ガイド

設計およびコンフィギュレーション ガイド：Cisco Nexus 7000 シリーズ スイッチの仮想ポート チャネル（vPC）のベスト プラクティス

改訂：2014 年 8 月

目次

はじめに

このマニュアルでは、Cisco Nexus® 7000 シリーズ スイッチで仮想ポート チャネル（vPC）を使用する場合のベスト プラクティスについて説明します。

このマニュアルは、http://www.cisco.com/en/US/products/ps9402/tsd_products_support_series_home.html にある Cisco Nexus 7000 シリーズのマニュアルと併せて使用してください。

vPC ユーザ ガイドは、次のリンク（CCO）にあります。
http://www.cisco.com/en/US/docs/switches/datacenter/sw/6_x/nx-os/interfaces/configuration/guide/if_vPC.html 。

（vPC のユーザ ガイドは、NX-OS インターフェイス コンフィギュレーション ガイドに格納されています）。

このマニュアルのベスト プラクティスは、一貫したパターンに従っており、各項の情報を容易に検索できます。vPC のベスト プラクティスは、次のように構成されています。

- vPC の説明と用語
- vPC の導入シナリオ
- vPC ドメインを作成するためのベスト プラクティス
- vPC コンポーネントの設定のベスト プラクティス
- 混合シャーシ モード（同じシステムまたは VDC の M1/F1 ポート）での vPC のベスト プラクティス
- vPC ドメインにデバイスを接続するためのベスト プラクティス
- データセンター インターコネクトおよび暗号化のベスト プラクティス
- スパニングツリー プロトコルの相互運用性のベスト プラクティス
- UDLD の相互運用性のベスト プラクティス
- レイヤ 3 および vPC のベスト プラクティス
- HSRP/VRRP と vPC のベスト プラクティス
- ネットワーク サービスと vPC のベスト プラクティス
- マルチキャストおよび vPC のベスト プラクティス
- FEX と vPC のベスト プラクティス
- VDC と vPC のベスト プラクティス

このマニュアルでは、vPC に関する ISSU 動作について説明し、最新の vPC 拡張（オブジェクト トラッキング、ピア ゲートウェイ、ピア スイッチ、リロード復元、遅延の復元、グレースフル タイプ 1 チェック、自動リカバリ、孤立ポートの一時停止、ホスト vPC）に関する詳細を示します。

vPC のスケーラビリティ値は次のリンク（CCO）で公開されています。
http://www.cisco.com/en/US/docs/switches/datacenter/sw/verified_scalability/b_Cisco_Nexus_7000_Series_NX-OS_Verified_Scalability_Guide.html#reference_32EB4DB289634F6FA8885FDFD8E71F5F。

vPC テクノロジーに基づいて、ネットワークを適切に設計するには、これらのスケール番号を考慮してください。

注： このマニュアルでは、次の内容は取り扱いません。

- vPC+（FabricPath のコンテキストで使用する vPC）
- vPC 障害のシナリオ

vPC の説明と用語

vPC の利点

vPC は、レイヤ デバイスまたはエンドポイントにアクセスするための一意のレイヤ 2 論理ノードとして両方の Cisco Nexus 7000 シリーズのペア デバイスを示す仮想化テクノロジーです。vPC は、マルチシャーシ EtherChannel [MCEC] ファミリのテクノロジーに属します。

仮想ポート チャネル（vPC）は、物理的には 2 台の異なる Cisco Nexus 7000 シリーズ デバイスに接続されているリンクを、第 3 のデバイスには単一のポートに見えるようにします。第 3 のデバイスは、スイッチ、サーバ、リンク集約テクノロジーをサポートするその他の任意のネットワーキング デバイスのいずれでもかまいません。

vPC には次の技術的な利点があります。

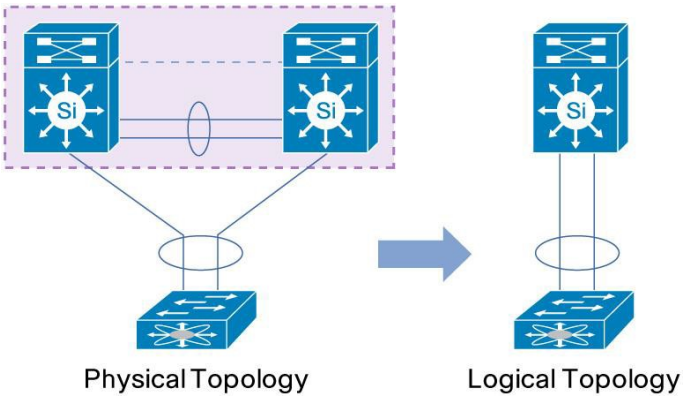
- スパニングツリー プロトコル（STP）のブロック ポートが不要になります
- 利用可能なすべてのアップリンク帯域幅を使用します
- デュアルホーム接続サーバがアクティブ - アクティブ モードで動作できるようになります
- リンクまたはデバイス障害の発生時に高速コンバージェンスを実行します
- サーバのデュアル アクティブ/アクティブ デフォルト ゲートウェイを提供します

vPC は、ポート チャネリング テクノロジーによって提供されるネイティブ スプリット ホライズン/ループ管理も利用します。ポート チャネルに入るパケットは、同じポート チャネルをすぐには出ることはできません。

vPC を使用すると、ユーザは運用上およびアーキテクチャ上の利点を即座に得られます。

- ネットワーク設計を簡素化します
- 復元性が高い、堅牢なレイヤ 2 ネットワークを構築します
- シームレスな仮想マシンのモビリティとサーバのハイ アベイラビリティ クラスタを実現できます
- バイセクショナルな帯域幅を追加して使用可能なレイヤ 2 帯域幅を拡張します
- レイヤ 2 ネットワークのサイズを大きくします

図 1. vPC（仮想ポート チャネル）テクノロジーによる単一の論理ノードの作成



vPC はハードウェアおよびソフトウェアの両方の冗長性を利用します。

- vPC は、個々のリンクが失敗した場合にハッシュ アルゴリズムがすべてのフローを残りのリンクへリダイレクトするために、使用可能なすべてのポート チャネル メンバー リンクを使用します。
- vPC ドメインは、2 台のピア デバイスで構成されます。各ピア デバイスはアクセス レイヤから発信されるトラフィックの半分を処理します。ピア デバイスが故障した場合、もう一方のピア デバイスはコンバージェンス時間の影響を最小限にしてすべてのトラフィックを取り込みます。
- vPC ドメインの各ピア デバイスは独自のコントロール プレーンを実行し、両方のデバイスは独立して動作します。どの潜在的なコントロール プレーンに関する問題も、ピア デバイスに対してローカルのまま留まり、他のピア デバイスに伝播または影響しません。

スパニングツリーの観点から、vPC は STP によってブロックされたポートを取り除き、すべての使用可能なアップリンク帯域幅を使用します。スパニングツリーはフェールセーフ メカニズムとして使用され、vPC 接続装置の L2 パスを示すものではありません。

vPC ドメイン内では、ユーザは複数の方法でアクセス デバイスを接続できます。ポート チャネルによるアクティブ/アクティブ動作を利用した vPC 接続、スパニングツリーを使用したアクティブ/スタンバイ接続、アクセス デバイスで動作するスパニングツリーを使用しないシングル接続などがあります。

これらの接続設定はすべて完全にサポートされ、次のマニュアルで詳しく説明しています。

vPC の NX-OS バージョン要件

vPC テクノロジーは NX-OS 4.1.3 以降でサポートされます。（つまり NEXUS 7000 プラットフォームの開始以降）。

NX-OS の適切なバージョンは、ラインカード設定（M1、F1、または F2）、シャーシ タイプ（7010、7018、または 7009）、およびファブリック モジュール世代（第 1 世代 FM（46 Gbps/モジュール）または第 2 世代 FM（110 Gbps/モジュール））によって異なります。

推奨されている NX-OS バージョンを確認するには、次の URL を参照してください。
http://www.cisco.com/en/US/docs/switches/datacenter/sw/nx-os/recommended_releases/recommended_nx- os_releases.html。

（Cisco Nexus 7000 シリーズ スイッチの最小推奨 Cisco NX-OS リリース）。

各コード リリースの NX-OS リリース ノートは、次の場所にあります。
http://www.cisco.com/en/US/products/ps9402/prod_release_notes_list.html。

vPC の NX-OS ライセンス要件

vPC 機能は、基本の NX-OS ソフトウェア ライセンスに含まれています。

ホットスタンバイ ルータ プロトコル（HSRP）、仮想ルータ冗長プロトコル（VRRP）、Link Aggregation Control Protocol（LACP）もこの基本ライセンスに含まれています。

Open Shortest Path First（OSPF）プロトコルや Intermediate System-to-Intermediate System（IS-IS）プロトコルなどのレイヤ 3 機能には LAN_ENTERPRISE_SERVICES_PKG ライセンスが必要です。

仮想デバイス コンテキスト（VDC）には LAN_ADVANCED_SERVICES_PKG ライセンスが必要です。

vPC のコンポーネント

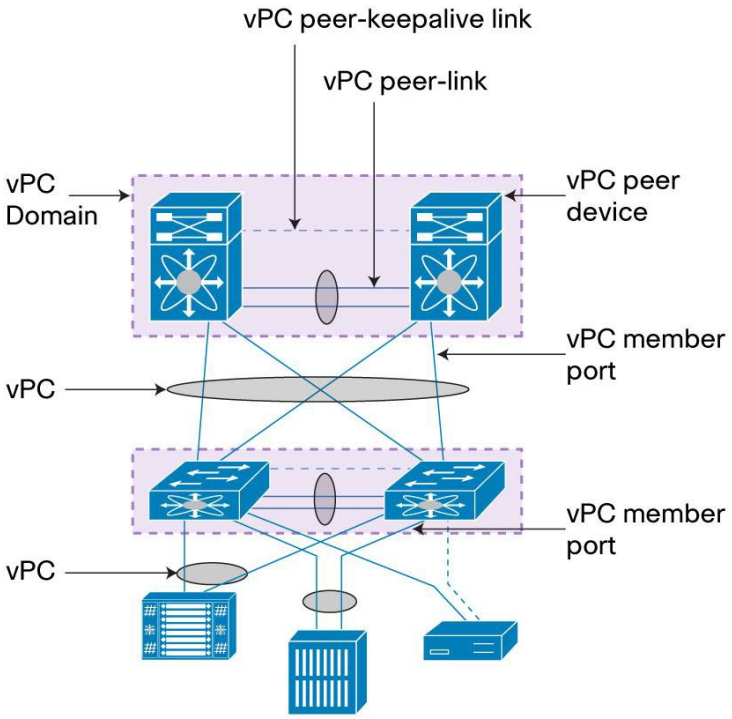
表 1 に、vPC テクノロジーを理解するために知っておく必要がある重要な用語を示します。これらの用語は、このマニュアル全体で使用されます。

表 1. vPC の用語

用語	意味
vPC	vPC ピアとダウンストリーム デバイス間の組み合わせたポート チャネル。 vPC は L2 ポート タイプの 1 つです。switchport mode trunk または switchport mode access のいずれかです。
vPC ピア デバイス	vPC スイッチ（Cisco Nexus 7000 シリーズ ペアの 1 つ）。
vPC ドメイン	2 台のピア デバイスを含むドメイン。 最大 2 台のピア デバイスを同じ vPC ドメインの一部にすることができます。
vPC メンバー ポート	vPC（または vPC のポート チャネル メンバー）を構成する一連のポート（ポート チャネル）の 1 つ。
vPC ピア リンク	vPC ピア デバイス間で状態を同期するために使用されるリンク。これは 10 ギガビット イーサネット リンクである必要があります。vPC ピア リンクは、vPC VLAN を伝送する L2 トランクです。
vPC ピア キープアライブ リンク	vPC ピア デバイス間のキープアライブ リンク。このリンクがピア デバイスの状態をモニタするために使用されます。
vPC VLAN	VLAN が vPC ピア リンクを引き継ぎ、vPC 経由で第 3 のデバイスと通信するために使用されます。 VLAN は、vPC ピア リンクで定義されるとすぐに、vPC VLAN になります
非 vPC VLAN	任意の vPC の一部**ではなく**、vPC ピア リンク上に存在しない VLAN。
孤立ポート	シングル接続デバイスに属するポート。 vPC VLAN がこのポートで通常使用されます。
Cisco Fabric Services（CFS）プロトコル	2 個のピア デバイス間に信頼性の高い同期および整合性検査のメカニズムを提供する vPC ピア リンク上で動作する基本プロトコル。

図 2 は、vPC のさまざまなコンポーネントおよびその関係を示します。

図 2. vPC コンポーネント



vPC ピア リンクおよび vPC ピア キープアライブ リンクを構築するベスト プラクティスは、「vPC ドメインを作成するためのベスト プラクティス」に説明されています。

vPC ドメインに孤立ポートを接続するための推奨事項は、「vPC ドメインにデバイスを接続するためのベスト プラクティス」に記載されています。

vPC のデータ プレーン ループの回避

vPC では、スパニングツリー プロトコルのためのコントロール プレーン レイヤではなくデータ プレーン レイヤでループの回避を実行します。

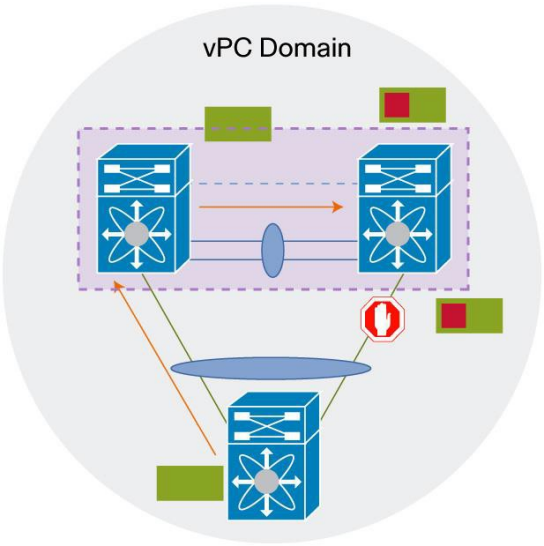
すべてのロジックが vPC ピア リンク ポートのハードウェアに直接実装され、CPU 使用率への依存を回避します。

vPC ピア デバイスは、可能な場合常にトラフィックをローカルに転送します。vPC ピア リンクは、一般にデータ パケットを転送しないため、通常は、定常ネットワークでのコントロール プレーンの拡張と見なされます（MAC アドレス、vPC メンバーの状態情報、IGMP などの情報を 2 個のピア デバイス間で同期するために使用される vPC ピア リンク）。

vPC ループ回避ルールでは、vPC メンバー ポートから発信されて、その後 vPC ピア リンクを通過するトラフィックが vPC メンバー ポートから出ることを許可しないように指定されています。ただし、他のタイプのポート（L3 ポート、孤立ポートなど）から出ることはできます。

このルールの唯一の例外は、vPC メンバー ポートが停止している場合です。vPC ピア デバイスは、メンバー ポート状態を交換し、ハードウェアに特定の vPC の vPC ループ回避ロジックを再プログラミングします。ピア リンクは最適な復元力のためにバックアップ パスとして使用されます。このルールを適用するために、トラフィックを vPC メンバー ポートに入れる必要はありません。vPC ループ回避ルールの例外を下の図に示します。

図 3. vPC ループ回避ルールの例外



vPC の導入シナリオ

vPC は、データセンターのアクセス レイヤまたは集約レイヤで通常使用されます。アクセス レイヤでは、ネットワーク エンドポイント（サーバ、スイッチ、NAS ストレージ デバイス）から vPC ドメインへのアクティブ/アクティブ接続に使用されます。集約レイヤでは、ネットワーク エンドポイントから vPC ドメインへのアクティブ/アクティブ接続と L2/L3 境界のアクティブ/アクティブのデフォルト ゲートウェイの両方に使用されます。

ただし、vPC はループ フリー トポロジを作成する機能を提供しているため、レイヤ 2 で 2 つの個別のデータセンターを相互接続するためにも一般的に使用され、2 つのサイトにわたる VLAN 拡張を可能にします。

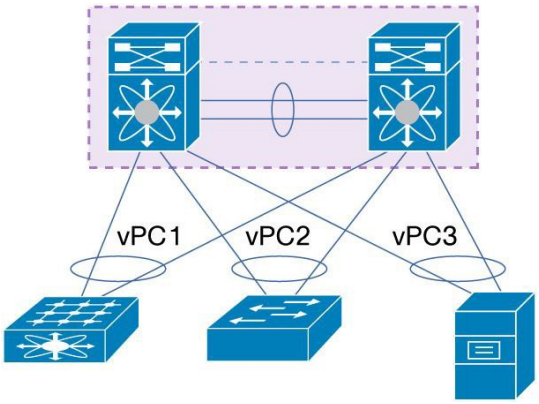
vPC テクノロジーを使用した 2 つの一般的な導入シナリオを次に示します。

- データセンター内:
  - シングルサイド vPC(アクセス レイヤまたは集約レイヤ)
  - マルチレイヤ vPC(vPC を使用するアクセス レイヤと vPC を使用する集約レイヤとを相互接続)とも呼ばれるダブルサイド vPC
- データセンター間(つまり、データセンター インターコネクト(DCI)のための vPC):
  - 集約と DCI のためのマルチレイヤ vPC
  - デュアル レイヤ 2/レイヤ 3 のポッド相互接続

シングルサイド vPC

図 4 に、シングルサイド vPC トポロジを示します。シングルサイド vPC では、アクセス デバイスは、vPC ドメインを構成する Cisco Nexus 7000 シリーズ スイッチ ペアに直接デュアル接続されます。

図 4. シングルサイド vPC トポロジ



アクセス デバイスは、エンドポイント装置(L2 スイッチ、ラックマウント サーバ、ブレード サーバ、ファイアウォール、ロード バランサ、Network Attached Storage(NAS)デバイス)にすることができます。アクセス デバイスの唯一の前提条件は、ポートチャネリング(またはリンク集約)テクノロジーのサポートです。

- LACP モード アクティブ
- LACP モード パッシブ
- スタティック バンドリング(モード オン)

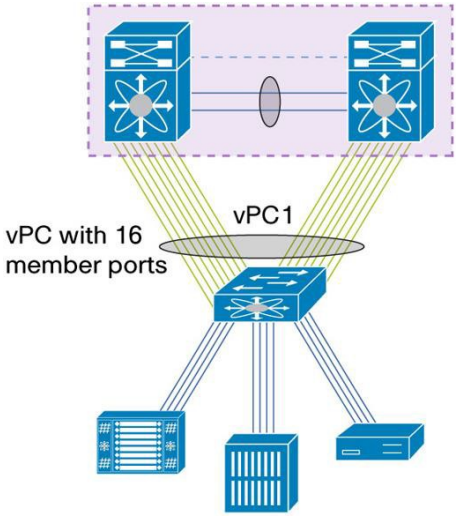
重要な推奨事項:
アクセス デバイスを vPC ドメインに接続する場合は、LACP プロトコルを使用してください。

vPC メンバー ポートに使用するラインカードのタイプに応じて、ポートチャネル メンバー ポートの最大数は 16 から 32 の範囲になります。

- Cisco Nexus M1 シリーズ モジュール ラインカードを搭載した vPC:16 のアクティブなメンバー ポート(ピア デバイス 1 に 8 個、ピア デバイス 2 に 8 個)
- Cisco Nexus F1/F2 シリーズ モジュール ラインカードを搭載した vPC:32 のアクティブなメンバー ポート(ピア デバイス 1 に 16 個、ピア デバイス 2 に 16 個)

Cisco NX-OS Software Release 4.1(3)N1(1a) 以降、Cisco Nexus 5000 シリーズはポート チャネルあたり 16 のアクティブなメンバー ポートをサポートできます。図 5 に示すように、vPC ドメインに Cisco Nexus 5000 シリーズ スイッチを接続することにより、vPC を最大 160 Gbps（16 x 10 Gbps ポート）に拡張できる魅力的なトポロジを提供します。

図 5. シングルサイド vPC トポロジでの 16 方向のポート チャネル



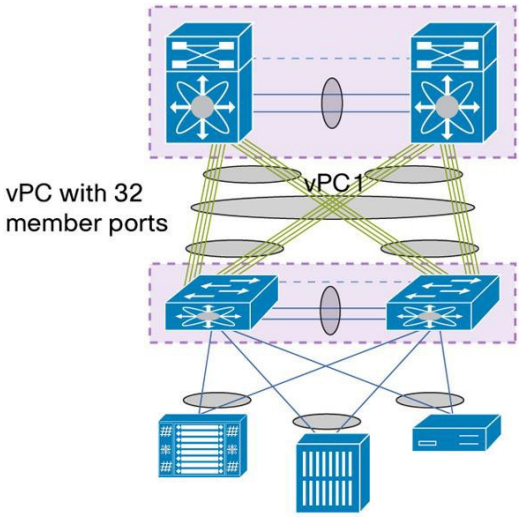
注： 図 4 または 5 で示されていませんが、孤立ポートまたはアクティブ/スタンバイの接続デバイス（つまり、スパニングツリー プロトコルを使用）が、vPC トポロジで完全にサポートされています。

ダブルサイド vPC

図 6 に、ダブルサイド vPC トポロジを示します。このトポロジは、vPC ドメインの 2 層を重ね、vPC ドメイン 1 および vPC ドメイン 2 間のバンドル自体が vPC です。

下部の vPC ドメインはエンドポイント デバイスからネットワーク アクセス レイヤへのアクティブ/アクティブ接続に使用されます。上部の vPC ドメインは L2/L3 境界集約レイヤでアクティブ/アクティブ FHRP に使用されます。

図 6. ダブルサイド vPC トポロジ



シングルサイド vPC トポロジよりも優れたダブルサイド vPC の利点は次のとおりです。

- より大規模なレイヤ 2 ドメインをイネーブルにします。
- より復元力の高いアーキテクチャを実現できます。ダブルサイド vPC では、2 台のアクセス スイッチが 2 台の集約スイッチに接続され、シングルサイド vPC では、1 台のアクセス スイッチが 2 台の集約スイッチに接続されます。
- 集約レイヤへのアクセスからより多くの帯域幅を提供します。vPC と Release 4.1(3) N1(1a) 以降の Cisco Nexus 5000 シリーズ スイッチに Cisco Nexus F1 または F2 シリーズ モジュールのラインカードを使用すると、32 のアクティブなメンバー ポート（つまり、320 Gbps）を使用した vPC をインスタンス化できます。

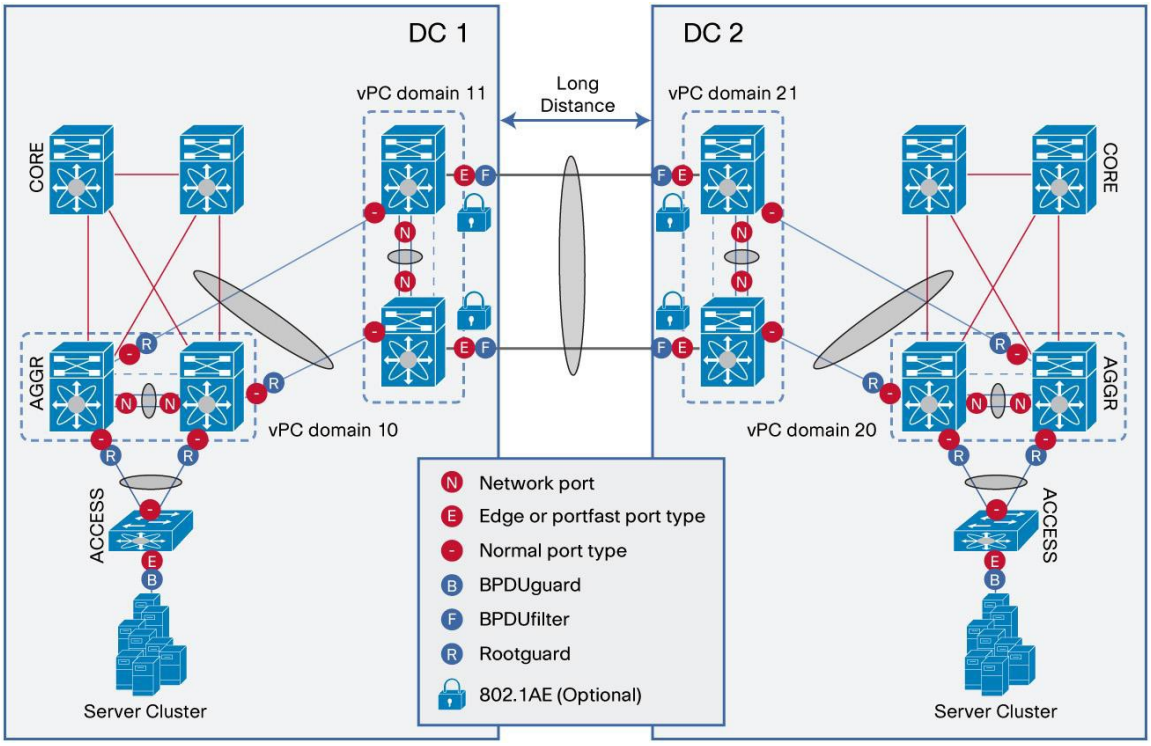
ダブルサイド vPC の設定例は vPC への接続に関する項で説明されています。

集約と DCI のためのマルチレイヤ vPC

vPC はループフリー トポロジを構築する機能を提供し、そのテクノロジーをデータセンター インターコネクト（DCI）の導入に適切に適合させます。このシナリオでは、（vPC も実行する集約レイヤに隣接する）vPC ドメインの専用レイヤが 2 つのデータセンターを相互接続するために使用されます。

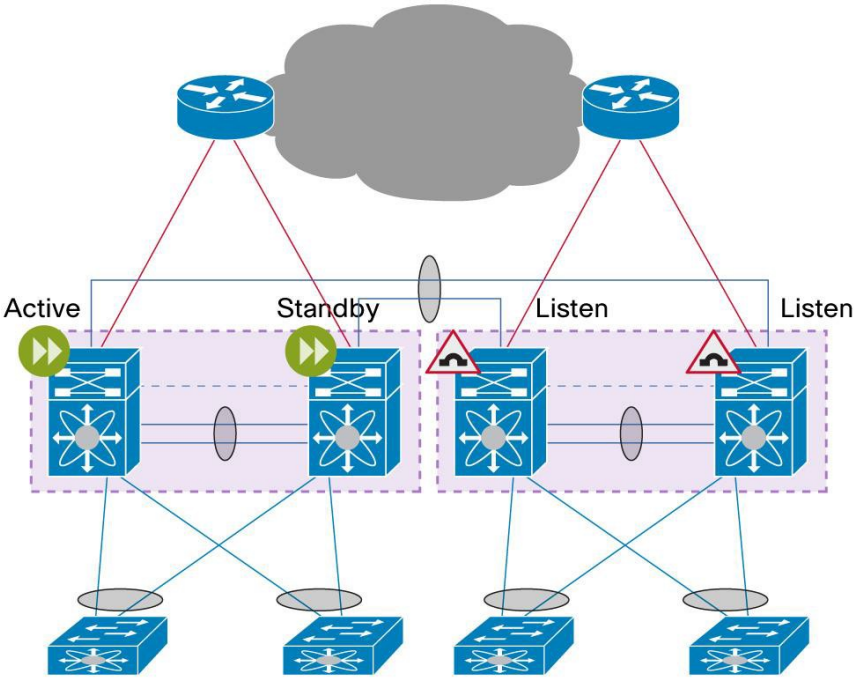
この設計は、図 7 のように集約と DCI のマルチレイヤ vPC と呼ばれます。

図 7. データセンター インターコネクトの vPC：集約と DCI のマルチレイヤ vPC



もう 1 つの設計では、DCI 専用の vPC のレイヤを使用しないで vPC 集約レイヤ間を直接相互接続します。この設計は、デュアル レイヤ 2/レイヤ 3 のポッド相互接続と呼ばれ、図 8 で示します。

図 8. データセンター インターコネクトの vPC：デュアル レイヤ 2/レイヤ 3 のポッド相互接続



DCI テクノロジーとしての vPC は最大の 2 つのデータセンターを相互接続することを目的としています。3 つ以上のデータセンターを相互接続する必要がある場合、推奨事項は Overlay Transport Virtualization（OTV）ソリューションを使用することです。

「データセンター インターコネクトおよび暗号化のベスト プラクティス」の項で DCI テクノロジーとして使用される vPC について説明します。

推奨事項:

最大 2 つのデータセンターを相互接続するには、vPC を使用してください。3 つ以上のデータセンターを相互接続する必要があるときは、OTV を使用してください。

vPC ドメインを作成するためのベスト プラクティス

vPC ドメインの作成

vPC ドメインは、vPC に参加するスイッチのグループを定義します。現時点では、2 台の Cisco Nexus 7000 シリーズ スイッチのみで vPC ドメインを形成できます。

設定の観点からすると、vPC ドメインはグローバルな vPC のシステム パラメータを定義するコンテキストを提供します。

ユーザは、vPC ドメイン サブコマンドを入力してピア ゲートウェイ、ピア スイッチなどの vPC オプションおよび機能を設定します。vPC ドメインの作成プロセスには、次の順序で実行する必要がある複数の手順が必要です。

1. グローバルに両方の vPC デバイスの vPC ドメイン ID を設定します。ドメイン ID は両方のピア デバイスで同じである必要があります。
2. 両方のピア デバイスの vPC ピア キープアライブ リンクを設定し、vPC ピア キープアライブ リンクが動作していることを確認します。そうでない場合は、vPC ドメインは正しく形成できません。

3. vPC ピア デバイス間の ISL（Inter Switch Link）L2 トランク ポート チャネルを設定したり、再利用します。ポート チャネルを両方のピア デバイスの vPC ピア リンクとして設定し、ポート チャネルが動作していることを確認します。
4. アクセス デバイスから vPC ドメインを構成する Cisco Nexus 7000 シリーズへのポート チャネルを設定したり、再利用します。その後、一意の論理 vPC を設定して、異なる複数の vPC ピア デバイスのポートチャネルに参加します。

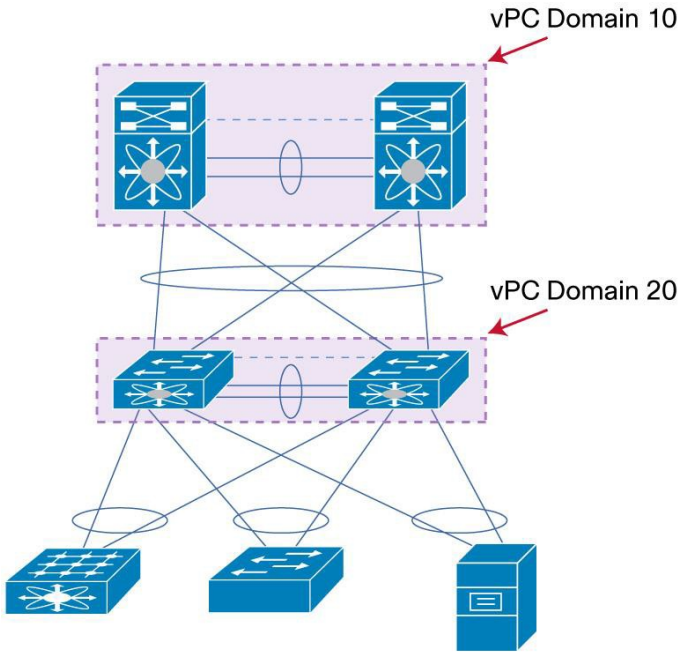
vPC ドメイン ID

vPC ドメイン ID はコマンド **vpc domain <domain-id>** によって定義されます。

これは、2 台のピア デバイスで同じでなければなりません。

場合によっては、vPC ドメイン ID を慎重に設定する必要があります。一般的なケースは、Cisco Nexus 5000 vPC レイヤが vPC を使用して Cisco Nexus 7000 vPC レイヤに接続されているダブルサイド vPC トポロジ（図 9）を扱います。このシナリオでは、vPC ドメイン ID はこの情報が LACP プロトコルの一部として使用されるため、両方のレイヤで異なっている**必要があります**。同じ vPC ドメイン ID を使用すると、NEXUS 7000 に NEXUS 5000 を相互接続する vPC に継続的なフラップが生成されます。

図 9. ダブルサイド vPC トポロジの別の vPC ドメイン ID の使用



DCI の目的で vPC を使用する場合は、vPC ドメイン ID は、2 つのデータセンター全体にわたって異なっている**必要があります**（前と同じ理由で、LACP プロトコルの一部として vPC ドメイン ID が使用されます）。

ユーザが両方の vPC ドメインに同じドメイン ID を使用する必要がある場合は、ノブ **system-mac** を（vPC ドメイン設定コンテキストで）使用して異なる vPC システム MAC 値を強制的に使用する必要があります。

必須の推奨事項:
ダブルサイド vPC トポロジと DCI トポロジの vPC では、常に異なるドメイン ID を使用してください。

vPC システム Mac および vPC ローカル システム Mac

設定されると、両方のピア デバイスが後で定義されているとおりに、一意の vPC システム MAC アドレスを自動的に割り当てるために vPC ドメイン ID を使用します。

```
vPC system-mac = 00:23:04:ee:be:<vpc domain-id in hexadecimal>
```

たとえば、vPC ドメイン 10 は 00:23:04:ee:be:0a の vPC システム MAC になります。

vPC システム MAC は両方のピア デバイス上で同じです。これは、vPC を使用した L2 仮想化方式の基礎になります。vPC システムが一意の論理デバイスとして自身を示す必要がある場合、2 台のピア デバイスでこの一意の共有情報を使用します。

注： vPC ドメイン設定コンテキスト内でコマンド **system-mac** を使用して vPC システム MAC 値を手動で設定できます。

vPC ローカル システム MAC は各ピア デバイスによって所有されるため、デバイスごとに一意です。vPC ローカル システム MAC は、システムまたは VDC MAC アドレス（show vdc コマンドで表示）から取得されます。vPC ローカル システム MAC は、vPC システムが一意の論理デバイスとして自身を示す必要がない場合に使用されます。たとえば、孤立ポートの場合です。

vPC ドメイン ID、vPC システム MAC、および vPC ローカル システム MAC を可視化するための show コマンドは、**show vpc** と **show vpc role** です。

これらのコマンドの出力例を次に示します。

```
APULIA-2-VPC_AGG2# sh vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Type-2 consistency status         : success
Type-2 consistency reason         : success
vPC role                          : secondary
Number of vPCs configured         : 6
Track object                      : 1
Peer Gateway                      : Enabled
Dual-active excluded VLANs        : -

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po10   up     1-20,23-24,40,50,100,200,300,400-401,501,600,1000-1100

vPC status
----------------------------------------------------------------------------
id   Port   Status Consistency Reason                Active vlans
--   ----   ------ ----------- ------                ------------
1    Po1    up     success     success               1000-1100
<省略>
```

```
APULIA-2-VPC_AGG2# sh vpc role

vPC Role status
----------------------------------------------------
vPC role                                : secondary
Dual Active Detection Status            : 0
vPC system-mac                          : 00:23:04:ee:be:0a
vPC system-priority                     : 32667
vPC local system-mac                    : 00:22:55:79:aa:c2
vPC local role-priority                 : 65534
```

vPC ローカル システム MAC がシステムや VDC MAC アドレスから取得されることを確認します。

```
APULIA-2-VPC AGG2# sh vdc

vdc_id  vdc_name             state          mac                        lc
------  ---------------      ---          ----------                 ------
2       VPC_AGG2             active       00:22:55:79:aa:c2    m1 f1 m1xl
```

vPC システム MAC と vPC ローカル システム MAC の両方が LACP システム ID として LACP プロトコルで使用されます。

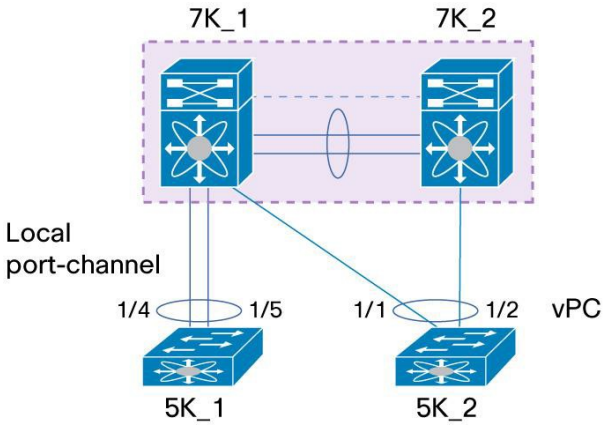
ただし、vPC システム MAC は vPC 接続アクセス デバイスでのみ使用され、vPC ローカル システム MAC はシングル接続デバイス（STP の有無を問わず孤立ポートまたはアクティブ/スタンバイ）によって使用されます。

vPC システム MAC と vPC ローカル システム MAC の使用方法を図 10 に示します。

この図では、Cisco Nexus 5000 シリーズ デバイス 1（5K_1）は、Cisco Nexus 7000 シリーズ デバイス 1（7K_1）とのローカル ポート チャネルを形成しています。その結果、7K_1 は vPC ローカル システム MAC を使用して 5K_1 と LACP 情報を交換します。

その一方で、Cisco Nexus 5000 シリーズ デバイス 2（5K_2）は、Cisco Nexus 7000 シリーズ デバイス 1（7K_1）および Cisco Nexus 7000 シリーズ デバイス 2（7K_2）を使用して vPC を形成しています。その結果、7K_1 および 7K_2 は両方とも共通の vPC システム MAC を使用して 5K_2 と LACP 情報を交換します。

図 10. vPC システム MAC および vPC ローカル システム MAC の使用



5K_1 で **show lacp neighbor** を実行すると、7K_1 で使用されている LACP システム ID（vPC ローカル システム MAC）が表示されます。

```
5K_1# sh lacp neighbor interface port-channel 1
Flags:  S - Device is sending Slow LACPDUs F - Device is sending Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode
port-channel1 neighbors
Partner's information
                Partner                   Partner
   Partner
Port            System ID                 Port Number         Age         Flags
Eth1/4      32667, 0-22-55-79-ab-42       0x4206              18999       SA

  LACP Partner                      Partner                   Partner
  Port Priority                     Oper Key                   Port State
  32768                             0x8001                    0x3d

Partner's information
                Partner                          Partner
   Partner
Port            System ID           Port Number         Age         Flags
Eth1/5      32667,0-22-55-79-ab-42   0x4208              18999       SA

LACP Partner                  Partner                   Partner
Port Priority                Oper Key                   Port State
32768                        0x8001                     0x3d
```

5K_2 で **show lacp neighbor** を実行すると、7K_1 と 7K_2 で使用されている LACP システム ID（共通の vPC システム MAC）が表示されます。

```
5K 2# sh lacp neighbor interface port-channel 1
Flags:  S - Device is sending Slow LACPDUs F - Device is sending Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode
port-channel1 neighbors
Partner's information
         Partner             Partner                   Partner
Port            System ID                 Port Number         Age         Flags
Eth1/1      32667,0-23-4-ee-be-a          0x4206              18999       SA


    LACP Partner                    Partner                    Partner
    Port Priority                   Oper Key                   Port State
    32768                           0x8001                     0x3d
Partner's information
   Partner                   Partner                   Partner
```

```
Port            System ID                  Port Number         Age         Flags
Eth1/2      32667,0-23-4-ee-be-a           0x4208              18999       SA

 LACP Partner                Partner                   Partner
 Port Priority               Oper Key                  Port State
 32768                       0x8001                     0x3d
```

vPC ロール

定義された vPC ロールには、プライマリとセカンダリの 2 種類があります。
vPC ロールは、2 つの vPC ピア デバイスのうちどちらがブリッジ プロトコル データ ユニット（BPDU）を処理し、アドレス解決プロトコル（ARP）に応答するかを定義します。

専用ピア デバイスのプライマリに vPC ロールを強制するには、**role priority <value>** コマンドを（vPC ドメイン設定コンテキストで）使用します。

<value> の範囲は 1～65535 で、最小値はプライマリ ピア デバイスを示します。

値が同じ（両方のピア デバイスに定義されているロール プライオリティ値が同じ）場合、最も小さいシステム MAC がプライマリ ピア デバイスを示します。

2 台のピア デバイスのどちらがプライマリまたはセカンダリであるかを確認するには、**show vpc role** コマンドを使用します。

```
APULIA-1-VPC_AGG1# sh vpc role

vPC Role status
----------------------------------------------------
vPC role                                : primary
Dual Active Detection Status            : 0
vPC system-mac                          : 00:23:04:ee:be:0a
vPC system-priority                     : 32667
vPC local system-mac                    : 00:22:55:79:ab:42
vPC local role-priority                 : 2
```

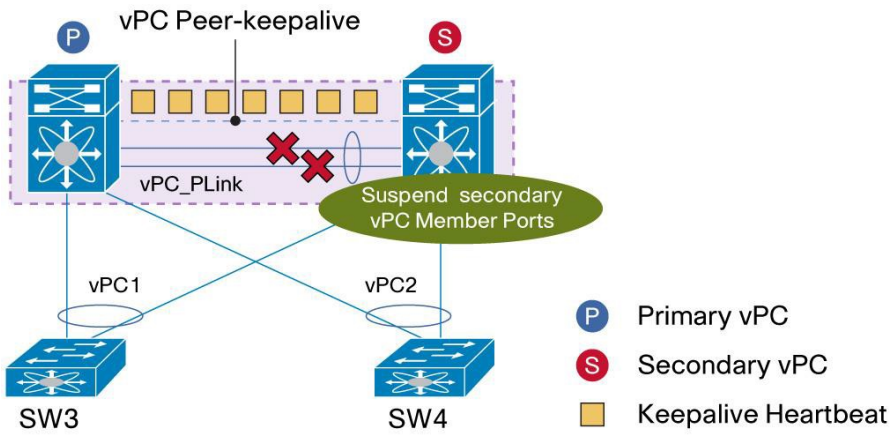
```
APULIA-2-VPC_AGG2# sh vpc role

vPC Role status
----------------------------------------------------
vPC role                                : secondary
Dual Active Detection Status            : 0
vPC system-mac                          : 00:23:04:ee:be:0a
vPC system-priority                     : 32667
vPC local system-mac                    : 00:22:55:79:aa:c2
vPC local role-priority                 : 65534
```

一般的な推奨事項:

操作を簡易化するために、左側の Nexus 7000 シリーズ デバイスで vPC プライマリ ピア デバイスを定義します。右側の Nexus 7000 シリーズ デバイスで vPC セカンダリ ピア デバイスを定義します。

vPC ロール(プライマリまたはセカンダリ)は、ピア リンク障害の発生時の動作に重要です。図 11 で説明するように、ピア リンクに障害が発生すると、セカンダリ ピア デバイスだけが vPC メンバー ポートをダウン状態にし、さらにすべての vPC VLAN インターフェイス(または SVI - スイッチ仮想インターフェイス(vPC VLAN に関連付けられた SVI))をシャットダウンします。

