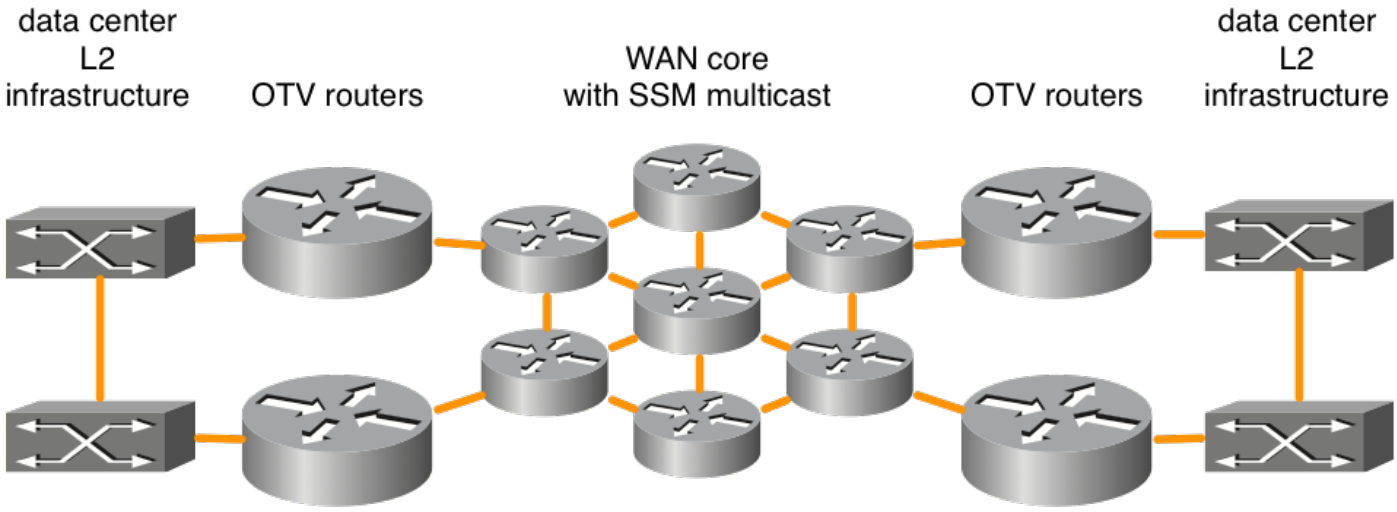
```
spanning-tree mode [ pvst | rapid-pvst | mst ]
```

VLANごとまたはサービスインスタンスごとに固有の設定は必要ありません。

マルチキャストコア

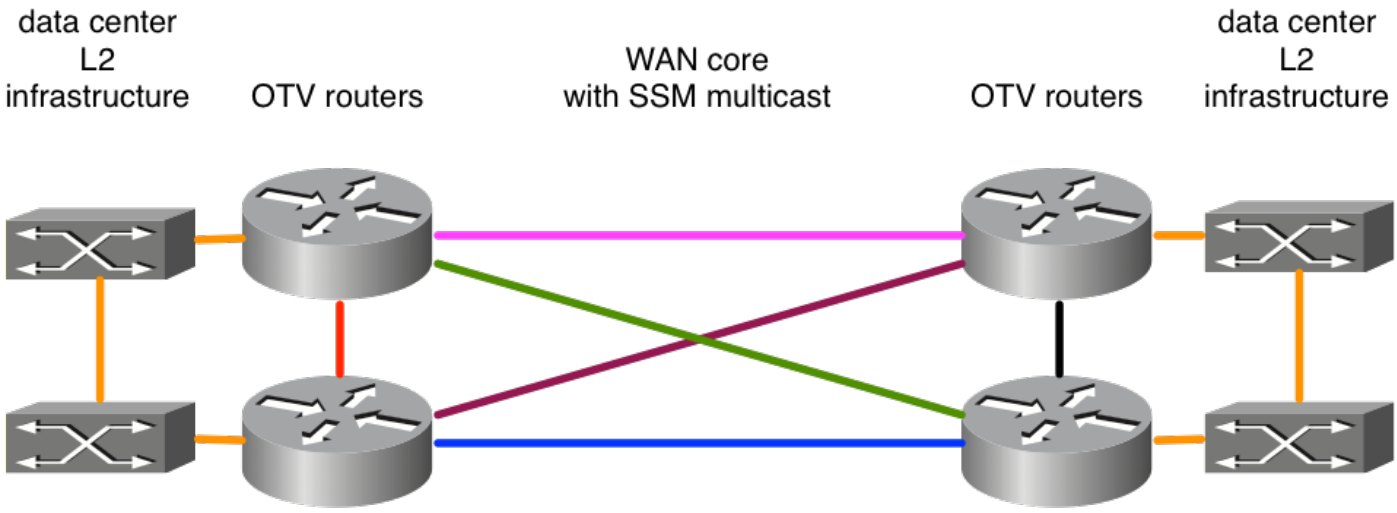
マルチキャストネットワークでは、WAN全体でフルメッシュ接続が必要です。すべてのOTVルータは、Joinインターフェイスを介して相互に接続されている必要があります。

図 1.サポートされるマルチキャストネットワークトポロジ



この図は、コアを介してフルメッシュで接続された2つのデータセンターの例を示しています。Source Specific Multicast(SSM)Protocol Independent Multicast(PIM)は、OTVルータとWANコアルータの間で実行されます。 フルメッシュ接続がある限り、任意の数のコアルータがサポートされます。 WANコアを介したOTV接続には、明示的な最大遅延要件はありません。

図 2：サポートされていないマルチキャストネットワークトポロジ



この例では、ASR1000/OTVはすべてのピアから1つの参加インターフェイスでマルチキャストメッセージを受信することを想定しているため、OTVの展開が不安定になる可能性があります。ピンクと青の東西リンクが結合インターフェイスとして設定されていると仮定します。 ピンクのリンクが失敗すると、ルータはそのインターフェイスでOTVアップデートを受信できなくなります。 join-interfaceが明示的に設定されているため、緑色または紫色のリンクを経由する代替パスは受け入れられません。 そのインターフェイスでアップデートを受信する必要があります。 現時点では、ループバックインターフェイスを結合インターフェイスとして使用することはサポートされていません。

ユーザがバックボーンを所有していない場合、サービスプロバイダーがコアでマルチキャストをサポートし、サービスプロバイダーがInternet Group Management Protocol(IGMP)クエリメッセージに応答できることを確認する必要があります。ASR1000のOTVは、コアWANマルチキャストトポロジへのマルチキャストルータとしてではなく、マルチキャストホストとして機能します（IGMP参加メッセージを転送します）。

OTVルータ間のトランスポートネットワークでは、プロバイダーマルチキャストグループに対してPIMスパースモード(Any Source Multicast [ASM])、配信グループに対してSSMをサポートする必要があります。

マルチキャストコアでは、オーバーレイインターフェイスでコントロールグループ用に特定の設定を行う必要があります。また、データの転送に使用される一連のデータマルチキャストグループも必要です。

```
ip multicast-routing distributed
ip pim ssm default
!
interface Port-channel60
 encapsulation dot1Q 30
 ip address 10.0.0.1 255.255.255.0
 ip pim passive
 ip igmp version 3
!
interface Overlay99
 no ip address
```

```
otv control-group 239.1.1.1
otv data-group 232.192.1.0/24
otv join-interface Port-ch60
```

