



vPC の設定

この章では、Cisco NX-OS デバイスに仮想ポートチャネル (vPCs) を構成する手順について説明します。

vPC ピア リンクに Nexus 3550-T デバイスの任意のインターフェイスを使用できます。

ポートチャ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ネルメンバーと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。



(注) ポートチャネルの互換性パラメータは、両方のピアのすべての vPC メンバー ポートで同じである必要があるため、各シャーシで同じタイプのモジュールを使用する必要があります。

- [vPCについて \(1 ページ\)](#)
- [注意事項と制約事項 \(22 ページ\)](#)
- [レイヤ 3 および vPC 設定のベスト プラクティス \(25 ページ\)](#)
- [デフォルト設定 \(33 ページ\)](#)
- [vPC の設定 \(34 ページ\)](#)
- [vPC 設定の確認 \(61 ページ\)](#)
- [vPC のモニタリング \(62 ページ\)](#)
- [vPC の設定例 \(62 ページ\)](#)

vPCについて

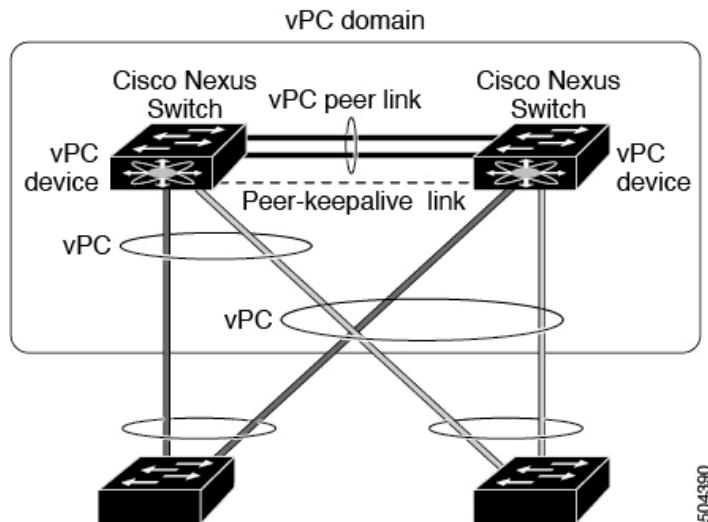
vPCの概要

仮想ポートチャネル (vPC) は、物理的には 2 台の Cisco Nexus 3550-T 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キ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

■ vPC の概要

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ポートチャネルだけです。ポートチャネルの設定は、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 ピアリンクチャネルも含めて) のポートチャネルを構成する場合は、各デバイスが、単一のポートチャネル内に最大4つのリンクを持ち、そして4つ全てのメンバーは、同じクラウドに属している必要があります。特定のクラウドからは、1つのポートチャネルのみを使用できます。



(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 3550-T シリーズ シャーシでポートチャネルを設定して 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 3550-T 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 チャネルを設定します。これらの 2 つのポート チャネルを接続すると、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。

vPC ピア リンクに Nexus 3550-T デバイスの任意のインターフェイスを使用できます。

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。

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 3550-T スイッチ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なります。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。

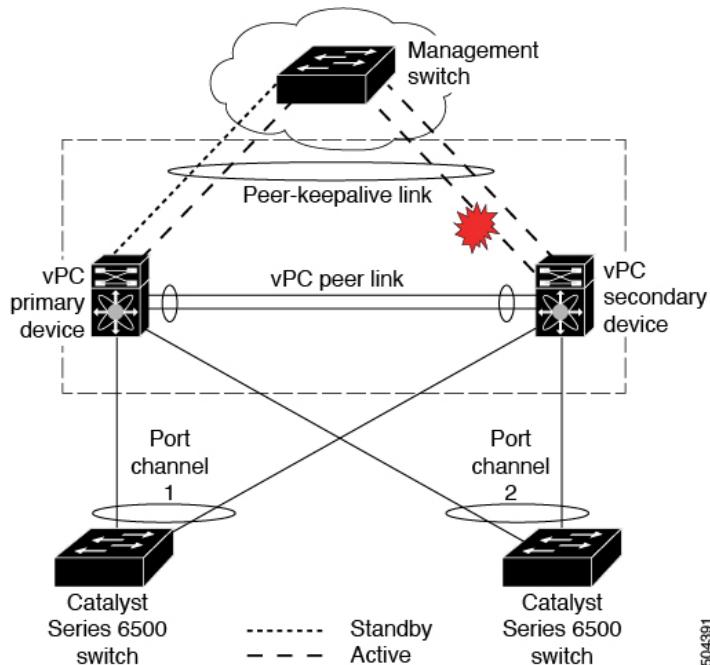
vPC の用語

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、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。
- vPC メンバポート : vPC に属するインターフェイス。
- 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ルink : ピアキープアライブルinkは、さまざまな vPC ピア Cisco Nexus 3550-T シリーズのデバイスをモニターします。ピアキープアライブルinkは、vPC ピアデバイス間での設定可能なキープアライブル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ルink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デフォルト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。

図 2: vPC ピアキープアライブルink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 ピアキープアライブ 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。

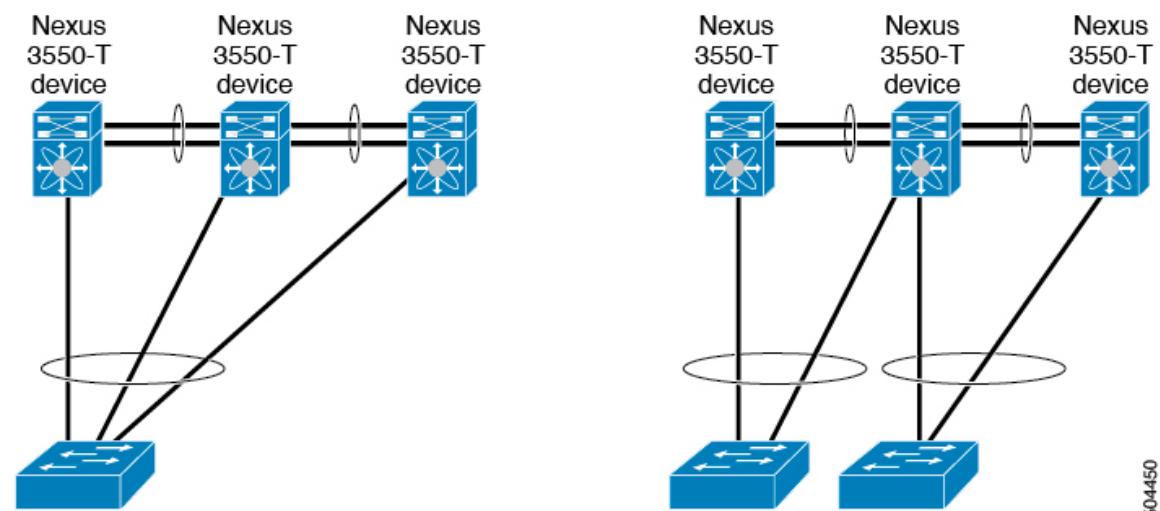
- vPC メンバ ポート：vPC に属するインターフェイス。
- デュアルアクティブ：プライマリとして動作する両方の vPC ピア。この状況は、両方のピアがまだアクティブなときに vPC ピアキープアライブとピア リンクがダウンした場合に発生します。この場合、セカンダリ vPC はプライマリ vPC が動作しないと想定し、プライマリ vPC として機能します。
- リカバリ：ピアキープアライブと vPC ピア リンクが起動すると、1台のスイッチがセカンダリ vPC になります。セカンダリ vPC になるスイッチで、vPC リンクが停止してから復帰します。