図 11. vPC ピア リンク障害:セカンダリ ピア デバイス上の動作



vPC は、動作可能ロールの概念を追加しています。それは、動作可能なプライマリおよび動作可能なセカンダリです。

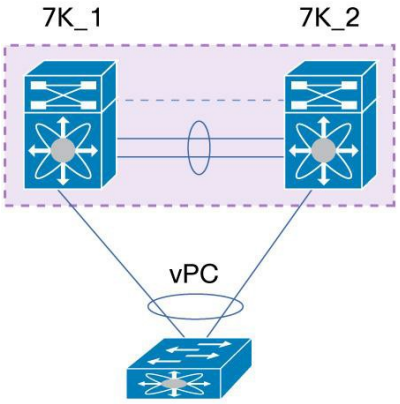
プライマリまたはセカンダリ vPC ロールは role priority コマンドを使用して CLI 設定によって決まります。

vPC の動作可能なプライマリ ロールまたは動作可能なセカンダリ ロールは、ピア デバイスのリアルタイムの動作により機能します。

vPC ドメインが起動すると、vPC ロールは、vPC の動作可能ロールに常に等しくなります。ただし、ネットワークが稼働中で動作イベントが発生した場合、動作可能ロールは元の vPC ロールと異なることがあります。

次のシーケンスは、vPC ロールと vPC 動作可能ロール間の相違を示します。

図 12. vPC ロールおよび vPC 動作可能ロール



イベント 1: vPC デバイスの電源投入	7K_1: vPC ロール = プライマリ	7K_2: vPC = セカンダリ
イベント 2: 7K_1 がリロード、回復	7K_1: vPC ロール = プライマリ、動作可能なセカンダリ	7K_2: vPC ロール = セカンダリ、動作可能なプライマリ
イベント 3: 7K_2 がリロード、回復	7K_1: vPC ロール = プライマリ	7K_2: vPC ロール = セカンダリ

vPC ロールはプリエンプティブではないため、vPC の動作可能ロールは 2 情報の中で最も関連性があります。

注: vPC ピア デバイスの動作可能なプライマリ ロールを手動でプリエンプション処理するには、管理者が次の手順を実行する必要があります。動作可能なプライマリ ロールに変更するピア デバイスにログインし、他のピア デバイスよりも小さい値のロール プライオリティを設定します。その後で、変更を強制するには、vPC ピア リンクをバウンスします（shut を実行してから no shut）。

ピア リンクがダウンすると動作可能なセカンダリ ピア デバイスが vPC メンバー ポートをシャットダウンするため、この操作が中断を伴うことに注意してください。

CLI エイリアス 機能を使用すれば、次のように vPC 動作可能ロールを変更するコマンド シーケンスを自動化できます。
cli alias name vpcpreempt conf t; vpc domain 1; role priority 1; int po 1; shut; no sh

Cisco Fabric Services（CFS）プロトコル

Cisco Fabric Services（CFS）プロトコルは、2 台のピア デバイス間に信頼性の高い同期および整合性検査のメカニズムを提供し、vPC ピア リンク上で動作します。プロトコルは、最初は MDS 製品（ネットワーク ストレージ デバイス）に実装されていましたが、NEXUS 7000 に移植されました。

Cisco Fabric Services（CFS）プロトコルは、次の機能を実行します。

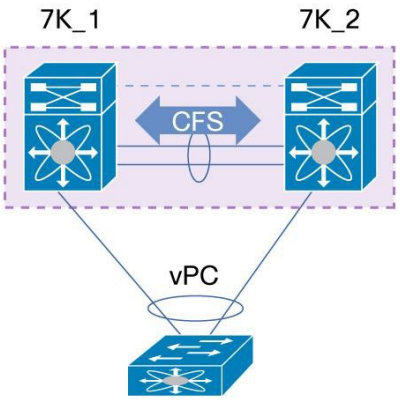
- 設定の確認と比較（整合性検査）
- vPC メンバー ポートの MAC アドレスの同期
- vPC メンバー ポートのステータスのアドバタイズメント
- スパニングツリー プロトコルの管理
- HSRP および IGMP スヌーピングの同期

Cisco Fabric Services は vPC 機能がオンになっていると、デフォルトでイネーブルになります。

実装する特定の Cisco Fabric Services 設定はありません。図 13 は、vPC ドメイン内の Cisco Fabric Service メッセージ パスを示します。

Cisco Fabric Services メッセージは、ピア リンクのピア間で排他的に提供される標準イーサネット フレームにカプセル化されます。Cisco Fabric Services メッセージには、信頼できる通信のために CoS 値 = 4 がタグ付けされます。

図 13. vPC ドメインの CFS メッセージ パス



Cisco Fabric Services アプリケーションの vPC と Cisco Fabric Service のステータスを確認するには、次のように **show cfs application** コマンドおよび **show cfs status** コマンドを使用します。

```
7K1# sh cfs application
----------------------------------------------------------------
Application     Enabled   Scope
----------------------------------------------------------------

arp             Yes       Physical-eth
pim             Yes       Physical-eth
stp             Yes       Physical-eth
vpc             Yes       Physical-eth
igmp            Yes       Physical-eth
l2fm            Yes       Physical-eth
```

```
7K1# sh cfs status
Distribution: Enabled
Distribution over IP: Disabled
IPv4 multicast address: 239.255.70.83
IPv6 multicast address: ff15::efff:4653
Distribution over Ethernet: Enabled
```

vPC ドメインを構築する場合の vPC 設定の整合性検査

ここでは、vPC ドメインを構築する際に互換性のないパラメータがないことを確認するのに役立つ推奨事項について説明します。

vPC ドメインの両方のスイッチは、個別のコントロール プレーンを維持します。Cisco Fabric Services プロトコルは、両方のピア（MAC アドレス テーブル、インターネット グループ管理プロトコル（IGMP）ステート、vPC ステートなど）間のステート同期を処理します。

システム設定の同期を維持する必要があります。現在これは手動のプロセス（設定はデバイスごとに個別にされます）で、正しいネットワーク動作を保証するための整合性検査は自動化されています。

2 種類の整合性検査があります。

- タイプ 1:ピア デバイスまたはインターフェイスを一時停止ステートにして、無効なパケットの転送動作を防ぎます。vPC のグレースフル整合性検査によって、一時停止はセカンダリ ピア デバイスでのみ発生します。
- タイプ 2:ピア デバイスまたはインターフェイスは、引き続きトラフィックを転送します。ただし、これらは望ましくないパケット転送動作の対象になります。

タイプ 1 およびタイプ 2 の整合性検査は、グローバル コンフィギュレーションと vPC インターフェイス コンフィギュレーションの両方に適用されます。

同じにする必要がある設定パラメータ(タイプ 1 整合性検査)

vPC 機能をイネーブルにし、両方のピア デバイスで vPC ピア リンクを設定すると、Cisco Fabric Service メッセージは、リモート vPC ピア デバイスにローカル vPC ピア デバイスの設定のコピーを提供します。これにより、システムが 2 つのデバイス上で異なっている重要な設定パラメータがないか調べます。

多くのグローバル コンフィギュレーション パラメータはおよび同じ vPC ドメイン内の vPC インターフェイス パラメータは同じにする必要があります。

デバイスは互換性を自動的にチェックします。インターフェイス別のパラメータはインターフェイスごとに整合性を保っていることが必要であり、グローバル パラメータはグローバルに整合性を保っていることが必要です。

タイプ 1 不一致チェックが検出されると、抜本的なアクションが実行されます。

グローバル コンフィギュレーションのタイプ 1 不一致チェックについては、すべての vPC メンバー ポートがダウン状態に設定されます。

vPC インターフェイス コンフィギュレーションのタイプ 1 不一致チェックについては、誤って設定された vPC がダウン状態に設定されます。

NX-OS バージョン 5.2 以降、タイプ 1 整合性検査に対する vPC システムの反応を穏やかにするために、グレースフル整合性検査が導入されました。

グローバル コンフィギュレーションのタイプ 1 不一致チェックについては、セカンダリ ピア デバイスの vPC メンバー ポートのみがダウン状態に設定されます。

vPC インターフェイス コンフィギュレーションのタイプ 1 不一致チェックについては、セカンダリ ピア デバイスの vPC メンバー ポートがダウンの状態に設定されます。

グローバル コンフィギュレーション値と vPC インターフェイス パラメータを表示するには、**show vpc consistency-parameters** コマンドを入力します。表示される出力は、vPC の稼働を制限する設定だけです。

表 2 に、タイプ 1 整合性検査で考慮するグローバル コンフィギュレーション パラメータを示します。

表 2. グローバル コンフィギュレーションのタイプ 1 整合性検査

Parameter Name	値
スパニング ツリー プロトコル(STP)モード	RPVST(Rapid Per LAN Spanning Tree)または MST(マルチ スパニングツリー)
各 VLAN の STP イネーブル/ディセーブル ステート	Yes または No
マルチ スパニングツリーの STP 領域コンフィギュレーション(MST)	リージョン名、リージョン リビジョン、VLAN マッピングへのリージョン インスタンス
STP グローバル設定	ブリッジ保証設定 ポート タイプの設定 ループ ガードの設定 BPDU フィルタの設定 MST Simulate PVST のイネーブルまたはディセーブル

show vpc consistency-parameters global コマンドを実行すると、グローバルなタイプ 1 整合性検査パラメータが表示されます。

出力例を次に示します。

```
7K1# sh vpc consistency-parameters global

Legend:
        Type 1: vPC will be suspended in case of mismatch

Name                          Type   Local Valu                Peer Value
-------------                 ----   ----------------------    ------------
STP Mode                      1      Rapid PVST                Rapid PVST
STP Disabled                  1      None                      None
STP MST Region Name           1      ""                        ""
STP MST Region Revision       1      0                         0
STP MST Region Instance to    1
 VLAN Mapping
STP Loopguard                 1      Disabled                  Disabled
STP Bridge Assurance          1      Enabled                   Enabled
STP Port Type、Edge           1      Normal, Disabled,         Normal, Disabled,
BPDUFilter、Edge BPDUGuard           Disabled                  Disabled
STP MST Simulate PVST         1      Enabled                   Enabled
interface-vlan admin up       2      200,3966-3967             200,3966-3967
Interface-vlan routing        2      1,40,200,3966-3967        1,40,200,3966-3967
capability

Allowed VLANs                 -      1-20,23-24,40,50,100,2    1-20,23-
                                                               24,40,50,100,2
                                     00,300,501,600,1000-11
                                     00,300,501,600,1000-11
                                     00,2015,3966-3967         00,2015,3966-3967
Local suspended VLANs         -      -                         -
```

表 3 に、タイプ 1 整合性検査で考慮する vPC インターフェイスごとのパラメータを示します。

表 3. vPC インターフェイスごとのタイプ 1 整合性検査

パラメータ	値
ポート チャネルの LACP モード	ON、ACTIVE、PASSIVE
ポート チャネルごとのリンク速度	速度（Mbps 単位）
ポート チャネルごとのデュプレックス モード	半二重または全二重
ポート チャネルごとのスイッチポート モード	トランクまたはアクセス ネイティブ VLAN
STP インターフェイス設定	ポート タイプの設定 ループ ガード ルート ガード
MST Simulate PVST	Enable または Disable
ポート チャネルごとの MTU	最大伝送単位（MTU）値

show vpc consistency-parameters interface port-channel <id> コマンドを実行すると、vPC インターフェイスごとにタイプ 1 整合性検査パラメータが表示されます。

出力例を次に示します。

```
7K1# sh vpc consistency-parameters interface port-channel 80

    Legend:
        Type 1 : vPC will be suspended in case of mismatch

Name                    Type   Local Value                Peer Value
-------------           ----  ---------------------- ------------------------
STP Port Type           1      Default             Default
STP Port Guard          1      None                None
STP MST Simulate PVST   1      Default             Default
lag-id                  1      [(7f9b,             [(7f9b,
                               0-23-4-ee-be-a,8050,  0-23-4-ee-be-a, 8050,
                               0, 0), (8000,         0, 0), (8000,
                               0-22-90-c2-8-3e, 1, 0, 0-22-90-c2-8-3e, 1, 0,
                               0)]                 0)]
mode                    1      active              active
Speed                   1      1000 Mb/s           1000 Mb/s
Duplex                  1      full                full
Port Mode               1      trunk                trunk
Native Vlan             1      1                    1
MTU                     1      1500                1500
Allowed VLANs           -      100,200,300         100,200,300
Local suspended VLANs   -      -                   -
```

同じにする必要がある設定パラメータ（タイプ 2 整合性検査）

タイプ 2 整合性検査が検出されたときは、適切なアクションが実行される場合と何もアクションが実行されない場合があります。グローバル コンフィギュレーションのタイプ 2 整合性検査では、すべての vPC メンバー ポートがアップ ステートのままになり、vPC システムが保護アクションをトリガーします。

vPC インターフェイス コンフィギュレーションのタイプ 2 不一致チェックについては、誤って設定された vPC がアップ ステートのままになります。ただし、不一致のタイプに応じて、vPC システムは保護アクションをトリガーします。最も一般的なものでは、vPC インターフェイス トランキング設定で許可された VLAN を扱います。この場合、vPC システムは、両側で一致しない vPC インターフェイス VLAN からディセーブルにします。

表 4 に、タイプ 2 整合性検査パラメータを示します。

一部のグローバル コンフィギュレーションの整合性検査パラメータは、（前述したように）**sh vpc consistency-parameters global** で表示されます。ただし、（タイプ 2 整合性検査の）vPC インターフェイス パラメータのほとんどは **sh vpc consistency-parameters interface port-channel** コマンドでは表示されません。

表 3 に記載されているパラメータが両方の vPC ピア デバイス上で同じように設定されていない場合、矛盾した設定により、トラフィック フローで予期しない動作が発生することがあります。

表 4. タイプ 2 整合性パラメータ

パラメータ	説明
MAC エージング タイマー	特定の VLAN の MAC エージング タイマーは、両方の vPC ピア デバイス上で同じにする必要があります。
スタティック MAC エントリ	特定の VLAN のスタティック MAC エントリは、両方の vPC ピア デバイスに適用する必要があります。
VLAN インターフェイス（スイッチ仮想インターフェイス（SVI））	各ピア デバイスは、VLAN インターフェイスが両端で同じ VLAN に設定されていなければならず、この VLAN インターフェイスが、同じ動作状態にある必要があります。
アクセス コントロール リスト（ACL）の設定とパラメータ	ACL 設定は、両方の vPC ピア デバイス上で同じにする必要があります。
Quality of Service（QoS）の設定とパラメータ	QoS 設定は、両方の vPC ピア デバイス上で同じにする必要があります。
スパニングツリー プロトコルのインターフェイス設定	ブリッジ プロトコル データ ユニット（BPDU） フィルタ リンク タイプ（自動、ポイントツーポイント、共有） コストポート プライオリティ STP インターフェイス設定は、両方の vPC ピア デバイス上で同じにする必要があります。
VLAN データベース	すべての VLAN をプライマリ vPC ピア デバイスとセカンダリ vPC ピア デバイスの両方で作成する必要があります。そうしない場合、VLAN は停止します。1 個のピア デバイスだけで設定されている VLAN は、vPC または vPC ピア リンクを使用してトラフィックを通過させません。
ポート セキュリティ	ネットワーク アクセス コントロール（NAC） ダイナミック ARP インスペクション（DAI） IP ソース ガード（IPSG） ポート セキュリティ設定は、両方の vPC ピア デバイス上で同じにする必要があります。
Cisco TrustSec	Cisco TrustSec 設定は、両方の vPC ピア デバイス上で同じにする必要があります。
ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピング	DHCP スヌーピング設定は、両方の vPC ピア デバイス上で同じにする必要があります。
インターネット グループ管理プロトコル（IGMP）スヌーピング	IGMP スヌーピング設定は、両方の vPC ピア デバイス上で同じにする必要があります。
ホットスタンバイ ルータ プロトコル（HSRP）	HSRP 設定は、両方の vPC ピア デバイス上で同じにする必要があります。
プロトコルに依存しないマルチキャスト（PIM）	PIM 設定は、両方の vPC ピア デバイス上で同じにする必要があります。
ゲートウェイ ロード バランシング プロトコル（GLBP）	GLBP 設定は、両方の vPC ピア デバイス上で同じにする必要があります。
すべてのルーティング プロトコル設定	ルーティング設定は、両方の vPC ピア デバイス上で一貫している必要があります。

一般的な推奨事項:

すべての設定パラメータで互換性が取れていることの確認を容易にするために、vPC の設定が終わったら、各 vPC ピア デバイスの設定を表示してみることを推奨します。

vPC ドメインの作成:ガイドラインおよび制約事項

vPC ドメインを作成するには、次の設定時のガイドラインを使用します。

- vPC ドメインを設定する前に、feature vPC をイネーブルにする(conf t; feature vpc)必要があります。
- vPC システムが起動できるようにピア リンクの前にピア キープアライブ リンクを設定する必要があります。
- 両方の vPC ピア デバイスを設定しなければなりません。設定が片方のデバイスから他方へ送信されることはありません。
- ダブルサイド vPC トポロジを設定するには、それぞれの vPC レイヤに一意の vPC ドメイン ID を割り当てる必要があります。
- DCI トポロジで vPC を使用するには、それぞれのデータセンターに一意の vPC ドメイン ID を割り当てる必要があります。
- 必要な設定パラメータが、vPC ピア リンクの両側で一貫していることをチェックします。
- LACP 機能をアクティブにしてから、LACP モードがアクティブに設定された vPC メンバー ポートを設定します。
- 特定の vPC ピアのすべてのポートが同じ VDC 内になくてはなりません。
- レイヤ 2 ポート チャネルだけを(switchport mode trunk または switchport mode access)vPC メンバー ポートで設定できます。
- PIM SM(スパース モード)は、vPC と完全な相互運用性があります。ソフトウェアは vPC での PIM BiDIR または PIM SSM(Source Specific Multicast)をサポートしません。
- ソフトウェアは vPC 環境で DAI(ダイナミック ARP インスペクション)または IPSG(IP ソース ガード)をサポートしません。
- DHCP リレーと DHCP スヌーピングは、vPC でサポートされます。
- ソフトウェアは、vPC での Cisco Fabric Services 領域をサポートしません。
- ポート セキュリティは、vPC メンバー ポートではサポートされません。
- この目的には vPC ピア リンクおよび SVI を使用するのではなく、vPC ピア デバイス(バックアップのルーティング パス)からのルーティング用に別個のレイヤ 3 リンクを設定します。
- 非 vPC VLAN トラフィックを伝送するスイッチ間リンクとして追加レイヤ 2 トランク ポート チャネルを作成することを推奨します。

注: vPC を使用する場合は、HSRP(ホット スタンバイ ルータ プロトコル)、VRRP(仮想ルータ冗長プロトコル)、および PIM(Protocol Independent Multicast)の設定でデフォルトのタイマーを使用するのが最良の方法です。

アグレッシブ タイマーを vPC 設定で使用する場合、ネットワーク コンバージェンス時間に関連するゲインはありません。

vPC コンポーネントの設定のベスト プラクティス

次の項では、vPC VLAN、vPC ピア キープアライブ リンク、vPC ピア リンク、vPC メンバー ポートなど、さまざまな vPC のコンポーネントを設定するための推奨事項を示します。

シャーシの 1 個の 10 G モジュールのみを使用した vPC ピア リンクに関する具体的な考慮事項についても、この章で説明します。

vPC VLAN 設定についての推奨事項

vPC VLAN は、vPC メンバー ポートおよび vPC ピア リンクで許可される VLAN です。

スイッチを動作させる最初の手順は、VLAN データベースの作成です。グローバル コンフィギュレーション モードで次のコマンドを入力します。

```
N7k(config) # vlan <vlan-id range>
```

vPC 環境で、多数の VLAN を設定する場合は、一度に 1 つの VLAN を個別に設定するのではなく、range コマンドを使用して VLAN を設定することを推奨します。

別の VLAN に名前を付ける必要がある場合は、range コマンドを使用して、まずすべての VLAN を作成します。効果的に VLAN を作成するには、グローバル コンフィギュレーション モードを終了します。その後、必要に応じて各 VLAN に名前を付けます。

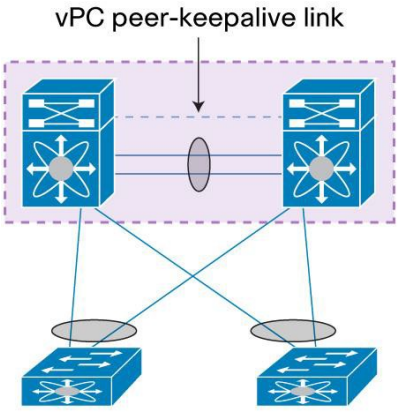
推奨事項:

vPC 環境で、多数の VLAN を設定する場合は、一度に 1 つの VLAN を個別に設定するのではなく、range コマンドを使用して VLAN を設定することを推奨します。

vPC ピア キープアライブ リンク設定の推奨事項

vPC ピア キープアライブ リンクは、図 14 に示すように、他の vPC ピア デバイスに 1 台の vPC ピア デバイスを参加させるレイヤ 3 リンクです。

図 14. vPC ピア キープアライブ リンク



vPC ピア キープアライブ リンクは、vPC ピア デバイス間の定期的なハートビートを伝送します。vPC ドメインを形成する前、および vPC ピア リンクがダウン状態に失敗した場合に両方のピア デバイスが稼働していることを保証するために、vPC システムのブート時に使用されます。後者の場合、vPC ピア キープアライブ リンクがスプリット ブレーンのシナリオを検出するのに利用されます（vPC ピア デバイスは両方ともアクティブ-アクティブ）（vPC ピア リンクがダウンすると、2 台のピア デバイス間のリアル タイムの同期が行われなくなるため、vPC システムはこのアクティブ-アクティブ状況に対応する必要があります。これはセカンダリ ピア デバイスの vPC メンバー ポートのシャットダウンによって実行されます）。

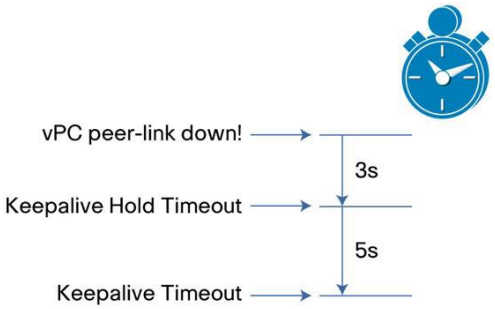
データ構造面では、vPC ピア キープアライブ メッセージは、32 バイトのペイロードを持つ、長さが 96 バイトのポート 3200 上のユーザ データグラム プロトコル（UDP）メッセージです。キープアライブ メッセージは、オンボードの Wireshark ツールキットを使用してキャプチャおよび表示できます。

表 5 に vPC ピア キープアライブ リンク タイマーのデフォルト値を、図 15 に vPC タイマーの概念を示します。

表 5. vPC ピア キープアライブ リンクのデフォルト値

タイマー	デフォルト値
キープアライブ インターバル	1 秒
キープアライブ ホールド タイムアウト（vPC ピア リンクの損失時）	3 秒
キープアライブ タイムアウト	5 秒

図 15. vPC タイマーの概念



キープアライブ ホールド タイムアウト

このタイマーは、vPC ピア リンクがダウン状態になると開始します。この間、セカンダリ vPC ピア デバイスはピア キープアライブの hello メッセージ（またはその欠如）を無視します。これは、何らかのアクションが実行される前にネットワーク コンバージェンスが実行されることを保証するものです。

キープアライブ タイムアウト

この間、セカンダリ vPC ピア デバイスは、プライマリ vPC ピア デバイスからの vPC ピア キープアライブ hello メッセージを探します。単一の hello を受信した場合、セカンダリ vPC ピアは、デュアル アクティブ シナリオが必要であるため、すべての vPC メンバー ポート（つまり、キーワード **vpc** を伝送するすべてのポート チャネル）をディセーブルにすることを決定します。

（vPC ドメイン設定コンテキストで）vPC タイマーを変更するコマンドライン設定は次のとおりです。

N7k(config-vpc-domain)# peer-keepalive destination ipaddress [**source** ipaddress | **hold-timeout** secs | **interval** msecs {**timeout** secs}]

show vpc peer-keepalive コマンドは、次のようにピア キープアライブ リンクに関するすべての情報を表示します。

```
7K1# sh vpc peer-keepalive

vPC keep-alive status               : peer is alive
--Peer is alive for                 : (22) seconds, (255) msec
--Send status                       : Success
--Last send at                      : 2011.06.07 15:24:28 339 ms
--Sent on interface                 : Eth1/24
--Receive status                    : Success
--Last receive at                   : 2011.06.07 15:24:27 597 ms
--Received on interface             : Eth1/24
--Last update from peer             : (0) seconds, (857) msec

vPC Keep-alive parameters
--Destination                       : 192.168.100.2
--Keepalive interval                : 1000 msec
--Keepalive timeout                 : 5 seconds
--Keepalive hold timeout            : 3 seconds
--Keepalive vrf                     : peerkeepalive
--Keepalive udp port                : 3200
--Keepalive tos                     : 192
```

強力な推奨事項:

vPC ピア キープアライブ リンクを作成するときには、優先順位の降順で次を使用します。

1. L3 として設定された専用リンク（1 ギガビット イーサネット ポートで十分）2 X 1 G ポートを搭載したポート チャネルがさらに適切です。
2. Mgmt0 インターフェイス（管理トラフィックとともに）
3. 最後の手段として、レイヤ 3 インフラストラクチャでピア キープアライブ リンクをルーティングします。

警告: vPC ピア リンク上に vPC ピア キープアライブ リンクを設定しないでください。ピア キープアライブ メッセージは、ピア リンクがダウンしたときにフェイト共有を回避するために vPC ピア リンク上で伝送する必要があります

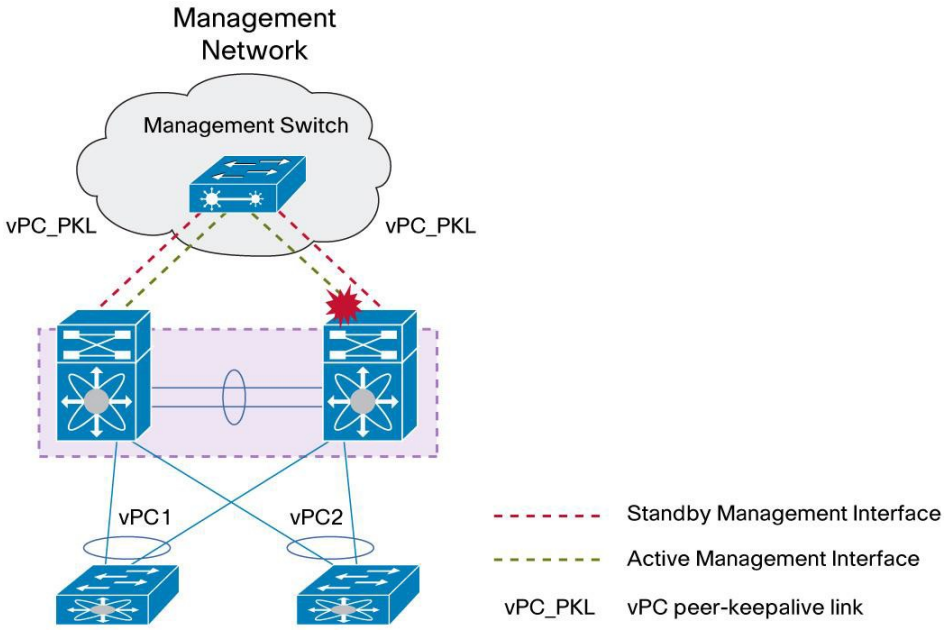
注： 純粋な Cisco Nexus F1 シリーズ システムまたは VDC（つまり、VDC のシャーシまたは F1 ポートだけで使用される F1 ラインカードだけ）を使用している場合は、mgmt0 インターフェイスまたは 10 ギガビット イーサネットの前面パネル ポートとのピア キープアライブ リンクを形成できます。後者の場合は、SVI で **management** コマンドを使用して、インバンド管理に対してイネーブルにします（それ以外の M1 モジュールがシステムまたは VDC に存在しないため、SVI はダウンします）。

デュアル スーパーバイザでの mgmt0 Cisco Nexus 7000 シリーズ ペアを使用した vPC ピア キープアライブ リンク

vPC ピア キープアライブ リンクの伝送にデュアル スーパーバイザと mgmt0 インターフェイスを使用する場合は、2 台のスイッチ（ピア デバイス 2 のスーパーバイザ 1 上の mgmt0 に直接接続しているピア デバイス 1 のスーパーバイザ 1 上の mgmt0 など）間で mgmt0 ポートをバックツーバック モードで接続しないでください。理由は、アクティブ スーパーバイザが mgmt0 ポートを制御し、スーパーバイザのスイッチオーバー時にキープアライブ接続が切断される可能性があるからです（ピア デバイス 1 のアクティブ スーパーバイザがピア デバイス 2 のスタンバイ スーパーバイザにキープアライブを送信）。

ベスト プラクティスは、図 16 に示すように、このような状況を回避するために異なるスーパーバイザ間に L2 スイッチを挿入することです。

図 16. mgmt0 とデュアル スーパーバイザを使用した vPC ピア キープアライブ リンク



強力な推奨事項:

デュアル スーパーバイザ構成で vPC ピア キープアライブ リンクに mgmt0 ポートを使用する場合、異なるスーパーバイザを相互接続するには、中間 L2 スイッチを必ず使用してください。

vPC ピア キープアライブ リンクおよび VRF

デフォルトでは、vPC ピア キープアライブは VRF 管理に配置されます。

必要に応じて、vPC ピア キープアライブは（vPC ドメイン設定コンテキストで）次のコマンドを使用して別の VRF に配置できます。

N7k(config-vpc-domain)# peer-keepalive destination <destination IP> source <source IP> **vrf <VRF name>**

一般的な推奨事項:
vPC ピア キープアライブ リンク（たとえば VRF PKL-VRF）の専用 VRF を作成してください

vPC ピア リンク設定の推奨事項

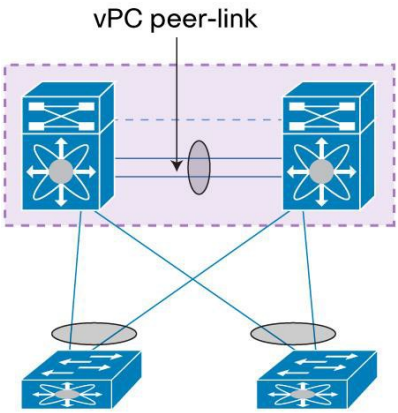
vPC ピア リンクは、次のアクションを実行できる標準 802.1Q トランクです。

- vPC および vPC 以外の VLAN を伝送する。
- 信頼できる通信のために CoS 値 = 4 がタグ付けされた Cisco Fabric Services メッセージを伝送する。
- 他の vPC ピア デバイスからのフラッディング トラフィックを伝送する。
- STP BPDU、HSRP Hello メッセージ、および IGMP 更新を伝送する。

vPC リンク レベルに vPC ループ回避メカニズム（データ プレーン レイヤ）が実装されています。これはソフトウェア要求なしでハードウェアで行います。

図 17 に、vPC ドメインの vPC ピア リンク コンポーネントを示します。

図 17. vPC ピア リンク



強力な推奨事項:
vPC ピア リンクを作成するときには、次のガイドラインに従ってください。

- メンバー ポートが 10 ギガビット イーサネット インターフェイスであることを確認します。
- 2 つ以上の 10 ギガビット イーサネット ポートを使用します。vPC ピア リンクのメンバー ポートは、ポートチャネルに関してラインカード容量まで拡張できます（M1 ラインカードは最大 8 個のメンバー ポートをサポートし、F1 および F2 は最大 16 のメンバー ポートをサポートします）。
- ピア リンクのハイ アベイラビリティを高めるために、少なくとも 2 つの異なるラインカードを使用します。
- M1 32 10 G ラインカードで専用の 10 ギガビット イーサネット ポートを使用します。共有モードのポートは使用しないでください。

- 異なるスイッチ間ポート チャネルで vPC および非 vPC VLAN を分割します（vPC VLAN を伝送する vPC ピア リンクと vPC 以外の VLAN を伝送する他のスイッチ間ポート チャネルを使用します）。
- vPC ピア間にデバイスを挿入しないでください。ピア リンクはポイントツーポイント リンクです。

vPC ピア リンクは、すべての出荷 10 G ラインカードでサポートされます。これは 1 G ラインカードでも任意の FEX ポート（10 G の前面パネル ポートを持つ 2232 モデルを含む）でもサポートされていません。

表 6 に、vPC ピア リンクをサポートできるすべてのラインカードを示します。

表 6. vPC ピア リンクでサポートされるラインカード。

ラインカード製品番号	ラインカードの説明
N7K-M132XP-12 **N7K-M132XP-12L**	32 10 ギガビット イーサネット ポート M1 シリーズ
N7K-M108X2-12L	8 10 ギガビット イーサネット ポート M1 シリーズ
N7K-F132XP-15	32 1/10 ギガビット イーサネット ポート F1 シリーズ
N7K-F248XP-25	48 1/10 ギガビット イーサネット ポート F2 シリーズ

vPC ピア リンクは、両端（M1 ～ M1）の M1 ポート、両端（F1 ～ F1）の F1 ポート、または両端（F2 ～ F2）の F2 ポートで形成できます。vPC ピア リンクの両端を厳密に同じにする必要があります。

結果として、（たとえば）片方の F1 ポートともう片方の M1 ポートを混在させることはできません。

M132XP および M108X2（つまり、それぞれ 32 10 ギガビット イーサネット ラインカードおよび 8 10 ギガビット イーサネット ラインカード）でポート チャネルを形成できます。ただし、ポートが専用モードに設定されている場合だけ M132XP のポートで M108X2 のポートを持つポート チャネルを形成できる要件に注意してください。

これは、vPC ピア リンクの推奨事項と一致しています。つまり、vPC ピア リンクのメンバー ポートには、完全な 10 ギガビット イーサネット機能が必要です、言い換えればオーバーサブスクリプションはありません。

図 18 および 19 に、サポートされる設定とサポートされない設定を示します。

図 18. vPC ピア リンクでサポートされる設定（両端が同じポート タイプでなければなりません）

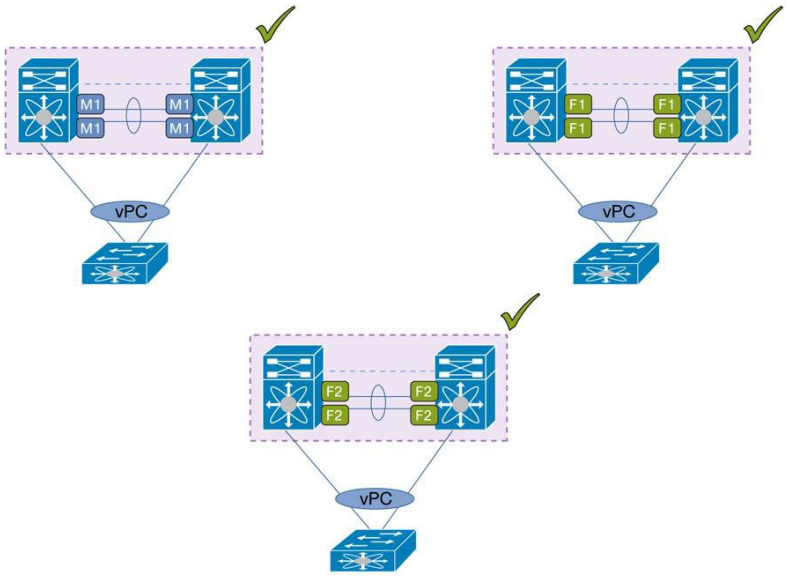
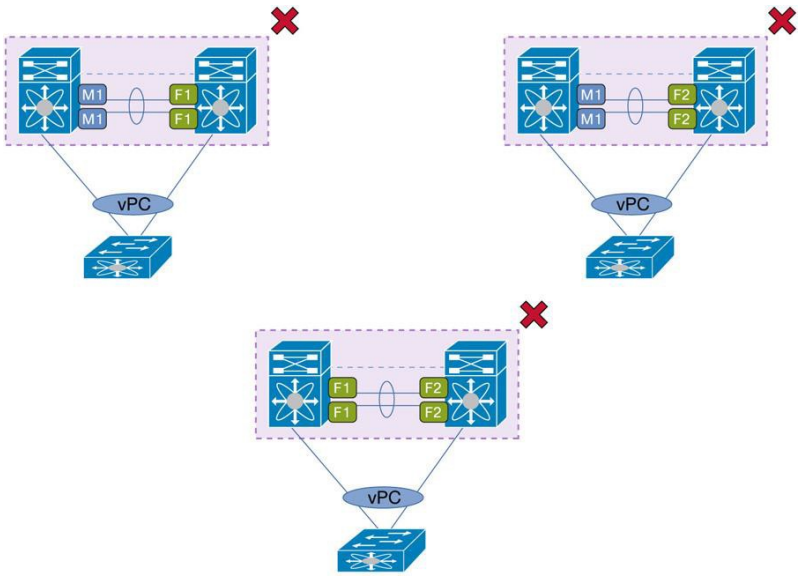


図 19. vPC ピア リンクでサポートされない設定（両端が同じポート タイプでなければなりません）



各ポート タイプには（転送、キューイング、セキュリティ面で）異なるハードウェア特性があるため、vPC ピア リンクの同じ端で異なるポート タイプを混在させる（たとえば vPC ピア リンク上の同じ端で M1 ポートおよび F1 ポートをバンドルする）ことはできません。

このルールは、vPC ピア リンクのみ適用されるものではありません。これはポート チャネルの汎用ステートメントです。

注： 混合シャーシ モード（つまり、同じシステムまたは同じ VDC に M1 および F1 ポートがある）および F1 ポート上の vPC ピア リンクでは、vPC ピア ゲートウェイ機能とバックアップ ルーティング パス機能を使用する場合は注意してください。

Cisco NX-OS Release 5.1.3 以降、ノブはピア ゲートウェイから特定の VLAN を除外するのに使用できます。これらの VLAN は、通常、バックアップ ルーティング パスに使用します。コマンドは、次のとおりです。

```
N7k(config-vpc-domain)# peer-gateway exclude-vlan <VLAN list>
```

ノブは vPC システムと vPC ピア リンクのその他の設定には役立ちません。

詳細については、このマニュアルのピア ゲートウェイの項で説明しています。

ユニキャスト トラフィックについては、vPC ピア デバイスが、vPC メンバー ポートを使用するローカル フォワーディング プリファレンスを常に使用します。

通常、vPC ピア リンクには、vPC ドメインの片側で vPC メンバー ポートの障害が発生した場合を除き、ユニキャスト トラフィックがロードされません。

マルチキャスト トラフィックについては、ストリームのコピーが vPC ピア リンクで複製されます（ラインカードがマルチキャスト環境でデュアル DR（指定ルータ）をサポートしないため、F2 ポートで vPC ピア リンクが構築されている場合を除く）。

このタイプのトラフィックは、vPC ピア リンクの寸法を測るときに考慮に入れる必要があります。

vPC ピア リンクの統計情報を表示するには、コマンド **show vpc statistics peer-link** を使用します。

vPC ピア リンクに関連する重要な側面は VLAN プルーニングです。vPC VLAN を動作可能にするには、次のコマンドを使用して vPC ピア リンクで定義する必要があります。

```
N7k(config)# interface port-channel 1          (int Po1: vPC peer-link)
   N7k(configif)# switchport trunk allowed vlan <VLAN-id list>
```

当然ながら、vPC VLAN は、以前 vPC メンバー ポートで許可（つまりプルーニング）されています。

必須の推奨事項:
VLAN プルーニングは、必ず vPC VLAN の許可リストを使用して vPC ピア リンク上で実行してください。vPC VLAN は、vPC メンバー ポートで前にプルーニングされている必要があります。

vPC ピア リンクがダウンした場合の vPC システムの動作
vPC ピア リンクがダウンし、vPC ピア キープアライブ リンクがまだ稼働している場合、vPC セカンダリ ピア デバイスは次の操作を実行します。

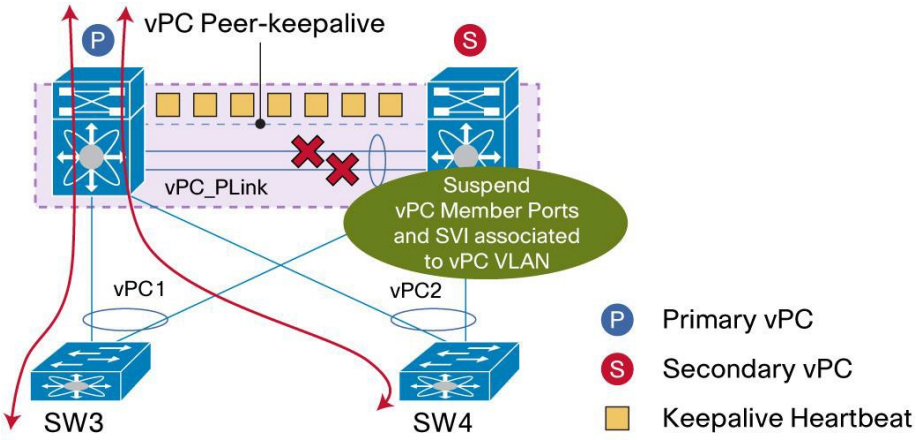
- vPC メンバー ポートを停止します
- vPC VLAN に関連付けられた SVI をシャットダウンします

vPC からのこの保護動作は、プライマリ ピア デバイスにすべてのサウスバウンドおよびノースバウンド トラフィックをリダイレクトできます。

vPC ピア リンクがダウン状態の場合、両方の vPC ピア デバイスは互いをもう同期できないため、設計済みの保護メカニズムによりデータ パスからピア デバイスの 1 つ（発生時にセカンダリ ピア デバイス）が分離されます。

vPC ピア リンクがダウンした場合に何が起きるかを図 20 に示します。

図 20. vPC ピア リンクのダウン：セカンダリ ピア デバイス上の動作



孤立ポートがセカンダリ vPC ピア デバイスに接続されている場合、ピア リンクがダウンすると隔離されます。

これらの孤立ポートへのレイヤ 3 接続を保持するには、コマンド **dual-active exclude interface-vlan** を使用して（vPC VLAN に関連付けられている）SVI のシャットダウンを防止できます。

vPC ピア リンクがダウンすると、目的の SVI の UP 状態を保持するために次のコマンドを使用します。

```
N7k(config-vpc-domain)# dual-active exclude interface-vlan <VLAN list>
```

ノブに示されている VLAN は vPC VLAN に関連付ける必要があります。非 vPC VLAN を使用しても、vPC ピア リンクがダウンするとこれらの VLAN に関連付けられた SVI がシャットダウンされないため、影響はありません。