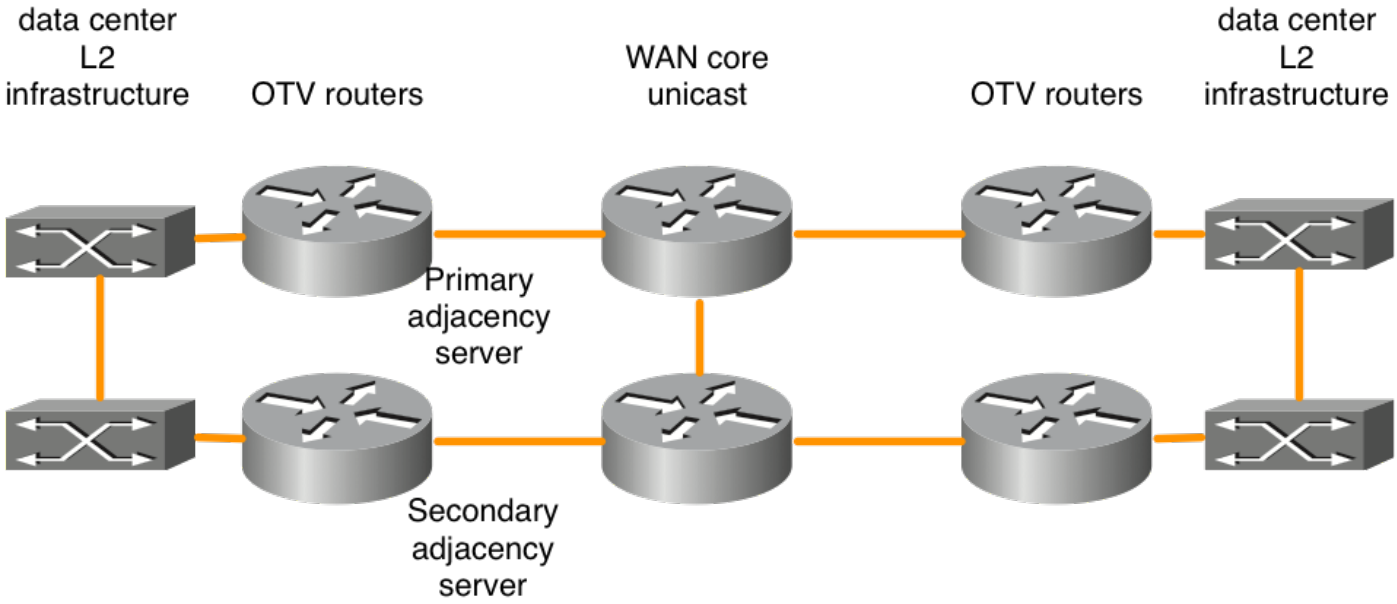
マルチキャストOTVの導入では、JoinインターフェイスをPIMパッシブインターフェイスとして設定する必要があります。 IGMPは、必要に応じて、異なるバージョンに対して設定できます。オーバーレイインターフェイスには、コントロールグループとデータグループが設定されている必要があります。 コントロールグループは、OTV管理に使用される単一のマルチキャストグループです。 data-groupは、データセンター間でユーザデータを転送するために使用されるマルチキャストアドレスの範囲です。 data-groupが232.0.0.0/8のIP空間にない場合、追加コマンド「ip pim ssm range」を設定して、OTVに必要な範囲を含める必要があります。

OTVルータ間のトランスポートネットワークでは、プロバイダーマルチキャストグループに対してはPIMスパースモード(Any Source Multicast [ASM])、配信グループに対してはSource Specific Multicast(SSM)をサポートする必要があります。

隣接関係サーバを使用するユニキャストコア

Cisco IOS® XE 3.9では、ユニキャストコアを使用したOTVのサポートが追加されました。OTVのユニキャストコアとマルチキャストコアは、すべてのASR1000プラットフォームとCisco IOS® XE 3.9からの今後のリリースで引き続きサポートされます。

図 3：ユニキャストネットワークトポロジ



OTV隣接関係サーバ機能は、OTVエッジ間のユニキャストのみの転送を可能にします。 隣接関係サーバの役割で設定されたOTVルータは、すべての既知のOTVルータのリストを保持します。このリストは、登録されているすべてのOTVルータに提供されるため、ルータは、複製されたブロードキャストおよびマルチキャストトラフィックを受信する必要があるデバイスのリストを持ちます。

ユニキャストのみのトランスポート経由のOTVコントロールプレーンは、マルチキャストコアを使用するOTVとまったく同じように機能します。ただし、ユニキャストコアネットワークでは、

各OTVエッジデバイスが各コントロールプレーンパケットの複数のコピーを作成し、同じ論理オーバーレイ内の各リモートエッジデバイスにユニキャストする必要があります。

同じ考え方で、データセンターからのすべてのマルチキャストトラフィックはローカルOTVルータで複製され、複数のコピーが各リモートデータセンターに送信されます。 この方法は、レプリケーションをWANコアに依存するよりも効率的ではありませんが、コアマルチキャストネットワークの設定と管理は必要ありません。 データセンターのマルチキャストトラフィックの量が少ない場合、またはデータセンターの場所の数が少ない場合（4つ以下）、通常はOTV転送用のユニキャストコアが最適な選択肢です。 全体として、ユニキャストのみのモデルは運用が簡素化されるため、4つ以下のデータセンター間でのみLAN拡張接続が必要なシナリオでは、ユニキャストコア導入オプションが優先されます。 少なくとも2つの隣接関係サーバ（プライマリとバックアップ）を設定することをお勧めします。 アクティブ/アクティブ隣接関係サーバ設定のオプションはありません。

OTVルータは、適切なアジャセンシー関係サーバを正しく識別して登録するように、適切に設定する必要があります。

	プライマリ隣接関係サーバ	セカンダリ隣接サーバ	その他のOTVルータ
OTV参加インターフェイスのIPアドレス	10.0.0.1	10.2.2.24	その他のIPアドレス
コンフィギュレーション	インターフェイスオーバーレイ1 otv adjacency-server unicast-only	インターフェイスオーバーレイ1 otv adjacency-server unicast-only otv use-adjacency-server 10.0.0.1 unicast-only	インターフェイスオーバーレイ1 otv use-adjacency-server 10.0.0.1 10.2.2.24 unicast-only

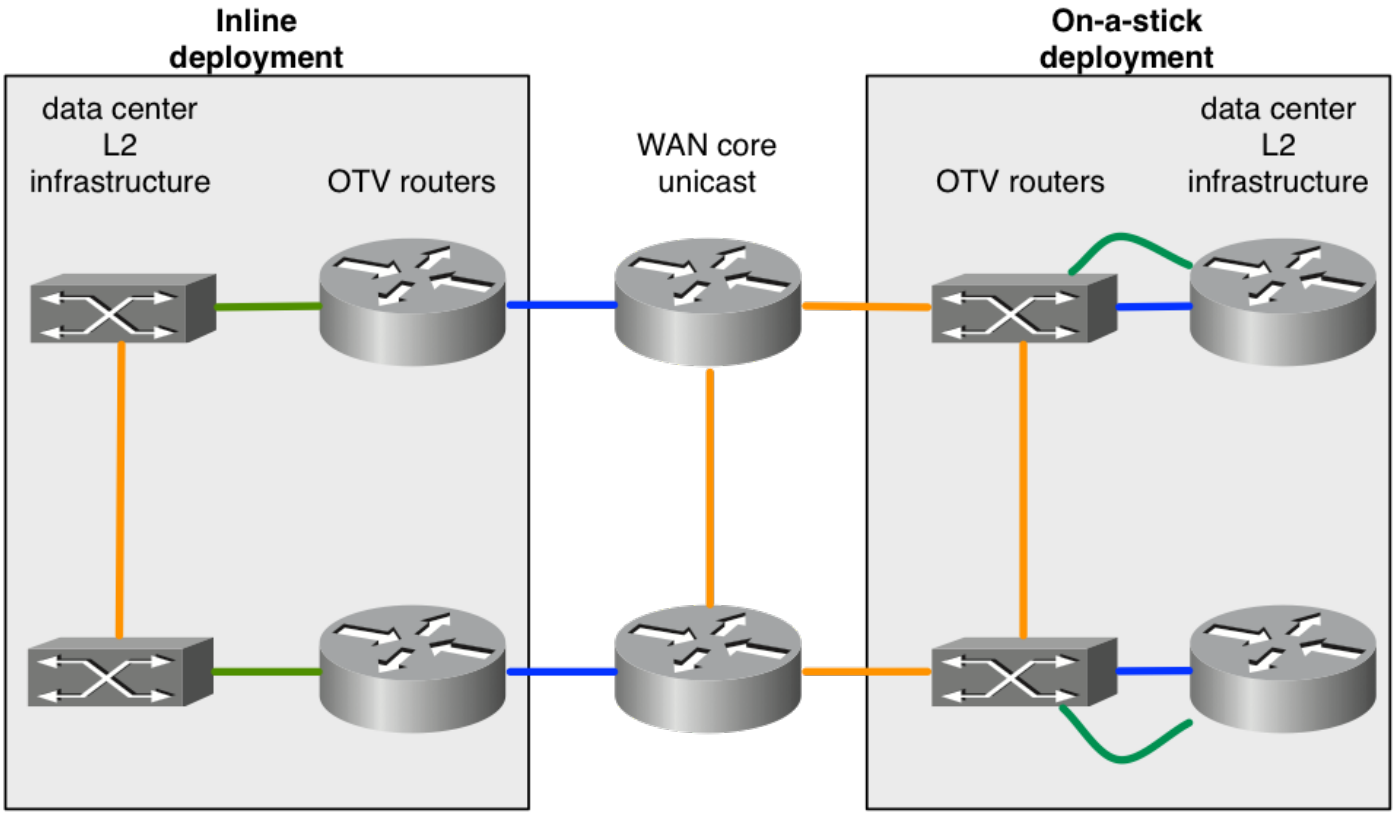
「フルメッシュ」ルールに従わないユニキャストOTV転送でサポートされるバックツーバック接続の設計がいくつかあります。 これらの設定はサポートされていますが、推奨されません。 このタイプの導入は、データセンターがダークファイバで接続されている場合に最も一般的です。この設定オプションの詳細については、後の「特殊なユニキャストトポロジ」の項を参照してください。