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 3: 許可されていない vPC ピア設定



504450

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 リンクを設定し終えたら、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。

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、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 \(21 ページ\)](#)」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 \(21 ページ\)](#)」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、ループやトライ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。
- VRRP アクティブ : vPC ピア デバイス上で Virtual Router Redundancy Protocol (VRRP) 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 VRRP マスターの最も高いプライオリティで構成します。バックアップ デバイスを VRRP スタンバイになるように構成し、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 ピア リンクのレイヤ3バックアップルートの構成

単方向リンク検出 (UDLD) の構成では、次の留意点に注意してください：

- LACP がポートチャ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 がポートチャネル集約プロトコル（静的なポートチャネル）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。

vPC ピア リンクのレイヤ3バックアップルートの構成

VRRP 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。

ピアキープアライブリンクとメッセージ

Cisco NX-OS ソフトウェアは、vPC ピア間でピアキープアライブリンクを使用して、設定可能なキープアライブメッセージを定期的に送信します。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接続がなくてはなりません。ピアキープアライブリンクが有効になっ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デフォルト VRF に関連付けることを推奨します。管理 VRF を構成しなかつた場合は、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、ピアキープ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じます。vPC ピアキープ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 ピアキープアライブ 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 ピアキープアライブ 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、受信したキープアライブ 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、キープ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プアライブ 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。

キープアライブ 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) ピアキープアライブ 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 ピアキープアライブ 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。

ピアキープアライブ 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 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、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 VRRP ゲートウェイではなく、送信元 Cisco Nexus 3550-T デバイスの MAC アドレスを使用して、トライ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、トライ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 トライ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。

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。



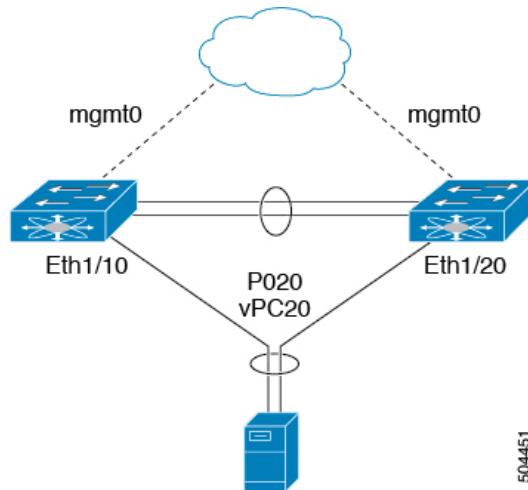
(注) システム プライオリティを手動で設定する場合は、必ず両方の vPC ピアデバイス上で同じプライオリティ値を割り当てる必要があります。vPC ピアデバイス同士が異なるシステム プライオリティ値を持っていると、vPC は稼働しません。

vPC トポロジ

次の図は、Cisco Nexus 3550-T 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ネルの一部として設定される基本設定を示しています。

■ vPC インターフェイスの互換パラメータ

図 4: vPC トポロジのスイッチ



この図では、vPC 20 がポート チャネル 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 Eth1/20 がメンバ ポートとしてあります。

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 チャネル メンバーと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 チャネルについては、「ポート チャネルの設定」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つていなければならず、グローバルパラメータはグローバルに一貫性を保つていなければなりません。

- ポートチャネルモード：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 トラフィックのタギング
- 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

同じにすべき設定パラメータ

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PEND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ず、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。そうなっていない VLAN は、停止します。
- ACL のすべて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+)
- 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
- 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
- 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

稼動中の 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 は稼動を継続し、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 リンクを作成し終えたら、ダウンストリーム 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 デバイスからダウンストリーム 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 デバイスからダウンストリーム 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ンストリーム 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 (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 デバイスからダウンストリーム 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。

他のポート チャネルの vPC への移行



(注) ダウンストリーム 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。

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

■ 他の機能との vPC の相互作用

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ありません。

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ネルも含めて、すべての vPC ポートチャネル上の 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します。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。



(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 (CFSoE) 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。CFSoE 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。そうなっていないと、トライ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。

vPC が有効な場合、**show spanning-tree** コマンドを使用して vPC に関する情報を表示できます。

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。

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、Cisco NX-OS に追加されました。この機能により、一対の Cisco Nexus 3550-T 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、トライ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。

vPC および ARP または ND

Cisco Fabric Service over Ethernet (CFSoE) 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 コマンドを有効化にし、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 : IGMP、および IGMP スヌーピング

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。

各vPCピアは、レイヤ2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2vPCクラウド内にあり、vPCメンバリンクが停止している場合。

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。

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ロールの変更期間に依存します。

次に、vPC IGMP/IGMPスヌーピングについて説明します。

- 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。

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ます、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) Cisco Nexus 3550-T は、vPC VLAN での PIM をサポートしていません。

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。仮想ルータ冗長プロトコル (VRRP) は、vPC と相互運用します。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 のトラブルシューティングを簡単にできます。

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 はルーティング 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 VRRP 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。VRRP 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。

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。



(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。

■ 停電後の vPC リカバリ

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。場合によつては、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 3550-T 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。

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。

- 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。
- 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。