1 つの M1 10 Gbps モジュールだけを含むシステムでの vPC ピア リンク設定の推奨事項

Cisco Nexus 7000 シリーズ スイッチ構成には、1 つの M1 10 Gbps モジュールおよび複数の 1 Gbps モジュールだけが含まれているものがあります。問題は、これらのスイッチがレイヤ 2/レイヤ 3 境界として定義されている場合（つまり、両方のレイヤ 3 アップリンク接続と vPC ピア リンクに同じ 10 Gbps ラインカードが使用されている場合）に起きる可能性があります。

このタイプの設定では、vPC のオブジェクト トラッキング機能（NX-OS 4.2 以降で使用可能）使用する必要があります。

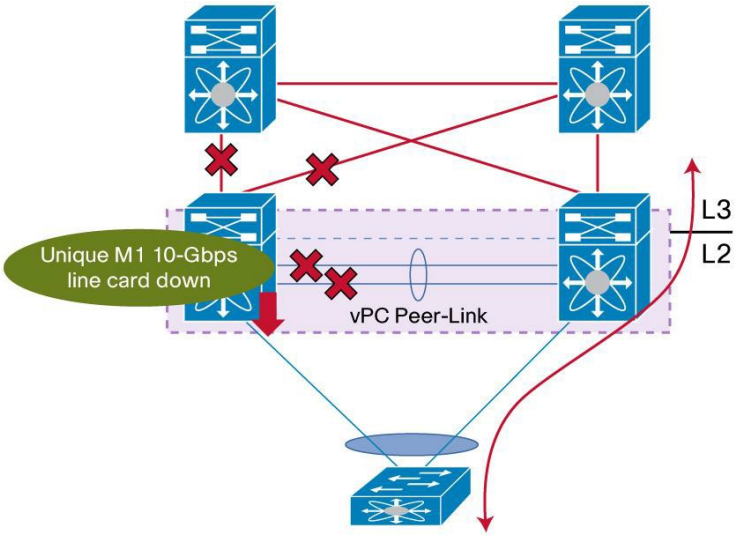
vPC オブジェクト トラッキング

L3 コア アップリンクおよび vPC ピア リンク インターフェイスが同じモジュール上でローカライズされている単一の Cisco Nexus 7000 シリーズ M132XP-12 モジュールまたは M108XP-12 モジュールによる vPC の導入は、10 Gbps モジュールがプライマリ vPC で故障した場合（1 Gbps ラインカードと 10 Gbps ラインカードの両方で vPC メンバー ポートが定義されている場合）、アクセス レイヤ隔離を受けやすくなります。

この特有のシナリオでは、M1 10 Gbps が破損しているピア デバイスの vPC メンバー ポートをシャットダウンする vPC オブジェクト トラッキング機能（プライマリまたはセカンダリ vPC ロールに関係なく）を使用します。このトリガーされるアクションは、トラフィック フロー（サウスバウンドおよびノースバウンド）が M1 10 Gbps ラインカードが稼働しているもう一方のピア デバイスを通過できるようにします。

図 21 に、vPC オブジェクト トラッキング機能の影響を示します。

図 21. vPC オブジェクト トラッキング機能：vPC ピア リンクがダウンした場合の動作



vPC オブジェクト トラッキング機能は、トラフィックを残りの vPC ピアに配信できるように、障害が発生したデバイスで vPC を一時停止します。

vPC オブジェクト トラッキングを使用するには、ブール オブジェクトのリストとしてピア リンク インターフェイスおよび L3 コア インターフェイスの両方を追跡します。ブール AND 演算は、vPC オブジェクト トラッキングでサポートされないことに注意してください。

次のサンプル設定では、vPC オブジェクト トラッキングをアクティブにするために必要なさまざまなコマンドを示します。

```
! Track the vpc peer link
track 1 interface port-channel11 line-protocol
! Track the uplinks to the core
track 2 interface Ethernet1/1 line-protocol
track 3 interface Ethernet1/2 line-protocol
```

```
! Combine all tracked objects into one.
! "OR" means if ALL objects are down, this object will go down
! ==> we have lost all connectivity to the L3 core and the peer link
track 10 list boolean OR
  object 1
  object 2
  object 3

! If object 10 goes down on the primary vPC peer,
! system will switch over to other vPC peer and disable all local vPCs
vpc domain 1
  track 10
```

vPC オブジェクト トラッキング設定は、両方の vPC ピア デバイスに適用する必要があります。

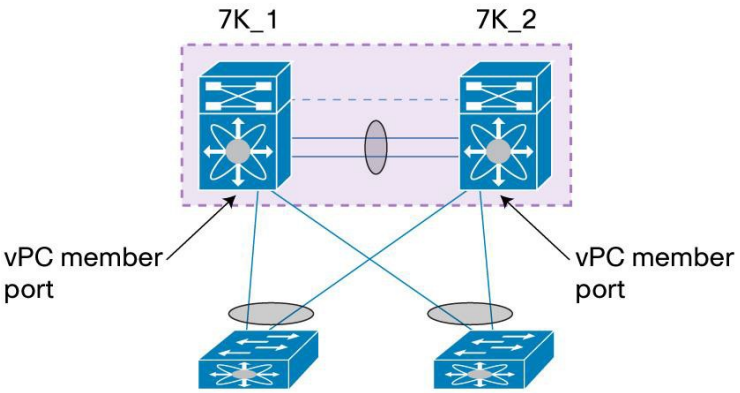
推奨事項:

特有の M1 シリーズ ラインカード（L3 コアへの vPC ピア リンクおよび L3 アップリンクの両方に使用される M1）を搭載した vPC ピア デバイスでは、vPC オブジェクト トラッキング機能を使用してください。

vPC メンバー ポート設定の推奨事項

定義上、vPC メンバー ポートは、図 22 に示すように、vPC のポート チャネル メンバーです。

図 22. vPC メンバー ポート



vPC メンバー ポートとして定義されたポート チャネルには、キーワード **vpc <vpc id>** が必ず含まれています。

ポート チャネル メンバー ポートには、1 つのメンバー ポートからラインカードのハードウェア制限までのポートが含まれます（M1 シリーズのラインカードでは、最大 8 個のメンバー ポートがサポートされ、F1 および F2 シリーズのラインカードでは、最大 16 個のメンバー ポートがサポートされます）。

レイヤ 2 ポート チャネルだけが vPC（レイヤ 3 なし）でサポートされます。ポート チャネルは、アクセスまたはトランク スイッチポート モードで設定できます。vPC メンバー ポートで許可される VLAN は、定義上は、vPC VLAN と呼ばれます。vPC VLAN は、vPC ピア リンクで許可する必要があります。

> **注： vPC VLAN は、vPC メンバー ポートで定義されるたびに、vPC ピア リンクにおいても定義する必要があります。vPC ピア リンクの vPC VLAN を定義しないと、VLAN は動作不可能になります。**

必須の推奨事項:

vPC メンバー ポートで許可されている vPC VLAN を vPC ピア リンクで許可する必要があります。

vPC メンバー ポートの設定例は次のとおりです。

```
7K1:
interface port-channel201
  switchport mode trunk
  switchport trunk native vlan 100
  switchport trunk allowed vlan 100-105
  vpc 201
```

```
7K2:
interface port-channel201
  switchport mode trunk
  switchport trunk native vlan 100
  switchport trunk allowed vlan 100-105
  vpc 201
```

vPC メンバー ポートを適切に構築するには、次の推奨事項に従います。

強力な推奨事項:

- vPC メンバー ポートの設定は、両方の vPC ピア デバイスで一致する必要があります。
- 不一致がある場合は、(vPC メンバー ポートのタイプ 1 またはタイプ 2 整合性検査に応じて)VLAN またはポート チャネル全体が一時停止する可能性があります。たとえば、MTU が不一致の場合、vPC メンバー ポートが停止されます。
- 設定、モニタリング、およびトラブルシューティングを簡略化するためにポート チャネル ID と同じ vPC ID を使用します。
- M1 シリーズ ラインカードの場合:同じ vPC メンバー ポートに 8 つまでのアクティブなポートをバンドルできます(その結果 vPC 全体に 16 方向のポート チャネルを組み込むことができます)。
- F1 および F2 シリーズ ラインカードの場合:同じ vPC メンバー ポートに 16 個までのアクティブなポートをバンドルできます(その結果 vPC 全体に 32 方向のポート チャネルを組み込むことができます)。
- 同じ vPC メンバー ポートに異なるポート タイプ(M1 ポート、F1 ポート、または F2 ポート)を混在させないでください。これはソフトウェアによって許可されません。
- vPC メンバー ポートの両側(つまり、7K1 の vPC メンバー ポートと 7K2 の vPC メンバー ポート)を同じポート タイプにする必要があります(M1 ポート、F1 ポート、または F2 ポート)。

vPC は両側(つまり、両方の vPC ピア デバイス上)で同じポート タイプを使用して形成できます。

ピア デバイス 1 の vPC メンバー ポートで M1 ポート タイプを使用する場合、ピア デバイス 2 の vPC メンバー ポートでも M1 ポート タイプを使用する必要があります。同じステートメントが F1 および F2 ポート タイプに適用されます。

ポートのハードウェア特性は異なるため(転送、キューイング、およびセキュリティ面で)、同じ vPC メンバー ポートに異なるポート タイプを混在させることはできません(ポート チャネルにも当てはまります)。

サポートされる vPC メンバー ポート設定およびサポートされない vPC メンバー ポート設定を図 23 および 24 に示します。

図 23. vPC メンバー ポートでサポートされる設定

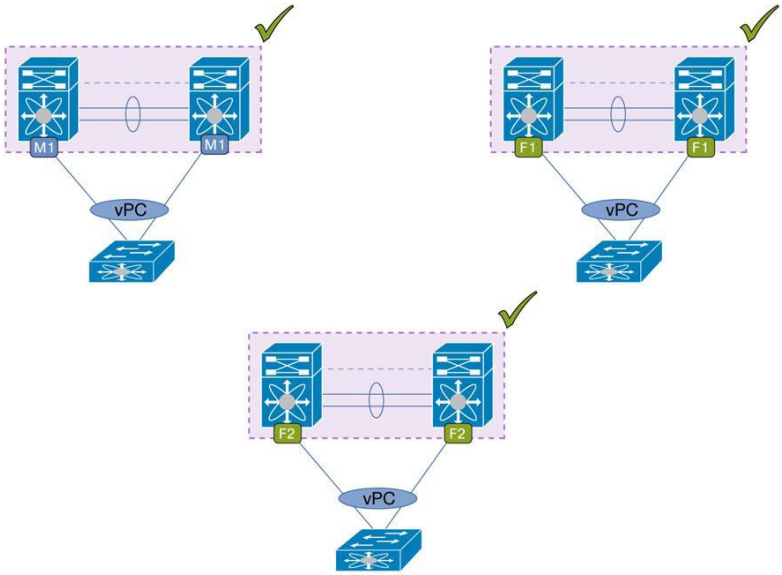
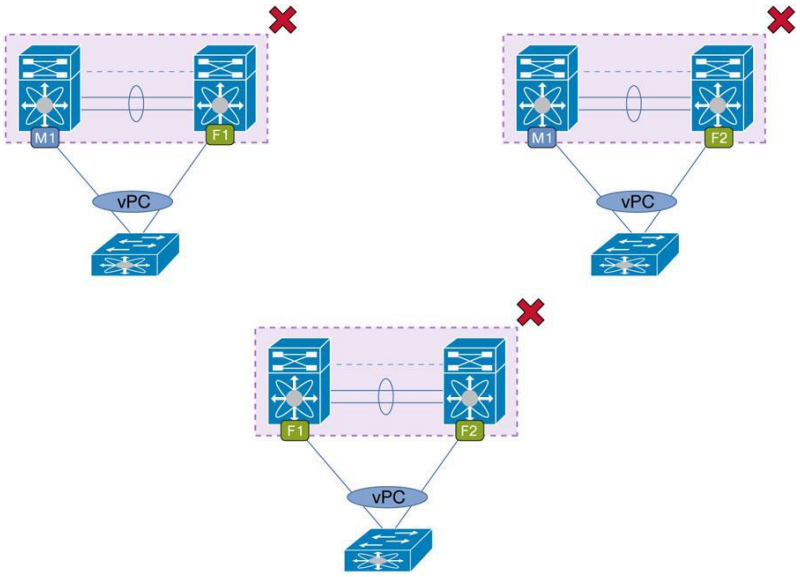


図 24. vPC メンバー ポートのサポートされていない設定



注: M132XP および M108X2（それぞれ 32 10 ギガビット イーサネット ラインカードおよび 8 10 ギガビット イーサネット ラインカード）はポート チャネルを形成し、同じ vPC メンバー ポートに共存できます。ただし M132XP のポートが専用モードで設定されている場合のみ M132XP ポートが M108X2 のポートでポート チャネルまたは vPC メンバー ポートを形成できるという要件に注意してください。

混合シャーシ モード（同じシステムまたは VDC の M1/F1 ポート）での vPC のベスト プラクティス

混合シャーシ モードは、M1 ポートおよび F1 ポートが同時に使用されるシステムです。

M1 シリーズ ラインカードは、スケーラブルなレイヤ 2 とレイヤ 3 の機能を提供します。F1 シリーズ ラインカードは、高密度の費用対効果が高いレイヤ 2 の 10 ギガビット イーサネット接続を提供します。F1 ポートに入るトラフィック（VLAN 間ルーティングの L3 トラフィックまたはデータセンターの外部に移動するトラフィック）をルーティングする必要がある場合、M1 ポートが L3 プロキシに使用される L3 内部プロキシ ルーティングによって M1 および F1 ポート間の相互運用性が提供されます。通常、M1 ラインカードは F1 ラインカードに代わってインターフェイス VLAN（つまり SVI（スイッチ仮想インターフェイス））をホストします。

レイヤ 3 内部プロキシ ルーティング

L3 内部プロキシ ルーティングには次の特性があります。

- ユニキャスト トラフィックについては、F1 モジュールのプロキシ レイヤ 3 ルーティングは VDC の一部またはすべての M1 インターフェイス間に広がる場合があります。
- マルチキャスト トラフィックについては、F1 モジュールのプロキシ レイヤ 3 のレプリケーションは、すべての M1 レプリケーション エンジン間に広がる場合があります。

L3 内部プロキシ ルーティングは、システムまたは VDC が混合シャーシ モードで設定されている場合にデフォルトでイネーブルになっています。Cisco Nexus 7000 シリーズは自動的に VDC のすべての M1 モジュールをプロキシ レイヤ 3 転送に使用できるようにします。

システムまたは VDC のすべての M1 前面パネル ポートまたはポート グループは、この L3 内部プロキシ ルーティングの一部になります。

ユーザは、コマンド **hardware proxy layer-3 forwarding** を使用してプロキシ ルーティング設定を変更できます。ノブを使用すると、L3 内部プロキシ ルーティングへの参加に特定の前面パネル ポートまたはポート グループを追加したり、参加から除外したりできます。

注： Cisco NX-OS Release 5.1(2) 以降、レイヤ 3 トラフィック（F1 シリーズ モジュールからのトラフィック）のプロキシに使用できるプロキシ フォワーダの最大数が 16 から 128 に増加しました。**show hardware proxy layer-3 detail** コマンドの出力には、最大 128 のレイヤ 3 フォワーダが表示されます。

```
7K1# sh hardware proxy layer-3 detail

Global Information:
        F1 Modules:     Count: 1           Slot: 8
        M1 Modules:     Count: 4           Slot: 1-3,9

        Replication Rebalance Mode:              Manual
        Number of proxy layer-3 forwarders:      16
        Number of proxy layer-3 replicators:     12

Forwarder Interfaces                      Status        Reason
------------------------------------------------------------------------------
Eth1/1-12                                   up          SUCCESS
Eth1/13-24                                  up          SUCCESS
Eth1/25-26                                  up          SUCCESS
Eth1/37-48                                  up          SUCCESS
<省略>
```

```
Replicator Interfaces                    #Interface-Vlan      Interface-Vlan
-------------------------------------------------------------------------------
Eth1/1-24                                  7                 1,40,200,400-401,
                                                               1000,3000
Eth1/25-48                                 6                 3030,3039,3049,3142,
                                                               3966-3967
```

sh hardware proxy layer-3 counters brief L3 フォワーダの使用状況に関する一部の統計データを提供します。

```
7K1# sh hardware proxy layer-3 counters brief

Summary:
-----------------------------
Proxy packets sent by all F-series module:
-------------------------------------------------------------------------
Router Interfaces             Tx-Pkts             Tx-Rate (pkts/sec approx.)
-------------------------------------------------------------------------
Eth1/1-12                       34453                 1443
Eth1/13-24                     323242               234
Eth1/25-26                     345435               213
Eth1/37-4                       345341                0234
<省略>
=============================================================
Total                                2341434             3453
=============================================================
```

混合シャーシ モードの vPC

集約スイッチでの M1 ポートおよび F1 ポートの混在（混合シャーシ モードとも呼ばれる）には複数の利点があります。

- ブリッジド トラフィックが F1 ポートに保持されます
- F1 ポートからのルーテッド トラフィックは M1 ポートにプロキシされ、F1 ポートにトラフィックの任意のタイプをサポートする機能が提供されます。

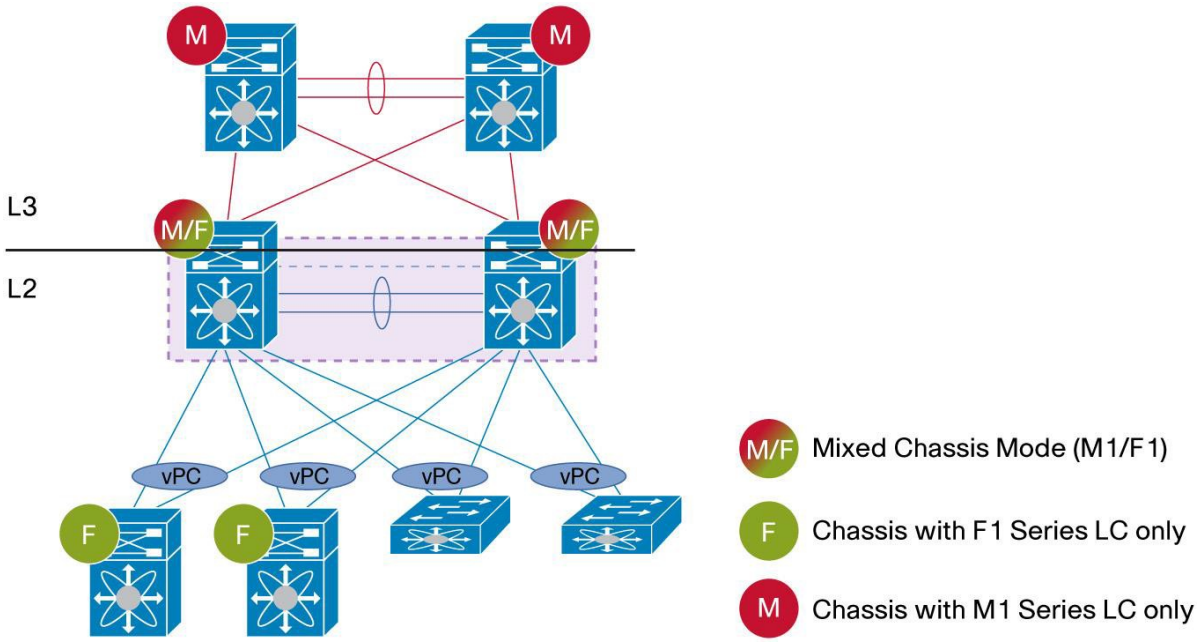
vPC は、vPC ピア リンクの両方のタイプについて（つまり、F1 ポートまたは M1 ポートで形成された vPC ピア リンク）混合シャーシ モード設定で完全にサポートされます。

注： 混合シャーシ モード（M1/F1）で VDC またはシステムを設定することは、vPC ドメインが L2/L3 境界のロール（つまり、インターフェイス VLAN と HSRP または VRRP 機能のホスティング）を果たす必要がある場合の前提条件です。

vPC ドメインが L2 ネットワークとしてのみ必要な状況では、大部分は F1 ポートだけで十分です。L3 機能が必要ないため、M1 ポートは不要です。

図 25 は、混合シャーシ モード設定の vPC システムがデータセンターでどのように適合するかを示しています。

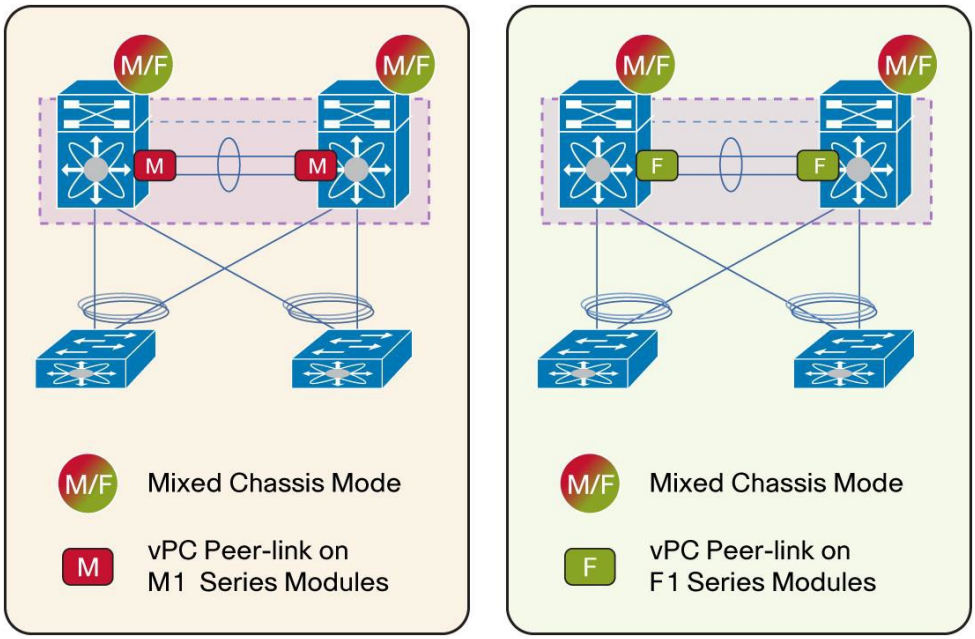
図 25. 混合シャーシ モード設定の vPC システム



vPC ピア リンク（M1 ポートのピア リンクおよび F1 ポートのピア リンク）の性質に応じて、混合シャーシ モードの vPC で 2 種類のトポロジを実装できます。

図 26 は、2 つの可能な設定を示しています。

図 26. 混合シャーシ モードの vPC：F1 ポートまたは M1 ポートのピア リンク



F1 ポートのピア リンクを使用した混合シャーシ モードの vPC システムは、次の特性を示します。

- サポートされる MAC アドレスの総数は、16K（F1 シリーズ ラインカードの 1 つの転送エンジン（つまり、チップのスイッチ）の容量）です
- M1 ポートは L3 アップリンクだけに使用されます
- F1 ポートは vPC メンバー ポートに使用されます（必要に応じて M1 ポートも使用できます）
- バックアップ ルーティング パスに属する VLAN を除外するには **peer-gateway exclude-vlan <VLAN list>** を使用する必要があります（このコマンドは、F1 の vPC ピア リンクを使用した混合シャーシ モードの vPC システムにのみ適用されます）

M1 ポートのピア リンクを使用した混合シャーシ モードの vPC システムは、次の特性を示します。

- サポートされる MAC アドレスの総数は 128K（M1 シリーズ ラインカードの転送エンジンの容量）です
- M1 ポートは L3 アップリンクと vPC ピア リンクに使用されます
- F1 ポートは vPC メンバー ポートに使用されます（必要に応じて M1 ポートも使用できます）
- **peer-gateway exclude-vlan <VLAN list>** ノブを使用する必要はありません

F1 ポートのピア リンクを使用した混合シャーシ モードの vPC システムを展開し、バックアップ ルーティング パスに加えてピアゲートウェイ機能を使用する必要がある場合は、注意してください。

peer-gateway ノブをイネーブルにすると、デフォルトでは、vPC ピア リンクに設定されているバックアップ ルーティング パスが CPU の介入によりソフトウェアで処理されます。

バックアップ ルーティング パスで伝送されたトラフィックをパフォーマンス ペナルティなしで強制的にハードウェアで処理するには、**peer-gateway exclude-vlan <VLAN list>** ノブを使用します。

このコマンド（NX-OS Release 5.1.3 から使用可能）を使用すると、ピアゲートウェイ メカニズムから目的の VLAN のアソシエーションを解除できます。

peer-gateway exclude-vlan については、このマニュアルで（ピアゲートウェイの項で）後述します。

強力な推奨事項:
混合シャーシ モードの vPC システム（F1 ポートまたは M1 ポートのピア リンク）の場合、推奨事項は同じシステムまたは VDC で少なくとも 2 つの M1 シリーズ ラインカードを使用することです。2 つの M1 シリーズ ラインカードを使用すると、L3 内部プロキシ ルーティングと L3 機能（L3 アップリンク、インターフェイス VLAN または SVI、および HSRP/VRRP 機能）の復元力が向上します。

F1 のピア リンクと 1 個の M1 ラインカードを使用した vPC 混合シャーシ モード

F1 ポートのピア リンクと 1 つの M1 ラインカードを使用した混合シャーシ モードの vPC システムは、推奨設定ではありません（推奨事項に従うには 2 つの M1 ラインカードを使用します）。

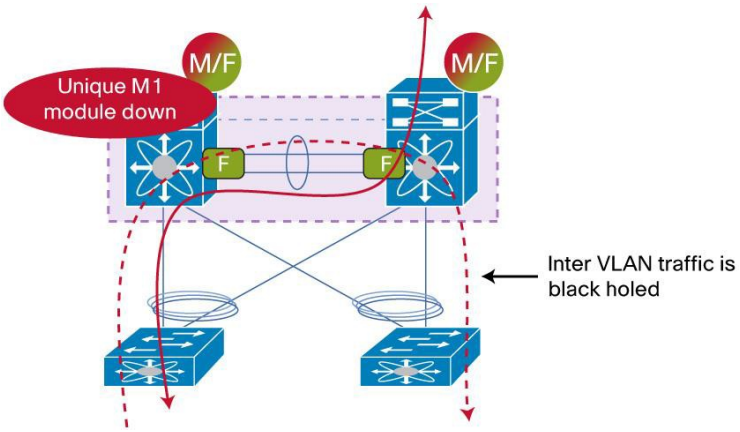
ただし、vPC はこのタイプの設定で正しく動作します。M1 シリーズ モジュールは、レイヤ 3 の内部プロキシ ルーティングとレイヤ 3 のアップリンク接続に使用されます。F1 モジュールは、レイヤ 2 ドメイン ブリッジングに使用されます。

固有の M1 モジュールに障害が発生した場合は、vPC システム動作について注意してください。

- vPC ループ回避ルールのため、VLAN 間トラフィックにブラック ホールがあります（動作している M1 モジュールは、HSRP または VRRP vMAC と等しい宛先 MAC を持つすべてのパケットを処理します）。
- L3 トラフィック（サウスバウンドまたはノースバウンド トラフィック）は問題なくシームレスに流れています（すべてのルーテッド トラフィックは、動作している M1 モジュールに配信されます）。

この動作を、図 27 に示します。

図 27. F1 のピア リンクと 1 つの M1 ラインカードを使用した vPC 混合シャーシ モード：vPC ピア リンクがダウンしたときのトラフィック フロー



強力な推奨事項:
F1 ポートの vPC ピア リンクを使用した混合シャーシ モードでは、少なくとも 2 つの M1 ラインカードを使用します。

2 つの M1 シリーズ ラインカードを使用すると、L3 内部プロキシ ルーティングと L3 機能（L3 アップリンク、インターフェイス VLAN または SVI、および HSRP/VRRP 機能）の復元力が向上します。

vPC ドメインにデバイスを接続するためのベスト プラクティス

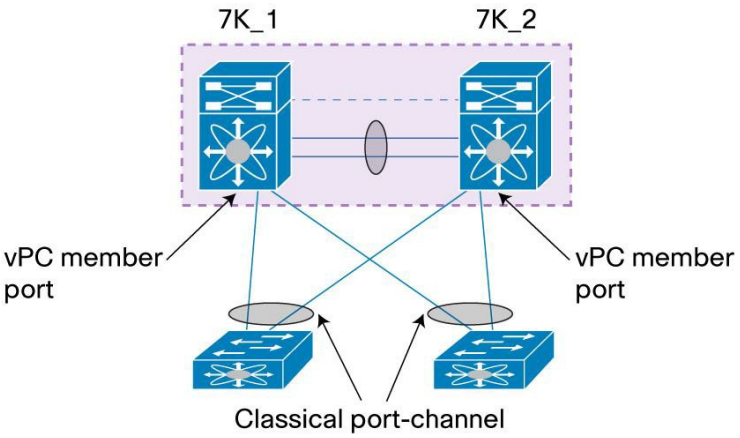
ここでは、vPC ドメインにアクセス デバイスまたはエンドポイント デバイスを接続するためのベスト プラクティスについて説明します。

vPC ドメインへのデバイスの接続方法

vPC ドメインにデバイスを接続するには、アクセス デバイスから 2 台の vPC ピア デバイスへのレイヤ 2 ポート チャネルを作成します。アクセス デバイスの観点からは、これは従来のポート チャネルです。各 vPC ピア デバイスの観点からは、これは vPC メンバー ポート（つまり、キーワード vPC を持つポート チャネル）です。

従来のポート チャネルと vPC メンバー ポートを vPC トポロジでどのように区別できるかを図 28 に示します。

図 28. 従来のポート チャネルおよび vPC メンバー ポート



注： レイヤ 3 ポート チャネルは vPC テクノロジーではサポートされません。

vPC ドメインへの接続により、異なるポート チャネル メンバー ポートへのロードバランシング機能が提供されます。

ポートチャネルは、スパニングツリー プロトコル（STP）の単一の論理エンティティと見なされます。結果として、ポート チャネルのメンバー ポートを追加または削除すると、トポロジ変更が作成されません。

アクセス デバイスはどのタイプにすることもできます。スイッチ、サーバ、ファイアウォール、ロード バランサ、NAS などを使用できます。vPC ドメインに適切に接続するためのアクセス デバイスの要件は、次のとおりです。

- 標準の 802.3ad 機能のサポート（LACP プロトコル）
- スタティック ポート チャネルのサポート（チャネル グループ モード on）

フェールオーバー コンバージェンス時間の短縮および設定ミスの保護に使用可能な場合は、Link Aggregation Control Protocol（LACP）の使用を推奨します。不可能な場合は、手動バンドリング メカニズム（チャネル グループ モード on）を使用してください。

注： Cisco Nexus 7000 シリーズは、ポート集約プロトコル（PAgP）をサポートしません。

NEXUS 7000 は、ポート チャネルのロードバランシング ハッシュ アルゴリズムのさまざまなオプションをサポートします。これはデフォルト VDC でグローバルに設定され、コマンドは **port-channel load-balance** です。

ハッシュ アルゴリズムに使用できるフィールドは次のとおりです。

- Ip　　IP
- ip-l4port　　IP および L4 ポート
- ip-l4port-vlan　　IP、L4 ポート、および VLAN
- ip-vlan　　IP および VLAN
- l4port　　L4 ポート
- mac　　MAC

これらは送信元フィールドとしてのみ、宛先フィールドとしてのみ、または送信元と宛先フィールドとして選択できます。

一般的な推奨事項:

- グレースフル フェールオーバーおよび設定ミスの保護に使用可能な場合は LACP を使用してください。
- LACP モードのアクティブ-アクティブ（ポート チャネルの両端で）が推奨設定です。それ以外の場合、LACP モードのアクティブ-パッシブを使用します。アクティブ-アクティブ モードのポート チャネルはアクティブ-パッシブ モードのポート チャネルよりも迅速に開始されます。
- アクセス デバイスが LACP をサポートしていない場合、手動バンドリング メカニズム（チャネル グループ モード on）を使用してください。
- ダウンストリーム アクセス スイッチが Cisco Nexus デバイスの場合、LACP graceful-convergence オプションをイネーブルにします（このオプションはデフォルトでオンになっています）。
- ダウンストリーム アクセス スイッチが Cisco Nexus デバイスでない場合は、LACP graceful-convergence オプションをディセーブルにします。
- 送信元/宛先 IP、L4 ポート、および VLAN をポート チャネルのロードバランシング ハッシュ アルゴリズムのフィールドとして使用します。これにより、ポート チャネルを形成するすべてのメンバー ポートの公平な使用状況を改善します。

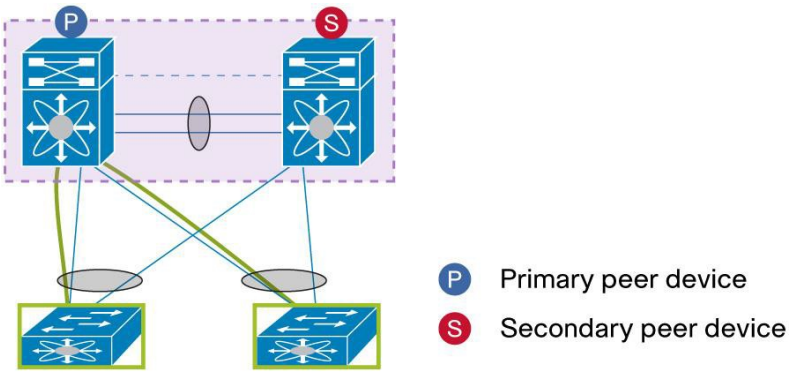
次の項では、vPC ドメインにアクセス デバイスまたはエンド ポイントを接続するすべての方法を示します。

vPC ドメインにデュアル接続されたアクセス デバイス

（図 29 に示すように）ポート チャネルのメンバー ポートの半分を使用してピア デバイス 1 に接続し、残り半分のメンバー ポートを使用してピア デバイス 2 に接続する vPC ドメインに接続されたアクセス デバイスは、vPC テクノロジーを使用する自然な方法です。

vPC ドメインへの接続を処理する場合、これが最も推奨する方法になります。

図 29. vPC ドメインにデュアル接続されたアクセス デバイス



ポート チャネルを使用してアクセス デバイスを vPC ドメインにデュアル接続すると、次の利点が得られます。

- ピア リンク フェールオーバーの場合に中断が最小限になり、vPC のデュアル アクティブ シナリオの一貫した動作が提供されます。
- vPC を介して完全に冗長なアクティブ-アクティブ パスを確保します。

このマニュアルでは、「アクセス デバイスのデュアル接続」は、「アクセス デバイスの vPC 接続」とも呼ばれます。

推奨事項:
可能な場合は、ポート チャネルを使用して常にアクセス デバイスを vPC ドメインにデュアル接続してください。

16 方向のポート チャネルを使用したシングルサイド vPC

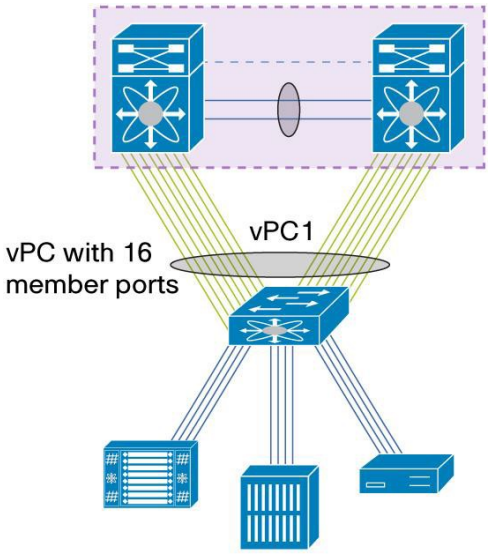
16 方向のポート チャネルを使用したシングルサイド vPC は、vPC ドメインにデュアル接続されたアクセス デバイスの特定の実装です。このような設計では、アクセス デバイスの最大ポート チャネル機能を利用します。

16 ポートのポート チャネルをサポートする Cisco Nexus 5000 は、Cisco NX-OS Software Release 4.1(3)N1(1a) で導入されました。これは 16 方向のポート チャネル トポロジを使用したシングルサイド vPC の基礎になります（図 30 はこの設定を示しています）。

16 方向のポート チャネル トポロジを使用したシングルサイド vPC には次の特性があります。

- アクセス デバイスは、16 のアクティブなメンバー ポートを使用したポートチャネルをサポートします。
- 各 vPC ピア デバイスには 8 個のアクティブ リンクで構成された vPC メンバー ポートがあり、ペア（つまり vPC）にはダウンストリーム デバイスへの 16 のアクティブなロード バランシング リンクがあります。
- vPC メンバー ポートは Cisco Nexus M1、F1、または F2 シリーズ ラインカードから選択できます。
- ノースバウンドからサウスバウンドへのトラフィックでは、サウスバンド デバイスへの一意のパスが vPC ピア リンクのみを経由する場合を除き、vPC ピア デバイスは vPC メンバー ポートから**ローカル** ロードバランシングを常に実行します。

図 30. 16 方向のポート チャネルを使用したシングルサイド vPC



32 方向のポート チャネルを使用したダブルサイド vPC

32 方向のポート チャネルを使用したダブルサイド vPC は、vPC ドメインにデュアル接続されたアクセス デバイスの 2 番目の特定の実装です。このような設計では、vPC ドメインを形成するアクセス デバイスの最大ポートチャネル機能を利用します。

ダブルサイド vPC は、vPC ドメインを形成する 2 台のアクセス レイヤ スイッチが大きい fat の vPC（最大 32 のメンバー ポート）を使用して別の vPC ドメインを形成する 2 台の集約レイヤ スイッチに接続される構成です。

図 31 に、32 方向のポート チャネル トポロジを使用したダブルサイド vPC を示します。

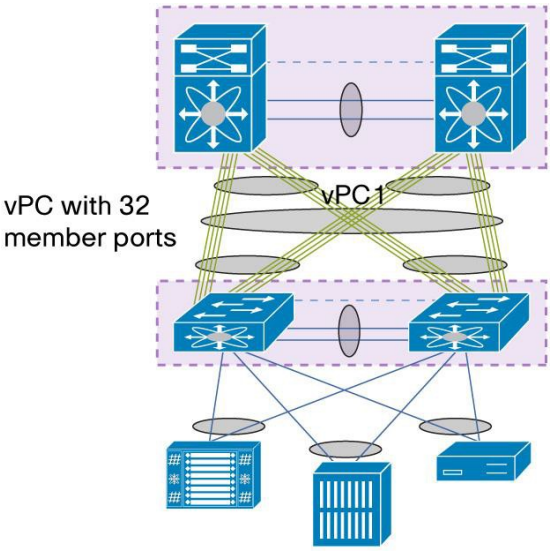
上部の vPC ドメインは通常、集約レイヤ（L2/L3 境界）として使用されます。

下部の vPC ドメインは通常、アクセス レイヤ（L2 のみ）として使用されます。

32 方向のポート チャネル トポロジを使用したダブルサイド vPC には次の特性があります。

- 集約レイヤの各 vPC ピアには 16 のアクティブ リンクで構成された vPC メンバー ポートがあり、ペア（つまり vPC）には 32 のアクティブなロード バランシング リンクがあります。
- F1 と F2 シリーズ ラインカードのみが 16 方向のアクティブなポート チャネル ロード バランシングをサポートします。そのため、vPC ピア デバイスには、これらのモジュールのいずれかを搭載する必要があります（M1 シリーズ ラインカードでは、ポート チャネル内で最大 8 個のメンバー ポートのみサポートされます）。
- ノースバウンドからサウスバウンドおよびその反対方向のトラフィックでは、サウスバウンド/ノースバウンド デバイスへの一意のパスが vPC ピア リンクのみを経由する場合を除き、vPC ピア デバイス（アクセス レイヤまたは集約レイヤ）は vPC メンバー ポートから**ローカル** ロードバランシングを常に実行します。

図 31. 32 方向のポート チャネルを使用したダブルサイド vPC

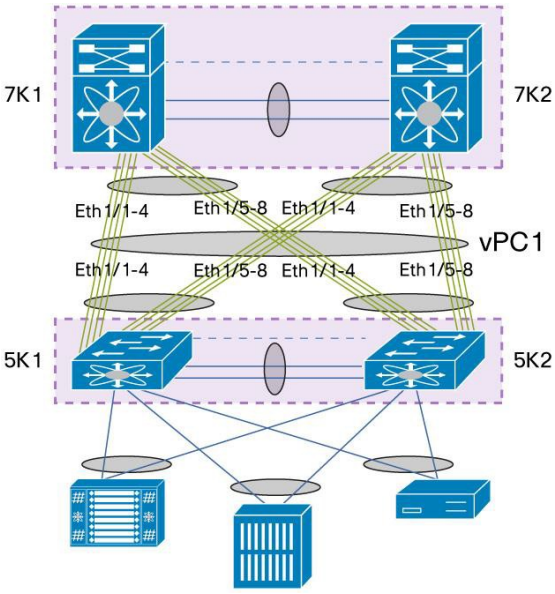


ダブルサイド vPC の設定例:

ここでは、集約レイヤの両方の NEXUS 7000 デバイスとアクセス レイヤの両方の NEXUS 5000 デバイスのダブルサイド vPC を設定する方法を示します。

設定例のポート接続を、図 32 に示します。

図 32. ダブルサイド vPC の設定例



7K1 configuration:

```
interface port-channel1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1000-1100
  vpc 1

interface Ethernet1/1-4
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1000-1100
  channel-group 1 mode active
  no shutdown

interface Ethernet1/5-8
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1000-1100
  channel-group 1 mode active
  no shutdown


! vPC peer-link
interface port-channel10
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1000-1100
  spanning-tree port type network
  vpc peer-link
```

7K2 configuration:

```
interface port-channel1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1000-1100
  vpc 1

interface Ethernet1/1-4
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1000-1100
```

```
  channel-group 1 mode active
  no shutdown

interface Ethernet1/5-8
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1000-1100
  channel-group 1 mode active
  no shutdown


! vPC peer-link
interface port-channel10
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1000-1100
  spanning-tree port type network
  vpc peer-link
```

5K1 configuration:

```
interface port-channel1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1000-1100
  vpc 1

interface Ethernet1/1-4
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1000-1100
  channel-group 1 mode active
  no shutdown

interface Ethernet1/5-8
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1000-1100
  channel-group 1 mode active
  no shutdown
```

```
! vPC peer-link
interface port-channel10
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1000-1100
  spanning-tree port type network
  vpc peer-link
```

```
5K2 configuration:

interface port-channel1

  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1000-1100
  vpc 1
interface Ethernet1/1-4

  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1000-1100
  channel-group 1 mode active
  no shutdown
interface Ethernet1/5-8

  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1000-1100
  channel-group 1 mode active
  no shutdown

! vPC peer-link
interface port-channel10
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1000-1100
  spanning-tree port type network
  vpc peer-link
```

