Cisco Nexus 3550-T NX-OS インターフェイス構成ガイド、リリース 10.6(x)

最終更新：2025 年 12 月 11 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

はじめに

この前書きは、次の項で構成されています。

対象読者

このマニュアルは、Cisco Nexus スイッチの設置、設定、および維持に携わるネットワーク管理者を対象としています。

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x | y]	いずれか1つを選択できる省略可能なキーワードや引数は、角かっこで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。

表記法	説明
[x {y | z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しないでください。引用符を使用すると、その引用符も含めて string と見なされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコ（< >）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

Cisco Nexus 3550-T スイッチの関連資料

Cisco Nexus 3550-T スイッチ全体のマニュアル セットは、次の URL にあります。

https://www.cisco.com/c/en/us/support/switches/nexus-3550-series/series.html

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

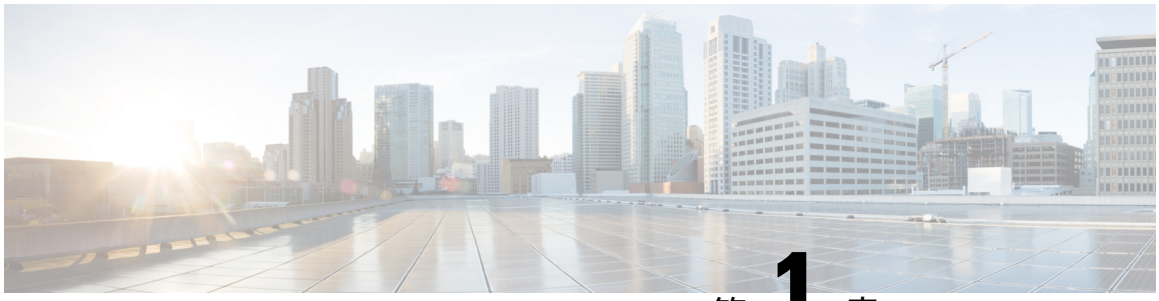
通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

Cisco バグ検索ツール

Cisco Bug Search Tool（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

通信、サービス、およびその他の情報



第 1 章

新機能および変更された機能に関する情報

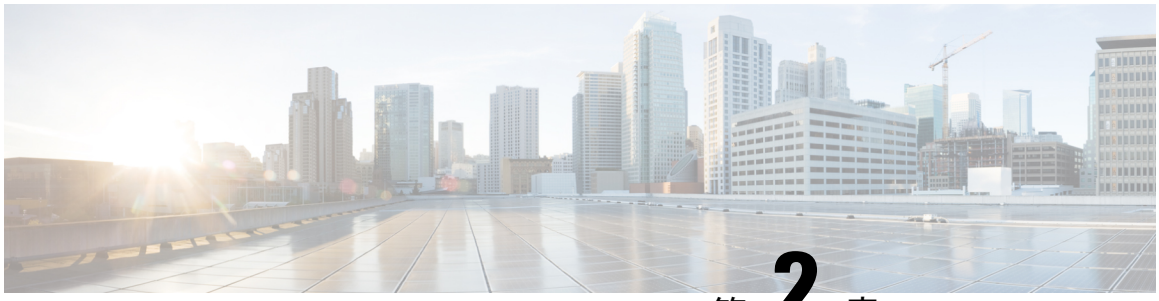
ここでは、このリリースで追加および変更された情報を示します。

新機能および変更された機能に関する情報

表 *1 : Cisco Nexus 3550-T NX-OS* リリース *10.6(x)* の新機能および変更された機能に関する情報

特長	説明	変更が行われたリリース	参照先
NA	このリリースでは、新しい機能はサポートされていません。	10.6(1)F	N/A

新機能および変更された機能に関する情報



第 2 章

『Interfaces Configuration Guide』

この前書きは、次の項で構成されています。

インターフェイスについて

Cisco NX-OS は、サポート対象の各インターフェイス タイプの複数の設定パラメータをサポートします。ほとんどのパラメータはこのマニュアルで説明しますが、一部は他のマニュアルで説明します。

イーサネット インターフェイス

イーサネット インターフェイスには、ルーテッド ポートが含まれます。

Cisco Nexus® 3550-T スイッチには、次の注意事項と制限事項があります。

- 同じクワッド内では混合速度はサポートされません。

アクセス ポート

アクセス ポートは 1 つの VLAN のトラフィックを送受信します。このポートのタイプはレイヤ 2 インターフェイスだけです。

アクセス ポートの詳細については、「アクセス インターフェイスとトランク インターフェイスについて」の項を参照してください。

ルーテッド ポート

ルーテッドポートは、IP トラフィックを他のデバイスにルーティングできる物理ポートです。ルーテッド ポートはレイヤ 3 インターフェイスだけです。

ルーテッド ポートの詳細については、「ルーテッド インターフェイス」のセクションを参照してください。

管理インターフェイス

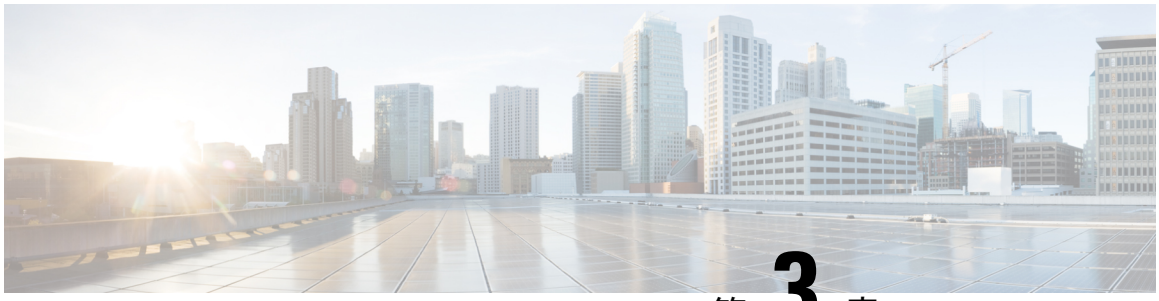
管理イーサネットインターフェイスを使用して、Telnetクライアント、簡易ネットワーク管理プロトコル（SNMP）、その他の管理エージェントを使用するリモート管理用ネットワークにデバイスを接続できます。管理ポート（mgmt0）は、自動検知であり、1000 Mb/s の速度の全二重モードで動作します。

ポートチャネル インターフェイス

ポートチャネルは、複数の物理インターフェイスを集約した論理インターフェイスです。最大8の物理ポートへの個別リンクを1つのポート チャネルにバンドルして、帯域幅と冗長性を向上させることができます。ポート チャネリングにより、これらの物理インターフェイス チャネルのトラフィックをロード バランスさせることもできます。ポート チャネル インターフェイスの詳細については、「ポート チャネルの構成」のセクションを参照してください。

ループバック インターフェイス

仮想ループバック インターフェイスは、常にアップ状態にあるシングル エンドポイントを持つ仮想インターフェイスです。パケットが仮想ループバック インターフェイスを通じて送信されると、仮想ループバック インターフェイスですぐに受信されます。ループバック インターフェイスは物理インターフェイスをエミュレートします。



第 3 章

スタティックおよびダイナミック NAT 変換の設定

ネットワーク アドレス変換の概要

ネットワークアドレス変換（NAT）は、登録されていないIPアドレスを使用してインターネットへ接続するプライベート IP インターネットワークをイネーブルにします。NAT はデバイス（通常、2 つのネットワークを接続するもの）で動作し、パケットを別のネットワークに転送する前に、社内ネットワークの（グローバルに一意のアドレスではなく）プライベート IP アドレスを正規の IP アドレスに変換します。NAT は、ネットワーク全体に対して 1 つの IP アドレスだけを外部にアドバタイズするように設定できます。この機能により、1 つの IP アドレスの後ろに内部ネットワーク全体を効果的に隠すことで、セキュリティが強化されます。

NAT が設定されたデバイスには、内部ネットワークと外部ネットワークのそれぞれに接続するインターフェイスが少なくとも 1 つずつあります。標準的な環境では、NAT はスタブ ドメインとバックボーンの間の出口ルータに設定されます。パケットがドメインから出て行くとき、NAT はローカルで意味のある送信元 アドレスをグローバルで一意の アドレスに変換します。パケットがドメインに入ってくる際は、NAT はグローバルに一意な宛先アドレスをローカル アドレスに変換します。出口点が複数存在する場合、個々の NAT は同じ変換テーブルを持っている必要があります。

NAT は RFC 1631 に記述されています。

スタティック NAT に関する情報

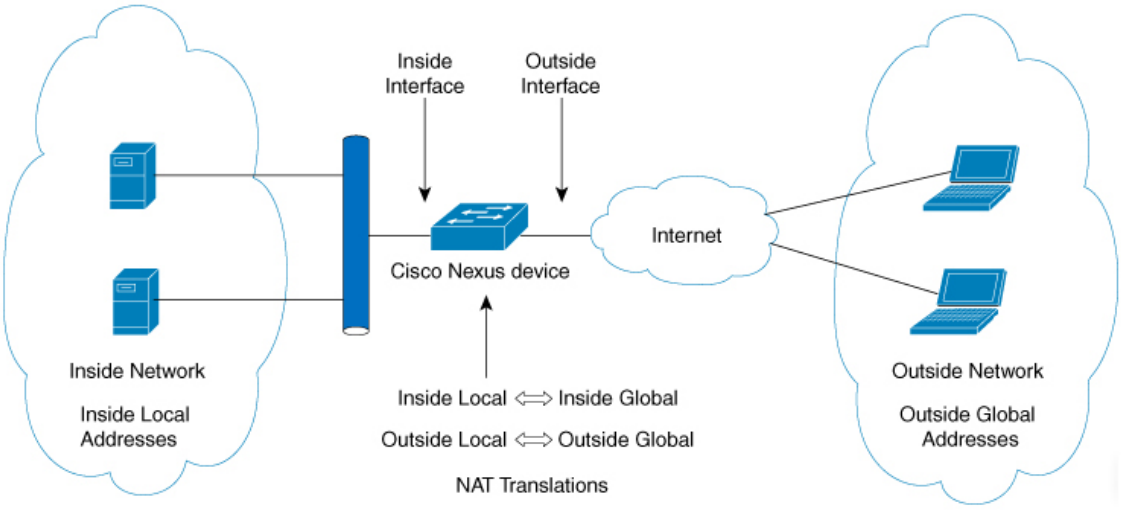
静的ネットワーク アドレス変換（NAT）を使用すると、ユーザは内部ローカル IP アドレスから内部グローバル IP アドレスへの 1 対 1 変換を構成することができます。これにより、内部から外部トラフィックおよび外部から内部トラフィックへの IP アドレスとポート番号の両方の変換が可能になります。Cisco Nexus デバイスはヒットレス NAT をサポートします。これは、既存の NAT トラフィック フローに影響を与えずに NAT 構成で NAT 変換を追加または削除できることを意味します。

スタティック NAT では、プライベート アドレスからパブリック アドレスへの固定変換が作成されます。スタティック NAT では 1 対 1 ベースでアドレスが割り当てられるため、プライベート アドレスと同じ数のパブリック アドレスが必要です。スタティック NAT では、パブリック アドレスは連続する各接続で同じであり、永続的な変換規則が存在するため、宛先ネットワークのホストは変換済みのホストへのトラフィックを開始できます（そのトラフィックを許可するアクセス リストがある場合）。

静的または、ダイナミック NAT の主な違いは、ダイナミック NAT の場合、変換対象のトラフィックデバイスに受信するまでは、NAT 変換テーブルには変換エントリが存在しません。ダイナミック変換は、新しいエントリ用のスペースを確保するために使用されていない場合、クリアまたはタイムアウトされます。静的エントリは、トラフィックを受信するデバイスに関係なく、常に存在します。ただし、静的 NAT とダイナミック NATの両方で、各ホストは、オーバーロードなどのさまざまな構成に基づいて、後続の変換ごとに異なるアドレスまたはポートを使用できます。

次の図に、一般的なスタティック NAT のシナリオを示します。変換は常にアクティブであるため、変換対象ホストとリモート ホストの両方で接続を生成でき、マップ アドレスは **static** コマンドによって静的に割り当てられます。

図 *1*:スタティック *NAT*



次に、スタティック NAT を理解するのに役立つ主な用語を示します。

- NAT の内部インターフェイス：プライベート ネットワークに面するレイヤ 3 インターフェイス。
- NAT の外部インターフェイス：パブリック ネットワークに面するレイヤ 3 インターフェイス。
- ローカルアドレス：ネットワークの内部（プライベート）部分に表示される任意のアドレス。
- グローバルアドレス：ネットワークの外部（パブリック）部分に表示される任意のアドレス。
- 正規の IP アドレス：Network Information Center（NIC）やサービス プロバイダーにより割り当てられたアドレス。
- 内部ローカル アドレス：内部ネットワーク上のホストに割り当てられた IP アドレス。このアドレスは正規の IP アドレスである必要はありません。
- 外部ローカル アドレス：内部ネットワークから見た外部ホストの IP アドレス。これは、内部ネットワークのルーティング可能なアドレス空間から割り当てられるため、正規のアドレスである必要はありません。
- 内部グローバルアドレス：1 つ以上の内部ローカル IP アドレスを外部に対して表すために使用できる正規の IP アドレス。
- 外部グローバル アドレス：ホスト所有者が外部ネットワーク上のホストに割り当てる IP アドレス。このアドレスは、ルート可能なアドレスまたはネットワーク空間から割り当てられた正規のアドレスです。

ダイナミック NAT の概要

ダイナミック ネットワーク アドレス変換（NAT）では、実際のアドレスのグループは、接続先ネットワーク上でルーティング可能なマッピング アドレスのプールに変換されます。またダイナミック NAT では、未登録の IP アドレスと登録済み IP アドレス間で一対一のマッピング確立しますが、通信時にプール内で利用可能な登録済みアドレスによって、マッピングは変化します。

ダイナミック NAT を設定自動Aすると、使用している内部ネットワークと外部ネットワークまたはインターネット間に、ファイウォールが構築されます。ダイナミックNATは、スタブドメイン内で発信された接続のみを許可します。外部ネットワーク上のデバイスは、接続を開始していない限り、ネットワーク内のデバイスに接続できません。

ダイナミック NAT の場合、変換対象のトラフィックデバイスに受信するまでは、NAT 変換テーブルには変換エントリが存在しません。ダイナミック変換は、新しいエントリ用のスペースを確保するために使用されていない場合、クリアまたはタイムアウトされます。通常、NAT 変換エントリはタイマーに基づいてクリアされます。ダイナミック NAT 変換のデフォルトの最小タイムアウトは 3600 秒です。

（注） この項で説明している **ip nat translation sampling-timeout** コマンドはサポートされていません。統計情報はインストール済みの NAT ポリシーに 60 秒ごとに収集されます。これらの統計情報はフローがアクティブかまたはアクティブでないかを決定するために使用されます。

ダイナミックNATは、ポートアドレス変換（PAT）およびアクセスコントロールリスト（ACL）をサポートします。PAT（暗号化ともいう）、オーバーロードは未登録の複数の IP アドレスを、さまざまなポートを使うことによって、登録済みの単一の IP アドレスにマッピングするダイナミック NAT の 1 形態です。

タイムアウトメカニズム

ダイナミック NAT 変換を作成した後は、特に TCAM エントリの数が制限されている場合、新しい変換を作成できるように、使用していないものをクリアする必要があります。このリリースでは、syn-timeout および finrst-timeout がサポートされています。スイッチでは、次のNAT変換タイムアウトタイマーがサポートされています。

スイッチでは、次のNAT変換タイムアウトタイマーがサポートされています。

- syn-timeout：TCPデータのパケットタイムアウト値。SYNリクエストを送信後、SYN-ACK応答を受信するまでの最大待ち時間です。タイムアウト値の範囲は、1～172800秒です。デフォルト値は 60 秒です。
- finrst-timeout ：RST またはFINパケットの受信によって接続が終了したときのフローエントリのタイムアウト値。RSTパケットとFINパケットの両方の動作を設定するには、同じキーワードを使用します。タイムアウト値の範囲は、1～172800秒です。デフォルト値は 60 秒です。

  接続が確立された後に SYN パケット（SYN >SYN-ACK >FIN）が受信されると、finrst タイマーが開始されます。

  相手側からFIN-ACKを受信すると、変換エントリはすぐにクリアされます。それ以外の場合は、タイムアウト値の完了後にクリアされます。

  接続が確立された後にRSTパケットを受信した場合（SYN>SYN-ACK>RST）、変換エントリはすぐにクリアされます。
- tcp-timeout：TCP 変換のタイムアウト値。3 ウェイ ハンドシェイク（SYN、SYN-ACK、ACK）の後に確立した接続の最大待ち時間です。接続が確立された後にアクティブ フローが発生しない場合、変換は設定されたタイム アウト値に従って期限切れになります。

  タイムアウト値の範囲は、60 ～ 172800 秒です。デフォルトは、3600 秒です。
- udp-timeout：すべての NAT UDP パケットのタイムアウト値。

  タイムアウト値の範囲は、60 ～ 172800 秒です。デフォルトは、3600 秒です。
- timeout：ダイナミック NAT 変換のタイムアウト値。

タイムアウト値の範囲は、60 ～ 172800 秒です。デフォルトは、3600 秒です。

- icmp-timeout：ICMP パケットのタイムアウト値。

  タイムアウト値の範囲は、60 ～ 172800 秒です。デフォルトは、3600 秒です。

（注） 構成されたタイムアウトのないダイナミック エントリを作成すると、3600 秒のデフォルトのタイムアウトが使用されます。デフォルトのタイムアウト値を新しい値に変更した後に作成された変換エントリは、最新のタイムアウト値を取得します。

NAT の内部アドレスおよび外部アドレス

NAT 内部とは、変換を必要とする組織が所有するネットワークを指します。NAT が設定されている場合、このネットワーク内のホストは、別の空間（グローバルアドレス空間として知られている）にあるものとしてネットワークの外側に現れる 1 つ空間（ローカルアドレス空間として知られている）内のアドレスを持つことになります。

同様に、NAT 外部とは、スタブ ネットワークが接続するネットワークを指します。通常、組織の管理下にはありません。外部ネットワーク内のホストを変換の対象にすることもできるため、これらのホストもローカル アドレスとグローバル アドレスを持つことができます。

NAT では、次の定義が使用されます。

- ローカル アドレス：ネットワークの内側部分に表示されるローカルな IP アドレスです。
- グローバル アドレス：ネットワークの外側部分に表示されるグローバルな IP アドレスです。
- 内部ローカル アドレス：内部ネットワーク上のホストに割り当てられた IP アドレス。このアドレスは、多くの場合、インターネット ネットワーク情報センター（InterNIC）やサービス プロバイダーにより割り当てられた正規の IP アドレスではありません。
- 内部グローバル アドレス：外部に向けて、1 つ以上の内部ローカル IP アドレスを表現した正規の IP アドレス（InterNIC またはサービス プロバイダーにより割り当てられたもの）。
- 外部ローカル アドレス：内部ネットワークから見た外部ホストの IP アドレス。必ずしも正規のアドレスでありません。内部でルート可能なアドレス空間から割り当てられたものです。
- 外部グローバルアドレス：外部ネットワークに存在するホストに対して、ホストの所有者により割り当てられた IP アドレス。このアドレスは、グローバルにルート可能なアドレス、またはネットワーク空間から割り当てられたものです。

ダイナミック NAT のプール サポート

Cisco NX-OS は、ダイナミック NAT のプールをサポートします。ダイナミック NAT を使用すると、グローバル アドレスのプールを設定して、新しい変換ごとにプールからグローバル アドレスを動的に割り当てることができます。アドレスは、セッションが期限切れになるか、閉じられた後にプールに返されます。これにより、要件に基づいてアドレスをより効率的に使用できます。

PAT のサポートには、グローバル アドレス プールの使用が含まれます。これにより、IP アドレスの使用率がさらに最適化されます。PAT は、ポート番号を使用して、一度に 1 つの IP アドレスを使い果たします。ポートが該当グループで見つけられなかった場合や、複数の IP アドレスが設定されている場合、PAT は次の IP アドレスに移動して、ユーザー定義プールに基づいて、（ソース ポートを無視するか、それを保存しようと試みて）割り当てを取得します。

ダイナミック NAT および PAT では、各ホストは変換するたびに異なるアドレスまたはポートを使用します。ダイナミック NAT とスタティック NAT の主な違いは、スタティック NAT ではリモート ホストが変換済みのホストへの接続を開始でき（それを許可するアクセス リストがある場合）、ダイナミック NAT では開始できないという点です。

静的およびダイナミック NAT の注意事項および制約事項

スタティック NAT 設定時の注意事項および制約事項は、次のとおりです。

- NAT は、IPv4 ユニキャストだけでサポートされています。
- 変換された IP が、外部インターフェイス サブネットの一部である場合、NAT の外部インターフェイスで **ip proxy-arp** コマンドを使用します。**add-route** キーワードを使用する場合は、**ip proxy-arp** を有効にする必要があります。
- Cisco Nexus デバイスは、次のインターフェイスタイプで NAT をサポートします。
  - スイッチ仮想インターフェイス（SVI）
  - 物理層レイヤ 3 インターフェイス
  - ポート チャンネル レイヤ 3 インターフェイス
- 非 TCP/UDP パケットは、常にソフトウェア変換されます。
- 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**
- IP アドレスがスタティック NAT 変換または PAT 変換に使用される場合、他の目的には使用できません。たとえば、インターフェイスに割り当てることはできません。
- （100 を超える）多数の変換を設定する場合、変換を設定してから NAT インターフェイスを設定する方が迅速に設定できます。
- Twice NAT はサポートされていません。

- NAT の内部ルールと外部ルールを同時に構成することはサポートされていません。
- IP NAT 内部または IP NAT 外部などの NAT 構成は、ループバック インターフェイスではサポートされていません。

ダイナミック NAT の制約事項

ダイナミックネットワークアドレス変換（NAT）には、次の制約事項が適用されます。

- 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**
- VXLANルーティングはCisco Nexusデバイスではサポートされません。
- フラグメント化されたパケットはサポートされません。
- アプリケーション層ゲートウェイ（ALG）変換はサポートされていません。ALG、またはアプリケーションレベル ゲートウェイは、アプリケーション パケットのペイロード内の IP アドレス情報を変換するアプリケーションです。
- 出力 ACL は、変換されたパケットには適用されません。
- MIB はサポートされていません。
- Cisco Data Center Network Manager（DCNM）はサポートされていません。
- Cisco Nexusデバイスでは、複数のグローバル仮想デバイスコンテキスト（VDC）はサポートされていません。
- ダイナミックNAT変換は、アクティブデバイスおよびスタンバイデバイスと同期されません。
- ステートフルNATはサポートされていません。ただし、NATとHot Standby Router Protocol（HSRP）は共存できます。
- のタイムアウト値は、設定されたタイムアウト+ 119秒までかかります。
- ダイナミックNATでは、プールのオーバーロードとインターフェイスのオーバーロードは外部NATではサポートされません。
- Cisco Nexus デバイスは、インターフェイス上で同時に設定された NAT および VLAN アクセス コントロール リスト（VACL）。
- [ip nat 内部（ip nat inside）] または [ip nat 外部（ip nat outside）] などの NAT 構成は、ループバック インターフェイスではサポートされていません。

スタティック NAT の設定

スタティック NAT のイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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)# **feature nat**	デバイス上でスタティック NAT 機能をイネーブルにします。
ステップ 3	switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に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て、変更を継続的に保存します。

インターフェイスでの NAT の構成

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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/port*	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)# **ip nat** {**inside** | **outside**}	内部または外部としてインターフェイスを指定します。 （注） マーク付きインターフェイスに到着したパケットだけが変換できます。
ステップ 4	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に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て、変更を継続的に保存します。

例

次に、内部からNATを構成する例を 2 つ示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# ip nat inside
```

```
switch# configure terminal
switch(config)# interface vlan 100
switch(config-if)# ip nat inside
```

次に、外部からNATを構成する例を 2 つ示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# ip nat outside
```

```
switch# configure terminal
switch(config)# interface vlan 102
switch(config-if)# ip nat ouside
```

