



## vPC の設定

---

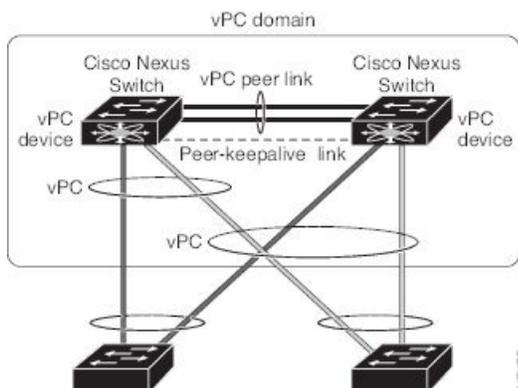
- [vPC について \(1 ページ\)](#)
- [注意事項と制約事項 \(33 ページ\)](#)
- [レイヤ 3 および vPC 設定のベストプラクティス \(41 ページ\)](#)
- [デフォルト設定 \(51 ページ\)](#)
- [vPC の設定 \(51 ページ\)](#)
- [vPC 設定の確認 \(78 ページ\)](#)
- [vPC のモニタリング \(79 ページ\)](#)
- [vPC の設定例 \(79 ページ\)](#)
- [関連資料 \(81 ページ\)](#)

## vPC について

### vPC の概要

仮想ポートチャネル (vPC) は、物理的には 2 台の異なる Cisco Nexus 9000 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 (図を参照)。第 3 のデバイスは、スイッチ、サーバ、ポートチャネルをサポートするその他の任意のネットワークングデバイスのいずれでもかまいません。vPC は、ノード間の複数の並列パスを可能にし、トラフィックのロードバランシングを可能にすることによって、冗長性を作り、バイセクショナルな帯域幅を増やすレイヤ 2 マルチパスを提供できます。

図 1: vPC のアーキテクチャ



vPC で使用できるのは、レイヤ 2 ポート チャンネルだけです。ポート チャンネルの設定は、次のいずれかを使用して行います。

- プロトコルなし
- リンク集約制御プロトコル (LACP)

LACP を使用せずに vPC (vPC ピア リンク チャンネルも含めて) のポート チャンネルを設定する場合は、各デバイスが、単一のポート チャンネル内に最大 8 つのアクティブリンクを持てます。LACP を使用して vPC (vPC ピア リンク チャンネルも含めて) のポート チャンネルを設定する場合は、各デバイスが、単一のポート チャンネル内に 32 個のアクティブリンクと 8 つのスタンバイリンクを持つことができます。(LACP と vPC の使用の詳細については、「その他の機能との vPC の相互作用」の項を参照)。



(注) vPC の機能を設定したり実行したりするには、まず vPC 機能をイネーブルにする必要があります。

vPC 機能をイネーブルにしたら、ピアキープアライブリンクを作成します。このリンクは、2 つの vPC ピア デバイス間でのハートビートメッセージの送信を行います。

1 ギガビットイーサネット以上の速度のイーサネットポートを 2 つ以上使用することにより、1 台の Cisco Nexus 9000 シリーズ シャーシでポート チャンネルを設定して vPC ピア リンクを作成できます。vPC を有効にして実行するための正しいハードウェアが揃っていることを確認するには、**show hardware feature-capability** と入力します コマンドを入力します。コマンド出力で vPC の向かいに X が表示されている場合、そのハードウェアでは vPC 機能をイネーブルにできません。

vPC ピア リンク レイヤ 2 ポート チャンネルは、トランクとして設定することを推奨します。もう 1 つの Cisco Nexus 9000 シリーズ シャーシで、再度専用ポート モードで 1 ギガビット以上の速度の 2 つ以上のイーサネットポートを使用して、もう 1 つのポート チャンネルを設定します。これらの 2 つのポート チャンネルを接続すると、リンクされた 2 つの Cisco Nexus デバイスが第 3 のデバイスには 1 つのデバイスとして見える vPC ピア リンクが作成されます。第 3 のデバイス、またはダウンストリームデバイスは、スイッチ、サーバ、vPC に接続された正規の

ポート チャンネルを使用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。

モジュラ Cisco Nexus 9500 スイッチの場合、異なるモジュールの専用ポート上で vPC ピア リンクを設定して、障害発生の可能性を下げることをお勧めします。復元力を最適にしたい環境では、少なくとも 2 つのモジュールを使用してください。

vPC ピア リンクに Nexus 9000 デバイスの任意のインターフェイスを使用できます。すべての vPC ピア リンクおよびコアに面したインターフェイスを 1 つのモジュール上で設定しなければならない場合、コアへのレイヤ 3 リンクに関連付けられているトラック オブジェクトおよび両方の vPC ピア デバイス上の vPC ピア リンク上のすべてのリンクを設定してください。

vPC ドメインには、両方の vPC ピア デバイス、vPC ピア キープ アライブ リンク、vPC ピア リンク、および vPC ドメイン内にあってダウンストリーム デバイスに接続されているすべてのポート チャンネルが含まれます。各デバイスに設定できる vPC ドメイン ID は、1 つだけです。

このバージョンでは、各ダウンストリーム デバイスを、単一のポート チャンネルを使用して単一の vPC ドメイン ID に接続できます。

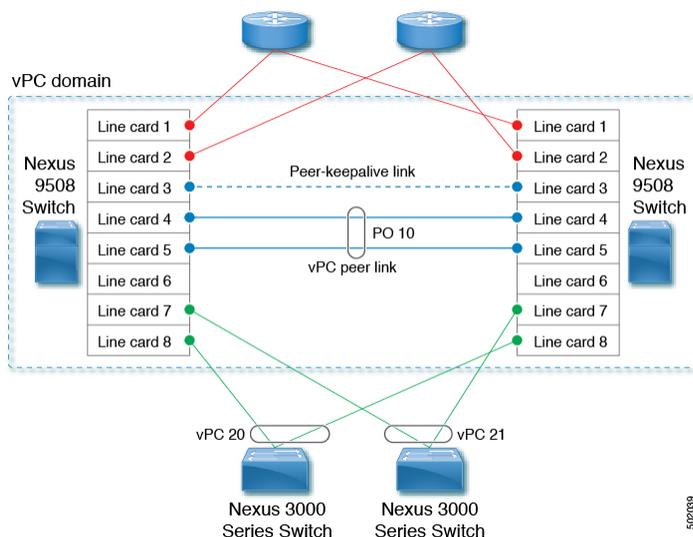


(注) ポート チャンネルを使用して vPC ドメインに接続されたデバイスは、両方の vPC ピア に接続する必要があります。

vPC (図を参照) には、次の利点があります。

- 単一のデバイスが 2 つのアップストリーム デバイスを介して 1 つのポート チャンネルを使用することを可能にします。
- 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。
- ループフリーなトポロジが実現されます。
- 利用可能なすべてのアップリンク帯域幅を使用します。
- リンクまたはデバイスに障害が発生した場合に、ファーストコンバージェンスを提供します。
- リンクレベルの復元力を提供します。
- ハイ アベイラビリティが保証されます。

図 2: vPC インターフェイス



## vPC の用語

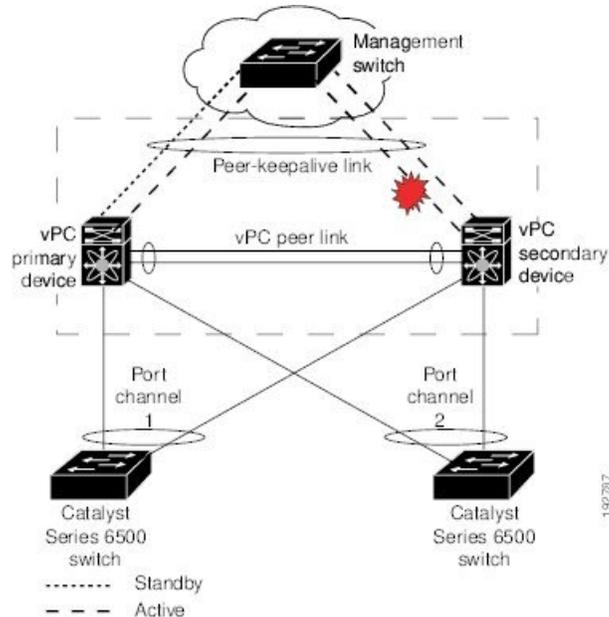
vPC で使用される用語は、次のとおりです。

- vPC : vPC ピア デバイスとダウンストリーム デバイスの間の結合されたポート チャネル。
- vPC ピア デバイス : vPC ピア リンクと呼ばれる特殊なポート チャネルで接続されている一対のデバイスの 1 つ。
- vPC ピア リンク : vPC ピア デバイス間の状態を同期するために使用されるリンク。このリンクは、少なくとも 10 ギガビットイーサネット インターフェイスを使用する必要があります。より広い帯域幅のインターフェイス (25 ギガビットイーサネット、40 ギガビットイーサネット、100 ギガビットイーサネットなど) も使用できます。
- vPC メンバ ポート : vPC に属するインターフェイス。
- ホスト vPC ポート : vPC に属するファブリック エクステンダのホスト インターフェイス。
- vPC ドメイン : このドメインには、両方の vPC ピア デバイス、vPC ピア キープアライブ リンク、vPC 内においてダウンストリーム デバイスに接続されているすべてのポート チャネルが含まれます。また、このドメインは、vPC グローバル パラメータを割り当てるために使用する必要があるコンフィギュレーション モードに関連付けられています。
- vPC ピア キープアライブ リンク : ピア キープアライブ リンクは、さまざまな vPC ピア Cisco Nexus 9000 シリーズのデバイスをモニタします。ピア キープアライブ リンクは、vPC ピア デバイス間での設定可能な キープアライブ メッセージの定期的な送信を行います。

ピア キープアライブ リンクを、各 vPC ピア デバイス内のレイヤ 3 インターフェイスにマッピングされている独立した仮想ルーティングおよび転送 (VRF) インスタンスに関連付けることを推奨します。独立した VRF を設定しなかった場合は、デフォルトで管理 VRF が使用されます。ただし、ピア キープアライブ リンクに管理 インターフェイスを使用する場

合は、各 vPC ピア デバイスのアクティブ管理ポートとスタンバイ管理ポートの両方に接続した管理スイッチを置く必要があります（図を参照）。

図 3: vPC ピアキーブアライブリンクの管理ポートを接続するための独立したスイッチが必要



vPC ピアキーブアライブ リンク上を移動するデータまたは同期トラフィックはありません。このリンクを流れるトラフィックは、送信元スイッチが稼働しており、vPC を実行していることを知らせるメッセージだけです。

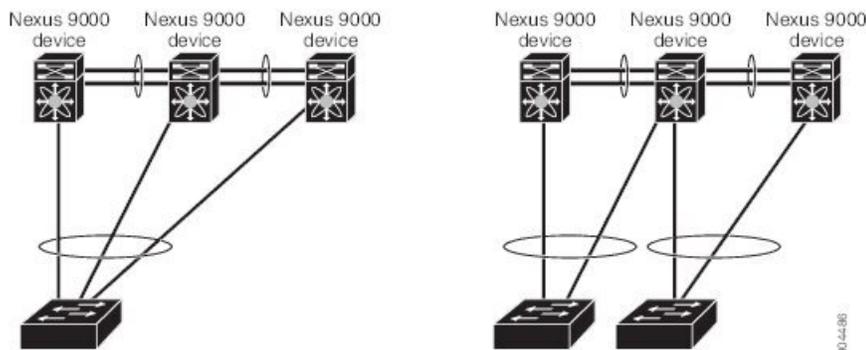
- vPC メンバ ポート：vPC に属するインターフェイス。
- デュアルアクティブ：プライマリとして動作する両方の vPC ピア。この状況は、両方のピアがまだアクティブなときに vPC ピアキーブアライブとピアリンクがダウンした場合に発生します。この場合、セカンダリ vPC はプライマリ vPC が動作しないと想定し、プライマリ vPC として機能します。
- リカバリ：ピアキーブアライブと vPC ピアリンクが起動すると、1 台のスイッチがセカンダリ vPC になります。セカンダリ vPC になるスイッチで、vPC リンクが停止してから復帰します。

## vPC ピア リンクの概要

vPC ピアとして持てるのは 2 台のデバイスだけです。各デバイスが、他方の 1 つの vPC ピアに対してだけ vPC ピアとして機能します。vPC ピア デバイスは、他のデバイスに対する非 vPC リンクも持つことができます。

無効な vPC ピア設定については、次の図を参照してください。

図 4: 許可されていない vPC ピア 設定



有効な設定を作成するには、まず各デバイス上でポートチャネルを設定してから、vPC ドメインを設定します。ポートチャネルを各デバイスに、同じ vPC ドメイン ID を使用して vPC ピア リンクとして割り当てます。vPC ピア リンクのインターフェイスの片方に障害が発生した場合に、デバイスが自動的に vPC ピア リンク内の他方のインターフェイスを使用するようにフォールバックするため、冗長性のために少なくとも 2 つの専用ポートをポートチャネルに設定することを推奨します。



(注) レイヤ 2 ポートチャネルをトランク モードで設定することを推奨します。

多くの動作パラメータおよび設定パラメータが、vPC ピア リンクによって接続されている各デバイスで同じでなければなりません（「vPC インターフェイスの互換パラメータ」の項を参照）。各デバイスは管理プレーンから完全に独立しているため、重要なパラメータについてデバイス同士に互換性があることを確認する必要があります。vPC ピア デバイスは、個別のコントロールプレーンを持ちます。vPC ピア リンクを設定し終わったら、各 vPC ピア デバイスの設定を表示して、設定に互換性があることを確認してください。



(注) vPC ピア リンクによって接続されている 2 つのデバイスが、特定の同じ動作パラメータおよび設定パラメータを持っていることを確認する必要があります。必要な設定の一貫性の詳細については、「vPC インターフェイスの互換パラメータ」の項を参照してください。

vPC ピア リンクを設定すると、vPC ピア デバイスは接続されたデバイスの一方がプライマリ デバイスで、もう一方の接続デバイスがセカンダリ デバイスであると交渉します（「vPC の設定」の項を参照）。Cisco NX-OS ソフトウェアは、最小の MAC アドレスを使用してプライマリ デバイスを選択します。特定のフェールオーバー条件の下でだけ、ソフトウェアが各デバイス（つまり、プライマリ デバイスおよびセカンダリ デバイス）に対して異なるアクションを取ります。プライマリ デバイスに障害が発生すると、システムの回復時にセカンダリ デバイスが新しいプライマリ デバイスになり、以前のプライマリ デバイスがセカンダリ デバイスになります。

どちらの vPC デバイスをプライマリ デバイスにするか設定することもできます。vPC ピア デバイスのプライオリティを変更すると、ネットワークでインターフェイスがアップしたりダウ

ンしたりする可能性があります。1 台の vPC デバイスをプライマリ デバイスにするよう再度 ロールプライオリティを設定する場合は、プライオリティ値が低いプライマリ vPC デバイスと値が高いセカンダリ vPC デバイスの両方でロールプライオリティを設定します。次に、**shutdown** コマンドを入力して、両方のデバイスで vPC ピア リンクであるポート チャネルをシャットダウンし、最後に **no shutdown** コマンドを入力して、両方のデバイスでポート チャネルを再度イネーブルにします。



- (注) 各 vPC ピア リンクの各 vPC ピア デバイスの冗長性のために、2 つの異なるモジュールを使用することを推奨します。

ソフトウェアは、vPC ピアを介して転送されたすべてのトラフィックをローカルトラフィックとしてキープします。ポートチャネルから入ってきたパケットは、vPC ピア リンクを介して移動するのではなく、ローカルリンクの1つを使用します。不明なユニキャスト、マルチキャスト、およびブロードキャストトラフィック (STP BPDU を含む) は、vPC ピア リンクでフラッディングされます。ソフトウェアが、マルチキャストフォワーディングを両方の vPC ピア デバイス上で同期された状態に保ちます。

両方の vPC ピア リンク デバイスおよびダウンストリームデバイスで、任意の標準ロードバランシングスキームを設定できます (ロードバランシングについては、「ポートチャネルの設定」の章を参照)。

設定情報は、Cisco Fabric Service over Ethernet (CFSoE) プロトコルを使用して vPC ピア リンクを転送されます。(CFSoE の詳細については、「[CFSoE \(28 ページ\)](#)」の項を参照)。

両方のデバイス上で設定されているこれらの VLAN の MAC アドレスはすべて、vPC ピア デバイス間で同期されています。この同期に、CFSoE が使用されます (CFSoE の詳細については、「[CFSoE \(28 ページ\)](#)」の項を参照)

vPC ピア リンクに障害が発生した場合は、ソフトウェアが、両方のデバイスが稼働していることを確認するための vPC ピア デバイス間のリンクであるピアキープアライブリンクを使用して、リモート vPC ピア デバイスのステータスをチェックします。vPC ピア デバイスが稼働している場合は、セカンダリ vPC デバイスは、ループやトラフィックの消失あるいはフラッディングを防ぐために、そのデバイス上のすべての vPC ポートをディセーブルにします。したがって、データは、ポートチャネルの残っているアクティブなリンクに転送されます。

ソフトウェアは、ピアキープアライブリンクを介したキープアライブメッセージが返されない場合に、vPC ピア デバイスに障害が発生したことを学習します。

vPC ピア デバイス間の設定可能なキープアライブメッセージの送信には、独立したリンク (vPC ピアキープアライブリンク) を使用します。vPC ピアキープアライブリンク上のキープアライブメッセージから、障害が vPC ピア リンク上でだけ発生したのか、vPC ピア デバイス上で発生したのかがわかります。キープアライブメッセージは、vPC ピア リンク内のすべてのリンクで障害が発生した場合にだけ使用されます。キープアライブメッセージについては、「ピアキープアライブリンクとメッセージ」の項を参照してください。

## プライマリおよびセカンダリ デバイス上で手動で設定する必要がある機能

各 vPC ピア デバイスのプライマリ/セカンダリ マッピングに従うために、次の機能を手動で設定する必要があります。

- **STP ルート**：プライマリ vPC ピア デバイスを STP プライマリ ルート デバイスとして設定し、vPC セカンダリ デバイスを STP セカンダリ ルート デバイスとして設定します。vPC および STP の詳細については、「vPC ピア リンクと STP」の項を参照してください。
- **Bridge Assurance** がすべての vPC ピア リンク上でイネーブルになるように、vPC ピア リンク インターフェイスを STP ネットワーク ポートとして設定することを推奨します。
- **VLAN 単位の高速スパンニングツリー (PVST+)** を設定してプライマリ デバイスがすべての VLAN のルートになるようにし、**マルチ スパンニングツリー (MST)** を設定してプライマリ デバイスがすべてのインスタンスのルートになるようにすることを推奨します。
- **レイヤ3 VLAN ネットワーク インターフェイス**：両方のデバイスから同じ VLAN の VLAN ネットワーク インターフェイスを設定することにより、各 vPC ピア デバイスのレイヤ3 接続を設定します。
- **HSRP アクティブ**：vPC ピア デバイス上でホットスタンバイ ルータ プロトコル (HSRP) と VLAN インターフェイスを使用する場合は、プライマリ vPC ピア デバイスを HSRP アクティブの最も高いプライオリティで設定します。セカンダリ デバイスを HSRP スタンバイになるように設定し、各 vPC デバイスの VLAN インターフェイスが同じ管理/動作モードにあることを確認します (vPC および HSRP の詳細については、「vPC ピア リンクとルーティング」の項を参照)。

単方向リンク検出 (UDLD) の設定では、次の留意点に注意してください。

- LACP がポート チャンネル集約プロトコルとして使用されている場合は、vPC ドメイン内に UDLD は必要ありません。
- LACP がポート チャンネル集約プロトコル (静的なポート チャンネル) として使用されていない場合は、vPC メンバー ポートの通常モードで UDLD を使用します。
- STP が Bridge Assurance なしで使用されている場合と LACP が使用されていない場合は、vPC 孤立ポートの通常モードで UDLD を使用します。