設定に関するダブルサイド vPC の特性は次のとおりです。

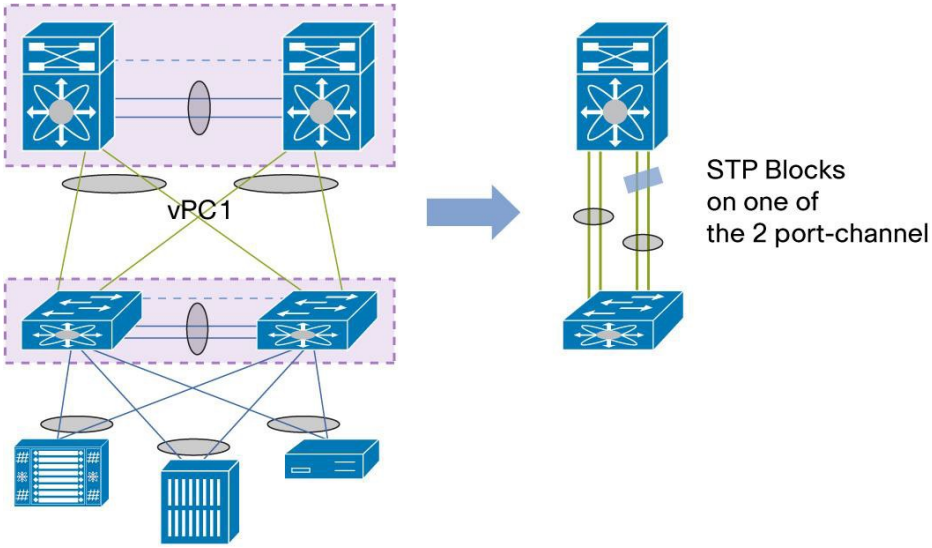
アクセス レイヤの vPC ピア デバイスから集約レイヤの vPC ドメインまでのすべてのポートは同じポート チャネルに属します。

集約レイヤの vPC ピア デバイスからアクセス レイヤの vPC ドメインまでのすべてのポートは同じポート チャネルに属します。

設定および動作を簡易化するためのベスト プラクティスは、相互接続リンクの両方の vPC ドメインで同じポート チャネル ID と同じ vPC ID を使用することです（つまり、2 つの vPC ドメインの中央にある vPC）。

ダブルサイド vPC トポロジについてよくある間違いの 1 つは、図 33 に示すように、アクセス レイヤの vPC ドメインでポート チャネルの作成を忘れることです。

図 33. ダブルサイド vPC トポロジの正しくない設定



アクセス レイヤの vPC ドメインではなく集約レイヤの vPC ドメインでポート チャネルを作成すると、2 つの別々のポート チャネルが 2 つのレイヤを相互接続するトポロジになります。この場合、スパニングツリー プロトコルはネットワーク ループを検出し、次に 2 つのポートチャネルの 1 つをブロックします。

必須の推奨事項:
ダブルサイド vPC トポロジでは、2 つの vPC ドメイン間のすべての相互接続リンクが同じ vPC に属します。すべてのリンクは(2 つの vPC ドメインの両側に)一意の vPC を形成します。VPC ID は 2 つの vPC ドメイン全体で異なる場合があります。ただし、vPC ID は、同じドメイン内の 2 台のピア デバイスで同じである必要があります。

vPC ドメインにシングル接続されたアクセス デバイス

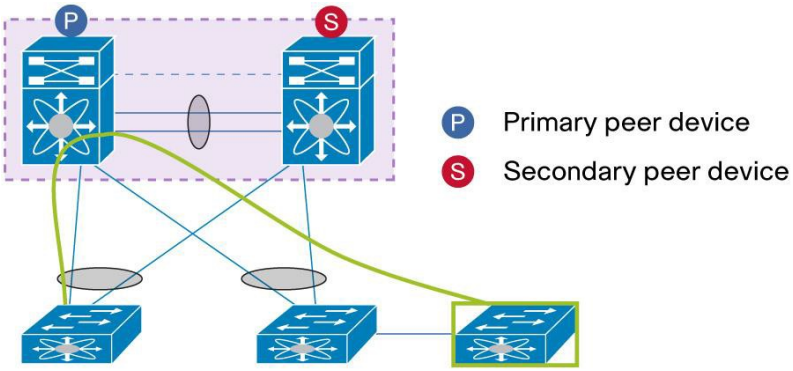
vPC ドメインにデバイスをデュアル接続できない場合は、主に 3 つの代替手段があります。優先順位の高い順にそれらの代替手段について説明します。

デュアル接続がオプションでない場合に最適な代替手段は、vPC 接続されたアクセス スイッチを使用してデバイスを接続することです(図 34)。このアプローチの利点は、ピア リンクのフェールオーバー時に中断が最小限になり、vPC のデュアル アクティブ シナリオの一貫した動作が提供されることです。

vPC 接続されたアクセス スイッチを使用してアクセス デバイスを接続する場合、2 つ欠点があります。

- 追加のアクセス スイッチを使用する必要があります(外部デバイスまたは VDC のインスタンスにすることができます)
- VDC の場合は、物理デバイスまたは仮想デバイスを設定および管理する管理上の負担が大きくなります。

図 34. vPC 接続されたアクセス スイッチを介して接続されたアクセス デバイス



中間 vPC 接続スイッチまたは VDC を使用できない場合、次に最適な代替手段は、非 vPC VLAN を使用してデバイスを vPC ピア デバイスに接続し（定義では、非 vPC VLAN はどの vPC にも vPC ピア リンクにも存在しない VLAN）、これらの非 vPC VLAN を伝送するための専用のスイッチ間ポート チャネルを作成することです（図 35）。

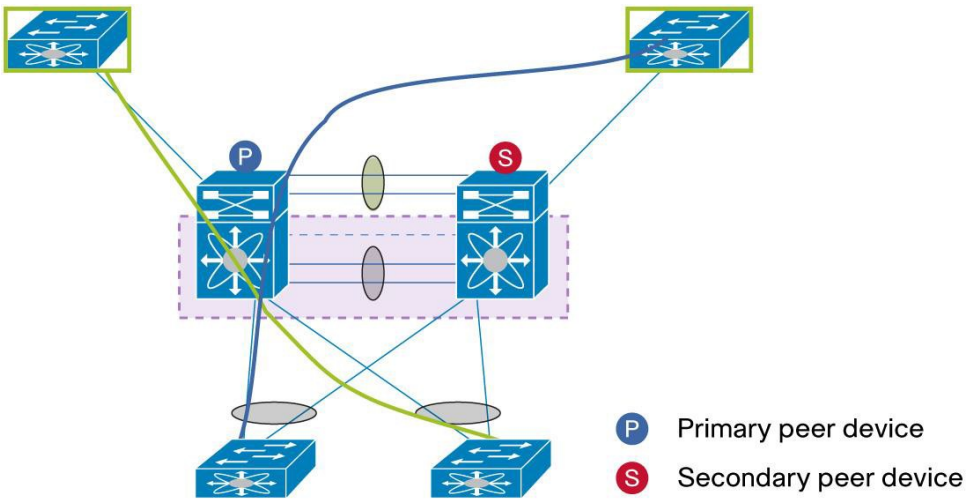
アクセス デバイスはプライマリ ピア デバイスまたはセカンダリ ピア デバイスに接続できます。vPC ピア リンクに障害が発生した場合、専用のスイッチ間ポート チャネルがバックアップ パスを保証するため、重要ではありません。

このアプローチの利点は、セカンダリ ピア デバイスに接続されたデバイスの分離を避けて、ピア リンクのフェールオーバー時にセカンダリ パスでトラフィックが転送される点です。

欠点は、Cisco Nexus 7000 シリーズ デバイス間の追加のポート チャネルを設定および管理する必要があることです。

非 vPC VLAN から vPC VLAN への通信は、2 つの VLAN が別のブリッジング ドメインに属する場合、VLAN 間ルーティングを使用して実行する必要があります。

図 35. 非 vPC VLAN を使用して vPC ドメインにシングル接続されたアクセス デバイス

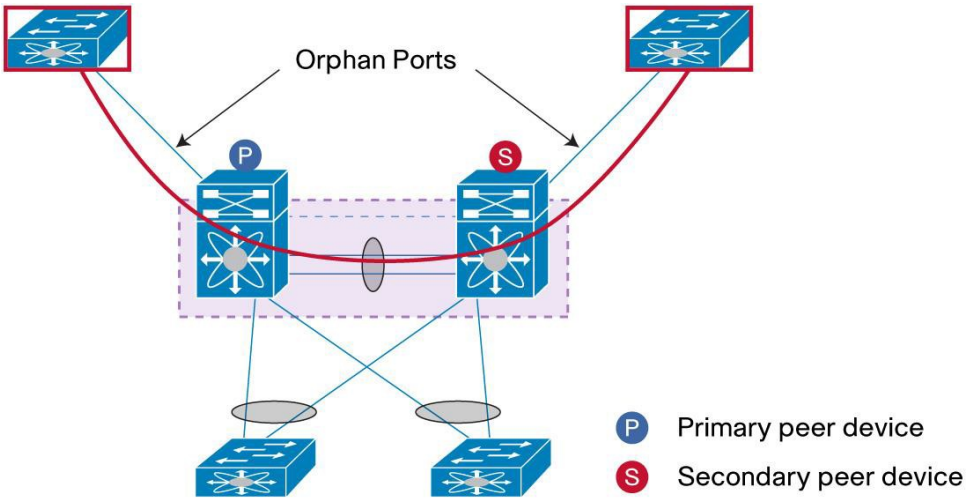


最後に、vPC ドメインにアクセス デバイスを接続するために非 vPC VLAN を使用しない場合（および、2 台のピア デバイス間で追加のスイッチ間リンクを作成しない場合）、vPC VLAN および vPC ピア リンクを使用してプライマリ ピア デバイスにアクセス デバイスを接続できます（図 36）。

この方法の利点は、導入の相対的な容易さです（プロビジョニングする新しい VLAN や追加する新しい追加スイッチ間リンクがありません）。

vPC でロールのプリエンプションが行われないため、この方法では、vPC ドメインが vPC ロールにバインドされます。その結果、動作可能なセカンダリ ピア デバイスに接続されたアクセス デバイスは、ピア リンクの障害時に完全に隔離されます。

図 36. vPC VLAN を使用して vPC ドメインにシングル接続アクセス デバイス



この特定のトポロジには孤立ポートの概念が導入されています。

vPC VLAN を使用してこれらのシングル接続デバイスに接続された Cisco Nexus 7000 シリーズ ポートは、孤立ポートと呼ばれます。

孤立ポートには次の特性があります。

- シングル接続デバイスに接続されている vPC ピア デバイス（プライマリまたはセカンダリ）のポート。
- vPC VLAN を伝送する vPC ピア デバイス（プライマリまたはセカンダリ）のポート。ポートが非 vPC VLAN を伝送している場合、孤立ポートとこれ以上定義されません。

vPC ピア デバイス上のすべての孤立ポートを表示するには、**show vpc orphan-ports** コマンドを使用します。このコマンドのサンプル出力を次に示します。

```
7K1# sh vpc orphan-ports
（注）
--------::Going through port database. Please be patient.::--------

VLAN            Orphan Ports
-------         -------------------------
11              Eth3/23
```

```
23              Eth3/21
50              Eth3/14
600             Eth1/41, Eth1/48
```

この例では、VLAN 11、23、50、600 は vPC VLAN です（したがって、その vPC ピア リンクにも定義されます）。

一般的な推奨事項：
シングル接続アクセス デバイスを vPC VLAN を使用して vPC ドメインに接続する場合は、vPC プライマリ ピア デバイスにそれを常に接続します。理由は、vPC ピア リンクがダウンした場合、（vPC VLAN を使用して）セカンダリ ピア デバイス接続されたシングル接続デバイスは、ネットワークの他の部分と完全に隔離されます。

この項（vPC ドメインへのシングル接続デバイス）の結論は次のとおりです。

一般的な推奨事項（優先順位の降順）：

- vPC ドメインにデュアル接続された中間スイッチにアクセス デバイスを接続します
- 非 vPC VLAN を使用して vPC ドメインにシングル接続デバイスを接続します。2 台のピア デバイス間にスイッチ間リンクを作成して非 vPC VLAN を転送します。
- vPC VLAN および vPC ピア リンクを使用して vPC ドメインにシングル接続デバイスを接続します。

vPC ドメインに STP 接続されたアクセス デバイス

アクセス デバイスがスパニングツリー プロトコル（STP）をサポートし、vPC ドメインに接続する必要がある場合は、「vPC ドメインにシングル接続されたアクセス デバイス」の項と同じ推奨事項に従うだけです。

前の状況と同様に、STP 接続されたアクセス デバイスを vPC ドメインに接続する 2 つのオプションがあります。

オプション 1：
スパニングツリー プロトコルを使用して 2 つの独立したリンク経由でアクセス デバイスを接続します。スパニングツリー プロトコルのスイッチだけで非 vPC VLAN を使用します。同じ STP モードを vPC ドメインとして実行し（RVPST または MST）、ホスト側のポート上でポート タイプ エッジ（つまり、PortFast）またはポート タイプ エッジ トランク（アクセス ポートがハイパーバイザ サーバに接続されている場合）をイネーブルにします。2 台のピア デバイス間に追加のスイッチ間リンクを挿入して非 vPC VLAN を伝送します。

このベスト プラクティスの利点は、ピア リンクのフェールオーバーの場合に、中断が最小限になり、vPC デュアル アクティブ シナリオの一貫した動作が提供されることです。また、vPC VLAN で完全に冗長なアクティブ-アクティブ パスを確保するのに役立ちます。

欠点は 2 台の vPC ピア デバイス間で追加のスパニングツリー プロトコルのポート チャネルを必要とすることです。

個別の STP および vPC VLAN インスタンスをプロビジョニングおよび設定するときに操作上の負荷もかかります。スパニングツリー プロトコル VLAN にはアクティブ-スタンバイ パスのみ存在します。

オプション 2：
スパニングツリー プロトコルを使用して 2 つの独立したリンク経由でアクセス デバイスを接続します。このスイッチで vPC VLAN を使用します。同じ STP モードを vPC ドメインとして実行し（RVPST または MST）、ホスト側のポート上でポート タイプ エッジ（つまり、PortFast）またはポート タイプ エッジ トランク（アクセス ポートがハイパーバイザ サーバに接続されている場合）をイネーブルにします。

vPC ピア リンクがアクセス デバイスから vPC VLAN を伝送するのに再利用されるため、2 台の vPC ピア デバイス間に追加のスイッチ間リンクを挿入する必要はありません。

このベスト プラクティスは VLAN のプロビジョニングを簡素化し（新しい VLAN を作成する必要はありません）、さらに 10 ギガビット イーサネット ポート チャネルを割り当てる必要はありません。欠点は、STP 転送リンクがセカンダリ ピア デバイスに接続され、ピア リンクがダウンした場合に、ネットワークの他の部分にアクセス デバイスが隔離される可能性があることです。そのため、オプション 2 では、ベスト プラクティスは、vPC プライマリ ピア デバイスにフォワーディング ステートの STP ポートを接続することです。

一般的な推奨事項（優先順位の降順）：

- 非 vPC VLAN を使用して vPC ドメインに STP 接続デバイスを接続します。2 台のピア デバイス間にスイッチ間リンクを作成して非 vPC VLAN を転送します。
- vPC VLAN および vPC ピア リンクを使用して vPC ドメインに STP 接続デバイスを接続します。vPC プライマリ ピア デバイスにフォワーディング ステートの STP ポートを常に接続します。

データセンター インターコネクトおよび暗号化のベスト プラクティス

データセンター インターコネクト（DCI）は、ほとんどの会社がハイ アベイラビリティおよび業務運用を向上させるために少なくとも 2 つの異なるデータセンターを構築するため、ますます普及しています。DCI の目的は、異なるデータセンターに特定の VLAN を拡張して、サーバと NAS デバイスについて複数マイル離れた L2 隣接関係を提供します。

複数のテクノロジーを OTV（Overlay Transport Virtualization）、VPLS（Virtual Private LAN Services）、vPC などの DCI に使用できます。

vPC を最大 2 つのデータセンターの相互接続に使用できます。複数のサイトにわたって VLAN を拡張するために 2 つ以上のデータセンターを相互接続する必要がある場合、推奨事項は OTV を使用することです。

vPC には 2 つのサイト（DCI vPC に BPDU なし）間でスパニングツリーを分離するという利点があるため、1 つのデータセンターの停止は他のデータセンターに伝播されません。

vPC は簡単に設定でき、堅牢で復元力のある相互接続ソリューションを提供します。vPC は、DCI リンク障害および vPC ピア デバイスの障害から保護します。

DCI テクノロジーとしての vPC は、2 通りの方法で導入できます。

- 集約と DCI のためのマルチレイヤ vPC
- デュアル L2/L3 POD 相互接続

最初の設定では、DCI の専用 vPC ドメインは集約レイヤと他のデータセンターの間に挿入されます。

2 番目の設定では、同じ集約 vPC ドメインは 2 つのデータセンターの相互接続に使用されます。

M1 シリーズ ラインカードは、ハードウェアで直接 802.1ae MACsec 暗号化をサポートします。M1 ポートを DCI vPC のメンバー ポートとして使用すると、2 つのデータセンター全体でこのセキュリティ機能を利用できます。フローは、2 つのファシリティ間のネットワーク侵入を使用不可にする相互接続 vPC 内で暗号化されます。

802.1ae MACsec 暗号化を使用するには、LAN のアドバンスト サービス ライセンスが必要です。関連するセキュリティ コマンド（int eth1/1; cts manual; no propagate-sgt; sap pmk <key>）で M1 ポートを設定する前に feature cts をイネーブルにします。

F1 および F2 シリーズ ラインカードはハードウェアの 802.1ae MACsec 暗号化をサポートしていません。

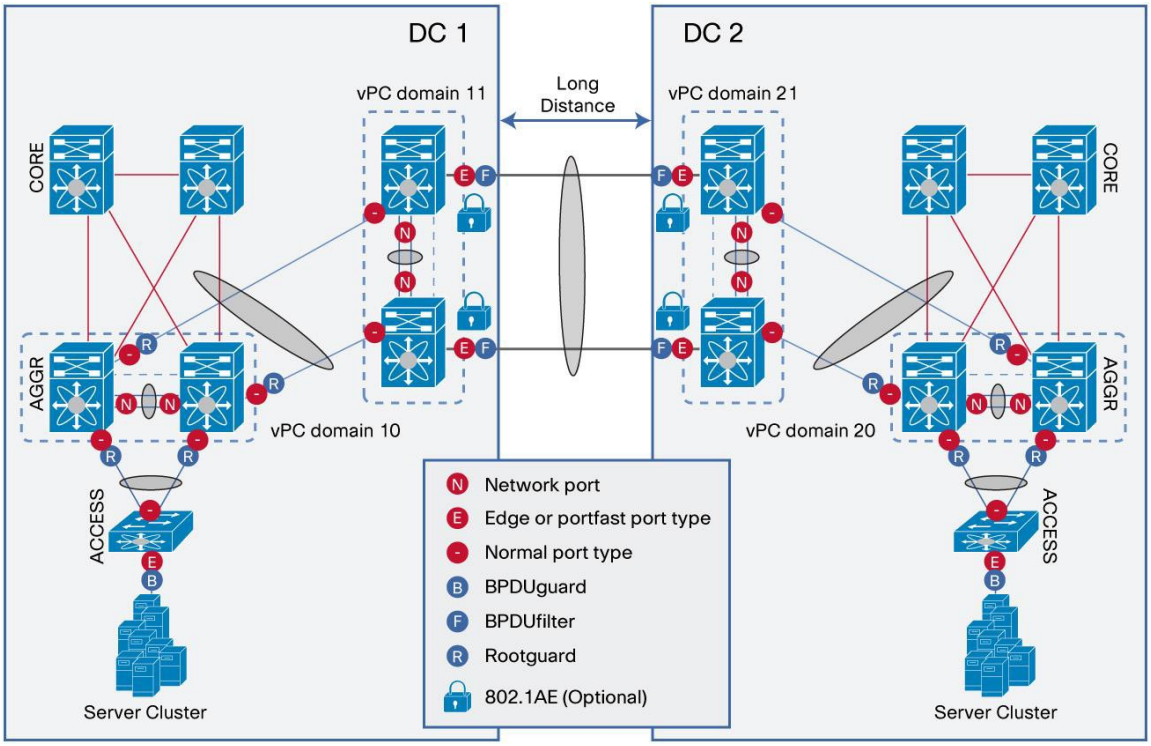
DCI に vPC を使用した HSRP 操作の考慮事項は、「HSRP と vPC のベスト プラクティス」で説明されています。

集約と DCI のためのマルチレイヤ vPC

集約と DCI のマルチレイヤ vPC は、専用 vPC ドメインが DCI の目的で使用されるソリューションです。

1 つの vPC ドメインはサーバ接続に使用され（「集約 vPC ドメイン」と呼ばれる）、他の vPC ドメインは DCI に排他的に使用されます（「DCI vPC ドメイン」と呼びます）。図 37 に示すように、このトポロジは各 vPC ドメインの機能を明確にし、迅速なトラブルシューティングと簡単なモニタリングを可能にします。

図 37. 集約と DCI のためのマルチレイヤ vPC



集約と DCI ソリューションのマルチレイヤ vPC を正常に構築するには、次のガイドラインとベスト プラクティスに従います。

必須の推奨事項:

- vPC ドメインごとに異なる vPC ドメイン ID（DC1：集約用の vPC ドメイン、DCI 用の vPC。DC2：集約用の vPC ドメイン、DCI 用の vPC）を使用します。
- データセンターごとに、vPC を使用して集約 vPC ドメインを DCI vPC ドメインに相互接続します（ダブルサイド トポロジ）。
- vPC（サイト 1 とサイト 2 の DCI vPC ドメイン間の vPC）を使用して 2 つのデータセンターを相互接続します。
- DCI に使用する vPC で BPDU フィルタをイネーブルにして（ポート チャネル設定で、コマンド **spanning-tree bpdufilter enable** を実行）BPDU の伝播を避けます。
- ポートが稼働している場合、ポート ステートの転送モードを固定するために spanning-tree port type edge（つまり PortFast）として DCI に使用する vPC を設定します。
- デフォルトでは、vPC ピア リンクはスパニングツリー ポート タイプ ネットワークで実行されます。つまり、Bridge Assurance はリンク上でアクティブになります。

- 集約 vPC ドメイン上（より正確には、この vPC ドメインと DCI vPC ドメイン間の vPC 上）のルート ガードを設定します。STP ルートはデータセンターの両側の集約 vPC ドメイン上に残す必要があります
- ループは、vPC ドメインの外部に存在していない必要があります
- データセンター間でレイヤ 3 ピアリングを使用しないでください（つまり、vPC 上にレイヤ 3 はありません）
- 相互接続 vPC（DCI vPC）に Bridge Assurance を使用しないでください
- 2 つのデータセンター間のフローを 802.1ae MACsec プロトコルを使用して暗号化する必要がある場合、DCI vPC に M1 ポートを使用します

デュアル レイヤ 2/レイヤ 3 のポッド相互接続

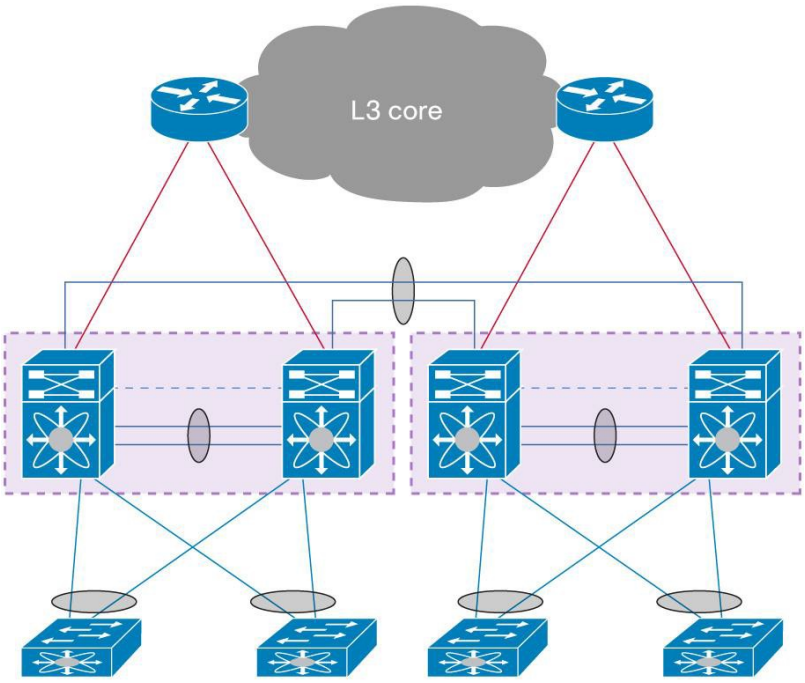
コストと統合が重要な検討事項の場合、DCI vPC ドメインを vPC ドメインで直接結合できます。

デュアル レイヤ 2/レイヤ 3 のポッド相互接続は、同じ設定内の 2 つの機能を提供します。

従来の集約レイヤ機能（L2/L3 境界）および 2 つのデータセンターにまたがる DCI 相互接続を提供します。ブリッジド トラフィックは専用 vPC DCI リンクを使用し、ルーテッド トラフィックは、アップストリーム ルーテッド コアへのインターフェイス VLAN（SVI）と専用レイヤ 3 リンクを使用します。

図 38 は、デュアル レイヤ 2/レイヤ 3 のポッド相互接続トポロジを示します。

図 38. デュアル レイヤ 2/レイヤ 3 のポッド相互接続トポロジ



デュアル レイヤ 2/レイヤ 3 のポッド相互接続トポロジを正しく構築するには、次のガイドラインとベスト プラクティスに従います。

必須の推奨事項:

- vPC ドメインごとに異なる vPC ドメイン ID を使用します
- vPC を使用して 2 つのデータセンターを相互接続します
- DCI に使用する vPC で BPDU フィルタをイネーブルにして（ポート チャネル設定で、コマンド **spanning-tree bpdufilter enable** を実行）BPDU の伝播を避けます。
- ポートが稼働している場合、ポート ステートの転送モードを固定するために spanning-tree port type edge（つまり PortFast）として DCI に使用する vPC を設定します。
- デフォルトでは、vPC ピア リンクはスパニングツリー ポート タイプ ネットワークで実行されます。つまり、Bridge Assurance はリンク上でアクティブになります。
- DCI の vPC にルート ガードを設定します。STP ルートはデータセンターの両側でローカルのままにする必要があります。
- ループは、vPC ドメインの外部に存在していない必要があります
- データセンター間でレイヤ 3 ピアリングを使用しないでください（つまり、vPC 上にレイヤ 3 はありません）
- 相互接続 vPC（DCI vPC）に Bridge Assurance を使用しないでください
- 2 つのデータセンター間のフローを 802.1ae MACsec プロトコルを使用して暗号化する必要がある場合、DCI vPC に M1 ポートを使用します

スパニングツリー プロトコルの相互運用性のベスト プラクティス

ここでは、vPC とのスパニングツリー プロトコル相互運用性のベスト プラクティスについて説明します。

vPC とのスパニングツリー プロトコル相互運用性について

vPC テクノロジーを使用すると、アクセス デバイスから vPC ドメインへのポート チャネルでループ フリー トポロジを構築できます。ポート チャネルは、STP の観点から論理リンクと見なされるため、vPC 接続アクセス デバイスを含む vPC ドメインは L2 のスタートポロジをグローバルに形成します（このタイプのトポロジに STP ブロック ポートはありません）。その場合、人為ミス（2 台の vPC ピア デバイスをループバック ケーブルを接続するなど）に起因するネットワーク ループを保護するために、フェールセーフ メカニズムとして STP が使用されます。

前に示したように、vPC ドメインへのあらゆる種類の接続が完全にサポートされます。従来の vPC 接続に加えてシングル接続アクセス デバイスや STP 接続アクセス デバイスがあります。

最初の 2 つの接続モードの場合は、再びネットワークでのループを回避して、L2 パスの決定に STP がアクティブに含まれている必要があります。

したがって、アクセス デバイスと vPC ドメイン間の接続タイプに応じて、ループフリー L2 パスを構築するために STP を多少使用する必要があります。

論理ポートの考慮事項は、vPC のコンテキストでも STP に適用されます。ただし、論理ポート数は計算が vPC メンバー ポート（つまりポート チャネル）について実行され、個々 のリンクについては実行されません。STP はポート チャネルを一意の論理リンクと見なします。

RPVST（Rapid Per VLAN Spanning Tree）は 16,000 論理ポートを、MST（Multiple Spanning Tree）は最大 90,000 個の論理ポートをサポートします。

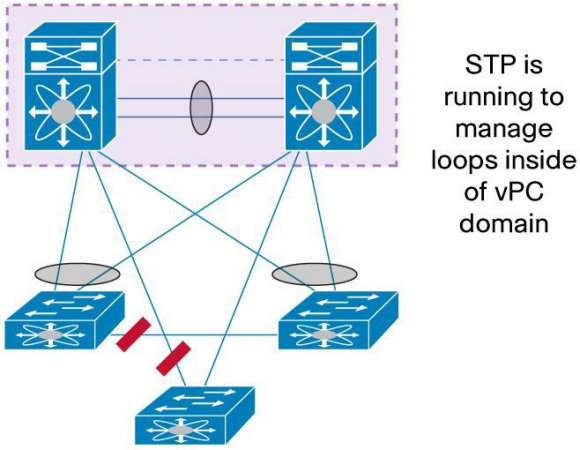
vPC ドメイン内でのスパニングツリー プロトコルの役割

vPC テクノロジーのコンテキストでは、スパニングツリー プロトコルは次の機能を提供します。

- 検出およびループの切断によって L2 ネットワークを保護します
- 非 vPC 接続デバイス（つまり、シングル接続デバイスまたは STP 接続装置）のレイヤ 2 パスを決定します
- vPC の追加または取り外しのループ管理（vPC に関連する特定のネットワーク設定イベント時の L2 ループを回避します）

図 39 では vPC ドメイン内の、または最初の vPC 設定前のループを管理するために、スパニングツリー プロトコルが実行中です。スパニングツリー プロトコルは、デバイスが vPC ドメインにシングル接続されている場合でもアクティブに動作しています。

図 39. vPC ドメイン内の STP の役割



vPC で推奨されるスパニングツリー プロトコル設定

次のグローバル パラメータおよびインターフェイス設定に同一のスパニングツリー プロトコル設定を使用して vPC の両端を設定することを推奨します。

グローバル パラメータ:

- STP モード（RPVST または MST）
- MST のための STP リージョン設定
- VLAN ごとのイネーブル/ディセーブル状態
- ブリッジ保証設定
- STP ポート タイプの設定（すべてのアクセス ポートのエッジ ポート タイプをデフォルトでイネーブルまたはディセーブルにします）
- ループ ガードの設定（すべてのポートのループ ガードをデフォルトでイネーブルまたはディセーブルにします）
- BPDU ガードの設定（すべてのエッジ ポートの BPDU ガードをデフォルトでイネーブルまたはディセーブルにします）
- BPDU フィルタの設定（すべてのエッジ ポートの BPDU フィルタをデフォルトでイネーブルまたはディセーブルにします）

インターフェイスの設定：

- STP ポート タイプの設定（エッジ、ネットワーク、標準）
- ループ ガード（イネーブルまたはディセーブル）
- ルート ガード（イネーブルまたはディセーブル）

注： これらのパラメータのいずれかの設定を誤ると、Cisco NX-OS ソフトウェアは、vPC 上のすべてのインターフェイスを停止します（これは、タイプ 1 整合性検査エラーです）。NX-OS 5.2 および vPC グレースフル整合性検査機能の導入以降、セカンダリ ピア デバイスのみ vPC でインターフェイスを停止します。プライマリ ピア デバイスは、vPC メンバー ポートの稼働および動作ステートを保持します。

vPC メンバー ポートが一時停止されると、syslog メッセージが送信されます。**show vpc brief** コマンドは、vPC ステートのステータスを示します。

トラフィック フローにおける予測できない動作を回避するには、次のスパニングツリー プロトコルのインターフェイス コンフィギュレーションが、vPC の両側で同じであることを確認します（これは、タイプ 2 整合性検査エラーです）。

- BPDU フィルタ
- BPDU ガード
- STP コスト（STP ポート パス コスト）
- STP リンク タイプ（自動、ポイントツーポイント、共有）
- STP プライオリティ（STP ポート プライオリティ）
- VLAN

次のコマンドを使用して、vPC の両側の設定を表示し、それらの設定が同じであることを確認してください。
sh run int port-channel <id> membership

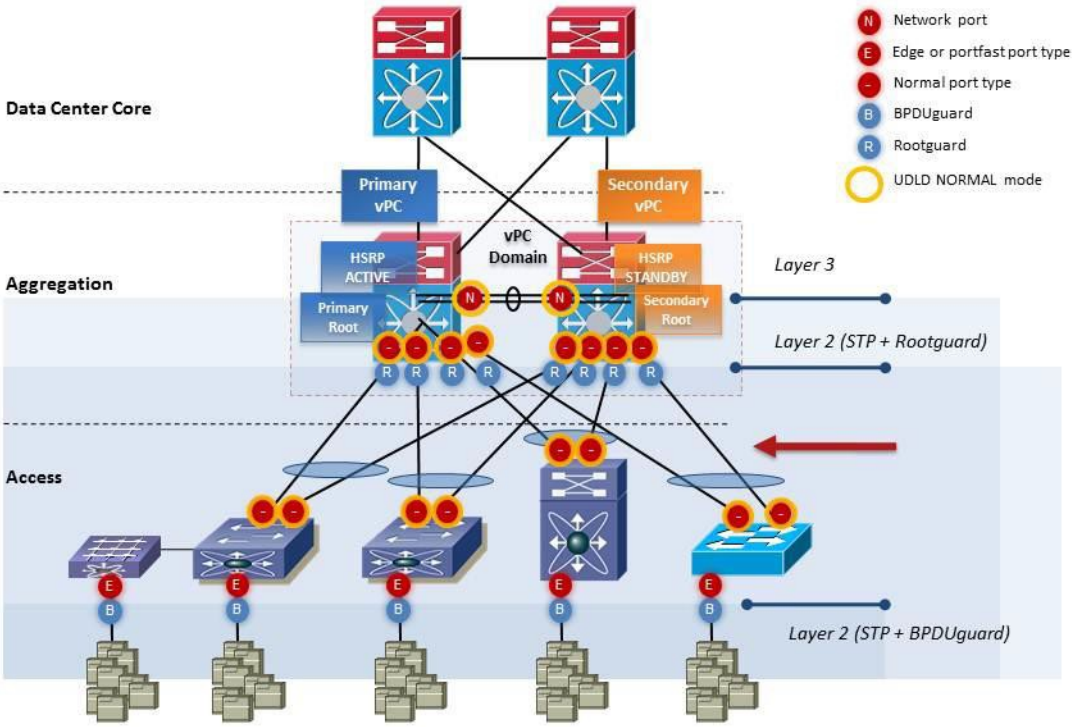
強力な推奨事項：

- （すべてのアクセス デバイスが vPC ドメインに vPC 接続されている場合でも）スパニングツリー プロトコルがすべての VLAN でイネーブルになっている必要があります。スパニングツリー プロトコルをディセーブルにしないでください。
- 大規模な L2 ドメインを作成する必要がある場合は、vPC で MST を使用します。vPC タイプ 1 整合性エラーをトリガーできる将来の設定変更を避けることを事前に計画します（グローバルなタイプ 1 パラメータのサンプルには、MST リージョン設定、STP モード、STP グローバル コンフィギュレーションが含まれます）。
- 同じ L2 ドメインに一貫した STP モードを実装します。遅いスパニングツリー プロトコル コンバージェンス（30 秒以上）を回避するために、レイヤ 2 ドメイン内のすべてのスイッチが、Rapid-PVST+ または MST を使用して動作していることを確認します。
- 内部リソースの消費を減らすために vPC メンバー ポート上で VLAN プルーニングを実行します。

vPC との STP 相互運用性：ブループリント図

次のブループリント図（図 40）は、vPC で推奨されるスパニングツリー プロトコルのポート設定を示しています。

図 40. スパニングツリー プロトコルおよび vPC：ポート設定の推奨事項



強力な推奨事項：

- ネットワークの集約レイヤ（集約 vPC ドメイン）にスパニングツリー プロトコルのルート機能を保持します。
- vPC ピア デバイスごとに、アクセス デバイスに接続されたポートのルート ガードを設定します。
- Bridge Assurance は、vPC ピア リンクを設定するとデフォルトでイネーブルになります。vPC ピア リンクでディセーブルにしないでください。
- vPC で Bridge Assurance をイネーブルにする必要はありません（vPC メンバー ポートがスパニングツリー ポート タイプ ネットワークとして定義されている場合、Bridge Assurance はイネーブルになります）。
- vPC メンバー ポートを spanning-tree port type normal で設定します（リンク上で Bridge Assurance を使用しません）。
- ポートがアップ ステートに遷移するときの遅いスパニングツリー プロトコル コンバージェンス（30 秒以上）を回避するために、ホスト方向のインターフェイスに PortFast（エッジ ポート タイプ）を設定します。
- ホスト方向のインターフェイスに BPDU ガードを設定して、ホストから送信された BPDU をブロックします（BPDU を受信しているアクセス スイッチ ポートは errdisable モードになります）。

vPC およびスパニングツリー プロトコルのブリッジ プロトコル データ ユニット

vPC はデュアル アクティブ コントロール プレーンを維持し、スパニングツリー プロトコルは両方のスイッチで動作します。

vPC テクノロジーと相互運用するために、STP 実装は、デュアル ペアのデバイス構成で動作するように適応しています。

vPC ポートでは vPC プライマリ スイッチだけが、これらの vPC ポートの STP トポロジを実行します。つまり、vPC のスパニングツリー プロトコルは vPC プライマリ ピア デバイスによって制御され、このデバイスだけがスパニングツリー プロトコルの指定ポートでブリッジ プロトコル データ ユニット（BPDU）を生成し、送信します。これは、指定されたスパニングツリー プロトコルのルートの場所に関係なく行われます。

セカンダリ vPC スイッチの STP をイネーブルにする必要がありますが、vPC メンバー ポート ステートを示すものではありません。

vPC セカンダリ ピア デバイスは、プライマリ vPC ピア デバイスにアクセス スイッチから受信したスパニングツリー プロトコル BPDU メッセージをプロキシします（図 41）。

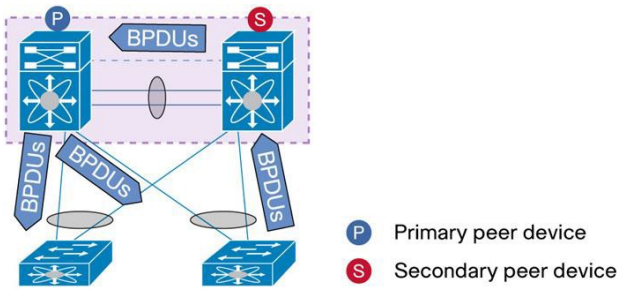
両方のピア デバイスの vPC メンバー ポートは両方とも同じ STP ポート ステート（安定したネットワークの FWD ステート）を常に共有します。

デフォルトでは、STP 実装は（vPC のコンテキストで）独自の bridgeID 値を使用して各 vPC ピア デバイスを割り当てます。vPC ドメインが通常ドメイン内のすべての VLAN の STP ルートであるため、rootID 値はプライマリ ピア デバイスまたはセカンダリ ピア デバイスの bridgeID と同じです。

強力な推奨事項:

- vPC ドメインをそのドメイン内のすべての VLAN の STP ルートとして必ず定義します（STP ルート プライマリおよび STP ルート セカンダリとして集約 vPC ピア デバイスを設定します）。
- 別の L2 スイッチに接続されている vPC ピア デバイス ポート上に STP ルート ガードを実装することによって、このルールを適用します。

図 41. vPC およびスパニングツリー プロトコル BPDU



vPC ドメインに接続されたアクセス スイッチについては、次のガイドラインとベスト プラクティスに従います。

強力な推奨事項:

- STP ポート タイプ「エッジ」およびホスト ポートのポート タイプ「エッジ トランク」をイネーブルにします
- STP BPDU-guard をグローバルにイネーブルにします
- アクセス スイッチでサポートされている場合、STP channel-misconfig ガードをディセーブルにします
- vPC でループ ガードをイネーブルにしないでください（デフォルトではディセーブル）
- vPC で Bridge Assurance をイネーブルにしないでください

操作および迅速な診断を簡易化するために、次の推奨事項が vPC のコンテキストで STP に適用されます。

一般的な推奨事項:

- vPC プライマリ デバイスのすべての VLAN についてスパニングツリー プロトコル ルートを設定します（spanning-tree vlan 100-102 root primary）。
- vPC セカンダリ デバイスのすべての VLAN についてスパニングツリー プロトコル セカンダリ ルートを設定します（spanning-tree vlan 100-102 root secondary）。

vPC ピア リンクは、STP の通常ポートです。

ただし、vPC は、このリンクが CFSoE などの重要なトラフィックを伝送するため、ピア リンクをブロックしないルールを課します。結果として、ピア リンクは常に、そのリンクのメンバーになっているすべての VLAN に対して転送します。

ユーザが（キーワード「vpc peer-link」を追加して）vPC ピア リンクとしてポート チャネルを設定すると、システムは自動的にリンク上で Bridge Assurance をオンにします。Bridge Assurance は物理ケーブル障害または隣接スイッチのコントロールプレーンの障害に起因する任意の単方向リンク イベントから L2 ネットワークを保護する STP 拡張機能です。

強力な推奨事項:

- vPC ピア リンク（デフォルト モード）で Bridge Assurance を実行し、Bridge Assurance をディセーブルにしないでください。
- vPC メンバー ポート上で Bridge Assurance をイネーブルにしないでください。

vPC ピア スイッチ

NX-OS 4.2(6)、5.0(2a) 以降、vPC のコンテキストで、vPC ピア スイッチと呼ばれる拡張機能が STP に導入されました。

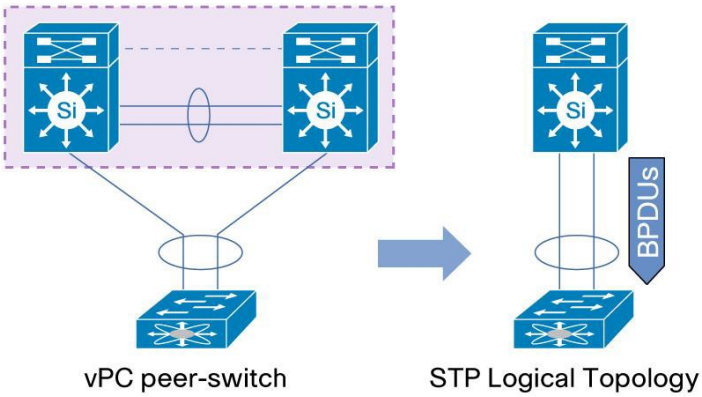
vPC ピア スイッチ機能（図 42）を使用すると、vPC ピア デバイスのペアをレイヤ 2 トポロジの単一スパニングツリー プロトコルのルートとして表示できます（同一のブリッジ ID があります）。vPC ピア スイッチは、両方の vPC ピア デバイス上で動作可能になるように設定する必要があります。コマンドは次のとおりです。