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。

- 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 3550-T 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。
- vPC 上のレイヤ 3 マルチキャストはサポートされていません。
- 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止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。
- 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。
- CFS リージョンはサポートされていません。
- ポート セキュリティがサポートされていません
- 2 つの Cisco Nexus 3550-T 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 リンクで有効にならない VLAN に対してもスパ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仮想ルータ冗長プロトコル (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。
-
- vPC を使用する場合は、VRRP にデフォルトのタイマーを使用することを推奨します。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。

■ 注意事項と制約事項

- 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
```

- STP ポートコストは、vPC 環境で 200 に固定されています。
- 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 のポートで使用することをお勧めします。
- 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。
- 2つの Cisco Nexus 3550-T 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。
- 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 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。
- 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 3550-T 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構成のベストプラクティス」の項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。

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。

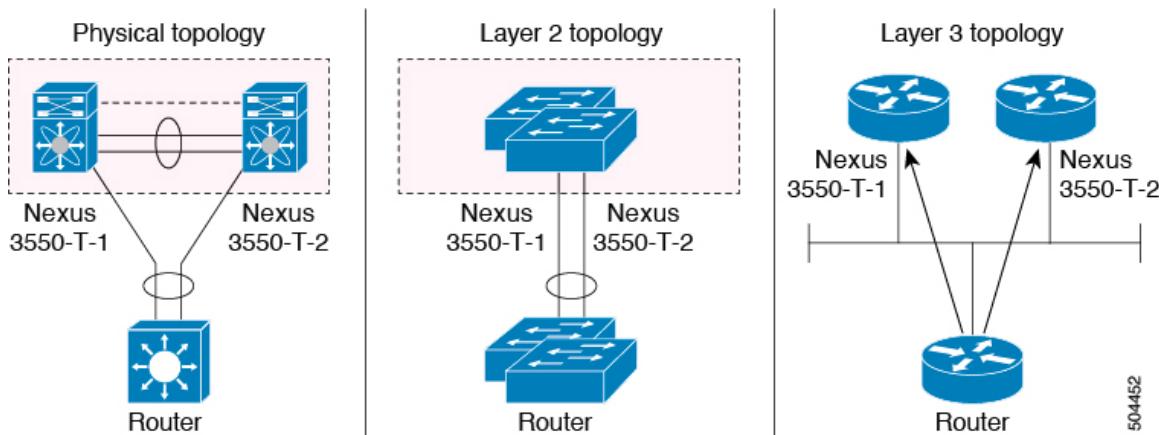
- ・レイヤ2では、レイヤ3デバイスはvPCピアデバイスによって提供される一意のレイヤ2スイッチを認識します。
- ・レイヤ3では、レイヤ3デバイスは2台の異なるレイヤ3デバイス(vPCピアデバイスごとに1台)を認識します。

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5: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

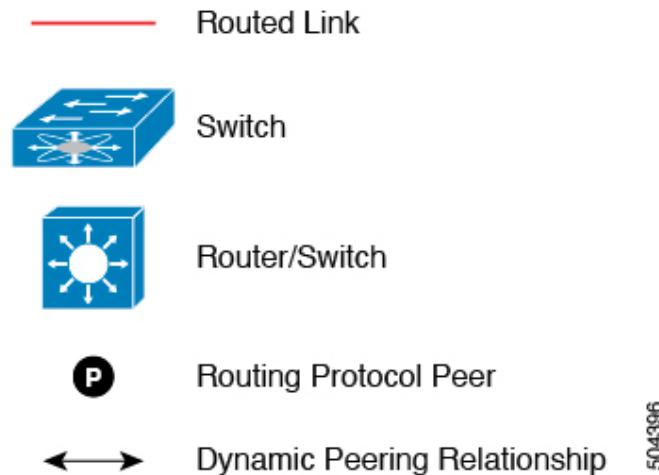
ここでは、レイヤ3およびvPCのネットワークトポロジの例を示します。

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

■ レイヤ3リンクを使用した外部ルータとのピアリング

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 6: 凡例



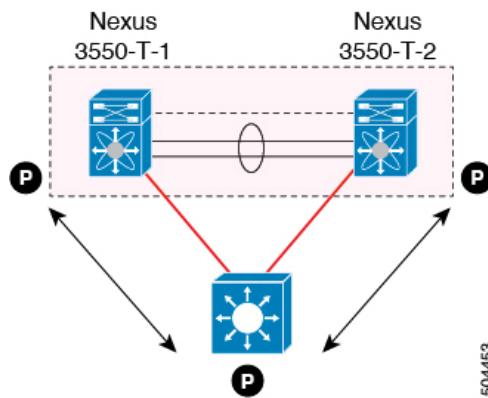
レイヤ3リンクを使用した外部ルータとのピアリング

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 3550-T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 7: 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。

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。

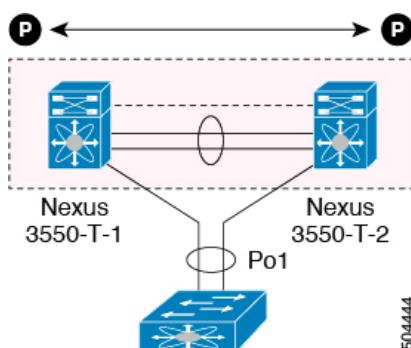
- レイヤ3デバイスを vPC ドメインに接続するには、独立したレイヤ3リンクを使用します。各リンクはポイントツーポイントレイヤ3接続を表し、小さなIPサブネット (/30 または /31) から取得されたIPアドレスが割り当てられます。

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ィングパスを持つ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 8: 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

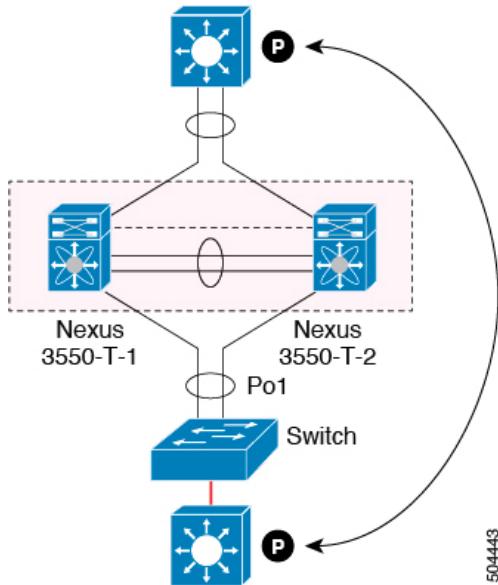


ルータ間の直接レイヤ3ピアリング

このシナリオでは、vPC ドメインの Nexus 3550-T 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。

■ 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

図 9: ルータ間ピアリング



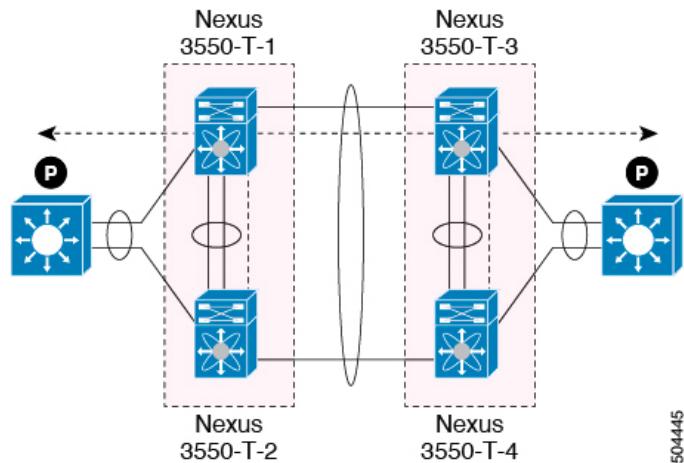
レイヤ 3 デバイスは、次の 2 つの方法で相互のピアとなることができます。また、ピアリングの方法は、このロールにどのようなデバイスが展開されるかによっても変わります。

- 中間の Cisco Nexus 3550-T 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。

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 3550-T 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 3550-T 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 10: 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 3550-T 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。

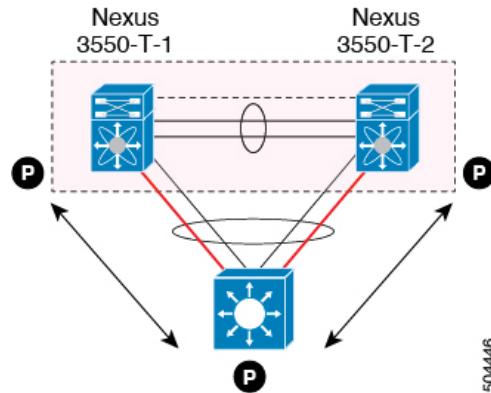
レイヤ2リンクは、ブリッジド トラフィック（同じ VLAN に保持されるトラフィック）または VLAN 間トラフィック（vPC ドメインがインターフェイス VLAN と関連 VRRP 構成をホストすることが前提）に使用されます。

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デバイスを通過す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。

■ 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

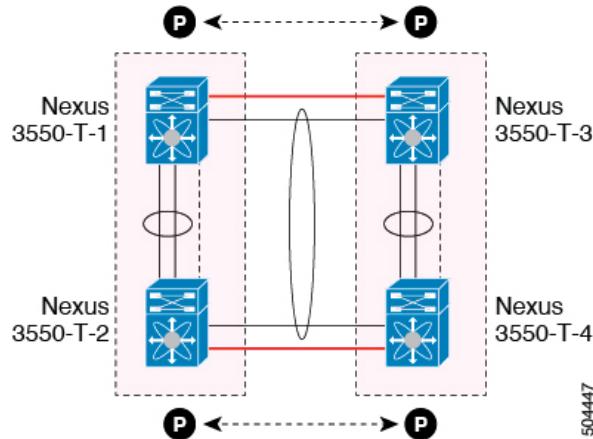
図 11: パラレル相互接続ルーテッドポート上の外部ルーターとのピアリング



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 3550-T 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 3550-T 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 12: 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 間トラフィックを传送し、専用レイヤ 3 リンクは 2 サイト間でルーテッド トラフィックを传送します。

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

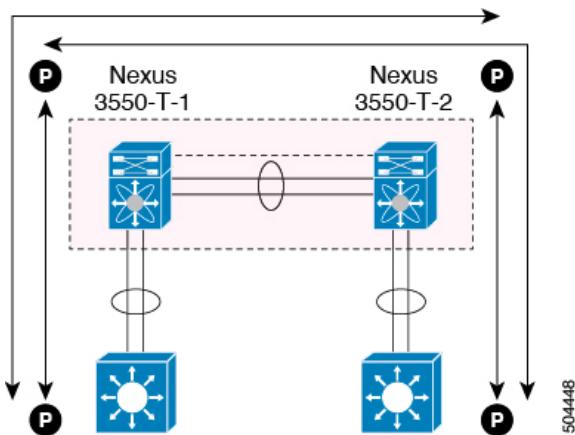
この例は、レイヤ 3 デバイスが vPC ドメインにシングル接続されている場合に、専用スイッチ間リンクで非 vPC VLAN を使用して、レイヤ 3 デバイスと各 vPC ピア デバイスとの間でルー

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 13: 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

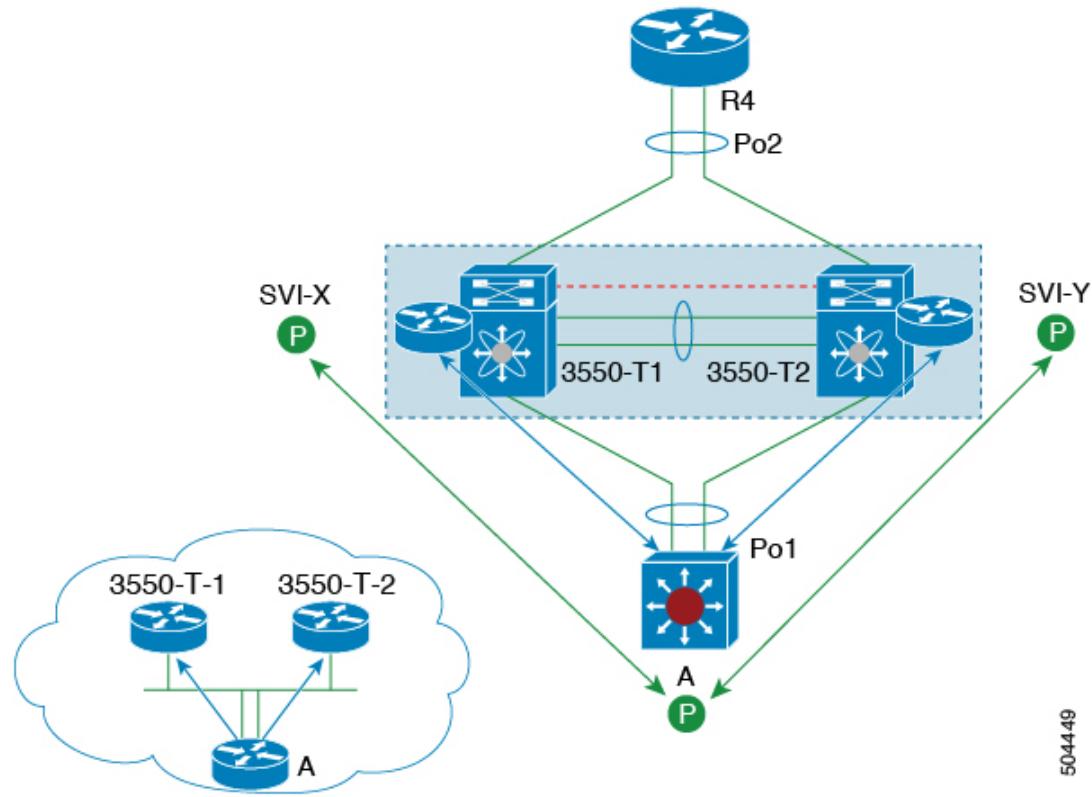