スティック上のOTVとインライン

データセンターにOTVを導入するには、on a stickとinlineの2つのモデルがあります。前述の設計シナリオでは、OTVルータはデータセンターとサービスプロバイダーコアネットワークの間にインライン配置されています。ただし、すべてのトラフィックのトランスポートパスにないことをアプライアンスとしてOTVルータを追加する方が望ましいと考えられます。現在の機器を使用してサービスプロバイダーに接続するために、現在のトポロジを変更しないことが要件になる場合

があります（たとえば、Catalyst 6000スイッチまたはOTVをサポートしないNexusスイッチハードウェアを使用した既存環境の導入）。そのため、OTVアプライアンスとしてオンアスティックでASR1000にOTVを導入することを推奨します。

図 4：インラインとスティック上のトポロジ



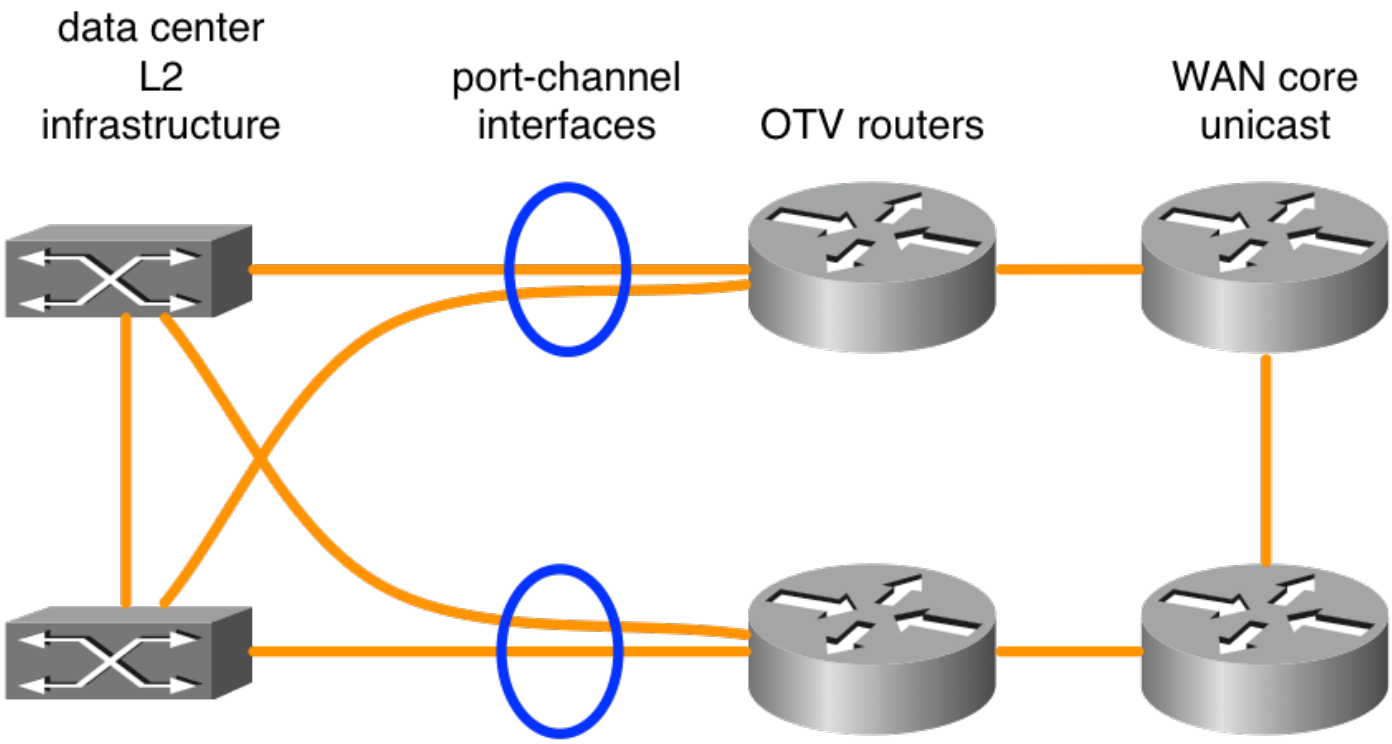
この図は、同じオーバーレイに含めることができる2つの導入モデルを示しています。 OTVルータに接続されている緑色のリンクは、VLANトラフィックを受け入れるL2アクセスインターフェイスとして設定されています。 OTVルータに接続されている青色のリンクは、OTVカプセル化VLANトラフィックを伝送する参加インターフェイスです。

OTVでサポートされていない機能を設定する必要がある場合があります。たとえば、OTVとMPLSを同じボックスに設定することはできません。その結果、ASR1000/OTV on a stickを使用し、OTVルータの前にあるルータでMPLSを設定することが適切なオプションになります。

レイヤ2およびレイヤ3用のポートチャネル

ASR1000用のCisco IOS® XE 3.10コードは、OTVを使用したレイヤ2およびレイヤ3ポートチャネル設定をサポートするように追加されました。レイヤ2ポートチャネルは、内部インターフェイスとして使用できます。 ポートチャネルは最大4つの物理インターフェイスで構成する必要があります。レイヤ3ポートチャネルは、結合インターフェイスとして使用できます。

図 5.L2接続に使用されるポートチャネル



この図は、VSS（Catalyst 6000シリーズ）またはVPC（Nexus 7000シリーズ）の2台のスイッチを使用した一般的なポートチャネルシナリオを示しています。 このタイプの設計では、デュアルOTVルータによる冗長性と、データセンターインフラストラクチャへのデュアル接続が提供されます。 OTVルータに隣接するL2スイッチング機器でVSSまたはVPCが使用されている場合は、基本的なポートチャネル設定以外にOTVの特別な設定は必要ありません。

[Default Gateway]

定義上、OTVは複数の場所に同じL3サブネットを作成します。 これには、拡張VLANとの間でL3トラフィックをルーティングする際に、特別な考慮事項がいくつかあります。 L3ルーティングは、OTVルータ自体に設定することも、拡張VLANに接続された他のデバイスに設定することもできます。 また、各シナリオでは、ホットスタンバイ冗長プロトコル(HSRP)や仮想ルータ冗長プロトコル(VRRP)などのファーストホップ冗長プロトコル(FHRP)を導入して冗長性を確保できます。 HSRPは、特定のデータセンターに対してローカルに実行することも、データセンター間で拡張することもできます（通常は使用しません）。