N7K(config-vpc-domain)# **peer-switch**

この機能により、同じスパニングツリー プロトコルのプライオリティで両方のピア デバイスの vPC VLAN を設定することによって、スパニングツリー プロトコルの設定が簡素化されます。vPC ピア スイッチでは vPC プライマリ ピア デバイスにスパニングツリー プロトコルのルートをマッピングする必要性がなくなります。

vPC ピア スイッチの主な利点は、vPC プライマリ ピア デバイスの障害およびリカバリ中のコンバージェンス時間が改善されることです。vPC ピア スイッチ機能がないと、vPC プライマリ ピア デバイスの障害とリカバリは、通常、約 3 秒間トラフィックが中断します（サウスバウンドからノースバウンドへのトラフィックの場合）。vPC ピア スイッチを使用すると、ピア デバイスのダウン イベントとアップ イベントによって高速スパニングツリー プロトコルの同期動作が生成されないため、トラフィックの中断は、サブセカンド値になります（STP の観点から、L2 トポロジに変更はありません）。

図 42. vPC ピア スイッチ



vPC ピア スイッチに関する最も一般的な間違いは、スパニングツリー設定の扱いです。

vPC ピア スイッチがアクティブになると、両方のピア デバイスにまったく同じスパニングツリー設定、より正確に言えばすべての vPC VLAN で同じスパニングツリー プロトコル プライオリティが必要です。

この要件は、vPC ピア スイッチの起点によるものです。両方のピア デバイスは、同一のブリッジ ID を使用して一意の STP ルート デバイスとして機能します。

vPC ピア スイッチの一般的な STP 設定は次のように表示されます。

```
7K1 (vPC peer device 1):
spanning-tree vlan 10-101 priority 8192

vpc domain 1
 peer-switch
```

```
7K2 (vPC peer device 2):
spanning-tree vlan 10-101 priority 8192

vpc domain 1
 peer-switch
```

必須の推奨事項:

- vPC ピア スイッチがアクティブになると、両方の vPC ピア デバイスに同じスパニングツリー設定（すべての vPC VLAN で同じスパニングツリー プロトコル プライオリティ）が必要です。

一般的な推奨事項:

- vPC 環境で vPC ピア スイッチをアクティブにします。

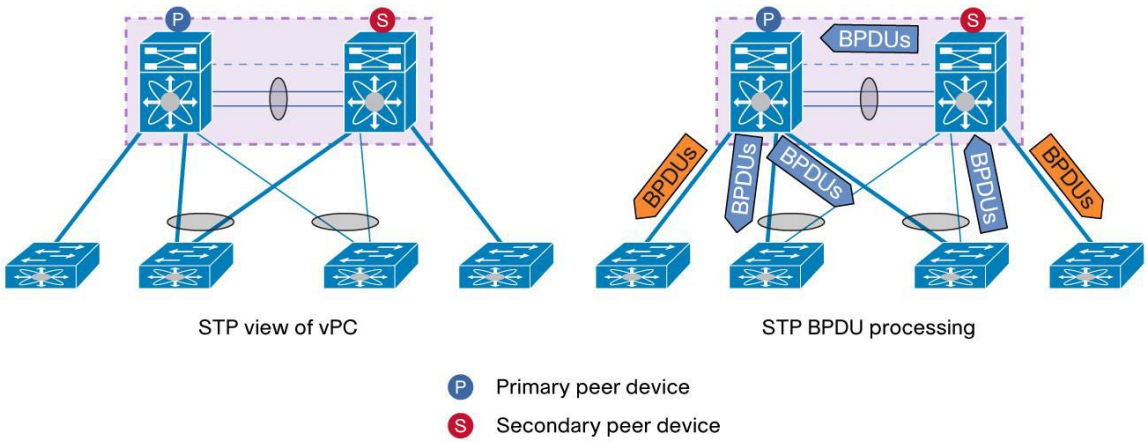
vPC ピア スイッチは異なるタイプのアクセス デバイスが接続された vPC ドメインで使用できます（これは、ハイブリッド トポロジとも呼ばれます）。アクセス デバイスは、vPC ドメインに vPC 接続でき、STP 接続することもできます。

シングル接続アクセス デバイスは、ピア スイッチが設定された vPC ドメインで必然的にサポートされます。

vPC ピア スイッチ機能を使用する場合と使用しない場合のスパニングツリー プロトコル BPDU を確認します。

図 43 がピア スイッチを使用しない vPC ドメインでの STP BPDU 処理を示し、図 44 はピア スイッチがアクティブな同じトポロジでの STP BPDU 処理を示しています。

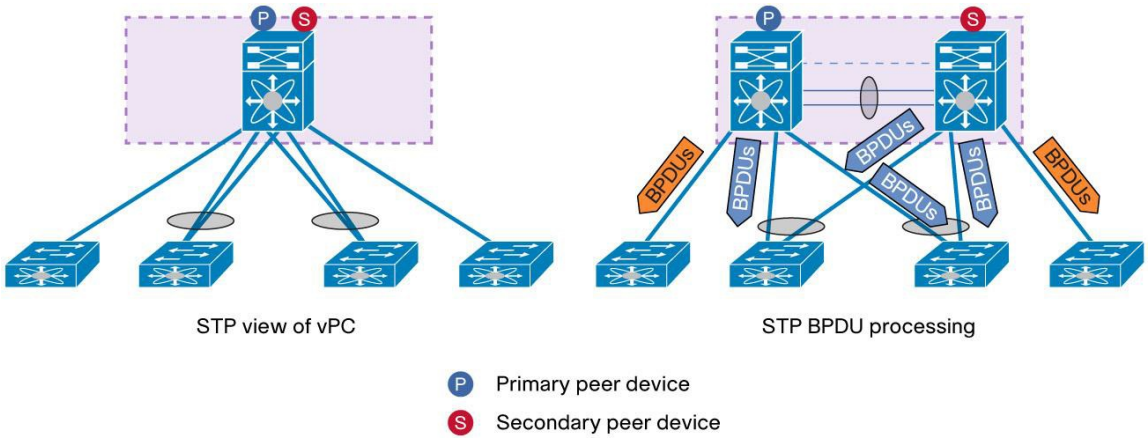
図 43. vPC ピア スイッチを使用しない STP BPDU 処理



vPC ピア スイッチを使用しない STP BPDU 処理の動作:
BPDU は、vPC 接続されたスイッチのプライマリ ピア デバイスによってのみ処理されます。

直接シングル接続されたスイッチでは、それぞれの接続された NEXUS 7000 スイッチが BPDU をローカルで処理します。

図 44. vPC ピア スイッチを使用した STP BPDU 処理



vPC ピア スイッチによる STP BPDU 処理の動作:

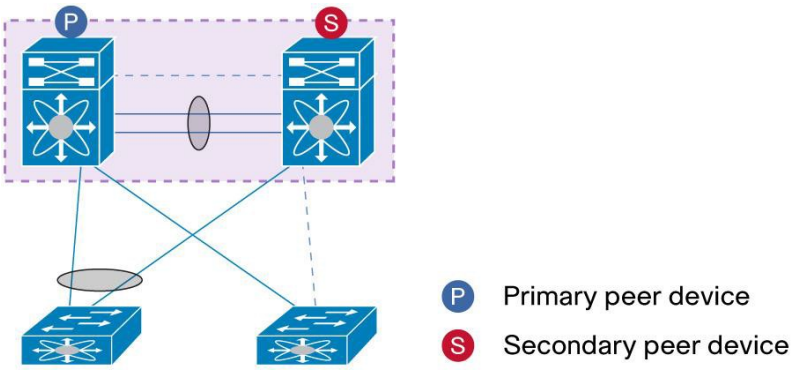
vPC ピア スイッチをアクティブにすると、STP BPDU は、2 台のピア デバイスによって形成される論理的なスパニングツリー プロトコルのルートで直接処理されます。vPC 接続されたアクセス デバイスが 2 つの BPDU（vPC ピア デバイスごとに 1 つ）を受信することに注意してください。BPDU の内容はまったく同じです。vPC ピア スイッチがアクティブになると、vPC ピア リンクを介した BPDU プロキシ処理は必要なくなります。

直接シングル接続されたスイッチでは、それぞれの接続された NEXUS 7000 スイッチが BPDU をローカルで処理します。

vPC ピア スイッチはハイブリッド トポロジをサポートします。ハイブリッド トポロジは、vPC 接続されたアクセス デバイスおよび STP 接続されたアクセス デバイスの両方が vPC ドメインに共存することを意味します。

図 45 は、両方のピア デバイスでピア スイッチがアクティブになっている vPC のコンテキストにおけるハイブリッド トポロジを表しています。

図 45. vPC ピア スイッチを使用するハイブリッド トポロジ（vPC および STP 接続されたアクセス デバイス）



spanning-tree pseudo-information ノブは、STP 接続されたアクセス デバイスの VLAN ロードバランシングをイネーブルにし、（障害またはリロード後に）ピア デバイスが回復したときのスパニングツリー トポロジの変更を避けるために追加されました。

Spanning-tree pseudo-information 設定には、2 つのサブコマンド **designated priority** および **root priority** が含まれます。

Designated priority は、ブリッジ（つまりピア デバイス）の VLAN の STP プライオリティを定義し、2 台のピア デバイスに異なる VLAN を効果的にロード バランスするために使用されます。

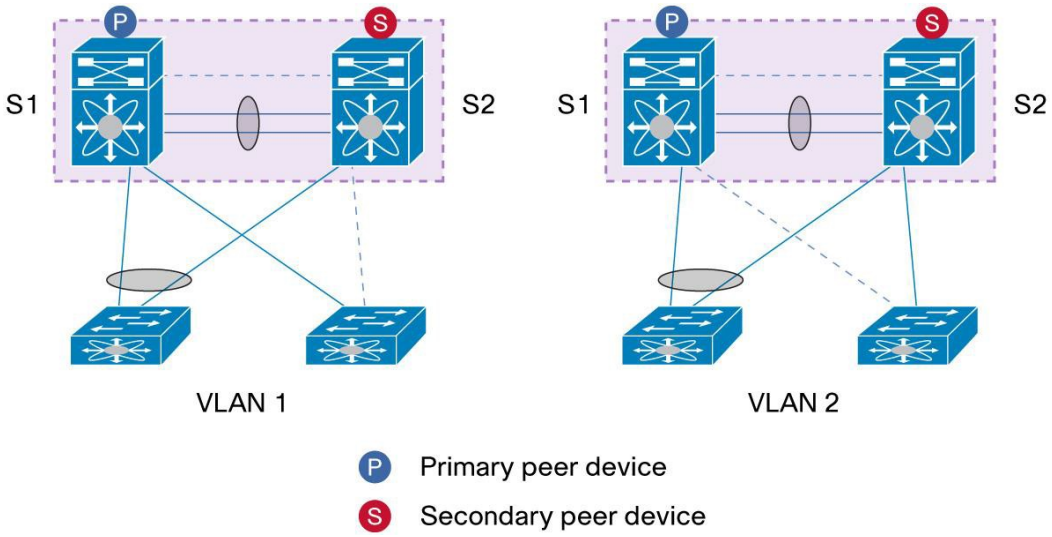
Root priority は、2 台のピア デバイスの一方が失敗して回復する特定の場合に使用されます。ハイブリッド トポロジでは、vPC ピア デバイス（S1）が通常の STP リンク（非 vPC）と vPC リンクの起動の違いが原因で回復時に STP トポロジが変更されます。通常の STP リンクは、vPC の前、したがって vPC ピア スイッチの形成前に起動できます。vPC ピア スイッチが形成されないため、ピア デバイス S1 は STP ブリッジ ID にローカル システム MAC を使用します。ローカル MAC アドレスが vPC システム MAC よりも適切な場合、STP ブリッジ プライオリティが両方の vPC ピア デバイス上で同じであるため STP トポロジの変更がトリガーされません。

S1 が回復したときに STP トポロジ変更を取り消すために、vPC ピア スイッチの STP ブリッジ プライオリティはローカル ブリッジ ID プライオリティよりも高くなります。

次の設定例に、**Spanning-tree pseudo-information** の使用方法を示します。

図 46 は、例の参照トポロジとして使用されます。S1 は VLAN 1 の STP ルート、S2 は VLAN 2 の STP ルートです。

図 46. Spanning-Tree Pseudo-Information の設定例におけるピア スイッチのハイブリッド トポロジ参照




```
S1 configuration:

S1(config)# spanning-tree pseudo-information
S1(config-pseudo)# vlan 1 designated priority 4096
S1(config-pseudo)# vlan 2 designated priority 8192
S1(config-pseudo)# vlan 1 root priority 4096
S1(config-pseudo)# vlan 2 root priority 4096

S1(config)# vpc domain 1
S1(config-vpc-domain)# peer-switch
```

```
S2 configuration:

S2(config)# spanning-tree pseudo-information
S2(config-pseudo)# vlan 1 designated priority 8192
S2(config-pseudo)# vlan 2 designated priority 4096
S2(config-pseudo)# vlan 1 root priority 4096
S2(config-pseudo)# vlan 2 root priority 4096

S2(config)# vpc domain 1
S2(config-vpc-domain)# peer-switch
```

強力な推奨事項:

vPC ピア スイッチをハイブリッド環境で使用する（つまりデュアル接続アクセス デバイスおよび STP 接続アクセス デバイスが同じ vPC ドメイン内に共存する）場合、spanning-tree pseudo-information を使用して 2 台のピア デバイスに VLAN をロード バランシングし、ピア デバイスが障害またはリロード イベントから回復したときのスパニングツリー トポロジの変更を回避します。

Bridge Assurance と vPC

Bridge Assurance は物理ケーブル障害または隣接スイッチのコントロール プレーンの障害に起因する任意の単方向リンク イベントから L2 ネットワークを保護する STP 拡張機能です。

Bridge Assurance によりスイッチは、STP ポート タイプ設定がネットワークである動作中のすべてのポートで BPDU をハロー タイムごとに送信します。ポートには代替ポートとバックアップ ポートも含まれます。ネイバー ポートが BPDU の受信を停止すると、ポートはブロッキング ステートへと遷移します。ブロックされたポートが BPDU の受信を再開すると、Bridge Assurance のブロッキング ステートが解除され、通常の Rapid-PVST 遷移の過程をたどります。

この双方向の hello メカニズムにより、単方向リンクや故障したスイッチに起因するループ状態を防止します（コントロール プレーンはダウンしますが、データ プレーン側ではまだ動作/転送します）。

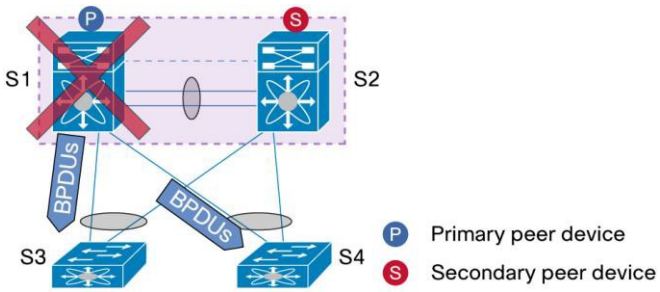
Bridge Assurance BPDU は SUPERVISOR CPU で直接処理されます（Bridge Assurance BPDU は STP BPDU です）。これはラインカードにオフロードされたハードウェアではありません（たとえば BFD）。

Bridge Assurance BPDU は定期的に送信されます。デフォルトの hello タイムは 2 秒です。

vPC のコンテキストにおいて、Bridge Assurance は vPC ではお勧めしません。

各 vPC メンバー ポート上で Bridge Assurance がイネーブルになっている図 47 のトポロジを想定します。

図 47. vPC での Bridge Assurance（BA）の使用



S1 はプライマリ ピア デバイスで、すべての vPC VLAN の STP ルートに設定されます。

S1、S2、S3、および S4 は vPC メンバー ポートおよびポート チャネルでそれぞれ Bridge Assurance がイネーブルに設定されます。

安定した状態で、プライマリ ピア デバイスが STP BPDU を処理します。プライマリ ピア デバイスがフェールオーバーすると、セカンダリ ピア デバイスは、BPDU の送信を開始必要があります。プライマリ ピア デバイスがスパニングツリー プロトコルのルートでもあったため、セカンダリもルートとしての STP ロールを引き継ぐ必要があります。このプロセスの存続時間が長すぎる場合は、アクセス デバイス（S3 および S4）のアップリンク ポートが Bridge Assurance の一貫性のない（BA_Inconsistent）ステートになることがあります。これは CPU 使用率が高い特定の場合に発生する可能性があります。

注： Bridge Assurance は、vPC ピア リンクでデフォルトでイネーブルです（リンクの作成時）。ピア リンクの Bridge Assurance が正常であるため、これをディセーブルにする必要はありません。

Bridge Assurance は、ポートが（双方向 BPDU を送信による）エラーでフォワーディング ステートに遷移しないようにするために STP によってブロックされたポートが設定された純粋なスパニングツリー プロトコル環境で意味をなします。ただし、vPC 環境では、vPC（vPC メンバー ポートは常にフォワーディング ステートです）に STP によってブロックされたポートがないため、Bridge Assurance 機能の有用性は低くなります。

強力な推奨事項:

- vPC メンバー ポート上で Bridge Assurance（BA）をイネーブルにしないでください。
- Bridge Assurance はリンクの作成時に vPC ピア リンク上で自動的にイネーブルになります。ピア リンクの Bridge Assurance が正常であるため、これをディセーブルにする必要はありません。
- ピア スイッチが vPC ドメインで使用されていても、推奨事項は、vPC で Bridge Assurance をディセーブルにすることです。

NX-OS および IOS 内部 VLAN 範囲の割り当て

Cisco NX-OS ソフトウェアおよび Cisco IOS ソフトウェアに別の内部 VLAN 範囲の割り当てがあります。

範囲番号を次に示します。

Cisco NX-OS ソフトウェアの内部 VLAN 範囲の割り当て:

```
7K1# sh vlan internal usage

VLAN        DESCRIPTION
---------   ------------------------------------------------------------
3968-4031        Multicast
4032             Online diagnostics vlan1
4033             Online diagnostics vlan2
4034             Online diagnostics vlan3
4035             Online diagnostics vlan4
4036-4041        Reserved
4042             Satellite
4043-4047        Reserved
4094             Reserved
```

Cisco IOS ソフトウェアの内部 VLAN 範囲の割り当て:

```
6500-1#sh vlan internal usage

VLAN Usage
---- --------------------
1006      online diag vlan0
1007      online diag vlan1
1008      online diag vlan2
1009      online diag vlan3
1010      online diag vlan4
1011      online diag vlan5
1012      PM vlan process (trunk tagging)
1013      Port-channel103
1014      Control Plane Protection
1015      Layer 3 multicast partial shortcuts for VPN 0
1016      Egress internal vlan
1017      Multicast VPN 0 QOS vlan
1018      IPv6 Multicast Egress multicast
```

Cisco Nexus デバイスを Cisco Catalyst® デバイスに接続する場合、NX-OS の範囲または IOS の範囲の予約済み VLAN を使用しないように、この目的に使用する VLAN に注意してください。

注： Cisco NX-OS Release 5.2 から、**system vlan {start-vlan} reserve** コマンドを使用して、予約された VLAN 範囲を変更できるようになりました。
詳細については、次の URL（『L2 switching configuration guide』の「hanging the range of reserved VLAN」）を参照してください。http://www.cisco.com/en/US/docs/switches/datacenter/sw/nx-os/layer2/configuration/guide/b_Cisco_Nexus_7000_Series_NX-OS_Layer_2_Switching_Configuration_Guide_chapter_0100.html#task_67E5266F50104AF38E5149C1CC56B1A7

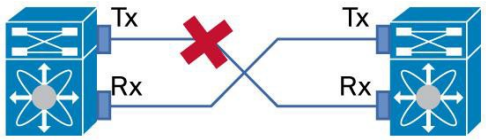
単方向リンク検出の相互運用性のベスト プラクティス

単方向リンク検出（UDLD）プロトコルは、スパニングツリー プロトコル ループなどの望ましくない状況が発生する前に単方向接続を検出してディセーブルにする軽量のレイヤ 2 プロトコルです。

UDLD はスパニングツリー プロトコルを補完します。ネットワーク コンバージェンス時間を短縮することを目的としていません。UDLD は定期的な hello メッセージを送信し、デフォルト タイマーは 15 秒に設定されます。

図 48 に、UDLD の一般的な使用例を示します。

図 48. 単一方向リンク検出（UDLD）



UDLD は条件機能です。UDLD 機能をイネーブルにすると、すべてのイネーブルなファイバ イーサネット インターフェイス（M1、F1、または F2）でデフォルトとして自動的にグローバルに動作します。

（M148 モジュールなどの）銅線イーサネット インターフェイスでは、UDLD はグローバルにディセーブルになり、インターフェイスごとにイネーブルまたはディセーブルにする必要があります（インターフェイス コンフィギュレーションはグローバル コンフィギュレーションを上書きします）。

```
7K1(config)# int eth1/1
7K1(config-if)# udld enable
```

UDLD には 2 種類の動作モードがあります。

- **通常モード**：UDLD は、ピア ポートからの着信 UDLD パケットを調べて、リンク エラーを検出します。これらのエラー状態には、空のエコー パケット、単方向、TX/RX ループ、およびネイバーの不一致があります。UDLD は、ポートを errdisable にします。
- **アグレッシブ モード**：動作は通常モードと同じですが、UDLD は、両方向の UDLD パケットが突然停止した場合にも、ポートを errdisable ステートにします。デフォルトでは、UDLD パケットを（3 X hello-time）+ 5 秒 =50 秒間受信しなかった場合にポートが errdisable モードになります。

UDLD は NEXUS 7000 SUPERVISOR CPU で直接処理されます。これは個々のラインカードにオフロードされたハードウェアではありません。CPU が過負荷状態の場合、UDLD メッセージが処理または送信されず、UDLD がアグレッシブ モードに設定されると errdisable 状況になる可能性があります。このような誤検出状態を防ぐには、通常モードで UDLD を使用することを推奨します。

強力な推奨事項:
vPC ピア リンクおよび vPC メンバー ポート上で通常モードの UDLD をイネーブルにします。

レイヤ 3 および vPC のベスト プラクティス

ここでは、vPC でレイヤ 3 を使用し、設定するためのベスト プラクティスについて説明します。

レイヤ 3 および vPC について

レイヤ 3 デバイス(ルーテッド モードで設定されたルータやファイアウォールなど)は、vPC を介して vPC ドメインに接続すると、次のようになります。

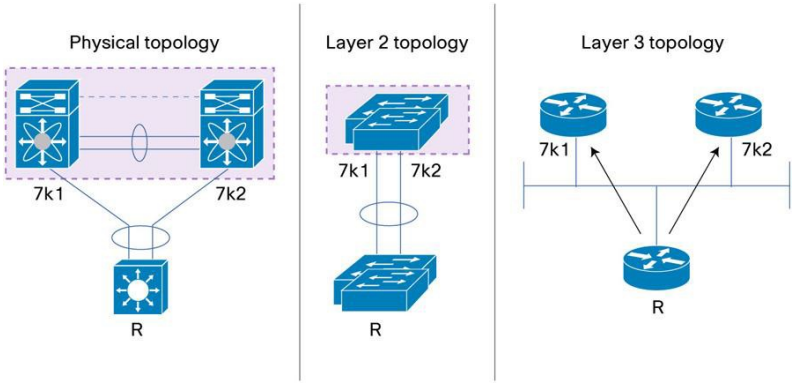
- レイヤ 2 では、L3 デバイスは vPC ピア デバイスによって形成された一意のレイヤ 2 スイッチを認識します。
- レイヤ 3 では、L3 デバイスは 2 台の異なるレイヤ 3 デバイス(vPC ピア デバイスごとに 1 台)を認識します。

vPC は、レイヤ 2 仮想化テクノロジーです。そのため、レイヤ 2 では、両方の vPC ピア デバイスがネットワークの他の部分に対して一意の論理デバイスとして機能します。

ただし、レイヤ 3 では、仮想化メカニズムは vPC テクノロジーで実装されません。これは、各 vPC ピア デバイスがネットワークの他の部分で別の L3 デバイスと見なされるからです。

図 49 は、ネットワークのレイヤ 2 またはレイヤ 3 ビジョンに応じた vPC テクノロジーの 2 つの異なる構成図を表しています。

図 49. ネットワークのレイヤ 2 またはレイヤ 3 ビジョンに応じた vPC ピア デバイスの異なる構成図



レイヤ 3 および vPC:ガイドラインおよび制約事項

vPC を使用して vPC ドメインに L3 デバイス(ルーテッド モードで設定されたルータやファイアウォールなど)を接続することは、vPC ループ回避ルールによりサポートされている設計ではありません。

vPC ドメインに L3 デバイスを接続するには、L3 デバイスから各 vPC ピア デバイスへの L3 リンクを使用するだけです。

L3 デバイスは、両方の vPC ピア デバイスとの L3 ルーティング プロトコルの隣接関係を開始できます。

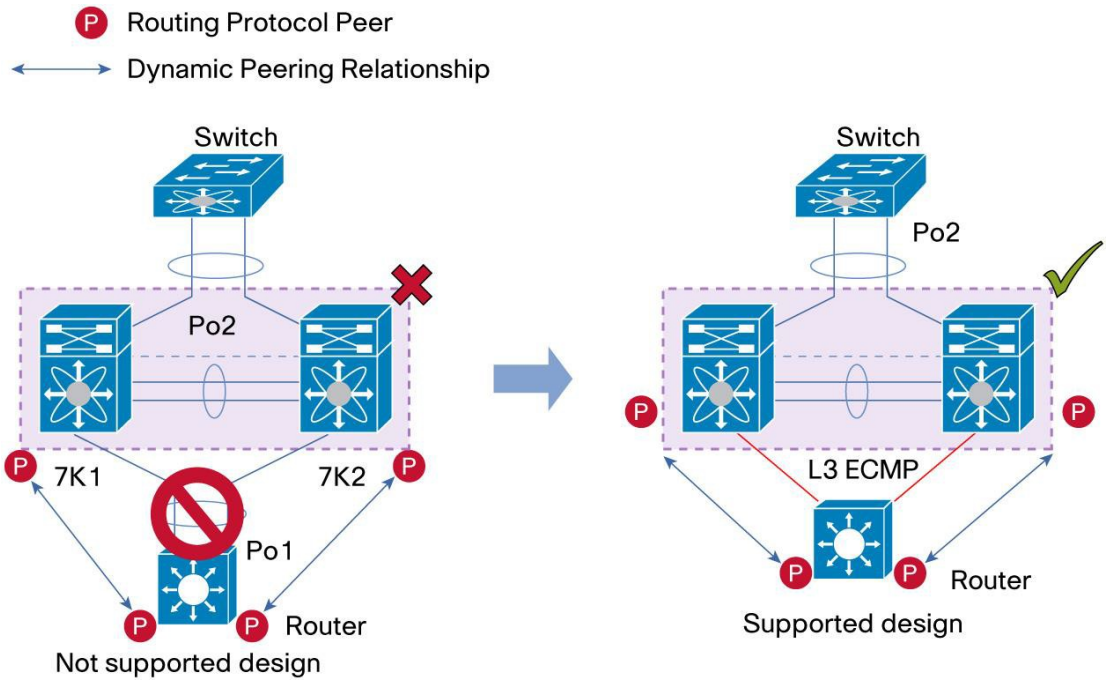
1 つまたは複数の L3 リンクを各 vPC ピア デバイスに L3 デバイスを接続するのに使用できます。NEXUS 7000 シリーズは、プレフィックスごとに最大 16 のハードウェア ロード シェアリング パスで L3 Equal Cost Multipathing（ECMP）をサポートします。vPC ピア デバイスから L3 デバイスへのトラフィックを、2 台のデバイスを相互接続するすべての L3 リンクにロードバランスできます。

L3 デバイスでレイヤ 3 ECMP を使用すると、このデバイスから vPC ドメインへのすべてのレイヤ 3 リンクを効果的に使用できます。L3 デバイスから vPC ドメイン（つまり vPC ピア デバイス 1 および vPC ピア デバイス 2）へのトラフィックは、2 つのエンティティを相互接続するすべての L3 リンクにロードバランスできます。

（L3 接続で複数リンクを利用することもできるという意味で）vPC 接続と比較して vPC ドメインへの L3 デバイスの接続に L3 リンクを使用するペナルティはありません。

vPC ドメインに対する L3 デバイスのサポートされる接続モデルは、図 50 に示されています。

図 50. 別のレイヤ 3 リンクを使用した vPC ドメインへの L3 デバイスの接続



レイヤ 3 デバイスを vPC ドメインに接続する場合は、次のガイドラインに従うことを強く推奨します。

強力な推奨事項：

- vPC ドメインに L3 デバイス（ルーテッド モードのルータやファイアウォールなど）を接続するには、別のレイヤ 3 リンクを使用します（図 50）。
- L3 デバイスが vPC ピア デバイスで設定された HSRP アドレスにスタティックにルーティングできない場合は、vPC ドメインに L3 デバイスを接続するのにレイヤ 2 の vPC を使用しないでください。
- ルーテッド トラフィックとブリッジド トラフィックの両方が必要な場合は、ルーテッド トラフィックに個々のレイヤ 3 リンクを使用し、ブリッジド トラフィックには別のレイヤ 2 ポート チャネルを使用します。
- 両方のデバイスからの同じ VLAN に対して VLAN ネットワーク インターフェイスを設定するか、2 台のピア デバイス間に専用 L3 リンクを使用することにより（L3 バックアップ ルーティング パスのため）、vPC ピア デバイス間のレイヤ 3 接続をイネーブルにします。

レイヤ 3 および vPC のインタラクション：サポートされている設計

図 51～59 に示すネットワークトポロジは、レイヤ 3 および vPC のサポートされている設計を表しています。

図 51 に、これらの図で使用される記号を定義します。

図 51. 以降の図（図 51～59）で使用される記号の意味

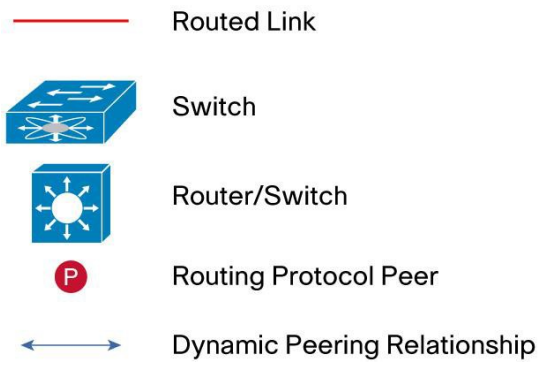
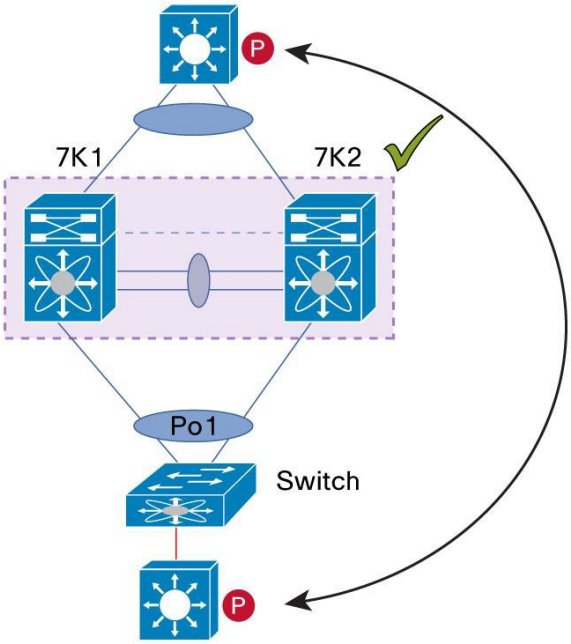
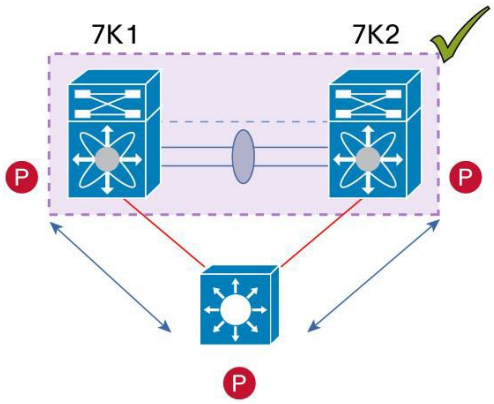


図 52. レイヤ 3 および vPC のサポートされている設計：ルータ間のピアリング



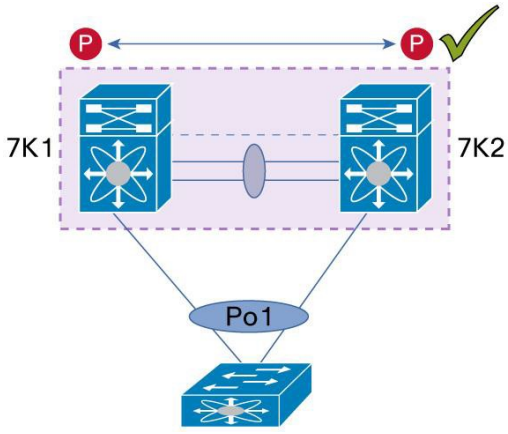
この設計では、vPC は純粋な L2 中継パスとして使用されます。L3 デバイスから vPC ピア デバイスへの直接的なルーティング プロトコル ピアリング隣接がないため、このトポロジは全体的に有効であり、完全にサポートされます。

図 53. レイヤ 3 および vPC のサポートされている設計：L3 リンクを使用した外部ルータとのピアリング



L3 リンクを使用して vPC ドメインに L3 デバイスを接続するのは、2 つのエンティティを相互接続するための最も推奨される方法です。

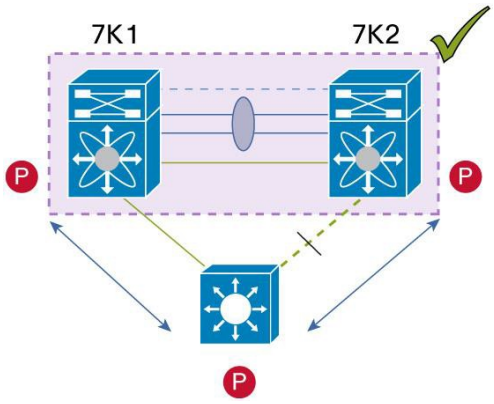
図 54. レイヤ 3 および vPC のサポートされている設計：vPC デバイスの間のピアリング（バックアップ ルーティング パス用）



2 台の vPC ピア デバイス間のピアリングが完全に機能し、このタイプの設計の使用例では、L3 バックアップ ルーテッド パスが扱われます。vPC ピア デバイス 1 またはピア デバイス 2 の L3 アップリンクがダウンした場合、2 台のピア デバイス間のパスを使用して、アップ ステートの L3 アップリンクを持つスイッチにトラフィックがリダイレクトされます。

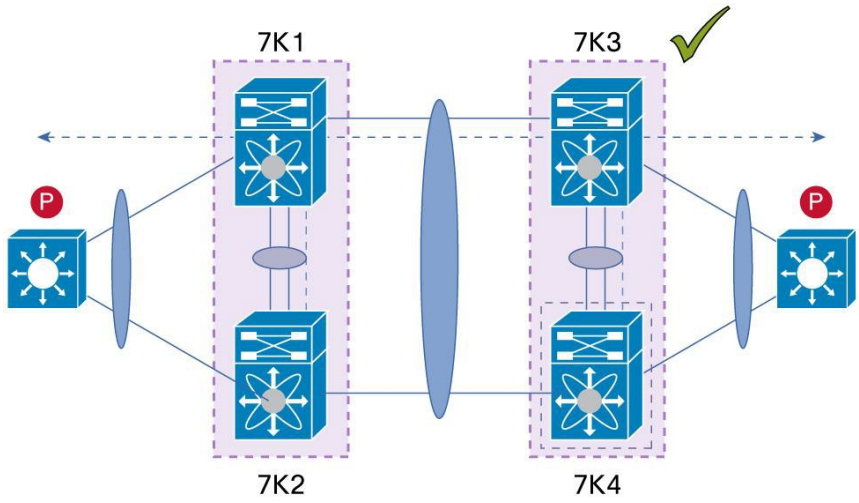
L3 バックアップ ルーティング パスは、vPC ピア リンク上の専用インターフェイス VLAN（つまり SVI）を使用するか、2 台の vPC ピア デバイス間の専用 L2 または L3 リンクを使用して実装できます。

図 55. レイヤ 3 および vPC のサポートされている設計：非 vPC VLAN を使用するスパニングツリー プロトコル相互接続を介したピアリング



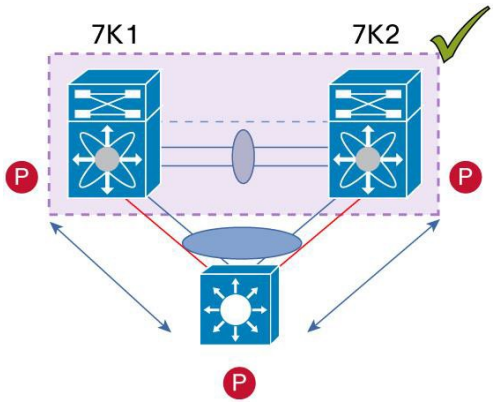
L3 デバイスは STP 相互接続リンクを使用して vPC ドメインに接続できます。非 vPC VLAN は、このタイプの接続に使用する必要があります。非 vPC VLAN トラフィックを伝送するために、専用スイッチ間リンクを 2 台の vPC ピア デバイス間に追加する必要があります。vPC ピア リンクは、この目的に使用しないでください。

図 56. レイヤ 3 および vPC でサポートされる設計：中継スイッチとして vPC デバイスを使用した 2 ルータの間のピアリング



このタイプの設計では、DCI の使用例が扱われます。機能や動作の点では、図 51 に示したトポロジにそっくりです（ルータ間のピアリング）。vPC ドメインは純粋な L2 中継パスとして単に使用されます。

図 57. レイヤ 3 および vPC でサポートされる設計：パラレル相互接続ルーテッド ポートでの外部ルータとのピアリング



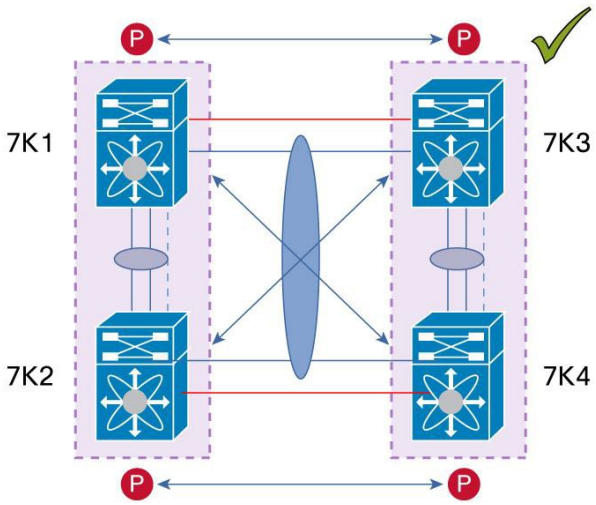
この設計では、L3 デバイスは 2 つの異なるリンク タイプ（L2 リンクと L3 リンク）を使用して vPC ドメインに接続されます。

L2 リンクは、ブリッジド トラフィック（同じ VLAN に保持されるトラフィック）または VLAN 間トラフィック（vPC ドメインがインターフェイス VLAN と関連 HSRP コンフィギュレーションをホストすることが前提）に使用されます。

L3 リンクは通常、各 vPC ピア デバイスとのルーティング プロトコル ピアリング隣接に使用されます。

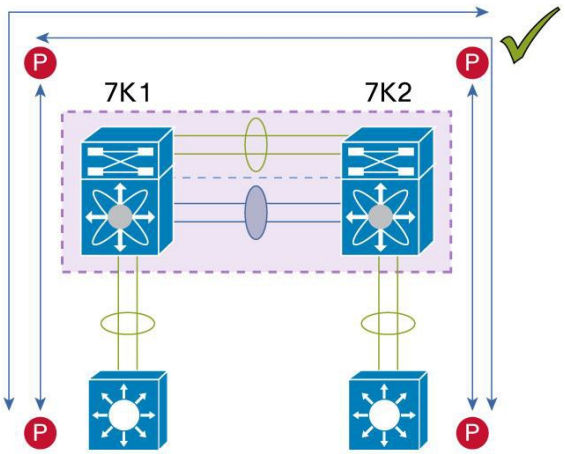
目的は、特定のトラフィックを集めて L3 デバイスを通過させることです（ルーテッド モードのファイアウォールはその一例です）。L3 リンクは、L3 デバイスから vPC ドメインにルーテッド トラフィックを伝送するのにも使用されます。

図 58. レイヤ 3 および vPC でサポートされる設計：パラレル相互接続ルーテッド ポートでの vPC 相互接続（DCI ケース）を介したピアリング



このタイプの設計では、DCI の使用例が扱われます。ルーティング プロトコル ピアリング隣接を 2 つのデータセンター間で確立する必要がある場合、推奨事項は図 59 に示すように 2 サイト間に専用 L3 リンクを追加することです。2 つのデータセンター間の vPC リンクは引き続きブリッジド トラフィックまたは VLAN 間トラフィックを伝送し、専用 L3 リンクは 2 サイト間でルーテッド トラフィックを伝送します。

図 59. レイヤ 3 および vPC でサポートされる設計：非 vPC VLAN を使用する PC 相互接続および専用スイッチ間リンクを介したピアリング



L3 デバイスが vPC ドメインにシングル接続されている場合、L3 デバイスと各 vPC ピア デバイスとの間でルーティング プロトコル ピアリング隣接を確立するには、専用スイッチ間リンクで非 vPC VLAN を使用します。