レイヤ 3 ルータと Cisco Nexus 3550-T vPC スイッチのペア間でレイヤ 3 ピアリングを確立する代替方法。



(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。

■ vPC 接続を介した直接ピアリング

図 14: 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。

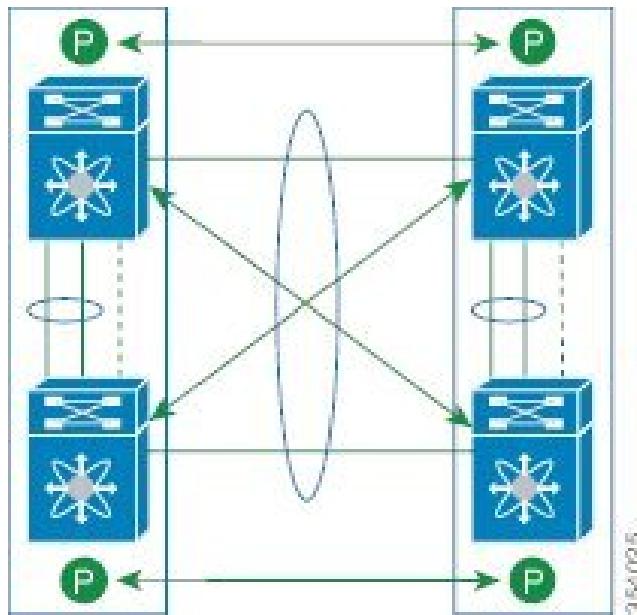


504449

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 3550-T 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 15: 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 3550-T スイッチすべてに同じ VLAN 内の SVI インターフェイスが構成され、これらの間でルーティング ピアリングと接続が確立されます。

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る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

	コマンドまたはアクション	目的
ステップ 1	configure terminal 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	feature vpc 例： <pre>switch(config)# feature vpc</pre>	デバイス上で vPC をイネーブルにします。
ステップ 3	exit 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 4	show feature 例： <pre>switch# show feature</pre>	(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。

	コマンドまたはアクション	目的
ステップ 5	copy running-config startup-config 例： switch# copy running-config startup-config	(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なると、デバイス上のすべての vPC 設定がクリアされます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal 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	no feature vpc 例： switch(config)# no feature vpc	デバイスの vPC をディセーブルにします。
ステップ 3	exit 例： switch(config)# exit 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	show feature 例： switch# show feature	(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。

■ vPC ドメインの作成と **vpc-domain** モードの開始

	コマンドまたはアクション	目的
ステップ 5	copy running-config startup-config 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。

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

	コマンドまたはアクション	目的
ステップ 1	configure terminal 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	vpc domain domain-id [shut no shut] 例： <pre>switch(config)# vpc domain 5 switch(config-vpc-domain)#</pre>	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	exit 例： <pre>switch(config)# exit switch#</pre>	vpc-domain 設定モードを終了します。
ステップ 4	show vpc brief 例：	(任意) 各 vPC ドメインに関する簡単な情報を表示します。

	コマンドまたはアクション	目的
	switch# show vpc brief	
ステップ 5	copy running-config startup-config 例： switch# copy running-config startup-config	(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、デフォルトのVRF インスタンスを構成して、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 の作成および構成方法については、『Cisco ユニキャスト 3550-T 構成ガイド』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。

■ 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

手順

	コマンドまたはアクション	目的
ステップ1	configure terminal 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	vpc domain domain-id [shut no shut] 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	peer-keepalive destination ipaddress [hold-timeout secs interval msecs {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}] 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 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。 管理ポートと VRF がデフォルトです。 (注) デフォルト VRF を構成し、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。
ステップ4	exit 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	show vpc statistics 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。
ステップ6	copy running-config startup-config 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。

例

次の例は、vPC ピアキープアライブ 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

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal 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	interface port-channel channel-number 例： switch(config)# interface port-channel 20 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	switchport mode trunk 例： switch(config-if)# switchport mode trunk	(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	switchport trunk allowed vlan vlan-list 例： switch(config-if)# switchport trunk allowed vlan 1-120,201-3967	(任意) 許容 VLAN リストを設定します。

■ vPC ピアゲートウェイの設定

	コマンドまたはアクション	目的
ステップ 5	vpc peer-link 例： switch(config-if)# vpc peer-link switch(config-vpc-domain)#+	選択したポートチャネルを 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	exit 例： switch(config)# exit switch#+	vpc-domain 設定モードを終了します。
ステップ 7	show vpc brief 例： switch# show vpc brief	(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	copy running-config startup-config 例： switch# copy running-config startup-config	(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 1-255