内部送信元アドレスのスタティック NAT のイネーブル化

内部送信元変換の場合、パケットの送信元アドレスは、内部インターフェイスから外部インターフェイスへ変換されます。リターン トラフィックでは、宛先の内部グローバル IP アドレスが内部ローカル IP アドレスに変換されて戻されます。

（注） が、内部送信元IPアドレス（Src:ip1）を外部送信元IPアドレス（newSrc:ip2）に変換するように設定されている場合、は内部宛先IPアドレス（newDst: ip1）への外部宛先IPアドレス（Dst: ip2）の変換をCisco Nexus デバイス暗黙的に追加します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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)# **ip nat inside source static** *local-ip-address global-ip-address* [**vrf** *vrf-name*] [**match-in-vrf**] [**add-route**][**group** *group-id*]	内部グローバル アドレスを内部ローカル アドレスに、またはその逆に（内部ローカル トラフィックを内部ローカル

	コマンドまたはアクション	目的
		（local） トラフィックに）変換するようにスタティック NAT を設定します。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に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て、変更を継続的に保存します。

例

次に、内部送信元アドレスのスタティック NAT を設定する例を示します。

```
switch# configure terminal
switch(config)# ip nat inside source static 1.1.1.1 5.5.5.5
switch(config)# copy running-config startup-config
```

外部送信元アドレスのスタティック NAT のイネーブル化

外部送信元変換の場合、接続先アドレスは内部インターフェイスから外部インターフェイスに変換されます。リターン トラフィックでは、宛先の外部グローバル IP アドレスが外部ローカル IP アドレスに変換されて戻されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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)# **ip nat outside source static** *outsideGlobalIP outsideLocalIP* [**vrf** *vrf-name* [**match-in-vrf**] [**add-route**]]	外部グローバル アドレスを外部ローカル アドレスに、またはその逆に（外部ローカル トラフィックを外部グローバル トラフィックに）変換するようにスタティック NAT を設定します。ポートなしで内部変換が設定されると、暗黙的な追加ルートが実行されます。外部変換の設定中、最初の追加ルート機能はオプションです。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に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て、変更を継続的に保存します。

例

次に、外部送信元アドレスのスタティック NAT を設定する例を示します。

```
switch# configure terminal
switch(config)# ip nat outside source static 2.2.2.2 6.6.6.6
switch(config)# copy running-config startup-config
```

内部送信元アドレスのスタティック PAT の設定

ポート アドレス変換（PAT）を使用して、特定の内部ホストにサービスをマッピングできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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)# **ip nat inside source static** {*inside-local-address inside-global-address* | {**tcp**| **udp**} *inside-local-address* {*local-tcp-port* | *local-udp-port*} *inside-global-address* {*global-tcp-port* | *global-udp-port*}} {**vrf** *vrf-name* {**match-in-vrf**} }	スタティック NAT を内部ローカル ポート、内部グローバル ポートにマッピングします。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に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て、変更を継続的に保存します。

例

次に、UDP サービスを特定の内部送信元アドレスおよび UDP ポートにマッピングする例を示します。

```
switch# configure terminal
switch(config)#  ip nat inside source static udp 20.1.9.2 63 35.48.35.48 130
switch(config)# copy running-config startup-config
```

外部送信元アドレスのスタティック PAT の設定

ポート アドレス変換（PAT）を使用して、サービスを特定の外部ホストにマッピングできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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)# **ip nat outside source static** {*outside-global-address* *outside-local-address* | {**tcp** | **udp**} *outside-global-address* {*global-tcp-port* | *global-udp-port*} *outside-local-address* {*global-tcp-port* | *global-udp-port*}} {**add-route**} {**vrf** *vrf-name* {**match-in-vrf**}}	スタティック NAT を、外部グローバル ポート、外部ローカル ポートにマッピングします。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に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て、変更を継続的に保存します。

例

次に、TCP サービスを特定の外部送信元アドレスおよび TCP ポートにマッピングする例を示します。

```
switch# configure terminal
switch(config)#  ip nat outside source static tcp 20.1.9.2 63 35.48.35.48 130
switch(config)# copy running-config startup-config
```

no-alias 設定の有効化と無効化

NAT デバイスは内部グローバル（IG）アドレスと外部ローカル（OL）アドレスを所有し、これらのアドレス宛ての ARP 要求に応答します。IG/OL アドレス サブネットがローカル インターフェイス サブネットと一致すると、NAT は IP エイリアスと ARP エントリをインストールします。この場合、デバイスは local-proxy-arp を使用して ARP 要求に応答します。

no-alias 機能は、アドレス範囲が外部インターフェイスの同じサブネットにある場合、特定の NAT プール アドレス範囲からのすべての変換された IP の ARP 要求に応答します。

NAT が設定されたインターフェイスで no-alias が有効になっている場合、外部インターフェイスはサブネット内の ARP 要求に応答しません。no-alias を無効にすると、外部インターフェイスと同じサブネット内の IP に対する ARP 要求が処理されます。

（注） この機能をサポートしていない古いリリースにダウングレードすると、*no-alias* オプションの設定が削除されることがあります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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)# **feature nat**	デバイス上でスタティック NAT 機能をイネーブルにします。
ステップ 3	switch(config)# **show run nat**	NAT の設定を表示します。
ステップ 4	switch(config)# **show ip nat-alias**	エイリアスが作成されたかどうかの情報を表示します。 （注） デフォルトでは、エイリアスが作成されます。エイリアスを無効にするには、*no-alias* キーワードをコマンドに追加する必要があります。
ステップ 5	switch(config)# **clear ip nat-alias** *ip address/all*	エイリアス リストからエントリを削除します。特定のエントリを削除するには、削除する IP アドレスを指定する必要があります。すべてのエントリを削除するには、すべてのキーワードを使用します。

例

次に、すべてのインターフェイスの情報を表示する例を示します。

```
switch# configure terminal
switch(config)# show ip int b
IP Interface Status for VRF "default"(1)
Interface            IP Address      Interface Status
Lo0                  100.1.1.1       protocol-up/link-up/admin-up
Eth1/1               7.7.7.1         protocol-up/link-up/admin-up
Eth1/3               8.8.8.1         protocol-up/link-up/admin-up
```

次に、実行コンフィギュレーションの例を示します。

```
switch# configure terminal
switch(config)# show running-config nat
!Command: show running-config nat
!Running configuration last done at: Thu Aug 23 11:57:01 2018
!Time: Thu Aug 23 11:58:13 2018

version 9.2(2) Bios:version 07.64
feature nat
interface Ethernet1/1
  ip nat inside
```

```
interface Ethernet1/3
  ip nat outside
switch(config)#
```

この例は、エイリアスを設定する例を示します。

```
switch# configure terminal
switch(config)# ip nat inside source static 1.1.1.2 8.8.8.3
switch(config)# ip nat outside source static 2.2.2.1 7.7.7.3
switch(config)# show ip nat-alias
Alias Information for Context: default
Address         Interface
7.7.7.2          Ethernet1/1
8.8.8.2          Ethernet1/3
switch(config)#
```

次に、*show ip nat-alias* の出力例を示します。デフォルトでは、エイリアスが作成されます。

```
switch# configure terminal
switch(config)# show ip nat-alias
Alias Information for Context: default
Address         Interface
7.7.7.2          Ethernet1/1
8.8.8.2          Ethernet1/3
switch(config)#
```

この例は、エイリアスを無効にする方法を示します。

```
switch# configure terminal
switch(config)# ip nat inside source static 1.1.1.2 8.8.8.3 no-alias
switch(config)# ip nat outside source static 2.2.2.1 7.7.7.3 no-alias
switch(config)# show ip nat-alias
Alias Information for Context: default
Address         Interface
7.7.7.2          Ethernet1/1
8.8.8.2          Ethernet1/3
switch(config)#

** None of the entry got appended as alias is disabled for above CLIs.
switch(config)#
```

この例は、エイリアスをクリアする方法を示します。エイリアス リストからエントリを削除するには、*clear ip nat-alias* を使用します。IP アドレスを指定して 1 つのエントリを削除することも、すべてのエイリアス エントリを削除することもできます。

```
switch# configure terminal
switch(config)# clear ip nat-alias address 7.7.7.2
switch(config)# show ip nat-alias
Alias Information for Context: default
Address         Interface
8.8.8.2          Ethernet1/3
switch(config)#
switch(config)# clear ip nat-alias all
switch(config)# show ip nat-alias
switch(config)#
```

スタティック NAT および PAT の設定例

次に、スタティック NAT の設定例を示します。

```
ip nat inside source static 103.1.1.1 11.3.1.1
ip nat inside source static 139.1.1.1 11.39.1.1
ip nat inside source static 141.1.1.1 11.41.1.1
ip nat inside source static 149.1.1.1 95.1.1.1
ip nat inside source static 149.2.1.1 96.1.1.1
ip nat outside source static 95.3.1.1 95.4.1.1
ip nat outside source static 96.3.1.1 96.4.1.1
ip nat outside source static 102.1.2.1 51.1.2.1
ip nat outside source static 104.1.1.1 51.3.1.1
ip nat outside source static 140.1.1.1 51.40.1.1
```

次に、スタティック PAT の設定例を示します。

```
ip nat inside source static tcp 10.11.1.1 1 210.11.1.1 101
ip nat inside source static tcp 10.11.1.1 2 210.11.1.1 201
ip nat inside source static tcp 10.11.1.1 3 210.11.1.1 301
ip nat inside source static tcp 10.11.1.1 4 210.11.1.1 401
ip nat inside source static tcp 10.11.1.1 5 210.11.1.1 501
ip nat inside source static tcp 10.11.1.1 6 210.11.1.1 601
ip nat inside source static tcp 10.11.1.1 7 210.11.1.1 701
ip nat inside source static tcp 10.11.1.1 8 210.11.1.1 801
ip nat inside source static tcp 10.11.1.1 9 210.11.1.1 901
ip nat inside source static tcp 10.11.1.1 10 210.11.1.1 1001
ip nat inside source static tcp 10.11.1.1 11 210.11.1.1 1101
ip nat inside source static tcp 10.11.1.1 12 210.11.1.1 1201
```

スタティック NAT の設定の確認

スタティック NAT の設定を表示するには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show ip nat translations**	内部グローバル、内部ローカル、外部ローカル、および外部グローバルの各 IP アドレスを示します。

例

次に、スタティック NAT の設定を表示する例を示します。

```
switch# sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global

--- ---                ---                51.3.1.1           104.1.1.1
--- ---                ---                95.4.1.1           95.3.1.1
--- ---                ---                96.4.1.1           96.3.1.1
--- ---                ---                51.40.1.1          140.1.1.1
--- ---                ---                51.42.1.1          142.1.2.1
--- ---                ---                51.1.2.1           102.1.2.1
--- 11.1.1.1           101.1.1.1          ---                ---
--- 11.3.1.1           103.1.1.1          ---                ---
--- 11.39.1.1          139.1.1.1          ---                ---
```

```
--- 11.41.1.1          141.1.1.1          ---                ---
--- 95.1.1.1           149.1.1.1          ---                ---
--- 96.1.1.1           149.2.1.1          ---                ---
    130.1.1.1:590      30.1.1.100:5000    ---                ---
    130.2.1.1:590      30.2.1.100:5000    ---                ---
    130.3.1.1:590      30.3.1.100:5000    ---                ---
    130.4.1.1:590      30.4.1.100:5000    ---                ---
    130.1.1.1:591      30.1.1.101:5000    ---                ---


switch# sh ip nat translations verbose
Pro Inside global      Inside local       Outside local      Outside global
any ---                ---                22.1.1.3           22.1.1.2
    Flags:0x200009 time-left(secs):-1 id:0 state:0x0 grp_id:10
any 11.1.1.130         11.1.1.3           ---                ---
    Flags:0x1 time-left(secs):-1 id:0 state:0x0 grp_id:0
any 11.1.1.133         11.1.1.33          ---                ---
    Flags:0x1 time-left(secs):-1 id:0 state:0x0 grp_id:10
any 11.1.1.133         11.1.1.33          22.1.1.3           22.1.1.2
    Flags:0x200009 time-left(secs):-1 id:0 state:0x0 grp_id:0
tcp 10.1.1.100:64490   10.1.1.2:0         20.1.1.2:0         20.1.1.2:0
    Flags:0x82 time-left(secs):43192 id:31 state:0x3 grp_id:0 vrf: default
N3550T-1#
```

ダイナミック NAT の設定

ダイナミック変換および変換タイムアウトの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Switch# 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 3	**ip access-list** *access-list-name* 例： `Switch(config)# ip access-list acl1`	アクセスリストを定義し、アクセスリスト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	**permit** *protocol source source-wildcard* **any** 例：	条件に一致するトラフィックを許可する条件をIPアクセスリストに設定します。

	コマンドまたはアクション	目的
	`Switch(config-acl)# permit ip 10.111.11.0/24 any`	
ステップ 5	**deny** *protocol source source-wildcard* **any** 例： `Switch(config-acl)# deny udp 10.111.11.100/32 any`	NAT 変換を拒否する条件を設定します。
ステップ 6	**exit** 例： `Switch(config-acl)# exit`	アクセスリストコンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**ip nat inside source list** *access-list-name* **interface** *type number* [**vrf** *vrf-name* [**match-in-vrf**] [**add-route**] [**overload**] 例： `Switch(config)# ip nat inside source list acl1 interface ethernet 1/1 overload`	ステップ 3 で定義したアクセス リストを指定して、ダイナミック送信元変換を設定します。
ステップ 8	**interface** *type number* 例： `Switch(config)# interface ethernet 1/4`	インターフェイスを設定し、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 9	**ip address** *ip-address mask* 例： `Switch(config-if)# ip address 10.111.11.39 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 10	**ip nat inside** 例： `Switch(config-if)# ip nat inside`	NAT の対象である内部ネットワークにインターフェイスを接続します。 （注） ループバック インターフェイスでは構成がサポートされていません。
ステップ 11	**exit** 例： `Switch(config-if)# exit`	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、グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**interface** *type number* 例： `Switch(config)# interface ethernet 1/1`	インターフェイスを設定し、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。

	コマンドまたはアクション	目的
ステップ 13	**ip address** *ip-address mask* 例： `Switch(config-if)# ip address 172.16.232.182 255.255.255.240`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 14	**ip nat outside** 例： `Switch(config-if)# ip nat outside`	インターフェイスを外部ネットワークに接続します。 （注） ループバック インターフェイスでは構成がサポートされていません。
ステップ 15	**exit** 例： `Switch(config-if)# exit`	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、グローバル コンフィギュレーション モードに戻ります。
ステップ 16	**ip nat translation max-entries** *number-of-entries* 例： `Switch(config)# ip nat translation max-entries 300`	ダイナミック NAT 変換の最大数を指定します。エントリの数は 1 ー 1023 です。
ステップ 17	**ip nat translation timeout** *seconds* 例： `switch(config)# ip nat translation timeout 13000`	ダイナミック NAT 変換のタイムアウト値を指定します。
ステップ 18	**end** 例： `Switch(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ダイナミック NAT プールの設定

NAT プールは、単一の **ip nat pool** コマンドか、または **ip nat pool** と **address** コマンドを使用して、IP アドレスの範囲を定義することで作成できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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。

	コマンドまたはアクション	目的
ステップ 2	switch (config)# **feature nat**	デバイスの NAT 機能をイネーブルにします。
ステップ 3	switch (config)# **ip nat pool** *pool-name* [*startip endip*] {**prefix** *prefix-length* | **netmask** *network-mask*}	グローバル IP アドレスの範囲で NAT プールを作成します。IP アドレスは、プレフィックス長またはネットワークマスクを使用してフィルタリングされます。
ステップ 4	（任意） switch (config-ipnat-pool)# **address** *startip endip*	グローバル IP アドレスの範囲を指定します（プールの作成時に指定していなかった場合）。
ステップ 5	（任意） switch (config)# **no ip nat pool** *pool-name*	指定した NAT プールを削除します。

例

次に、プレフィックス長を使用して NAT プールを作成する例を示します。

```
switch# configure terminal
switch(config)# ip nat pool pool1 30.1.1.1 30.1.1.2 prefix-length 24
switch(config)#
```

次に、ネットワークマスクを使用して NAT プールを作成する例を示します。

```
switch# configure terminal
switch(config)# ip nat pool pool5 20.1.1.1 20.1.1.5 netmask 255.255.255.0
switch(config)#
```

この例では **ip nat pool** と **address** コマンドを使用してNAT プールを作成し、グローバル IP アドレスの範囲を定義します。

```
switch# configure terminal
switch(config)# ip nat pool pool7 netmask 255.255.0.0
switch(config-ipnat-pool)# address 40.1.1.1 40.1.1.5
switch(config-ipnat-pool)#
```

次の例は、NAT プールの削除方法を示します。

```
switch# configure terminal
switch(config)# no ip nat pool pool4
switch(config)#
```

送信元リストの設定

内部インターフェイスと外部インターフェイスのIPアドレスの送信元リストを設定できます。

始める前に

プールの送信元リストを設定する前に、必ずプールを設定してください。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	（任意） switch# **ip nat inside source list** *list-name* **pool** *pool-name* [**overload**]	オーバーロードの有無にかかわらず、プールを使用して NAT 内部送信元リストを作成します。
ステップ 3	（任意） switch# **ip nat outside source list** *list-name* **pool** *pool-name* [**add-route**]	オーバーロードなしでプールを使用して NAT 外部送信元リストを作成します。

例

次に、オーバーロードのないプールを使用してNAT内部送信元リストを作成する例を示します。

```
switch# configure terminal
switch(config)# ip nat inside source list list1 pool pool1
switch(config)#
```

次に、オーバーロードのあるプールを使用してNAT内部送信元リストを作成する例を示します。

```
switch# configure terminal
switch(config)# ip nat inside source list list2 pool pool2 overload
switch(config)#
```

次に、オーバーロードのないプールを使用してNAT外部送信元リストを作成する例を示します。

```
switch# configure terminal
switch(config)# ip nat outside source list list3 pool pool3
switch(config)#
```

ダイナミック NAT 変換のクリア

ダイナミック変換をクリアするには、次の作業を実行します。

コマンド	目的
clear ip nat translation [**all** | **inside** *global-ip-address local-ip-address* [**outside** *local-ip-address global-ip-address*] | **outside** *local-ip-address global-ip-address*]	すべてまたは特定のダイナミックNAT変換を削除します。

例

次に、すべてのダイナミック変換をクリアする例を示します。

```
switch# clear ip nat translation all
```

次に、内部アドレスと外部アドレスのダイナミック変換をクリアする例を示します。

```
switch# clear ip nat translation inside 2.2.2.2 4.4.4.4 outside 5.5.5.5 7.7.7.7
```

ダイナミック NAT の設定の確認

ダイナミック NAT の設定を表示するには、次の作業を行います。

コマンド	目的
show ip nat translations	アクティブなネットワーク アドレス変換（NAT）変換を表示します。 エントリが作成および使用された日時など、各変換テーブル エントリの追加情報を表示します。
show run nat	NAT の設定を表示します。
show ip nat max	アクティブなネットワーク アドレス変換（NAT）の最大値を表示します。
show ip nat statistics	NAT 統計情報をモニタします。

例

次に、IP NAT 最大値を表示する例を示します。

```
switch# show ip nat max

IP NAT Max values
====================
Max Dyn Translations:80
Max all-host:0
```

```
No.Static:0
No.Dyn:1
No.Dyn-ICMP:1
====================
Switch(config)#
```

次に、NAT 統計情報を表示する例を示します。

```
switch# show ip nat statistics

IP NAT Statistics
==================================================
Stats Collected since: Mon Feb 24 18:27:34 2020
--------------------------------------------------
Total active translations: 1
No.Static: 0
No.Dyn:    1
No.Dyn-ICMP:   1
--------------------------------------------------
Total expired Translations: 0
SYN timer expired:          0
FIN-RST timer expired:      0
Inactive timer expired:     0
--------------------------------------------------
Total Hits:  2                  Total Misses:  2
In-Out Hits: 0                  In-Out Misses: 2
Out-In Hits: 2                  Out-In Misses: 0
--------------------------------------------------
Total SW Translated Packets: 2
In-Out SW Translated: 2
Out-In SW Translated: 0
--------------------------------------------------
Total SW Dropped Packets: 0
In-Out SW Dropped: 0
Out-In SW Dropped: 0

Address alloc. failure drop:      0
Port alloc.  failure drop:        0
Dyn. Translation max limit drop:  0
ICMP max limit drop:              0
Allhost max limit drop:           0
--------------------------------------------------
Total TCP session established: 0
Total TCP session closed:      0
--------------------------------------------------
NAT Inside Interfaces:  1
Ethernet1/34

NAT Outside Interfaces: 1
Ethernet1/32
--------------------------------------------------
Inside source list:
++++++++++++++++++++

Access list: T2
RefCount: 1
Pool: T2     Overload
Total addresses: 10
Allocated: 1    percentage: 10%
Missed: 0


Outside source list:
```

```
++++++++++++++++++++
------------------------------------------------------
======================================================
Switch(config)#
Switch(config)#


**No.Dyn-ICMP  field is to display the no of icmp dynamic translations , its a subset
of  "No.Dyn" field.
```

（注） Cisco NX-OS リリース 10.2（3u）以降では、**No.Dyn-ICMP** フィールドは **No.Dyn** フィールドのサブセットであり、ICMP ダイナミック変換の数が表示されます。

次に、NAT の実行コンフィギュレーションを表示する例を示します。

```
switch# show run nat

!Command: show running-config nat
!Time: Wed Apr 23 11:17:43 2014

version 6.0(2)A3(1)
feature nat

ip nat inside source list list1 pool pool1
ip nat inside source list list2 pool pool2 overload
ip nat inside source list list7 pool pool7 overload
ip nat outside source list list3 pool pool3
ip nat pool pool1 30.1.1.1 30.1.1.2 prefix-length 24
ip nat pool pool2 10.1.1.1 10.1.1.2 netmask 255.0.255.0
ip nat pool pool3 30.1.1.1 30.1.1.8 prefix-length 24
ip nat pool pool5 20.1.1.1 20.1.1.5 netmask 255.0.255.0
ip nat pool pool7 netmask 255.255.0.0
  address 40.1.1.1 40.1.1.5
```

次に、アクティブな NAT 変換を表示する例を示します。

オーバーロードのある内部プール

```
switch# show ip nat translation
Pro  Inside global      Inside local       Outside local      Outside global
icmp 20.1.1.3:64762     10.1.1.2:133       20.1.1.1:0         20.1.1.1:0
icmp 20.1.1.3:64763     10.1.1.2:134       20.1.1.1:0         20.1.1.1:0
```

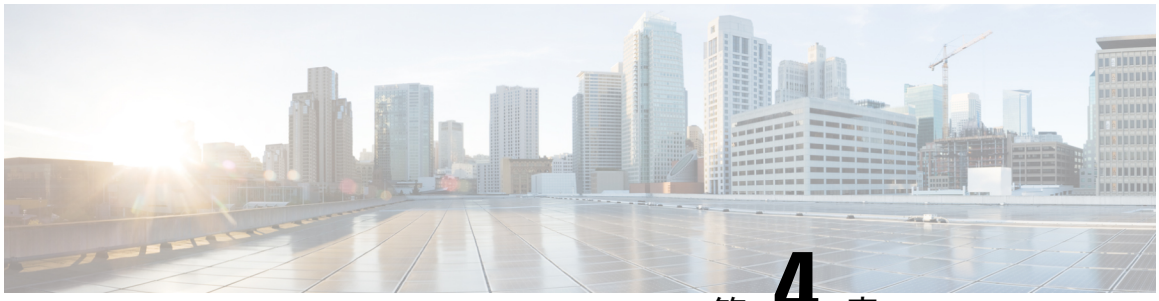
オーバーロードのない外部プール

```
switch# show ip nat translation
Pro  Inside global      Inside local       Outside local      Outside global
any  ---                ---                177.7.1.1:0        77.7.1.64:0
any  ---                ---                40.146.1.1:0       40.46.1.64:0
any  ---                ---                10.4.146.1:0       10.4.46.64:0
```