このタイプの設計はサポートされていないため、vPC VLAN（および vPC ピア リンク）をこの目的に使用しないでください。

レイヤ 3 および vPC のインタラクション：サポートされていない設計

図 60～64 に示すネットワーク トポロジはレイヤ 3 および vPC のサポートされていない設計です。

図 60 に、これらの図で使用される記号を定義します。

図 60. 以降の図（図 60～64）で使用される記号の意味

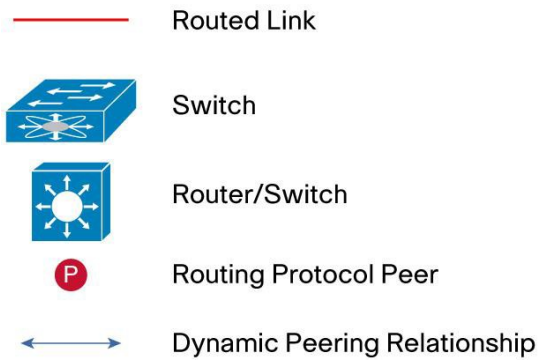
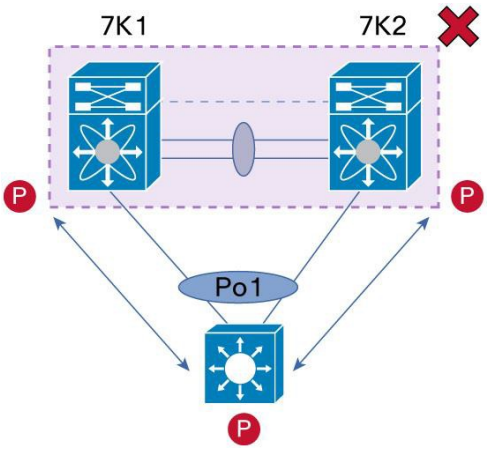
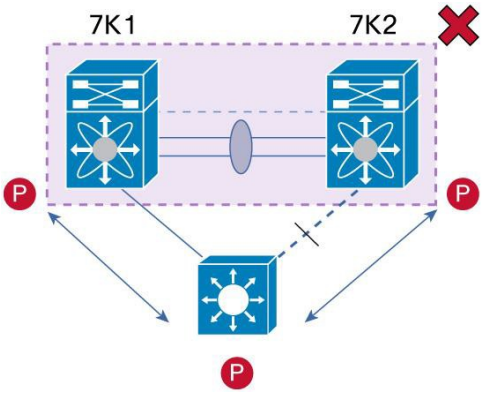


図 61. レイヤ 3 および vPC のサポートされていない設計：vPC 相互接続を介したピアリング



L3 デバイスが vPC ドメインに vPC 接続され、各 vPC ピア デバイスとの L3 ルーティング プロトコル ピアリング隣接を確立する設計はサポートされません。理由は、vPC ループ回避のためにトラフィックがブラックホール化される可能性があることです（L3 ECMP の決定と L2 ポート チャネル ハッシュ アルゴリズムは、独立して動作するため、トラフィックは vPC ピア デバイスである次の L3 ホップに到達するために vPC ピア リンクを通過する必要があります）。

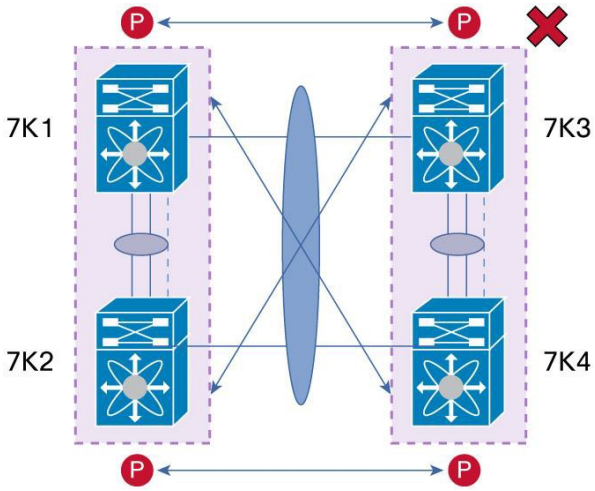
図 62. レイヤ 3 および vPC のサポートされていない設計：vPC VLAN を使用するスパニングツリー プロトコル相互接続を介したピアリング



vPC VLAN で STP リンクを使用して vPC ドメインに L3 デバイスを接続するのは、サポートされている設計ではありません。

このタイプの設計に完全に対応するには、非 vPC VLAN を専用スイッチ間リンクで使用して非 vPC VLAN を伝送します（前の項の図 55）。

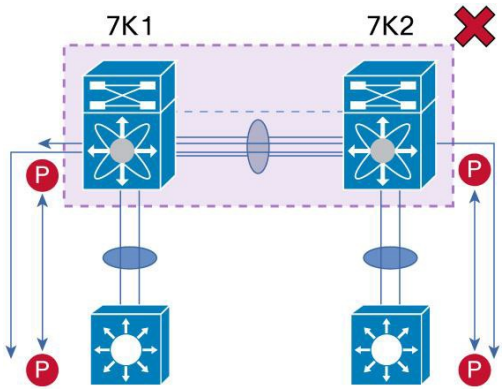
図 63. レイヤ 3 および vPC のサポートされていない設計：vPC 相互接続（DCI ケース）を介したピアリング



DCI の展開で、DCI vPC を使用して異なる vPC ピア デバイス上にルーティング プロトコル ピアリング隣接を確立するのは（図 63 で示されているように、7K1 と 7K3 のピアリングおよび 7K2 と 7K4 のピアリング）、vPC ループ回避ルールに従うためサポートされていない設計です。

代替のサポートされているトポロジを図 64（前のセクション）に示します。2 つのデータセンターにまたがる専用 L3 リンクを追加することによって、この設計には vPC 回避ルールが適用されなくなります。L3 ルーテッド トラフィックは DCI vPC リンク上ではなく L3 リンク上で伝送されます。

図 64. レイヤ 3 および vPC のサポートされていない設計：PC 相互接続および vPC VLAN を使用する vPC ピア リンクを介したピアリング



vPC VLAN を使用して vPC ドメインにシングル接続された L3 デバイスは、サポートされている設計ではありません。

設計を変更し、完全に公式サポートされるようにするには、L3 デバイスと vPC ドメイン間の相互接続リンクに非 vPC VLAN を使用し、この非 vPC VLAN を伝送するために 2 台の vPC ピア デバイスに専用スイッチ間リンクを追加します。このトポロジは、前の項の図 59 に示されています。

vPC および L3 バックアップ ルーティング パス

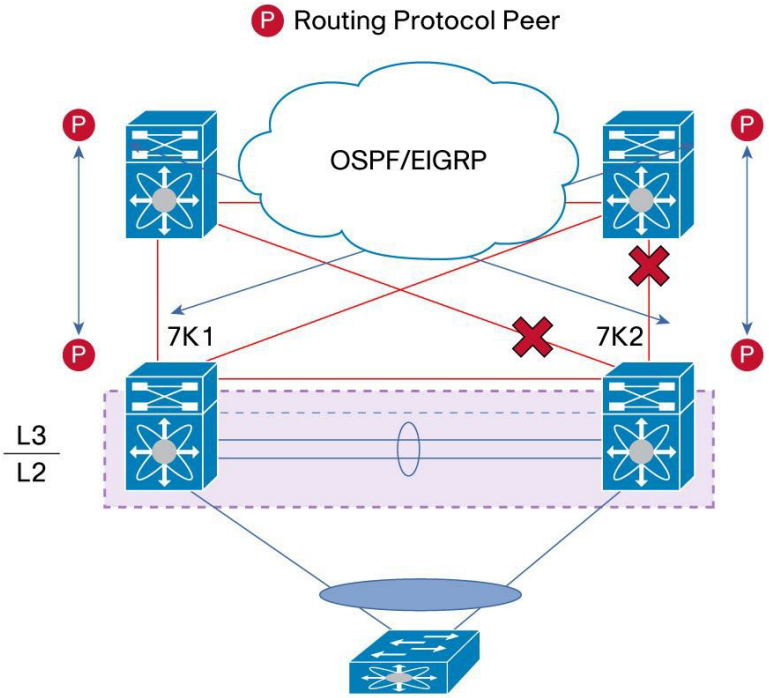
L3 バックアップ ルーティング パスを設定する目的は、L3 アップリンク障害が発生した場合に、コアに別のレイヤ 3 パスを確立することです（図 65）。

L3 バックアップ ルーティング パス（2 台の vPC ピア デバイス間）は、ダイナミック ルーティング プロトコル ピアリング隣接が 2 台のスイッチ/ルータの間で確立されたポイントツーポイント リンクです。

7K2 上の L3 アップリンクがダウンし、ルーテッド トラフィックがアクセス スイッチから 7K2 に送信された場合、L3 バックアップ ルーティング パスが利用されます。7K1 は 7K2 からルーテッド トラフィックを受信し、動作している L3 アップリンクから転送できます。

L3 バックアップ ルーティング パスは、L3 コアの到達可能性に関して vPC ドメインのハイ アベイラビリティのレベルを向上させます。

図 65. vPC ピア デバイス間の L3 バックアップ ルーティング パスの確立



強力な推奨事項:

ネットワークの復元力と可用性を高めるには、vPC ドメインの L3 バックアップ ルーテッド パスを常に構築します。アップリンク障害が生じた場合は、2 台の vPC ピア デバイス間の OSPF ポイントツーポイント隣接（または同等のレイヤ 3 プロトコル）を使用して、コアへのレイヤ 3 バックアップ パスを確立します。

L3 バックアップ ルーティング パスを実装する方法は複数あります。

強力な推奨事項:

L3 バックアップ ルーティング パスを構築するには、優先順位の降順で示されている次のオプションを使用します。

- vPC ピア デバイス間の専用レイヤ 3 ポイントツーポイント リンクを使用して、コアへのレイヤ 3 バックアップ パスを確立します。

- 既存のレイヤ 2 ポート チャネル トランク ISL（Inter Switch Link）を非 vPC VLAN に使用し、専用 VLAN/SVI を作成してレイヤ 3 ネイバーシップを確立します。
- vPC ピア リンクを使用し、専用 VLAN/SVI を作成して、レイヤ 3 ネイバーシップを確立します（最も推奨されないソリューション）。

HSRP/VRRP と vPC のベスト プラクティス

ここでは、vPC で HSRP（ホット スタンバイ ルータ プロトコル）または VRRP（仮想ルータ冗長プロトコル）を使用するためのベスト プラクティスについて説明します。

vPC での HSRP/VRRP アクティブ/アクティブ

HSRP（ホット スタンバイ ルータ プロトコル）および VRRP（仮想ルータ冗長プロトコル）は、両方ともサーバ IP デフォルト ゲートウェイにハイ アベイラビリティを提供するネットワーク プロトコルです。

集約レイヤの vPC ドメインは通常、L2/L3 境界を実行します。したがって、各 vPC ピア デバイスにはインターフェイス VLAN（または SVI）が設定され、HSRP または VRRP はこのインターフェイス上で動作します。

vPC のコンテキストにおける HSRP および VRRP は、vPC テクノロジーによって提供される L2 デュアル アクティブ ピア デバイスの性質の利点を得るために、機能や実装の観点から改善されました。

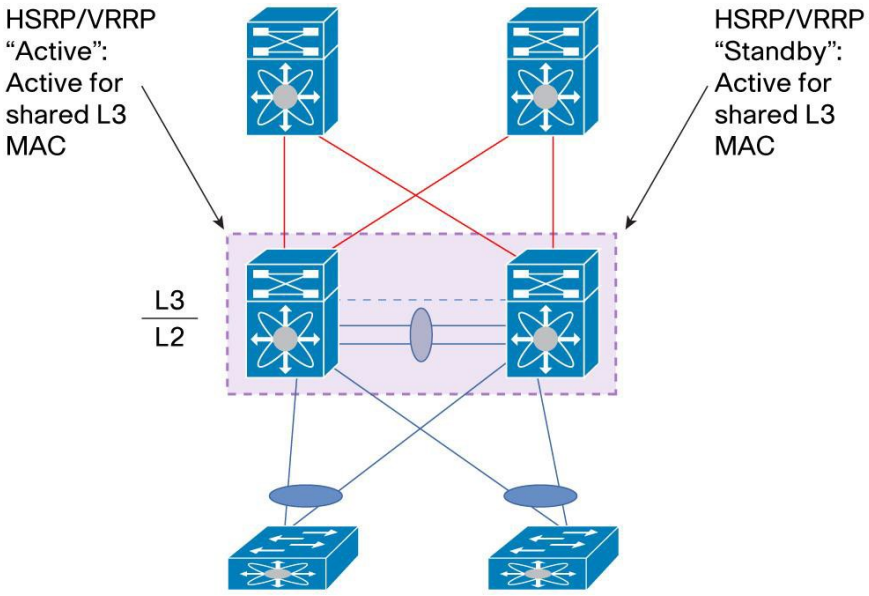
HSRP および VRRP は STP ベースのネットワークによる従来のアクティブ/スタンバイ実装とは対照的に、データ プレーンの観点からアクティブ-アクティブ モードで動作します。

設定を追加する必要はありません。vPC ドメインが設定され、関連する HSRP または VRRP グループのインターフェイス VLAN がアクティブになるとすぐに、HSRP または VRRP がデフォルトでアクティブ/アクティブ モードで動作します（データ プレーン側）。

コントロール プレーンに関しては、アクティブ-スタンバイ モードは、vPC のコンテキストで HSRP/VRRP に適用されます。アクティブな HSRP/VRRP インスタンスは ARP 要求に応答します。

図 66 は、vPC での HSRP または VRRP のアクティブ/アクティブ特性を示しています。

図 66. vPC での HSRP/VRRP アクティブ/アクティブ



show hsrp group コマンドを確認すると、1 台の vPC ピア デバイスがアクティブ インスタンスとして表示され、他の vPC ピア デバイスがスタンバイ インスタンスとして表示されます。これは HSRP/VRRP のコントロール プレーン情報です。

アクティブな HSRP/VRRP ピア デバイスの特性は HSRP/VRRP VIP（仮想 IP）の ARP 要求に応答する唯一のデバイスであるということです。ARP 応答には、両方の vPC ピア デバイス上で同じ HSRP/VRRP vMAC が含まれます。

スタンバイ HSRP/VRRP の vPC ピア デバイスが、vPC ピア リンクを介してアクティブな HSRP/VRRP ピア デバイスに ARP 要求を中継します。

```
7K1# sh hsrp group 400
Vlan400 - Group 400 (HSRP-V2) (IPv4)
  Local state is Active, priority 100 (Cfged 100)
    Forwarding threshold(for vPC), lower: 1 upper: 100
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 0.383000 sec(s)
  Virtual IP address is 40.40.40.254 (Cfged)
  Active router is local
  Standby router is 40.40.40.2, priority 100 expires in 7.386000 sec(s)
  Authentication text "cisco"
  Virtual mac address is 0000.0c9f.f190 (Default MAC)
  2 state changes, last state change 6d01h
  IP redundancy name is hsrp-Vlan400-400 (default)
```

```
7K2# sh hsrp group 400
Vlan400 - Group 400 (HSRP-V2) (IPv4)
  Local state is Standby, priority 100 (Cfged 100)
    Forwarding threshold(for vPC), lower: 1 upper: 100
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 0.848000 sec(s)
  Virtual IP address is 40.40.40.254 (Cfged)
  Active router is 40.40.40.1, priority 100 expires in 7.852000 sec(s)
  Standby router is local
  Authentication text "cisco"
  Virtual mac address is 0000.0c9f.f190 (Default MAC)
  7 state changes, last state change 01:08:24
  IP redundancy name is hsrp-Vlan400-400 (default)
```

データ プレーンの観点からは、両方のピア デバイスが転送しています。これは、次のように、両方の vPC ピア デバイスに、MAC アドレス テーブルの HSRP/VRRP vMAC の G ビット（ゲートウェイ ビット）を課すことによって実装されます。

```
7K1# sh mac address-table address 0000.0c9f.f190
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link
```

```
   VLAN     MAC Address       Type      age     Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
G 400      0000.0c9f.f190    static       -       F    F    sup-eth1(R)
```

```
7K2# sh mac address-table address 0000.0c9f.f190
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link
   VLAN     MAC Address       Type      age     Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
G 400      0000.0c9f.f190    static       -       F    F    vPC Peer-Link(R)
```

アクティブな HSRP/VRRP インスタンスでは vMAC が sup-eth1(R) を指し、スタンバイ HSRP/VRRP インスタンスでは vMAC が vPC ピア リンクを指していることに注意してください。これは HSRP/VRRP のアクティブまたはスタンバイであるスイッチを迅速に認識する方法です（コントロール プレーンの観点から）。

HSRP/VRRP のガイドラインおよび制約事項

vPC ドメイン内で HSRP/VRRP を使用する場合は、次の推奨されるベスト プラクティスに従ってください。

強力な推奨事項:

- アクティブ-アクティブ モードで HSRP/VRRP を実行すると（データ プレーンの観点から）、アグレッシブ タイマーを緩和できます。デフォルトの HSRP/VRRP タイマーを使用します。
- vPC ピア リンクでルーティング隣接を形成しないようにするには、FHRP/VRRP に関連付けられた SVI をパッシブ ルーティング インターフェイスとして定義します。
- 操作が容易になるように、vPC プライマリ ピア デバイスをアクティブな HSRP/VRRP インスタンスとして定義し、vPC セカンダリ ピア デバイスをスタンバイ HSRP/VRRP（コントロール プレーンの観点から）として定義します。
- HSRP/VRRP が設定されているインターフェイス VLAN で IP リダイレクトをディセーブルにします（コマンドは **no ip redirect**）。これは HSRP/VRRP に関連する一般的なベスト プラクティスです。

注: データセンターが停電した場合に、vPC が正常に稼働し始める前に HSRP がイネーブルになると、トラフィック損失が発生します。HSRP 遅延タイマーをイネーブルにして、vPC が安定する十分な時間を設ける必要があります。HSRP 遅延タイマーと HSRP プリエンプション遅延の両方をイネーブルにすると、Cisco Nexus 7000 シリーズ デバイスは、両方のタイマーが期限切れになった後にのみレイヤ 3 スイッチングを許可します。

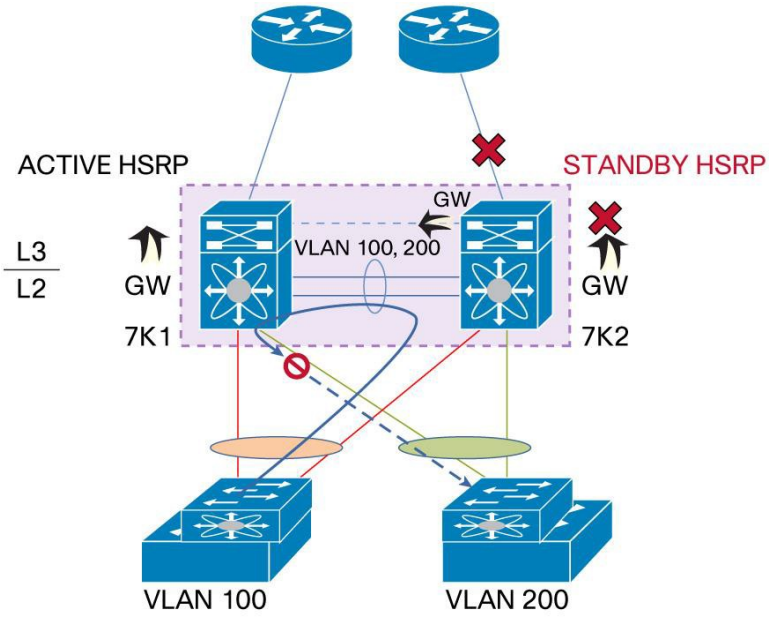
vPC および HSRP/VRRP オブジェクト トラッキング

図 67 に示すように、vPC 設定で HSRP/VRRP リンクのトラッキングを使用しないことが重要です。

HSRP/VRRP オブジェクト トラッキングが両方の vPC ピア デバイスで設定され、スイッチ 7K2 で L3 アップリンク障害が発生したとします。このイベントは HSRP/VRPP オブジェクト トラッキングをトリガーし、関連する HSRP/VRRP 設定を持つ SVI がダウン ステートに設定されます。したがって、7K2 が HSRP/VRRP vMAC を宛先とするフレームを受信するたびに、（関連する HSRP/VRRP 設定を持つ SVI はまだアップ ステートであるため）他の vPC ピア デバイスがこのフレームを処理できるため、このフレームを vPC ピア リンク上にブリッジングします。

HSRP/VRRP オブジェクト トラッキングで vPC を使用すると、オブジェクト トラッキングがトリガーされるときにトラフィックがブラックホール化される可能性があります。理由は、リモート vPC メンバー ポートの障害の場合を除き、(vPC ループ回避ルールにより)パケットが一度ピア リンクを通過すると、vPC システムが vPC でパケットを転送しなくなるからです。

図 67. vPC 設定の HSRP/VRRP オブジェクト トラッキングの問題



強力な推奨事項:

vPC ドメインで HSRP/VRRP オブジェクト トラッキングを使用しないでください。

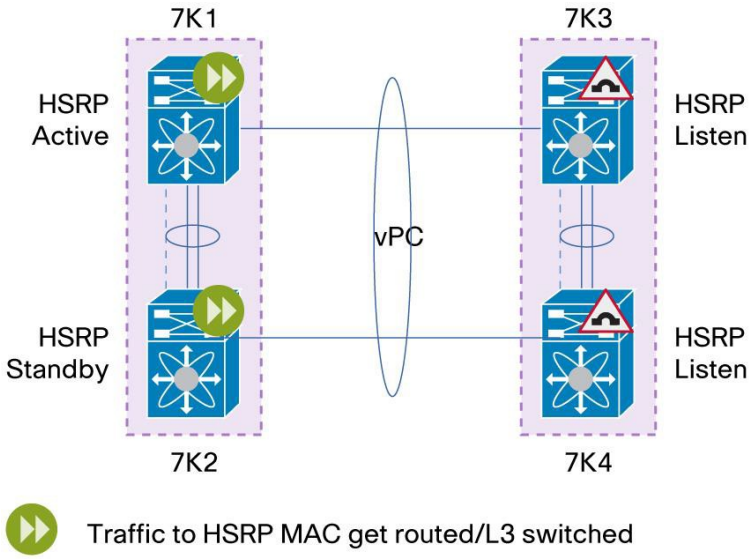
DCI のコンテキストにおける vPC および HSRP/VRRP

拡張機能が DCI の vPC のコンテキストで HSRP/VRRP に導入されました。

2 つのデータセンターにまたがる単一の HSRP/VRRP グループを作成し、HSRP/VRPP は一方のペアのアクティブ/アクティブをサポートし(データ プレーンの観点)、もう一方のペア(1 つの HSRP グループですべて)における通常の HSRP 動作を可能にします。VLAN 間トラフィックとレイヤ 3 トラフィックはアクティブ/アクティブ以外のレイヤ 3 ペアの DCI vPC リンクで動作します。

図 68 および 69 は、各データセンターにおける HSRP モードの 2 つのシナリオを示しています。

図 68. 単一 HSRP/VRRP グループの DCI：DC1 のアクティブ/アクティブおよび DC2 のリッスン/リッスン

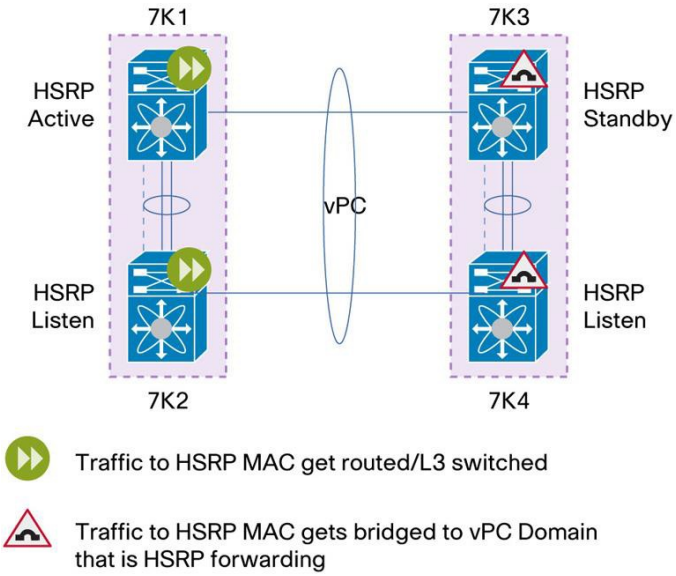


シナリオ 1 では、7K1 および 7K2（データセンター 1 の一部）には、HSRP のアクティブ/スタンバイ モードが設定されています（コントロール プレーンの観点）。データ プレーンの観点では、両方がアクティブ/アクティブです。

7K3 および 7K4（データセンター 2 の一部）には、HSRP のリッスン/リッスン モードが設定されています。

7K1 および 7K2 は HSRP 転送を実行する vPC ドメインを形成します。7K3 または 7K4 が受信した HSRP vMAC へのトラフィックは、L3 ルックアップおよび転送のために 7K1 または 7K2 を宛先として DCI vPC リンク上にブリッジングされます。

図 69. 単一 HSRP/VRRP グループの DCI：DC1 のアクティブ/アクティブおよび DC2 のリッスン/リッスン



シナリオ 2 では、7K1 および 7K2（データセンター 1 の一部）には、HSRP のアクティブ/リッスン モードが設定されています（コントロール プレーンの観点）。データ プレーンの観点では、両方がアクティブ/アクティブです。

7K3 および 7K4（データセンター 2 の一部）には、HSRP のスタンバイ/リッスン モードが設定されています。

7K1 および 7K2 は HSRP 転送を実行する vPC ドメインを形成します。7K3 または 7K4 が受信した HSRP vMAC へのトラフィックは、L3 ルックアップおよび転送のために 7K1 または 7K2 を宛先として DCI vPC リンク上にブリッジングされます。

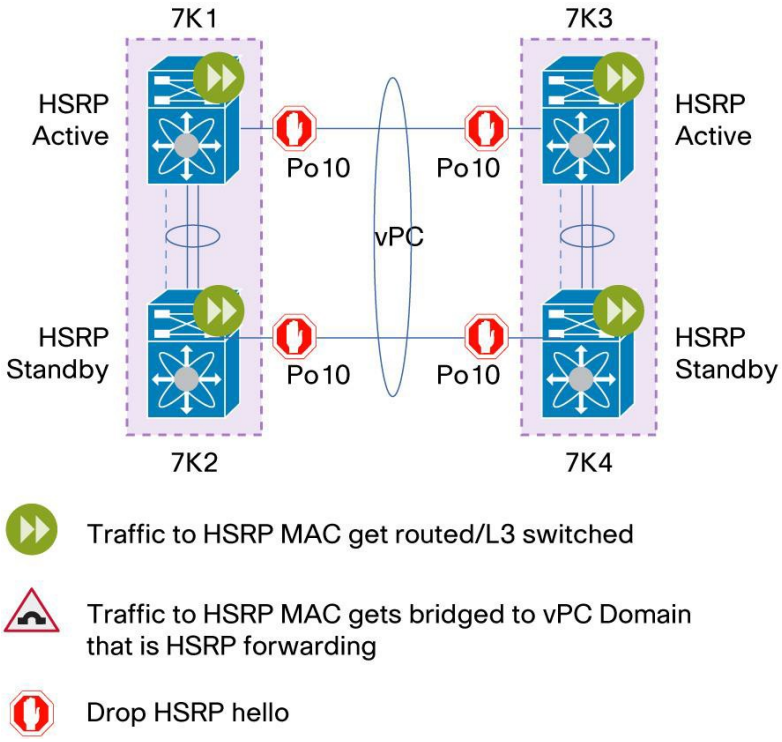
DCI の vPC のコンテキストにおける HSRP/VRRP のこの動作モードは、デフォルトで設定されます（単一 HSRP/VRRP グループの DCI）。この動作のために実装する特定の設定はありません。

両方のデータセンターで（HSRP/VRRP vMAC 宛てのパケットに対して DCI vPC リンクを介したブリッジド トラフィックを回避するために）HSRP（または VRRP）のアクティブ/アクティブを使用する場合は、このタイプの動作を実装するための技術ソリューションがあります。ソリューションは DCI vPC リンクでの PACL（ポート ACL）に基づき、このリンクを介した HSRP/VRRP hello メッセージの伝播を停止します。

図 70 は、両方のデータセンターにおける HSRP/VRRP のアクティブ/アクティブ（データ プレーンの観点）動作およびこのタイプの設計に従うための DCI vPC リンクを介した PACL の適用を示しています。

両方のデータセンターで HSRP（または VRRP）のアクティブ/アクティブを利用する一般的なアプリケーションは、L2 の VMOTION です（1 台の物理サーバから別の物理サーバへの仮想サーバの移動）です。

図 70. 単一 HSRP/VRRP グループの DCI：DC1 のアクティブ/アクティブおよび DC2 のアクティブ/アクティブ



HSRPv1 hello メッセージを停止する PACL 設定:

```
ip access-list HSRPv1_Filtering
  10 deny udp any 224.0.0.2/32 eq 1985
  20 permit ip any any
```

HSRPv2 hello メッセージを停止する PACL 設定:

```
ip access-list HSRPv2_Filtering
  10 deny udp any 224.0.0.102/32 eq 1985
  20 permit ip any any
```

VRRP hello メッセージを停止する PACL 設定:

```
ip access-list VRRP_Filtering
  10 deny udp any 224.0.0.18/32 eq 1985
  20 permit ip any any
```

DCI vPC リンクに PACL を適用するには、PACL を各メンバー ポートで適用します(HSRPv1 の例)。

```
Interface Po10
  ip port access-group HSRPv1_Filtering
```

ネットワーク サービスと vPC のベスト プラクティス

ここでは、vPC とのネットワーク サービスの統合のベスト プラクティスについて説明します。ネットワーク サービス デバイスには、ロード バランサやファイアウォールなどのアプライアンスとサービス モジュールが含まれます。

VDC サンドイッチ設計のネットワーク サービス シャーシ

ネットワーク サービスは、Cisco Catalyst 6500 シリーズ サービス シャーシの一部として配置できます。専用の 6500 が ASA サービス モジュールまたは FWSM(ファイアウォール サービス モジュール)や ACE サービス モジュールをホストするために使用されます。

6500 サービス シャーシは、データセンターにファイアウォールやサーバのロードバランシング機能を提供します。
ASA または ACE は異なるモード(ルーテッド モード、トランスペアレント モード、ワンアーム モード)で動作します。

ただし、次に説明する設計では、トランスペアレント モードだけがサポートされます。

6500 サービス シャーシは、vPC とのインタラクションにポート チャネル(または EtherChannel)機能を提供しています。すべてのサービス モジュールはトランスペアレント モードで設定されます。複数のトランスペアレント コンテキストは必要に応じて使用できます。

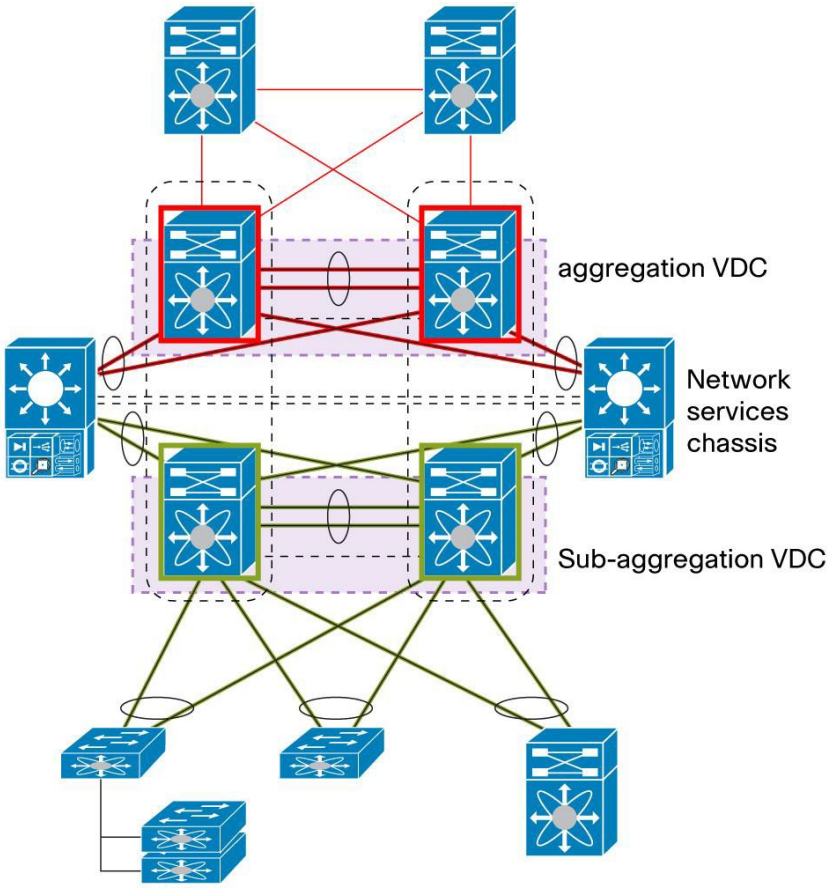
2 つの Cisco Nexus 7000 シリーズ VDC がスイッチング レイヤ間のサービスの「サンドイッチ」に使用されます。vPC は両方の VDC ペアでサービス シャーシへの inside インターフェイスと outside インターフェイスの両方にポート チャネルを提供するために実行されます(図 71)。

ここでは、図 71 に示す vPC とのサービス シャーシ統合のためのいくつかの重要な設計上の考慮事項について説明します。

- サービスを必要とするアクセス スイッチは下位集約 VDC(下部の vPC ドメイン(緑色))に接続されます。
- サービスを必要としないアクセス スイッチは、VDC(上部の vPC ドメイン(赤色))に接続されることがあります。

ネットワーク サービス シャーシと 2 台の vPC ピア デバイス間でレイヤ 3 のピアリングが必要な場合、代替設計を調べる必要があります（たとえば、サービス シャーシを接続する vPC ではなくスパニングツリー プロトコルを使用）。これは、通常、ネットワーク サービス シャーシ内のサービス モジュールがルーテッド モードで設定されている場合の例です。

図 71. VDC サンドイッチ設計のネットワーク サービス シャーシ



vPC で動作するようにネットワーク サービス モジュールを設定する場合は、次の推奨されるベスト プラクティスに従ってください。

一般的な推奨事項:

- 仮想スイッチング レイヤ間にサービスを挿入するように Cisco Nexus 7000 シリーズ VDC を設定します。
- トランスペアレント モードでネットワーク サービスのシャーシ内のサービス モジュールを設定します。
- vPC ドメインとのインタラクションにサービス シャーシによって提供されるポート チャネル（または EtherChannel）機能を使用します。
- サービス シャーシへの inside インターフェイスと outside インターフェイスの両方にポート チャネル接続を提供するために、両方の VDC ペアで実行されるように vPC ドメインを設定します。
- サービスを必要とするアクセス スイッチを下位集約 VDC レイヤに接続します。
- サービスを必要としないアクセス スイッチを集約 VDC レイヤに接続します。

- 必要に応じて、複数の仮想化サービス コンテキストに対応するようにサポートを拡張するために、下位集約 VDC レイヤで複数の VRF インスタンスを使用します。
- 次の vPC を介したレイヤ 3 の設計上の警告に注意してください。レイヤ 3 のピアリングが 2 つの vPC レイヤで必要な場合は、vPC ではなくスパニングツリー プロトコルなどの代替ソリューションを使用して、サービス シャーシに接続することを検討してください。

vPC を使用したトランスペアレント モードのネットワーク サービス アプライアンス

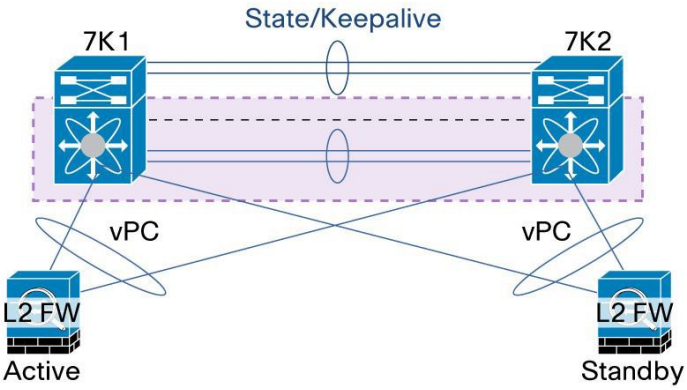
vPC とのトランスペアレント モード統合におけるサービス アプライアンスは、単純な実装です。このタイプの設計について特に警告はありません。

サービス アプライアンスは、ポート チャネルの機能および VLAN 変換をサポートする必要があります。

トランスペアレント モードのサービス アプライアンスは、2 台の vPC ピア デバイスとあらゆる種類の L3 ピアリング隣接を確立する必要がないため、この設計を展開することが非常に簡単になります。

図 72 は、この種のトポロジを示します。

図 72. vPC ドメインに接続されているトランスペアレント モードで設定されたネットワーク サービス アプライアンス



トランスペアレント モードのサービス アプライアンスは、Bump In The Wire のように動作し、VLAN ID を交換することによって inside インターフェイスから outside インターフェイスにトラフィックをブリッジングします。入力 VLAN と出力 VLAN が同じ IP サブネットに関連付けられていることに注意してください。

インターフェイス VLAN（つまり SVI）は、L2/L3 境界を実行する vPC ドメインに残ります（vPC ドメインに定義されたインターフェイス VLAN は下部に接続されたサーバのデフォルト ゲートウェイとして使用されます）。

vPC を使用してトランスペアレント モードでネットワーク サービス アプライアンスを設定する場合は、次の推奨されるベストプラクティスに従ってください。

強力な推奨事項:

- vPC ドメインとのインタラクションにサービス アプライアンスによって提供されるポート チャネル機能を使用します。
- レイヤ 2 ポート チャネルをサービス アプライアンスのステートおよびキープアライブ VLAN 専用にします（vPC ピア リンクを使用しないことを推奨します）。

vPC を使用したトランスペアレント モードでの Cisco ASA サービス アプライアンスの設定

リリース 8.4 以降、Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス ソリューションは、Link Aggregation Control Protocol（LACP）をサポートします。ASA のポート チャネルには、8 つまでのアクティブなメンバー ポートが含まれます。

サポートされている LACP モードは、アクティブ、パッシブ、およびオンです（オンは手動ポート バンドルを意味します。つまダイナミック ポート チャネリング制御プロトコルを使用しません）。

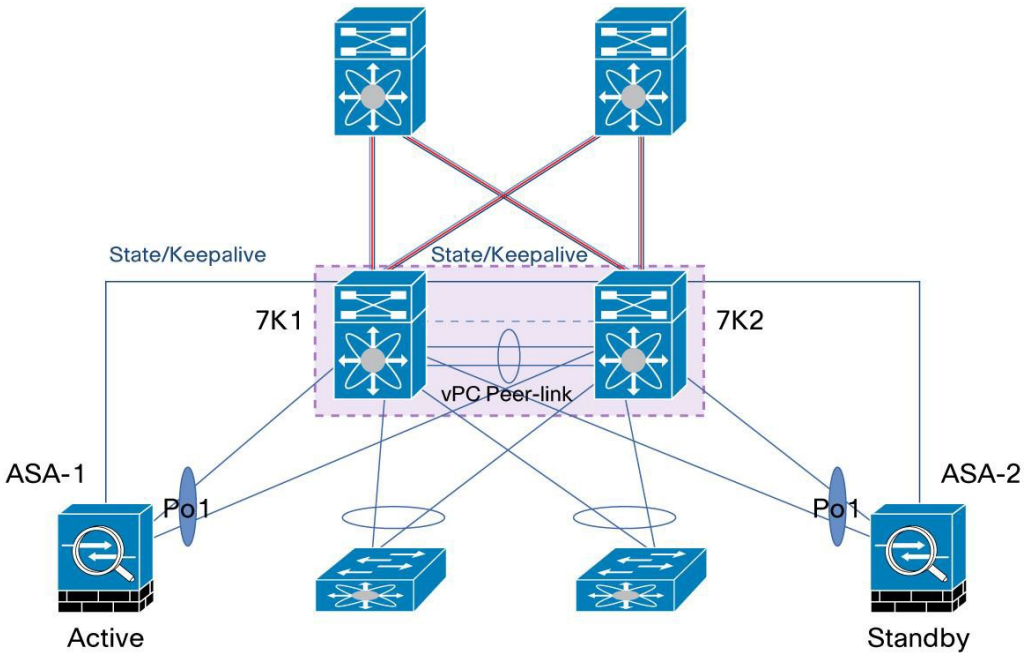
ポート チャネル（または EtherChannel）リンクは Cisco ASA アプライアンスの物理および論理インターフェイスと同様に扱われます。

ASA は、トランスペアレント モードまたはルーテッド モードで設定できます。どちらのモードも、ASA を Cisco Nexus 7000 シリーズの vPC と統合する場合にサポートされます。

ここでは、vPC のコンテキストにおいてトランスペアレント モードで ASA を設定する方法について説明します。ASA デバイスは、vPC リンクを使用して vPC ドメインに接続します。

図 73 で示されているトポロジを参考に見てみましょう。

図 73. vPC ドメインに接続されているトランスペアレント モードで設定された ASA サービス アプライアンス



ASA-1 および ASA-2 はハイ アベイラビリティ（HA）で実行されています。ASA-1 がアクティブ モードで動作し、ASA-2 がスタンバイ モードで動作しています。ASA-1 では、ネットワークからのすべてのフローが処理されます。ASA-1 がダウンした場合、ASA-2 がアクティブになり、後続のフローを処理できます。

VLAN 100 は、入力側（または inside インターフェイス）で使用され、VLAN 200 は出力側（outside インターフェイス）で使用されます。両方とも、IP サブネット 100.100.100.0/24 に関連付けられています。

図 74 は、ASA を使用したネットワークの論理トポロジ構成図を表します。

図 74. vPC ドメインに接続されているトランスペアレント モードの ASA：論理構成図

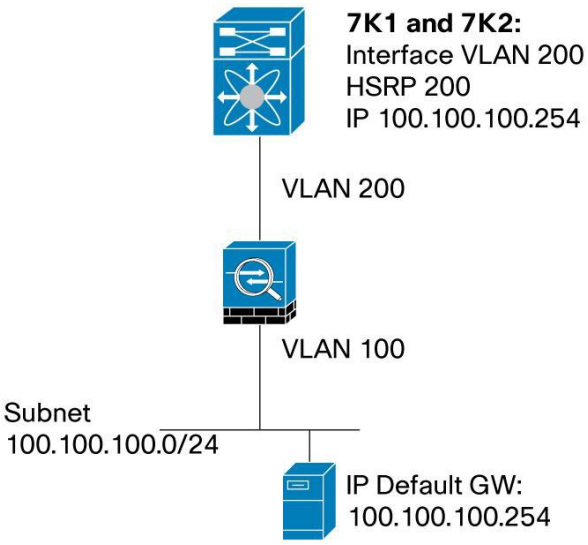


図 74 に示すように、デフォルト ゲートウェイ（HSRP）は、Cisco Nexus 7000 シリーズでホストされます。

サーバが VLAN 100 にある場合、デフォルト ゲートウェイ（GW）は VLAN 200 でホストされます（VLAN 200 上の FHRP）。

理由は ASA ファイアウォールは、inside インターフェイスから outside インターフェイスへの VLAN 変換を実行するからです。

トランスペアレント モードの ASA のサンプル ポート チャネル設定は次のとおりです。

```
ASA configuration:

interface GigabitEthernet0/0
 channel-group 1 mode active
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/2
 channel-group 1 mode active
 no nameif
 no security-level
 no ip address
!
interface Port-channel1
 port-channel load-balance vlan-src-dst-ip
 no nameif
 no security-level
 no ip address
!
```

```
interface Port-channel1.100
 vlan 100
 nameif inside
 bridge-group 1
 security-level 99
!

interface Port-channel1.200
 vlan 200
 nameif outside
 bridge-group 1
 security-level 1
!

interface BVI1
 ip address 100.100.100.5 255.255.255.0 standby 100.100.100.6
!
```