## ピアキーブアライブリンクとメッセージ

Cisco NX-OS ソフトウェアは、vPC ピア間でピアキーブアライブリンクを使用して、設定可能なキーブアライブメッセージを定期的送信します。これらのメッセージを送信するには、ピアデバイス間にレイヤ3接続がなくはなりません。ピアキーブアライブリンクが有効になつて稼働していないと、システムは vPC ピア リンクを稼働させることができません。



- (注) vPC ピアキーブアライブリンクを、各vPCピアデバイス内のレイヤ3インターフェイスにマッピングされている独立した VRF に関連付けることを推奨します。独立した VRF を設定しなかった場合は、デフォルトで管理 VRF と管理ポートが使用されます。vPC ピア キープアライブ メッセージの送受信に vPC ピア リンク 自体を使用することはしないでください。

片方の vPC ピア デバイスに障害が発生したら、vPC ピア リンクの他方の側にある vPC ピア デバイスは、ピアキーブアライブメッセージを受信しなくなることによってその障害を感知します。vPC ピアキーブアライブ メッセージのデフォルトの間隔は、1 秒です。この間隔は、400 ミリ秒～ 10 秒の範囲内で設定可能です。

ホールドタイムアウト値は、3～10秒の範囲内で設定可能で、デフォルトのホールドタイムアウト値は3秒です。このタイマーは、vPC ピアリンクがダウンすると開始します。セカンダリ vPC ピア デバイスは、ネットワークの収束が確実に発生してから vPC アクションが発生するようにするために、このホールドタイムアウト期間の間は vPC ピアキーブアライブ メッセージを無視します。ホールドタイムアウト期間の目的は、誤ったポジティブケースを防ぐことです。

タイムアウト値は、3～20秒の範囲内で設定可能で、デフォルトのタイムアウト値は5秒です。このタイマーは、ホールドタイムアウト間隔が終了した時点で開始します。このタイムアウト期間の間は、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 vPC ピアキーブアライブ hello メッセージが送信されてこないかチェックします。セカンダリ vPC ピア デバイスが1つの hello メッセージを受信したら、そのデバイスは、セカンダリ vPC ピア デバイス上のすべての vPC インターフェイスをディセーブルにします。

ホールドタイムアウトパラメータとタイムアウトパラメータの相違点は、次のとおりです。

- ホールドタイムアウトの間は、vPCセカンダリ デバイスは、受信したキーブアライブメッセージに基づいてアクションを起こしません。それにより、たとえばスーパーバイザがピアリンクがダウンした数秒後に失敗した場合などに、キーブアライブが一時的に受信される可能性がある場合に、システムがアクションを起こすのを回避できます。
- タイムアウト中は、vPCセカンダリ デバイスは、設定された間隔が終了するまでにキーブアライブメッセージを受信できないと、vPCプライマリ デバイスになるというアクションを取ります。

キーブアライブメッセージへのタイマーの設定については、「vPC キープアライブリンクとメッセージの設定」の項を参照してください。



- (注) ピアキーブアライブメッセージに使用される送信元 IP アドレスと宛先 IP アドレスがどちらもネットワーク上で一意であり、かつそれらの IP アドレスがその vPC ピアキーブアライブリンクに関連付けられている VRF から到達可能であることを確認してください。

ピアキーブアライブ IP アドレスは、グローバルユニキャストアドレスである必要があります。リンクローカルアドレスはサポートされていません。

コマンドラインインターフェイス (CLI) を使用して、vPC ピアキープアライブメッセージを使用するインターフェイスを信頼できるポートとして設定してください。優先順位をデフォルト (6) のままにしておくか、またはもっと高い値に設定します。

## vPC ドメイン

vPC ドメイン ID を使用すれば、vPC ダウンストリーム デバイスに接続されている vPC ピアリンクとポートを識別できます。

vPC ドメインは、キープアライブメッセージや他の vPC ピアリンク パラメータを、デフォルト値をそのまま使用するのではなく値を設定する場合に使用する構成モードでもあります。これらのパラメータの設定の詳細については、「vPC の設定」の項を参照してください。

vPC ドメインを作成するには、まず各 vPC ピア デバイス上で、1 ~ 1000 の値を使用して vPC ドメイン ID を作成しなければなりません。vPC ピアごとに設定できる vPC ドメイン ID は 1 つだけです。

各デバイス上で、vPC ピアリンクとして機能させるポートチャネルを明示的に構成する必要があります。各デバイス上で vPC ピアリンクにしたポートチャネルを、1 つの vPC ドメインからの同じ vPC ドメイン ID に関連付けます。このドメイン内で、システムはループフリートポロジとレイヤ 2 マルチパスを提供します。

これらのポートチャネルと vPC ピアリンクは、静的にしか構成できません。ポートチャネルおよび vPC ピアリンクは、LACP を使用するかまたはプロトコルなしのいずれかで構成できます。各 vPC でポートチャネルを設定するにはアクティブモードのインターフェイスで LACP を使用することを推奨します。それにより、ポートチャネルのフェールオーバーシナリオの最適でグレースフルなリカバリが保証され、ポートチャネル間の設定不一致に対する設定検査が行われます。

vPC ピア デバイスは、設定された vPC ドメイン ID を使用して、一意の vPC システム MAC アドレスを自動的に割り当てます。各 vPC ドメインが、具体的な vPC 関連操作に ID として使用される一意の MAC アドレスを持ちます。ただし、デバイスは vPC システム MAC アドレスを LACP などのリンクスコープでの操作にしか使用しません。連続したレイヤ 2 ネットワーク内の各 vPC ドメインを、一意のドメイン ID で作成することを推奨します。Cisco NX-OS ソフトウェアにアドレスを割り当てさせるのではなく、vPC ドメインに特定の MAC アドレスを設定することもできます。

vPC MAC テーブルを表示する詳細については、「vPC および孤立ポート」の項を参照してください。

vPC ドメインを作成した後は、Cisco NX-OS ソフトウェアによって vPC ドメインのシステムプライオリティが作成されます。vPC ドメインに特定のシステムプライオリティを設定することもできます。



---

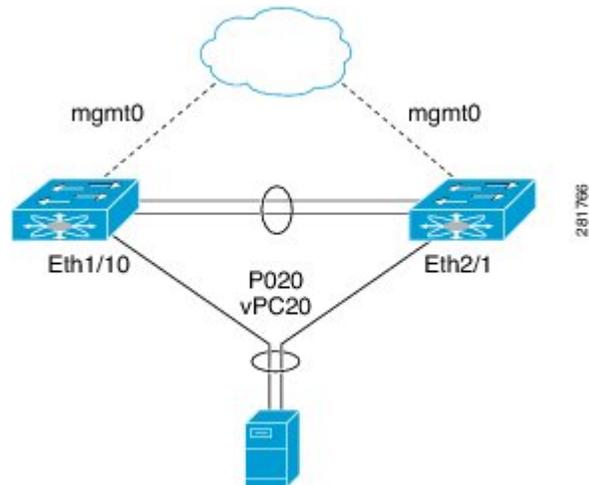
(注) システムプライオリティを手動で設定する場合は、必ず両方の vPC ピア デバイス上で同じプライオリティ値を割り当てる必要があります。vPC ピア デバイス同士が異なるシステムプライオリティ値を持っていると、vPC は稼働しません。

---

## vPC トポロジ

次の図は、Cisco Nexus 9000 シリーズ デバイス ポートが別のスイッチまたはホストに直接接続され、vPC の一部となるポート チャンネルの一部として設定される基本設定を示しています。

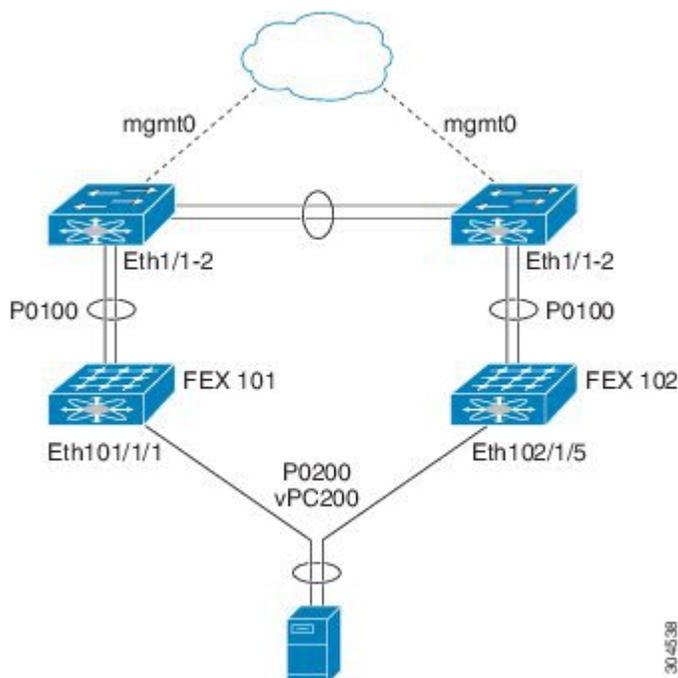
図 5: vPC トポロジのスイッチ



この図では、vPC 20 がポート チャンネル 20 で設定され、最初のデバイスには Eth1/10 が、2 番目のデバイスには Eth2/1 がメンバポートとしてあります。

図で示されるように、ファブリック エクステンダ (FEX) を通してピア デバイスから vPC を設定できます。

図 6: FEX Straight-Through トポロジ (ホスト vPC)



この図では、各 FEX は Cisco Nexus 9000 シリーズ デバイスがあるシングル ホーム接続 (Straight-Through FEX トポロジ) です。この FEX 上のホストインターフェイスはポートチャネルとして設定され、それらのポートチャネルは vPC として設定されています。Eth101/1/1 および Eth102/1/5 は、PO200 のメンバーとして設定され、PO200 は vPC 200 に対し設定されます。

どちらのトポロジでも、ポートチャネル P020 および P0200 をピアスイッチ上でまったく同じように設定する必要があります。その後、設定の同期を使用して vPC スイッチの設定を同期します。

FEX ポートの設定に関する詳細は、『[Cisco Nexus 2000 Series NX-OS Fabric Extender Configuration Guide for Cisco Nexus 9000 Series Switches](#)』を参照してください。

## vPC インターフェイスの互換パラメータ

多くの設定パラメータおよび動作パラメータが、vPC 内のすべてのインターフェイスで同じでなければなりません。vPC ピアリンクに使用するレイヤ 2 ポートチャネルはトランクモードに設定することを推奨します。

vPC 機能をイネーブルにし、さらに両方の vPC ピアデバイス上でピアリンクを設定すると、シスコファブリックサービス (CFS) メッセージにより、ローカル vPC ピアデバイスに関する設定のコピーがリモート vPC ピアデバイスへ送信されます。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 (CFS の詳細については、「vPC および孤立ポート」の項を参照)。



- (注) **show vpc consistency-parameters** を入力します。vPC 内のすべてのインターフェイスで設定されている値を表示します。表示される設定は、vPC ピア リンクおよび vPC の稼働を制限する可能性のある設定だけです。



- (注) ポート チャンネルの互換性パラメータは、物理スイッチのすべてのポート チャンネル メンバーで同じである必要があります。vPC の一部になるように共有インターフェイスを設定できません。

vPC の互換性チェックプロセスは、正規のポートチャンネルの互換性チェックとは異なります。  
正規のポート チャンネルについては、「ポート チャンネルの設定」の章を参照してください。

## 同じでなければならない設定パラメータ

このセクションの設定パラメータは、vPC ピア リンクの両方のデバイスで同じに設定する必要があります。そうしないと、vPC は一時停止モードに完全にまたは部分的に移動します。



- (注) ここで説明する動作パラメータおよび設定パラメータは、vPC 内のすべてのインターフェイスで一致している必要があります。



- (注) **show vpc consistency-parameters** を入力します。vPC 内のすべてのインターフェイスで設定されている値を表示します。表示される設定は、vPC ピア リンクおよび vPC の稼働を制限する可能性のある設定だけです。

vPC インターフェイスでのこれらのパラメータの一部は、デバイスによって自動的に互換性がチェックされます。インターフェイスごとのパラメータは、インターフェイスごとに一貫性を保っていなければならない、グローバルパラメータはグローバルに一貫性を保っていなければならない。

- ポートチャンネル モード：オン、オフ、またはアクティブ（ただし、ポートチャンネル モードは vPC ピアの各サイドでアクティブ/パッシブにできます）
- チャンネル単位のリンク速度
- チャンネル単位のデュプレックス モード
- チャンネルごとのトランク モード：
  - ネイティブ VLAN
  - トランク上で許可される VLAN

- ネイティブ VLAN トラフィックのタグging
- スパニング ツリー プロトコル (STP) モード
- Multiple Spanning Tree 用の STP リージョン コンフィギュレーション
- VLAN ごとのイネーブル/ディセーブル状態
- STP グローバル設定 :
  - ブリッジ保証設定
  - ポート タイプ設定
  - ループ ガード設定
- STP インターフェイス設定 :
  - ポート タイプ設定
  - ループ ガード
  - ルート ガード
- 最大伝送単位 (MTU)

これらのパラメータのいずれかがイネーブルになっていなかったり、片方のデバイスでしか定義されていないと、vPC の一貫性チェックではそのパラメータは無視されます。



(注) どの vPC インターフェイスもサスペンドモードになっていないことを確認するには、**show vpc brief** および **show vpc consistency-parameters** コマンドを実行し、syslogメッセージを確認します。

## 同じにすべき設定パラメータ

次の挙げるパラメータのいずれかが両方の vPC ピア デバイス上で同じように設定されていないと、誤設定が原因でトラフィックフローに望ましくない動作が発生する可能性があります。

- MAC エージング タイマー
- スタティック MAC エントリ
- VLAN インターフェイス : vPC ピア リンク エンドにある各デバイスの VLAN インターフェイスが両エンドで同じ VLAN 用に設定されていなければならない、さらに同じ管理モードで同じ動作モードになっていなければなりません。vPC ピア リンクの 1 個の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。すべての VLAN をプライマリ vPC デバイスとセカンダリ vPC デバイスの両方で作成する必要があります。そうならない VLAN は、停止します。
- ACL のすべての設定とパラメータ

- Quality of Service (QoS) の設定とパラメータ
- STP インターフェイス設定：
  - BPDU フィルタ
  - BPDU ガード
  - コスト
  - リンク タイプ
  - プライオリティ
  - VLAN (Rapid PVST+)
- ポート セキュリティ
- Cisco Trusted Security (CTS)
- 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
- 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)
- 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
- ホット スタンバイ ルーティング プロトコル (HSRP)
- プロトコルに依存しないマルチキャスト (PIM)
- すべてのルーティング プロトコル設定

すべての設定パラメータで互換性が取れていることを確認するために、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。

## パラメータの不一致によってもたらされる結果

稼働中の vPC で不一致が発生した場合にセカンダリ ピア デバイス上のリンクのみを一時停止する、グレースフル整合性検査機能を設定できます。この機能は CLI のみで設定可能で、デフォルトでイネーブルになっています。

graceful consistency-check コマンドはデフォルトで設定されます。

一致しなければならないパラメータのリストのすべてのパラメータに関する整合性検査の一部として、システムはすべての VLAN の一貫性をチェックします。

vPC は稼働を継続し、矛盾した VLAN のみがダウンします。この VLAN 単位の整合性検査機能はディセーブルにできず、マルチ スパニングツリー (MST) VLAN には適用されません。

## vPC 番号

vPC ドメイン ID と vPC ピア リンクを作成し終わったら、ダウストリーム デバイスを各 vPC ピア デバイスに接続するためのポート チャネルを作成します。つまり、プライマリ vPC ピア デバイスからダウストリーム デバイスへのポート チャネルを 1 つ作成し、もう 1 つ、セカンダリ ピア デバイスからダウストリーム デバイスへのポート チャネルも作成します。



- (注) スイッチとしてもブリッジとしても機能しないホストまたはネットワーク デバイスに接続されているダウストリーム デバイス上のポートは、STP エッジ ポートとして設定することを推奨します。

各 vPC ピア デバイス上で、ダウストリーム デバイスに接続するポート チャネルに vPC 番号を割り当てます。vPC の作成時にトラフィックが中断されることはほとんどありません。すべてのポート番号に、ポート チャネル自体と同じ vPC ID 番号を割り当てると（つまり、ポート チャネル 10 には vPC ID 10）、設定が簡単になります。



- (注) vPC ピア デバイスからダウストリーム デバイスに接続するためにポート チャネルに割り当てる vPC 番号は、両方の vPC ピア デバイスで同じである必要があります。

## ヒットレス vPC ロールの変更

仮想ポート チャネル (vPC) は、2 つの異なる Cisco Nexus 9000 シリーズ デバイスに物理的に接続されたリンクを、単一のポート チャネルとして扱えるようにします。vPC ロールの変更機能は、トラフィック フローに影響を与えることなく、vPC ピア間で vPC ロールを切り替えることができるようにします。vPC ロールの切り替えは、vPC ドメインに属しているデバイスのロール優先順位の値に基づいて行われます。vPC ロールの切り替え中にロール優先順位が低い vPC ピア デバイスがプライマリ vPC デバイスとして選択されます。vpc role preempt コマンドを使用して、ピア間で vPC ロールを切り替えることができます。

ヒットレス vPC ロール変更の設定方法については、[ヒットレス vPC ロール変更の設定 \(71 ページ\)](#) を参照してください。

## 他のポート チャネルの vPC への移行



- (注) ダウストリーム デバイスは、ポート チャネルを使用して両方の vPC ピア デバイスに接続する必要があります。

ダウストリーム デバイスを接続するために、プライマリ vPC ピア デバイスからダウストリーム デバイスへのポート チャネルを作成し、セカンダリ ピア デバイスからダウストリー

ム デバイスへのもう 1 つのポート チャンネルを作成します。各 vPC ピア デバイス上で、ダウンストリーム デバイスに接続するポート チャンネルに vPC 番号を割り当てます。vPC の作成時にトラフィックが中断されることはほとんどありません。

## vPC オブジェクト トラッキング



- (注) Cisco Nexus 9500 デバイスの異なるモジュールの専用ポート上で vPC ピア リンクを設定して、障害発生の可能性を下げることをお勧めします。これは、障害の可能性を減らすために推奨されます。復元力を最適にしたい環境では、少なくとも 2 つのモジュールを使用してください。

vPC オブジェクト トラッキングは、vPC ピア リンクとコアへのアップリンクの両方が存在するモジュールで障害が発生した場合、トラフィックのブラックホールになってしまうことを防止するために使用されます。トラッキングインターフェイス機能により、影響を受けるスイッチで vPC を一時停止し、トラフィックのブラックホールとなるのを防ぐことができます。

すべての vPC ピア リンクとコアに面するインターフェイスを単一モジュール上で設定しなければならない場合は、両方の vPC ピア デバイス上のすべての vPC ピア リンク上にあり、コアへのレイヤ 3 リンクに関連付けられているトラック オブジェクトとトラック リストをコマンドラインインターフェイスを使用して設定してください。トラック リスト上のすべてのトラッキング対象オブジェクトが停止した場合、システムは次のように動作するため、この設定を使用すれば、その特定のモジュールが停止した場合のトラフィックのドロップを避けることができます。

- vPC プライマリ ピア デバイスによるピアキープアライブメッセージの送信を停止します。これにより、vPC セカンダリ ピア デバイスが強制的に引き継がされます。
- その vPC ピア デバイス上のすべてのダウンストリーム vPC を停止させます。これにより、すべてのトラフィックが強制的に他の vPC ピア デバイスに向けてそのアクセス スイッチでルーティングされます。

いったんこの機能を設定したら、モジュールに障害が発生した場合には、システムが自動的にプライマリ vPC ピア デバイス上のすべての vPC リンクを停止させ、ピアキープアライブメッセージを停止します。このアクションにより、vPC セカンダリ デバイスが強制的にプライマリ ロールを引き継がされ、システムが安定するまで、すべての vPC トラフィックがこの新しい vPC プライマリ デバイスに送られます。

コアに対するすべてのリンクおよびすべての vPC ピア リンクを含むトラック リストを、そのオブジェクトとして作成する必要があります。このトラック リストの指定した vPC ドメインに対して、トラッキングをイネーブルにします。この同じ設定を他方の vPC ピア デバイスにも適用します。オブジェクト トラッキングおよびトラック リストの詳細については、『[Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide](#)』を参照してください。