例：ダイナミック変換および変換タイムアウトの設定

次に、アクセスリストを指定してダイナミックオーバーロードネットワークアドレス変換（NAT）を設定する例を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# ip access-list acl1
Switch(config-acl)# permit ip 10.111.11.0/24 any
Switch(config-acl)# deny udp 10.111.11.100/32 any
Switch(config-acl)# exit
Switch(config)# ip nat inside source list acl1 interface ethernet 1/1 overload
Switch(config)# interface ethernet 1/4
Switch(config-if)# ip address 10.111.11.39 255.255.255.0
Switch(config-if)# ip nat inside
Switch(config-if)# exit
Switch(config)# interface ethernet 1/1
Switch(config-if)# ip address 172.16.232.182 255.255.255.240
Switch(config-if)# ip nat outside
Switch(config-if)# exit
Switch(config)# ip nat translation max-entries 300
Switch(config)# ip nat translation timeout 13000
Switch(config)# end
```



第 4 章

レイヤ 2 インターフェイスの設定

アクセス インターフェイスとトランク インターフェイスについて

（注） このデバイスは、IEEE 802.1Q タイプ VLAN トランク カプセル化だけをサポートします。

アクセス インターフェイスとトランク インターフェイスの概要

レイヤ 2 ポートは、アクセスまたはトランク ポートとして次のように設定できます。

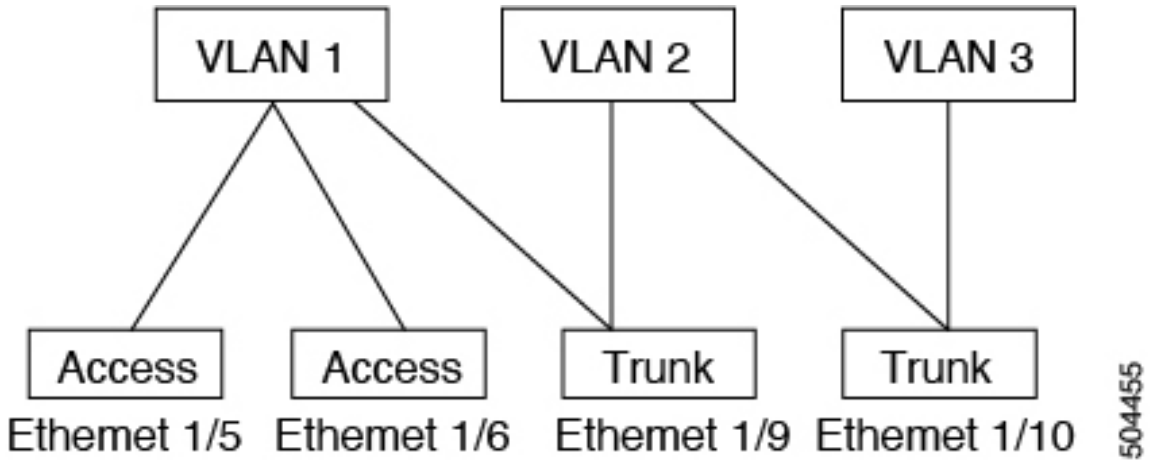
- アクセス ポートでは VLAN を 1 つだけ設定でき、1 つの VLAN のトラフィックだけを伝送できます。
- トランク ポートには複数の VLAN を設定でき、複数の VLAN のトラフィックを同時に伝送できます。

デフォルトでは、Cisco Nexus® 3550-T スイッチのすべてのポートはレイヤ 3 ポート/レイヤ 2 ポートです。

セットアップ スクリプトを使用するか、**system default switchport** コマンドを入力して、すべてのポートをレイヤ 2 ポートにできますすべてのポートをレイヤ 2 ポートにできます。セットアップ スクリプトを使用する詳細については、「*Cisco Nexus® 3550-T Fundamentals* 構成」のセクションを参照してください。CLI を使用して、ポートをレイヤ 2 ポートとして設定するには、**switchport** コマンドを使用します。

次の図は、ネットワークにおけるトランク ポートの使い方を示したものです。トランク ポートは、2 つ以上の VLAN のトラフィックを伝送します。

図 *2:* トランクおよびアクセス ポートと *VLAN* トラフィック



（注） VLAN については、「*Cisco Nexus® 3550-T Layer 2 Switching* 構成」のセクションを参照してください。

複数の VLAN に接続するトランク ポートのトラフィックを正しく伝送するために、デバイスは IEEE 802.1Q カプセル化（タギング方式）を使用します（詳細については、「IEEE 802.1Q カプセル化」の項を参照）。

アクセス ポートでのパフォーマンスを最適化するには、そのポートをホスト ポートとして設定します。ホスト ポートとして設定されたポートは、自動的にアクセス ポートとして設定され、チャネル グループ化はディセーブルになります。ホストを割り当てると、割り当てたポートがパケット転送を開始する時間が短縮されます。

ホストポートとして設定できるのは端末だけです。端末以外のポートをホストとして設定しようとするとエラーになります。

アクセス ポートは、アクセス VLAN 値の他に 802.1Q タグがヘッダーに設定されたパケットを受信すると、送信元の MAC アドレスを学習せずにドロップします。

レイヤ 2 インターフェイスはアクセス ポートまたはトランク ポートとして機能できますが、両方のポート タイプとして同時に機能できません。

レイヤ 2 インターフェイスをレイヤ 3 インターフェイスに戻すと、このインターフェイスはレイヤ 2 の設定をすべて失い、デフォルト VLAN 設定に戻ります。

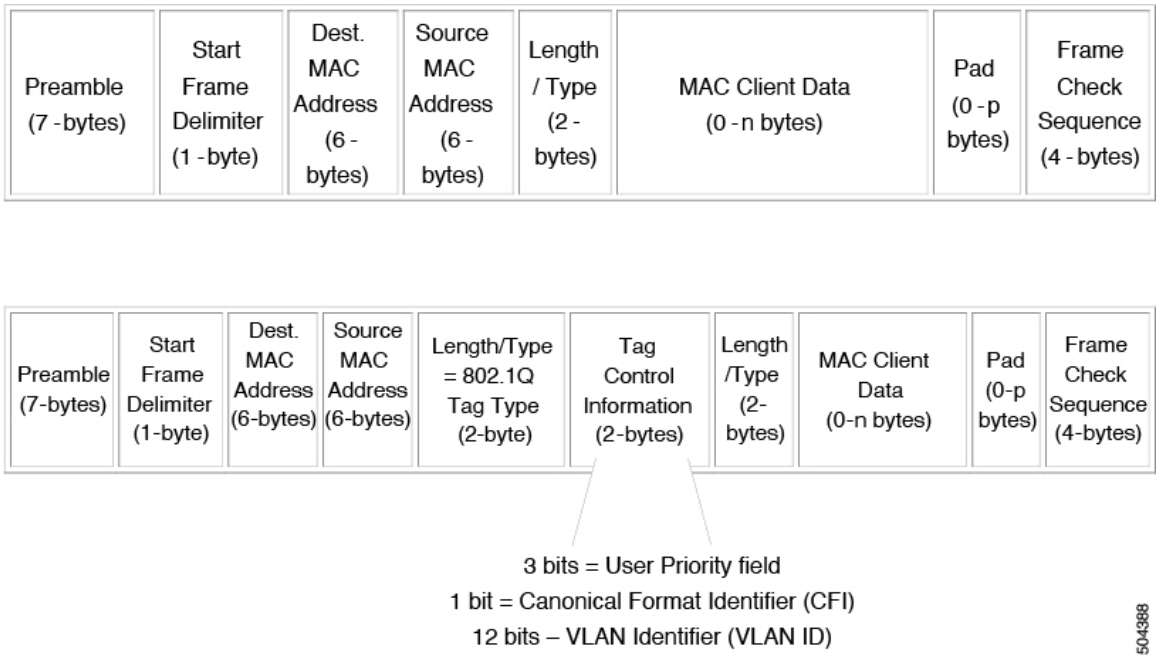
IEEE 802.1Q カプセル化

（注） VLAN については、「*Cisco Nexus® 3550-T Layer 2 Switching* 構成」のセクションを参照してください。

トランクとは、スイッチと他のネットワーキングデバイス間のポイントツーポイントリンクです。トランクは 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張することができます。

複数の VLAN に接続するトランク ポートのトラフィックを正しく配信するために、デバイスは IEEE 802.1Q カプセル化（タギング方式）を使用します。この方式では、フレーム ヘッダーに挿入したタグが使用されます。このタグには、そのフレームおよびパケットが属する特定の VLAN に関する情報が含まれます。タグ方式を使用すると、複数の異なる VLAN 用にカプセル化されたパケットが、同じポートを通過しても、各 VLAN のトラフィックを区別することができます。また、カプセル化された VLAN タグにより、トランクは同じ VLAN 上のネットワークの端から端までトラフィックを移動させます。

図 *3 : 802.1Q* タグなしヘッダーと *802.1Q* タグ付きヘッダー



アクセス VLAN

アクセス モードでポートを設定すると、そのインターフェイスのトラフィックを伝送する VLAN を指定できます。アクセス モードのポート（アクセス ポート）用に VLAN を設定しないと、そのインターフェイスはデフォルトの VLAN（VLAN1）のトラフィックだけを伝送します。

VLANのアクセスポートメンバーシップを変更するには、新しいVLANを指定します。VLANをアクセス ポートのアクセス VLAN として割り当てるには、まず、VLAN を作成する必要があります。アクセス ポートのアクセス VLAN をまだ作成していない VLAN に変更すると、アクセス ポートがシャットダウンされます。

アクセス ポートは、アクセス VLAN 値の他に 802.1Q タグがヘッダーに設定されたパケットを受信すると、送信元の MAC アドレスを学習せずにドロップします。

トランク ポートのネイティブ VLAN ID

トランク ポートは、タグなしパケットと 802.1Q タグ付きパケットを同時に伝送できます。デフォルトのポート VLAN ID をトランク ポートに割り当てると、すべてのタグなしトラフィックが、そのトランク ポートのデフォルトのポート VLAN ID で伝送され、タグなしトラフィックはすべてこの VLAN に属するものと見なされます。この VLAN のことを、トランク ポートのネイティブ VLAN ID といいます。つまり、トランク ポートでタグなしトラフィックを伝送する VLAN がネイティブ VLAN ID となります。

（注） ネイティブ VLAN ID 番号は、トランクの両端で一致していなければなりません。

トランク ポートは、デフォルトのポート VLAN ID と同じ VLAN が設定された出力パケットをタグなしで送信します。他のすべての出力パケットは、トランク ポートによってタグ付けされます。ネイティブ VLAN ID を設定しないと、トランク ポートはデフォルト VLAN を使用します。

Allowed VLANs

デフォルトでは、トランク ポートはすべての VLAN に対してトラフィックを送受信します。各トランク上では、すべての VLAN ID が許可されます。この包括的なリストから VLAN を削除することによって、特定の VLAN からのトラフィックが、そのトランクを通過するのを禁止できます。後ほど、トラフィックを伝送するトランクの VLAN を指定してリストに追加し直すこともできます。

デフォルトVLANのスパニングツリープロトコル（STP）トポロジを区切るには、許容VLANのリストからVLAN1を削除します。この分割を行わないと、VLAN1（デフォルトでは、すべてのポートでイネーブル）が非常に大きなSTPトポロジを形成し、STPのコンバージェンス中に問題が発生する可能性があります。VLAN1 を削除すると、そのポート上で VLAN1 のデータ トラフィックはすべてブロックされますが、制御トラフィックは通過し続けます。

（注） STP の詳細については、「*Cisco Nexus® 3550-T Layer 2 Switching* 構成」のセクションを参照してください。

デフォルト インターフェイス

デフォルト インターフェイス機能を使用して、イーサネット、ループバック、VLAN ネットワーク、およびポートチャネルインターフェイスなどの物理インターフェイスおよび論理インターフェイスの両方に対する構成済みパラメータを消去できます。

（注） すべての 48 ポートがデフォルト インターフェイスに選択できます。

スイッチ仮想インターフェイスおよび自動ステート動作

Cisco NX-OS では、スイッチ仮想インターフェイス（SVI）は、デバイスの VLAN のブリッジング機能とルーティング機能間の論理インターフェイスを表します。

このインターフェイスの動作状態は、その対応する VLAN 内のさまざまなポートの状態によって決まります。VLAN の SVI インターフェイスは、その VLAN 内の少なくとも 1 個のポートがスパニングツリー プロトコル（STP）のフォワーディング ステートにある場合に稼働します。同様に、このインターフェイスは最後の STP 転送ポートがダウンするか、別の STP 状態になったとき、ダウンします。

カウンタ値

設定、パケットサイズ、増分カウンタ値、およびトラフィックについては、次の情報を参照してください。

設定	パケット サイズ	増分カウンタ	トラフィック
L2 ポート	<1500	入力エラー	破棄

（注） CRC 不良の 64バイトを超えるパケット：CRC カウンタが増加します。

レイヤ 2 インターフェイスの前提条件

レイヤ 2 インターフェイスには次の前提条件があります。

- デバイスにログインしている。
- デフォルトでは、Cisco NX-OS はレイヤ 3 パラメータを設定します。レイヤ 2 パラメータを設定するには、ポート モードをレイヤ 2 に切り替える必要があります。**switchport** コマンドを使用すれば、ポート モードを変更できます。

- **switchport mode** コマンドを使用する前に、ポートをレイヤ 2 ポートとして設定する 必要があります。デフォルトでは、デバイスのポートはすべてレイヤ 3 ポートです。デフォルトでは、Cisco Nexus® 3550-T デバイスのすべてのポートはレイヤ 2 ポートです。

レイヤ 2 インターフェイスのガイドラインおよび制約事項

VLAN トランキングには次の設定上のガイドラインと制限事項があります。

- ポートはレイヤ 2 またはレイヤ 3 インターフェイスのいずれかです。両方が同時に成立することはありません。
- レイヤ 3 ポートをレイヤ 2 ポートに変更する場合またはレイヤ 2 ポートをレイヤ 3 ポートに変更する場合は、レイヤに依存するすべての設定は失われます。アクセスまたはトランク ポートをレイヤ 3 ポートに変更すると、アクセス VLAN、ネイティブ VLAN、許容 VLAN などの情報はすべて失われます。
- アクセス リンクを持つデバイスには接続しないでください。アクセス リンクにより VLAN が区分されることがあります。
- 802.1Q トランクを介してシスコ デバイスを接続するときは、802.1Q トランクのネイティブ VLAN がトランク リンクの両端で同じであることを確認してください。トランクの一端のネイティブ VLAN と反対側の端のネイティブ VLAN が異なると、スパニングツリー ループの原因になります。
- ネットワーク上のすべてのネイティブ VLAN についてスパニングツリーをディセーブルにせずに、802.1Q トランクの VLAN 上のスパニングツリーをディセーブルにすると、スパニングツリー ループが発生することがあります。802.1Q トランクのネイティブ VLAN のスパニングツリーはイネーブルのままにしておく必要があります。スパニングツリーをイネーブルにしておけない場合は、ネットワークの各 VLAN のスパニングツリーをディセーブルにする必要があります。スパニングツリーをディセーブルにする前に、ネットワークに物理ループがないことを確認してください。
- 802.1Q トランクを介して 2 台のシスコ デバイスを接続すると、トランク上で許容される VLAN ごとにスパニングツリー ブリッジ プロトコル データ ユニット（BPDU）が交換されます。トランクのネイティブ VLAN 上の BPDU は、タグなしの状態で予約済み IEEE 802.1D スパニングツリー マルチキャスト MAC アドレス（01-80-C2-00-00-00）に送信されます。トランクの他のすべての VLAN 上の BPDU は、タグ付きの状態で、予約済み Cisco Shared Spanning Tree（SSTP）マルチキャスト MAC アドレス（01-00-0c-cc-cc-cd）に送信されます。
- シスコ デバイスは、トランクのネイティブ VLAN 以外の VLAN にある SSTP マルチキャスト MAC アドレスに BPDU を伝送します。したがって、他社製のデバイスではこれらのフレームが BPDU として認識されず、対応する VLAN のすべてのポート上でフラッディングされます。他社製の 802.1Q クラウドに接続された他のシスコ デバイスは、フラッディングされたこれらの BPDU を受信します。BPDU を受信すると、Cisco スイッチは、他社

製の 802.1Q デバイス クラウドにわたって、VLAN 別のスパニングツリー トポロジを維持できます。シスコ デバイスを隔てている他社製の 802.1Q クラウドは、802.1Q トランクを介して他社製の 802.1Q クラウドに接続されたすべてのデバイス間の単一のブロードキャスト セグメントとして処理されます。

- シスコ デバイスを他社製の 802.1Q クラウドに接続するすべての 802.1Q トランク上で、ネイティブ VLAN が同じであることを確認します。
- 他社製の特定の 802.1Q クラウドに複数のシスコ デバイスを接続する場合は、すべての接続に 802.1Q トランクを使用する必要があります。シスコ デバイスを他社製の 802.1Q クラウドにアクセス ポート経由で接続することはできません。この場合、シスコ製のアクセス ポートはスパニングツリー「ポート不一致」状態になり、トラフィックはポートを通過しません。
- トランク ポートをポートチャネル グループに含めることができますが、そのグループのトランクはすべて同じ設定にする必要があります。グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。パラメータの設定を変更すると、許容 VLAN やトランク ステータスなど、デバイスのグループのすべてのポートにその設定を伝えます。たとえば、ポート グループのあるポートがトランクになるのを中止すると、すべてのポートがトランクになるのを中止します。
- clear mac address-table dynamicコマンドを使用してVLANのMACアドレスをクリアすると、そのVLANのダイナミックARP（Address Resolution Protocol）エントリが更新されます。
- VLAN上にスタティックARPエントリが存在し、MACアドレスからポートへのマッピングが存在しない場合、スーパーバイザはARP要求を生成してMACアドレスを学習できます。MACアドレスを学習すると、隣接エントリは正しい物理ポートをポイントします。
- Cisco NX-OS は、SVI の1つが BIA MAC（バーンドイン MAC アドレス）を使用してCisco Nexus 3550-T 上にある場合、2 つの VLAN 間のトランスペアレントブリッジングをサポートしません。これは、BIA MACがSVI/VLAN間で共有される場合に発生します。BIA MACとは異なるMACを、トランスペアレントブリッジングが正しく動作するようにSVIで設定できます。
- インターフェイス モードをトランク VLAN とトランク VLAN に同時に設定しようとすると、エラー メッセージが表示されることがあります。Cisco NX-OS インターフェイスでは、インターフェイス モードのデフォルト値は access です。トランク関連の設定を実装するには、最初にインターフェイス モードを trunk に変更してから、トランク VLAN 範囲を設定する必要があります。
- VLAN タグ付きパケットのスパニングは、 Cisco Nexus 3550-T スイッチではサポートされていません。

レイヤ 2 インターフェイスのデフォルト設定

次の表に、デバイスのアクセスおよびトランク ポート モード パラメータのデフォルト設定を示します。

表 *2:* デフォルトのアクセスおよびトランク ポート モード パラメータ

パラメータ	デフォルト
スイッチポート モード	アクセス
Allowed VLANs	1 ～ 3967 （注） 最大 255 個の VLAN がサポートされます。
アクセス VLAN ID	VLAN1
Native VLAN ID	VLAN1
ネイティブ VLAN ID タギング	ディセーブル
管理状態	閉じる
SVI 自動ステート	有効（Enabled）

アクセス インターフェイスとトランク インターフェイスの設定

（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。

レイヤ 2 アクセス ポートの構成

レイヤ 2 ポートをアクセス ポートとして設定できます。アクセス ポートは、パケットを、1 つのタグなし VLAN 上だけで送信します。インターフェイスが伝送する VLAN トラフィックを指定します。これがアクセス VLAN になります。アクセス ポートの VLAN を指定しない場合、そのインターフェイスはデフォルト VLAN のトラフィックだけを伝送します。デフォルトの VLAN は VLAN 1 です。

VLAN をアクセス VLAN として指定するには、その VLAN が存在しなければなりません。システムは、存在しないアクセス VLAN に割り当てられたアクセス ポートをシャット ダウンします。

始める前に

レイヤ 2 インターフェイスを設定す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：
	`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 ethernet** {{*type slot/port*} | {**port-channel** *number*}}
	例：
	`switch(config)# interface ethernet 1/5`
	`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 3	**switchport mode** [**access** | **trunk**] 例： `switch(config-if)# switchport mode access`	インターフェイスを、非トランキング、タグなし、シングル VLAN レイヤ 2 インターフェイスとして設定します。アクセス ポートは、1 つの VLAN のトラフィックだけを伝送できます。デフォルトでは、アクセス ポートは VLAN1 のトラフィックを伝送します。異なる VLAN のトラフィックを伝送するようにアクセス ポートを設定するには、**switchport access vlan** を使用します コマンドを使用します。
ステップ 4	**switchport access vlan** *vlan-id* 例： `switch(config-if)# switchport access vlan 5`	このアクセス ポートでトラフィックを伝送する VLAN を指定します。このコマンドを入力しないと、アクセス ポートは VLAN1 だけのトラフィックを伝送します。このコマンドを使用して、アクセス ポートがトラフィックを伝送する VLAN を変更できます。

ステップ 5	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		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	**show interface** 例： `switch# show interface`	（任意）インターフェイスのステータスと内容を表示します。

ステップ 7	**no shutdown**
	例：
	`switch# configure terminal`
	`switch(config)# int e1/5`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 8	**copy running-config startup-config** 例： `switch(config)# 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、イーサネット1/5をレイヤ2アクセス ポートとして設定し、VLAN5のトラフィックだけを伝送する例を示します：

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 5
switch(config-if)#
```

アクセス ホスト ポートの設定

（注） switchport host コマンドは、端末に接続するインターフェイスだけに使用します。

端末に接続されたアクセス ポートでのパフォーマンスを最適化するには、そのポートをホスト ポートとしても設定します。アクセス ホスト ポートはエッジ ポートと同様に STP を処理し、ブロッキング ステートおよびラーニング ステートを通過することなくただちにフォワーディング ステートに移行します。インターフェイスをアクセス ホスト ポートとして設定すると、そのインターフェイス上でポート チャネル動作がディセーブルになります。

始める前に

エンドステーションのインターフェイスに接続された適切なインターフェイスを設定することを確認してください。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`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 ethernet** *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 3	**switchport host** 例： switch(config-if)# **switchport host**	インターフェイスをアクセス ホスト ポートとして設定します。このポートはただちに、スパニングツリー フォワーディング ステートに移行し、このインターフェイスのポート チャネル動作をディセーブルにします。 （注） このコマンドは端末だけに適用します。

ステップ 4	**exit**
	例：
	`switch(config-if-range)# exit`
	`switch(config)#`
		インターフェイスモードを終了します。

ステップ 5	**show interface** 例： `switch# show interface`	（任意）インターフェイスのステータスと内容を表示します。