switch(config-if)# vpc peer-link
switch(config-vpc-domain)#+
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

	コマンドまたはアクション	目的
ステップ1	configure terminal 例： switch# configure terminal 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	vpc domain domain-id [shut no shut] 例： switch(config-if)# vpc domain 5 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	peer-gateway 例： switch(config-vpc-domain)# peer-gateway (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	exit 例： switch(config)# exit switch#	vpc-domain 設定モードを終了します。
ステップ5	show vpc brief 例： switch# show vpc brief	(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	copy running-config startup-config 例： switch# copy running-config startup-config	(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。

高速コンバージェンスの構成

高速コンバージェンス機能は、Cisco Nexus 9000 シリーズ プラットフォームでサポートされています。このコマンドを使用して、vPC の最適化を有効または無効にすることができます。より高速なコンバージェンスを実現するには、両方の vPC ピアで **[no] fast-convergence** を有効にして、高速コンバージェンスを実現する必要があります。最適化は、セカンダリ スイッチ、vPC メンバー ポート、および **vpc orphan-ports suspend** コマンドを使用した孤立ポートにア

■ 高速コンバージェンスの構成

カイブされます。vPC ピアリンクに障害が発生すると、これらのポートはただちに一時停止され、トラフィックはプライマリ vPC ピアに転送されます。これはコンバージェンスを向上させる目的でのみ行われます。

Cisco NX-OS リリース 7.0(3)I7(1) 以降、高速コンバージェンス機能は、Cisco Nexus 9000 シリーズプラットフォームでサポートされています。このコマンドを使用して、vPC の最適化を有効または無効にすることができます。より高速なコンバージェンスを実現するには、両方の vPC ピアで **[no] fast-convergence** を有効にして、高速コンバージェンスを実現する必要があります。最適化は、セカンダリ スイッチ、vPC メンバー ポート、および **vpc orphan-ports suspend** コマンドを使用した孤立ポートにアーカイブされます。vPC ピアリンクに障害が発生すると、これらのポートはただちに一時停止され、トラフィックはプライマリ vPC ピアに転送されます。これはコンバージェンスを向上させる目的でのみ行われます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal	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) # vpc domain <domain>	VPC ドメイン番号の構成
ステップ 3	switch(config) # peer-switch	ピア スイッチを定義します。
ステップ 4	switch(config) # show vpc peer-keepalive	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。
ステップ 5	switch(config) # delay restore { time }	復元された vPC ピアデバイスが稼働するまで遅延時間（単位は秒）です。値の範囲は 1 ~ 3600 です。
ステップ 6	switch(config) # peer-gateway	仮想ポート チャネル（vPC）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転送をイネーブルにするには、ピアゲートウェイ コマンドを使用します。レイヤ3フォワーディング パケットを無効にするには、このコマンドの no 形式を使用します。
ステップ 7	switch(config) # delay restore orphan-port	復元されたデバイスの孤立ポートがアップするまでの遅延秒数
ステップ 8	switch(config-vpc-domain)# fast-convergence	vPC 高速コンバージェンスを構成します。

LACP vPC コンバージェンスの構成

Cisco NX-OS リリース 7.0 (3) I7 (1) 以降、Link Aggregation Control Protocol (LACP) vPC コンバージェンス機能は、Cisco Nexus 9200 および 9300 シリーズスイッチでサポートされます。LACP vPC コンバージェンス機能を構成して、メンバーリンクがダウンして最初のメンバーが起動する際の vPC ポートチャネルのコンバージェンス時間を短縮することで、ポートチャネルをより効率的に使用できます。

Cisco NX-OS リリース 7.0(3)I7(5) 以降、Link Aggregation Control Protocol (LACP) vPC コンバージェンス機能は、9700-EX および 9700-FX ラインカードを搭載した Cisco Nexus 9500 シリーズスイッチでサポートされます。この機能は、9400、9500、および 9600 および 9600-R ラインカードを搭載した Nexus 9500 ではサポートされません。

Link Aggregation Control Protocol (LACP) vPC コンバージェンス機能は、9700-EX および 9700-FX ラインカードを搭載した Cisco Nexus 9500 シリーズスイッチでサポートされます。この機能は、9400、9500、および 9600 および 9600-R ラインカードを搭載した Nexus 9500 ではサポートされません。

Link Aggregation Control Protocol (LACP) vPC コンバージェンス機能は、Cisco Nexus 9200 および 9300 シリーズスイッチでサポートされます。LACP vPC コンバージェンス機能を構成して、メンバーリンクがダウンして最初のメンバーが起動する際の vPC ポートチャネルのコンバージェンス時間を短縮することで、ポートチャネルをより効率的に使用できます。

Cisco Nexus 9000 スイッチで LACP vPC コンバージェンスを構成すると、すべての VLAN が初期化およびプログラムされるまで待機してから、LACP 同期 PDU を送信します。これにより、ドロップすることなく VPC ドメインへのトラフィックの送信が開始されます。LACP をサポートするホストへの vPC ポートチャネルを持つ VXLAN および 非 VXLAN 環境で **lacp vpc-convergence** コマンドを構成することができます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal	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) # interface {type/slot portchannel number}	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 3	switch(config-if) # lacp vpc-convergence	<p>LACP コンバージェンスの構成します。メンバーリンクがダウンして最初のメンバーがアップするための vPC ポートチャネルのコンバージェンス時間を短縮します。</p> <p>(注) 両方の vPC ピアスイッチでこのコマンドをイネーブルにする必要があります。</p>

■ グレースフル整合性検査の設定

	コマンドまたはアクション	目的
		<p>このコマンドは、 PortFast ポート（スパンニングツリー ポート タイプ エッジ [トランク] が有効になっている vPC ポート チャネル）でのみ構成する必要があります。</p> <p>（注） vPC 環境では、 LACP をサポートするデバイスへの vPC ポート チャネル インターフェイスでこのコマンドが構成されておらず、 vPC ピアの 1 つがリロードされるか、リンクの 1 つが起動すると、「アップ」状態の vPC ピア スイッチはアクティブなままで、トラフィックを転送します。他のリンクがダウンする可能性があり、「アップ」状態に移行します。「アップ」状態に移行しているリンクは、 VLAN の初期化を開始します。 VLAN が初期化されると、初期化された VLAN ごとに LACP 同期 PDU が送信されます。これにより、ポート チャネルが「アップ」状態になり、理想的でない VLAN でトラフィックのブラックホールが発生します。</p>