- (注) 次の例では、BooleanORを追跡リストで使用し、完全なモジュール障害の場合にのみすべてのトラフィックがvPCピアデバイスへ流れるよう強制します。コアインターフェイスまたはvPCピアリンクがダウンしたときにスイッチオーバーをトリガーする場合は、次の追跡リストでブールANDを使用します。

単一モジュール上の関連するすべてのインターフェイスが故障したときにvPCをリモートピアに切替えるように追跡リストを設定するには、次の手順に従います。

1. インターフェイス上（コアへのレイヤ3）およびポートチャネル上（vPCピアリンク）でトラックオブジェクトを設定します。

```
switch(config-if)# track 35 interface ethernet 8/35 line-protocol
switch(config-track)# track 23 interface ethernet 8/33 line-protocol
switch(config)# track 55 interface port-channel 100 line-protocol
```

2. ブールORを使って追跡リスト内のすべてのインターフェイスを含むトラックリストを作成して、すべてのオブジェクトに障害が発生したときにトリガーします。

```
switch(config)# track 44 list boolean OR
switch(config-track)# object 23
switch(config-track)# object 35
switch(config-track)# object 55
switch(config-track)# end
```

3. このトラックオブジェクトをvPCドメインに追加します。

```
switch(config)# vpc domain 1
switch(config-vpc-domain)# track 44
```

4. トラックオブジェクトを表示します。

```
switch# show vpc brief
Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id : 1
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
Configuration consistency status: success
vPC role : secondary
Number of vPCs configured : 52
Track object : 44
vPC Peer-link status
-----
id Port Status Active vlans
-----
1 Po100 up 1-5,140
vPC status
-----
id Port Status Consistency Reason Active vlans
-----
```

```
1 Pol up success success 1-5,140
```

次に、オブジェクト トラッキングに関する情報を表示する例を示します。

```
switch# show track brief
Track Type Instance Parameter State Last
Change
23 Interface Ethernet8/33 Line Protocol UP 00:03:05
35 Interface Ethernet8/35 Line Protocol UP 00:03:15
44 List ----- Boolean
or UP 00:01:19
55 Interface port-channel100 Line Protocol UP 00:00:34
```

## その他の機能との vPC の相互作用

### vPC と LACP

LACP は、vPC ドメインのシステム MAC アドレスを使用して、vPC の LACP Aggregation Group (LAG) ID を形成します (LAG-ID および LACP については、「ポートチャンネルの設定」の章を参照)。

ダウンストリームデバイスからのチャンネルも含めて、すべての vPC ポートチャンネル上の LACP を使用できます。LACP は、vPC ピア デバイスの各ポートチャンネル上のインターフェイスのアクティブモードで設定することを推奨します。この設定により、デバイス、単方向リンク、およびマルチホップ接続の間の互換性をより簡単に検出できるようになり、実行時の変更およびリンク障害に対してダイナミックな応答が可能になります。

vPC ピア リンク デバイスのシステム プライオリティを手動で設定して、vPC ピア リンク デバイスが、接続されているダウンストリーム デバイスより確実に高い LACP プライオリティを持つようにすることを推奨します。システム プライオリティの値が低いほど、高い LACP プライオリティを意味します。



- (注) システム プライオリティを手動で設定する場合は、必ず両方の vPC ピア デバイス上で同じプライオリティ値を割り当てる必要があります。vPC ピア デバイス同士が異なるシステム プライオリティ値を持っていると、vPC は稼働しません。

### vPC ピア リンクと STP

vPC はループフリーなレイヤ 2 トポロジを提供しますが、それでもやはり、誤った配線やケーブルの欠陥、誤設定などから保護するためのフェールセーフ メカニズムを STP が提供する必要があります。vPC を初めて稼働させたときに、STP による再コンバージェンスが発生します。STP は、vPC ピア リンクを特殊なリンクとして扱い、常に vPC ピア リンクを STP のアクティブ トポロジに含めます。

すべての vPC ピア リンク インターフェイスを STP ネットワーク ポートタイプに設定して、すべての vPC リンク上でブリッジアシュアランスが自動的に有効になるようにすることを推

奨めます。また、vPC ピアリンク上ではどの STP 拡張機能も有効にしないことも推奨します。STP 拡張がすでに設定されている場合、その拡張が vPC ピアリンクの問題の原因となることはありません。

MST と Rapid PVST+ の両方を実行している場合は、必ず PVST シミュレーション機能を正しく設定してください。

STP 拡張機能および PVST シミュレーションについては、『[Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide](#)』を参照してください。



(注) パラメータのリストは、vPC ピアリンクの両サイドの vPC ピアデバイス上で同じになるように設定する必要があります。このような一致が必要な設定については、「vPC インターフェイスの互換パラメータ」の項を参照してください。

STP は分散しています。つまり、このプロトコルは、両方の vPC ピアデバイス上で実行され続けます。ただし、プライマリデバイスとして選択されている vPC ピアデバイス上での設定が、セカンダリ vPC ピアデバイス上の vPC インターフェイスの STP プロセスを制御します。

プライマリ vPC デバイスは、Cisco Fabric Services over Ethernet (CFS over E) を使用して、vPC セカンダリピアデバイス上の STP の状態を同期させます。CFS over E の詳細については、「vPC および孤立ポート」の項を参照してください。

vPC の STP プロセスも、ピアリンク上で接続されているデバイスの 1 つに障害が発生したときにそれを検出するために、定期的なキープアライブメッセージに依存しています。これらのメッセージについては、「ピアキープアライブリンクとメッセージ」の項を参照してください。

vPC マネージャが、vPC ピアデバイス間で、プライマリデバイスとセカンダリデバイスを設定して 2 つのデバイスを STP 用に調整する提案/ハンドシェイク合意を実行します。その後、プライマリ vPC ピアデバイスが、プライマリデバイスとセカンダリデバイス両方での STP プロトコルの制御を行います。プライマリ vPC ピアデバイスを STP プライマリルートデバイスとして設定し、セカンダリ vPC デバイスを STP セカンダリルートデバイスになるように設定することを推奨します。

プライマリ vPC ピアデバイスがセカンダリ vPC ピアデバイスにフェールオーバーした場合、STP トポロジには何の変化も発生しません。

BPDU は、代表ブリッジ ID フィールドで、STP ブリッジ ID の vPC に設定されている MAC アドレスを使用します。vPC プライマリデバイスが、vPC インターフェイス上でこれらの BPDU を送信します。

次のパラメータについて同じ STP 設定を使用して、vPC ピアリンクの両エンドを設定する必要があります。

- STP グローバル設定：
  - STP モード
  - 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
  - ポート タイプ設定
  - ループ ガード設定
- STP インターフェイス設定：
    - ポート タイプ設定
    - ループ ガード
    - ルート ガード



(注) これらのパラメータのいずれかに誤設定があった場合、Cisco NX-OS ソフトウェアが vPC 内のすべてのインターフェイスを停止します。syslog をチェックし、**show vpc brief** を開始します。コマンドを入力して、vPC インターフェイスが停止していないか確認してください。

次の STP インターフェイス設定が、vPC ピアリンクの両側で同じになっていることを確認します。そうならないと、トラフィックフローに予測不能な動作が発生する可能性があります。

- BPDU フィルタ
- BPDU ガード
- コスト
- リンク タイプ
- プライオリティ
- VLAN (PVRST+)



(注) vPC ピアリンクの両側での設定を表示して、設定が同じであることを確認してください。

**show spanning-tree** コマンドを使用すればコマンドで vPC に関する情報を表示できます。例については、『[Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide](#)』を参照してください。



- (注) ダウンストリームデバイスのポートは、STP エッジポートとして設定することを推奨します。スイッチに接続されているすべてのホストポートを STP エッジポートとして設定してください。STP ポート タイプの詳細については、『[Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide](#)』を参照してください。

## vPC ピア スイッチ

vPC ピア スイッチ機能は、STP コンバージェンスに関連するパフォーマンス上の問題を解決するために、Cisco NX-OS に追加されました。この機能により、一対の Cisco Nexus 9000 シリーズ デバイスをレイヤ 2 トポロジ内に 1 つの STP ルートとして表示できます。この機能は、STP ルートを vPC プライマリ スイッチに固定する必要性をなくし、vPC プライマリ スイッチに障害が発生した場合の vPC コンバージェンスを向上させます。

ループを回避するために、vPC ピア リンクは STP 計算からは除外されます。vPC ピア スイッチ モードでは、ダウンストリーム スイッチでの STP BPDU タイムアウトに関連した問題（この問題は、トラフィックの中断につながります）を避けるために、STP BPDU が両方の vPC ピア デバイスから送信されます。

この機能は、すべてのデバイス vPC に属する純粋なピア スイッチ トポロジで使用できます。



- (注) ピア スイッチ機能は、vPC を使用するネットワークでサポートされ、STP ベースの冗長性はサポートされません。ハイブリッドピア スイッチ設定で vPC ピア リンクに障害が発生すると、トラフィックが失われる場合があります。このシナリオでは、vPC ピア は同じ STP ルート ID や同じブリッジ ID を使用します。アクセス スイッチのトラフィックは 2 つに別れ、その半分が最初の vPC ピア に、残りの半分が 2 番目の vPC ピア に転送されます。vPC ピア リンク障害は、南北のトラフィックには影響がありませんが、東西のトラフィックが失われます。

STP 拡張機能および Rapid PVST+ については、『[Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide](#)』を参照してください。

## vPC ピア ゲートウェイ

vPC ピア デバイスを、vPC ピア デバイスの MAC アドレスに送信されるパケットに対してもゲートウェイとして機能するように設定できます。

**peer-gateway** コマンドを使用し、**peer-gateway** コマンドを使用します。



- (注) この項で説明している **peer-gateway exclude-vlan** コマンド (vPC ピア デバイスでレイヤ 3 バックアップルーティングの VLAN インターフェイスを構成する際に使用) は、サポートされていません。

一部のネットワーク接続ストレージ (NAS) デバイスまたはロードバランサは、特定のアプリケーションのパフォーマンスを最適化するのに役立つ機能を備えている場合があります。これらの機能により、同じサブネットにローカルに接続されていないホストから送信された要求に応答するときに、デバイスはルーティングテーブルのルックアップを回避できます。このようなデバイスは、一般的な HSRP ゲートウェイではなく、送信元 Cisco Nexus 9000 シリーズデバイスの MAC アドレスを使用して、トラフィックに応答する場合があります。この動作は、一部の基本的なイーサネット RFC 基準に準拠していません。ローカルではないルータ MAC アドレスの vPC デバイスに到達するパケットは、vPC ピア リンクを介して送信され、最終的な宛先が他の vPC の背後にある場合には、組み込みの vPC ループ回避メカニズムによってドロップされる場合があります。

vPC ピアゲートウェイ機能は、vPC スイッチが、vPC ピアのルータ MAC アドレスを宛先とするパケットに対して、アクティブなゲートウェイとして機能することを可能にします。この機能は、このようなパケットが vPC ピア リンクを通過する必要なしにローカルに転送されることを可能にします。このシナリオでは、この機能によって vPC ピア リンクの使用が最適化され、トラフィック損失が回避されます。

ピアゲートウェイ機能の設定は、プライマリ vPC ピアとセカンダリ vPC ピアの両方で行う必要がありますが、デバイスの稼働も vPC トラフィックも中断しません。vPC ピアゲートウェイ機能は、vPC ドメイン サブモードの下でグローバルに設定できます。

この機能をイネーブルにすると、ピアゲートウェイルータを介してスイッチングされたパケットの IP リダイレクトメッセージの発生を避けるために、Cisco NX-OS は vPC VLAN を介してマッピングされるすべてのインターフェイス VLAN 上で IP リダイレクトを自動的にディセーブルにします。

TTL が 1 のパケットが TTL の有効期限が原因で伝送中にドロップされるように、ピアゲートウェイ vPC デバイスに到達するパケットは、デクリメントされたパケット存続時間 (TTL) を有しています。ピアゲートウェイ機能がイネーブルで、TTL が 1 のパケットを送信する特定のネットワーク プロトコルが vPC VLAN で動作する場合は、この状況を考慮する必要があります。

## vPC および ARP または ND

Cisco Fabric Service over Ethernet (CFSoS) プロトコルの信頼性が高いトランスポートメカニズムを使用した、vPC ピア間のテーブル同期に対応する機能が Cisco NX-OS に追加されました。**ip arp synchronize** を有効にする必要があります および **ipv6 nd synchronize** コマンドをイネーブルにし、vPC ピア間のアドレステーブルのコンバージェンスの高速化をサポートする必要があります。このコンバージェンスにより、vPC ピアリンクポートチャネルがフラップしたり、vPC ピアがオンラインに戻るときに、IPv4 の場合は ARP テーブルの復元でまたは IPv6 の場合は ND テーブルの復元で発生する遅延を解消できます。

## vPC マルチキャスト : PIM、IGMP、および IGMP スヌーピング

Nexus 9000 シリーズデバイス用の Cisco NX-OS ソフトウェアは、vPC で次をサポートします。

- PIM Any Source Multicast (ASM)。
- PIM Source-Specific Multicast (SSM)。



(注) Cisco NX-OS ソフトウェアは、vPC での双方向 (BIDR) をサポートしません。

ソフトウェアが、マルチキャストフォワーディングを両方の vPC ピア デバイス上で同期された状態に保ちます。vPC ピア デバイス上の IGMP スヌーピング プロセスは、学習したグループ情報を vPC ピア リンクを通じて他の vPC ピア デバイスと共有します。マルチキャスト状態は、常に両方の vPC ピア デバイス上で同期されます。vPC モードでの PIM プロセスは、1 つの vPC ピア デバイスだけが受信者に向けてマルチキャストトラフィックを転送する状態を確保します。

各 vPC ピアは、レイヤ 2 またはレイヤ 3 デバイスです。マルチキャストトラフィックは 1 つの vPC ピア デバイスだけから伝送されます。次のシナリオで、重複したパケットが観察される場合があります。

- 孤立ホスト
- 送信元と受信者が、マルチキャストルーティングのイネーブルになった異なる VLAN 内のレイヤ 2 vPC クラウド内にあり、vPC メンバリンクが停止している場合。

次のシナリオで、ごくわずかなトラフィック損失が観察される場合があります。

- トラフィックを転送している vPC ピア デバイスをリロードした場合。
- トラフィックを転送している vPC ピア デバイスの PIM を再起動した場合。

全体的なマルチキャストコンバージェンス時間は、スケールと vPC ロールの変更 / PIM 再起動期間に依存します。

必ずすべてのレイヤ 3 デバイスを両方の vPC ピア デバイスにデュアル接続してください。片方の vPC ピア デバイスが停止した場合、他方の vPC ピア デバイスが、通常どおりにすべてのマルチキャストトラフィックを転送し続けます。

次に、vPC PIM および vPC IGMP/IGMP スヌーピングについて説明します。

- vPC PIM : vPC モードの PIM プロセスは、1 台の vPC ピア デバイスのみがマルチキャストトラフィックを転送する状態を確保します。vPC モードの PIM プロセスは、送信元の状態を両方の vPC ピア デバイスと同期させ、トラフィックを転送する vPC ピア デバイスを選択します。
- vPC IGMP/IGMP スヌーピング : vPC モードの IGMP プロセスは、両方の vPC ピア デバイスで指定ルータ (DR) 情報を同期させます。デュアル DR は、vPC モードのときに IGMP で利用可能です。デュアル DR は、vPC モードでない場合は利用できません。これは、両方の vPC ピア デバイスがピア間のマルチキャストグループ情報を保持するためです。



- (注) vPC VLAN (vPC ピアリンクで伝送される VLAN) 上のスイッチ仮想インターフェイス (SVI) とダウンストリーム デバイス間の PIM 隣接関係はサポートされません。この設定により、マルチキャストパケットがドロップされる可能性があります。ダウンストリームデバイスと PIM ネイバー関係が必要な場合は、vPC SVI ではなく、物理レイヤ 3 インターフェイスを Nexus スイッチで使用する必要があります。

vPC VLAN 上の SVI では、vPC ピアスイッチとの PIM 隣接関係が 1 つだけサポートされます。vPC-SVI の vPC ピアスイッチ以外のデバイスとの vPC ピアリンク上の PIM 隣接関係はサポートされていません。

IGMP スヌーピングは、両方の vPC ピアデバイス上で同じようにイネーブルにしたりディセーブルにしたりする必要があり、すべての機能設定を同じにする必要があります。IGMP スヌーピングは、デフォルトで有効になっています。



- (注) 次のコマンドは、vPC モードでサポートされていません。

- **ip pim spt-threshold infinity**
- **ip pim use-shared-tree-only**

マルチキャストの詳細については、『Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide』を参照してください。

## マルチキャスト PIM デュアル DR (プロキシ DR)

デフォルトでは、マルチキャスト ルータは該当する受信先が存在する場合のみ PIM ジョインをアップストリームに送信します。これらの該当する受信先は、IGMP ホスト (IGMP レポートを通じて通信します) または他のマルチキャスト ルータ (PIM ジョインを通じて通信します) のどちらかの場合があります。

Cisco NX-OS vPC 実装では、PIM はデュアル指定ルータ (DR) モードで動作します。つまり、vPC デバイスが vPC SVI の発信インターフェイス (OIF) 上の DR である場合、そのピアは自動的にプロキシ DR ロールを引き継ぎます。IGMP は、OIF が DR である場合、OIF (レポートはその OIF で学習されます) をフォワーディングに追加します。デュアル DR では、両方の vPC デバイスには、次の例に示すように、vPC SVI OIF に対して同一のエントリ (\*,G) があります。

```
VPC Device1:
-----
(*,G)
oif1 (igmp)
VPC Device2:
-----
(*,G)
oif1 (igmp)
```

## IP PIM PRE-BUILD SPT

マルチキャストソースがレイヤ3クラウド (vPC ドメイン外) にある場合、1つの vPC ピアが送信元のフォワーダとして選定されます。このフォワーダの選択は、送信元に到達するためのメトリックに基づきます。関係がある場合、vPC プライマリはフォワーダとして選択されます。フォワーダのみがその関連する (S,G) 内に vPC OIF を持っており、非フォワーダ (S,G) は 0 OIF を持っています。したがって、フォワーダのみがこの例に示すように、送信元へ PIM (S,G) ジョインを送信します。

```
VPC Device1 (say this is Forwarder for Source 'S'):
-----
(*,G)
oif1 (igmp)
(S,G)
oif1 (mrib)
VPC Device2:
-----
(*,G)
oif1 (igmp)
(S,G)
NULL
```

障害が発生した場合 (たとえば、フォワーダのレイヤ3リバースパス転送 (RPF) リンクが動作しない、またはフォワーダがリロードされるなど)、現在の非フォワーダが最終的にフォワーダになる場合は、トラフィック取得するために送信元への (S,G) に対する PIM ジョインの送信を開始をする必要があります。送信元に到達するホップ数によって、この操作には時間がかかる場合があります (PIM はホップバイホッププロトコルです)。

この問題を排除し、より優れたコンバージェンスを取得するには、**ip pim pre-build-spt** を使用します コマンドを使用します。このコマンドにより、マルチキャストルートに 0 OIF があっても PIM はジョインを送信できます。vPC デバイスでは、非フォワーダは送信元へ PIM (S,G) ジョインをアップストリームに送信します。欠点は、非フォワーダからのリンク帯域幅のアップストリームが最終的にそれによってドロップされるトラフィックに使用されることです。コンバージェンスの向上によるメリットは、リンク使用帯域幅をはるかに上回っていることです。したがって、vPC を使用する場合は、このコマンドを使用することを推奨します。

## vPC ピア リンクとルーティング

ファーストホップ冗長性プロトコル (FHRP) は、vPC と相互運用します。Hot Standby Routing Protocol (HSRP)、および Virtual Router Redundancy Protocol (VRRP) のすべてが、vPC と相互運用できます。すべてのレイヤ3 デバイスを両方の vPC ピア デバイスにデュアル接続することを推奨します。