ステップ 6	**no shutdown**
	例：
	`switch# configure terminal`
	`switch(config)# int e1/3`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `switch(config)# 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、イーサネット 1/3 をレイヤ 2 アクセス ポートとして設定し、PortFast を有効化してポート チャネルを無効化にする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# switchport host
switch(config-if)#
```

トランク ポートの設定

レイヤ 2 ポートをトランク ポートとして設定できます。トランク ポートは、1 つの VLAN の非タグ付きパケットと、複数の VLAN のカプセル化されたタグ付きパケットを伝送します（カプセル化については、「*IEEE 802.1Q* カプセル化」のセクションを参照してください）。

（注） デバイスは 802.1Q カプセル化だけをサポートします。

始める前に

トランク ポートを設定する前に、レイヤ 2 インターフェイスを設定す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：
	`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** {*type slot/port* | **port-channel** *number*}
	例：
	`switch(config)# interface ethernet 1/4`
	`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。

	コマンドまたはアクション	目的
ステップ 3	**switchport mode** [**access** | **trunk**] 例： `switch(config-if)# switchport mode trunk`	インターフェイスをレイヤ 2 トランク ポートとして設定します。トランク ポートは、同じ物理リンクで 1 つ以上の VLAN 内のトラフィックを伝送できます（各 VLAN はトランキングが許可された VLAN リストに基づいています）。デフォルトでは、トランク インターフェイスはすべての VLAN のトラフィックを伝送できます。指定したトランクで特定の VLAN のみが許可されるように指定するには、**switchport trunk allowed vlan** コマンドを使用します。

ステップ 4	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 5	**show interface** 例： `switch# show interface`	（任意）インターフェイスのステータスと内容を表示します。

ステップ 6	**no shutdown**
	例：
	`switch# configure terminal`
	`switch(config)# int e1/4`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# 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、イーサネット 1/4 をレイヤ 2 トランク ポートとして設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# switchport mode trunk
switch(config-if)#
```

トランキング ポートの許可 VLAN の設定

特定のトランク ポートで許可されている VLAN の ID を指定できます。

（注） **switchport trunk allowed vlan** *vlan-list* コマンドは、指定されたポートの現在のVLANリストを新しいリストに置き換えます。新しいリストが適用される前に確認を求められます。

大規模な設定のコピー アンド ペーストをしている場合は、CLI が他のコマンドを受け入れる前に確認のため待機しているので障害が発生する場合があります。この問題を回避するため、**terminal dont-ask** を使用してプロンプトを無効にできます。 コマンドを入力してから、設定を貼り付けます。

始める前に

指定トランク ポートの許可 VLAN を設定する前に、正しいインターフェイスを設定していること、およびそのインターフェイスがトランクであることを確認してください。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`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** {**ethernet** *slot/port* | **port-channel** *number*} 例： `switch(config)# interface ethernet 1/3`	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	**switchport trunk allowed vlan** {*vlan-list* **add** *vlan-list* | **all** | **except** *vlan-list* | **none** | **remove** *vlan-list*} 例： `switch(config-if)# switchport trunk allowed vlan add 15-20#`	トランク インターフェイスの許可VLANを設定します。デフォルトでは、トランク インターフェイス上のすべてのVLAN（1 ～ 3967 および 4048 ～ 4094）が許可されます。Cisco Nexus 3550-T スイッチでは、255 の VLAN のみがサポートされます。 （注） 内部で割り当て済みの VLAN を、トランク ポート上の許可 VLAN として追加することはできません。内部で割り当て済みの VLAN を、トランク ポートの

	コマンドまたはアクション	目的
		許可 VLAN として登録しようとすると、メッセージが返されます。

ステップ 4	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 5	**show vlan** 例： `switch# show vlan`	（任意）VLANのステータスと内容を表示します。

ステップ 6	**no shutdown**
	例：
	`switch# configure terminal`
	`switch(config)# int e1/3`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# 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、VLAN 15 ～ 20 をイーサネット 1/3、レイヤ 2 トランク ポートの許容 VLAN リストに追加する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# switchport trunk allowed vlan 15-20
switch(config-if)#
```

デフォルト インターフェイスの設定

デフォルトインターフェイス機能によって、イーサネット、ループバック、VLANネットワーク、およびポート チャネル インターフェイスなどの複数インターフェイスの既存の構成を消去できます。特定のインターフェイスでのすべてのユーザ コンフィギュレーションは削除されます。後で削除したコンフィギュレーションを復元できるように、任意でチェックポイントを作成してからインターフェイスのコンフィギュレーションを消去できます。

（注） デフォルトのインターフェイス機能は、管理インターフェイスに対しサポートされていません。それはデバイスが到達不能な状態になる可能性があるためです。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`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	**default interface** *int-if* [**checkpoint** *name*] 例： `switch(config)# default interface ethernet 1/3 checkpoint test8`	インターフェイスの設定を削除しデフォルトの設定を復元します。**?** キーワードを使用して、サポートされるインターフェイスを表示します。 **checkpoint** コマンドを使用し、キーワードを使用して、設定を消し去ってしまう前にインターフェイスの実行コンフィギュレーションを保存します。

ステップ 3	**exit**
	例：
	`switch(config)# exit`
	`switch(config)#`
		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 interface** 例： `switch# show interface`	（任意）インターフェイスのステータスと内容を表示します。

ステップ 5	**no shutdown**
	例：
	`switch# configure terminal`
	`switch(config)# int e1/3`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

例

次に、ロールバック目的で実行コンフィギュレーションのチェックポイントを保存する際にイーサネット インターフェイスの設定を削除する例を示します。

```
switch# configure terminal
switch(config)# default interface ethernet 1/3 checkpoint test8
.......Done
switch(config)#
```

システムのデフォルト ポート モードをレイヤ 2 に変更

システムのデフォルト ポート モードをレイヤ 2 アクセス ポートに設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	**system default switchport** [**shutdown**] 例： switch(config-if)# **system default switchport**	システムのすべてのインターフェイスに対するデフォルトのポート モードをレイヤ 2 アクセス ポート モードに設定し、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。デフォルトでは、すべてのインターフェイスがレイヤ 3 です。 （注） クライアントが **system default switchport shutdown** コマンドが発行されます。 • **no shutdown** で明示的に設定されていないレイヤ 2 ポートはシャットダウンされます。シャットダウンを回避するには、**no shut** でレイヤ 2 ポートを設定します。

ステップ 3	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		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 4	**show interface brief** 例： `switch# show interface brief`	（任意）インターフェイスのステータスと内容を表示します。

ステップ 5	**no shutdown**
	例：
	`switch# configure terminal`
	`switch(config)# int e1/3`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 6	**copy running-config startup-config** 例： `switch(config)# 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、システム ポートをデフォルトでレイヤ 2 アクセス ポートに設定する例を示します。

```
switch# configure terminal
switch(config-if)# system default switchport
switch(config-if)#
```

インターフェイス コンフィギュレーションの確認

アクセスおよびトランク インターフェイス設定情報を表示するには、次のタスクのいずれかを行います。

コマンド	目的
show interface ethernet *slot/port* [**brief** | | **counters** | **debounce** | **description** | **flowcontrol** | **mac-address** | **status** | **transceiver**]	インターフェイスの設定を表示します。
show interface brief	インターフェイス設定情報を、モードも含めて表示します。
show interface switchport	アクセスおよびトランク インターフェイスも含めて、すべてのレイヤ 2 インターフェイスの情報を表示します。

コマンド	目的
show interface trunk [**module** *module-number* | **vlan** *vlan-id*]	トランク設定情報を表示します。
show interface capabilities	インターフェイスの機能に関する情報を表示します。
show running-config [**all**]	現在の設定に関する情報を表示します。 **all** コマンドを使用すると、デフォルトの設定と現在の設定が表示されます。
show running-config interface ethernet *slot/port*	指定されたインターフェイスに関する設定情報を表示します。
show running-config interface port-channel *slot/port*	指定されたポートチャネル インターフェイスに関するコンフィギュレーション情報を表示します。
show running-config interface vlan *vlan-id*	指定された VLAN インターフェイスに関するコンフィギュレーション情報を表示します。

レイヤ 2 インターフェイスのモニタリング

レイヤ 2 インターフェイスを表示するには、次のコマンドを使用します。

コマンド	目的
clear counters interface [**interface**]	カウンタをクリアします。
load- interval {**counter** {**1** | **2** | **3**}} *seconds*	Cisco Nexus 3550-T デバイスは、ビットレートおよびパケットレートの統計情報に 3 種類のサンプリング インターバルを設定します。
show interface counters [**module** *module*]	入力および出力オクテット ユニキャスト パケット、マルチキャスト パケット、ブロードキャスト パケットを表示します。

コマンド	目的
show interface counters detailed [**all**]	入力パケット、バイト、マルチキャストを、出力パケットおよびバイトとともに表示します。 （注） *[*出力ドロップ エラーを無視（*Ignore Output Dropped Errors*） *]* は、ポートに向けられたトラフィックの入力ドロップの累積を表します。ポートでの入力ドロップは、入力破棄エラーの一部として表示されます。
show interface counters errors [**module** *module*]	エラー パケットの数を表示します。 （注） *OutDiscards* は 、ポートに向けられたトラフィックの累積入力ドロップを表すため、無視します。ポートでの入力ドロップは、*InDiscards* の一部として表示されます。

アクセス ポートおよびトランク ポートの設定例

次に、レイヤ2アクセスインターフェイスを設定し、このインターフェイスにアクセスVLANモードを割り当てる例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/30
switch(config-if)# switchport
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 5
switch(config-if)#
```