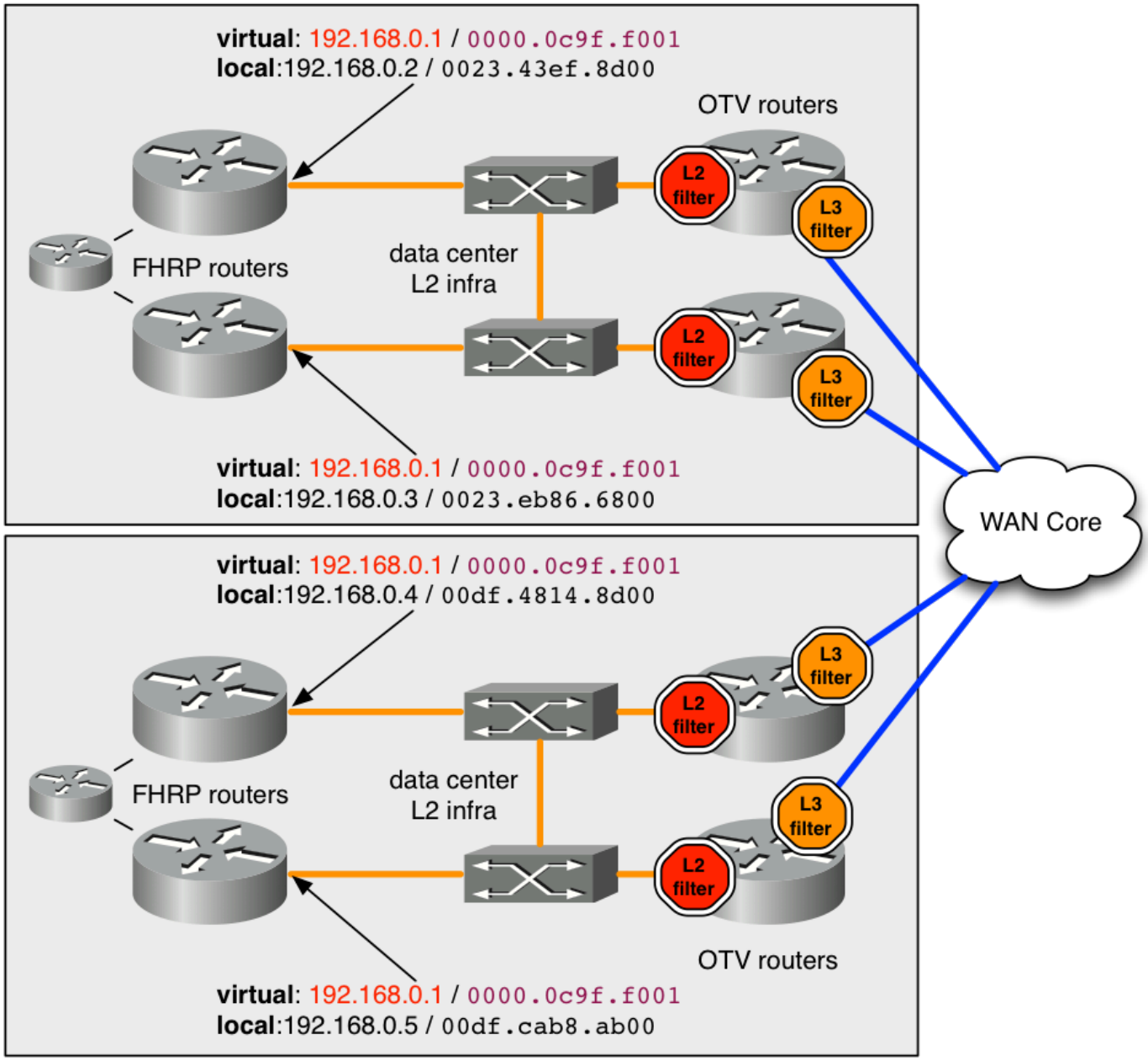
FHRPを使用するOTV導入のベストプラクティスは、FHRPのローカルインスタンスを各データセンターで実行させることです。 FHRPのこれらのインスタンスは同じ仮想MACアドレスとIPアドレスを使用するため、仮想マシン(VM)がデータセンター間を移動しても中断することなく接続が維持されます。 デフォルトルータのMACアドレスがデータセンター間で変更される場合、VMのデフォルトゲートウェイARPエントリがタイムアウトするまで、VMはサブネット外で通信できません。

OTVでFHRPを適切に展開するには、どのL2およびL3トラフィックをフィルタリングして、OTVから分離する必要があるかを考慮する必要があります。L2レベルでは、これは複数の場所でFHRPによって使用される同じL2仮想MACをOTVが認識しないようにする必要があります。 アクティブ/リスニング/スタンバイの選択が各データセンターにローカライズされるように、HSRPおよびVRRPアドバタイズメントを各データセンターに対して隔離するには、L3レベルで

フィルタが必要です。

デフォルトでは、OTVが有効になるとFHRPフィルタが有効になります。 FHRPをデータセンター間で拡張する必要がある設計の場合は、これを無効にすることができます。 仮想MACアドレスのL2フィルタリングは、デフォルトでは無効になっているため、手動で設定する必要があります。

図 6. FHRPの推奨導入例



この例では、仮想MACアドレス0000.0c9f.f001が、サブネット外の接続のために拡張VLAN上でホストするIPアドレス192.168.0.1に使用されています。 両方のデータセンターで同じ仮想MACおよびIPを使用すると、ホストはデータセンター間で転送する際にサブネットからシームレスに接続できます。

MACアドレス0000.0c9f.f001を複数の場所のOTVから隠すには、VLANにサービスを提供する入力L2フィルタ（図中の赤い停止）を各OTVルータに導入する必要があります。ACLフィルタによって、L2サービスインスタンスで設定されたフィルタACLが入力のために使用され、そのMACから

送信されたすべてのパケットは、ASRのOTVプロセスが前にドロップされます。 そのため、OTVはMACについて学習せず、リモートデータセンターにアドバタイズしません。

既知またはデフォルトのFHRP仮想MACトラフィックをすべて捕捉するための推奨設定を次に示します。

```
mac access-list extended otv_filter_fhrp
 deny 0000.0c07.ac00 0000.0000.00ff any
 deny 0000.0c9f.f000 0000.0000.0fff any
 deny 0007.b400.0000 0000.0000.00ff any
 deny 0000.5e00.0100 0000.0000.00ff any
 permit any any
```

このACLは、HSRPバージョン1および2、ゲートウェイロードバランシングプロトコル(GLBP)、およびVRRPに関連付けられた既知のMACアドレス空間に（この順序で）照合されます。仮想MACがFHRPグループ番号に基づかない標準外の値を使用するように設定されている場合、その仮想MACアドレスをACLの例に明示的に追加する必要があります。 ACLをL2サービスインスタンスに追加する必要があります（以下を参照）。

```
interface Port-channel10
  description *** OTV internal interface ***
  no ip address
  no negotiation auto
!
  service instance 800 ethernet
    encapsulation dot1q 800
    mac access-group otv_filter_fhrp in
    bridge-domain 800
```

また、FHRPホスト間の通信もL3レベルで管理する必要があります。 この図では、単一の拡張サブネット上に4台のFHRPルータが設定されています。 ある程度のL3フィルタがないと、4台すべてのルータが互いを認識し、単一のアクティブデバイスを選出し、さまざまなスタンバイ状態で3台になります。 したがって、1つのデータセンターには2つのローカルスタンバイFHRPルータがありますが、前述のL2フィルタにより、リモートアクティブルータへのL2接続はありません。

望ましい結果は、各データセンターにアクティブFHRPルータ1台とスタンバイFHRPルータ1台を設置することです。 前述の入力L2フィルタは、選出プロセスがルータの実際のIPアドレスとMACアドレスを使用するため、この選出トラフィックを捕捉しません。 デフォルトでは、後続のACLはオーバーレイインターフェイスの出力として適用されます。 オーバーレイインターフェイスの出力は、WANコアへのトラフィックです。 ACLは実行コンフィギュレーションには表示されませんが、「show ip access-list」で確認できます。 UDPポート番号に基づいてFHRP選択トラフィックをフィルタリングする

```
Extended IP access list otv_fhrp_filter_acl
    10 deny udp any any eq 1985 3222
```

```
    20 deny 112 any any
    30 permit ip any
```

このフィルタを無効にする唯一の理由は、VLAN上のすべてのFHRPルータを、アクティブステータスに対する同じ選択に参加させる場合です。 このフィルタを無効にするには、オーバーレイインターフェイスで「no otv filter-fhrp」を設定します。

不明なユニキャスト トラフィック

デフォルトでは、OTVルータによってLANから受信された、リモートOTVロケーションに存在することが不明なMACアドレス宛てのユニキャストトラフィックは廃棄されます。 このトラフィックは不明なユニキャストと呼ばれます。 この廃棄アクションは、ブロードキャストトラフィックによってWANで消費される帯域幅の量を制限するWANコアに向けて行われます。 一般に、LAN上のすべてのホストが十分なブロードキャストトラフィック（ARP、プロトコルブロードキャストなど）を発行し、それが常にOTVルータによって認識され、アドバタイズされて、「既知」であることが期待されます。