プライマリ FHRP デバイスは、たとえセカンダリ vPC デバイスがデータトラフィックを転送したとしても、ARP 要求に応答します。

プライマリ vPC ピア デバイスを FHRP アクティブルータの最も高いプライオリティで設定しておくと、初期の設定確認と vPC/HSRP のトラブルシューティングを簡単にできます。

さらに、if-hsrp コンフィギュレーションモードで **priority** コマンドを使用して、vPC ピアリンク上でイネーブルになっているグループの状態がスタンバイになっているか、またはリッスン

状態になっている場合のフェールオーバーのしきい値を設定できます。インターフェイスがアップまたはダウンするのを防ぐために下限および上限しきい値を設定できます。

VRRP は、vPC ピア デバイス上で実行されている場合に HSRP とよく似た動作を示します。VRRP は、HSRP を設定したのと同じ方法で設定してください。

プライマリ vPC ピア デバイスに障害が発生した場合は、セカンダリ vPC ピア デバイスにフェールオーバーされ、FHRP トラフィックはシームレスに流れ続けます。

バックアップルーティングパスとして機能するように2台のvPCピアデバイス間にルーティング隣接を設定することを推奨します。1台のvPCピアデバイスがレイヤ3アップリンクを失うと、そのvPCはルーテッドトラフィックを他のvPCピアデバイスにリダイレクトでき、そのアクティブレイヤ3アップリンクを活用できます。

次の方法で、バックアップのルーティングパス用のスイッチ間リンクを設定できます。

- 2台のvPCピアデバイス間でレイヤ3リンクを作成します。
- 専用のVLANインターフェイスを持つ非VPC VLAN トランクを使用します。
- 専用のVLANインターフェイスを持つvPCピアリンクを使用します。

vPC 環境での HSRP の焼き付け MAC アドレス オプション (use-bia) の設定、および任意の FHRP プロトコルのための仮想 MAC アドレスの手動での設定は、推奨できません。これらの設定は、vPC ロード バランシングに不利な影響を与えるためです。HSRP use-bia オプションは、vPC ではサポートされていません。カスタム MAC アドレスを設定する際には、両方の vPC ピア デバイスに同じ MAC アドレスを設定する必要があります。

**delay restore** コマンドを使用すればコマンドを使用して、ピアの隣接が形成され、VLAN インターフェイスがバックアップされるまで、vPC+ の回復を遅らせるようにリストア タイマーを設定します。この機能により、vPC が再びトラフィックの受け渡しをし始める前にルーティングテーブルが収束できなかった場合のパケットのドロップを回避できます。**delay restore** コマンドを使用して、この機能を設定します。

復元した vPC ピア デバイス上の VLAN インターフェイスが起動するのを遅延するには、**interfaces-vlan** オプションを **delay restore** のオプション コマンドを使用します。

FHRP およびルーティングに関する詳細情報については、『[Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide](#)』を参照してください。

## vPC ピアリンクのレイヤ3バックアップルートの構成

HSRP や PIM などのアプリケーションを使用するネットワークのレイヤ3にリンクするために、vPC ピア デバイス上の VLAN ネットワーク インターフェイスを使用できます。各ピア デバイス上で VLAN ネットワーク インターフェイスが設定されており、そのインターフェイスが各デバイス上で同じ VLAN に接続されていることを確認してください。また、各 VLAN インターフェイスが、同じ管理/動作モードになっていなければなりません。VLAN ネットワーク インターフェイスの設定の詳細については、「レイヤ3インターフェイスの設定」の章を参照してください。

vPC ピア リンクでフェールオーバーが発生すると、vPC ピア デバイス上の VLAN インターフェイスも影響を受けます。vPC ピア リンクに障害が発生すると、セカンダリ vPC ピア デバイス上の関連付けられている VLAN インターフェイスがシステムによって停止されます。

vPC ピア リンクに障害が発生したときに特定の VLAN インターフェイスが vPC セカンダリ デバイス上で停止しないようにできます。

## CFSoE

Cisco Fabric Services over Ethernet (CFSoE) は、vPC ピア デバイスのアクションを同期化するために使用される信頼性の高い状態転送メカニズムです。CFSoE は、vPC にリンクされている、STP、IGMP などの多くの機能のメッセージとパケットを伝送します。情報は、CFS/CFSoE プロトコルデータ ユニット (PDU) に入れて伝送されます。

CFSoE は、vPC 機能をイネーブルにすると、デバイスによって自動的にイネーブルになります。何も設定する必要はありません。vPC の CFSoE 分散には、IP を介してまたは CFS リージョンに分散する機能は必要ありません。CFSoE 機能が vPC 上で正常に機能するために必要な設定は一切ありません。

CFSoE 転送は、各 VDC にローカルです。

**show mac address-table** コマンドを使用すればコマンドを使用すれば、CFSoE が vPC ピア リンクのために同期する MAC アドレスを表示できます。



- (注) **no cfs eth distribute** または **no cfs distribute** コマンドは入力しないでください。CFSoE for vPC 機能のための CFSoE をイネーブルにしなければなりません。vPC をイネーブルにしてこれらのコマンドのいずれかを入力すると、エラー メッセージが表示されます。

引数を使用せずに **show cfs application** コマンドを入力すると、出力に「Physical-eth」と表示されます。これは、CFSoE を使用しているアプリケーションを表します。

CFS は、TCP/IP を介したデータも転送します。IP 経由の CFS の詳細については、『[Cisco Nexus 9000 Series NX-OS System Management Configuration Guide](#)』を参照してください。



- (注) CFS リージョンはサポートされていません。

## vPC および孤立ポート

vPC 対応でないデバイスが各ピアに接続するとき、接続されたポートはvPCのメンバではないため、孤立ポートと称されます。一方のピアへのデバイスのリンクがアクティブ（フォワーディング）になり、他方のリンクは STP のためスタンバイ（ブロッキング）になります。

vPC ピア リンク障害またはリストアが発生すると、孤立ポートの接続は vPC 障害または復元プロセスにバインドされる可能性があります。たとえば、デバイスのアクティブな孤立ポートがセカンダリ vPC ピアに接続する場合、vPC ピア リンク障害が発生し、vPC ポートがセカンダリ ピアによって一時停止されると、そのデバイスはプライマリ ピアを経由する接続を失い

ます。セカンダリ ピアがアクティブな孤立ポートも一時停止した場合は、デバイスのスタンバイポートがアクティブになり、プライマリピアへの接続が提供され、接続が復元されます。セカンダリピアがvPCポートを一時停止するときに特定の孤立ポートがそのピアによって一時停止され、vPCが復元されるとそのポートが復元されるようにCLIで設定できます。

## 仮想化のサポート

1つのvPC内のすべてのポートが、同じVDC内にはなりません。このバージョンのソフトウェアは、VDCごとに1つのvPCドメインしかサポートしません。各VDCで1～4096の番号を使用してvPCに番号を付けることができます。

## 停電後のvPCリカバリ

データセンターが停止すると、vPCドメインの両方のvPCピアがリロードされます。場合によっては、1つのピアのみが復元される場合があります。機能するピアキープアライブまたはvPCピアリンクがないと、vPCは正常に機能することができません。vPCサービスが機能するピアのローカルポートのみを使用するようにする方法が利用可能です。

## 自動リカバリ

Cisco Nexus 9000 シリーズ デバイスは、そのピアがオンラインになるのに失敗した場合に、**auto-recovery** コマンドを使用して、vPC サービスを復元するように設定できます。この設定は、スタートアップ コンフィギュレーションに保存しなければなりません。リロード時に、vPC ピア リンクがダウンし、3 回連続してピア キープアライブ メッセージが失われた場合、セカンダリ デバイスはプライマリ STP ロールとプライマリ LACP ロールを引き継ぎます。ソフトウェアがvPCを初期化し、そのローカルポートを稼働させ始めます。ピアがないため、ローカルvPCポートの一貫性チェックはバイパスされます。デバイスは、自身をそのロールプライオリティに関係なくSTPプライマリに選出し、LACPポートロールのプライマリデバイスとしても機能します。

## 自動回復リロード遅延

vPCピアの自動回復は、**auto-recovery reload-delay** コマンドを使用して遅延させることができます。自動回復リロード遅延時間は、最初にアップしたピアで使用されます。**reload-delay time** コマンドは、両方のピアが回復するのを待機し、既存のロールを保持してから自動回復を開始するために使用します。デバイスは、回復したスイッチに対してプライマリロールを再開します。

## リカバリ後のvPCピアロール

ピアデバイスのリロードが完了し、隣接が形成されたら、次のプロセスが発生します。

1. 最初のvPCピアがその現在のロールを維持して、その他のプロトコルへの任意の移行リセットを回避します。ピアが、他の可能なロールを受け入れます。
2. 隣接が形成されたら、整合性検査が実行され、適切なアクションが取られます。

## 高可用性

In-Service Software Upgrade (ISSU) では、最初の vPC デバイス上のソフトウェア リロード プロセスが、vPC 通信チャンネルを介した CFS メッセージングを使用して、その vPC ピア デバイスをロックします。1 度に 1 つのデバイスだけアップグレードできます。最初のデバイスは、そのアップグレードが完了したら、そのピアデバイスのロックを解除します。次に、2 つ目のデバイスが、最初のデバイスが行ったのと同じように最初のデバイスをロックして、アップグレードプロセスを実行します。アップグレード中は、2 つの vPC デバイスが一時的に異なるリリースの Cisco NX-OS を実行することになりますが、その下位互換性サポートにより、システムは正常に機能します。



(注) ハイアベイラビリティ機能の詳細については、『[Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide](#)』を参照してください。

## vPC フォークリフト アップグレードシナリオ

次の手順では、vPC ドメイン内の Cisco Nexus 9500 スイッチのペアを、同じタイプのラインカードを使用する、Cisco Nexus 9500 スイッチの別のペアに移行するためのシナリオについて説明します。このような移行の一般的な例としては、より多くのインターフェイスが必要な場合に、Cisco Nexus 9504 スイッチから Cisco Nexus 9508 スイッチに移行するケースがあります。次の移行シナリオはサポートされていません。

- 異なるラインカードセットを使用する Cisco Nexus 9500 スイッチへの移行。例えば、N9K-X94xx ラインカードを搭載した Cisco Nexus 9500 スイッチから、N9K-X97xx ラインカードを搭載した Cisco Nexus 9500 スイッチへの移行です。
- 異なる世代の Cisco Nexus 9300 スイッチ間の移行。例えば、Cisco Nexus N9K-C9372PX から Cisco Nexus N9K-93180YC-EX スイッチへの移行です。
- vPC ドメインでの、異なる世代の Cisco Nexus 9000 スイッチの使用はサポートされていません

vPCフォークリフトアップグレードの考慮事項：

- vPCロール選択とスティッキビット

2つのvPCシステムを結合してvPCドメインを形成する場合、優先順位によって、どのデバイスがvPCプライマリで、どのデバイスがvPCセカンダリであるかが決まります。プライマリデバイスがリロードされると、システムがオンラインに戻り、vPCセカンダリデバイス（現在動作可能なプライマリ）への接続が復元されます。セカンダリデバイス（動作プライマリ）の動作ロールは変更されません（不要な中断を回避するため）。この動作は、スティッキ情報がスタートアップコンフィギュレーションに保存されないスティッキビットで実現されます。この方法では、稼働中のデバイスがリロードされたデバイスに勝ちます。したがって、vPCプライマリはvPCの動作セカンダリになります。スティッキビット

は、vPCノードがvPCピアリンクおよびピアキープアライブダウンで起動し、自動回復期間後にプライマリになるときにも設定されます。

- vPC の遅延復元

遅延復元タイマーは、ピア隣接が既に確立されている場合、リロードの後で復元済みのvPCピアデバイスで起動するvPCの遅延のために使用されます。

復元したvPCピアデバイス上のVLANインターフェイスが起動するのを遅延するには、**interfaces-vlan** オプションを **delay restore** のオプションコマンドを使用します。

- vPC 自動リカバリ

両方のvPCピアスイッチがダウンしたデータセンターの停電中に、1つのスイッチのみが復元された場合、自動回復機能により、そのスイッチがプライマリスイッチの役割を引き継ぎ、自動回復期間後にvPCリンクが起動します。デフォルトの自動回復期間は240秒です。

次の例は、vPCピアノードNode1とNode2をNew\_Node1とNew\_Node2に置き換える移行シナリオです。

	移行ステップ	予想される動作	Node1 Configured role (Ex : role priority 100)	Node1 動作のロール	Node2 Configured role (Ex : role priority 200)	Node2 動作のロール
1	初期状態です。	トラフィックはvPCピア (Node1とNode2) の両方によって転送されます。  Node1はプライマリで、Node2はセカンダリです。	プライマリ	プライマリ  ステイキービット : False	セカンダリ	セカンダリ  ステイキービット : False
2	Node2 の交換 – Node2 のすべてのvPCとアップリンクをシャットダウンします。vPCピアリンクおよびvPCピアキープアライブは、管理上のアップ状態です。	プライマリvPCピアNode1でトラフィックが収束しました。	プライマリ	プライマリ  ステイキービット : False	セカンダリ	セカンダリ  ステイキービット : False

	移行ステップ	予想される動作	Node1 Configured role (Ex : role priority 100)	Node1 動作のロール	Node2 Configured role (Ex : role priority 200)	Node2 動作のロール
3	Node2を削除します。	Node1は引き続きトラフィックを転送します。	プライマリ	プライマリ ステイックキービット : False	適用対象外	適用対象外
4	New_Node2を設定します。構成を管理アップ状態のvPCピアリンクおよびピアキーブアライブでスタートアップ構成にコピーします。 New_Node2の電源をオフにします。 すべての接続を確立します。 New_Node2の電源をオンにします。	New_Node2がセカンダリとして起動します。 Node1は引き続きプライマリです。 トラフィックはNode01で引き続き転送されます。	プライマリ	プライマリ ステイックキービット : False	セカンダリ	セカンダリ ステイックキービット : False
5	New_Node2のすべてのvPCとアップリンクポートを起動します。	トラフィックは、ノード1とNew_Node2の両方によって転送されます。	プライマリ	プライマリ ステイックキービット : False	セカンダリ	セカンダリ ステイックキービット : False
6	Node1の交換 : Node1でvPCとアップリンクをシャットダウンします。	トラフィックはNew_Node2に収束します。	プライマリ	プライマリ ステイックキービット : False	セカンダリ	セカンダリ ステイックキービット : False

	移行ステップ	予想される動作	Node1 Configured role (Ex : role priority 100)	Node1 動作のロール	Node2 Configured role (Ex : role priority 200)	Node2 動作のロール
7	Node1を削除します。	New_Node2がセカンダリになり、プライマリが動作し、スティッキービットがTrueに設定されます。	適用対象外	適用対象外	セカンダリ	プライマリ スティッキービット : True
8	New_Node1を設定します。スタートアップ実行をコピーします。  新しいNode1の電源をオフにします。すべての接続を確立します。New_Node1の電源をオンにします。	New_Node1がプライマリ、運用セカンダリとして起動します。	プライマリ	セカンダリ  スティッキービット : False	セカンダリ	プライマリ  スティッキービット : True
9	New_Node1のすべてのvPCとアップリンクポートを起動します。	トラフィックは、新しいノード1と新しいノード2の両方によって転送されます。	プライマリ	セカンダリ  スティッキービット : False	セカンダリ	プライマリ  スティッキービット : True



- (注) 設定済みのセカンダリノードを動作可能なセカンダリとして設定し、設定済みのプライマリを動作可能なプライマリとして使用する場合は、移行の最後にNode2をリロードできます。これオプションであり、機能上の影響はありません。

## 注意事項と制約事項

vPC 設定時のガイドラインと制限事項は次のとおりです。

- 2つの Cisco Nexus 9300 シリーズ スイッチ間で vPC ドメインを形成する場合、サポートされる vPC ドメインを形成するには、両方のスイッチがまったく同じモデルである必要があ

ります。2つの Cisco Nexus 9500 シリーズ スイッチ間で vPC ドメインを形成する場合、両方のスイッチは、サポートされる vPC ドメインを形成するために、シャーシの同じスロットに挿入された同じモデルのラインカード、ファブリック モジュール、スーパーバイザ モジュール、およびシステム コントローラで構成されている必要があります。

- ピアキープアライブ リンクを設定し、システムが vPC ピア リンクを確立する前に、ピア間の隣接関係を形成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。
- vPC に入れられるのは、レイヤ 2 ポート チャンネルだけです。
- vPC 内の LACP を使用するすべてのポート チャンネルを、アクティブモードのインターフェイスで設定することを推奨します。
- vPC ドメインに接続されているすべてのデバイスは、デュアルホームである必要があります。
- 必要な設定パラメータが、vPC ピア リンクの両側で互換性を保っているか確認する必要があります。互換性の推奨については、「vPC インターフェイスの互換パラメータ」の項を参照してください。
- 既存のポート チャンネルで vPC の設定中に、最小限のトラフィックの中断が発生する可能性があります。
- CFS リージョンはサポートされていません。
- vPC ピアリンクでは、デフォルトで MTU が 9216 に設定されています。
- STP ポート コストは、vPC 環境で 200 に固定されています。
- マルチレイヤ (バックツーバック) vPC を設定するには、それぞれの vPC に一意の vPC ドメイン ID を割り当てる必要があります。
- vPC がダウンし、トラフィックが vPC ピア リンクを通過する必要があるときに、増加するトラフィックに対応するためのベスト プラクティスは、vPC ピア リンクのラインカードを横断して複数の高帯域幅インターフェイス (Cisco Nexus 9000 スイッチの 40G インターフェイスなど) を使用することです。
- 次の場合、L3 リンクとバックツーバック vPC でマルチキャストストリームが重複する可能性があります。
  - SVI は、バックツーバック vPC の一部である 4 つすべてのスイッチで設定されます。
  - vPC の一部である 4 つのスイッチを接続する追加の L3 リンクがあります。
  - PIM は、すべての SVI およびスイッチ間の L3 リンクでイネーブルです。

ストリームの重複を防ぐには、vPC スイッチペアの 1 つから SVI または PIM 設定を削除します。

- Cisco NX-OS リリース 7.0(3)I5(1) 以降では、vPC を介したレイヤ 3 は、レイヤ 3 ユニキャスト通信の Cisco Nexus 9000 シリーズ スイッチでのみサポートされます。vPC 上のレイヤ 3 は、レイヤ 3 マルチキャストトラフィックではサポートされません。詳細については、「レイヤ 3 および vPC 設定のベストプラクティス」セクションを参照してください。
- デフォルトでは、レイヤ 3 vPC は、ピア vPC ノード宛てのすべてのパケット (TTL=1) を転送します。OSPF/BGP は、この転送が原因でフラップする可能性があります。スイッチハードウェアを前進させるには、ing-sup TCAM をサイズ 768 に切り分ける必要があります。TCAM カービング後にスイッチをリロードしてください。次に例を示します。

```
show hardware access-list tcam region | gr ing-sup
Ingress SUP [ing-sup] size = 768
```

- Cisco Nexus 9000 シリーズ スイッチは、vPC トポロジでの NAT をサポートしていません。
- vPC ピアは同じ Cisco NX-OS リリースを実行する必要があります。ソフトウェアアップグレード中は、最初にプライマリ vPC ピアをアップグレードする必要があります。
- 無停止アップグレードを実行する前に、vPC の両方のピアが同じモード (通常 ISSU モードまたは拡張 ISSU モード) であることを確認します。



(注) 拡張 ISSU モード (ブートモード lxc) が設定されたスイッチと非拡張 ISSU モードスイッチ間の vPC ピアリングはサポートされていません。