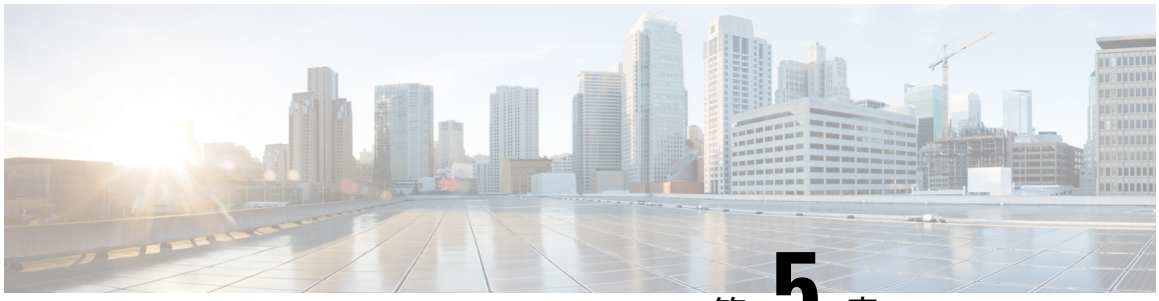
次に、レイヤ 2 トランク インターフェイスを設定してネイティブ VLAN および許容 VLAN を割り当て、デバイスにトランク インターフェイスのネイティブ VLAN トラフィックのタグを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/35
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk native vlan 10
switch(config-if)# switchport trunk allowed vlan 5, 10
switch(config-if)# exit
```

関連資料

関連資料	マニュアル タイトル
レイヤ 3 インターフェイスの設定	「レイヤ2インターフェイスの構成」セクション
ポート チャネル	「ポート チャネルの構成」セクション
システム管理	「*Cisco Nexus® 3550-T* システム管理構成」章
ハイアベイラビリティ	『*Cisco Nexus Series* 高可用性および冗長性ガイド』
ライセンス	『*Cisco NX-OS Licensing Guide*』
リリース ノート	『*Cisco Nexus® Series NX-OS* リリース ノート』

関連資料



第 5 章

ポート チャネルの構成

ポート チャネルについて

ポートチャネルは複数の物理インターフェイスの集合体で、論理インターフェイスを作成します。1 つのポート チャネルに最大 8 つの個別アクティブ リンクをバンドルして、帯域幅と冗長性を向上させることができます。これらの集約された各物理インターフェイス間でトラフィックのロード バランシングも行います。ポート チャネルの物理インターフェイスが少なくとも 1 つ動作していれば、そのポート チャネルは動作しています。

システム全体で許可される最大ポート チャネルの制限は 48 です。各ポート グループには 8 ポートが含まれている 6 つのポート グループがあります。ポート グループごとに最大 8 つのポート チャネルを作成できます。同じポート グループに属する最大 8 個の物理ポートを特定のポート チャネルにバンドルすることができます。異なるポート グループに属するポートからポート チャネルを作成することはできません。

表 *3*: ポート グループ名とポート グループ範囲

ポート グループ名	ポート グループ範囲
1	1/1 ー 1/8

ポート グループ名	ポート グループ範囲
2	1/9 ～ 1/16
3	1/17 ー 1/24
4	1/25 ～ 1/32
5	1/33 ～ 1/40
6	1/41 ～ 1/48

レイヤ 2 ポート チャネルに適合するレイヤ 2 インターフェイスをバンドルすれば、レイヤ 2 ポート チャネルを作成できます。レイヤ 3 ポート チャネルに適合するレイヤ 3 インターフェイスをバンドルすれば、レイヤ 3 ポート チャネルを作成できます。レイヤ 2 インターフェイスとレイヤ 3 インターフェイスを同一のポート チャネルで組み合わせることはできません。

ポート チャネルをレイヤ 3 からレイヤ 2 に変更することもできます。レイヤ 2 インターフェイスの作成については、「レイヤ *2* インターフェイスの構成」の章を参照してください。

レイヤ 2 ポート チャネル インターフェイスとそのメンバー ポートは、異なる STP パラメータを持つことができます。ポート チャネルの STP パラメータを変更しても、メンバー ポートがバンドルされている場合はポート チャネル インターフェイスが優先されるため、メンバー ポートの STP パラメータには影響しません。

（注） レイヤ 2 ポートがポート チャネルの一部になった後に、すべてのスイッチポートの設定をポート チャネルで実行する必要があります。スイッチポートの設定を各ポート チャネル メンバに適用できません。レイヤ 3 の設定を各ポート チャネル メンバに適用できません。設定をポート チャネル全体に適用する必要があります。

集約プロトコルが関連付けられていない場合でもスタティック ポート チャネルを使用して設定を簡略化できます。

柔軟性を高めたい場合は LACP を使用できます。Link Aggregation Control Protocol（LACP）は IEEE 802.3ad で定義されています。LACP を使用すると、リンクによってプロトコル パケットが渡されます。共有インターフェイスでは LACP を設定できません。

LACP については、「*LACP* の概要」のセクションを参照してください。

ポート チャネル

ポート チャネルは、物理リンクをまとめて 1 つのチャネル グループに入れ、最大 8 の物理リンクの帯域幅を集約した単一の論理リンクを作ります。ポート チャネル内のメンバー ポートに障害が発生すると、障害が発生したリンクで伝送されていたトラフィックはポート チャネル内のその他のメンバー ポートに切り替わります。

ただし、LACP をイネーブルにすればポート チャネルをより柔軟に使用できます。LACP を使ってポート チャネルを設定する場合と静的ポート チャネルを使って設定する場合では、手順が多少異なります（「ポート チャネルの構成」のセクションを参照してください）。

（注） デバイスはポート チャネルに対するポート集約プロトコル（PAgP）をサポートしません。

各ポートにはポート チャネルが 1 つだけあります。ポート チャネルのすべてのポートには互換性があり、同じ速度とデュプレックスモードを使用します（「互換性要件」のセクションを参照してください）。集約プロトコルを使わずに静的ポートチャネルを実行する場合、物理リンクはすべて on チャネル モードです。このモードは、LACP を有効化しない限り変更できません（「ポート チャネル モード」のセクションを参照してください）。

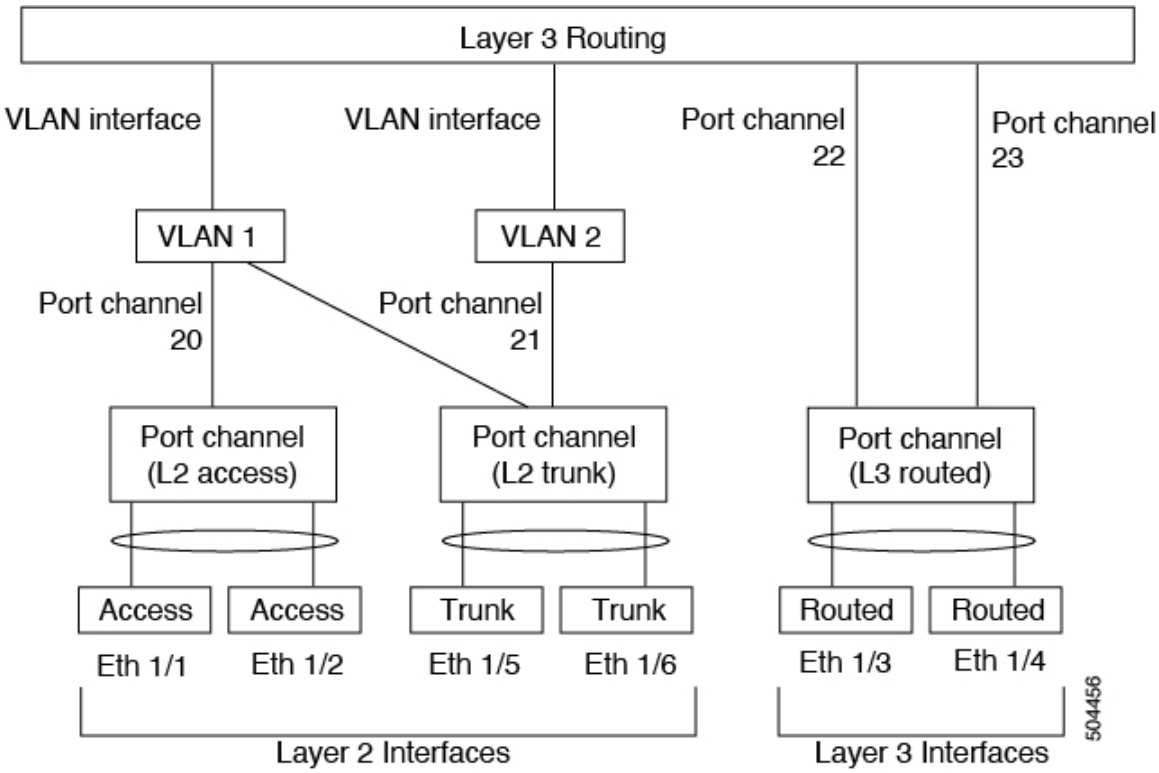
ポート チャネル インターフェイスを作成すると、ポート チャネルを直接作成できます。またはチャネル グループを作成して個別ポートをバンドルに集約させることができます。インターフェイスをチャネル グループに関連付けると、ポート チャネルがない場合は対応するポートチャネルが自動的に作成されます。この場合、ポートチャネルは最初のインターフェイスのレイヤ 2 またはレイヤ 3 設定を行います。最初にポートチャネルを作成することもできます。この場合は、Cisco NX-OS ソフトウェアがポート チャネルと同じチャネル番号の空のチャネル グループを作成してデフォルトレイヤ 2 またはレイヤ 3 設定を行い、互換性も構成します（「互換性要件」のセクションを参照してください）。

（注） 少なくともメンバ ポートの 1 つがアップしており、かつそのポートのチャネルが有効であれば、ポート チャネルは動作上アップ状態にあります。メンバー ポートがすべてダウンしていれば、ポート チャネルはダウンしています。

ポートチャネル インターフェイス

次に、ポートチャネル インターフェイスを示します。

図 *4:* ポートチャネル インターフェイス



ポート チャネル インターフェイスは、レイヤ 2 またはレイヤ 3 インターフェイスとして分類できます。さらに、レイヤ 2 ポート チャネルはアクセス モードまたはトランク モードに設定できます。レイヤ 3 ポート チャネル インターフェイスのチャネル メンバにはルーテッド ポートがあます。

レイヤ 3 ポート チャネルにスタティック MAC アドレスを設定できます。この値を設定しない場合、レイヤ 3 ポート チャネルは、最初にアップになるチャネル メンバのルータ MAC を使用します。レイヤ 3 ポート チャネルで静的 MAC アドレスを構成するための詳細については、「*Cisco Nexus® 3550-T* レイヤ *2* スイッチング構成」のセクションを参照してください。

アクセス モードまたはトランク モードでのレイヤ 2 ポートの構成については、「レイヤ *2* インターフェイスの構成」の章を、レイヤ 3 インターフェイスの構成については、「レイヤ *3* インターフェイスの構成」の章を参照してください。

基本設定

ポート チャネル インターフェイスには次の基本設定ができます。

- 帯域幅：この設定は情報目的で使用します。上位レベルプロトコルで使用されます。
- 遅延：この設定は情報目的で使用します。上位レベルプロトコルで使用されます。
- 説明

- デュプレックス
- IP アドレス
- シャットダウン
- 速度

互換性要件

チャネル グループにインターフェイスを追加する場合、そのインターフェイスにチャネル グループとの互換性があるかどうかを確認するために、特定のインターフェイス属性がチェックされます。たとえば、レイヤ 2 チャネル グループにレイヤ 3 インターフェイスを追加できません。また Cisco NX-OS ソフトウェアは、インターフェイスがポート チャネル集約に参加することを許可する前に、そのインターフェイスの多数の動作属性もチェックします。

互換性チェックの対象となる動作属性は次のとおりです。

- ネットワーク層
- （リンク）速度性能
- 速度設定
- デュプレックス性能
- デュプレックス設定
- ポート モード
- アクセス VLAN
- トランク ネイティブ VLAN
- タグ付きまたは非タグ付き
- 許可 VLAN リスト
- フロー制御性能
- フロー制御設定
- メディア タイプ、銅線またはファイバ

show port-channel compatibility-parameters を使用します Cisco NX-OS で使用される互換性チェックの全リストを表示するは、コマンドを使用します。

チャネル モードが on に設定されているインターフェイスは、スタティックなポート チャネルにだけ追加できます。また、チャネル モードが active または passive に設定されているインターフェイスは、LACP が実行されているポート チャネルにだけ追加できます。これらのアトリビュートは個別のメンバ ポートに設定できます。設定するメンバ ポートの属性に互換性がない場合、ソフトウェアはこのポートをポート チャネルで一時停止させます。

または、次のパラメータが同じ場合、パラメータに互換性がないポートを強制的にポートチャネルに参加させることもできます。

- （リンク）速度性能
- 速度設定
- デュプレックス性能
- デュプレックス設定
- フロー制御性能
- フロー制御設定

インターフェイスがポートチャネルに参加すると、一部のパラメータが削除され、ポートチャネルの値が次のように置き換わります。

- 帯域幅
- 遅延
- UDP の拡張認証プロトコル
- VRF
- IP アドレス
- MAC アドレス
- スパニングツリー プロトコル

インターフェイスがポートチャネルに参加または脱退しても、次に示す多くのインターフェイス パラメータは影響を受けません。

- ビーコン
- 説明
- CDP
- LACP ポート プライオリティ
- Debounce
- UDLD
- MDIX
- レート モード
- シャットダウン
- SNMP トラップ

（注） ポート チャネルを削除すると、すべてのメンバ インターフェイスはポート チャネルから削除されたかのように設定されます。

ポート チャネルを使ったロード バランシング

Cisco NX-OS ソフトウェアは、ポート チャネルにおけるすべての動作インターフェイス間のトラフィックをロード バランシングします。その際、フレーム内のアドレスをハッシュして、チャネル内の 1 つのリンクを選択する数値にします。ポート チャネルはデフォルトでロード バランシングを備えています。ポート チャネル ロード バランシングでは、MAC アドレス、または IP アドレスを使用してリンクを選択します。ポート チャネル ロード バランシングは、送信元または宛先アドレスの両方またはどちらか一方を使用します。

ロード バランシング モードを設定して、デバイス全体に設定したすべてのポート チャネルに適用することができます。デバイス全体で 1 つのロード バランシング モードを設定できます。ポート チャネルごとにロード バランシング方式を設定することはできません。

使用するロード バランシング アルゴリズムのタイプを設定できます。ロード バランシング アルゴリズムを指定し、フレームのフィールドを見て出力トラフィックに選択するメンバ ポートを決定します。

レイヤ 3 インターフェイスのデフォルト ロード バランシング モードは、発信元および宛先 IP L4 ポートです。非 IP トラフィックのデフォルト ロード バランシング モードは、送信元および宛先 MAC アドレスです。**port-channel load-balance** コマンドを使用し、 して、チャネル グループ バンドルのインターフェイス間のロード バランシング方式を設定します。レイヤ 2 パケットのデフォルト方式は src-dst-mac です。レイヤ 3 パケットのデフォルトの方式は src-dst IP です。

次のいずれかの方式を使用するデバイスを設定し、ポート チャネル全体をロード バランシングできます。

- 宛先 IP アドレス
- 送信元 IP アドレス
- 送信元および宛先 IP アドレス
- 送信元 MAC アドレス
- 宛先 MAC アドレス
- 送信元および宛先 MAC アドレス

非 IP およびレイヤ 3 ポート チャネルはどちらも設定したロード バランシング方式に従い、発信元、宛先、または発信元および宛先パラメータを使用します。たとえば、発信元 IP アドレスを使用するロード バランシングを設定すると、すべての非 IP トラフィックは発信元 MAC アドレスを使用してトラフィックをロードバランシングしますが、レイヤ 3 トラフィックは発信元 IP アドレスを使用してトラフィックをロード バランシングします。同様に、宛先 MAC

アドレスをロードバランシング方式として設定すると、すべてのレイヤ3トラフィックは宛先IPアドレスを使用しますが、非IPトラフィックは宛先MACアドレスを使用してロードバランシングします。

ユニキャストおよびマルチキャスト トラフィックは、**show port-channel load-balancing**コマンド出力に表示される設定済みのロードバランシングアルゴリズムに基づいて、ポートチャネルリンク間でロードバランシングが行われます。

マルチキャスト トラフィックは、次の方式を使用してポート チャネルのロード バランシングを行います。

- レイヤ4情報を持つマルチキャスト トラフィック：送信元IPアドレス、送信元ポート、宛先IPアドレス、宛先ポート
- レイヤ4情報を持たないマルチキャスト トラフィック：発信元IPアドレス、宛先IPアドレス
- 非IPマルチキャスト トラフィック：発信元MACアドレス、宛先MACアドレス

（注） Cisco IOSを実行するデバイスは、port-channel hash-distributionコマンドによって単一のメンバーに障害が発生した場合、メンバー ポートASICの動作を最適化できます。Cisco Nexus 3550-Tのデバイスはこの最適化をデフォルトで実行し、このコマンドを必要とせず、またサポートしません。Cisco NX-OSは、デバイス全体に対して、port-channel load-balanceコマンドによるポート チャネル上のロードバランシング基準のカスタマイズをサポートします。

LACP

LACPでは、最大4のインターフェイスを1つのポート チャネルに設定できます。

LACPの概要

イーサネットのリンク アグリゲーション制御プロトコル（LACP）は、IEEE 802.1AXおよびIEEE 802.3adで定義されています。このプロトコルは、物理ポートをまとめて1つの論理チャネルを形成する方法を制御します。

（注） LCAPは、使用する前にイネーブルにする必要があります。デフォルトでは、LACPはディセーブルです。LACPの有効化については、「*LACP*の有効化」のセクションを参照してください。

システムはこの機能をディセーブルにする前のチェックポイントを自動的に取得するため、このチェックポイントにロールバックできます。ロールバックおよびチェックポイントについては、『*Cisco Nexus® 3550-T* システム管理構成』のセクションを参照してください。

個別リンクを LACP ポート チャネルおよびチャネル グループに組み込み、個別リンクとして機能させることが可能です。

LACP では、最大 4 つのインターフェイスを 1 つのチャネル グループにまとめることができます。

（注） ポート チャネルを削除すると、ソフトウェアは関連付けられたチャネル グループを自動的に削除します。すべてのメンバ インターフェイスはオリジナルの設定に戻ります。

LACP 設定が 1 つでも存在する限り、LACP をディセーブルにはできません。

ポートチャネル モード

ポートチャネルの個別インターフェイスは、チャネルモードで設定します。スタティック ポート チャネルを集約プロトコルを使用せずに実行すると、チャネル モードは常に **on** に設定されます。デバイス上で LACP をグローバルにイネーブルにした後、各チャネルの LACP をイネーブルにします。それには、各インターフェイスのチャネル モードを **active** または **passive** に設定します。チャネル グループにリンクを追加すると、LACP チャネル グループの個別リンクにチャネル モードを設定できます。

（注） **active** または **passive** のチャネル モードで、個々のインターフェイスを設定するには、まず、LACP をグローバルにイネーブルにする必要があります。

次の図は、チャネル モードをまとめたものです。

表 *4:* ポート チャネルの個別リンクのチャネル モード

チャネル モード	説明
passive	LACP はこのポート チャネルでイネーブルになっており、ポートはパッシブ ネゴシエーション状態になっています。ポートは受信した LACP パケットに応答しますが、LACP ネゴシエーションは開始しません。
active	LACP はこのポートチャネルでイネーブルになっており、ポートはアクティブ ネゴシエーション状態です。アクティブモードでは、ポートは LACP パケットを送信することによって他のポートとのネゴシエーションを開始します。

チャネル モード	説明
on	LACP はこのポート チャネルでディセーブルであり、ポートは非ネゴシエーション状態です。ポートチャネルが **on** 状態であることは、スタティック モードであることを表します。 ポートはポート チャネル メンバーシップの確認またはネゴシエートを行いません。LACP をイネーブルにする前にチャネル モードをアクティブまたはパッシブにしようとすると、デバイス表示はエラー メッセージを表示します。LACP は、**on** 状態のインターフェイスとネゴシエートする場合、LACP パケットを受信しないため、そのインターフェイスと個別のリンクを形成します。つまり、LACP チャネル グループには参加しません。**on** 状態が、デフォルト ポート チャネル モードです。

LACPは、パッシブおよびアクティブ モードの両方でポート間をネゴシエートして、ポート速度やトランキング ステートなどを基準にしてポート チャネルを形成できるかどうかを決定します。パッシブ モードは、リモート システムやパートナーが LACP をサポートするかどうか不明の場合に役に立ちます。

次の例のようにモードに互換性がある場合、ポートの LACP モードが異なれば、2 つのデバイスは LACP ポート チャネルを形成できます。

表 *5:* チャネルモードの互換性

デバイス 1 > ポート-1	デバイス 2 > ポート-2	結果
アクティブ	アクティブ	ポート チャネルを形成できます。
Active	Passive	ポート チャネルを形成できます。
パッシブ	パッシブ	ネゴシエーションを開始できるポートがないため、ポート チャネルを形成できません。
点灯	アクティブ	LACPが片側でのみ有効になっているため、ポート チャネルを形成できません。
点灯	パッシブ	LACP が有効になっていないため、ポート チャネルを形成できません。

LACP ID パラメータ

ここでは、LACP パラメータについて説明します。

LACP システム プライオリティ

LACP を実行するどのシステムにも LACP システム プライオリティ値があります。このパラメータのデフォルト値である 32768 をそのまま使用するか、1 ～ 65535 の範囲で値を設定できます。LACP は、このシステム プライオリティと MAC アドレスを組み合わせてシステム ID を生成します。また、システム プライオリティを他のデバイスとのネゴシエーションにも使用します。システム プライオリティ値が大きいほど、プライオリティは低くなります。

（注） LACP システム ID は、LACP システム プライオリティ値と MAC アドレスを組み合わせたものです。

LACP ポート プライオリティ

LACP を使用するように設定されたポートにはそれぞれ LACP ポート プライオリティがあります。デフォルト値である 32768 をそのまま使用するか、1 ～ 65535 の範囲で値を設定できます。LACP では、ポート プライオリティおよびポート番号によりポート ID が構成されます。

また、互換性のあるポートのうち一部を束ねることができない場合に、どのポートをスタンバイ モードにし、どのポートをアクティブ モードにするかを決定するのに、ポート プライオリティを使用します。LACP では、ポート プライオリティ値が大きいほど、プライオリティは低くなります。指定ポートが、より低い LACP プライオリティを持ち、ホット スタンバイ リンクではなくアクティブ リンクとして選択される可能性が最も高くなるように、ポート プライオリティを設定できます。

LACP 管理キー

LACP は、LACP を使用するように設定されたポートごとに、チャネル グループ番号と同じ管理キー値を自動的に設定します。管理キーにより、他のポートとともに集約されるポートの機能が定義されます。他のポートとともに集約されるポートの機能は、次の要因によって決まります。

- ポートの物理特性。データ レートやデュプレックス性能などです。
- ユーザが作成した設定に関する制約事項

LACP がイネーブルのポート チャネルとスタティック ポート チャネルの相違点

次の表に、LACP がイネーブルのポート チャネルとスタティック ポート チャネルの主な相違点を示します。

表 *6 : LACP* がイネーブルのポート チャネルとスタティック ポート チャネル

構成	LACP がイネーブルのポート チャネル	スタティック ポート チャネル
適用されるプロトコル	グローバルにイネーブル	N/A
リンクのチャネル モード	次のいずれか • Active • Passive	On だけ
チャネルを構成する最大リンク数	4	4

LACP 互換性の拡張

Cisco Nexus 3550-T のデバイスが非 Nexus ピアに接続されている場合、そのグレースフル フェールオーバーのデフォルトが、無効にされたポートがダウンになるための時間を遅らせる可能性があります。また、ピアからのトラフィックを喪失する原因にもなります。これらの条件に対処するため、 **lacp graceful-convergence** コマンドが追加されました。

デフォルトで、ピアから LACP PDU を受信しない場合、ポートは一時停止状態に設定されます。 **lacp suspend-individual** は Cisco Nexus® 3550-T スイッチではデフォルト構成です。このコマンドは、LACP PDU を受信しない場合、ポートを中断状態にします。場合によっては、この機能は誤設定によって作成されるループの防止に役立ちますが、サーバが LACP にポートを論理的アップにするように要求するため、サーバの起動に失敗する原因になることがあります。 **no lacp suspend-individual** コマンドを使用して、ポートを個別の状態に設定できます。個々に設定されているポートは、ポート設定に基づいて個々のポートの属性を取得します。

LACP ポートチャネルは、サーバとスイッチを接続すると、リンクの迅速なバンドルのために LACP PDU を交換します。ただし、PDU が受信されない場合は、リンクが中断状態になります。

delayed LACP 機能により、LACP PDU の受信前に 1 つのポートチャネル メンバー（遅延 LACP ポート）がまず通常のポートチャネルのメンバーとしてアップできます。このメンバーが LACP モードで接続した後に、他のメンバー（補助 LACP ポート）がアップします。これにより、PDU が受信されない場合にリンクが中断状態になることが回避されます。

ポートチャネルのどのポートが最初に起動するかは、ポートのポートプライオリティ値によって決まります。プライオリティ値が最も低いポート チャネルのメンバー リンクが、LACP 遅延ポートとして最初に起動します。リンクの動作ステータスに関係なく、LACP ポートに設定されたプライオリティが使用され、遅延 lacp ポートが選択されます。

この機能は、レイヤ 2 ポート チャネル、トランク モード スパニング ツリーをサポートします。

- 同じポートチャネルで **no lacp suspend-individuallacp mode delay** を使用することは、非 lacp 遅延ポートを個別の状態にする可能性があるため、推奨されません。ベスト プラクティスとして、これら 2 つの設定を組み合わせないようにする必要があります。
- レイヤ 3 ポート チャネルではサポートされません。

LACP ポート チャネルの最小リンクおよび MaxBundle

ポートチャネルは、同様のポートを集約し、単一の管理可能なインターフェイスの帯域幅を増加させます。

最小リンクおよびmaxbundle機能の導入により、LACP ポート チャネル動作を改善し、単一の管理可能なインターフェイスの帯域幅を増加させます。

LACP ポート チャネルの最小リンク機能は次の処理を実行します。

- LACP ポート チャネルにリンク アップし、バンドルする必要があるポートの最小数を設定します。
- 低帯域幅の LACP ポート チャネルがアクティブにならないようにします。
- 必要な最小帯域幅を提供するアクティブ メンバー ポートが少数の場合、LACPポートチャネルが非アクティブになります。

LACP MaxBundle は、LACP ポート チャネルで許可されるバンドル ポートの最大数を定義します。

LACP MaxBundle 機能では、次の処理が行われます。

- LACP ポート チャネルのバンドル ポートの上限数を定義します。
- バンドル ポートがより少ない場合のホット スタンバイ ポートを可能にします。（たとえば、5 つのポートを含む LACP ポート チャネルにおいて、ホット スタンバイ ポートとしてそれらのポートの 2 つを指定できます）。

（注） 最小リンクおよびmaxbundle機能は、LACP ポート チャネルだけで動作します。ただし、デバイスでは非 LACP ポート チャネルでこの機能を設定できますが、機能は動作しません。

LACP 高速タイマー

LACP タイマー レートを変更することにより、LACP タイムアウトの時間を変更することができます。lacp rate コマンドを使用すれば、LACP がサポートされているインターフェイスに LACP制御パケットを送信する際のレートを設定できます。タイムアウト レートは、デフォルトのレート（30 秒）から高速レート（1 秒）に変更することができます。このコマンドは、LACP がイネーブルになっているインターフェイスでのみサポートされます。LACP 高速タイ

マー レートを構成するには、「*LACP* 高速タイマー レートの構成」のセクションを参照してください。

ポート チャネリングの前提条件

ポート チャネリングには次の前提条件があります。

- デバイスにログインしていること。
- シングル ポート チャネルのすべてのポートは、レイヤ 2 またはレイヤ 3 ポートであること。
- シングル ポート チャネルのすべてのポートが、互換性の要件を満たしていること。互換性の要件の詳細については、互換性要件 （55 ページ） セクションを参照してください。

注意事項と制約事項

ポート チャネル設定時のガイドラインおよび制約事項は、次のとおりです。

- キーワードが付いている**show**コマンド**internal**はサポートされていません。
- LACP ポートチャネルの最小リンクおよび maxbundle 機能は、ホスト インターフェイス ポート チャネルではサポートされていません。
- この機能を使用する前に LACP をイネーブルにする必要があります。
- デバイスに複数のポート チャネルを設定できます。
- 共有および専用ポートは同じポート チャネルに設定できません（共有ポートおよび専用ポートについては、「基本インターフェイス パラメータの構成」のセクションを参照してください。）
- レイヤ 2 ポート チャネルでは、ポートに互換性が設定されていれば、STP ポート パス コストが異なる場合でもポートチャネルを形成できます。互換性の要件の詳細については、互換性要件 （55 ページ） セクションを参照してください。
- STP では、ポートチャネルのコストはポート メンバーの集約帯域幅に基づきます。
- ポートチャネルを設定した場合、ポートチャネルインターフェイスに適用した設定はポートチャネル メンバ ポートに影響を与えます。メンバ ポートに適用した設定は、設定を適用したメンバ ポートにだけ影響します。
- LACP は半二重モードをサポートしません。LACP ポート チャネルの半二重ポートは中断ステートになります。
- Cisco Nexus 3550-T スイッチは、システム全体で最大 48 個のポート チャネルをサポートできます。

- Cisco Nexus 3550-T スイッチでは、8 個のポートが同じポート グループに属しています。同じポート グループのすべてのポートは同じ速度である必要があります。ポート チャネルごとに最大 8 つのメンバー ポート。すべてのメンバー ポートは同じポート グループである必要があります。

デフォルト設定

次の表に、ポートチャネル パラメータのデフォルト設定を示します。

表 7: デフォルト ポート チャネル パラメータ

パラメータ	デフォルト
ポート チャネル	管理アップ
レイヤ 3 インターフェイスのロード バランシング方式	送信元および宛先 IP アドレス
レイヤ 2 インターフェイスのロード バランシング方式	送信元および宛先 MAC アドレス
モジュールごとのロード バランシング	ディセーブル
LACP	ディセーブル
チャンネル モード	on
LACP システム プライオリティ	32768
LACP ポート プライオリティ	32768
LACP 用最少リンク数	1
Maxbundle	8
Maxbundle	4

ポート チャネルの構成

（注） ポート チャネル インターフェイスに IPv4 アドレスを構成する手順については、「レイヤ *3* インターフェイスの構成」の章を参照してください。

（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。

ポート チャネルの作成

チャネル グループを作成する前に、ポート チャネルを作成します。関連するチャネル グループは自動的に作成されます。

（注） ポート チャネルがチャネル グループの前に作成されると、ポート チャネルは、メンバー インターフェイスが設定されるインターフェイス属性のすべてを使用して設定される必要があります。**switchport mode trunk** {*allowed vlan vlan-id* | *native vlan-id*} コマンドを使用して、 メンバーを設定します。

これは、チャネル グループのメンバがレイヤ 2 ポート（switchport）およびトランク（switchport mode trunk）の場合にのみ必要です。

（注） **no interface port-channel** コマンドを使用して、ポート チャネルを削除し、関連するチャネル グループを削除します。

コマンド	目的
no interface port-channel *channel-number* 例： `switch(config)# no interface port-channel 1`	ポートチャネルを削除し、関連するチャネル グループを削除します。

始める前に

LACP ベースのポート チャネルにする場合は LACP をイネーブルにします。

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

	コマンドまたはアクション	目的

ステップ 2	**interface port-channel** *channel-number*
	例：
	`switch(config)# interface port-channel 1`
	`switch(config-if)`
		設定するポート チャネル 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。範囲は 1 ～ 4096 です。Cisco NX-OS ソフトウェアは、チャネル グループがない場合はそれを自動的に作成します。

ステップ 3	**show port-channel summary** 例： `switch(config-router)# show port-channel summary`	（任意）ポート チャネルに関する情報を表示します。

ステップ 4	**no shutdown**
	例：
	`switch# configure terminal`
	`switch(config)# int e1/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 5	**copy running-config startup-config** 例： `switch(config)# 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、ポート チャネルの作成方法を示しています。

```
switch# configure terminal
switch (config)# interface port-channel 1
```

ポート チャネルを削除したときのインターフェイス構成の変化について詳しくは、互換性要件 （55 ページ） のセクションを参照してください。

レイヤ 2 ポートをポート チャネルに追加

新しいチャネル グループまたはすでにレイヤ 2 ポートを含むチャネル グループにレイヤ 2 ポートを追加できます。ポート チャネルがない場合は、このチャネル グループに関連付けられたポート チャネルが作成されます。

（注） **no channel-group** コマンドを使用して、チャネル グループからポートを削除します。

コマンド	目的
no channel-group 例： `switch(config)# no channel-group`	チャネル グループからポートを削除します。

始める前に

LACP ベースのポート チャネルにする場合は LACP をイネーブルにします。

すべてのレイヤ 2 メンバ ポートは、全二重モードで同じ速度で実行されている必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`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** *type slot/port*
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		チャネル グループに追加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	**switchport** 例： `switch(config)# switchport`	インターフェイスをレイヤ 2 アクセス ポートとして設定します。
ステップ 4	**switchport mode trunk** 例： `switch(config)# switchport mode trunk`	（任意）インターフェイスをレイヤ2 トランク ポートとして設定します。

ステップ 5	**switchport trunk** {**allowed vlan** *vlan-id* | **native** *vlan-id*}
	例：
	`switch(config)# switchport trunk native 3`
	`switch(config-if)#`
		（任意）レイヤ 2 トランク ポートに必要なパラメータを設定します。

	コマンドまたはアクション	目的
ステップ 6	**channel-group** *channel-number*[**force**] [**mode** {**on** | **active** | **passive**}] 例： • `switch(config-if)# channel-group 5` • `switch(config-if)# channel-group 5 force`	チャネル グループ内にポートを設定し、モードを設定します。channel-number の指定できる範囲は 1 ～ 4096 です。ポート チャネルがない場合は、このチャネル グループに関連付けられたポート チャネルが作成されます。すべてのスタティック ポート チャネル インターフェイスは、**on** モードに設定されます。すべての LACP 対応ポート チャネルインターフェイスを **active** または **passive** に設定する必要があります。デフォルト モードは **on** です。 （任意）一部の設定に互換性がないインターフェイスをチャネルに追加します。強制されるインターフェイスは、チャネル グループと同じ速度、デュプレックス、およびフロー制御設定を持っている必要があります。
ステップ 7	**show interface** *type slot/port* 例： `switch# show interface port channel 5`	（任意）インターフェイスの内容を表示します。

ステップ 8	**no shutdown**
	例：
	`switch# configure terminal`
	`switch(config)# int e1/4`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 9	**copy running-config startup-config** 例： `switch(config)# 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、レイヤ 2 イーサネット インターフェイス 1/4 をチャネル グループ 5 に追加する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
```

```
switch(config-if)# switchport
switch(config-if)# channel-group 5
```

レイヤ 3 ポートをポート チャネルに追加

新しいチャネル グループまたはすでにレイヤ 3 ポートが設定されているチャネル グループにレイヤ 3 ポートを追加できます。ポート チャネルがない場合は、このチャネル グループに関連付けられたポート チャネルが作成されます。

追加するレイヤ 3 ポートに IP アドレスが設定されている場合、ポートがポート チャネルに追加される前にその IP アドレスは削除されます。レイヤ 3 ポート チャネルを作成したら、ポート チャネル インターフェイスに IP アドレスを割り当てることができます。

（注） **no channel-group** コマンドを使用して、チャネル グループからポートを削除します。チャネル グループから削除されたポートは元の設定に戻ります。このポートの IP アドレスを再設定する必要があります。

コマンド	目的
no channel-group 例： `switch(config)# no channel-group`	チャネル グループからポートを削除します。

始める前に

LACP ベースのポート チャネルにする場合は LACP をイネーブルにします。

レイヤ 3 インターフェイスに設定した IP アドレスがあれば、この IP アドレスを削除します。

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** *type slot/port*
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		チャネル グループに追加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	**no switchport** 例：	インターフェイスをレイヤ 3 ポートとして設定します。

	コマンドまたはアクション	目的
	`switch(config-if)# no switchport`	
ステップ 4	**channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}] 例： • `switch(config-if)# channel-group 5` • `switch(config-if)# channel-group 5 force`	チャネル グループ内にポートを設定し、モードを設定します。channel-number の指定できる範囲は 1 ～ 4096 です。ポート チャネルがない場合は、このチャネル グループに関連付けられたポート チャネルが作成されます。 （任意）一部の設定に互換性がないインターフェイスをチャネルに追加します。強制されるインターフェイスは、チャネル グループと同じ速度、デュプレックス、およびフロー制御設定を持っている必要があります。
ステップ 5	**show interface** *type slot/port* 例： `switch# show interface ethernet 1/4`	（任意）インターフェイスの内容を表示します。

ステップ 6	**no shutdown**
	例：
	`switch# configure terminal`
	`switch(config)# int e1/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# 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、レイヤ 3 イーサネット インターフェイス 1/5 を on モードのチャネル グループ 6 に追加する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/5
switch(config-if)# switchport
switch(config-if)# channel-group 6
```

次の例では、レイヤ 3 ポート チャネル インターフェイスを作成し、IP アドレスを割り当てる方法を示します。

```
switch# configure terminal
switch (config)# interface port-channel 4
switch(config-if)# ip address 192.0.2.1/8
```

情報目的としての帯域幅および遅延の設定

ポートチャネルの帯域幅は、チャネル内のアクティブ リンクの合計数によって決定されます。

情報目的でポート チャネル インターフェイスに帯域幅および遅延を設定します。

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 2`
	`switch(config-if)#`
		設定するポート チャネル 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	**bandwidth** *value*
	例：
	`switch(config-if)# bandwidth 60000000`
	`switch(config-if)#`
		情報目的で使用される帯域幅を指定します。有効な範囲は 1 ～ 3,200,000,000 kbs です。デフォルト値はチャネル グループのアクティブ インターフェイスの合計によって異なります。

ステップ 4	**delay** *value*
	例：
	`switch(config-if)# delay 10000`
	`switch(config-if)#`
		情報目的で使用されるスループット遅延を指定します。範囲は、1 ～ 16,777,215（10 マイクロ秒単位）です。デフォルト値は 10 マイクロ秒です。

ステップ 5	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了し、コンフィギュレーション モードに戻ります。

ステップ 6	**show interface port-channel** *channel-number* 例： `switch# show interface port-channel 2`	（任意）指定したポート チャネルのインターフェイス情報を表示します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `switch(config)# 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、ポート チャネル 5 の帯域幅および遅延の情報パラメータを設定する例を示します。