特定のアプリケーションでは、サイレントホストを利用します。 通常のスイッチングインフラストラクチャでは、LAN上で不明なユニキャストMACアドレスをL2ブロードキャストすると、サイレントホストがトラフィックを見ることができるため、これは問題にはなりません。 ただし、OTV環境では、OTVルータがデータセンター間のトラフィックをブロックします。

これを補うために、選択的ユニキャストフォワーディングと呼ばれる機能がCisco IOS® XEに統合されました。XE 3.10.6、XE3.13.3、XE 3.14.1、XE3.15以降のすべてのリリースでは、選択的ユニキャストフォワーディングがサポートされています。

オーバーレイインターフェイスでは、MACアドレスごとに1つのコマンドを追加して設定します。 例：

```
interface Overlay1
  service instance 100 ethernet
    encapsulation dot1q 100
    otv mac flood 0000.0000.0001
    bridge-domain 100
```

0000.0001.0001宛てのトラフィックは、この例のVLAN 100を持つすべてのリモートOTVルータにフラッディングされる必要があります。 これは、次のコマンドで確認できます。

<#root>

OTV_router_1#

show otv route

```
Codes: BD - Bridge-Domain, AD - Admin-Distance,SI - Service Instance, * - Backup Route
OTV Unicast MAC Routing Table for Overlay99
```

```
 Inst VLAN BD     MAC Address    AD    Owner  Next Hops(s)
------------------------------------------------------------
 0    100  100    0000.0000.0001 20    OTV    Flood
```

そのMACアドレスがリモートサイトで学習された場合は、フラッドエントリよりも優先される転送テーブルにエントリを追加する必要があります。

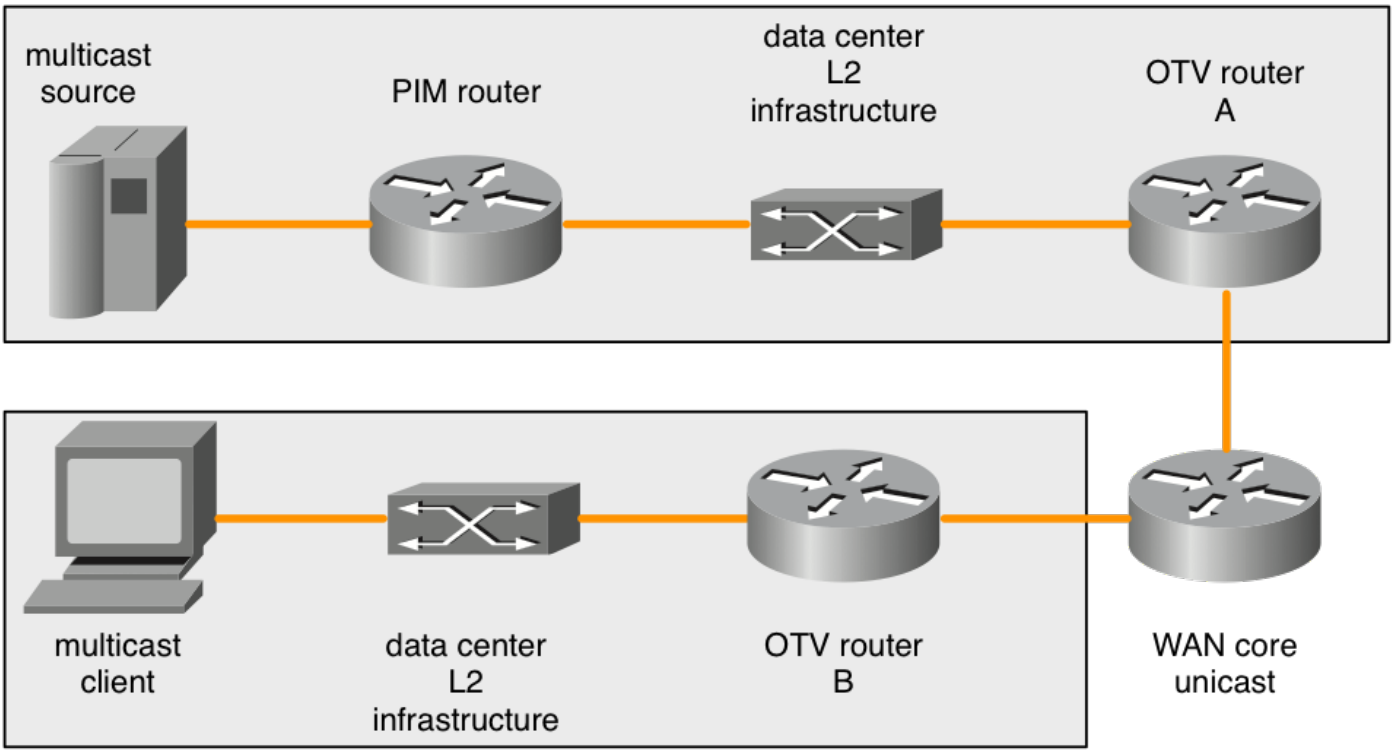
```
<#root>

OTV_router_1#

show otv route


Codes: BD - Bridge-Domain, AD - Admin-Distance,SI - Service Instance, * - Backup Route
OTV Unicast MAC Routing Table for Overlay99
 Inst VLAN BD     MAC Address    AD    Owner  Next Hops(s)
------------------------------------------------------------
 0    100  100    0000.0000.0001 20    OTV    Flood
 0    100  100    0000.0000.0001 50    ISIS   OTV_router_3
```

一般に、特定のMACアドレスのフラッディングエントリは、そのVLANを持つすべてのOTVルータで設定する必要があります。

リモートマルチキャストソース

OTVルータを搭載したASR1000は、LANから受信したマルチキャストIGMP参加要求を転送しません。次の図は、この問題が発生する可能性のあるトポロジの詳細を示しています。

図 7リモートマルチキャストソース



マルチキャストIGMP加入がマルチキャストクライアントから送信されると、ASR1000（OTVルータB）はそれを監視し、マルチキャストグループへの関心をアドバタイズします。 リモートOTVルータ（OTVルータA）は、ローカルL2ブロードキャストドメインで認識されるそのマルチキャストグループにトラフィックを転送する必要があります。 ただし、マルチキャストグループへの関心がクライアントのOTVルータ（OTVルータB）からアドバタイズされた場合、リモートASR1000（OTVルータA）はマルチキャストIGMP参加要求を再生成しません。

マルチキャスト送信元がOTVルータと同じL2ブロードキャストドメインにある場合、これは問題ではありません。 OTVルータは、IGMPクエリアとして設定する必要があります。 これは、L2ブロードキャストドメインに存在するすべてのマルチキャストトラフィックに表示されます。ただし、PIM join要求だけが原因で、PIMルータは別のL2ブロードキャストドメインからのマルチキャスト送信元を、OTVルータが存在するL2ブロードキャストドメインに転送します。

リモートIGMP参加要求は転送も再生成もされません。OTVルータもPIMルータではありません。 そのため、マルチキャスト送信元がL2ブロードキャストドメインに直接存在しない、OTVルータを持つトポロジでは、リモートクライアントが関心を持つ場合にPIMルータから入って送信元トラフィックを転送する方法がありません。

この問題には2つの回避策があります。

まず、ローカルIGMPクライアントをOTVルータ（OTVルータA）に接続されたL2ブロードキャストドメインに展開できます。そのIGMPクライアントは、リモートクライアントがサブスクライブできるマルチキャストグループにサブスクライブする必要があります。 これにより、PIMルータはマルチキャストトラフィックをOTVルータAに隣接するブロードキャストドメインに転送します。 その後、IGMPクエリはマルチキャストトラフィックを取り込み、オーバーレイ経由で送信されます。

もう1つの解決策は、リモートクライアントがサブスクライブする可能性のあるすべてのグループに「ip igmp static-join」を設定することです。 これにより、PIMルータはマルチキャストトラフ

ィックをOTVルータAに隣接するブロードキャストドメインに転送します。

この制限は既知であり、設計仕様の一部です。 これはバグではなく、現時点でサポートされているトポロジの制限と見なされます。

QOS の注意事項

ASR1000のデフォルトでは、追加されたOTVヘッダーのTOS値はL2パケットの802.1pビットからコピーされます。 L2パケットにタグが付けられていない場合は、値0が使用されます。