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

	コマンドまたはアクション	目的
ステップ 1	configure terminal 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。

	コマンドまたはアクション	目的
ステップ 2	vpc domain domain-id [shut no shut] 例： switch(config-if)# vpc domain 5 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	graceful consistency-check 例： switch(config-vpc-domain)# graceful consistency-check	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 no 形式を使用します。
ステップ 4	exit 例： switch(config)# exit switch#	vpc-domain 設定 モードを終了します。
ステップ 5	show vpc brief 例： switch# show vpc brief	(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 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

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例：	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。

他のポート チャネルの vPC への移行

	コマンドまたはアクション	目的
	switch# configure terminal switch(config)#	
ステップ 2	show vpc consistency-parameters {global interface port-channel channel-number} 例： switch(config)# show vpc consistency-parameters global switch(config)#	(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。

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 の作成時にトライフィックが中断されることはありません。

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

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例：	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
	switch# configure terminal switch(config)#	
ステップ 2	interface port-channel channel-number 例： switch(config)# interface port-channel 20 switch(config-if)#	ダウンストリーム デバイスに接続するため vPC に入るポート 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	vpc number 例： switch(config-if)# vpc 5 switch(config-vpc-domain)#	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。 (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。
ステップ 4	exit 例： switch(config)# exit switch#	vpc-domain 設定モードを終了します。
ステップ 5	show vpc brief 例： switch# show vpc brief	(任意) vPC に関する情報を表示します。
ステップ 6	copy running-config startup-config 例： switch# copy running-config startup-config	(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 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

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal 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	vpc domain domain-id [shut no shut] 例： switch(config)# vpc domain 5 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	system-mac mac-address 例： switch(config-vpc-domain)# system-mac 23fb.4ab5.4c4e 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 aaaa.bbbb.cccc の形式で入力します。
ステップ 4	exit 例： switch(config-vpc-domain)# exit switch#	vpc-domain 設定 モードを終了します。
ステップ 5	show vpc role 例： switch# show vpc brief	(任意) vPC システム MAC アドレスを表示します。
ステップ 6	copy running-config startup-config 例： switch# copy running-config startup-config	(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

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal 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	vpc domain domain-id [shut no shut] 例： switch(config)# vpc domain 5 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	system-priority priority 例： switch(config-vpc-domain)# system-priority 4000 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。

■ vPC ピア デバイス ロールの手動での設定

	コマンドまたはアクション	目的
ステップ 4	exit 例： <pre>switch(config-vpc-domain) # exit switch#</pre>	vpc-domain 設定モードを終了します。
ステップ 5	show vpc role 例： <pre>switch# show vpc role</pre>	(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	copy running-config startup-config 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。

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プ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

	コマンドまたはアクション	目的
ステップ1	configure terminal 例： switch# configure terminal 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	vpc domain domain-id [shut no shut] 例： switch(config)# vpc domain 5 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	role priority priority 例： switch(config-vpc-domain)# role priority 4 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	exit 例： switch(config)# exit switch#	vpc-domain 設定 モードを終了します。
ステップ5	show vpc role 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	copy running-config startup-config 例： switch# copy running-config startup-config	(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)#[/pre]
```