```
switch# configure terminal
switch (config)# interface port-channel 5
switch(config-if)# bandwidth 60000000
switch(config-if)# delay 10000
switch(config-if)#
```

ポート チャネル インターフェイスのシャットダウンと再起動

ポート チャネル インターフェイスをシャットダウンして再起動できます。ポート チャネル インターフェイスをシャットダウンすると、トラフィックは通過しなくなりインターフェイスは管理ダウンします。

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 2`
	`switch(config-if)#`
		設定するポート チャネル 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	**shutdown**
	例：
	`switch(config-if)# shutdown`
	`switch(config-if)#`
		インターフェイスをシャットダウンします。トラフィックは通過せず、インターフェイスは管理ダウン状態になります。デフォルトはシャットダウンなしです。
		（注）
		インターフェイスを開くには、 **no shutdown** コマンドを使用します。

	コマンドまたはアクション	目的
		インターフェイスは管理アップとなります。操作上の問題がなければ、トラフィックが通過します。デフォルトはシャットダウンなしです。

ステップ 4	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了し、コンフィギュレーション モードに戻ります。

ステップ 5	**show interface port-channel** *channel-number* 例： `switch(config-router)# show interface port-channel 2`	（任意）指定したポート チャネルのインターフェイス情報を表示します。

ステップ 6	**no shutdown**
	例：
	`switch# configure terminal`
	`switch(config)# int e1/4`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# 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、ポート チャネル 2 のインターフェイスをアップする例を示します。

```
switch# configure terminal
switch (config)# interface port-channel 2
switch(config-if)# no shutdown
```

ポート チャネルの説明の設定

ポート チャネルの説明を設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`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 2`
	`switch(config-if)#`
		設定するポート チャネル 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	**description**
	例：
	`switch(config-if)# description engineering`
	`switch(config-if)#`
		ポート チャネル インターフェイスに説明を追加できます。説明に 80 文字まで使用できます。デフォルトでは、説明は表示されません。このパラメータを設定してから、出力に説明を表示する必要があります。

ステップ 4	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了し、コンフィギュレーション モードに戻ります。

ステップ 5	**show interface port-channel** *channel-number* 例： `switch# show interface port-channel 2`	（任意）指定したポート チャネルのインターフェイス情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# 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、ポート チャネル 2 に説明を追加する例を示します。

```
switch# configure terminal
switch (config)# interface port-channel 2
switch(config-if)# description engineering
```

LACP のイネーブル化

LACP はデフォルトではディセーブルです。LACP の設定を開始するには、LACP をイネーブルにする必要があります。LACP 設定が 1 つでも存在する限り、LACP をディセーブルにはできません。

LACP は、LAN ポート グループの機能を動的に学習し、残りの LAN ポートに通知します。LACP は、正確に一致しているイーサネット リンクを識別すると、リンクを 1 つのポート チャネルとしてまとめます。次に、ポート チャネルは単一ブリッジ ポートとしてスパニング ツリーに追加されます。

LACP を設定する手順は次のとおりです。

- LACP をグローバルにイネーブルにするには、**feature lacp** コマンドを使用します。
- LACP をイネーブルにした同一ポート チャネルでは、異なるインターフェイスに異なるモードを使用できます。指定したチャネル グループに割り当てられた唯一のインターフェイスである場合に限り、モードを **active** と **passive** で切り替えることができます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	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	**feature lacp** 例： `switch(config)# feature lacp`	デバイスの LACP をイネーブルにします。
ステップ 3	**copy running-config startup-config** 例： `switch(config)# 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、LACP をイネーブルにする例を示します。

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

LACP ポート チャネル ポート モードの設定

LACP をイネーブルにしたら、LACP ポート チャネルのそれぞれのリンクのチャネル モードを **active** または **passive** に設定できます。このチャネル コンフィギュレーション モードを使用すると、リンクは LACP で動作可能になります。

関連する集約プロトコルを使用せずにポート チャネルを設定すると、リンク両端のすべてのインターフェイスは **on** チャネル モードを維持します。

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** *type slot/port*
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		チャネル グループに追加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	**channel-group** *number* **mode** {**active** | **on** | **passive**} 例： `switch(config-if)# channel-group 5 mode active`	ポート チャネルのリンクのポート モードを指定します。LACP をイネーブルにしたら、各リンクまたはチャネル全体を active または passive に設定します。 関連する集約プロトコルを使用せずにポート チャネルを実行する場合、ポートチャネル モードは常に on です。 デフォルト ポート チャネル モードは **on** です。
ステップ 4	**show port-channel summary** 例： `switch(config-if)# show port-channel summary`	（任意）ポート チャネルの概要を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# 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、LACP をイネーブルにしたインターフェイスを、チャネル グループ 5 のイーサネット インターフェイス 1/4 のアクティブ ポートチャネル モードに設定する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# channel-group 5 mode active
```

LACP ポート チャネル最少リンク数の設定

LACP の最小リンク機能を設定できます。最小リンクと maxbundles は LACP でのみ動作します。ただし、非 LACP ポート チャネルに対してこれらの機能の CLI コマンドを入力できますが、これらのコマンドは動作不能です。

（注） **no lacp min-links** コマンドを使用して、デフォルト ポートチャネル最小リンクの設定を復元します。

コマンド	目的
no lacp min-links 例： `switch(config)# no lacp min-links`	デフォルトのポートチャネル最小リンク設定を復元します。

始める前に

正しいポートチャネル インターフェイスであ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：
	`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** *number*
	例：
	`switch(config)# interface port-channel 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。

	コマンドまたはアクション	目的
ステップ 3	**lacp min-links** *number* 例： `switch(config-if)# lacp min-links 3`	ポート チャネル インターフェイスを指定して、最小リンクの数を設定します。指定できる範囲は 1 ～ 4 です。
ステップ 4	**show running-config interface port-channel** *number* 例： `switch(config-if)# show running-config interface port-channel 3`	（任意）ポート チャネル最小リンク設定を表示します。

例

次に、アップ/アクティブにするポート チャネルに関して、アップ/アクティブにするポート チャネル メンバー インターフェイスの最小数を設定する例を示します。

```
switch# configure terminal
switch(config)# interface port-channel 3
switch(config-if)# lacp min-links 3
```

LACP ポートチャネル MaxBundle の設定

LACP の maxbundle 機能を設定できます。最小リンクと maxbundles は LACP でのみ動作します。ただし、非 LACP ポート チャネルに対してこれらの機能の CLI コマンドを入力できますが、これらのコマンドは動作不能です。

（注） デフォルトのポートチャネル max-bundle 設定を復元するには、**no lacp max-bundle** コマンドを使用します。

コマンド	目的
no lacp max-bundle 例： `switch(config)# no lacp max-bundle`	デフォルトのポートチャネル max-bundle 設定を復元します。

始める前に

正しいポート チャネル インターフェイス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：
	`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** *number*
	例：
	`switch(config)# interface port-channel 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 3	**lacp max-bundle** *number* 例： `switch(config-if)# lacp max-bundle`	max-bundle を設定するポートチャネル インターフェイスを指定します。 ポート チャネルの max-bundle のデフォルト値は 8 です。指定できる範囲は 1 ～ 8 です。 ポート チャネルの max-bundle のデフォルト値は 4 です。指定できる範囲は 1 ～ 4 です。 （注） デフォルト値は 8 ですが、ポート チャネルのアクティブ メンバ数は、pc_max_links_config およびポートチャネルで許可されている pc_max_active_members の最小数です。 デフォルト値は 4 ですが、ポート チャネルのアクティブ メンバ数は、pc_max_links_config およびポートチャネルで許可されている pc_max_active_members の最小数です。
ステップ 4	**show running-config interface port-channel** *number* 例： `switch(config-if)# show running-config interface port-channel 3`	（任意）ポートチャネル max-bundle 設定を表示します。

例

次に、ポート チャネル インターフェイスの max-bundle を設定する例を示します。

```
switch# configure terminal
switch(config)# interface port-channel 3
switch(config-if)# lacp max-bundle 3
```

LACP 高速タイマー レートの設定

LACP タイマー レートを変更することにより、LACP タイムアウトの時間を変更することができます。**lacp rate** コマンドを使用し、 コマンドを使用すれば、LACP がサポートされているインターフェイスに LACP 制御パケットを送信する際のレートを設定できます。タイムアウトレートは、デフォルトのレート（30 秒）から高速レート（1 秒）に変更することができます。このコマンドは、LACP がイネーブルになっているインターフェイスでのみサポートされます。

（注） LACP タイマー レートの変更は推奨しません。HA および SSO は、LACP 高速レートのタイマーが設定されている場合はサポートされません。

始める前に

LACP 機能がイネーブルになっ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：
	`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** *type slot/port*
	例：
	`switch(config)# interface ethernet 1/4`
	`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 3	**lacp rate fast** 例： `switch(config-if)# lacp rate fast`	LACP がサポートされているインターフェイスに LACP 制御パケットを送信する際のレートとして高速レート（1 秒）を設定します。

	コマンドまたはアクション	目的
		タイムアウト レートをデフォルトにリセットするには、コマンドの **no** 形式を使用します。

例

次の例は、イーサネット インターフェイス 1/4 に対して LACP 高速レートを設定する方法を示したものです。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# lacp rate fast
```

次の例は、イーサネット インターフェイス 1/4 の LACP レートをデフォルトのレート（30 秒）に戻す方法を示したものです。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# no lacp rate fast
```

LACP システム プライオリティの設定

LACP システム ID は、LACP システム プライオリティ値と MAC アドレスを組み合わせたものです。

始める前に

LACP をイネーブルにします。

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	**lacp system-priority** *priority* 例： `switch(config)# lacp system-priority 40000`	LACP で使用するシステム プライオリティを設定します。指定できる範囲は 1 ～ 65535 で、値が大きいほどプライオリティは低くなります。デフォルト値は 32768 です。
ステップ 3	**show lacp system-identifier** 例：	（任意）LACP システム識別子を表示します。

	コマンドまたはアクション	目的
	`switch(config-if)# show lacp system-identifier`	
ステップ 4	**copy running-config startup-config** 例： `switch(config)# 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、LACP システム プライオリティを 2500 に設定する例を示します。

```
switch# configure terminal
switch(config)# lacp system-priority 2500
```

LACP ポート プライオリティの設定

LACP をイネーブルにしたら、ポート プライオリティの LACP ポート チャネルにそれぞれのリンクを設定できます。

始める前に

LACP をイネーブルにします。

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** *type slot/port*
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		チャネル グループに追加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	**lacp port-priority** *priority* 例： `switch(config-if)# lacp port-priority 40000`	LACP で使用するポート プライオリティを設定します。指定できる範囲は 1 ～ 65535 で、値が大きいほどプライオリティは低くなります。デフォルト値は 32768 です。

	コマンドまたはアクション	目的
ステップ 4	**copy running-config startup-config** 例： `switch(config-if)# 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、イーサネット インターフェイス 1/4 の LACP ポート プライオリティを 40000 に設定する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# lacp port-priority 40000
```

LACP システム MAC およびロールの設定

プロトコル交換用の LACP で使用される MAC アドレスとオプションのロールを設定できます。デフォルトでは、ロールはプライマリです。

この手順は、Cisco Nexus 3550-T スイッチでサポートされています。

始める前に

LACP を有効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# 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	**lacp system-mac** *mac-address* **role** *role-value*
	例：
	`switch(config)# lacp system-mac 000a.000b.000c role primary`
	`switch(config)# lacp system-mac 000a.000b.000c role secondary`
		LACP プロトコル交換で使用する MAC アドレスを指定します。ロールはオプションです。プライマリがデフォルトです。

ステップ 3	（任意） **show lacp system-identifier** 例： `switch(config)# show lacp system-identifier`	設定されている MAC アドレスを表示します。

	コマンドまたはアクション	目的
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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、スイッチのロールをプライマリとして設定する例を示します。

```
Switch1# sh lacp system-identifier
32768,0-b-0-b-0-b
Switch1# sh run  | grep lacp
feature lacp
lacp system-mac 000b.000b.000b role primary
```

セカンダリとしてスイッチのロールを設定する例を示します。

```
Switch2# sh lacp system-identifier
32768,0-b-0-b-0-b
Switch2# sh run | grep lacp
feature lacp
lacp system-mac 000b.000b.000b role secondary
```

LACP グレースフル コンバージェンスのディセーブル化

デフォルトで、LACP グレースフル コンバージェンスはイネーブルになっています。あるデバイスとのLACP相互運用性をサポートする必要がある場合、コンバージェンスをディセーブルにできます。そのデバイスとは、グレースフル フェールオーバーのデフォルトが、ディセーブルにされたポートがダウンになるための時間を遅らせる可能性がある、または、ピアからのトラフィックを喪失する原因にもなるデバイスです。ダウンストリーム アクセス スイッチが Cisco Nexus デバイスでない場合は、LACP グレースフル コンバージェンス オプションをディセーブルにします。

（注） このコマンドを使用する前に、ポート チャネルが管理ダウン状態である必要があります。

始める前に

LACP をイネーブルにします。

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** *number*
	例：
	`switch(config)# interface port-channel 1`
	`switch(config-if)#`
		設定するポート チャネル 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	**shutdown** 例： `switch(config-if) shutdown`	ポート チャネルを管理シャットダウンします。
ステップ 4	**no lacp graceful-convergence** 例： `switch(config-if)# no lacp graceful-convergence`	ポート チャネルの LACP グレースフル コンバージェンスをディセーブルにします。
ステップ 5	**no shutdown** 例： `switch(config-if) no shutdown`	ポート チャネルを管理アップします。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# 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、ポート チャネルの LACP グレースフル コンバージェンスをディセーブルにする方法を示します。

```
switch# configure terminal
switch (config)# interface port-channel 1
switch(config-if)# shutdown
switch(config-if)# no lacp graceful-convergence
switch(config-if)# no shutdown
```

LACP グレースフル コンバージェンスの再イネーブル化

デフォルトの LACP グレースフル コンバージェンスが再度必要になった場合、コンバージェンスを再度イネーブルにできます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`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** *number*
	例：
	`switch(config)# interface port-channel 1`
	`switch(config-if)#`
		設定するポート チャネル 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	**shutdown** 例： `switch(config-if) shutdown`	ポート チャネルを管理シャットダウンします。
ステップ 4	**lacp graceful-convergence** 例： `switch(config-if)# lacp graceful-convergence`	ポート チャネルの LACP グレースフル コンバージェンスをイネーブルにします。
ステップ 5	**no shutdown** 例： `switch(config-if) no shutdown`	ポート チャネルを管理アップします。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# 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、ポート チャネルの LACP グレースフル コンバージェンスをイネーブルにする方法を示します。

```
switch# configure terminal
switch (config)# interface port-channel 1
switch(config-if)# shutdown
switch(config-if)# lacp graceful-convergence
switch(config-if)# no shutdown
```

LACP の個別一時停止のディセーブル化

ポートがピアから LACP PDU を受信しない場合、LACP はポートを中断ステートに設定します。このプロセスは、サーバがLACPにポートを論理的アップにするように要求するときに、サーバの起動に失敗する原因になることがあります。

（注） **lacp suspend-individual** のみを入力する必要があります エッジ ポートのコマンド。このコマンドを使用する前に、ポート チャネルが管理上のダウン状態である必要があります。

始める前に

LACP をイネーブルにします。

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** *number*
	例：
	`switch(config)# interface port-channel 1`
	`switch(config-if)#`
		設定するポート チャネル 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	**shutdown** 例： `switch(config-if) shutdown`	ポート チャネルを管理シャットダウンします。
ステップ 4	**no lacp suspend-individual** 例： `switch(config-if)# no lacp suspend-individual`	ポート チャネルで LACP 個別ポートの一時停止動作をディセーブルにします。
ステップ 5	**no shutdown** 例： `switch(config-if) no shutdown`	ポート チャネルを管理アップします。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# 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、ポート チャネルで LACP 個別ポートの一時停止をディセーブルにする方法を示します。

```
switch# configure terminal
switch (config)# interface port-channel 1
switch(config-if)# shutdown
switch(config-if)# no lacp suspend-individual
switch(config-if)# no shutdown
```

LACP の個別一時停止の再イネーブル化

デフォルトの LACP 個別ポートの一時停止を再度イネーブルにできます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`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** *number*
	例：
	`switch(config)# interface port-channel 1`
	`switch(config-if)#`
		設定するポート チャネル 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	**shutdown** 例： `switch(config-if) shutdown`	ポート チャネルを管理シャットダウンします。
ステップ 4	**lacp suspend-individual** 例： `switch(config-if)# lacp suspend-individual`	ポート チャネルで LACP 個別ポートの一時停止動作をイネーブルにします。
ステップ 5	**no shutdown** 例： `switch(config-if) no shutdown`	ポート チャネルを管理アップします。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# 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、ポート チャネルで LACP 個別ポートの一時停止を再度イネーブルにする方法を示します。

```
switch# configure terminal
switch (config)# interface port-channel 1
switch(config-if)# shutdown
switch(config-if)# lacp suspend-individual
switch(config-if)# no shutdown
```

遅延 LACP の設定

遅延 LACP 機能により、LACP PDU の受信前に 1 つのポートチャネル メンバー（遅延 LACP ポート）がまず通常のポート チャネルのメンバーとしてアップできます。遅延 LACP 機能を設定するには、ポートチャネルでコマンドを使用してから、ポートチャネルの 1 つのメンバー ポートで LACP ポート プライオリティを設定します。**lacp mode delay**

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	**interface port-channel** *number*	設定するポート チャネル 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	**lacp mode delay**	遅延 LACP を有効化します。 （注） 遅延 LACP を無効にするには、 **no lacp mode delay** コマンドを使用します。 LACP ポート プライオリティを設定して、遅延 LACP の設定を完了します。詳細については、「LACP ポート プライオリティの設定」を参照してください。 LACP ポートのプライオリティによって、遅延 LACP ポートの選択が決まります。プライオリティの数値が最小のポートが選択されます。 遅延 LACP 機能を設定し、ポートチャネル フラップで有効にすると、遅延 LACP

	コマンドまたはアクション	目的
		ポートは通常のポートチャネルのメンバーとして動作し、サーバとスイッチ間でデータを交換できるようになります。最初の LACP PDU を受信すると、遅延 LACP ポートは通常のポート メンバーから LACP ポート メンバーに移行します。 （注） 遅延 LACP ポートの選択は、ポートチャネルがスイッチまたはリモート サーバでフラップするまで完了または有効になりません。

例

次に、遅延 LACP を設定する例を示します。

```
switch# config terminal
switch(config)# interface po 1
switch(config-if)# lacp mode delay


switch# config terminal
switch(config)# interface ethernet 1/1
switch(config-if)# lacp port-priority 1
switch(config-if)# channel-group 1 mode active
```

次に、遅延 LACP をディセーブルにする例を示します。

```
switch# config terminal
switch(config)# interface po 1
switch(config-if)# no lacp mode delay
```

ポートチャネル設定の確認

ポート チャネルの設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show interface port-channel *channel-number*	ポート チャネル インターフェイスのステータスを表示します。
show feature	イネーブルにされた機能を表示します。

コマンド	目的
load- interval {**interval** *seconds* {**1** | **2** | **3**}}	ビットレートとパケットレートの統計情報に対して 3 つの異なるサンプリング間隔を設定します。
show port-channel compatibility-parameters	ポート チャネルに追加するためにメンバー ポート間で同じにするパラメータを表示します。
show port-channel database [**interface port-channel** *channel-number*]	1 つ以上のポート チャネル インターフェイスの集約状態を表示します。
show port-channel load-balance	ポートチャネルで使用するロードバランシングのタイプを表示します。
show port-channel summary	ポートチャネルインターフェイスのサマリーを表示します。
show port-channel traffic	ポート チャネルのトラフィック統計情報を表示します。
show port-channel usage	使用済みおよび未使用のチャネル番号の範囲を表示します。
show lacp {**counters** [**interface port-channel** *channel-number*] | [**interface** *type/slot*] | **neighbor** [**interface port-channel** *channel-number*] | **port-channel** [**interface port-channel** *channel-number*] | **system-identifier**]]}	LACP に関する情報を表示します。
show running-config interface port-channel *channel-number*	ポート チャネルの実行コンフィギュレーションに関する情報を表示します。

ポート チャネル インターフェイス コンフィギュレーションのモニタリング

次のコマンドを使用すると、ポート チャネル インターフェイス構成情報を表示することができます。

コマンド	目的
clear counters interface port-channel *channel-number*	カウンタをクリアします。
clear lacp counters [**interface port-channel** *channel-number*]	LACP カウンタをクリアします。

コマンド	目的
load- interval {**interval** *seconds* {**1** | **2** | **3**}}	ビットレートとパケットレートの統計情報に対して 3 つの異なるサンプリング間隔を設定します。
show interface counters [**module** *module*]	入力および出力オクテット ユニキャスト パケット、マルチキャスト パケット、ブロードキャスト パケットを表示します。
show interface counters detailed [**all**]	入力パケット、バイト、マルチキャストおよび出力パケット、バイトを表示します。 （注） *[*出力ドロップ エラーを無視（*Ignore Output Dropped Errors*） *]* は、ポートに向けられたトラフィックの入力ドロップの累積を表します。ポートでの入力ドロップは、入力破棄エラーの一部として表示されます。
show interface counters errors [**module** *module*]	エラー パケットの数を表示します。 （注） *OutDiscards* は 、ポートに向けられたトラフィックの累積入力ドロップを表すため、無視します。ポートでの入力ドロップは、*InDiscards* の一部として表示されます。
show lacp counters	LACP の統計情報を表示します。

ポート チャネルの設定例

次に、LACP ポート チャネルを作成し、そのポート チャネルに 2 つのレイヤ 2 インターフェイスを追加する例を示します。

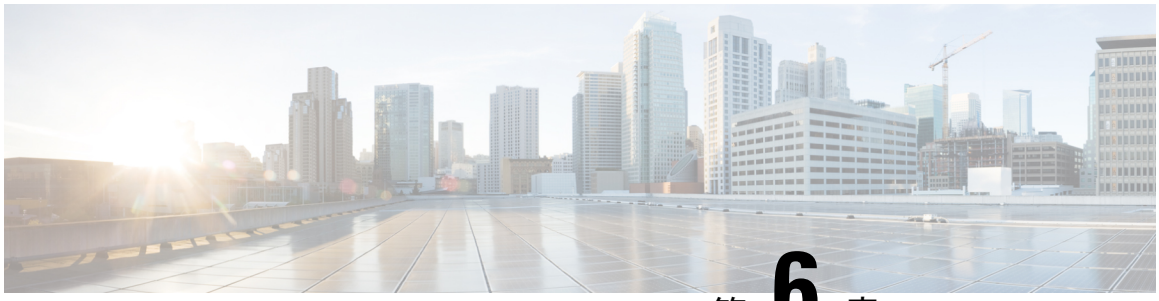
```
switch# configure terminal
switch (config)# feature lacp
switch (config)# interface port-channel 5
switch (config-if)# interface ethernet 1/4
switch(config-if)# switchport
switch(config-if)# channel-group 5 mode active
switch(config-if)# lacp port priority 40000
switch(config-if)# interface ethernet 1/7
switch(config-if)# switchport
switch(config-if)# channel-group 5 mode
```

次に、チャネル グループに 2 つのレイヤ 3 インターフェイスを追加する例を示します。Cisco NX-OS ソフトウェアはポート チャネルを自動的に作成します。