Nexus 7000のデフォルト動作は、5.2.1以降のソフトウェアでは異なります。 望ましい動作が内部パケットのTOS値を外部にコピーすることである場合は、追加のQoS設定でこれを実現できます。 これにより、新しいNexus 7000ソフトウェアと同じ動作が提供されます。

L2パケットのL3 TOS値をOTVパケットの最も外側のヘッダーにコピーする設定が、その後に続きます。

```
class-map dscp-af11
 match dscp af11
!
class-map dscp-af21
 match dscp af21
!
class-map qos11
 match qos-group 11
!
class-map qos21
 match qos-group 21
!
policy-map in-mark
 class dscp-af11
  set qos-group 11
 class dscp-af21
  set qos-group 21
!
policy-map out-mark
 class qos11
  set dscp af11
 class qos21
  set dscp af21
!
interface Gig0/0/0
 ! L2 interface
 service instance 100 ethernet
  encapsulation dot1q 100
  service-policy in-mark
  bridge-domain 100
!
interface Gig0/0/1
 ! OTV join interface
 service-policy out-mark
```

指定する設定は、入力のさまざまなDSCP値のトラフィックと一致する必要があります。 ローカルで有効なqos-groupタグは、ルータを通過する際にトラフィックを内部的にマークするために使用されます。 出力インターフェイスでは、qos-groupが照合され、それに応じて最も外側のTOSバイトが更新されます。

WAN MTUの考慮事項/フラグメンテーション

OTVでは、基本的にGREヘッダーを使用して、WAN経由でL2トラフィックを転送します。このGREヘッダーのサイズは42バイトです。 理想的なネットワーク展開では、WANリンクの最大伝送ユニット(MTU)は、OTVが処理すると予想される最大パケットよりも少なくとも42バイト大きい必要があります。

L2インターフェイスのMTUが1500バイトの場合、加入インターフェイスのMTUは1542バイト以上である必要があります。 L2インターフェイスのMTUが2000バイトであっても、1500バイトのパケットしか処理しないことが想定されている場合は、1542バイトのWAN MTUで十分ですが、標準の方法で2000に42を追加するのが理想的です。

```
interface GigabitEthernet0/0/0
  mtu 1600
!
interface Overlay 1
  otv join-interface GigabitEthernet0/0/0
!
interface GigabitEthernet0/0/1
  mtu 1500
  service instance 100 ethernet
    encapsulation dot1q 100
    bridge-domain 100
  service instance 101 ethernet
    encapsulation dot1q 101
    bridge-domain 101
```

一部のサービスプロバイダーは、WAN回線に対してより大きなMTU値を提供できません。 この場合、ASR1000はOTV転送データのフラグメンテーションを実行できます。 Nexus 7000にはこの機能はありません。 フラグメンテーションが有効になっているASR1000とNexus 7000 OTVネットワークの混在はASR1000ではサポートされません。

OTVフラグメンテーションの設定は次のとおりです。

```
otv fragmentation join-interface GigabitEthernet0/0/0
!
interface Overlay 1
  otv join-interface GigabitEthernet0/0/0
```

グローバルレベルコマンドは、オーバーレイインターフェイスのjoin-interfaceコマンドの前に設

定することが重要です。 オーバーレイインターフェイスのotv join-interfaceコマンドが最初に設定されていた場合は、オーバーレイインターフェイスからotv join-interfaceコマンドを削除し、otv fragmentation join-interfaceコマンドを設定してから、オーバーレイインターフェイスのotv join-interfaceコマンドを再度設定します。

OTVフラグメンテーションが有効になっていない場合、カプセル化されたL2データを伝送するすべてのOTVパケットは、転送中にフラグメント化されないようにDFビットを設定して送信されます。 フラグメンテーションコマンドが追加されると、DFビットは0に設定されます。OTVルータ自体でパケットをフラグメント化でき、他のルータによって転送中にフラグメント化できます。

ASR1000プラットフォームで使用できるパケット再構成バッファの量は限られているため、パケットを送信するために細かく分割する必要があるフラグメントが少ないほど優れています。 これにより、効率が向上し、WAN全体の帯域幅使用量が減少します（これが問題になる場合）。 OTVフラグメンテーションを有効にするためのパフォーマンス上の影響があります。 フラグメンテーションが存在し、1 Gb/秒を超えるOTVトラフィックが処理されることが予想される場合は、OTVのパフォーマンスをさらに調査する必要があります。

特殊なユニキャストトポロジ

OTVのフィールド展開では、2つのデータセンターのOTVルータ間に直接バックツーバックファイバ接続が確立されることがよくあります。

シングルホーム接続トポロジの場合、これはOTVおよび非OTVトラフィックが参加インターフェイスを共有する標準的な導入に適しています。 この設定に関して特別な考慮事項は必要ないため、このセクションは適用されません。

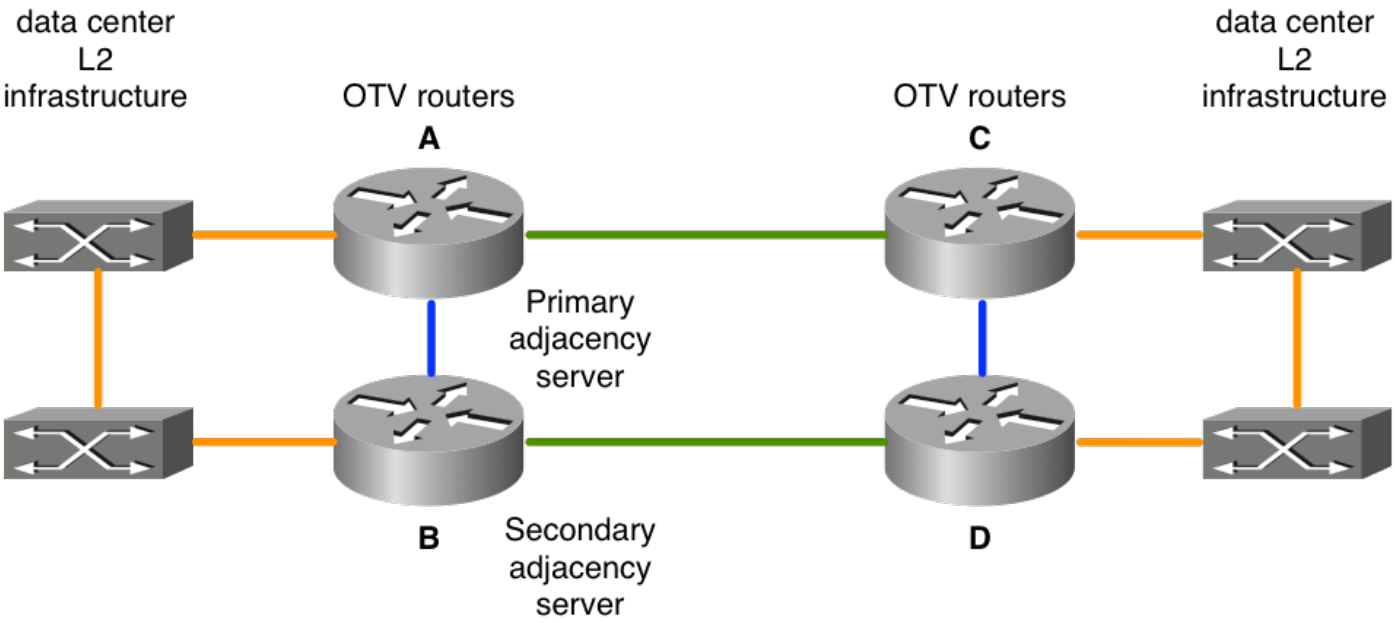
ただし、展開に2つのデータセンターのマルチホームOTVルータがある場合は、いくつかの特別な考慮事項があります。 追加の設定が必要です。

2つ以上のデータセンターが関係する場合、この特別な設定は適用されません。

シングルホームまたはマルチホームのOTVルータを使用する3つ以上のデータセンターのシナリオでは、標準のユニキャストまたはマルチキャストOTV展開を使用する必要があります。