注： ASA のステート/キープアライブ リンクの設定は、上記の例で表示されません。

NEXUS 7000 側（7K1 および 7K2）では、ASA に接続される vPC メンバー ポートの設定は次のとおりです。

```
7K1 and 7K2 configuration - vPC member ports connected to ASA-1:

interface port-channel1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 100,200
  vpc 1
```

```
7K1 and 7K2 configuration - vPC member ports connected to ASA-2:

interface port-channel2
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 100,200
  vpc 2
```

NEXUS 7000 (7K1 および 7K2)のインターフェイス VLAN 200(つまり、SVI 200)の設定は次の通りです。

```
7K1 configuration:

interface Vlan200
  ip address 100.100.100.1/24
  no ip redirect
```

```
  hsrp 200
    ip 100.100.100.254
  no shutdown
```

```
7K2 configuration:

interface Vlan200
  ip address 100.100.100.2/24
  no ip redirect
  hsrp 200
    ip 100.100.100.254
  no shutdown
```

ASA のポート チャネル ハッシュ アルゴリズムおよび Cisco Nexus vPC のハッシュ アルゴリズムが両側で同じであることを推奨します。これにより、アップストリームおよびダウンストリームのトラフィックが同じポート チャネル メンバー ポートを使用できます（ただし、一貫した結果を得るには、パス全体に（つまり、L3 コアまで）同じロード バランシング ハッシュ アルゴリズムを適用します）。ASA ファイアウォールおよび NEXUS 7000 vPC ピア デバイスに設定したロードバランシング ハッシュ アルゴリズムを確認するには、次の show コマンドを使用します。

```
ASA-1# sh port-channel 1 load-balance
EtherChannel Load-Balancing Configuration:
        vlan-src-dst-ip-port

EtherChannel Load-Balancing Addresses UsedPer-Protocol:
Non-IP: Source XOR Destination MAC address
  IPv4: Vlan ID and Source XOR Destination IP address and TCP/UDP (layer-4)port
number
  IPv6: Vlan ID and Source XOR Destination IP address and TCP/UDP (layer-4)port
number
```

```
7K1# sh port-channel load-balance

Port Channel Load-Balancing Configuration:
System: src-dst ip-l4port-vlan

Port Channel Load-Balancing Addresses Used Per-Protocol:
Non-IP: src-dst mac
IP: src-dst ip-l4port-vlan
```

vPC を使用したルーテッド モードのネットワーク サービス アプライアンス

L3 リンクを使用して vPC ドメインに接続されるルーテッド モードのサービス アプライアンスは、単純な設計で、vPC 設定に関する特別な注意なしに完全に動作します。これは、vPC ドメインにルーテッド モードのサービス アプライアンスを接続する推奨方法です。

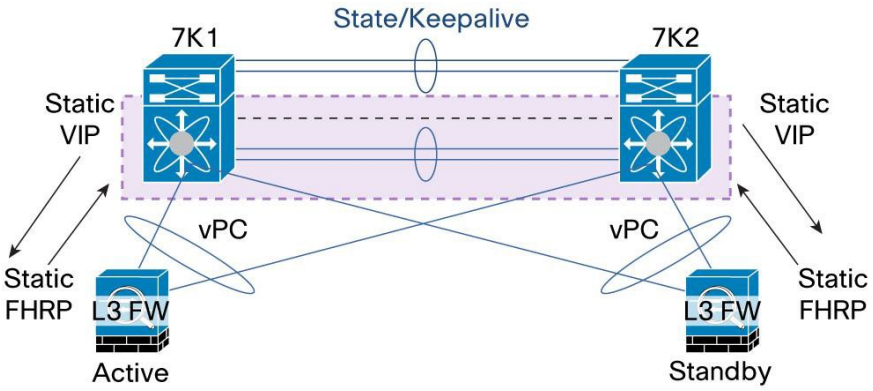
強力な推奨事項:

可能であれば L3 リンクを使用して vPC ドメインにルーテッド モードのサービス アプライアンスを接続します。これは、vPC ドメインにサービス アプライアンスを接続するための最も推奨される方法です。

ただし、前の推奨事項を満たすことができない場合、2 つのエンティティ間の vPC リンクまたはシングル リンクを使用して vPC ドメインにサービス アプライアンスを接続することもできます。これは、特定の設計ガイドラインに沿っている場合に限り実行できます。設計目的は、vPC 上の L3 の問題を避けることです。

vPC リンクまたはシングル リンクを使用して vPC ドメインにサービス アプライアンスを接続するには、次の 2 つの方法があります。これらを、図 75 および 76 に示します。

図 75. vPC リンクを使用して vPC ドメインに接続されるルーテッド モードのサービス アプライアンス



この設計（図 75）では、L3 サービス アプライアンスは各 vPC ピア デバイスに vPC 接続されています。

L3 サービス アプライアンスは、アクティブ-スタンバイ モードで動作しています。1 台のデバイスがアクティブ ステート、もう一方のデバイスがスタンバイ モードになっています。

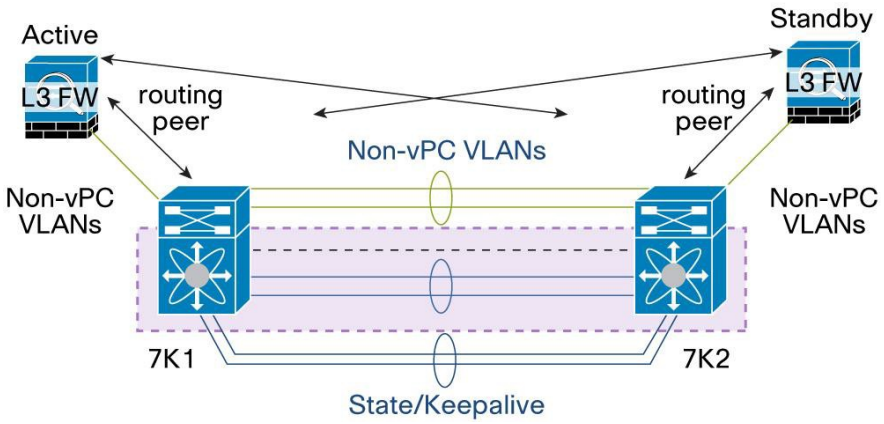
vPC ループ回避状況になるのを回避するには、次のルールを使用して、L3 サービス アプライアンスと vPC ドメイン間の L3 隣接を正しく設定します。

L3 サービス アプライアンスで、vPC ドメインで定義されている HSRP/VRRP VIP（仮想 IP）を指し示すスタティック ルート（デフォルト ルートにすることができます）を作成します。このようにすると、L3 サービス アプライアンス（アクティブ ステートのいずれかのアプライアンス）は任意の vPC デバイスにトラフィックを送信できます。vPC ピア デバイスは両方とも HSRP アクティブ（データ プレーンの観点から）であるため、L3 サービス アプライアンスから着信するトラフィックをルーティングできます。

vPC ドメインから L3 サービス アプライアンスへのリターン トラフィックについては、L3 サービス アプライアンスで定義されたスタティック VIP を指す各 vPC ピア デバイス上でスタティック ルートを作成します。L3 サービス アプライアンスの VIP がアクティブ インスタンスとスタンバイ インスタンスの両方で同一です。アクティブな L3 サービス アプライアンスのみが VIP（つまり、VIP アドレスを宛先としたパケット）を所有します。

この設計では、通常、L3 サービス アプライアンスは vPC ドメインに接続されているサーバのデフォルト IP ゲートウェイをホストし、vPC ドメインで作成された HSRP/VRRP グループは L3 サービス アプライアンスと各 vPC ピア デバイス間の L3 接続だけに使用されます。

図 76. シングル リンクを使用して vPC ドメインに接続されるルーテッド モードのサービス アプライアンス



この設計（図 76）では、L3 サービス アプライアンスは各 vPC ピア デバイスにシングル接続されています。

vPC ドメインにシングル接続されたデバイスで一般的に推奨されるため、非 vPC VLAN をこの目的に使用し、2 台の vPC ピア デバイスに非 vPC VLAN トラフィックを伝送するための専用スイッチ間リンクを追加します。

L3 サービス アプライアンスは、問題なくこの専用インフラストラクチャ上に両方の vPC ピア デバイスとの L3 ルーティング プロトコル ピアリング隣接関係を確立できます。

この設計では、両方の vPC ピア デバイスが vPC ドメインに接続されているサーバのデフォルト IP ゲートウェイをホストします。

L3 サービス アプライアンスは、ルーティング ポリシーで定義された L3 パスに応じてサーバ間におけるトラフィックを処理します。

vPC ドメインに接続されているルーテッド モードのネットワーク サービス アプライアンスを設定する場合は、次の推奨されるベスト プラクティスに従ってください。

強力な推奨事項:

- レイヤ 2 ポート チャネルをサービス アプライアンスのステートおよびキープアライブ VLAN 専用にします（vPC ピア リンクを使用しないことを推奨します）。
- サービス アプライアンスを vPC 経由で vPC ドメインに接続し、サービス アプライアンス側で HSRP/VRRP アドレスへのスタティック ルートを設定します。Cisco Nexus 7000 シリーズ側で、サービス アプライアンスの VIP を指し示すスタティック ルートを作成します（図 75）。
- 非 vPC VLAN を使用してシングル リンク経由で各 vPC ピア デバイスにサービス アプライアンスを接続します。2 台の vPC ピア デバイスにわたる非 vPC VLAN トラフィック用に個別のスイッチ間レイヤ 2 ポート チャネルを実装します（図 76）。

vPC を使用したルーテッド モードでの Cisco ASA サービス アプライアンスの設定

リリース 8.4 以降、Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス ソリューションは、Link Aggregation Control Protocol（LACP）をサポートします。ASA のポート チャネルには、8 つまでのアクティブなメンバー ポートが含まれます。

サポートされている LACP モードは、アクティブ、パッシブ、およびオンです（オンは手動ポート バンドルを意味します。つまダイナミック ポート チャネリング制御プロトコルを使用しません）。

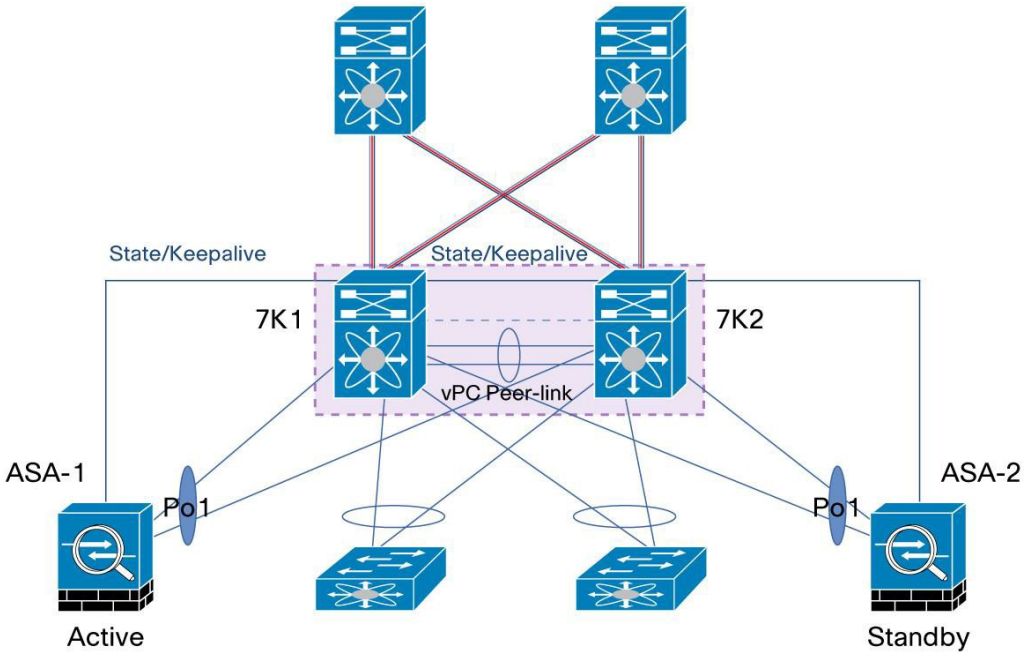
ポート チャネル（または EtherChannel）リンクは Cisco ASA アプライアンスの物理および論理インターフェイスと同様に扱われます。

ASA は、トランスペアレント モードまたはルーテッド モードで設定できます。どちらのモードも、ASA を Cisco Nexus 7000 シリーズの vPC と統合する場合にサポートされます。

ここでは、vPC のコンテキストにおいてルーテッド モードで ASA を設定する方法について説明します。ASA デバイスは、vPC リンクを使用して vPC ドメインに接続します。

図 77 で示されているトポロジを参考に見てみましょう

図 77. vPC ドメインに接続されているルーテッド モードで設定された ASA サービス アプライアンス



ASA-1 および ASA-2 はハイ アベイラビリティ（HA）で実行されています。ASA-1 がアクティブ モードで動作し、ASA-2 がスタンバイ モードで動作しています。ASA-1 では、ネットワークからのすべてのフローが処理されます。ASA-1 がダウンした場合、ASA-2 がアクティブになり、後続のフローを処理できます。

VLAN 100 は、入力側（または inside インターフェイス）で使用され、VLAN 200 は出力側（outside インターフェイス）で使用されます。VLAN 100 は IP サブネット 100.100.100.0/24 に関連付けられ、VLAN 200 は IP サブネット 200.200.200.0/24 に関連付けられています。

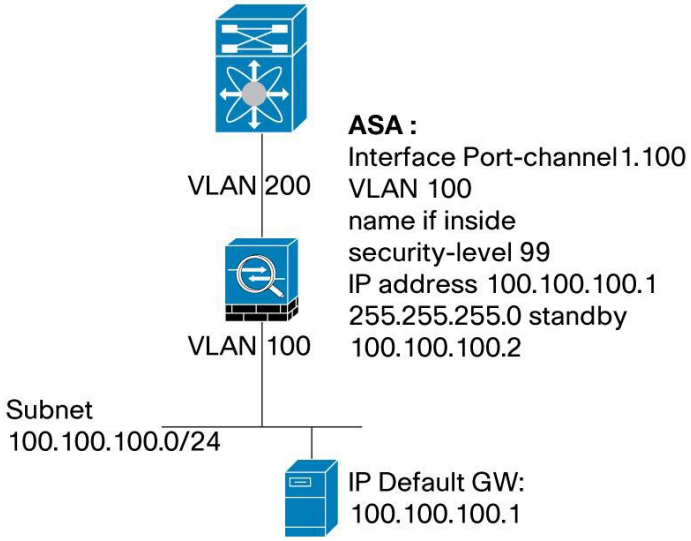
ASA は vPC ドメインに接続されているサーバのデフォルト IP ゲートウェイをホストします。この設計では、ポート チャネル 1 にはサブインターフェイス Po1.100 が設定されています。VLAN 100 は Po1.100 内で伝送され、サブインターフェイスには、サーバがデフォルト ゲートウェイとして使用する IP アドレスである 100.100.100.1/24 が設定されています。

サブインターフェイス Po1.100 が inside インターフェイスとして定義されていることに注意してください（つまり、ASA ファイアウォールで最もセキュアなインターフェイス）。

ポート チャネル 1 には、サブインターフェイス Po1.200 も設定されています。VLAN 200 は Po1.200 内で伝送され、サブインターフェイスには IP アドレス 200.200.200.1/24 が設定されています。サブインターフェイス Po1.200 は outside インターフェイス（ASA ファイアウォールであまりセキュアではないインターフェイス）として定義されます。

図 78 は、ASA を使用したネットワークの論理トポロジ構成図を表します。

図 78. vPC ドメインに接続されているルーテッド モードの ASA：論理構成図



ルーテッド モードの ASA のサンプル ポート チャネル設定は次のとおりです。

```
ASA configuration:

interface GigabitEthernet0/0
 channel-group 1 mode active
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/2
 channel-group 1 mode active
 no nameif
 no security-level
 no ip address
!
interface Port-channel1
 port-channel load-balance vlan-src-dst-ip
 no nameif
 no security-level
 no ip address
!
interface Port-channel1.100
 vlan 100
 nameif inside
 security-level 99
 ip address 100.100.100.1 255.255.255.0 standby 100.100.100.2
!
```

```
interface Port-channel1.200
 vlan 200
 nameif outside
 security-level 1
 ip address 200.200.200.1 255.255.255.0 standby 200.200.200.2
!
```

注: ASA のステート/キープアライブ リンクの設定は、上記の例で表示されません。

NEXUS 7000 側（7K1 および 7K2）では、ASA に接続される vPC メンバー ポートの設定は次のとおりです。

```
7K1 and 7K2 configuration - vPC member ports connected to ASA-1:

interface port-channel1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 100,200
  vpc 1
```

```
7K1 and 7K2 configuration - vPC member ports connected to ASA-2:

interface port-channel2
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 100,200
  vpc 2
```

ASA と NEXUS 7000（7K1 および 7K2）の L3 設定を次に示します。

```
ASA configuration:

route outside 0.0.0.0 0.0.0.0 200.200.200.200 1
```

```
7K1 configuration:

interface Vlan200
  ip address 200.200.200.10/24
  no ip redirect
  hsrp 200
    ip 200.200.200.200

ip route 100.100.100.0/24 Vlan200 200.200.200.1 name ASA
```

（サブネット 100.100.100.0/24 は、ASA ファイアウォールによって処理されるサブネットです）

```
7K2 configuration:

interface Vlan200
  ip address 200.200.200.11/24
  no ip redirect
  hsrp 200
    ip 200.200.200.200

ip route 100.100.100.0/24 Vlan200 200.200.200.1 name ASA
```

（サブネット 100.100.100.0/24 は、ASA ファイアウォールによって処理されるサブネットです）

ASA のポート チャネル ハッシュ アルゴリズムおよび Cisco Nexus vPC のハッシュ アルゴリズムが両側で同じであることを推奨します。これにより、アップストリームおよびダウンストリームのトラフィックが同じポート チャネル メンバー ポートを使用できます（ただし、一貫した結果を得るには、パス全体に（つまり、L3 コアまで）同じロード バランシング ハッシュ アルゴリズムを適用します）。ASA ファイアウォールおよび NEXUS 7000 vPC ピア デバイスに設定したロードバランシング ハッシュ アルゴリズムを確認するには、次の show コマンドを使用します。

```
ASA-1# sh port-channel 1 load-balance
EtherChannel Load-Balancing Configuration:
        vlan-src-dst-ip-port

EtherChannel Load-Balancing Addresses UsedPer-Protocol:
Non-IP: Source XOR Destination MAC address
  IPv4: Vlan ID and Source XOR Destination IP address and TCP/UDP (layer-4)port
number
  IPv6: Vlan ID and Source XOR Destination IP address and TCP/UDP (layer-4)port
number
```

```
7K1# sh port-channel load-balance

Port Channel Load-Balancing Configuration:
System: src-dst ip-l4port-vlan

Port Channel Load-Balancing Addresses Used Per-Protocol:
Non-IP: src-dst mac
IP: src-dst ip-l4port-vlan
```

マルチキャストおよび vPC のベスト プラクティス

マルチキャスト トラフィックは、複数のシナリオで vPC ドメイン上を伝送できます。

- マルチキャスト送信元は、vPC リンクの背後の L2 ドメインまたは vPC ドメインの外部の L3 コアで接続できます
- マルチキャスト受信側は、vPC リンクの背後の L2 ドメインまたは vPC ドメインの外部の L3 コアで接続できます。

L3 マルチキャスト ルーティング プロトコルの観点から、vPC は PIM SM（Protocol Independent Multicast Sparse Mode）を完全にサポートします。各 vPC ピア デバイスは PIM SM 関連のコマンドで設定でき、vPC ドメインは同様に PIM SM で設定された L3 コアと対話できます。1 つの VLAN からのマルチキャスト トラフィックは、マルチキャスト受信側が接続されている他の VLAN に適切にルーティングできます。

Cisco Nexus 7000 シリーズは、(*, G) および (S, G) の両方の mroute エントリについて、ハードウェアでの PIM スパース モードをサポートします。

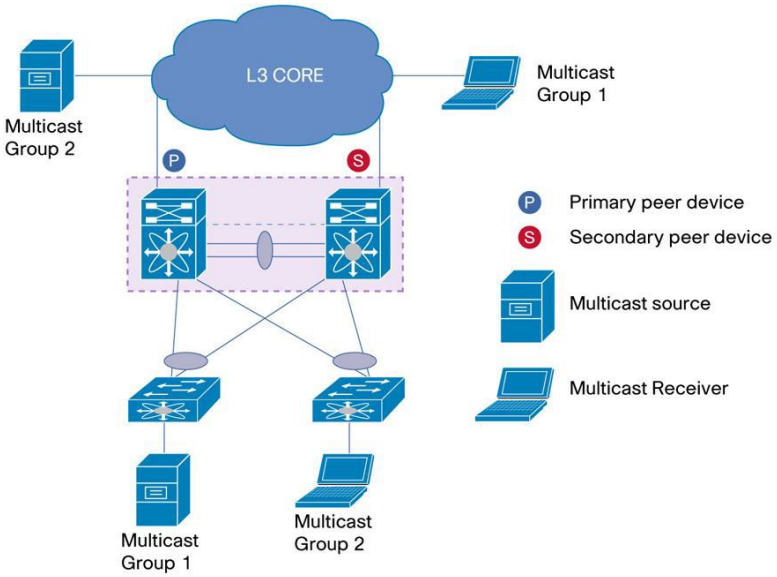
図 79 は、vPC でのマルチキャストのシナリオを示します（vPC ドメインの内部または外部のマルチキャスト送信元および受信側）。

注： マルチキャスト送信元およびマルチキャスト受信側が同じ VLAN にある場合、ダイナミック マルチキャスト ルーティング プロトコルをオンにする必要はありません。

PIM-SSM（Source Specific Multicast）および PIM Bidir（BiDirectional）は vPC でサポートされていないことに注意してください。

2 つのマルチキャスト ルーティング プロトコルの 1 つがネットワークで必須の場合、vPC テクノロジーに基づいていない L2 ネットワーク設計の他の実装を検討してください。

図 79. vPC でのマルチキャスト



vPC は、インターネット グループ管理プロトコル（IGMP）ステートを同期するために Cisco Fabric Services（CFS）を使用します。IGMP パケットが送信元インターフェイスの情報とともに送信されるため、同等のステートを両方の vPC ピアの vPC メンバーで確立でききます。

vPC ドメイン内にあるマルチキャスト送信元については、vPC ピア デバイスは両方ともアクティブ フォワーダです。重複は、vPC ループ回避ロジックによって避けられます。

レイヤ 3 コア内のマルチキャスト送信元については、マルチキャスト送信元への最適なユニキャスト メトリックを持つ vPC ピア デバイスがアクティブなフォワーダになります。Cisco Fabric Services を使用すると、vPC ピア デバイス間の通信でアクティブなフォワーダを判別できるようになります（マルチキャスト送信元 wins への最適なユニキャスト メトリックがアクティブになります）。メトリックが両方の vPC ピア デバイスで同じ場合、機能上のプライマリ vPC ピア デバイスがアクティブなフォワーダになります。

vPC テクノロジーでは、アクティブなフォワーダの概念が、マルチキャスト送信元（L3 コアの場合のマルチキャスト送信元）単位であることに注意してください。マルチキャスト送信元 S1 と S2 に vPC デバイスに関して同じユニキャスト ルーティング メトリックがない場合、アクティブなフォワーダはそれに合わせて変更されます（例として、vPC ピア デバイス 1 は S1 のアクティブなフォワーダになることができ、vPC ピア デバイス 2 は S2 のアクティブなフォワーダになることができます）。

必須の推奨事項:

- vPC では PIM SM（Protocol Independent Multicast Sparse Mode）のみを使用します。PIM SSM（Source Specific Mode）および PIM BiDir（Bidirectional）は vPC と相互運用しません。

一般的な推奨事項:

- 操作を簡易化するために、vPC プライマリ ピア デバイスで PIM DR（指定ルータ）を設定します。

マルチキャストが vPC でどのように動作するかを理解するために、図 80 で示されているトポロジを見てみましょう。マルチキャスト送信元は L3 コアにあり、マルチキャスト受信側は vPC ドメインにあります。

マルチキャスト PIM RP（Rendez-vous Point）は L3 コアにあり、vPC ピア デバイスに接続されているルータにエニーキャスト RP が設定されています。

図 80. vPC でのマルチキャストの動作（マルチキャスト パケット フロー）

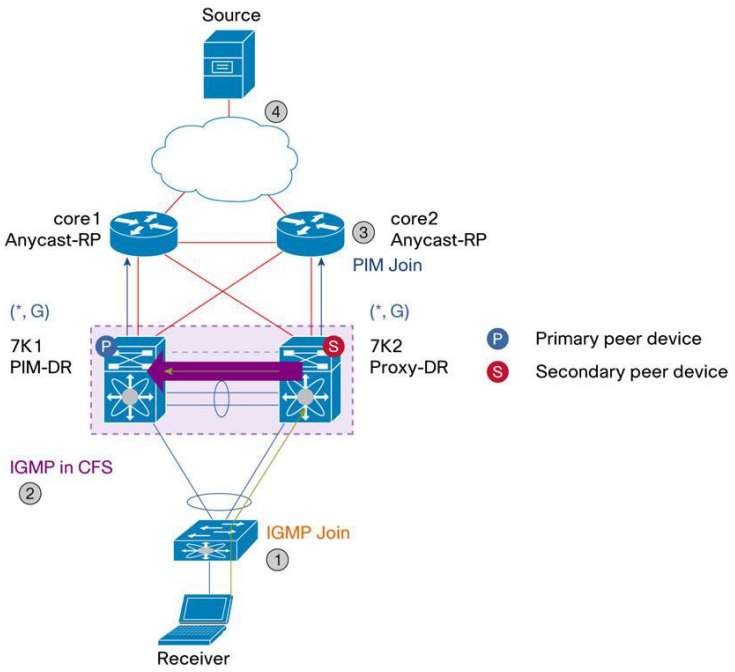
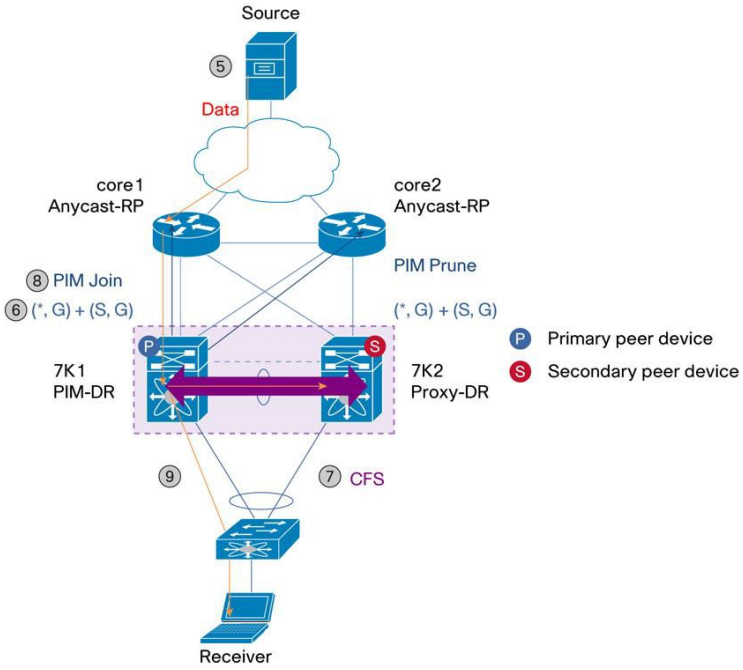


図 80 に示すように、マルチキャスト パケット フローは、次のとおりです。

1. 受信側は IGMP Join を送信し、アクセス スイッチのポート チャネル ハッシュが vPC ピア デバイス 2（7K2）へのリンクを選択します。7K2 は OIF（発信インターフェイス リスト）として VPC VLAN のスヌーピング、IGMP、および (*,G) mroute ステートを作成します。
2. vPC ピア デバイス 2（7K2）は、CFS にカプセル化された IGMP パケットを vPC ピア デバイス 1（7K1）に送信します。7K1 は、vPC ピア デバイス 2（7K2）と同一のマルチキャスト ステートを作成します。
3. 両方の vPC ピア デバイスが RPT（RP ツリー）に参加する RP に PIM (*,G) Join を送信します。RPT は、PIM SM のコンテキストで共有ツリーとも呼ばれます。
4. ECMP への RP の場合、ハッシュが RPF インターフェイスを選択します。

図 81. vPC でのマルチキャストの動作（マルチキャスト パケット フロー）：続き



5. 送信元は送信し始めます。ファースト ホップ ルータは RP に送信元を登録します
6. 一方または両方の VPC ピアは共有ツリーで (S,G) トラフィックを受信します（アップストリーム ステートによって異なります）
7. vPC ピア デバイスがアクティブなフォワーダのロールをネゴシエートします。フォワーダを決定するために交換される CFS（Cisco Fabric Services）メッセージ、マルチキャスト送信元 wins への最適なユニキャスト ルーティング メトリック、同じ場合は vPC の動作可能なプライマリ ピア デバイス wins。このマルチキャスト送信元のアクティブなフォワーダとして vPC ピア デバイス 1（7K1）が選択されていることを想定します。
8. (S,G) のアクティブなフォワーダとして選択されている vPC ピア デバイス 1（7K1）は、PIM (S,G) Join を送信元に送信します。これは SPT（最短パス ツリー）に参加し、RPT（RP ツリー、別名共有ツリー）をプルーニングして、vPC VLAN に関連付けられた SVI を L3 OIF として追加します。
9. マルチキャスト データ トラフィックは送信元ツリーを通過してアクティブな転送 vPC ピア デバイスに伝送されます。

   vPC ピア デバイス 1（7K1）は、アクセス スイッチに接続された vPC メンバー ポートからマルチキャスト トラフィックのコピーを送信します。もう一方のコピーは vPC ピア リンクから送信されます。反対側にこのマルチキャスト トラフィックに関心のあるシングル接続デバイス（または孤立ポートが）がないため vPC ピア デバイス 2（7K2）は、vPC ピア リンクから受信したマルチキャスト トラフィックをドロップします。

vPC（PIM pre-build-spt）でのマルチキャスト用の短いパスの事前構築

vPC でのマルチキャストのデフォルト動作には次の特性があります。

- アクティブ フォワーダの変更時のコンバージェンス遅延により、新規フォワーダがアップストリーム Join をトリガーして、SPT（最短パス ツリー）を再構築します。これは、たとえばアクティブなフォワーダがダウンしたときに発生します。
- 定期的な (S,G) ステートの期限切れのときに (*,G) で転送が行われるため、非フォワーダからの定期的な複製が行われることがあります

これらの問題に対応するために、PIM Pre-build SPT と呼ばれる vPC によるマルチキャストの拡張機能が開発されました。

目的は、vPC テクノロジーのデュアル フォワーダの動作を利用して、両方の vPC ピア デバイスでアクティブ/アクティブ マルチキャスト パケット転送（ライブ/ライブ データ ストリーム）を作成することです。

非フォワーダの PIM Pre-build SPT は、OIF（発信インターフェイス）リストのインターフェイスを設定しないでアップストリーム PIM J/Ps（Join/Prune）をトリガーすることによって、マルチキャスト トラフィックを引き付けます。マルチキャスト トラフィックは常に非アクティブ フォワーダに引き込まれ、OIF がないため最後にドロップされます。PIM Pre-build SPT 機能は、次のグローバル コンフィギュレーション ノブ経由でオンまたはオフにすることができます。

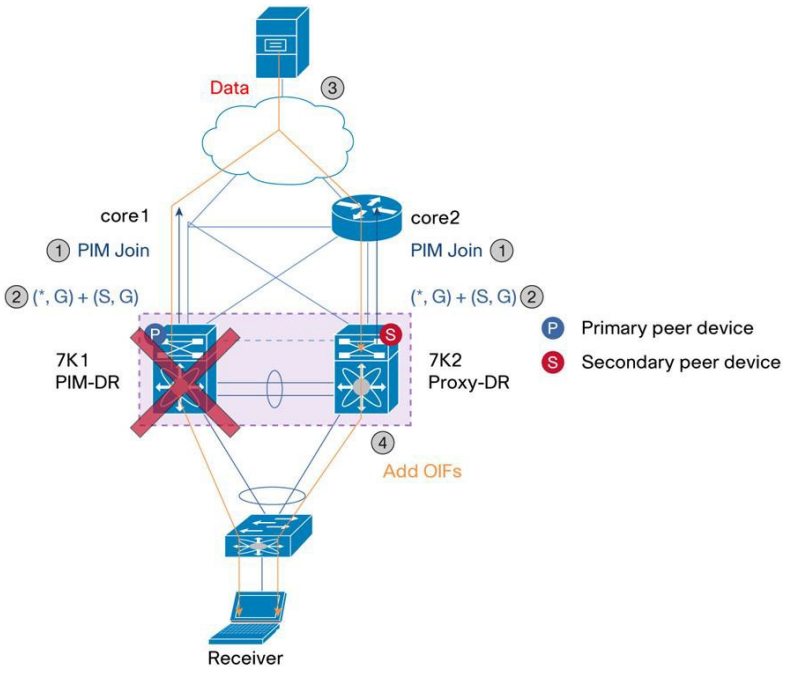
```
7K(config)# ip pim pre-build-spt
```

PIM Pre-build SPT は即座に有効になるため、アクティブ フォワーダの障害時のコンバージェンス時間が短縮されます（その結果、コンバージェンス時間は 1～3 秒になります）。（非アクティブ フォワーダではない）他の vPC ピア デバイスは、新しいアップストリームのマルチキャスト ステートを作成する必要はないため、OIF（発信インターフェイス）リストを正しくプログラミングすることによって、アクティブなフォワーダのロールにすぐに遷移できます。

PIM prebuild SPT のイネーブル化による影響は安定状態のプライマリおよびセカンダリ データ パス（つまり、vPC プライマリおよびセカンダリ ピア デバイス）の帯域幅とレプリケーションの容量を消費することです。

PIM prebuild SPT の機能と、vPC システムがどのようにアクティブなフォワーダの障害イベントに反応するかを図 82 に示します。

図 82. vPC でのマルチキャスト：PIM Prebuild SPT



1. フォワーダと非フォワーダの両方の vPC ピア デバイスは新しいマルチキャスト送信元の SPT（最短パス ツリー）に参加します。
2. マルチキャスト データ トラフィックは、送信元ツリーから両方の vPC ピア デバイス（7K1 および 7K2）に伝送されます。7K1 はアクティブなフォワーダです。そのため、vPC メンバー ポートからマルチキャスト トラフィックを伝播します。他の vPC ピア デバイス（7K2）は非アクティブ フォワーダであるため、アップストリーム ネットワークから受信したマルチキャスト トラフィックをドロップします（OIF リストは空です）。
3. アクティブなフォワーダ（vPC ピア デバイス 1、つまり 7K1）に障害が発生した場合、他の vPC ピア デバイス（7K2）が新しいアクティブ フォワーダになります。7K2 がすでにハードウェアにプログラミングされた (S,G) ステートで、マルチキャスト トラフィックを受信しているため、実行する必要がある唯一のアクションは OIF リストで vPC メンバー ポートをプログラミングすることです。

強力な推奨事項:

- vPC でマルチキャストを使用する場合は、PIM prebuild SPT を常にイネーブルにします。

FEX と vPC のベスト プラクティス

FEX（ファブリック エクステンダ、別名 NEXUS 2000）は、NEXUS 7000 デバイスそのものである一意の設定管理ポイントを維持しながら、サーバの近くに TOR（トップ オブ ラック）デバイス（つまり、FEX）を配置できるポート拡張テクノロジーです。

FEX を NEXUS 7000 スイッチに接続すると、次の利点が得られます。

- サーバ ケーブル接続コスト面での FEX としての TOR の利点は、サーバの近くに配置できることです。
- FEX の設定およびモニタリング面での EOR（End Of Row）の利点は、親スイッチ（1 つの一意の管理ポイント）にあります。FEX のポートは、親スイッチのインターフェイス リストに表示され、FEX に関連する SNMP/SYSLOG 情報は NEXUS 7000 デバイスで直接管理されます。

FEX は次の親ラインカードに接続できます。

- 32 X 10 Gbps ETH ポート ラインカード（N7K-M132XP-12 および N7K-M132XP-12L）
- NX-OS 6.0 以降でサポートされる FEX の 48 X 1/10-Gbps ETH ポート ラインカード（N7K-F248XP-25）

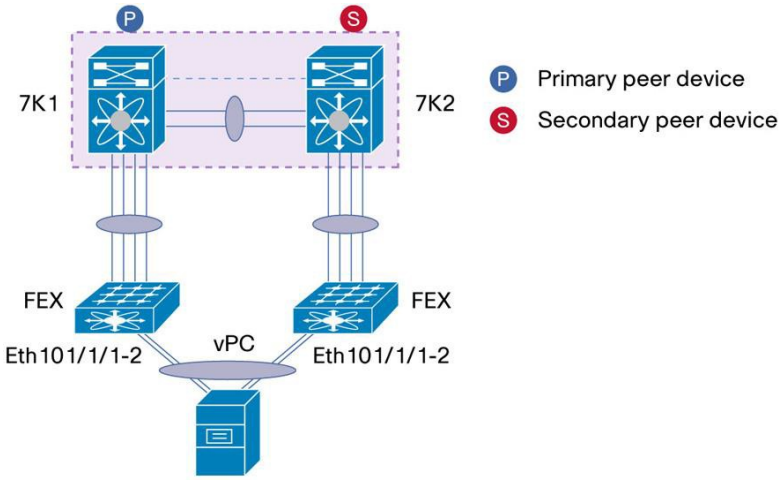
モデルは次のとおりです。

- 2232PP（32 X 1/10 Gbps ファイバ ホスト インターフェイスと 8 X 10 Gbps FEX アップリンク）
- 2248（48 X 100 Mbps/1 Gbps 銅線ホスト インターフェイスと 4 X 10 Gbps FEX アップリンク）
- 2224（24 X 100 Mbps/1 Gbps 銅線ホスト インターフェイスと 4 X 10 Gbps FEX アップリンク）

FEX を使用するために NX-OS ライセンスは必要ありません。

NX-OS 5.2 コード リリースは、FEX の vPC 機能をサポートする最初のリリースです。機能は、**ホスト vPC** とも呼ばれ、サーバはポート チャネル経由で 2 つの異なる FEX にデュアル接続されます。各 FEX は 1 台の親スイッチと vPC ドメインを形成する 2 台の親スイッチに接続されます。ホスト vPC は、図 83 に示されています。

図 83. vPC の FEX：ホスト vPC



FEX（2224、2248、および 2232）のすべてのモデルでは最大 8 個のポート チャネル メンバー ポートをサポートします。

ホスト vPC 設定におけるメンバー ポートの総数の最大は 16 です。

ホスト vPC 設定では、両方の FEX モデルが vPC の両側で一致する必要はありません。

FEX 2224 を左側で使用し、FEX 2248 をインターフェイスの右側で使用できます。

注： FEX 2232PP は HIF（ホスト インターフェイス ポート）のファイバ接続をサポートしています。したがって、一方の 2232PP ともう一方の 2248 の混在は、2248 で銅線接続がサポートされているため技術的には可能ではありません（同じポート チャネル バンドルにファイバおよび銅線ポートを混在させることはできません）。

操作を簡易化するための推奨事項は、VPC の両側で同じ FEX モデルを使用することです。

FEX のホスト側のポートは、switchport mode access または switchport mode trunk（したがって、複数の VLAN の伝送）で設定できます。これらのポートを spanning-tree port type edge または edge trunk で設定して、フォワーディング ステートにすばやく遷移するようにポートに強制します。

注： デフォルトでは、FEX のホスト側のポートにはスパニングツリー BPDU ガードが設定され、機能をディセーブルにするノブはありません。FEX ホスト インターフェイスは STP BPDU を処理できず、発生した場合、ポートが err-disabled ステートに設定されます。

ホスト vPC 設定は、従来の vPC 設定に似ており、次に示します。

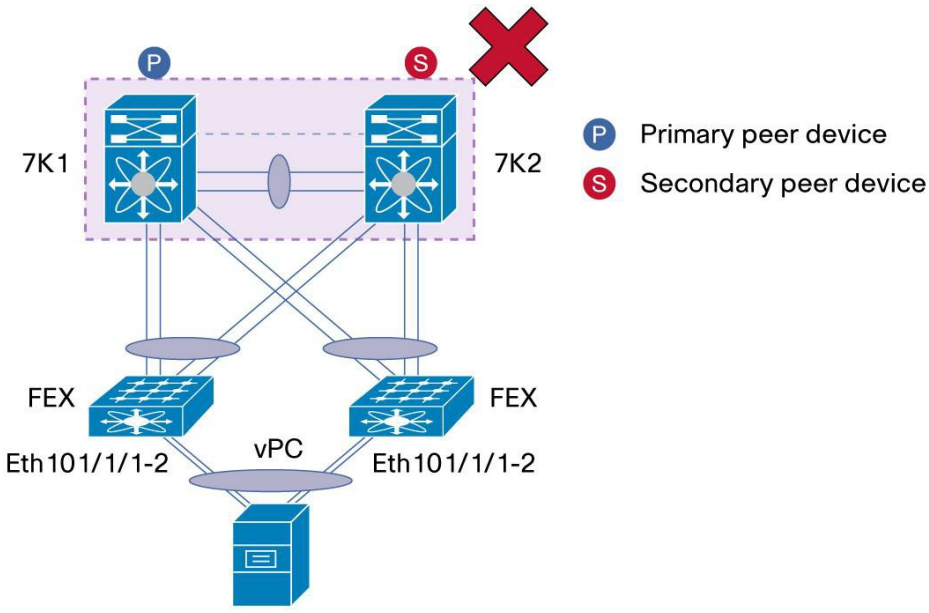
```
7K1:
interface eth101/1/1-2
channel-group 10 mode active

Int port-channel10
switchport
  switchport mode trunk
  switchport trunk allowed vlan 1-20
vpc 10
```

```
7K2:
interface eth101/1/1-2
channel-group 10 mode active

Int port-channel10
switchport
  switchport mode trunk
  switchport trunk allowed vlan 1-20
vpc 10
```