■ 停電後のリカバリの設定

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 3550-T 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。

リロード復元の設定

この項で説明している **reload restore** コマンドおよび手順は廃止されます。代わりに、**auto-recovery** コマンドおよび手順を使用することを推奨します。

Cisco Nexus 3550-T 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、**reload restore** 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。

始める前に

vPC 機能が有効なことを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal 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	vpc domain domain-id [shut no shut] 例： switch(config)# vpc domain 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	reload restore [delay time-out] 例： switch(config-vpc-domain)# reload restore	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ます。デフォルト遅延値は 240 秒です。タイムアウト遅延は 240 ~ 3600 秒の間で設定できます。 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 no 形式を使用します。
ステップ 4	exit 例： switch(config-vpc-domain)# exit switch#	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
ステップ 5	show running-config vpc 例： switch# show running-config vpc	(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	show vpc consistency-parameters interface port-channel number 例： switch# show vpc consistency-parameters interface port-channel 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	copy running-config startup-config 例： switch# copy running-config startup-config	(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。 (注) リロード機能がインエ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 リロード復元機能を設定し、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)# reload restore

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

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

!Command: show running-config vpc
!Time: Wed Mar 24 18:43:54 2010
version 5.0(2)
feature vpc
logging level vpc 6
vpc domain 5
reload restore
```

次の例は、一貫性パラメータを確認する方法を示します。

```
switch# show vpc consistency-parameters interface port-channel 1

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

■ 自動リカバリの設定

```
Name Type Local Value Peer Value
-----
STP Port Type 1 Default -
STP Port Guard 1 None -
STP MST Simulate PVST 1 Default -
mode 1 on -
Speed 1 1000 Mb/s -
Duplex 1 full -
Port Mode 1 trunk -
Native Vlan 1 1 -
MTU 1 1500 -
Allowed VLANs - 1-3967,4048-4093
Local suspended VLANs
```

自動リカバリの設定

Cisco Nexus 3550-T 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 3550-T 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。

始める前に

vPC 機能が有効なことを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 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	vpc domain domain-id [shut no shut] 例 : <pre>switch(config)# vpc domain 5 switch(config-vpc-domain) #</pre>	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	auto-recovery [reload-delay time] 例 : <pre>switch(config-vpc-domain) # auto-recovery</pre>	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

	コマンドまたはアクション	目的
		ト遲延値は 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 no 形式を使用します。
ステップ 4	exit 例： switch(config-vpc-domain) # exit switch#	vpc-domain 設定モードを終了します。
ステップ 5	show running-config vpc 例： switch# show running-config vpc	(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	show vpc consistency-parameters interface port-channel number 例： switch# show vpc consistency-parameters interface port-channel 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	copy running-config startup-config 例： switch# copy running-config startup-config	(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。 (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
```

■ 孤立ポートの一時停止の設定

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えてセカンダリ 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 チャネルでのみ設定できます。ただし、個々のポート チャネル 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

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal 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	show vpc orphan-ports 例： switch# show vpc orphan-ports	(任意) 孤立ポートのリストを表示します。
ステップ 3	interface type slot/port 例： switch(config)# interface ethernet 1/3 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	vpc orphan-port suspend 例： switch(config-if)# vpc orphan-ports suspend	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	exit 例： switch(config-if)# exit 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。

	コマンドまたはアクション	目的
ステップ 6	copy running-config startup-config 例： switch# copy running-config startup-config	(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、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 1/3
switch(config-if)# vpc orphan-ports suspend
switch(config-if)# exit
switch(config)#
```

孤立ポートでの遅延復元の構成

Cisco Nexus 9000 シリーズスイッチで **delay restore orphan-port** コマンドを構成すると、Cisco NX-OS リリース 7.0 (3) I7 (1) 以降、復元されたデバイスの孤立ポートの起動を遅らせる復元タイマーを構成できます。

Cisco Nexus 9000 シリーズスイッチで **delay restore orphan-port** コマンドを構成すると、復元されたデバイスの孤立ポートの起動を遅らせる復元タイマーを構成できます。