他にサポートされている選択肢はありません。

図 8. 特殊なユニキャスト



示されているトポロジでは、緑色のリンクは2つのデータセンター間のダークファイバリンクです。 これらのダークファイバは、OTVルータに直接接続されています。 OTVルータ間の青色のリンクは、緑色のリンクで障害が発生した場合に非OTVトラフィックを再ルーティングするために使用されます。 上の緑色のリンク（AからC）に障害が発生した場合、最上位のOTVルータをデフォルトルートとして使用する非OTVトラフィックは、南北青色のリンク（AからB、およびCからD）経由で、下のOTVルータペア（BからD）間の引き続き動作可能な緑色のリンクにルーティングされます。

OTVの設定では結合インターフェイスとして物理インターフェイスを指定しているため、この基本的なトラフィックの再ルーティングはOTVトラフィックには機能しません。 OTVルータAの「グリーンインターフェイス」がダウンした場合、OTVトラフィックは代替インターフェイスのOTVルータBから送信できません。また、WANコアを経由した完全な接続がないため、障害が発生したときにすべてのOTVルータに通知できません。 この問題を回避するには、Embedded Event Manager(EEM)スクリプトとともに、双方向フォワーディング検出(BFD)を使用します。

BFDは、東西OTVルータペア（A/CおよびB/D）間のWANリンクを監視する必要があります。リモートルータへの接続が失われた場合、OTVオーバーレイインターフェイスは、その東西OTVルータペア上のEEMスクリプトによってシャットダウンされます。 これにより、ペアになったマルチホームルータは、すべてのVLANに対して転送を想定します。 BFDがリンクの回復を検出すると、EEMスクリプトがトリガーして、オーバーレイインターフェイスが再度有効になります。

リンク障害を検出するには、BFDを使用することが非常に重要です。 これは、オーバーレイインターフェイスを「障害が発生した」側とイーストウェストペアの両方でシャットダウンする必要があるためです。 サービスプロバイダーが提供する接続のタイプによって異なりますが、1つの物理リンク（OTVルータAでは緑色のインターフェイス）がダウンしても、対応するeast-westペアルータのインターフェイス（OTVルータCでは緑色のインターフェイス）はアップ状態のままです。BFDは、インターフェイスの障害または転送中の他の問題を検出し、両方のペアに同時に通知します。 ルータにリカバリリンクを通知する必要がある場合も同様です。

この導入の設定は他の導入と同じですが、次の項目が追加されています。

- WANインターフェイスでのBFD設定

- 後続のEEMスクリプト
- 偶数/奇数のVLANディストリビューションに一致するOTV ISIS ID

OTV参加インターフェイスでのBFDの設定は、このドキュメントの範囲外です。 ASR1000でBFDを設定する方法については、次を参照してください。

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/xe-3s/irb-xe-3s-book.html

Joinインターフェイスペア（図中の緑色のリンク）間でBFD障害検出が正しく動作したら、EEMスクリプトを導入する必要があります。 EEMスクリプトを特定のルータに合わせて調整し、正しいオーバーレイインターフェイスを変更する必要があります。また、BFD障害と回復を監視して、ログ内のより正確な文字列を確認する必要もあります。

```
event manager environment _OverlayInt Overlay1
!
event manager applet WatchBFDdown
description "Monitors BFD status, if it goes down, bring OVERLAY int down"
event syslog pattern "BFD peer down notified" period 1
action 1.0 cli command "enable"
action 2.0 cli command "config t"
action 2.1 syslog msg "EEM: WatchBFDdown will shut int $_OverlayInt"
action 3.0 cli command "interface $_OverlayInt"
action 4.0 cli command "shutdown"
action 5.0 syslog msg "EEM WatchBFDdown COMPLETE ..."
!
event manager applet WatchBFDup
description "Monitors BFD status, if it goes up, bring OVERLAY int up"
event syslog pattern "new adjacency" period 1
action 1.0 cli command "enable"
action 2.0 cli command "config t"
action 2.1 syslog msg "EEM: WatchBFDup bringing up int $_OverlayInt"
action 3.0 cli command "interface $_OverlayInt"
action 4.0 cli command "no shutdown"
action 5.0 syslog msg "EEM WatchBFDup COMPLETE ..."
!
```

また、このタイプの導入では、奇数番目と偶数番目のVLANの転送において、東西のルータペア（A/CおよびB/D）が一致している必要があります。

たとえば、定常状態の公称動作では、AとCは偶数のVLANを転送し、BとDは奇数のVLANを転送する必要があります。

奇数/偶数の配分はOTVの序数によって決まります。この序数は「show otv site」コマンドで確認できます。

2つのサイトルータ間の序数は、OTV ISISネットIDに基づいて決定されます。

```
OTV_router_A#show otv site
Site Adjacency Information (Site Bridge-Domain: 99)
```

```
Overlay99 Site-Local Adjacencies (Count: 2)
  Hostname       System ID      Last Change Ordinal    AED Enabled Status
* OTV_router_A   0021.D8D4.F200 19:32:02    0          site       overlay
  OTV_router_B   0026.CB0C.E200 19:32:46    1          site       overlay
```

すべてのOTVルータでOTV ISISネットIDを設定する必要がある IDを設定するときは、すべてのOTVルータが引き続き互いを認識するように注意する必要があります。

<#root>

```
OTV router A:
otv isis Site
 net
```

49

.

0001

.

0001

.

0001

.

000a

.

00

```
OTV router B:
otv isis Site
 net
```

49

.

0001

.

0001

.

0001

.

000b

.

00

```
OTV router C:
otv isis Site
 net
```

49

.

0001

.

0001

.

0001

.

000c

.

00

```
OTV router
```

```
      D:
otv isis Site
 net
```

49

.

0001

.

0001

.

0001

.

000d

.

00

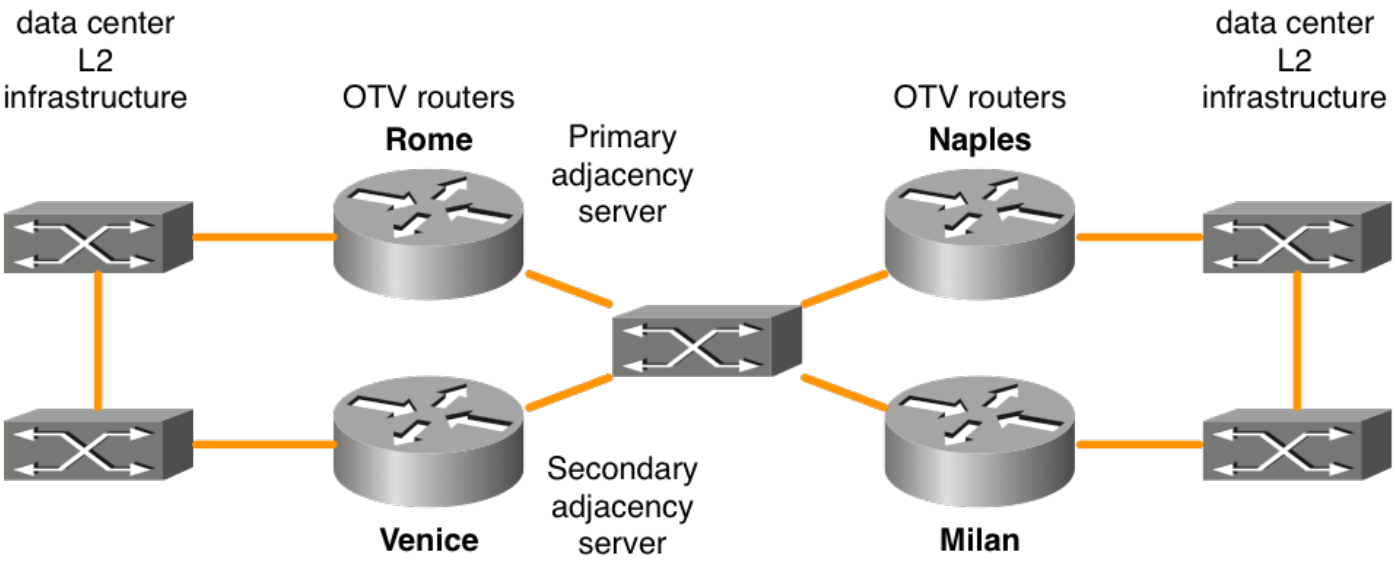
黒の識別子の部分は、オーバーレイに参加するすべてのOTVルータで一致する必要があります。 赤色の識別子の部分は変更できます。 サイトで最小のネットワークIDは序数0を取得し、次に偶数のVLANを取得します。 サイトの最大のネットワークIDは序数1を取得し、奇数のVLANを転送