- **vpc orphan-ports suspend** コマンドは、vPC VLAN を持つインターフェイスで使用することを推奨します。コマンドは、非 vPC VLAN のポートおよびレイヤ 3 ポートにも適用可能です。
- このソフトウェアでは、vPC 上での BIDR PIM はサポートされていません。
- vPC 環境での DHCP スヌーピング、DAI、IPSG はサポートされていません。DHCP リレーはサポートされています。
- ポートチャネル上でのポートセキュリティは、サポートされていません。
- 2 つの Cisco Nexus 9000 シリーズ スイッチで **vpc domain** 構成モードでピアスイッチ機能を設定すると、vPC ピアリンクで有効になっていない VLAN のスパンニングツリールートも変更されます。両方のスイッチは、ブリッジアドレスとして 1 つの MAC アドレスを持つ 1 つのシステムとして機能します。これは、non-vPC mst-instance または VLAN でも true です。したがって、2 つのスイッチ間の非 vPC ピアリンクはバックアップリンクとしてブロックされます。これは予期された動作です。
- ダブルサイド vPC 上のすべてのノードで同じ Hot Standby Router Protocol (HSRP) /Virtual Router Redundancy Protocol (VRRP) グループを持つことは、Cisco NX-OS 7.0(3)I2(1) 以降のリリースでサポートされています。

- スパインノードのペアからCisco Nexus 9000デバイスのペアに移行する場合、Cisco Nexus 9000 vPCピアがアクティブ/スタンバイ状態になるようにHSRPプライオリティを設定する必要があります。HSRP状態のCisco Nexus 9000 vPCをアクティブ/リッスン状態またはスタンバイ/リッスン状態にすることはサポートされていません (7.(0)I2(2)以降)。
- NX-OS リリース 7.0(3)I2(2) 以降では、以前に **ip pim pre-build-spt** コマンドによって提供されていた動作がデフォルトで自動的に有効になっており、無効にはできません。
- Cisco NX-OS リリース NX-OS 7.0(3)I2(2) 以降では、個別の状態で作動作する vPC ポートチャネル メンバー リンクが、VLAN の不整合の検査時にフラップされます。サーバのプロビジョニング時にリンクがフラップされることを回避するには、**no graceful consistency-check** コマンドによって vPC グレースフル整合性検査を無効にします。
- vPC を使用する場合は、FHRP (HSRP、VRRP) にデフォルトのタイマーを使用し、PIM 設定を行うことを推奨します。アグレッシブタイマーをvPC設定で使用すると、コンバージェンス時間のメリットがありません。
- vPC 環境で **open shortest path first (OSPF)** を設定する場合は、コアスイッチ上でルータ コンフィギュレーション モードで次のタイマー コマンドを使用することにより、vPC ピア リンクがシャットダウンしたときに OSPF の高速コンバージェンスを実現します。

```
switch (config-router)# timers throttle spf 1 50 50
switch (config-router)# timers lsa-arrival 10
```

OSPF の詳細については、「Cisco Nexus 9000 シリーズ NX-OS ユニキャストルーティング 設定ガイド」を参照してください。

- VRRP/HSRP の BFD は、vPC 環境ではサポートされていません。
- Cisco Nexus 9000 リリース 7.0(3)I7(1) 以降では、vPC STP ヒットレス ロール変更機能がサポートされています。
- vPC ロール変更はいずれかのピア デバイスで実行できます。
- 元のセカンダリ デバイスに高プライオリティ値がある場合、元のプライオリティ デバイスはロール スワッピングは実行できません。vPC デバイスのいずれかでロール プライオリティを変更すると、元のセカンダリ デバイスの値は元のプライマリ デバイスの値よりも低くなります。デバイスの既存のロールを確認するには、ローカルおよびピアスイッチで **show vpc role** コマンドを使用します。
- vPC ドメインで vPC ヒットレス ロール変更機能を設定する前に、既存の設定済みロール プライオリティをチェックし、**peer-switch** コマンドを有効にします。これにより、両方の vPC ピアが同じ STP プライオリティになり、ロールの変更を発行する前にピアが稼働可能になることが保証されます。**peer-switch** コマンドを有効にできない場合、コンバージェンスの問題が発生する可能性があります。**show spanning-tree summary | grep peer** コマンドを使用して、ピア vPC スイッチが動作しているかどうかを確認します。
- Cisco NX-OS リリース 7.0(3)I5(2) 以降では、FEX-AA (デュアルホーム FEX) および FEX-ST (FEX ストレートスルー) トポロジ (FEX-AA および FEX-ST) がサポートされています。次の親スイッチの組み合わせはサポートされていません。

- Cisco Nexus 9300-EX および 9300 スイッチ。
  - Cisco Nexus 9300 および 9500 スイッチ。
  - Cisco Nexus 9300-EX および 9500 スイッチ。
- 第 1 世代の Broadcom ベースの Nexus 9300 シリーズ スイッチおよび Nexus 9500 シリーズ ライン カードは、vPC コンバージェンス TCAM リージョンが割り当てられている間に、出カインターフェイスが vPC ピア リンクである ip ネクスト ホップ ステートメントを設定しているポリシー ベースのルーティング ルート マップをサポートしていません。この制限は、This limitation does not apply to cloud scale based EX/FX/FX2 ラインカードを搭載した Nexus 9000 シリーズ デバイスや、9700-EX/FX ラインカードを搭載した Nexus 9500 プラットフォーム スイッチなど Nexus 9000 シリーズ デバイスに基づきクラウドスケールには適用されません。
- **show** コマンドで **internal** キーワードを指定することはサポートされていません
  - vPC を介したレイヤ 3 は、レイヤ 3 ユニキャスト通信の Cisco Nexus 9000 シリーズ スイッチでのみサポートされます。vPC 上のレイヤ 3 は、レイヤ 3 マルチキャストトラフィックではサポートされません。詳細については、「レイヤ 3 および vPC 設定のベストプラクティス」を参照してください。
  - vPC ピアの IP を宛先としたレイヤ 3 ピア ルータ および TTL=1 パケットのデフォルトの動作では、パケットを CPU にパントし、ソフトウェアを vPC ピア に転送します。これは、クラウドスケールベースの EOR スイッチに適用されます。
  - Cisco NX-OS リリース 7.0(3)I7(9) および Cisco NX-OS リリース 9.3(5)以降、クラウドスケールベースの TOR スイッチは、ハードウェア/データプレーンの vPC ピア宛での TTL=1 パケットを転送できます。機能のシームレスな動作のために、これらのリリースまたはそれ以降のリリースのいずれかを使用することを推奨します。
    - Cisco NX-OS リリース 9.3(4)にはこのデフォルトの動作がありますが、クラウドスケールベースの TOR スイッチに対する vPC ピアへのパケットのハードウェアリダイレクトには TCAM 再分割オプションを使用できます。これには、ing-sup リージョンに少なくとも 768 スペースを割り当てる必要があり、リロードが必要であり、操作上のオーバーヘッドがあります。
  - STP プライオリティの vPC ペアを設定する場合は、両方の vPC ピアを STP ルートとして機能させるために、両方の vPC ピア スイッチに同じプライオリティ レベルを設定する必要があります。
  - クラウドスケール ASIC ベースのスイッチでレイヤ 3 ピア ルータを設定すると、ユニキャストパケットで次の動作が発生することがあります。
    - vPC ピア ノード宛での TTL=0 のユニキャストパケットは、ピアに転送されます。
    - TTL=0 のユニキャストパケットはピアによってドロップされず、代わりに SUP にパントされます。

- VPC ピア ノード宛での TTL = 1 および TTL = 0 のユニキャスト パケットは、ソフトウェア転送およびハードウェア転送が可能です。そのため、ピア ノードで重複パケットが確認されます。
- vPC ポート チャネルの LACP 設定は、vPC ピア リンク上の両方の Cisco Nexus スイッチで一貫している必要があります。
- VPC の両方のピアが同じモード（通常モードまたは拡張モード）であることを確認してから、無停止アップグレードを実行してください。



(注) 拡張 ISSU モード（ブートモード lxc）が設定されたスイッチと非拡張 ISSU モードスイッチ間の vPC ピアリングはサポートされていません。

- キーワードが付いている **show** コマンドはサポートされていません。 **internal**
- Cisco Nexus 9000 シリーズスイッチは、vPC トポロジでの NAT をサポートしていません。
- Cisco NX-OS リリース 9.2(1) 以降の Cisco Nexus 9000 スイッチでは、**show vpc consistency-checker** コマンドは使用できません。
- Cisco NX-OS リリース 9.2(1) 以降の Cisco Nexus 9500-R プラットフォーム スイッチでは、**delay restore interface-bridge-domain** および **peer-gateway exclude-bridge-domain** コマンドは使用できません。
- vPC ピアは同じ Cisco NX-OS リリースを実行する必要があります。ソフトウェアのアップグレード中は、必ずプライマリ vPC ピアをアップグレードしてください。
- 1 つの vPC のすべてのポートが、同じ VDC 内になくてはなりません。
- vPC を設定するには、まず vPC をイネーブルにする必要があります。
- システムが vPC ピア リンクを形成する前に、ピア キープアライブリンクとメッセージを設定する必要があります。
- vPC に入れられるのは、レイヤ 2 ポート チャネルだけです。
- 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。
- マルチレイヤ（バックツーバック）vPC を設定するには、それぞれの vPC 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 リンクの両側で互換性を保っているかチェックしてください。互換性の推奨については、「vPC インターフェイスの互換パラメータ」の項を参照してください。
- vPC の設定中に、最小限のトラフィックの中断が発生する可能性があります。
- vPC 上での BIDR PIM はサポートされていません。

- CFS リージョンはサポートされていません。
- ポート チャネル上でのポート セキュリティは、サポートされていません。
- 2つの Cisco Nexus 9000 シリーズ スイッチで **vpc domain** 構成モードの下にある **peer-switch** 機能を設定すると、vPC ピアリンクで有効になっていない VLAN に対してもスパンニングツリー ルートが変更されます。両方のスイッチは、ブリッジアドレスとして1つの MAC アドレスを持つ1つのシステムとして機能します。これは、non-vPC mst-instance または VLAN でも true です。したがって、2つのスイッチ間の非 vPC ピア リンクはバックアップリンクとしてブロックされます。これは予期された動作です。
- vPC 内の LACP を使用するすべてのポートチャネルを、アクティブモードのインターフェイスで設定することを推奨します。
- バックツーバックのマルチレイヤ vPC トポロジでは、それぞれの vPC に一意のドメイン ID が必要です。
- ダブルサイド vPC 上のすべてのノードで同じ Hot Standby Router Protocol (HSRP) /Virtual Router Redundancy Protocol (VRRP) グループを持つことはサポートされています。
- スパイン ノードのペアから Cisco Nexus 9000 デバイスへ移行するとき、HSRP プライオリティが設定される必要があります。これにより Cisco Nexus 9000 vPC ピアはアクティブ/スタンバイ状態になります。HSRP 状態をアクティブ/リッスン状態、またはスタンバイ/リッスン状態にすることは Cisco Nexus 9000 vPC ピアでサポートされていません。
- vPC を使用する場合は、FHRP (HSRP、VRRP、) にデフォルトのタイマーを使用し、PIM 設定を行うことを推奨します。アグレッションタイマーを vPC 設定で使用すると、コンバージェンス時間のメリットがありません。
- vPC 環境で open shortest path first (OSPF) を設定する場合は、コア スイッチ上でルータ コンフィギュレーション モードで次のタイマー コマンドを使用することにより、vPC ピア リンクがシャットダウンしたときに OSPF の高速コンバージェンスを実現します。

```
switch (config-router)# timers throttle spf 1 50 50
switch (config-router)# timers lsa-arrival 10
```

OSPF に関する詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

- VRRP/HSRP の BFD は、vPC 環境ではサポートされていません。
- STP ポート コストは、vPC 環境で 200 に固定されています。
- ジャンボ フレームは、vPC ピア リンクではデフォルトで有効に設定されます。
- vPC がダウンし、トラフィックが vPC ピア リンクを通過する必要があるときに、増加するトラフィックに対応するためはのベスト プラクティス、vPC ピア リンクのラインカードを横断して複数の高帯域幅インターフェイス (Cisco Nexus 9000 の 40G インターフェイスなど) を使用することです。

- この項で説明している **vpc orphan-ports suspend** コマンドは、非 vPC VLAN のポートおよびレイヤ3ポートにも適用可能です。ただし、VPC VLAN のポートでを使用することをお勧めします。
- FEX-AA (デュアルホーム FEX) および FEX-ST (FEX ストレート) トポロジ (FEX-AA および FEX-ST) がサポートされています。次の混合は、親スイッチとしてサポートされていません。
  - Cisco Nexus 9300-EX および 9300 スイッチ
  - Cisco Nexus 9300 および 9500 スイッチ
  - Cisco Nexus 9300-EX および 9500 スイッチ

- 以前に `ip pim pre-build-spt` コマンドによって提供されていた動作がデフォルトで自動的に有効になっており、無効にはできません。
- 個別の状態で作動する vPC ポートチャネル メンバー リンクが、VLAN の不整合の検査時にフラップされます。サーバのプロビジョニング時にリンクがフラップされることを回避するには、**no graceful consistency-check** コマンドによって vPC グレースフル整合性検査を無効にします。

次の例では、VPC グレースフル整合性チェックを無効にします。

```
switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.

switch(config)# vpc domain 1
switch(config-vpc-domain)# no graceful consistency-check
```

- vPC STP ヒットレス ロール変更機能がサポートされています。
- vPC ロール変更はいずれかのピア デバイスで実行できます。
- 元のセカンダリ デバイスに高プライオリティ値がある場合、元のプライオリティ デバイスはロール スワッピングは実行できません。vPC デバイスのいずれかでロール プライオリティを変更すると、元のセカンダリ デバイスの値は元のプライマリ デバイスの値よりも低くなります。デバイスの既存のロールを確認するには、ローカルおよびピアスイッチで `show vpc role` コマンドを使用します。
- サポートされている vPC ドメインを形成するには、次の点に注意してください。
  - Cisco Nexus 9300 シリーズ スイッチの場合、両方のスイッチがまったく同じモデルである必要があります。
  - 2つの Cisco Nexus 9500 シリーズ スイッチ間で vPC ドメインを形成する場合、両方のスイッチは、サポートされる vPC ドメインを形成するために、シャーシの同じスロットに挿入された同じモデルのラインカード、ファブリック モジュール、スーパーバイザ モジュール、およびシステム コントローラで構成されている必要があります。
- vPC ヒットレス ロールの変更機能を設定する前に、必ず、既存の設定されたロール プライオリティをチェックしてください

- vPC ドメインで `peer-switch` コマンドを有効にします。これにより、両方の vPC ピアが同じ STP プライオリティになり、ロールの変更を発行する前にピアが稼働可能になることが保証されます。`peer-switch` コマンドを有効にできない場合、コンバージェンスの問題が発生する可能性があります。`show spanning-tree summary | grep peer` コマンドを使用して、ピア vPC スイッチが操作可能かどうか確認します。
- vPC ドメインに接続されているすべてのデバイスは、デュアルホームである必要があります。
- 第 1 世代の Broadcom ベースの Nexus 9300 シリーズ スイッチおよび Nexus 9500 シリーズ ライン カードは、vPC コンバージェンス TCAM リージョンが割り当てられている間に、出力インターフェイスが vPC ピア リンクである ip ネクスト ホップ ステートメントを設定しているポリシー ベースのルーティング ルート マップをサポートしていません。この制限は、`This limitation does not apply to cloud scale based EX/FX/FX2` ラインカードを搭載した Nexus 9000 シリーズ デバイスや、9700-EX/FX ラインカードを搭載した Nexus 9500 プラットフォーム スイッチなど Nexus 9000 シリーズ デバイスに基づきクラウドスケールには適用されません。
- `lacp suspend-individual` および `lacp mode delay` を実行して、PXE で vPC 経由で Cisco Nexus 9000 スイッチに接続しているサーバを起動する必要があります。

## レイヤ 3 および vPC 設定のベスト 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 設定の概要

レイヤ 3 デバイスが vPC を介して vPC ドメインに接続されている場合、次のビューがあります。

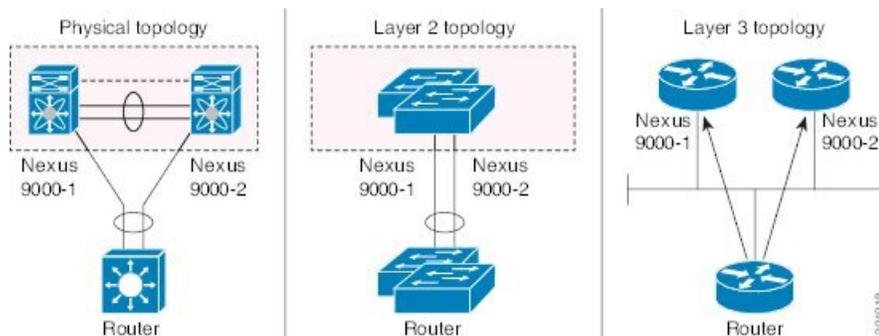
- レイヤ 2 では、レイヤ 3 デバイスは vPC ピア デバイスによって提供される一意のレイヤ 2 スイッチを認識します。
- レイヤ 3 では、レイヤ 3 デバイスは 2 台の異なるレイヤ 3 デバイス (vPC ピア デバイスごとに 1 台) を認識します。

vPC はレイヤ 2 仮想化テクノロジーであるため、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固有の論理デバイスとして表示されます。

レイヤ 3 には仮想化テクノロジーがないため、各 vPC ピア デバイスは、ネットワークの他の部分では別個のレイヤ 3 デバイスと見なされます。

次の図は、vPC を使用した 2 つの異なるレイヤ 2 およびレイヤ 3 ビューを示しています。

図 7: vPCピアデバイスのさまざまなビュー

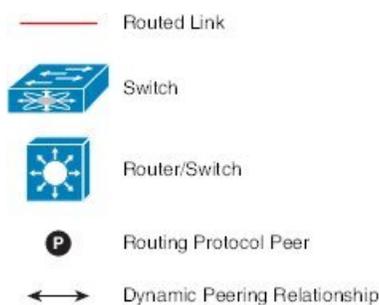


## レイヤ 3 および vPC のサポートされるトポロジ

ここでは、レイヤ 3 および vPC のネットワーク トポロジの例を示します。

レイヤ 3 と vPC のインタラクションには 2 つのアプローチがあります。1 つ目は、専用のレイヤ 3 リンクを使用してレイヤ 3 デバイスを各 vPC ピア デバイスに接続する方法です。2 つ目は、vPC 接続で伝送される専用 VLAN 上で、レイヤ 3 デバイスが各 vPC ピア デバイスで定義された SVI とピアリングできるようにすることです。次のセクションでは、次の図の凡例に記載されている要素を利用して、サポートされているすべてのトポロジについて説明します。

図 8: 凡例



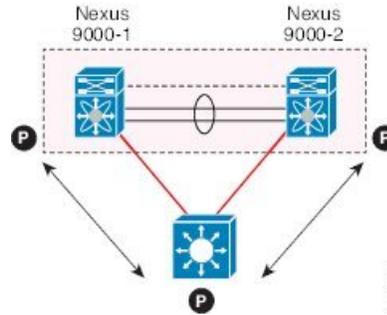
### レイヤ 3 リンクを使用した外部ルータとのピアリング

この例は、レイヤ 3 リンクを使用してレイヤ 3 デバイスを vPC ドメインの一部である Cisco Nexus 9000 スイッチに接続するトポロジを示しています。



(注) この方法で 2 つのエンティティを相互接続すると、レイヤ 3 ユニキャストおよびマルチキャスト通信をサポートできます。

図 9: レイヤ 3 リンクを使用した外部ルータとのピアリング



レイヤ 3 デバイスは、両方の vPC ピア デバイスとのレイヤ 3 ルーティング プロトコルの隣接関係を開始できます。

1 つまたは複数のレイヤ 3 リンクを、各 vPC ピア デバイスにレイヤ 3 デバイスを接続するために使用できます。Cisco Nexus 9000 シリーズ デバイスは、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 パスでレイヤ 3 Equal Cost Multipathing (ECMP) をサポートします。vPC ピア デバイスからレイヤ 3 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レイヤ 3 リンクにロードバランスできます。

レイヤ 3 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。レイヤ 3 デバイスから vPC ドメインへのトラフィックを、2 つのエンティティを相互接続するすべてのレイヤ 3 リンクにロードバランスできます。