```
switch# configure terminal
switch (config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# no ip address
switch(config-if)# channel-group 6 mode active
switch (config)# interface ethernet 1/6
switch(config-if)# no switchport
switch(config-if)# no ip address
switch(config-if)# channel-group 6 mode active
switch (config)# interface port-channel 6
switch(config-if)# ip address 192.0.2.1/8
```

関連資料

関連項目	マニュアル タイトル
システム管理	「*Cisco Nexus 3550-T NX-OS* システム管理構成」セクション
ライセンス	『*Cisco NX-OS Licensing Guide*』



第 6 章

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。

（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。

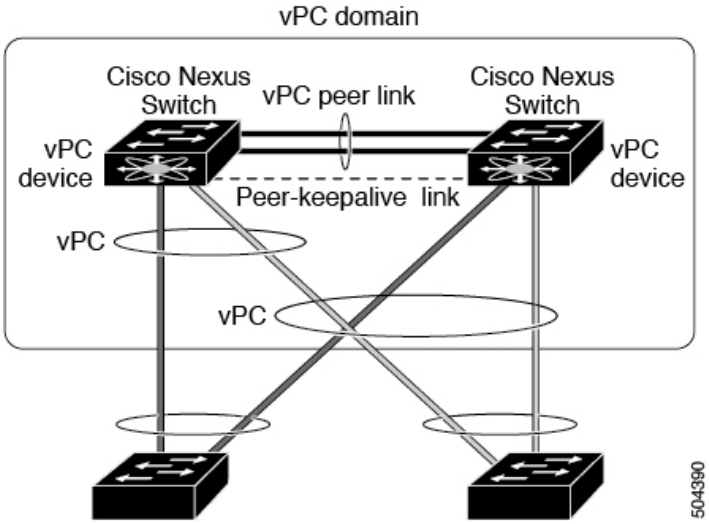
vPC について

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

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 *5: 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、同じクワッドに属している必要があります。特定のクワッドからは、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にするには、**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。

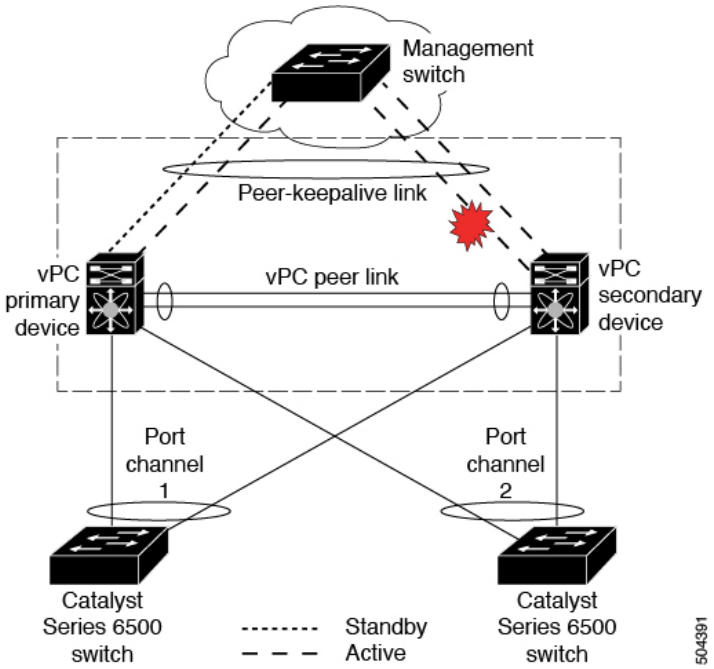
vPC の用語

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 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 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 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 *6 : vPC* ピアキープアライブ 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。

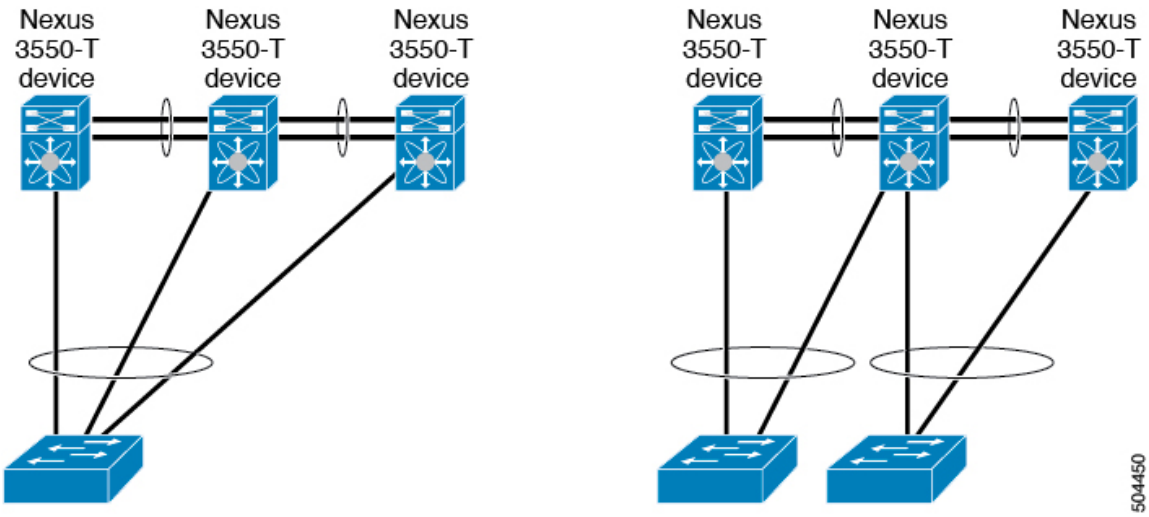
- vPC メンバ ポート：vPC に属するインターフェイス。
- デュアル アクティブ：プライマリとして動作する両方の vPC ピア。この状況は、両方のピアがまだアクティブなときに vPC ピアキープアライブとピア リンクがダウンした場合に発生します。この場合、セカンダリ vPC はプライマリ vPC が動作しないと想定し、プライマリ vPC として機能します。
- リカバリ：ピアキープアライブと vPC ピア リンクが起動すると、1 台のスイッチがセカンダリ vPC になります。セカンダリ vPC になるスイッチで、vPC リンクが停止してから復帰します。

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 *7*: 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 （115 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 （115 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。

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知します。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。

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。

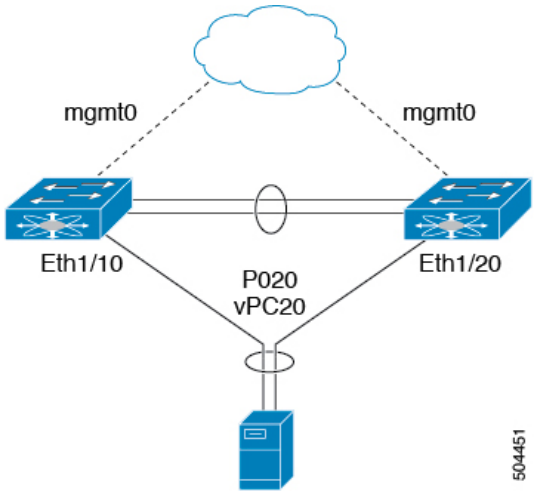
vPC ドメインを作成した後は、Cisco NX-OS ソフトウェアによって vPC ドメインのシステム プライオリティが作成されます。vPC ドメインに特定のシステム プライオリティを設定することもできます。

（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。

図 *8 : 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っ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っ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

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。

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に、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 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。

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、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 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

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 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。

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。

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。
- 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っていない 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。

- 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。

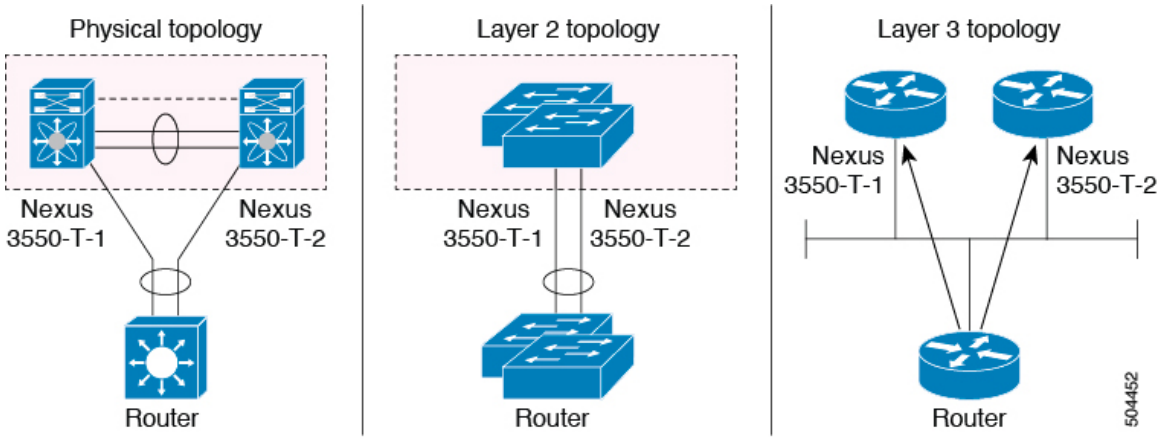
- レイヤ2では、レイヤ3デバイスはvPCピアデバイスによって提供される一意のレイヤ2スイッチを認識します。
- レイヤ 3 では、レイヤ 3 デバイスは 2 台の異なるレイヤ 3 デバイス（vPC ピア デバイスごとに 1 台）を認識します。

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 *9 : vPC*ピアデバイスのさまざまなビュー



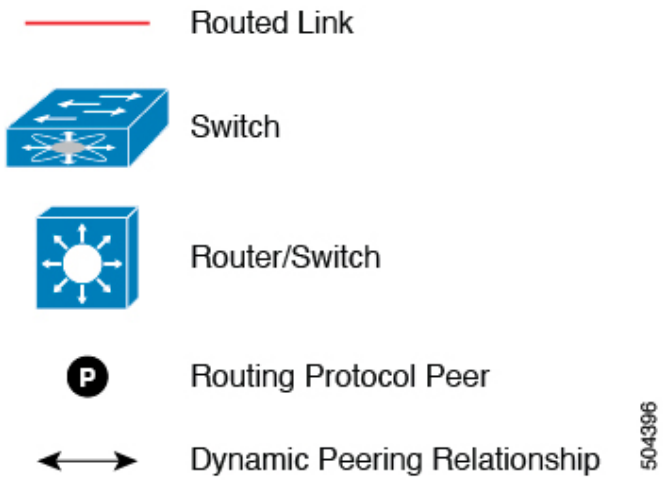
レイヤ 3 および vPC のサポートされるトポロジ

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 *10* : 凡例

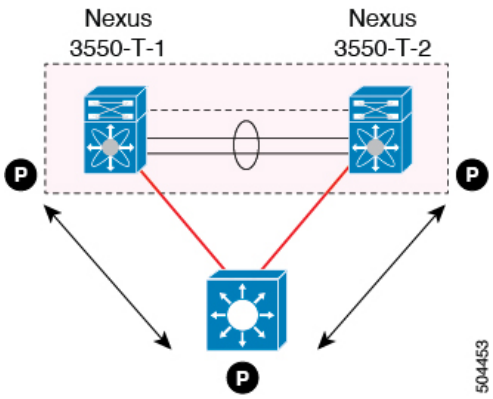


レイヤ 3 リンクを使用した外部ルータとのピアリング

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 *11* : 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。

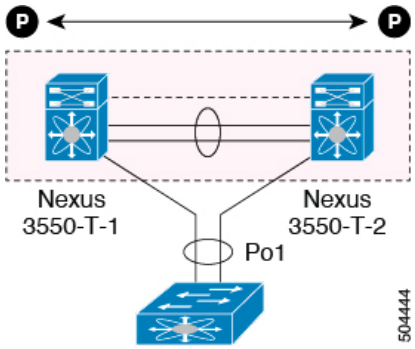
- レイヤ 3 デバイスを vPC ドメインに接続するには、独立したレイヤ 3 リンクを使用します。各リンクはポイントツーポイント レイヤ 3 接続を表し、小さな IP サブネット（/30 または /31）から取得された IP アドレスが割り当てられます。

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。

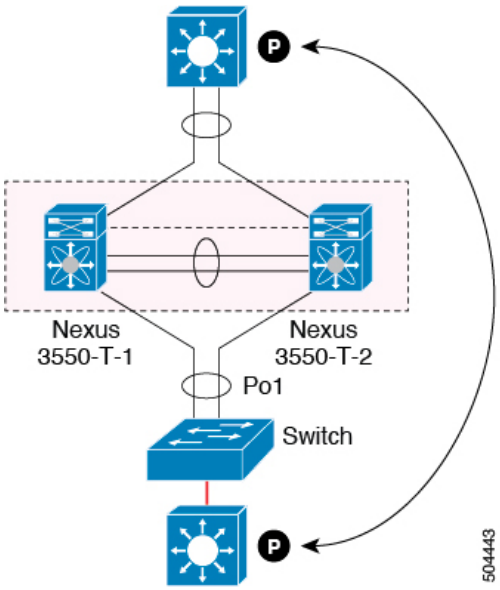
図 *12 :* バックアップ ルーティング パス用 *vPC* デバイス間のピアリング



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。

図 *13 :* ルータ間ピアリング



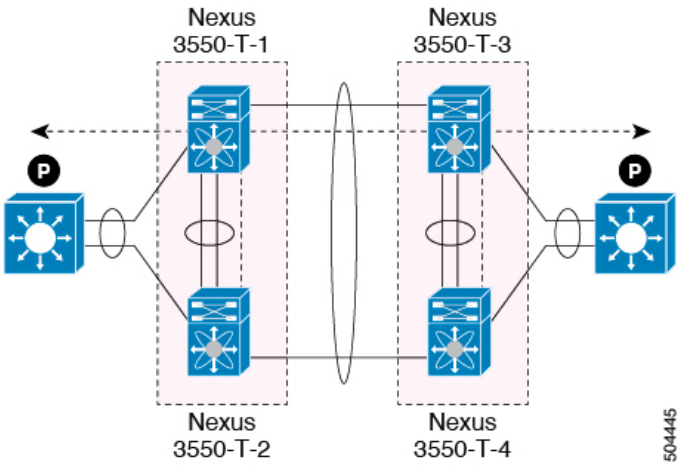
レイヤ 3 デバイスは、次の 2 つの方法で相互のピアとなることができます。また、ピアリングの方法は、このロールにどのようなデバイスが展開されるかによっても変わります。

- 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 *14* : 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

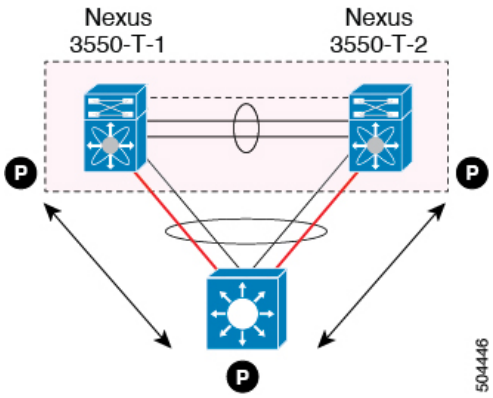
次の図に示すように、ルーテッド トラフィックとブリッジ トラフィックの両方が必要な場合は、ルーテッド トラフィックに個別のレイヤ 3 リンクを使用し、ブリッジ トラフィックに個別のレイヤ 2 ポート チャネルを使用します。

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。

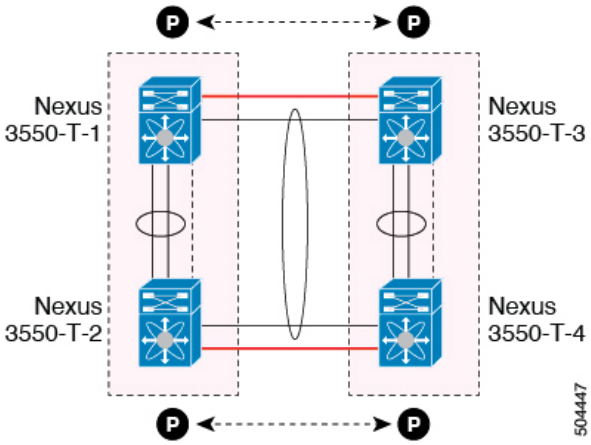
図 *15* : パラレル相互接続ルーテッド ポート上の 外部ルーターとのピアリング



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 *16* : 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。

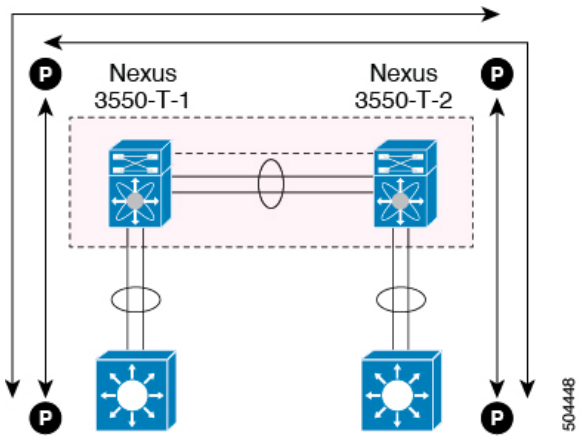
非 vPC VLAN を使用する PC 相互接続および専用スイッチ間リンクを介したピアリング

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 *17* : 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

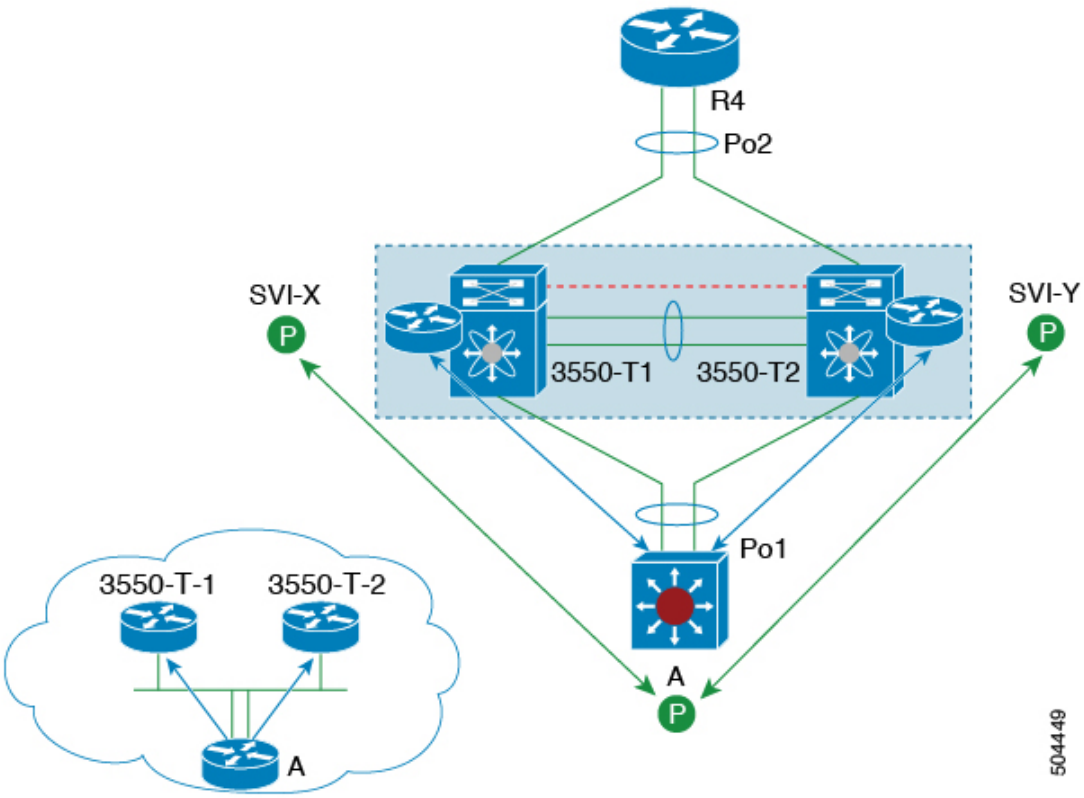


vPC 接続を介した直接ピアリング

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。

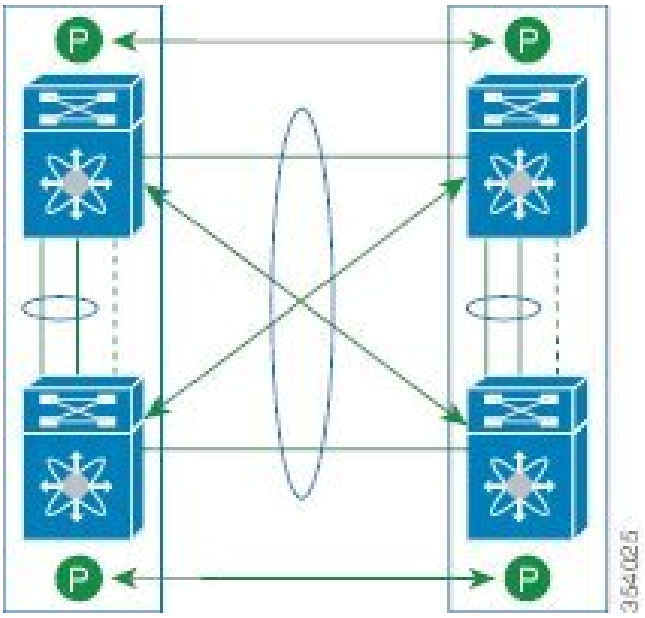
図 *18 :* サポート：ルータが両方の *vPC* ピアとピアリングする *vPC* 相互接続を介するピアリング。



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 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 *19 :* 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 *8 :* 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

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：
	`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	**feature vpc** 例： `switch(config)# feature vpc`	デバイス上で vPC をイネーブルにします。

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。

	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

	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。

	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：
	`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)#`
		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：
	`switch(config)# exit`
	`switch#`
		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。

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)#`
		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：
	`switch(config-vpc-domain)# peer-keepalive destination 172.28.230.85`
	`switch(config-vpc-domain)#`
		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：
	`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 5	**show vpc statistics** 例： `switch# show vpc statistics`	（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： `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。

	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)# 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

	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。

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 ポートチャンネルを持つ 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**	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。 （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。

	コマンドまたはアクション	目的
		このコマンドは、 PortFast ポート（スパニングツリー 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。 （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。

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：
	`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。

	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。

	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

	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	**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

	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。

	コマンドまたはアクション	目的

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 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 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)#
```

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 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
```

```
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：
	`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	**auto-recovery** [**reload-delay** *time*] 例： `switch(config-vpc-domain)# auto-recovery`	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 **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

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。

	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：
	`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。

	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 **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_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)#
```

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：
	`switch# vpc role preempt`
	`switch(config)#`
		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： `switch(config)# show vpc role`	（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 rolevPC 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

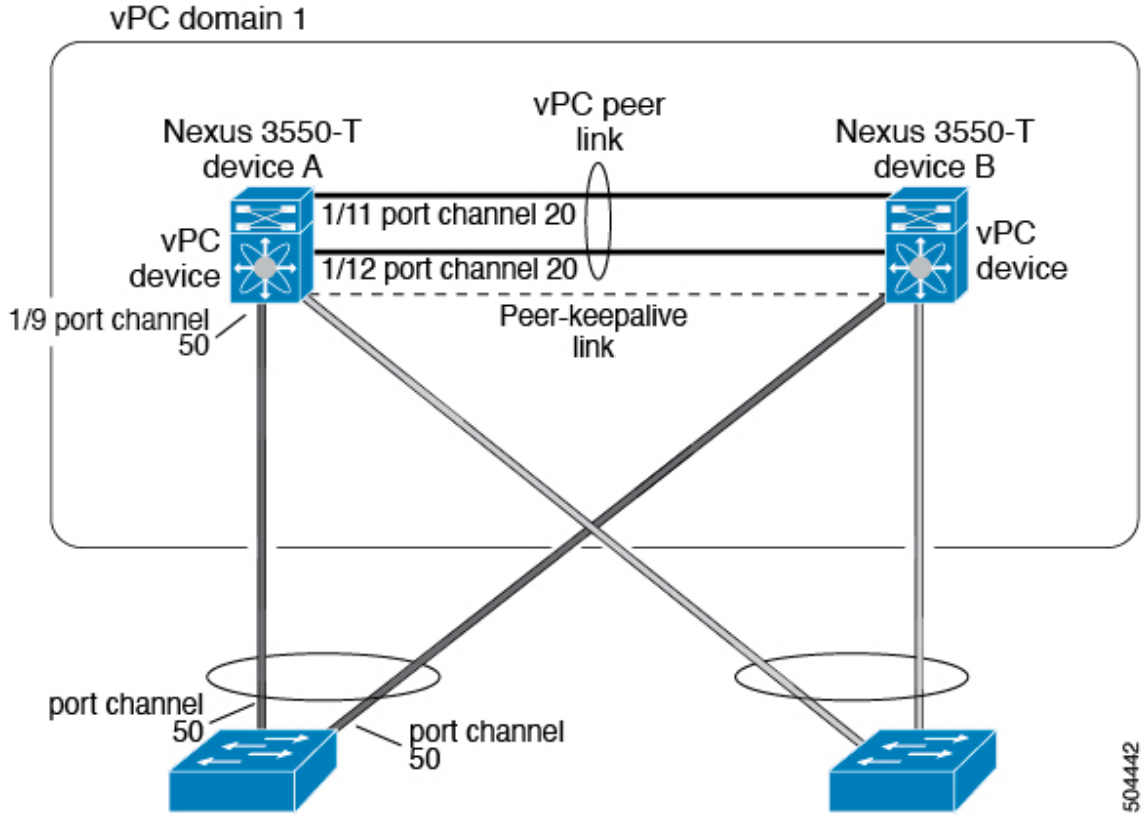
show vpc statistics コマンドを使用し、vPC統計情報を表示します。

（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 *20 : 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 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)#
```