します。

設定例

ユニキャスト

図 9.ユニキャストの設定例



Romeの設定：

```
!
hostname Rome
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0001
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet1/0/0
 otv adjacency-server unicast-only
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
interface GigabitEthernet1/0/0
 ip address 172.16.0.1 255.255.255.0
 negotiation auto
 cdp enable
```

```
!
interface GigabitEthernet1/0/1
 no ip address
 negotiation auto
 cdp enable
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
```

Venice設定：

```
!
hostname Venice
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0001
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet0/0/0
 otv adjacency-server unicast-only
 otv use-adjacency-server 172.16.0.1 unicast-only
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet0/0/0
 ip address 172.16.0.2 255.255.255.0
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 cdp enable
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
```

```
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
```

Naples設定：

```
!
hostname Naples
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0002
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet0/0/0
 otv use-adjacency-server 172.16.0.1 172.16.0.2 unicast-only
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet0/0/0
 ip address 172.16.0.3 255.255.255.0
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 cdp enable
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
```

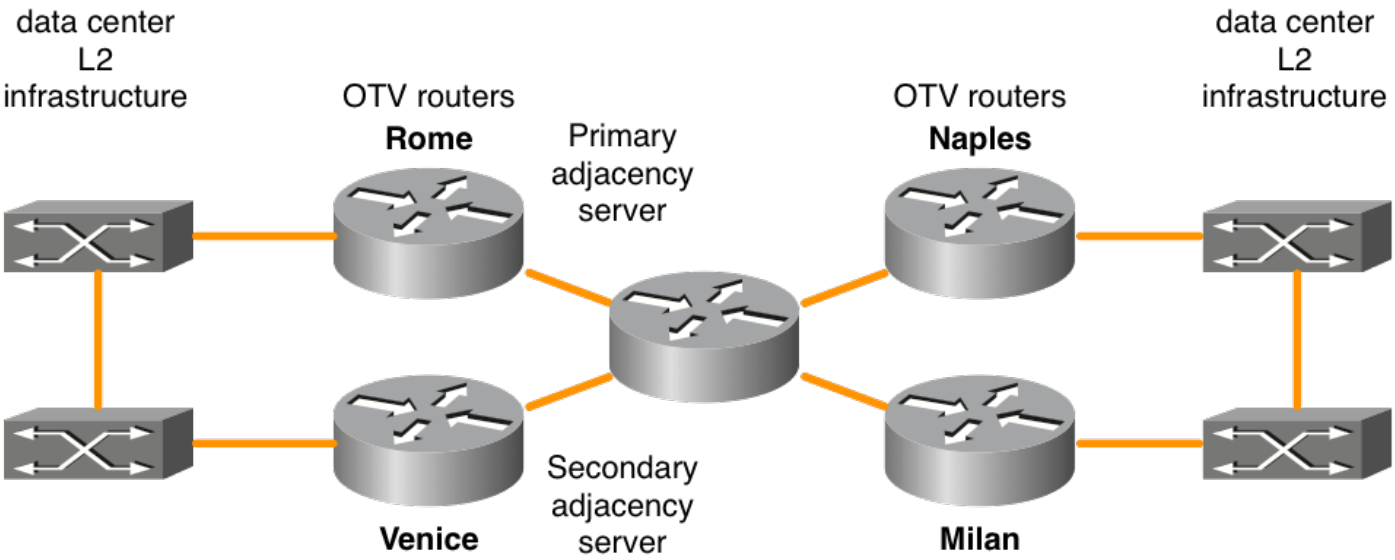
```
!
```

Milanの設定：

```
!
hostname Milan
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0002
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet0/0/0
 otv use-adjacency-server 172.16.0.1 172.16.0.2 unicast-only
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet0/0/0
 ip address 172.16.0.4 255.255.255.0
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 cdp enable
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
```

マルチキャスト

図 10マルチキャストの設定例



Romeの設定：

```
!
hostname Rome
!
ip multicast-routing distributed
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0001
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet1/0/0
 otv control-group 239.0.0.1
 otv data-group 238.1.2.0/24
!
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet1/0/0
 ip address 192.168.0.1 255.255.255.0
 ip pim passive
 ip igmp version 3
 negotiation auto
 cdp enable
!
interface GigabitEthernet1/0/1
```

```
 no ip address
 negotiation auto
 cdp enable
!
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
```

Venice設定：

```
!
hostname Venice
!
ip multicast-routing distributed
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0001
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet0/0/0
 otv control-group 239.0.0.1
 otv data-group 238.1.2.0/24
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet0/0/0
 ip address 172.17.0.1 255.255.255.0
 ip pim passive
 ip igmp version 3
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
```

```
 cdp enable
!
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
```

Naples設定：

```
!
hostname Naples
!
ip multicast-routing distributed
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0002
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet0/0/0
 otv control-group 239.0.0.1
 otv data-group 238.1.2.0/24
!
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet0/0/0
 ip address 172.18.0.1 255.255.255.0
 ip pim passive
 ip igmp version 3
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 cdp enable
 service instance 99 ethernet
```

```
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
```

Milanの設定：

```
!
hostname Milan
!
ip multicast-routing distributed
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0002
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet0/0/0
otv control-group 239.0.0.1
 otv data-group 238.1.2.0/24
!
  service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet0/0/0
 ip address 172.19.0.1 255.255.255.0
 ip pim passive
 ip igmp version 3
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 cdp enable
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
```

```
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
```

よく寄せられる質問（FAQ）

Q)プライベートVLANは、OTVと組み合わせてサポートされますか。

A)はい、OTVでは特別な設定は必要ありません。プライベートVLAN設定では、OTV L2インターフェイスに接続されているスイッチポートが混合モードで設定されていることを確認します。

Q) OTVはIPSEC暗号化でサポートされていますか。

A)はい。joinインターフェイスでのクリプトマップ設定はサポートされています。 OTVで暗号化をサポートするために特別な設定は必要ありません。 ただし、暗号設定では追加のオーバーヘッドが追加されるため、これをLAN MTUに対するWAN MTUの増加によって補正する必要があります。これが不可能な場合は、OTVフラグメンテーションが必要になります。 OTVのパフォーマンスは、IPSECハードウェアのパフォーマンスに制限されます。

Q) OTVはMACSECでサポートされていますか。

A)はい。ASR1001-Xには、組み込みインターフェイスのMACSECサポートが含まれています。OTVは、LANまたはWANインターフェイスで設定されたMACSECと連動します。 OTVのパフォーマンスは、MACSECハードウェアのパフォーマンスに制限されます。

Q)ループバックインターフェイスを結合インターフェイスとして使用できますか。

A)いいえ。OTV加入インターフェイスとして使用できるのは、イーサネット、PortChannel、またはPOSインターフェイスだけです。 OTVループバック参加インターフェイスはロードマップに記載されていますが、現時点ではリリースの予定はありません。

Q)トンネルインターフェイスを結合インターフェイスとして使用できますか。

A)いいえ。GREトンネル、DMVPNトンネル、またはその他のトンネルタイプは、参加インターフェイスとしてサポートされていません。 OTV加入インターフェイスとして使用できるのは、イーサネット、PortChannel、またはPOSインターフェイスだけです。

Q)オーバーレイインターフェイスが異なれば、異なるL2インターフェイスやJoinインターフェイスを使用できますか。

A)すべてのオーバーレイインターフェイスは、同じ結合インターフェイスを指す必要があります。 すべてのオーバーレイは、データセンターへのL2接続のために同じ物理インターフェイスにリンクする必要があります。

Q) OTVサイトVLANをOTV拡張VLANとは異なる物理インターフェイスに設定できますか。

A) OTVサイトのVLANと拡張VLANは、同じ物理インターフェイス上に存在する必要があります。

Q) OTVに必要な機能セットは何ですか。

A) OTVには、Advanced IP Services(AIS)またはAdvanced Enterprise Services(AES)が必要です。

Q)固定構成プラットフォームのOTVには、別途ライセンスが必要ですか。

A)いいえ。ASR1000が事前サービスまたは事前ブートレベルが設定された状態で稼働している限り、OTVは使用できます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。