レイヤ 3 デバイスをレイヤ 3 リンクを使用している vPC ドメインに接続する際は、次の注意事項に従ってください。

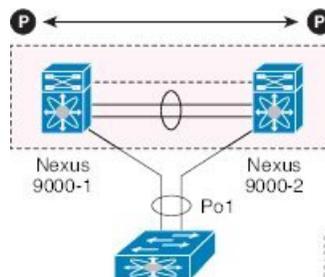
- レイヤ 3 デバイスを vPC ドメインに接続するには、独立したレイヤ 3 リンクを使用します。各リンクはポイントツーポイントレイヤ 3 接続を表し、小さな IP サブネット (/30 または /31) から取得された IP アドレスが割り当てられます。
- 複数の VRF にレイヤ 3 ピアリングが必要な場合は、それぞれが個別の VRF にマッピングされる複数のサブインターフェイスを定義することを推奨します。

## バックアップルーティングパス用 vPC デバイス間のピアリング

この例では、レイヤ 3 バックアップルーテッドパスを持つ 2 つの vPC ピア デバイス間のピアリングを示します。vPC ピア デバイス 1 または vPC ピア デバイス 2 のレイヤ 3 アップリンクに障害が発生した場合、2 つのピア デバイス間のパスを使用して、レイヤ 3 アップリンクがアップ状態のスイッチにトラフィックがリダイレクトされます。

レイヤ 3 バックアップルーティングパスは、vPC ピア リンク上で専用インターフェイス VLAN (SVI など) を使用するか、2 つの vPC ピア デバイス間で専用のレイヤ 2 またはレイヤ 3 リンクを使用して実装できます。

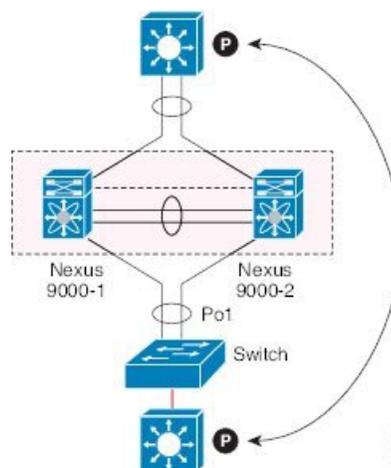
図 10: バックアップルーティングパス用 vPC デバイス間のピアリング



## ルータ間の直接レイヤ3 ピアリング

このシナリオでは、vPC ドメインの Nexus 9000 デバイスの部分が単にレイヤ2 中継パスとして使用され、接続されたルータがレイヤ3 ピアリングおよび通信を確立できるようにします。

図 11: ルータ間ピアリング



レイヤ3 デバイスは、次の2つの方法で相互のピアとなることが可能です。また、ピアリングの方法は、このロールにどのようなデバイスが展開されるかによっても変わります。

- 中間の Cisco Nexus 9000 vPC ピアスイッチを介してレイヤ3 デバイス間で拡張される VLAN の VLAN ネットワーク インターフェイス (SVI) を定義します。
- 各レイヤ3 デバイスでレイヤ3 ポートチャンネルインターフェイスを定義し、ポイントツーポイント レイヤ3 ピアリングを確立します。

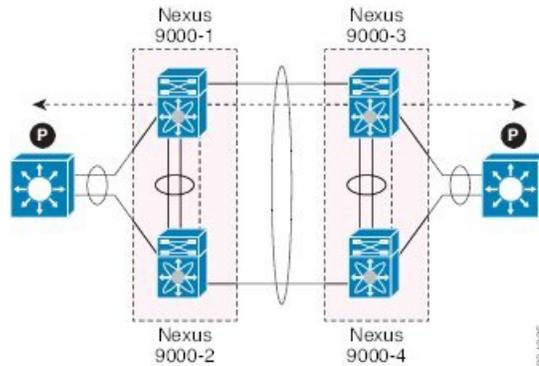


(注) 複数の VRF に対してレイヤ3 ピアリングを確立する必要がある展開の場合、最初の方法では、VRF ごとに VLAN (および SVI) のレイヤ3 デバイスで定義する必要があります。2 番目の方法では、VRF ごとにレイヤ3 ポートチャンネル サブインターフェイスを作成できます。

## トランジットスイッチとして vPC デバイスを使用した 2 ルータの間のピアリング

この例は、「ルータ間のピアリング」トポロジと似ています。この場合も、同じ vPC ドメインの一部である Cisco Nexus 9000 デバイスは、レイヤ 2 中継パスとしてのみ使用されます。ここでの違いは、Cisco Nexus 9000 スイッチのペアが 2 つあることです。vPC 接続を使用してレイヤ 3 デバイスに接続されている各スイッチは、それらの間のバックツーバック vPC 接続も確立します。異なる点は、vPC ドメインがレイヤ 2 中継パスとしてのみ使用されていることです。

図 12: トランジットスイッチとして vPC デバイスを使用した 2 ルータの間のピアリング



このトポロジは、直接リンク（ダークファイバまたはDWDM回線）で相互接続された個別のデータセンター間の接続を確立する場合によく使用されます。この場合、Cisco Nexus 9000 スイッチの 2 つのペアはレイヤ 2 拡張サービスのみを提供し、レイヤ 3 デバイスがレイヤ 3 で相互にピアリングできるようにします。

## パラレル相互接続ルーテッドポート上の外部ルーターとのピアリング

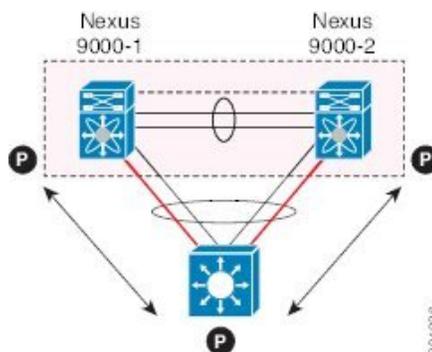
次の図に示すように、ルーテッドトラフィックとブリッジトラフィックの両方が必要な場合は、ルーテッドトラフィックに個別のレイヤ 3 リンクを使用し、ブリッジトラフィックに個別のレイヤ 2 ポートチャンネルを使用します。

レイヤ 2 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。

レイヤ 3 リンクは、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。

このトポロジの目的は、レイヤ 3 デバイスを通る特定のトラフィックを引き付けることです。レイヤ 3 リンクは、レイヤ 3 デバイスから vPC ドメインにルーティングされたトラフィックを伝送するためにも使用されます。

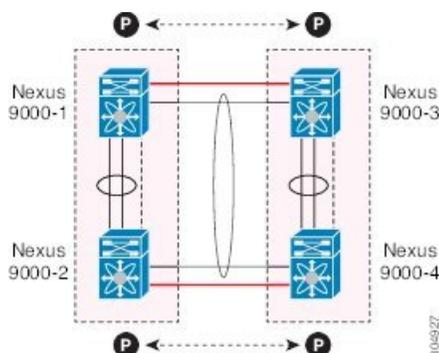
図 13: パラレル相互接続ルーテッドポート上の 外部ルーターとのピアリング



## パラレル相互接続ルーテッドポート上の vPC スイッチペア間のピアリング

前の項（中継スイッチとして vPC デバイスを使用した 2 台のルータ間のピアリング）で示したものに代わる設計では、レイヤ 2 とレイヤ 3 の両方の拡張サービスを提供するために、各データセンターに導入された 2 ペアの Cisco Nexus 9000 スイッチを使用します。ルーティングプロトコルピアリング隣接を 2 ペアの Cisco Nexus 9000 デバイス間で確立する必要がある場合、ベストプラクティスは、次の例に示すように 2 サイト間に専用のレイヤ 3 リンクを追加することです。

図 14: パラレル相互接続ルーテッドポートでの vPC 相互接続を介したピアリング



2 つのデータセンター間のバックツーバック vPC 接続は、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、専用レイヤ 3 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。

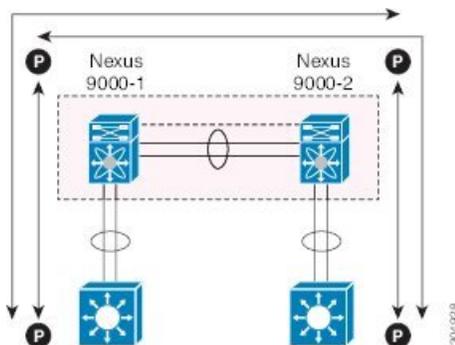
## 非 vPC VLAN を使用する PC 相互接続および専用スイッチ間リンクを介したピアリング

この例は、レイヤ 3 デバイスが vPC ドメインにシングル接続されている場合に、専用スイッチ間リンクで非 vPC VLAN を使用して、レイヤ 3 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できることを示しています。ただし、非 vPC VLAN は、vPC VLAN とは異なるスタティック MAC を使用するように設定する必要があります。



- (注) この目的のために vPC VLAN (および vPC ピア リンク) を設定することはサポートされていません。

図 15: 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



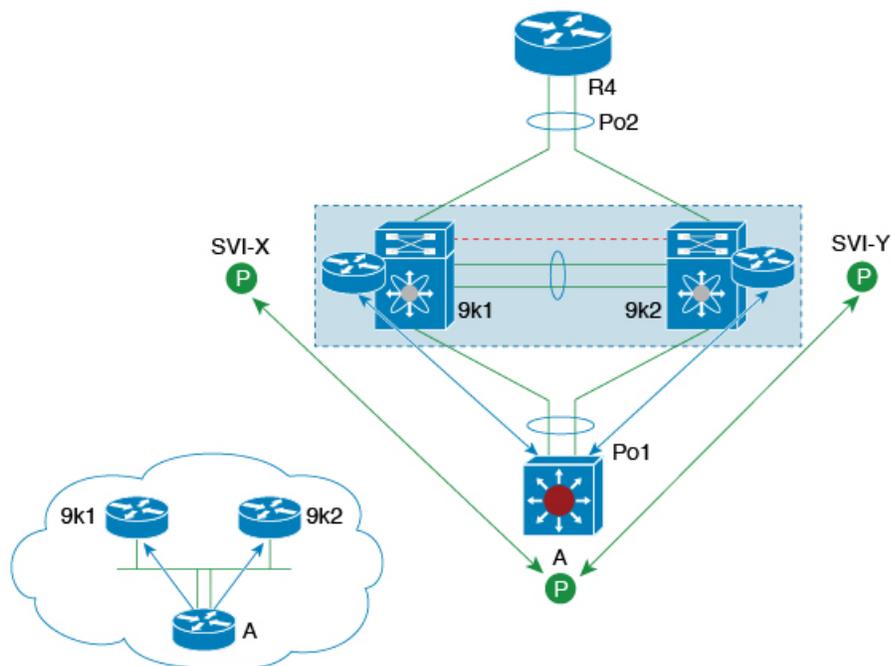
## vPC 接続を介した直接ピアリング

Cisco NX-OS リリース 7.0(3)I5(1) 以降では、レイヤ 3 ルータと Cisco Nexus 9000 vPC スイッチのペア間にレイヤ 3 ピアリングを確立するための代替方法が導入されています。



- (注) vPC 接続を介した直接ピアリングは、レイヤ 3 ユニキャスト通信でのみサポートされ、レイヤ 3 マルチキャストトラフィックではサポートされません。レイヤ 3 マルチキャストが必要な場合は、専用のレイヤ 3 リンクでピアリングを確立する必要があります。

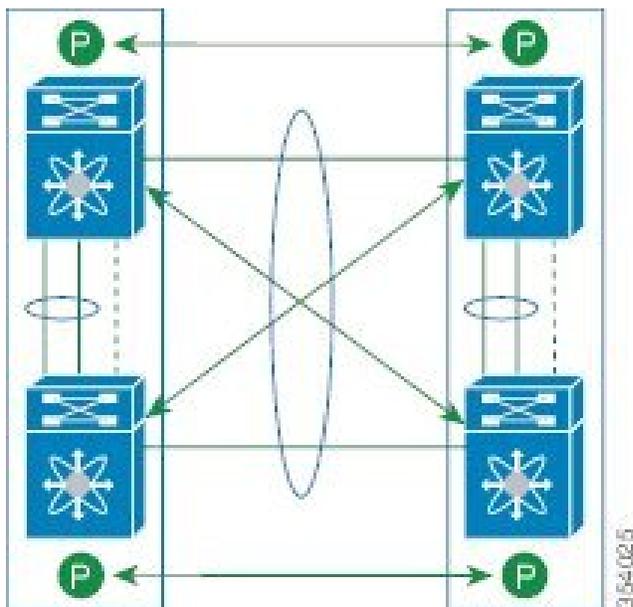
図 16: サポート : ルータが両方の vPC ピアとピアリングする vPC 相互接続を介するピアリング。



このシナリオでは、同じ vPC ドメインの一部である外部ルータと Cisco Nexus 9000 スイッチ間のレイヤ 3 ピアリングは、vPC 接続で伝送される VLAN 上で直接確立されます。この場合の外部ルータは、各 vPC デバイスで定義された SVI インターフェイスとピアリングします。前の図 12 のシナリオでは、外部ルータは SVI またはレイヤ 3 ポートチャネルを使用して vPC デバイスとピアリングできます（複数の SVI またはポートチャネルサブインターフェイスをマルチ VRF 展開に使用できます）。

この展開モデルでは、vPC ドメインの一部として **layer3 peer-router** コマンドを設定する必要があります。vPC スイッチの 2 つの個別のペア間で確立された vPC バックツーバック接続でレイヤ 2 およびレイヤ 3 接続を確立するために、同じアプローチを採用できます。

図 17: サポート : 各 Nexus デバイスが 2つの vPC ピアとピアリングする vPC 相互接続を介したピアリング。



この展開モデルでは、4つの Cisco Nexus 9000 スイッチすべてに同じ VLAN 内の SVI インターフェイスが設定され、これらの中でルーティングピアリングと接続が確立されます。

## レイヤ 3 vPC 経路の設定

### 始める前に

ピア ゲートウェイ機能が両方のピアで有効かつ設定済みで、両方のピアが vPC 経路のレイヤ 3 に対応したイメージを実行していることを確認します。ピアゲートウェイ機能を有効にせずに **layer3 peer-router** コマンドを入力した場合は、ピアゲートウェイ機能を有効にするように勧める syslog メッセージが表示されます。

vPC ピアリンクがアップしていることを確認します。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **vpc domain domain-id**
3. switch(config-vpc-domain)#**layer3 peer-router**
4. switch(config-vpc-domain)# **exit**
5. (任意) switch# **show vpc brief**
6. (任意) switch# **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b> 例： switch# <b>configure terminal</b> switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>vpc domain domain-id</b> 例： switch(config)# <b>vpc domain 5</b> switch(config-vpc-domain)#	vPC ドメインがまだ存在しなかった場合はそれを作成し、vpc-domain コンフィギュレーションモードを開始します。デフォルトはありません。指定できる範囲は <1 ~ 1000> です。
ステップ 3	switch(config-vpc-domain)# <b>layer3 peer-router</b>	両方のピアとのピアリング隣接関係を形成するためレイヤ 3 デバイスを有効にします。  (注) 両方のピアでこのコマンドを設定します。このコマンドをピアのうち1つでのみ設定するか、1つのピアで無効にすると、レイヤ3 ピアルータの動作状態が無効になります。動作状態に変更があると、通知が表示されます。
ステップ 4	switch(config-vpc-domain)# <b>exit</b>	vpc-domain コンフィギュレーションモードを終了します。
ステップ 5	(任意) switch# <b>show vpc brief</b>	各 vPC ドメインに関する要約情報を表示します。
ステップ 6	(任意) switch# <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## 例

次に、vPC 機能経由でレイヤ 3 を設定する例を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# layer3 peer-router

switch(config-vpc-domain)# exit

switch(config)#
```

次に、vPC 経由でレイヤ 3 機能が設定されているかどうかを確認する例を示します。  
動作レイヤ 3 ピアは、vPC 経由のレイヤ 3 の動作状態の設定に応じて有効または無効になります。

```
switch# show vpc brief

vPC domain id : 5
```

```

Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
Configuration consistency status : success
Per-vlan consistency status : failed
Type-2 consistency status : success
vPC role : secondary
Number of vPCs configured : 2
Peer Gateway : Enabled
Peer gateway excluded VLANs : -
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Enabled (timeout = 240 seconds)
Operational Layer3 Peer : Enabled

```

## デフォルト設定

次の表は、vPC パラメータのデフォルト設定をまとめたものです。

表 1: デフォルト vPC パラメータ

パラメータ	デフォルト
vPC システム プライオリティ	32667
vPC ピアキープアライブ メッセージ	ディセーブル
vPC ピアキープアライブ間隔	1 秒
vPC ピアキープアライブ タイムアウト	5 秒
vPC ピアキープアライブ UDP ポート	3200

## vPC の設定



- (注) vPC ピアリンクの両側のデバイス両方でこれらの手順を使用する必要があります。両方の vPC ピア デバイスをこの手順で設定します。

ここでは、コマンドラインインターフェイス (CLI) を使用して vPC を設定する方法を説明します。



- (注) Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合がありますので注意してください。

## vPC のイネーブル化

vPC を設定して使用する場合は、事前に vPC 機能をイネーブルにしておく必要があります。

### 手順の概要

1. **configure terminal**
2. **feature vpc**
3. **exit**
4. **show feature**
5. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b> switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>feature vpc</b> 例： switch(config)# <b>feature vpc</b>	デバイス上で vPC をイネーブルにします。
ステップ 3	<b>exit</b> 例： switch(config)# <b>exit</b> switch#	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。
ステップ 4	<b>show feature</b> 例： switch# <b>show feature</b>	(任意) デバイス上でイネーブルになっている機能を表示します。
ステップ 5	<b>copy running-config startup-config</b> 例： switch# <b>copy running-config startup-config</b>	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

### 例

次の例は、vPC 機能をイネーブルにする方法を示します。

```
switch# configure terminal
switch(config)# feature vpc
switch(config)# exit
switch(config)#
```

## vPC のディセーブル化



(注) vPC 機能をディセーブルにすると、デバイス上のすべての vPC 設定がクリアされます。

### 手順の概要

1. **configure terminal**
2. **no feature vpc**
3. **exit**
4. **show feature**
5. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b> switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>no feature vpc</b> 例： switch(config)# <b>no feature vpc</b>	デバイスの vPC をディセーブルにします。
ステップ 3	<b>exit</b> 例： switch(config)# <b>exit</b> switch#	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。
ステップ 4	<b>show feature</b> 例： switch# <b>show feature</b>	(任意) デバイス上でイネーブルになっている機能を表示します。
ステップ 5	<b>copy running-config startup-config</b> 例： switch# <b>copy running-config startup-config</b>	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

### 例

次の例は、vPC 機能をディセーブルにする方法を示します。

```
switch# configure terminal
switch(config)# no feature vpc
```

```
switch(config)# exit
switch#
```

## vPC ドメインの作成と vpc-domain モードの開始

vPC ドメインを作成し、両方の vPC ピア デバイス上で vPC ピア リンク ポート チャネルを同じ vPC ドメイン内に置くことができます。1 つの VDC 全体を通じて一意の vPC ドメイン番号を使用するこのドメイン ID は、vPC システム MAC アドレスを自動的に形成するのに使用されます。

このコマンドを使用して、vpc-domain コマンドモードを開始することもできます。

### 手順の概要

1. **configure terminal**
2. **vpc domain *domain-id* [shut | no shut]**
3. **exit**
4. **show vpc brief**
5. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b> switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>vpc domain <i>domain-id</i> [shut   no shut]</b> 例： switch(config)# <b>vpc domain 5</b> switch(config-vpc-domain)#	デバイス上に vPC ドメインを作成し、設定目的で vpc-domain コンフィギュレーションモードを開始します。デフォルトはありません。指定できる範囲は 1 ~ 1000 です。
ステップ 3	<b>exit</b> 例： switch(config)# <b>exit</b> switch#	vpc-domain 設定モードを終了します。
ステップ 4	<b>show vpc brief</b> 例： switch# <b>show vpc brief</b>	(任意) 各 vPC ドメインに関する簡単な情報を表示します。
ステップ 5	<b>copy running-config startup-config</b> 例： switch# <b>copy running-config startup-config</b>	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

## 例

次に、vpc-domain コマンドモードを開始して、既存の vPC ドメインを設定する例を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# exit
switch(config)#
```