注: 次の設計は、NX-OS 6.0 で FEX および vPC でサポートされていません。

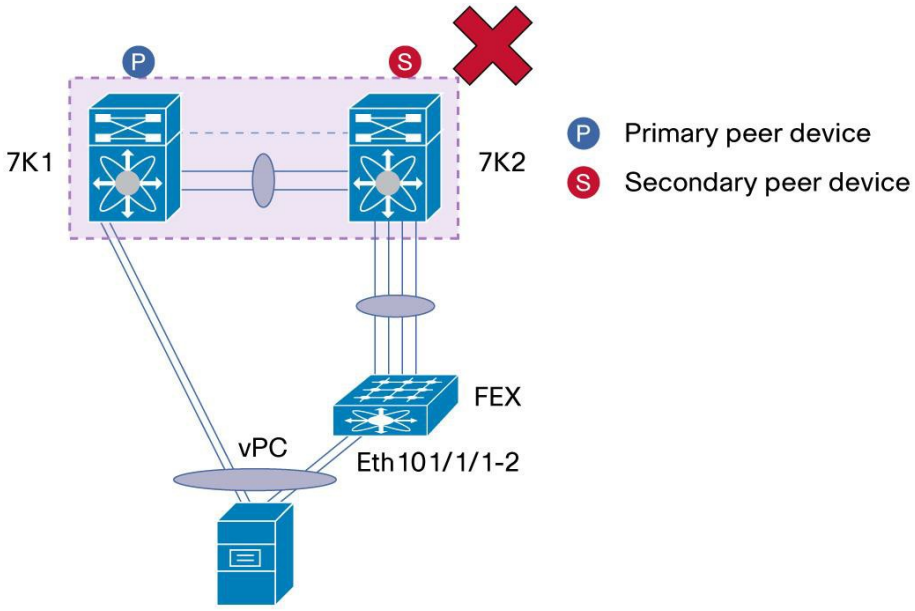
- eVPC(拡張 vPC):図 84
- 一方のレッグが FEX にあり、もう一方のレッグが NEXUS 7000 ラインカードにある vPC

図 84. vPC の FEX:eVPC(拡張 vPC):未サポート



eVPC(拡張 vPC)は FEX が 2 台の異なる親スイッチに vPC 接続され、サーバが 2 つの FEX に vPC 接続される(この設計は、2 レイヤ vPC とも呼ばれます)構成です。これは、vPC モードの NEXUS 7000 シリーズ スイッチの FEX ではサポートされません。

図 85. vPC の FEX：一方のレッグが FEX にあり、もう一方のレッグが NEXUS 7000 ラインカードにある vPC：未サポート



この設計では、サーバが次のタイプの接続を使用して vPC ドメインに vPC 接続されます。
左側の vPC レッグが NEXUS 7000 統合ラインカードに、右側の vPC レッグが FEX に接続されます。

このタイプの設計はサポートされません。

サーバは 2 台の異なる FEX デバイスに vPC 接続するか、2 つの異なる NEXUS 7000 統合ラインカードに vPC 接続する必要があります。vPC 接続用に FEX および統合ラインカードを混在させることは許可されません。

ホスト vPC 設定を適切に構築するには、次のベスト プラクティスおよび推奨事項に従います。

強力な推奨事項:

- それぞれ 1 台の vPC ピア デバイスに接続された 2 つの異なる FEX にサーバをデュアル接続します。他のタイプの接続（たとえば、一方の vPC レッグを NEXUS 7000 統合ラインカードに、もう一方の vPC レッグを FEX に接続）を使用しないでください。
- vPC のスケーラビリティ番号（マニュアルの最初のリンク）がテストおよびサポートされている vPC 設定内にあることを確認します。

一般的な推奨事項:

- vPC の両側で同じ FEX モデルを使用します（つまり、2224-2224、2248-2248、2232-2232）。

VDC と vPC のベスト プラクティス

仮想デバイス コンテキスト（VDC）は、Cisco Nexus 7000 シリーズで動作するスイッチの仮想インスタンスです。

NX-OS 6.0 リリースでは、Cisco Nexus 7000 シリーズ シャーシは最大 4 つの VDC をサポートします。

同じシャーシ内の VDC インスタンスは、他の VDC の動作に影響を与えることなく VDC 内で機能をオンにできるという意味で、互いに依存しません。

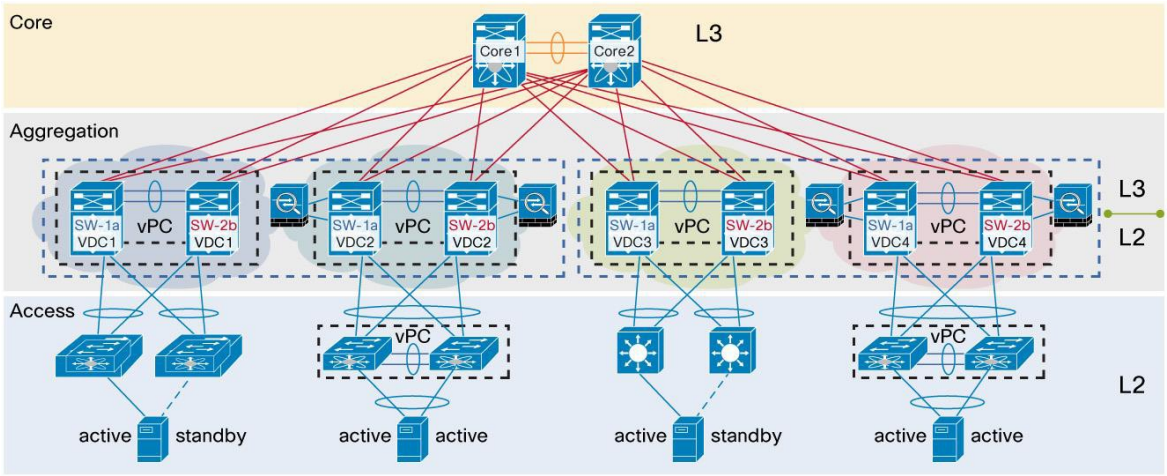
vPC テクノロジーは、VDC でシームレスに機能します。vPC 機能を VDC でイネーブルにする場合、特に制約はありません。vPC 機能に加え、他のすべての L2 や L3、またはセキュリティや QoS 機能を、他の VDC とのコリジョンを作成せずにイネーブルにできます。たとえば、インターフェイス VLAN 機能、OSPF 機能、PIM 機能、および QoS 設定は、vPC 機能がイネーブルになっている VDC に適用できます。

Cisco Nexus 7000 シリーズ シャーシの VDC 機能を使用するには、LAN_ADVANCED_SERVICES_PKG ライセンスをインストールする必要があります。

VDC には 1 つの vPC ドメインだけ設定できます。同じ VDC 内に複数の vPC ドメインを定義することはできません（同じことは VDC のない NEXUS 7000 シリーズ シャーシでも同様です）。

強力なトポロジは VDC を使用した vPC で展開できます。図 86 に、L2/L3 境界ポイントを提供する集約レイヤで使用されている従来の vPC トポロジを示します。図 86 に示したように、集約レイヤに 4 つの独立した vPC ドメインを作成するには、2 台の物理 NEXUS 7000 シャーシで十分です。

図 86. vPC と VDC のインタラクション：2 台の Nexus 7000 シリーズ シャーシによる 4 つの独立した vPC ドメインの作成



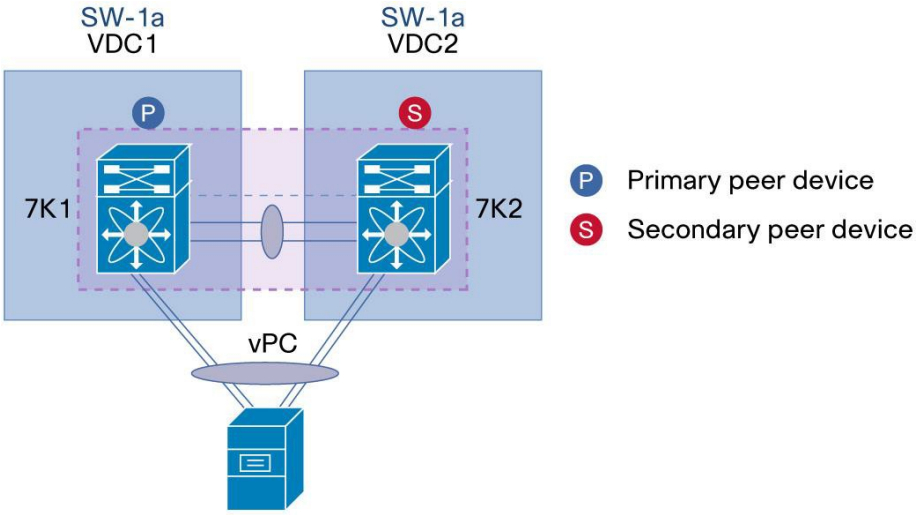
最初の Cisco Nexus 7000 シリーズ シャーシ（SW-1a）は各 vPC ドメインの左側の vPC ピア デバイスをホストします（vPC ドメイン 1 に VDC 1、vPC ドメイン 2 に VDC2 を使用）。

2 番目の Cisco Nexus 7000 シリーズ シャーシ（SW-2b）は各 vPC ドメインの右側の vPC ピア デバイスをホストします（vPC ドメイン 1 に VDC 1、vPC ドメイン 2 に VDC2 を使用）。

VDC によって、vPC のコンテキストにおいて導入の面で柔軟性が大幅に向上します。

ただし、図 87 に示すように 2 つの異なる VDC を使用して同じ NEXUS 7000 シャーシ内に作成された vPC ドメインについて注意が必要な特定の設計が 1 つあります。

図 87. 2 つの異なる VDC を使用して同じ NEXUS 7000 シャーシ内に作成された vPC ドメイン



この設計は完全に正常動作しますが、シスコは正式にはサポートしていません。その理由は、このタイプの設計では vPC のハイ アベイラビリティの側面が保証されないからです（NEXUS 7000 シャーシがダウンすると、vPC ドメイン全体がアウト オブ サービス状態になり、ISSU（In Service Software Upgrade）はこの特定の設計で効率的に動作できません）。実稼働環境にこのタイプの設定を使用しないことを推奨します（ただし、vPC の機能的な動作をテストおよび確認するために LAB ファシリティで使用できます）。

VDC で vPC を正常に展開するには、次のベスト プラクティスおよび推奨事項を使用します。

強力な推奨事項:

- VDC ごとに 1 つの vPC ドメインがサポートされ、NEXUS 7000 シリーズ シャーシで VDC の最大数までサポートされます。
- 配置する各 VDC では、独立した vPC ピア リンクと vPC ピア キープアライブ リンクのインフラストラクチャが必要です。
- 同じ NEXUS 7000 シリーズ シャーシの VDC 間における vPC ドメインの稼働は公式にサポートされておらず、実稼働環境には推奨されません。
- vPC 機能を実行する複数の VDC をサポートするには、スーパーバイザ モジュールに 8 GB の RAM を推奨します。

注: VDC のすべての一般的な推奨事項が、vPC に関係なく、VDC に適用されます。デフォルトの VDC を管理目的だけで使用し、可能であれば、完全なラインカードを VDC 専用にします。

vPC での ISSU（In-Service Software Upgrade）のベスト プラクティス

ここでは、vPC ドメインが設定されている場合に Cisco In-Service Software Upgrade（ISSU）を使用して非中断ソフトウェア アップグレードを実行するためのベスト プラクティスについて説明します。

vPC システム NX-OS アップグレード（またはダウングレード）

vPC 機能は、Cisco ISSU（In-Service Software Upgrade）または ISSD（In-Service Software Downgrade）に完全に対応しています。vPC システムの Cisco NX-OS コード アップグレード（またはダウングレード）は、パケット損失なしで実行できます。

わかりやすくするために、ISSD に関する記述は、マニュアルのこの時点から ISSU にも当てはまります。

vPC 環境で（VDC の使用の有無に関係なく）、ISSU はシステムをアップグレードする推奨方法です。vPC システムはトラフィックの中断なしで個別にアップグレードできます。アップグレードはシリアル化され、一度に 1 つずつ実行する必要があります。ISSU 中の設定ロックは、両方の vPC ピア デバイス上の同期アップグレードを防止します（ISSU の開始時にコンフィギュレーションは他の vPC ピア デバイスで自動的にロックされます）。

ISSU 操作を実行するには、1 つの単一のノブが必要です。デフォルトの VDC から、次のコマンドを入力します。

```
install all kickstart <bootflash_kickstart-image> system <bootflash_system-image>
```

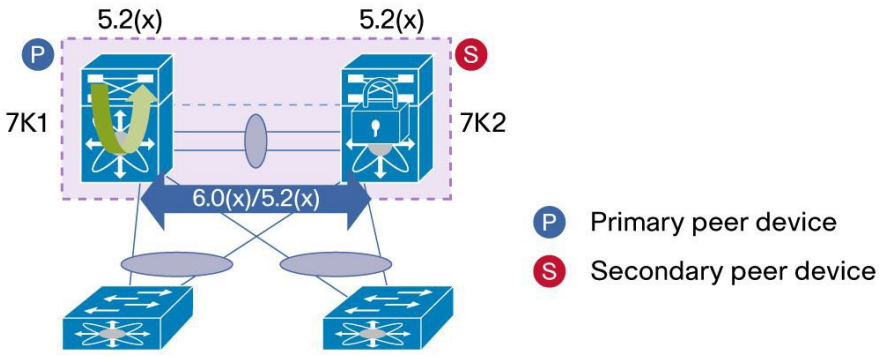
vPC には、2 台の vPC ピア デバイスが異なる NX-OS コードで動作する場合でもシームレスに動作するという利点があります。

たとえば、vPC ピア デバイス 1 は NX-OS 5.2 リリースで動作できますが、他の vPC ピア デバイスは NX-OS 6.0 コードで動作します。このことは、vPC ドメインのヒットレス アップグレードをサポートするために重要です。

注： FEX を搭載した vPC（ホスト vPC）でも ISSU は完全にサポートされます。FEX を含む vPC ドメインをアップグレードする場合、パケット損失はゼロです。標準のポート チャネルを使用して 2 つの異なる FEX にデュアル接続されたサーバは、ネットワークで発生するアップグレード操作を認識しません。

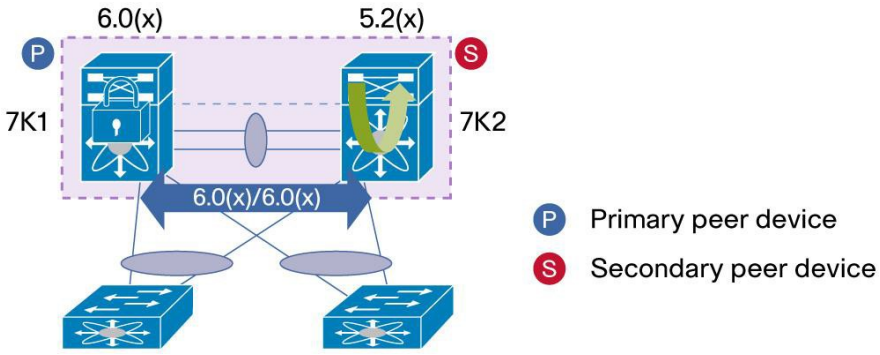
図 88～90 は、Cisco NX-OS Software Release 5.2 から Release 6.0 への vPC システム アップグレード シーケンスを示しています。

図 88. vPC の ISSU：ステップ 1



ステップ 1 では、図 88 に示されているように、両方の vPC ピア デバイスが両方のリリース 5.2 のコードを実行します。リリース 6.0 のコードは、ISSU を使用して vPC ピア デバイス 1 の 7K1（プライマリまたはセカンダリ vPC ピア デバイスにコードを最初にロードすることに重要性はありません）にロードされます。もう一方の vPC ピア デバイス（7K2）の設定は、スイッチに対する任意の操作から保護するためにロックされていることに注意してください。

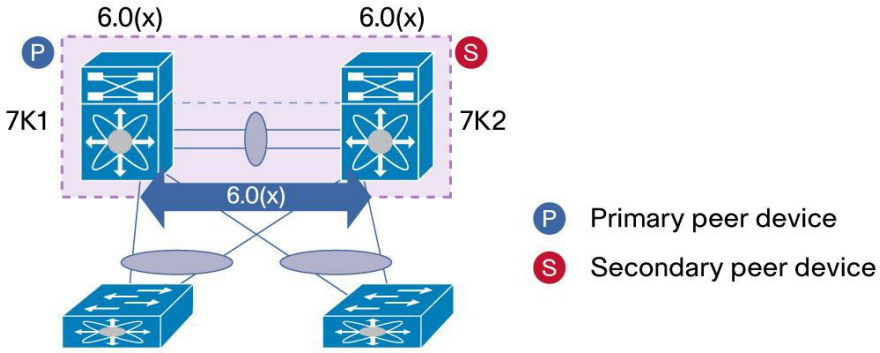
図 89. vPC の ISSU：ステップ 2



ステップ 2 では、vPC ピア デバイス 1（7K1）に NX-OS Release 6.0 がロードされています。ここで vPC ピア デバイス 2（7K2）が ISSU を使用してリリース 6.0 のコードをロードします。7K1 の設定は、アップグレード中に変更できないようにロックされます。

この遷移フェーズ中は、vPC システムは両方のピア デバイスに別の NX-OS コードがあっても正常に動作します。

図 90. vPC の ISSU：ステップ 3



ステップ 3 では、両方の vPC ピア デバイスがリリース 6.0 のコードを実行します。これで ISSU プロセスが完了しました。

強力な推奨事項：

- vPC ドメインの NX-OS コード リリースを変更するには、ISSU（In-Service Software Upgrade）または ISSD（In-Service Software Downgrade）を使用します。操作を順番に、つまり、一度に vPC ピア デバイスを 1 台ずつ実行します。
- 実行中のコードに基づいてターゲットの NX-OS コード リリースを適切に選択するには、NX-OS リリース ノート（ISSU 互換性マトリクス）を参照してください。

注： ISSU および ISSD に関するすべての一般的な推奨事項が、vPC に関係なく、ここにも適用されます。

NX-OS リリース ノートをよく確認し、ISSU または ISSD 操作を正しく実行するための推奨ガイドラインに従ってください。

vPC 拡張

ここでは、vPC に対する拡張機能とその推奨される使用方法について説明します。

vPC ピア ゲートウェイ

vPC ピアゲートウェイ拡張機能（図 91）により、通常のデフォルト ゲートウェイの ARP 要求をブートアップ時に実行しない Network-Attached Storage（NAS）またはロードバランサ デバイスと vPC の相互運用が可能になります。vPC ピアゲートウェイを使用すると、vPC ピア デバイスが他のピア デバイスのルータ MAC を宛先とするパケットのアクティブなゲートウェイとして機能できます。これは、vPC ピア デバイスにローカルなトラフィックの転送を保持し、ピア リンクの使用を回避します（他の vPC ピア デバイスにトラフィックをブリッジングしません）。ピアゲートウェイ機能をアクティブにしても、トラフィックおよび既存の機能に影響はありません。

図 91. vPC ピア ゲートウェイ

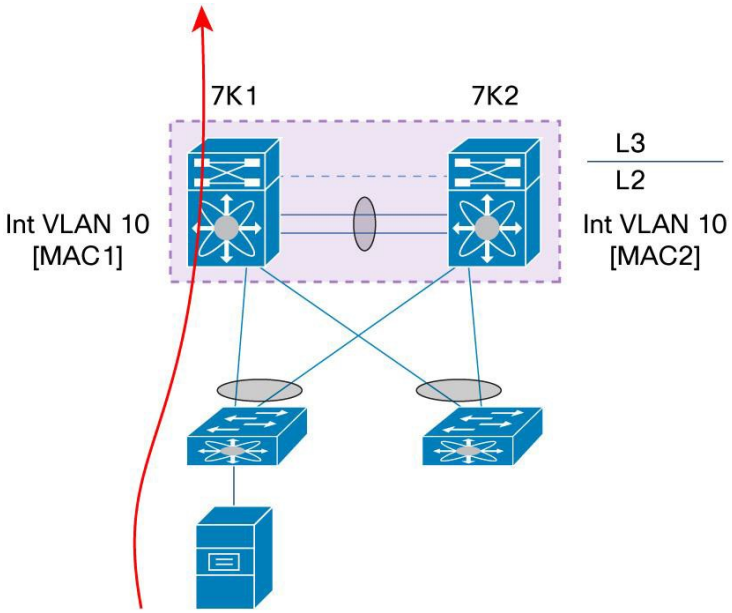


図 91 に示すように、NAS デバイス（IP デフォルト ゲートウェイの標準の ARP 要求を実行しない）は、vPC ピア デバイス 7K1 および 7K2 に vPC 接続されたアクセス スイッチに接続されます。

7K1 および 7K2 には、NAS デバイスがに接続されている VLAN のインターフェイス VLAN（つまり SVI）（VLAN 10）が設定されています。NAS デバイスは、デフォルト ゲートウェイの MAC アドレスを取得するための標準の ARP 要求を行わないため、他の方法でこの MAC アドレスを学習します。これは、ネットワーク トラフィックをリッスンし、デフォルト ゲートウェイの MAC アドレスとして最初に受信した送信元 MAC アドレスを選択することによって行うことができます。

NAS デバイスが vPC ピア デバイス 7K2 から最初のパケットを受信すると想定します。この場合、デフォルト ゲートウェイの MAC アドレスとして 7K2 でインターフェイス VLAN 10 の MAC アドレスを使用します。NAS デバイスによって送信されたすべてのルーテッド トラフィックは、正しくルーティングされるために 7K2 に到達する必要があります（vPC ドメインから送信される L3 トラフィックまたは VLAN 間トラフィック）。VLAN 間トラフィックについては、vPC ループ回避の問題が発生するリスクがあります。NAS デバイスはルーテッド トラフィックを送信し、アクセス スイッチは 7K1 方向にトラフィックをハッシュします。7K1 は、7K2 MAC アドレス（より正確にはインターフェイス VLAN 10 の MAC アドレス）はこのトラフィックの L2 宛先であるため、vPC ピア リンク上でトラフィックをブリッジする必要があります。トラフィックが vPC メンバー ポートから出る必要がある場合、vPC ループ回避のルールにより、ハードウェアでドロップされます。

vPC ピアゲートウェイ機能をイネーブルにすると、各 vPC ピア デバイスは他の vPC ピア デバイスに定義されている G フラグ（ゲートウェイ フラグ）を持つインターフェイス VLAN の MAC アドレスをローカルに複製します。上の図では、7K1 は MAC2（インターフェイス VLAN 10 の MAC アドレス）を MAC テーブルにプログラムし、この MAC アドレスの G フラグを設定します。7K2 は MAC1 に対して同じことを行います。

vPC ピアゲートウェイ機能をアクティブにするには、（vPC 設定コンテキスト モードで）次のコマンドラインを使用します。

```
N7k(config-vpc-domain)# peer-gateway
```

両方の vPC ピア デバイスをこのコマンドで設定する必要があります。

強力な推奨事項:

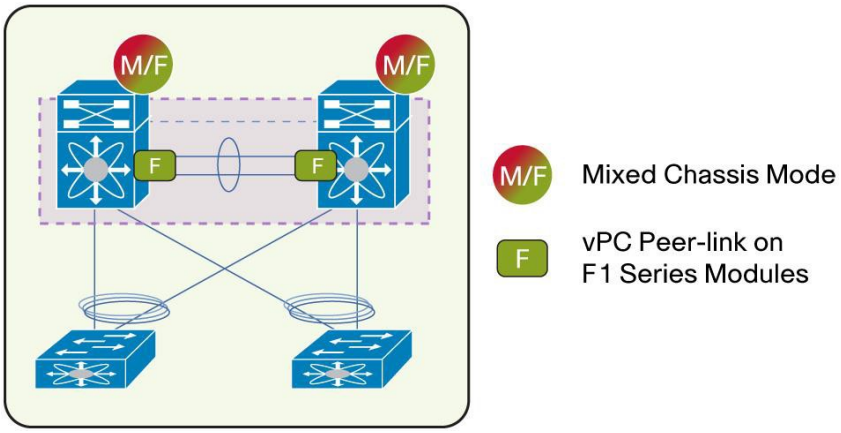
この機能を使用するエンド デバイス（デフォルト IP ゲートウェイの標準の ARP 要求を実行しないデバイス）がない場合でも、vPC ドメインの vPC ピア ゲートウェイを常にイネーブルにします（つまり、両方の vPC ピア デバイスでピア ゲートウェイを設定します）。イネーブル化の副作用はありません。

vPC peer-gateway exclude-vlan

vPC peer-gateway exclude-vlan 機能は、混合シャーシ モード（M1/F1）で F1 ポートの vPC ピア リンクを使用した特定のトポロジに対応するために、NX-OS 5.1.3 から導入されました。

機能は、このタイプのトポロジにだけ関連します（図 92）。vPC ドメインが（混合シャーシ モード M1/F1 ではなく）完全な F1 トポロジ、完全な M1 トポロジ、または完全な F2 トポロジの場合、この機能は適用されません。M1 ポートの vPC ピア リンクを使用した混合シャーシ モードの場合でも、この機能は適用されません。

図 92. vPC peer-gateway exclude-vlan：機能が適用される一意のトポロジ



vPC peer-gateway exclude-vlan 機能は、CPU にパントされる vPC ピア リンクを使用して vPC ピア デバイス間の中継トラフィックを回避するために開発され、直接 HW スイッチングを可能にします。

vPC peer-gateway exclude-vlan の一般的な適用例は、vPC ピア リンク上の専用 VLAN（中継 VLAN とも呼ばれる）がこの目的のために使用される場合の L3 バックアップ ルーテッド パスです。vPC ピア デバイス上のすべての L3 アップリンクに障害が発生した場合、L3 コアに接続している他の vPC ピア デバイスにトラフィックを伝送するために、バックアップ ルーテッド パスが使用されます。

この場合、1 台の vPC ピア デバイスから他の vPC ピア デバイスにトラフィックを伝送する中継 VLAN は、次のコマンドを使用して適切に動作するように宣言する必要があります（そうしなければ、中継トラフィックは数 Mbps に制限されます）。

```
N7k(config-vpc-domain)# peer-gateway exclude-vlan <vlan list>
```

必須の推奨事項:

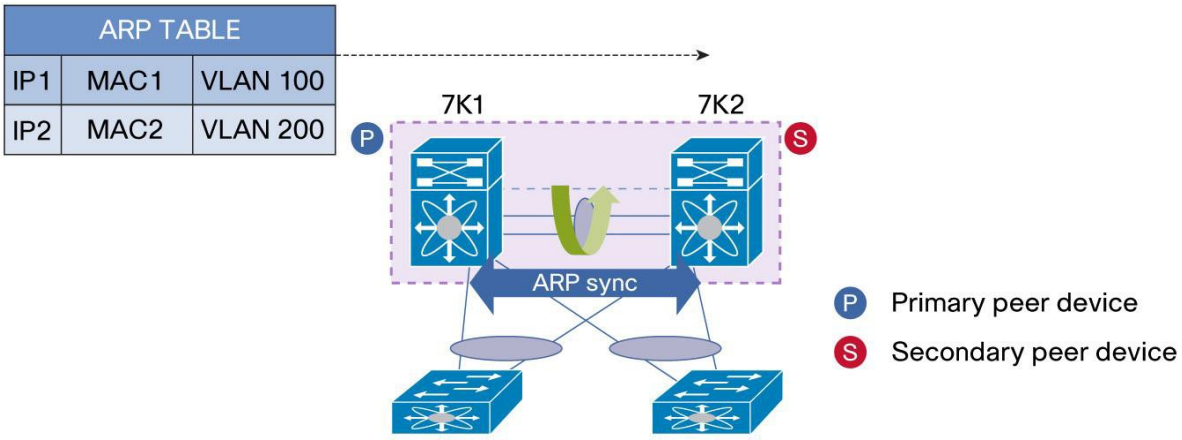
中継 VLAN（vPC ピア リンク上）を vPC ドメインで使用する場合は、常に vPC peer-gateway exclude-vlan を使用します。これは、F1 ポートの vPC ピア リンクを使用した混合シャーシ モード（M1/F1）だけに適用されます。

vPC ARP 同期

vPC ARP 同期を使用すると、レイヤ 3 フロー（ノースバウンドからサウスバウンドへのトラフィック）のコンバージェンス時間が向上します。

vPC ピアリンクに障害が発生し、その後回復した場合、vPC ARP 同期は、Cisco Fabric Services（CFS）を介して、vPC プライマリ ピア デバイスから vPC セカンダリ ピア デバイスへの ARP バルク同期を実行します。

図 93. vPC ARP 同期：vPC ピア リンクの障害および回復



vPC ARP 同期は、次のコマンドを使用して、両方の vPC ピア デバイス上でイネーブルにする必要があります。

```
N7k(config-vpc-domain)# ip arp synchronize
```

強力な推奨事項:

両方の vPC ピア デバイスで vPC ARP 同期を常にイネーブルにします。

vPC の遅延復元

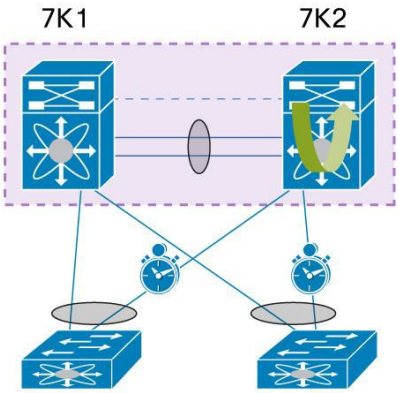
vPC ピア デバイスのリロードおよび復旧後、ルーティング プロトコルに再コンバージェンスの時間が必要です。

vPC レッグの回復により、レイヤ 3 接続が再度確立されるまでアクセスからコアへのルーテッド トラフィックがブラック ホール状態になる場合があります。

vPC の遅延復元機能は、vPC ピア デバイスの回復時に、vPC レッグの起動を遅らせます。vPC の遅延復元を使用すると、vPC レッグのトラフィックを許可する前に、レイヤ 3 ルーティング プロトコルでコンバージェンス処理が可能になります。その結果、リカバリ フェーズ中にグレースフル復元が行われ、パケット損失はゼロです（トラフィックは引き続きアライブ vPC ピア デバイス上で転送されます）。

この機能は、vPC 復元のデフォルト タイマーが 30 秒でデフォルトでイネーブルになります。タイマーは、1～3600 秒の特定のレイヤ 3 コンバージェンス ベースラインに合わせて調整できます。

図 94. vPC の遅延復元：7K2 の障害および回復



vPC の遅延復元を設定するコマンドは、次のとおりです。

```
N7K(config-vpc-domain)# delay restore <1-3600 sec>
```

両方の vPC ピア デバイスをこのコマンドで設定する必要があります。

類似のコマンド **delay restore interface-vlan <1-3600 sec >** は、vPC ピア デバイスの障害および回復時に SVI の起動タイミングを遅らせるために使用できます。

強力な推奨事項:
vPC の遅延復元を（両方の vPC ピア デバイス上で）常にイネーブルにし、ネットワーク プロファイルに基づいてタイマーを調整します。

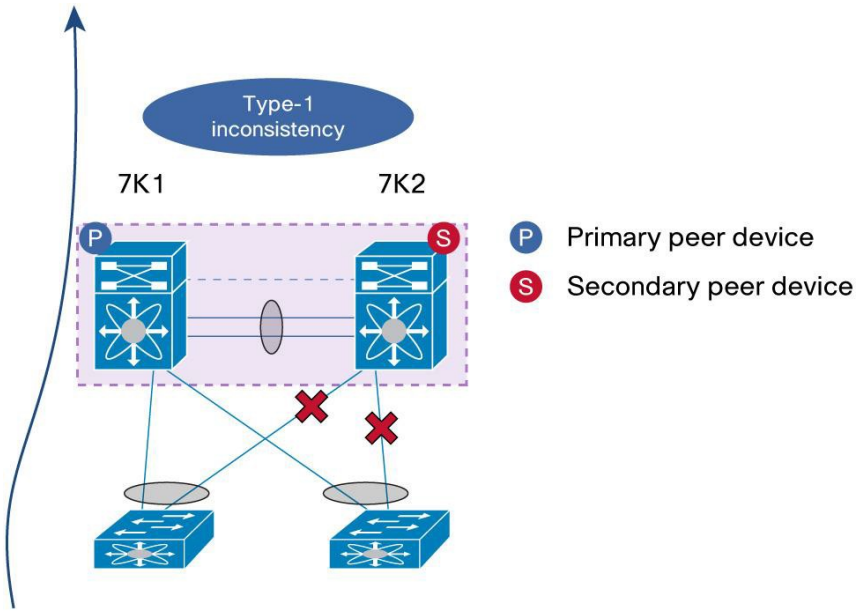
vPC グレースフル タイプ 1 チェック

両方の vPC ピア デバイス上の vPC メンバー ポートでパラメータ（MTU、速度など）が同じである必要があります。

このようなパラメータの不一致がタイプ 1 です。結果として、両方の vPC メンバー ポートのすべての VLAN がこのような不一致でダウンします。

vPC グレースフル タイプ 1 チェック機能を使用すると、セカンダリ vPC ピア デバイスのメンバー ポートのみがダウンします。プライマリ vPC ピア デバイスの vPC メンバー ポートはアップ ステートが保持され、アクセス デバイスからの着信トラフィックまたはアクセス デバイスへの発信トラフィックをすべて処理します。

図 95. vPC グレースフル タイプ 1 チェック



vPC グレースフル タイプ 1 チェックはデフォルトでイネーブルになっています。関連するコマンドは次のとおりです。

```
N7K(config-vpc-domain)# graceful consistency-check
```

両方の vPC ピア デバイスをこのコマンドで設定する必要があります。

強力な推奨事項:
両方の vPC ピア デバイスで vPC グレースフル タイプ 1 チェックを常にイネーブルにします。

vPC 自動リカバリ

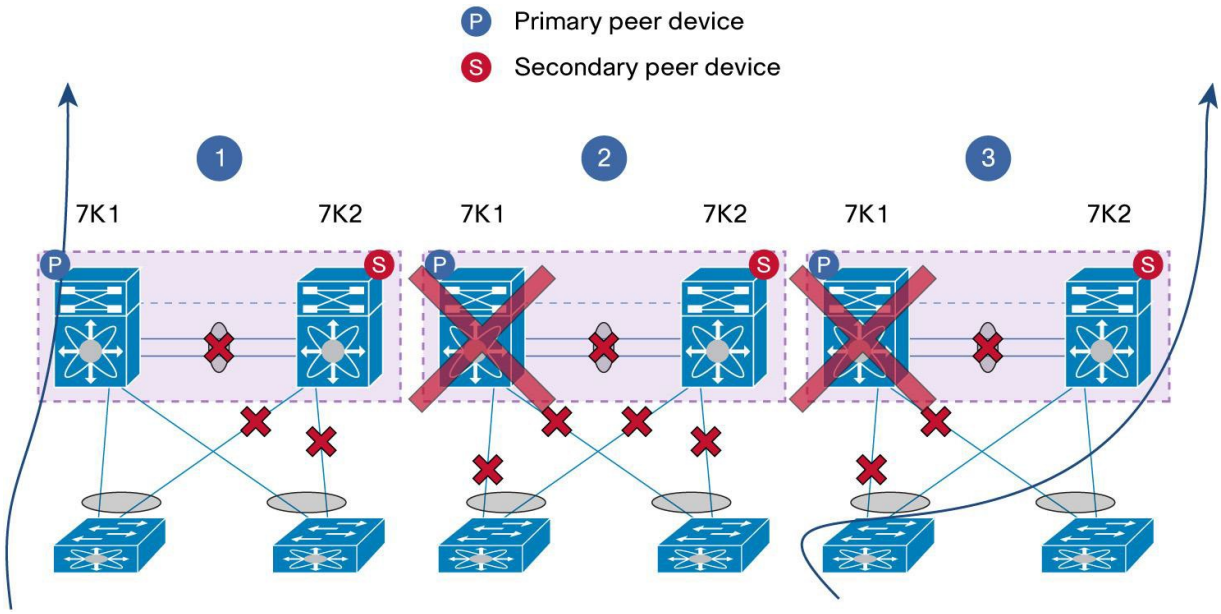
vPC 自動リカバリ機能は、vPC の 2 個の拡張機能に対処できるように設計されました。

最初の 1 つは、vPC プライマリ ピア デバイスの障害に続けて vPC ピア リンクの障害が発生した場合にバックアップ メカニズムを提供することです（vPC 自動リカバリ機能）。

2 つ目は、両方の vPC ピア デバイスがリロードし、一方のみが回復する特定のケースを処理することです（vPC 自動リカバリのリロード遅延機能）。

最初の拡張機能を見てみましょう。図 96 は、vPC 自動リカバリのさまざまな障害フェーズおよび動作を示しています。

図 96. vPC 自動リカバリ：vPC ピア リンクの障害後、vPC プライマリ ピア デバイス障害が発生



1. vPC ピア リンクがダウンします。vPC セカンダリ ピア デバイス（7K2）は、すべての vPC メンバー ポートを終了します。
2. 次に、プライマリ vPC ピア デバイス（7K1）がダウンします。7K2 は vPC ピア キープアライブ リンクでメッセージを受信しません。
3. 3 回の連続キープアライブ タイムアウト後、vPC セカンダリ ピア デバイス（7K2）は、プライマリ ピア デバイスにロールを変更し、vPC メンバー ポートをアップ ステートに戻します。

前述のケースを目的とした vPC 自動リカバリは、デフォルトでイネーブルになっていません。次のコマンドを使用して、vPC 自動リカバリをアクティブにします。

```
N7K(config-vpc-domain)# auto-recovery
```

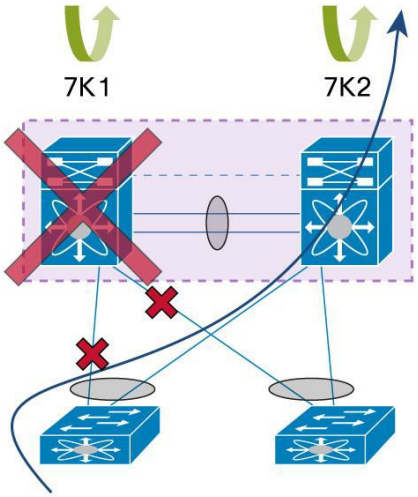
両方の vPC ピア デバイスをこのコマンドで設定する必要があります。

強力な推奨事項:

両方の vPC ピア デバイスで vPC 自動リカバリを常にイネーブルにします。

2 つ目の拡張機能は、図 97 に示されています。両方の vPC ピア デバイスがリロードしますが、7K2 のみ回復します。

図 97. vPC 自動リカバリのリロード遅延：vPC ピア デバイスがリロードし、7K2 のみ回復



両方の vPC ピア デバイスがリロードすると、両方がピア隣接が vPC デバイスの間で再確立されるまで、デフォルトですべての vPC メンバー ポートが一時停止されます。1 台の vPC ピア デバイスだけが動作可能になった場合、ローカル vPC ポートは中断状態のままとなります。

vPC 自動リカバリのリロード遅延機能を使用すると、一意のアライブ vPC ピア デバイスで遅延タイマーの満了後に vPC プライマリ ロールを使用してすべてのローカル vPC ポートを起動できます。遅延は 240 秒 ～ 3600 秒の間で調整できます。

vPC 自動リカバリのリロード遅延はデフォルトでイネーブルになっていません。次のコマンドを使用してアクティブにします。

```
N7K(config-vpc-domain)# auto-recovery reload-delay <240-3600 seconds>
```

両方の vPC ピア デバイスをこのコマンドで設定する必要があります。

強力な推奨事項:
両方の vPC ピア デバイスで vPC 自動リカバリのリロード遅延を常にイネーブルにします。

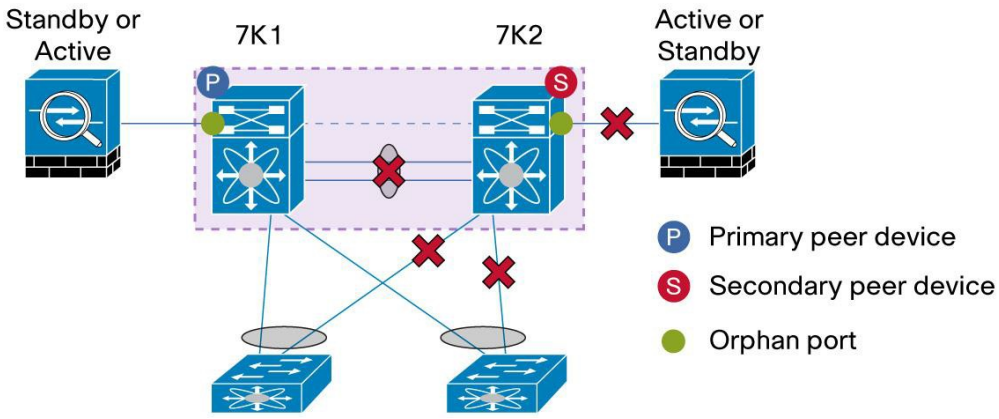
注: vPC 自動リカバリのリロード遅延は、以前の vPC リロード復元と呼ばれる機能を置き換えます。

vPC 孤立ポートの一時停止

孤立ポートの一時停止機能は、vPC ドメインにシングル接続され、オプションでアクティブ/スタンバイ モードで動作するデバイス（たとえばファイアウォールまたはロードバランサ）のために開発されました。

vPC ピア リンクがダウンすると、vPC セカンダリ ピア デバイスがすべての vPC メンバー ポートをシャットダウンしますが、vPC 孤立ポートはシャット ダウンしません。vPC **孤立ポートの一時停止**が設定されている場合は、ピア リンクがダウンしたときに vPC メンバー ポートと一緒に孤立ポートもシャットダウンされます（図 98）。vPC ピア リンクが復元されると、セカンダリ vPC ピア デバイスに設定されている vPC 孤立ポートは、vPC メンバー ポートとともに起動します。

図 98. vPC 孤立ポートの一時停止



vPC ピア リンクに障害が発生した場合に一時停止する必要がある vPC 孤立ポートは、次のコマンドを使用して明示的に設定する必要があります。

```
N7K (config)# int eth 1/1
N7K (config-if)# vpc orphan-ports suspend
```

vpc orphan-ports suspend CLI は物理ポートだけでサポートされ、ポート チャネルではサポートされません。ポート チャネルの孤立ポートの一時停止を設定するには、ポート チャネルのすべてのメンバー ポートに上記の設定を適用します。

強力な推奨事項:

vPC ピア リンクに障害が発生した場合に、vPC ドメインに接続されているシングル接続デバイスをネットワークから切断する必要がある場合は、vPC 孤立ポートの一時停止を使用します。

お問い合わせ先

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/