(注) **delay restore orphan-port suspend** コマンドは、**vpc orphan-port suspend** コマンドが構成されているインターフェイスにのみ適用されます。他の孤立ポートがデバイスの稼働を遅らせることはありません。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal	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) # vpc domain <domain>	VPC ドメイン番号の構成
ステップ 3	switch(config) # peer-switch	ピアスイッチを定義します。
ステップ 4	switch(config) # show vpc peer-keepalive	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。

■ vPC ピアスイッチの設定

	コマンドまたはアクション	目的
ステップ 5	switch(config) # delay restore { time }	復元された vPC ピアデバイスが稼働するまで遅延時間（単位は秒）です。値の範囲は 1 ~ 3600 です。
ステップ 6	switch(config) # peer-gateway	仮想ポートチャネル（vPC）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転送をイネーブルにするには、ピアゲートウェイコマンドを使用します。レイヤ3フォワーディングパケットを無効にするには、このコマンドの no 形式を使用します。
ステップ 7	switch(config) # delay restore orphan-port	復元されたデバイスの孤立ポートがアップするまでの遅延秒数

vPC ピアスイッチの設定

Cisco Nexus 3550-T 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構成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

	コマンドまたはアクション	目的
ステップ 1	configure terminal 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。

	コマンドまたはアクション	目的
ステップ 2	vpc domain domain-id [shut no shut] 例： switch(config)# vpc domain 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	peer-switch 例： switch(config-vpc-domain)# peer-switch	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なります。 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 no 形式を使用します。
ステップ 4	spanning-tree vlan vlan-range priority value 例： switch(config)# spanning-tree vlan 1 priority 8192	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	exit 例： switch(config-vpc-domain)# exit switch#	vpc-domain 設定モードを終了します。
ステップ 6	show spanning-tree summary 例： switch# show spanning-tree summary	(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	copy running-config startup-config 例： switch# copy running-config startup-config	(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_PEER_SWITCH_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
```

ヒットレス vPC ロール変更の設定

```
switch(config-vpc-domain) # exit
switch(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

	コマンドまたはアクション	目的
ステップ 1	vpc role preempt 例： <pre>switch# vpc role preempt switch(config) #</pre>	ヒットレス vPC ロールの変更を有効にします。
ステップ 2	show vpc role 例： <pre>switch(config) # show vpc role</pre>	(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 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
show feature	vPC がイネーブルになっているかどうかを表示します。
show vpc brief	vPC に関する要約情報を表示します。
show vpc consistency-parameters	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。

コマンド	目的
show running-config vpc	vPC の実行コンフィギュレーションの情報を表示します。
show port-channel capacity	設定されているポートチャネルの数、およびデバイス上でまだ使用可能なポートチャネル数を表示します。
show vpc statistics	vPC に関する統計情報を表示します。
show vpc peer-keepalive	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。
show vpc role	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。

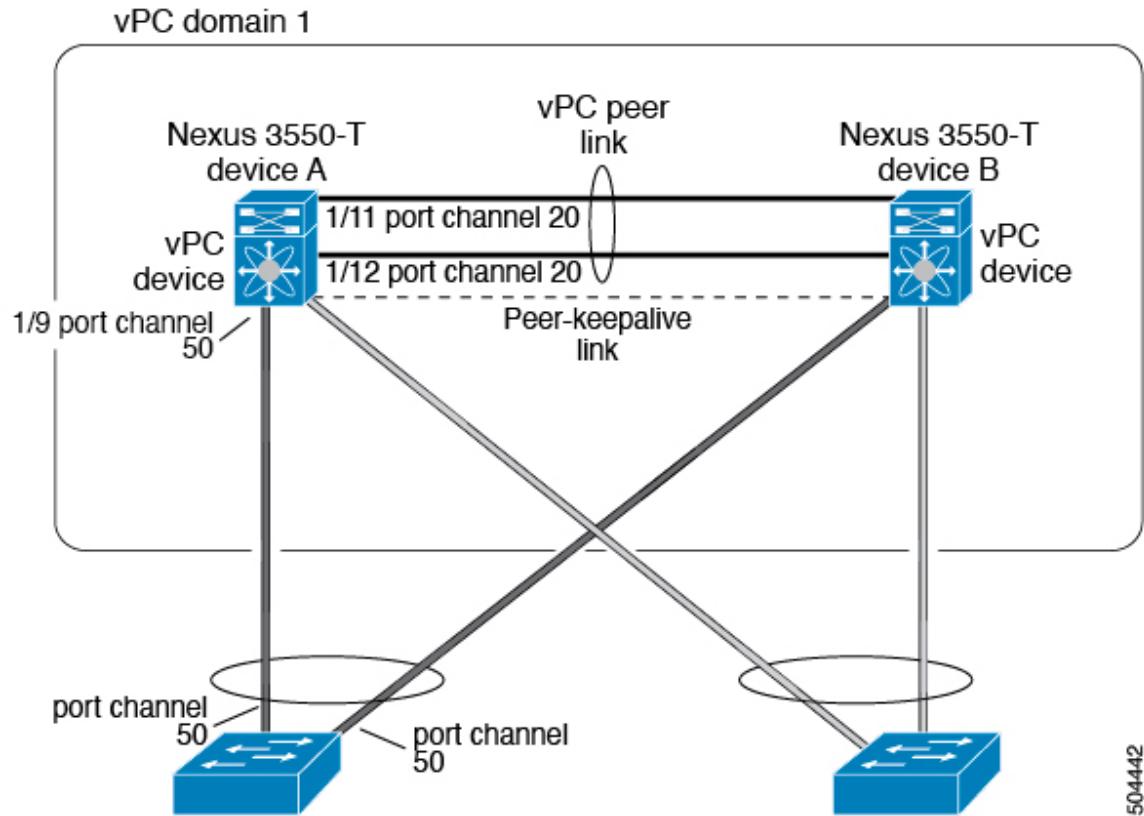


(注) このコマンドは、現在作業している vPC ピア デバイスの vPC 統計情報しか表示しません。

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 16: vPC の設定例



504442

- 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
```

- (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 1/7,
ethernet 1/3, ethernet 1/5. ethernet 1/7
switch(config-if)# shutdown
switch(config-if)# exit
switch(config)# interface ethernet 1/7

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

- (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 1/2, ethernet 1/4,
ethernet 1/6. ethernet 1/8
switch(config-if)# shutdown
switch(config-if)# exit
switch(config)# interface ethernet 1/2
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)#
```

vPC の設定例

4. vPC ピア リンクに入る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 チャネルに構成します。

```
switch(config)# interface ethernet 1/1-2
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 1/20
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 1/9
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。

■ vPC の設定例

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。