# vPC キープアライブリンクと vPC キープアライブメッセージの設定

キープアライブメッセージを伝送するピアキープアライブリンクの宛先 IP を設定できます。必要に応じて、キープアライブメッセージのその他のパラメータも設定できます。



- (注) システムで vPC ピアリンクを形成できるようにするには、まず vPC ピアキープアライブリンクを設定する必要があります。



- (注) vPC ピアキープアライブリンクを使用する際は、個別の VRF インスタンスを設定して、各 vPC ピアデバイスからその VRF にレイヤ 3 ポートを接続することを推奨します。ピアリンク自体を使用して vPC ピアキープアライブメッセージを送信しないでください。VRF の作成および設定方法については、『[Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide](#)』を参照してください。ピアキープアライブメッセージに使用される送信元と宛先の両方の IP アドレスがネットワーク内で一意であることを確認してください。管理ポートと管理 VRF が、これらのキープアライブメッセージのデフォルトです。

## 始める前に

vPC 機能が有効なことを確認します。

## 手順の概要

1. **configure terminal**
2. **vpc domain domain-id [shut | no shut]**
3. **peer-keepalive destination ipaddress [hold-timeout secs | interval msec {timeout secs} | precedence {prec-value | network | internet | critical | flash-override | flash | immediate priority | routine}] | tos {tos-value | max-reliability | max-throughput | min-delay | min-monetary-cost | normal} | tos-byte tos-byte-value | source ipaddress | vrf {name | management vpc-keepalive}]**
4. **exit**
5. **show vpc statistics**
6. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>vpc domain domain-id [shut   no shut]</b> 例 : <pre>switch(config)# vpc domain 5 switch(config-vpc-domain)#</pre>	デバイスで vPC ドメインを作成し、vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	<b>peer-keepalive destination ipaddress [hold-timeout secs   interval msec {timeout secs}   {precedence {prec-value}   network   internet   critical   flash-override   flash   immediate priority   routine}]   tos {tos-value}   max-reliability   max-throughput   min-delay   min-monetary-cost   normal}]   tos-byte tos-byte-value}   source ipaddress   vrf {name   management vpc-keepalive}]</b> 例 : <pre>switch(config-vpc-domain)# peer-keepalive destination 172.28.230.85 switch(config-vpc-domain)#</pre>	vPC ピアキープアライブリンクのリモートエンドの IPv4 および IPv6 アドレスを設定します。 (注) vPC ピアキープアライブリンクを設定するまで、vPC ピアリンクは構成されません。 (注) vPC ピアキープアライブリンクのリモートエンドに IPv6 アドレスを設定するときに送信元 IP アドレスを指定しないと、次のエラーメッセージが表示されることがあります。 <pre>Cannot configure IPV6 peer-keepalive without source IPV6 address</pre> 管理ポートと VRF がデフォルトです。 (注) 独立した VRF を設定し、vPC ピアキープアライブリンクのための VRF 内の各 vPC ピア デバイスからのレイヤ 3 ポートを使用することを推奨します。VRF の作成および設定の詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。
ステップ 4	<b>exit</b> 例 : <pre>switch(config)# exit switch#</pre>	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。
ステップ 5	<b>show vpc statistics</b> 例 : <pre>switch# show vpc statistics</pre>	(任意) キープアライブメッセージの設定に関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 6	<b>copy running-config startup-config</b> 例 : switch# <b>copy running-config startup-config</b>	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

### 例

VRF の設定方法については、『[Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide](#)』を参照してください。

次の例は、vPC ピアキーブアライブ リンクの宛先と送信元の IP アドレスおよび VRF を設定する方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 100
switch(config-vpc-domain)# peer-keepalive destination 172.168.1.2 source 172.168.1.1 vrf vpc-keepalive
switch(config-vpc-domain)# exit
switch#
```

## vPC ピア リンクの作成

指定した vPC ドメインの vPC ピア リンクとして設定するポートチャネルを各デバイス上で指定して、vPC ピア リンクを作成します。冗長性を確保するため、トランク モードで vPC ピア リンクとして指定したレイヤ 2 ポートチャネルを設定し、各 vPC ピア デバイス上の個別のモジュールで 2 つのポートを使用することを推奨します。

### 始める前に

vPC 機能が有効なことを確認します。

### 手順の概要

1. **configure terminal**
2. **interface port-channel *channel-number***
3. **switchport mode trunk**
4. **switchport trunk allowed vlan *vlan-list***
5. **vpc peer-link**
6. **exit**
7. **show vpc brief**
8. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b> switch(config)#	グローバル コンフィギュレーション モードを開始します
ステップ 2	<b>interface port-channel channel-number</b> 例： switch(config)# <b>interface port-channel 20</b> switch(config-if)#	このデバイスの vPC ピア リンクとして使用するポート チャンネルを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>switchport mode trunk</b> 例： switch(config-if)# <b>switchport mode trunk</b>	(任意) このインターフェイスをトランク モードで設定します。
ステップ 4	<b>switchport trunk allowed vlan vlan-list</b> 例： switch(config-if)# <b>switchport trunk allowed vlan 1-120,201-3967</b>	(任意) 許容 VLAN リストを設定します。
ステップ 5	<b>vpc peer-link</b> 例： switch(config-if)# <b>vpc peer-link</b> switch(config-vpc-domain)#	選択したポート チャンネルを vPC ピア リンクとして設定し、vpc-domain コンフィギュレーション モードを開始します。
ステップ 6	<b>exit</b> 例： switch(config)# <b>exit</b> switch#	vpc-domain 設定モードを終了します。
ステップ 7	<b>show vpc brief</b> 例： switch# <b>show vpc brief</b>	(任意) 各 vPC に関する情報を表示します。vPC ピア リンクに関する情報も表示されます。
ステップ 8	<b>copy running-config startup-config</b> 例： switch# <b>copy running-config startup-config</b>	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

## 例

次の例は、vPC ピア リンクを設定する方法を示しています。

```
switch# configure terminal
switch(config)# interface port-channel 20
switch(config-if)# switchport mode
```

```
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1-120,201-3967
switch(config-if)# vpc peer-link
switch(config-vpc-domain)# exit
switch(config)#
```

## 他のポートチャネルの vPC への移行

冗長性を確保するために、vPC ドメイン ダウンストリーム ポートチャネルを 2 つのデバイスに接続することを推奨します。

ダウンストリーム デバイスに接続するには、ダウンストリーム デバイスからプライマリ vPC ピア デバイスへのポートチャネルを作成し、ダウンストリーム デバイスからセカンダリ ピア デバイスへのもう 1 つのポートチャネルを作成します。各 vPC ピア デバイス上で、ダウンストリーム デバイスに接続するポートチャネルに vPC 番号を割り当てます。vPC の作成時にトラフィックが中断されることはほとんどありません。

### 始める前に

vPC 機能が有効なことを確認します。

レイヤ 2 ポートチャネルを使用していることを確認します。

### 手順の概要

1. **configure terminal**
2. **interface port-channel *channel-number***
3. **vpc *number***
4. **exit**
5. **show vpc brief**
6. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b> switch(config)#	グローバル コンフィギュレーション モードを開始します
ステップ 2	<b>interface port-channel <i>channel-number</i></b> 例： switch(config)# <b>interface port-channel 20</b> switch(config-if)#	ダウンストリーム デバイスに接続するために vPC に入れるポートチャネルを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>vpc <i>number</i></b> 例：	選択したポートチャネルを vPC に入れてダウンストリーム デバイスに接続するように設定します。こ

	コマンドまたはアクション	目的
	<pre>switch(config-if)# vpc 5 switch(config-vpc-domain)#</pre>	<p>これらのポートチャネルには、デバイス内の任意のモジュールを使用できます。範囲は、1～4096です。</p> <p>(注) vPC ピア デバイスからダウンストリームデバイスに接続されているポートチャネルに割り当てる vPC 番号は、両方の vPC デバイスで同じでなければなりません。</p>
ステップ 4	<p><b>exit</b></p> <p>例 :</p> <pre>switch(config)# exit switch#</pre>	vpc-domain 設定モードを終了します。
ステップ 5	<p><b>show vpc brief</b></p> <p>例 :</p> <pre>switch# show vpc brief</pre>	(任意) vPC に関する情報を表示します。
ステップ 6	<p><b>copy running-config startup-config</b></p> <p>例 :</p> <pre>switch# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

### 例

次に、ダウンストリーム デバイスに接続するポートチャネルを設定する例を示します。

```
switch# configure terminal
switch(config)# interface port-channel 20
switch(config-if)# vpc 5
switch(config-if)# exit
switch(config)#
```

## vPC ピア リンクの構成の互換性チェック

両方の vPC ピア デバイス上の vPC ピア リンクを設定した後に、すべての vPC インターフェイスで設定が一貫していることをチェックします。vPC での一貫した設定については、「vPC インターフェイスの互換パラメータ」の項を参照してください。

### 手順の概要

1. **configure terminal**
2. **show vpc consistency-parameters {global | interface port-channel channel-number}**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>show vpc consistency-parameters {global   interface port-channel channel-number}</b> 例 : <pre>switch(config)# show vpc consistency-parameters global switch(config)#</pre>	(任意) すべての vPC インターフェイス全体で一貫している必要があるパラメータのステータスを表示します。

## 例

次の例は、すべての vPC インターフェイスの間で必須設定の互換性が保たれているかチェックする方法を示します。

```
switch# configure terminal
switch(config)# show vpc consistency-parameters global
switch(config)#
```



(注) vPC インターフェイス設定の互換性に関するメッセージが syslog にも記録されます。

## グレースフル整合性検査の設定

デフォルトでイネーブルになるグレースフル整合性検査機能を設定できます。この機能がイネーブルでない場合、必須互換性パラメータの不一致が動作中の vPC で導入されると、vPC は完全に一時停止します。この機能がイネーブルの場合、セカンダリ ピア デバイスのリンクだけが一時停止します。vPC での一貫した設定については、「vPC インターフェイスの互換パラメータ」の項を参照してください。

## 手順の概要

1. **configure terminal**
2. **vpc domain domain-id [shut | no shut]**
3. **graceful consistency-check**
4. **exit**
5. **show vpc brief**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b> switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>vpc domain domain-id [shut   no shut]</b> 例： switch(config-if)# <b>vpc domain 5</b> switch(config-vpc-domain)#	vPC ドメインがまだ存在していない場合はそれを作成し、vpc-domain コンフィギュレーションモードを開始します。
ステップ 3	<b>graceful consistency-check</b> 例： switch(config-vpc-domain)# <b>graceful consistency-check</b>	必須互換性パラメータで不一致が検出された場合に、セカンダリ ピア デバイスのリンクのみが一時停止するということを指定します。  この機能を無効にするには、このコマンドの <b>no</b> 形式を使用します。
ステップ 4	<b>exit</b> 例： switch(config)# <b>exit</b> switch#	vpc-domain 設定モードを終了します。
ステップ 5	<b>show vpc brief</b> 例： switch# <b>show vpc brief</b>	(任意) vPC に関する情報を表示します。

## 例

次に、グレースフル整合性検査機能をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# graceful consistency-check
switch(config-vpc-domain)# exit
switch(config)#
```

## vPC ピアゲートウェイの設定

vPC ピア デバイスを、vPC ピア デバイスの MAC アドレスに送信されるパケットに対してゲートウェイとして機能するように設定できます。

## 始める前に

vPC 機能が有効なことを確認します。

## 手順の概要

1. **configure terminal**
2. **vpc domain *domain-id* [shut | no shut]**
3. **peer-gateway**
4. **exit**
5. **show vpc brief**
6. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>vpc domain <i>domain-id</i> [shut   no shut]</b> 例 : <pre>switch(config-if)# vpc domain 5 switch(config-vpc-domain)#</pre>	vPC ドメインがまだ存在していない場合はそれを作成し、vpc-domain コンフィギュレーションモードを開始します。
ステップ 3	<b>peer-gateway</b> 例 : <pre>switch(config-vpc-domain)# peer-gateway</pre> (注) この機能を正常に動作させるために、このvPCドメインのすべてのインターフェイス VLAN 上で IP リダイレクトをディセーブルにします。	ピアのゲートウェイ MAC アドレスを宛先とするパケットのレイヤ3 フォワーディングをイネーブルにします。
ステップ 4	<b>exit</b> 例 : <pre>switch(config)# exit switch#</pre>	vpc-domain 設定モードを終了します。
ステップ 5	<b>show vpc brief</b> 例 : <pre>switch# show vpc brief</pre>	(任意) 各 vPC に関する情報を表示します。vPC ピアリンクに関する情報も表示されます。
ステップ 6	<b>copy running-config startup-config</b> 例 : <pre>switch# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

## vPC ピアスイッチの設定

Cisco Nexus 9000 シリーズ デバイスは、一対の vPC デバイスがレイヤ 2 トポロジ内で 1 つの STP ルートとして現れるように設定することができます。

### 純粋な vPC ピアスイッチ トポロジの設定

純粋な vPC ピアスイッチ トポロジを設定するには、`peer-switch` コマンドを使用し、次に可能な範囲内で最高の（最も小さい）スパンニングツリーブリッジプライオリティ値を設定します。

始める前に

vPC 機能が有効なことを確認します。



(注) VPC ピア間の非 VPC 専用トランクリンクを使用する場合は、STP が VLAN をブロックするのを防ぐために、非 VPC VLAN はピアによって異なるグローバルプライオリティが必要です。

#### 手順の概要

1. `configure terminal`
2. `vpc domain domain-id [shut | no shut]`
3. `peer-switch`
4. `spanning-tree vlan vlan-range priority value`
5. `exit`
6. `show spanning-tree summary`
7. `copy running-config startup-config`

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： <code>switch# configure terminal</code> <code>switch(config)#</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>vpc domain domain-id [shut   no shut]</b> 例： <code>switch(config)# vpc domain 5</code> <code>switch(config-vpc-domain)#</code>	設定する vPC ドメインの番号を入力し、vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	<b>peer-switch</b> 例： <code>switch(config-vpc-domain)# peer-switch</code>	vPC スイッチ ペアがレイヤ 2 トポロジ内で 1 つの STP ルートとして現れるようにします。  ピア スイッチ vPC トポロジをディセーブルにするには、このコマンドの <b>no</b> 形式を使用します。

	コマンドまたはアクション	目的
ステップ 4	<b>spanning-tree vlan <i>vlan-range</i> priority <i>value</i></b> 例： switch(config)# <b>spanning-tree vlan 1 priority 8192</b>	VLAN のブリッジプライオリティを設定します。有効な値は、4096 の倍数です。デフォルト値は 32768 です。
ステップ 5	<b>exit</b> 例： switch(config-vpc-domain)# <b>exit</b> switch#	vpc-domain 設定モードを終了します。
ステップ 6	<b>show spanning-tree summary</b> 例： switch# <b>show spanning-tree summary</b>	(任意) スパニングツリーポートの状態の概要を表示します。これに、vPC ピア スイッチも含まれます。
ステップ 7	<b>copy running-config startup-config</b> 例： switch# <b>copy running-config startup-config</b>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

### 例

次の例は、純粋な vPC ピア スイッチ トポロジを設定する方法を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vpc domain 5
switch(config-vpc-domain)# peer-switch

2010 Apr 28 14:44:44 switch %STP-2-VPC_PEERSWITCH_CONFIG_ENABLED: vPC peer-switch
configuration is enabled. Please make sure to configure spanning tree "bridge" priority
as
per recommended guidelines to make vPC peer-switch operational.

switch(config-vpc-domain)# spanning-tree vlan 1 priority 8192
switch(config-vpc-domain)# exit
switch(config)#
```

## 孤立ポートの一時停止の設定

vPC 対応でないデバイスが各ピアに接続するとき、接続されたポートは vPC のメンバではないため、孤立ポートと称されます。vPC ピア リンクまたはピア キープアライブ障害に応じてセカンダリピアが vPC ポートを一時停止するときに、セカンダリピアによって一時停止 (シャットダウン) される孤立ポートとして物理インターフェイスを明示的に宣言できます。孤立ポートは vPC が復元されたときに復元されます。



(注) vPC 孤立ポートの一時停止は、物理ポート、ポート チャンネルでのみ設定できます。ただし、個々のポート チャンネル メンバー ポートで同じ設定はできません。

#### 始める前に

vPC 機能が有効なことを確認します。

#### 手順の概要

1. **configure terminal**
2. **show vpc orphan-ports**
3. **interface type slot/port**
4. **vpc orphan-port suspend**
5. **exit**
6. **copy running-config startup-config**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b> switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>show vpc orphan-ports</b> 例： switch# <b>show vpc orphan-ports</b>	(任意) 孤立ポートのリストを表示します。
ステップ 3	<b>interface type slot/port</b> 例： switch(config)# <b>interface ethernet 3/1</b> switch(config-if)#	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 4	<b>vpc orphan-port suspend</b> 例： switch(config-if)# <b>vpc orphan-ports suspend</b>	選択したインターフェイスをvPC障害時にセカンダリピアにより一時停止されるvPC孤立ポートとして設定します。
ステップ 5	<b>exit</b> 例： switch(config-if)# <b>exit</b> switch#	インターフェイス コンフィギュレーション モードを終了します。
ステップ 6	<b>copy running-config startup-config</b> 例：	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

コマンドまたはアクション	目的
switch# <b>copy running-config startup-config</b>	

### 例

次に、インターフェイスを vPC 障害時にセカンダリ ピアにより一時停止される vPC 孤立ポートとして設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# vpc orphan-ports suspend
switch(config-if)# exit
switch(config)#
```

Cisco NX-OS リリース 9.2(1) 以降では、**show vpc orphan-ports** コマンドの出力が以前のリリースの出力と若干異なります。次に、**show vpc orphan-ports** コマンドの出力例を示します。

```
switch# show vpc orphan-ports
-----::Going through port database. Please be patient.::-----
VLAN          Orphan Ports
-----
1              Eth1/18, Eth3/23
2              Eth3/23
3              Eth3/23
4              Eth3/23
5              Eth3/23
```

## シングルモジュール vPC オブジェクト トラッキングでのトラッキング機能の設定

すべての vPC ピア リンクとコアに面するインターフェイスを単一モジュール上で設定しなければならない場合は、両方のプライマリ vPC ピア デバイス上の vPC ピア リンクのすべてのリンク上にあり、コアへのレイヤ 3 リンクに関連付けられているトラックオブジェクトとトラックリストを設定しなければなりません。いったんこの機能を設定したら、プライマリ vPC ピア デバイスに障害が発生した場合には、プライマリ vPC ピア デバイス上のすべての vPC リンクを、システムが自動的に停止します。システムが安定するまでは、このアクションにより、すべての vPC トラフィックが強制的にセカンダリ vPC ピア デバイスに送られます。

この設定は、両方の vPC ピア デバイスに置かなければなりません。さらに、いずれの vPC ピア デバイスも機能上のプライマリ vPC ピア デバイスになる場合があるため、両方の vPC ピア デバイスに同じ設定を置いておく必要があります。

### 始める前に

vPC 機能が有効なことを確認します。

トラックオブジェクトとトラックリストが設定済みであることを確認します。コアおよびvPCピアリンクに接続されているすべてのインターフェイスが両方のvPCピアデバイス上のトラックオブジェクトに割り当てられていることを確認します。

## 手順の概要

1. **configure terminal**
2. **vpc domain** *domain-id* [**shut** | **no shut**]
3. **track** *track-object-id*
4. **exit**
5. **show vpc brief**
6. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b> switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>vpc domain</b> <i>domain-id</i> [ <b>shut</b>   <b>no shut</b> ] 例： switch(config)# <b>vpc domain</b> 5 switch(config-vpc-domain)#	設定する vPC ドメインの番号を入力し、vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	<b>track</b> <i>track-object-id</i> 例： switch(config-vpc-domain)# <b>track object</b> 23 switch(config-vpc-domain)#	以前に関連するインターフェイスで設定されたトラックリストオブジェクトをvPCドメインに追加します。オブジェクトトラッキングおよびトラックリストの詳細については、『 <a href="#">Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide</a> 』を参照してください。
ステップ 4	<b>exit</b> 例： switch(config-vpc-domain)# <b>exit</b> switch#	vpc-domain 設定モードを終了します。
ステップ 5	<b>show vpc brief</b> 例： switch# <b>show vpc brief</b>	(任意) 追跡対象オブジェクトに関する情報を表示します。
ステップ 6	<b>copy running-config startup-config</b> 例： switch# <b>copy running-config startup-config</b>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

## 例

次に、以前に設定されたトラックリストオブジェクトを、vPC ピアデバイス上の vPC ドメインに配置する例を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# track object 5
switch(config-vpc-domain)# exit
switch(config)#
```

## 停電後のリカバリの設定

停電が発生すると、vPC はピア隣接がスイッチリロード時に形成するのを待ちます。この状況は、許容範囲内に収まらないほど長いサービスの中断に至る場合があります。Cisco Nexus 9000 シリーズ デバイスは、そのピアがオンラインになるのに失敗した場合に vPC サービスを復元するように設定できます。

### 自動リカバリの設定

Cisco Nexus 9000 シリーズ デバイスは、**auto-recovery** コマンドを使用して、そのピアがオンラインになるのに失敗した場合に vPC サービスを復元するように設定できます。

Cisco Nexus 9000 シリーズ デバイスは、**auto-recovery** コマンドを使用して、vPC プライマリ ピアが失敗し、ピア キープアライブと vPC ピア リンクを停止するとき、セカンダリ vPC ピアの vPC サービスを復元するように構成できます。ピア キープアライブと vPC ピア リンクの両方がダウンしているプライマリ スイッチに障害が発生すると、セカンダリ スイッチは vPC メンバーを一時停止します。ただし、キープアライブ ハートビートが 3 回失われると、セカンダリ スイッチはプライマリ スイッチの役割を再開し、vPC メンバーポートを起動します。

**auto-recovery reload restore** コマンドは、vPC プライマリ スイッチがリロードするシナリオで使用できます。この場合、セカンダリ スイッチは vPC プライマリの役割を再開し、IP VPC メンバー ポートを持ち込みます。



- (注) Cisco Nexus 9000 スイッチでは、自動回復機能はデフォルトで有効になっていません。オブジェクト トラッキングがトリガーされると、vPC セカンダリ ピア デバイスはそのプライマリ デバイスへのロールを変更せず、vPC レッグを再初期化します。プライマリ ロールを引き継いで vPC レッグを再初期化できるように、vPC セカンダリ ピア デバイスで自動回復を手動で設定する必要があります。

### 始める前に

vPC 機能が有効なことを確認します。

### 手順の概要

#### 1. configure terminal

2. **vpc domain** *domain-id* [**shut** | **no shut**]
3. **auto-recovery** [ **reload-delay** *time*]
4. **exit**
5. **show running-config vpc**
6. **show vpc consistency-parameters interface port-channel** *number*
7. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b> switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>vpc domain</b> <i>domain-id</i> [ <b>shut</b>   <b>no shut</b> ] 例： switch(config)# <b>vpc domain</b> 5 switch(config-vpc-domain)#	設定する vPC ドメインの番号を入力し、vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	<b>auto-recovery</b> [ <b>reload-delay</b> <i>time</i> ] 例： switch(config-vpc-domain)# <b>auto-recovery</b>	vPC がそのピアが機能しないことを前提として vPC を稼働させ始めるように設定し、vPC を復元するためのリロード後に待機する時間を指定します。デフォルト遅延値は 240 秒です。240 ~ 3600 秒の遅延を設定できます。  vPC をデフォルト設定にリセットするには、このコマンドの <b>no</b> 形式を使用します。
ステップ 4	<b>exit</b> 例： switch(config-vpc-domain)# <b>exit</b> switch#	vpc-domain 設定モードを終了します。
ステップ 5	<b>show running-config vpc</b> 例： switch# <b>show running-config vpc</b>	(任意) vPC に関する情報、特にリロードステータスを表示します。
ステップ 6	<b>show vpc consistency-parameters interface port-channel</b> <i>number</i> 例： switch# <b>show vpc consistency-parameters interface port-channel</b> 1	(任意) 指定したインターフェイスの vPC の一貫性パラメータに関する情報を表示します。
ステップ 7	<b>copy running-config startup-config</b> 例：	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

	コマンドまたはアクション	目的
	switch# <b>copy running-config startup-config</b>	(注) 自動リカバリ機能がイネーブルになっていることを確認するには、この手順を実行します。

### 例

次に、vPC 自動リカバリ機能を設定し、それをスイッチのスタートアップ コンフィギュレーションに保存する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vpc domain 5
switch(config-vpc-domain)# auto-recovery
switch(config-vpc-domain)# auto-recovery auto-recovery reload-delay 100
```

Warning:  
Enables restoring of vPCs in a peer-detached state after reload, will wait for 240 seconds to determine if peer is un-reachable

```
switch(config-vpc-domain)# exit
switch(config)# exit
switch# copy running-config startup-config
```

## ヒットレス vPC ロール変更の設定

ヒットレス vPC ロールの変更を有効にするには、次の手順を実行します。

### 始める前に

- vPC 機能がイネーブルになっていることを確認します。
- vPC ピア リンクがアップしていることを確認します
- デバイスのロール プライオリティを検証します

### 手順の概要

1. **vpc role preempt**
2. **show vpc role**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>vpc role preempt</b>  例 : switch# <b>vpc role preempt</b> switch(config)#	ヒットレス vPC ロールの変更を有効にします。

	コマンドまたはアクション	目的
ステップ 2	<b>show vpc role</b> 例 : switch(config)# <b>show vpc role</b>	(任意) ヒットレスvPCロール変更機能を確認します。

### 例

次に、ヒットレス vPC ロールの変更を設定する例を示します。

```
switch# show vpc role
vPC Role status
-----
vPC role                : secondary
vPC system-mac          : 00:23:04:ee:be:01
vPC system-priority     : 32667
vPC local system-mac    : 8c:60:4f:03:84:41
vPC local role-priority : 32668
vPC peer system-mac     : 8c:60:4f:03:84:43
vPC peer role-priority  : 32667

! Configure vPC hitless role change on the device!

switch(config)# vpc role preempt
! The following is an output from the show vpc role command after the
vPC hitless feature is configured
switch(config)# show vpc role
vPC Role status
-----
vPC role                : primary
vPC system-mac          : 00:00:00:00:00:00
vPC system-priority     : 32667
vPC local system-mac    : 8c:60:4f:03:84:41
vPC local role-priority : 32666
vPC peer system-mac     : 8c:60:4f:03:84:43
vPC peer role-priority  : 32667

switch(config)#
```

## vPC ロールの変更に関する使用ケース シナリオ

ヒットレス vPC ロール変更機能は、次のシナリオで使用できます。

- ロール変更要求 : vPC ドメインのピアデバイスのロールを変更する場合。
- プライマリ スイッチのリロード : リロード後にロールが定義され、ロールが定義されると、ヒットレス vPC ロール変更機能を使用してロールを復元できます。たとえば、リロード後にプライマリデバイスが動作可能なセカンダリの役割を果たし、セカンダリデバイスがプライマリの動作の役割を担う場合、**vpc role preempt** コマンドを使用してvPCピアの役割を元の定義済みの役割に変更できます。



(注) vPC ロールを切り替える前に、必ず、既存のデバイスロールプライオリティをチェックしてください。

- デュアルアクティブリカバリ：デュアルアクティブリカバリ シナリオでは、vPC プライマリ スイッチが引き続き（動作中）プライマリになりますが、vPC セカンダリ スイッチがターゲットプライマリ スイッチになり、vPC メンバー ポートがアップ状態になります。vPC ヒットレス機能を使用して、デバイス ロールを復元できます。デュアルアクティブリカバリ後は、一方が稼働可能なプライマリで、もう一方が稼働可能なセカンダリの場合に、**vpc role preempt** コマンドを使用して、プライマリにするデバイス ロールとセカンダリにするデバイス ロールを復元できます。

## vPC ドメイン MAC アドレスの手動での設定

vPC ドメインを作成すると、Cisco NX-OS ソフトウェアが自動的に vPC システム MAC アドレスを作成します。このアドレスは、LACP など、リンク スコープに制限される操作に使用されます。ただし、vPC ドメインの MAC アドレスを手動で設定するように選択することもできます。

### 始める前に

vPC 機能が有効なことを確認します。

### 手順の概要

1. **configure terminal**
2. **vpc domain *domain-id* [shut | no shut]**
3. **system-mac *mac-address***
4. **exit**
5. **show vpc role**
6. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b> switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>vpc domain <i>domain-id</i> [shut   no shut]</b> 例： switch(config)# <b>vpc domain 5</b> switch(config-vpc-domain)#	設定する vPC ドメインの番号を入力します。システムは、vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	<b>system-mac <i>mac-address</i></b> 例： switch(config-vpc-domain)# <b>system-mac 23fb.4ab5.4c4e</b> switch(config-vpc-domain)#	指定した vPC ドメインに割り当てる MAC アドレスを <b>aaaa.bbbb.cccc</b> の形式で入力します。

	コマンドまたはアクション	目的
ステップ 4	<b>exit</b> 例： switch(config-vpc-domain)# <b>exit</b> switch#	vpc-domain 設定モードを終了します。
ステップ 5	<b>show vpc role</b> 例： switch# <b>show vpc brief</b>	(任意) vPC システム MAC アドレスを表示します。
ステップ 6	<b>copy running-config startup-config</b> 例： switch# <b>copy running-config startup-config</b>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

### 例

次の例は、vPC ドメイン MAC アドレスを手動で設定する方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# system-mac 13gb.4ab5.4c4e
switch(config-vpc-domain)# exit
switch(config)#
```

## システム プライオリティの手動での設定

vPC ドメインを作成すると、vPC システムプライオリティが自動的に作成されます。ただし、vPC ドメインのシステムプライオリティは手動で設定することもできます。



- (注) LACP の実行時には、vPC ピア デバイスが LACP のプライマリ デバイスになるように、vPC システムプライオリティを手動で設定することを推奨します。システムプライオリティを手動で設定する場合には、必ず同じプライオリティ値を両方のvPC ピアデバイスに設定します。これらの値が一致しないと、vPC は起動しません。

### 始める前に

vPC 機能が有効なことを確認します。

### 手順の概要

1. **configure terminal**
2. **vpc domain domain-id [shut | no shut]**
3. **system-priority priority**
4. **exit**

5. **show vpc role**
6. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b> switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>vpc domain domain-id [shut   no shut]</b> 例： switch(config)# <b>vpc domain 5</b> switch(config-vpc-domain)#	設定する vPC ドメインの番号を入力します。システムは、vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	<b>system-priority priority</b> 例： switch(config-vpc-domain)# <b>system-priority 4000</b> switch(config-vpc-domain)#	指定した vPC ドメインに割り当てるシステム プライオリティを入力します。指定できる値の範囲は、1 ~ 65535 です。デフォルト値は 32667 です。
ステップ 4	<b>exit</b> 例： switch(config-vpc-domain)# <b>exit</b> switch#	vpc-domain 設定モードを終了します。
ステップ 5	<b>show vpc role</b> 例： switch# show vpc role	(任意) vPC システム プライオリティを表示します。
ステップ 6	<b>copy running-config startup-config</b> 例： switch# <b>copy running-config startup-config</b>	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

## 例

次の例は、vPC ドメインのシステム プライオリティを手動で設定する方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# system-priority 4000
switch(config-vpc-domain)# exit
switch(config)#
```

## vPC ピア デバイス ロールの手動での設定

デフォルトでは、vPC ドメインと、vPC ピア リンクの両端を設定すると、Cisco NX-OS ソフトウェアはプライマリとセカンダリの vPC ピア デバイスを選択します。ただし、vPC のプライマリ デバイスとして、特定の vPC ピア デバイスを選択することもできます。選択したら、プライマリ デバイスにする vPC ピア デバイスに、他の vPC ピア デバイスより小さいロール値を手動で設定します。

vPC はロールのプリエンブションをサポートしません。プライマリ vPC ピア デバイスに障害が発生すると、セカンダリ vPC ピア デバイスが、vPC プライマリ デバイスの機能を引き継ぎます。ただし、以前のプライマリ vPC が再起動しても、機能のロールは元に戻りません。

### 始める前に

vPC 機能が有効なことを確認します。

### 手順の概要

1. **configure terminal**
2. **vpc domain *domain-id* [shut | no shut]**
3. **role priority *priority***
4. **exit**
5. **show vpc role**
6. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b> switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>vpc domain <i>domain-id</i> [shut   no shut]</b> 例： switch(config)# <b>vpc domain 5</b> switch(config-vpc-domain)#	設定する vPC ドメインの番号を入力します。システムは、vpc-domain コンフィギュレーションモードを開始します。
ステップ 3	<b>role priority <i>priority</i></b> 例： switch(config-vpc-domain)# <b>role priority 4</b> switch(config-vpc-domain)#	vPC システムプライオリティとして使用するロールプライオリティを指定します。値の範囲は1～65636で、デフォルト値は32667です。低い値は、このスイッチがプライマリ vPC になる可能性が高いということを意味します。
ステップ 4	<b>exit</b> 例：	vpc-domain 設定モードを終了します。

	コマンドまたはアクション	目的
	switch(config)# <b>exit</b> switch#	
ステップ 5	<b>show vpc role</b>  例： switch# <b>show vpc role</b>	(任意) vPC システム プライオリティを表示します。
ステップ 6	<b>copy running-config startup-config</b>  例： switch# <b>copy running-config startup-config</b>	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

### 例

次の例は、vPC ピアデバイスのロールプライオリティを手動で設定する方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# role priority 4
switch(config-vpc-domain)# exit
switch(config)#
```

## Cisco MAC アドレスを使用するための STP の有効化

この手順により、STP が Cisco MAC アドレス (00 : 26 : 0b : xx : xx : xx) を使用できるようになります。

### 始める前に

vPC 機能が有効なことを確認します。

### 手順の概要

1. **configure terminal**
2. **vpc domain domain-id**
3. **[no] mac-address bpdu source version 2**
4. **exit**
5. (任意) **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	<b>vpc domain</b> <i>domain-id</i> 例： switch(config)# <b>vpc domain</b> 5	vPC ドメインがまだ存在していない場合はそれを作成し、vpc-domain コンフィギュレーションモードを開始します。
ステップ 3	<b>[no] mac-address bpd</b> source version 2 例： switch(config-vpc-domain)# <b>mac-address bpd</b> source version 2	STP がシスコの MAC アドレス (00:26:0b:xx:xx:xx) を、vPC ポートで生成される BDPU の発信元アドレスとして使用できるようになります。
ステップ 4	<b>exit</b> 例： switch(config-vpc-domain)# <b>exit</b>	vpc-domain 設定モードを終了します。
ステップ 5	(任意) <b>copy running-config startup-config</b> 例： switch(config)# <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## vPC 設定の確認

vPC 設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
<b>show feature</b>	vPC がイネーブルになっているかどうかを表示します。
<b>show vpc brief</b>	vPC に関する要約情報を表示します。
<b>show vpc consistency-parameters</b>	すべての vPC インターフェイス全体で一貫している必要があるパラメータのステータスを表示します。
<b>show running-config vpc</b>	vPC の実行コンフィギュレーションの情報を表示します。
<b>show port-channel capacity</b>	設定されているポート チャンネルの数、およびデバイス上でまだ使用可能なポート チャンネル数を表示します。
<b>show vpc statistics</b>	vPC に関する統計情報を表示します。
<b>show vpc peer-keepalive</b>	ピアキープアライブ メッセージに関する情報を表示します。

コマンド	目的
<b>show vpc role</b>	ピア ステータス、ローカル デバイスのロール、vPC システム MAC アドレスとシステム プライオリティ、およびローカル vPC デバイスの MAC アドレスとプライオリティを表示します。

## vPC のモニタリング

**show vpc statistics** コマンドを使用し、vPC 統計情報を表示します。

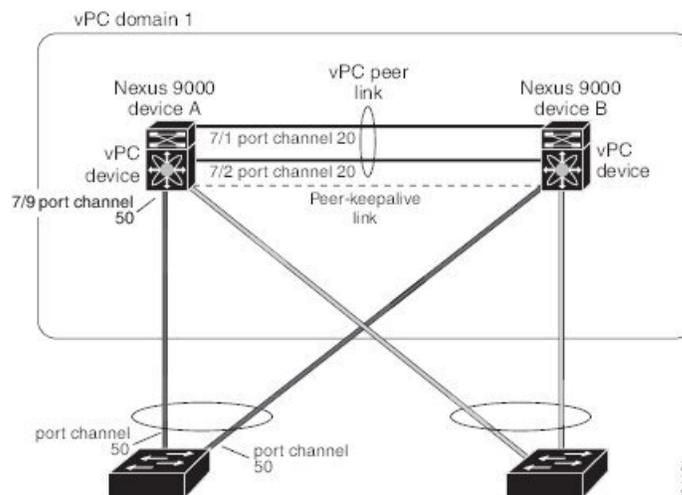


(注) このコマンドは、現在作業している vPC ピア デバイスの vPC 統計情報しか表示しません。

## vPC の設定例

次の例は、の図に示すように、デバイス A 上で vPC を設定する方法を示します。

図 18: vPC の設定例



1. vPC および LACP をイネーブルにします。

```
switch# configure terminal
switch(config)# feature vpc
switch(config)# feature lacp
```

2. (任意) vPC ピア リンクにするインターフェイスの 1 つを専用モードに構成します。

```
switch(config)# interface ethernet 7/1,
ethernet 7/3, ethernet 7/5. ethernet 7/7
```

```
switch(config-if)# shutdown
switch(config-if)# exit
switch(config)# interface ethernet 7/1
```

```
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)#
```

3. (任意) vPC ピア リンクにする 2 つ目の冗長インターフェイスを専用ポートモードに構成します。

```
switch(config)# interface ethernet 7/2, ethernet 7/4,
ethernet 7/6. ethernet 7/8
switch(config-if)# shutdown
switch(config-if)# exit
switch(config)# interface ethernet 7/2
```

```
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)#
```

4. vPC ピア リンクに入れる 2 つのインターフェイス (冗長性のために) をアクティブ レイヤ 2 LACP ポート チャンネルに構成します。

```
switch(config)# interface ethernet 7/1-2
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1-50
switch(config-if)# switchport trunk native vlan 20
switch(config-if)# channel-group 20 mode active
switch(config-if)# exit
```

5. VLAN を作成し、イネーブルにします。

```
switch(config)# vlan 1-50
switch(config-vlan)# no shutdown
switch(config-vlan)# exit
```

6. vPC ピアキープアライブ リンク用の独立した VEF を作成し、レイヤ 3 インターフェイスをその VRF に追加します。

```
switch(config)# vrf context pkal
switch(config-vrf)# exit
switch(config)# interface ethernet 8/1
switch(config-if)# vrf member pkal
switch(config-if)# ip address 172.23.145.218/24
switch(config-if)# no shutdown
switch(config-if)# exit
```

7. vPC ドメインを作成し、vPC ピアキープアライブ リンクを追加します。

```
switch(config)# vpc domain 1
switch(config-vpc-domain)# peer-keepalive
destination 172.23.145.217 source 172.23.145.218 vrf pkal
switch(config-vpc-domain)# exit
```

8. vPC vPC ピア リンクを構成します。

```
switch(config)# interface port-channel 20
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1-50
switch(config-if)# vpc peer-link
```

```
switch(config-if) # exit
switch(config) #
```

9. vPC のダウンストリーム デバイスへのポート チャネルのインターフェイスを設定します。

```
switch(config) # interface ethernet 7/9
switch(config-if) # switchport mode trunk
switch(config-if) # allowed vlan 1-50
switch(config-if) # native vlan 20
switch(config-if) # channel-group 50 mode active
switch(config-if) # exit
switch(config) # interface port-channel 50
switch(config-if) # vpc 50
switch(config-if) # exit
switch(config) #
```

10. 設定を保存します。

```
switch(config) # copy running-config startup-config
```



(注) まずポート チャネルを設定する場合は、それがレイヤ 2 ポート チャネルであることを確認してください。

## 関連資料

関連項目	関連項目
システム管理	システム管理
高可用性	高可用性
リリース ノート	リリース ノート



## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。