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 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)#
```

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)#
```

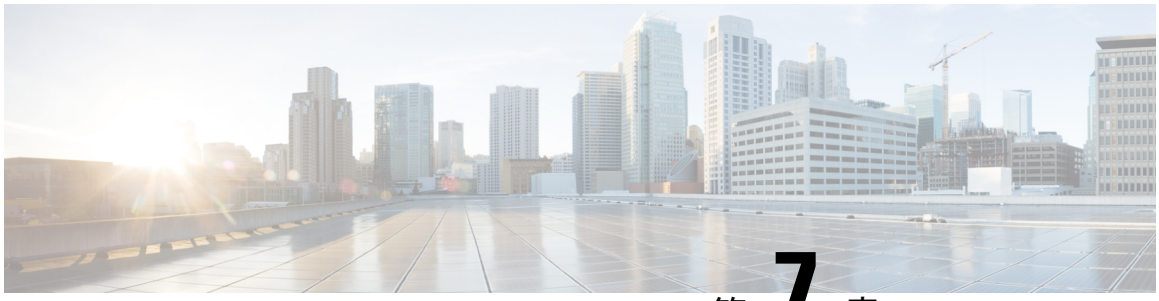
9. vPC のダウンストリーム デバイスへのポート チャネルのインターフェイスを設定します。

```
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。



第 7 章

単方向リンク検出の構成

この章は、次の項で構成されています。

単方向リンク検出

シスコ独自の単方向リンク検出（UDLD）プロトコルにより、光ファイバまたは銅線（カテゴリ 5 ケーブルなど）イーサネット ケーブルを使用して接続されたデバイスで、ケーブルの物理構成をモニタし、単一方向リンクの存在を検出することができます。デバイスで単一方向リンクが検出されると、UDLD が関係のある LAN ポートをシャットダウンし、ユーザに通知します。単一方向リンクは、さまざまな問題を引き起こす可能性があります。

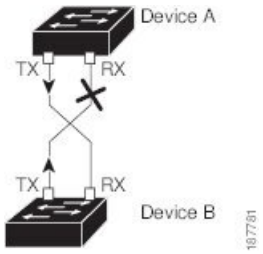
リンク上でローカルデバイスから送信されたトラフィックはネイバーで受信されるのに対し、ネイバーから送信されたトラフィックはローカルデバイスで受信されない場合には常に、単方向リンクが発生します。

Cisco Nexus 3550-T シリーズのデバイスは、UDLD をイネーブルにした LAN ポート上のネイバー デバイスに定期的に UDLD フレームを送信します。一定の時間内にフレームがエコーバックされてきて、特定の確認応答（echo）が見つからなければ、そのリンクは単一方向のフラグが立てられ、その LAN ポートはシャットダウンされます。UDLD プロトコルにより単方向リンクが正しく識別されその使用が禁止されるようにするためには、リンクの両端のデバイスで UDLD がサポートされている必要があります。UDLD フレームの送信間隔は、グローバル単位でも指定されたインターフェイスにも設定できます。

（注） UDLD は、銅線の LAN ポート上では、このタイプのメディアでの不要な制御トラフィックの送信を避けるために、ローカルでデフォルトでディセーブルになっています。

図は、単方向リンクが発生した状態の一例を示したものです。デバイス B はこのポートでデバイス A からのトラフィックを正常に受信していますが、デバイス A は同じポート上でデバイス B からのトラフィックを受信していません。UDLD によって問題が検出され、ポートがディセーブルになります。

図 *21 :* 単方向リンク



次の表に、UDLD のデフォルト設定を示します。

表 *9 : UDLD* のデフォルト設定

機能	デフォルト値
UDLD グローバル イネーブル ステート	グローバルにディセーブル
ポート別の UDLD イネーブル ステート（光ファイバ メディア用）	すべてのイーサネット光ファイバLANポートでイネーブル
ポート別のUDLDイネーブル ステート（ツイストペア（銅製）メディア用）	すべての 10Gイーサネット ポートでディセーブル済み
UDLD アグレッシブ モード	ディセーブル
UDLD メッセージの間隔	15 秒

UDLD モード

UDLD は、アグレッシブ モードと非アグレッシブ モードの2 つのモードで動作できます。

デフォルトでは、UDLDアグレッシブ モードはディセーブルになっています。UDLDアグレッシブ モードは、UDLD アグレッシブ モードをサポートするネットワーク デバイスの間のポイントツーポイントのリンク上に限って設定できます。UDLD アグレッシブ モードをイネーブルに設定した場合、UDLD近接関係が設定されている双方向リンク上のポートがUDLDフレームを受信しなくなったとき、UDLDはネイバーとの接続を再確立しようとします。この再試行に 8 回失敗すると、ポートはディセーブルになります。

UDLD アグレッシブ モードをイネーブルにすると、次のようなことが発生します。

リンクの一方にポート スタックが生じる（送受信どちらも）

リンクの一方がダウンしているにもかかわらず、リンクのもう一方がアップしたままになる

このような場合、UDLD アグレッシブ モードでは、リンクのポートの 1 つがディセーブルになり、トラフィックが廃棄されるのを防止します。

（注） UDLD アグレッシブ モードをすべてのファイバ ポートでイネーブルにするには、UDLD アグレッシブ モードをグローバルでイネーブルにします。指定されたインターフェイスの銅ポートで、UDLD アグレッシブ モードをイネーブルにする必要があります。

UDLD モードの設定

単一方向リンク検出（UDLD）を実行するように設定されているデバイス上のイーサネットインターフェイスには、ノーマル モードの UDLD を設定できます。

インターフェイスの UDLD モードをイネーブルにするには、そのインターフェイスを含むデバイス上で UDLD を事前にイネーブルにしておく必要があります。UDLD は他方のリンク先のインターフェイスおよびそのデバイスでもイネーブルになっている必要があります。

（注） インターフェイスが銅線ポートの場合は、enable UDLD コマンドを使用して UDLD をイネーブルにする必要があります。インターフェイスがファイバ ポートの場合、インターフェイスで UDLD を明示的にイネーブルにする必要はありません。ただし、enable UDLD コマンドを使用してファイバポートで UDLD をイネーブルにしようとすると、それが有効なコマンドではないことを示すエラー メッセージが表示されることがあります。

以下の表に、異なるインターフェイスで UDLD をイネーブルおよびディセーブルにする CLI 詳細を示します。

表 *10*：異なるインターフェイスで *UDLD* をイネーブルおよびディセーブルにする *CLI* 詳細

説明	ファイバ ポート	銅線またはファイバ以外のポート
デフォルト設定	有効	無効
enable UDLD コマンド	**no udld disable**	**udld enable**
disable UDLD コマンド	**udld disable**	**no udld enable**

始める前に

他方のリンク先ポートおよびデバイスで UDLD をイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	[**no**] **feature udld**
	例：
	`switch(config)# feature udld`
	`switch(config)#`
	`switch(config)# no feature udld`
	`switch(config)#`
		デバイスの UDLD をイネーブル/ディセーブルにします。

ステップ 3	**udld message-time** *seconds*
	例：
	`switch(config)# udld message-time 30`
	`switch(config)#`
		（任意）UDLD メッセージを送信する間隔を指定します。有効な範囲は 7 ～ 90 秒で、デフォルトは 15 秒です。

ステップ 4	**udld aggressive**
	例：
	`switch(config)# udld aggressive`
	`switch(config)#`
		（任意）UDLD モードをアグレッシブに指定します。
		（注）
		銅インターフェイスの場合、UDLD アグレッシブ モードに設定するインターフェイスのインターフェイス コマンド モードを入力し、インターフェイス コマンド モードでこのコマンドを発行します。

ステップ 5	**interface ethernet** *slot/port*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		（任意）設定するインターフェイスを指定します。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 6	**udld** [**enable** | **disable**]
	例：
	`switch(config-if)# udld enable`
	`switch(config-if)#`
		（任意）指定した銅線ポートの UDLD をイネーブルにしたり、指定したファイバ ポートの UDLD をディセーブルにします。
		銅線ポートで UDLD をイネーブルにするには、**udld enable** コマンドを入力します。ファイバ ポートで UDLD をイネーブルにするには、**no udld disable** コマンドを入力します。

	コマンドまたはアクション	目的

ステップ 7	**show udld** [**ethernet** *slot/port* | **global** | **neighbors**]
	例：
	`switch(config)# show udld`
	`switch(config)#`
		（任意）UDLDのステータスを表示します。

ステップ 8	**exit**
	例：
	`switch(config-if-range)# exit`
	`switch(config)#`
		インターフェイスモードを終了します。

ステップ 9	**copy running-config startup-config** 例： `switch(config)# 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、デバイスの UDLD をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature udld
switch(config)#
```

次の例では、UDLD メッセージの間隔を 30 秒に設定する方法を示します。

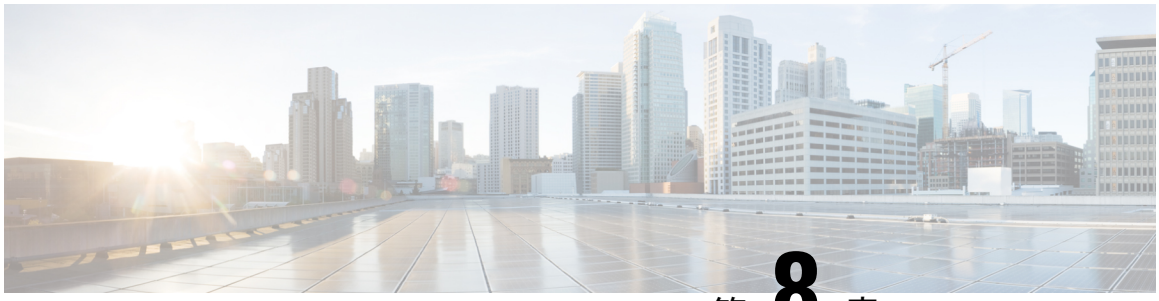
```
switch# configure terminal
switch(config)# feature udld
switch(config)# udld message-time 30
switch(config)#
```

次に、イーサネット ポートの 1/1 の UDLD を無効化にする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if-range)# no udld enable
switch(config-if-range)# exit
```

次に、デバイスの UDLD をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature udld
switch(config)# exit
```



第 8 章

マルチキャスト フェアネス調整

マルチキャスト フェアネス

マルチキャスト トラフィックでは、1 つの送信元から複数の宛先に同時にデータを送信するため、遅延が異なる場合があります。マルチキャスト フェアネス調整機能は、異なるポート間でのマルチキャスト ストリームの遅延差を最小限に抑えることを目的としています。

Cisco NX-OS リリース 10.5(2)F 以降、Cisco Nexus 3550-T スイッチのマルチキャスト フェアネス調整機能を使用すると、特定のポートのイコライゼーション遅延を構成することで、出力マルチキャスト トラフィックを調整できます。したがって、この機能により、出力トラフィックがほぼ同時に宛先に到達することが保証されます。

高速ポートに遅延を追加することで、ポート間のマルチキャスト ストリームの遅延差を調整できます。ただし、各ポートの遅延または遅延を事前に測定し、デフォルトの遅延に注意する必要があります。そうしないと、より高速なポートで遅延を均等化できます。偏差は、250 ピコ秒未満の無視できる差に減少します。

たとえば、マルチキャスト ストリームがインターフェイス イーサネット 1/2、イーサネット 1/3、およびイーサネット 1/4 を介して送信されているとします。マルチキャスト ストリームのタイムスタンプから、N3550-T がイーサネット 1/2 から 6.85 ナノ秒、イーサネット 1/3 から 5.70 ナノ秒、イーサネット 1/4 から 6.20 ナノ秒で出ていることがわかります。調整機能を使用すると、イーサネット 1/3 で約 1000 ピコ秒の遅延を追加し、イーサネット 1/4 で約 600 ピコ秒の遅延を追加して、これらのポートから 250 ピコ秒の範囲内で各ストリームを送信できます。

マルチキャストフェアネス調整に関する注意事項と制限事項

マルチキャストフェアネス調整機能を構成する際は、次の注意事項と制約事項に従ってください。

- ライン レートよりも多くのトラフィックを送信すると、輻輳が発生し、インターフェイスは公平性を維持できなくなります。ただし、トラフィック レートが低下するとすぐに、公平性が復元されます。
- 複数の送信元からのトラフィックが同じインターフェイスから発信するために競合する場合、そのインターフェイスの遅延の公平性に影響します。
- トラフィックが実行されている特定のポートで遅延を構成しようとすると、ドロップまたは破損の形でトラフィックが短時間中断されます。

マルチキャスト フェアネス調整の構成

マルチキャスト フェアネス調整機能はインターフェイス固有の機能であるため、必要なインターフェイスに移動して機能を構成します。マルチキャストフェアネス調整機能を構成するには、次のステップを実行します。

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** *type slot/port*
	例：
	`switch(config)# interface ethernet 1/10`
	`switch(config-if)#`
		設定するインターフェイスを指定します。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	[**no**] **equalization-delay** *value*
	例：
	`switch(config-if)# equalization-delay 10`
	`switch(config-if)#`
		指定したインターフェイスで設定するイコライゼーション遅延値を指定します。デフォルト値は 0 です。
		10G ポートのイコライゼーション遅延値の範囲は 0 ～ 15 です。1 = 100 ピコ秒です。したがって、10G ポートに設定できる最大遅延は 1500 ピコ秒です。

	コマンドまたはアクション	目的
		遅延を 4 に構成すると、400 ピコ秒になります。 このコマンドの **no** 形式を使用するとコライゼーション遅延が無効になります。

ステップ 4	**shut**
	例：
	`switch(config-if)# shut`
	`switch(config)#`
		指定されたインターフェイスを無効にします。

ステップ 5	**no shut**
	例：
	`switch(config-if)# no shut`
	`switch(config)#`
		指定されたインターフェイスを有効にします。

ステップ 6	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		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。

例

次に、特定のインターフェイスでマルチキャスト フェアネス調整を構成する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/10
switch(config-if)# equalization-delay 10
switch(config-if)# shut
switch(config-if)# no shut
switch(config-if)# exit
```

マルチキャスト公平性調整の構成の検証

テーブルに記載されている関連する show コマンドを実行して、マルチキャスト公平性調整の構成に関する必要な情報を表示します。

コマンド	目的
show interface *type slot/port*	指定されたインターフェイスのインターフェイス ステータスと情報を、構成されたイコライゼーション遅延（ピコ秒単位）とともに表示します。

コマンド	目的
show interface *type slot/port* **equalization-delay**	指定されたインターフェイスの等化遅延の値だけをピコ秒単位で表示します。
show interface *type range of slots/ports* **equalization-delay**	指定したインターフェイス範囲の等化遅延のすべての値をピコ秒単位で表示します。
show running-config [**all**]	現在の設定に関する情報を表示します。**all** オプションを使用すると、デフォルトの構成と現在の構成が表示されます。 このコマンドは、各インターフェイスに構成されているイコライゼーション遅延も表示します。

Show コマンドの出力例

次に、指定したインターフェイスの等化遅延を表示する **show run interface** *type slot/port* コマンドの出力例を示します。

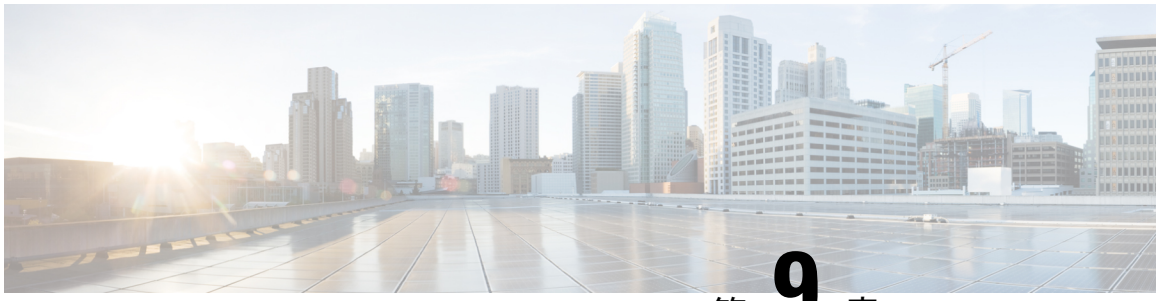
```
show run interface ethernet 1/10
  interface Ethernet1/10
  equalization-delay 10
```

次に、インターフェイスのイコライゼーション遅延に関する情報を含む、指定されたインターフェイスのインターフェイスステータスと情報を表示する **show interface** *type slot/port* コマンドの出力例を示します。

```
switch(config-if)# show int eth1/10
Ethernet1/10 is up
admin state is up, Dedicated Interface
Hardware: 1000/10000 Ethernet, address: 643f.5f84.c5bc (bia 643f.5f84.c5bc)
MTU 1500 bytes, BW 10000000 Kbit , DLY 10 usec
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, medium is broadcast
Port mode is access
full-duplex, 10 Gb/s, media type is 10G
Beacon is turned off
Auto-Negotiation is turned on FEC mode is Auto
Input flow-control is off, output flow-control is off
Auto-mdix is turned off
Rate mode is dedicated
Switchport monitor is off
EtherType is 0x8100
EEE (efficient-ethernet) : n/a
admin fec state is auto, oper fec state is auto
Equalization delay 1000 picosec
Last link flapped 4week(s) 5day(s)
Last clearing of "show interface" counters 4w4d
0 interface resets
Load-Interval #1: 30 seconds
30 seconds input rate 0 bits/sec, 0 packets/sec
30 seconds output rate 0 bits/sec, 0 packets/sec
input rate 0 bps, 0 pps; output rate 0 bps, 0 pps
Load-Interval #2: 5 minute (300 seconds)
300 seconds input rate 0 bits/sec, 0 packets/sec
```

```
300 seconds output rate 0 bits/sec, 0 packets/sec
input rate 0 bps, 0 pps; output rate 0 bps, 0 pps
RX
0 unicast packets 0 multicast packets 0 broadcast packets
0 input packets 0 bytes
0 jumbo packets 0 storm suppression packets
0 runts 0 giants 0 CRC 0 no buffer
0 input error 0 short frame 0 overrun 0 underrun 0 ignored
0 watchdog 0 bad etype drop 0 bad proto drop 0 if down drop
0 input with dribble 0 input discard
0 Rx pause
0 Stomped CRC
TX
0 unicast packets 30000 multicast packets 0 broadcast packets
30000 output packets 0 bytes
0 jumbo packets
0 output error 0 collision 0 deferred 0 late collision
0 lost carrier 0 no carrier 0 babble 0 output discard
0 Tx pause

switch(config-if)#
```



第 9 章

レイヤ 3 インターフェイスの設定

レイヤ 3 インターフェイスについて

レイヤ 3 インターフェイスは、IPv4 パケットを静的またはダイナミック ルーティング プロトコルを使って別のデバイスに転送します。レイヤ 2 トラフィックの IP ルーティングおよび内部 Virtual Local Area Network（VLAN）ルーティングにはレイヤ 3 インターフェイスが使用できます。

ルーテッド インターフェイス

ポートをレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスとして設定できます。ルーテッド インターフェイスは、IP トラフィックを他のデバイスにルーティングできる物理ポートです。ルーテッド インターフェイスはレイヤ 3 インターフェイスだけで、スパニング ツリー プロトコル（STP）などのレイヤ 2 プロトコルはサポートしません。

すべてのイーサネット ポートは、デフォルトでルーテッド インターフェイスです。CLI セットアップ スクリプトでこのデフォルトの動作を変更できます。

（注） Cisco Nexus® 3550-T スイッチ インターフェイスのデフォルト モードはレイヤ 3 です。

ポートに IP アドレスを割り当て、ルーティングをイネーブルにし、このルーテッド インターフェイスにルーティング プロトコル特性を割り当てることができます。

ルーテッド インターフェイスからレイヤ 3 ポート チャネルも作成できます。ポート チャネルの詳細については、「ポート チャネルの構成」のセクションを参照してください。

ルーテッド インターフェイス は、指数関数的に減少するレート カウンタをサポートします。Cisco NX-OS はこれらの平均カウンタを用いて次の統計情報を追跡します。

- 入力パケット数/秒
- 出力パケット数/秒

VLAN インターフェイス

VLAN インターフェイス、またはスイッチ仮想インターフェイス（SVI）、は、デバイス上の VLAN を同じデバイス上のレイヤ 3 ルータ エンジンに接続する仮想ルーテッド インターフェイスです。VLAN には 1 つの VLAN インターフェイスだけを関連付けることができますが、VLAN に VLAN インターフェイスを設定する必要があるのは、VLAN 間でルーティングする場合か、または管理 VRF（仮想ルーティング/転送）以外の VRF インスタンスを経由してデバイスを IP ホスト接続する場合だけです。VLAN インターフェイスの作成を有効にすると、Cisco NX-OS によってデフォルト VLAN（VLAN 1）に VLAN インターフェイスが作成され、リモート スイッチ管理が許可されます。

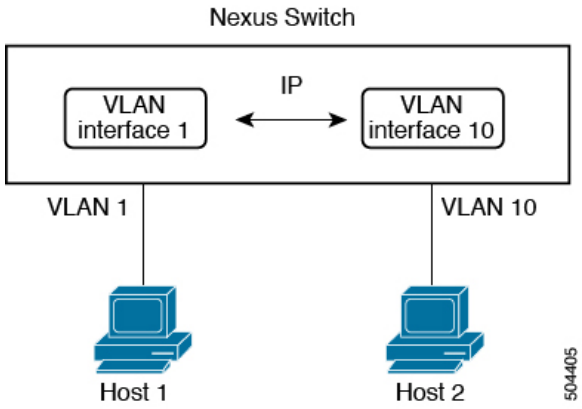
設定の前に VLAN ネットワーク インターフェイス機能をイネーブルにする必要があります。システムはこの機能をディセーブルにする前のチェックポイントを自動的に取得するため、このチェックポイントにロールバックできます。ロールバックおよびチェックポイントについては、「*Cisco Nexus® 3550-T* システム管理構成」のセクションを参照してください。

（注） VLAN 1 の VLAN インターフェイスは削除できません。

VLAN インターフェイスをルーティングするには、トラフィックをルーティングする VLAN ごとに VLAN インターフェイスを作成し、その VLAN インターフェイスに IP アドレスを割り当ててレイヤ 3 内部 VLAN ルーティングを実現します。IP アドレスおよび IP ルーティングの詳細については、「*Cisco Nexus® 3550-T* ユニキャスト ルーティングの構成」セクションを参照してください。

次の図に、デバイス上の 2 つの VLAN に接続されている 2 つのホストを示します。VLAN ごとに VLAN インターフェイスを設定し、VLAN 間の IP ルーティングを使ってホスト 1 とホスト 2 を通信させることができます。VLAN 1 は VLAN インターフェイス 1 のレイヤ 3 で、VLAN 10 は VLAN インターフェイス 10 のレイヤ 3 で通信します。

図 *22 : VLAN* インターフェイスによる *2* つの *VLAN* の接続



インターフェイスの VRF メンバーシップの変更

インターフェイスで **vrf member** コマンドを使用すると、インターフェイス設定の削除に関するアラートが表示されます。また、そのインターフェイスに関する設定を削除するようにクライアント/リスナー（CLI サーバなど）に通知されます。

system vrf-member-change retain-l3-config コマンドを入力すると、インターフェイスの VRF メンバーの変更時にもレイヤ 3 構成が保持されます。これは、既存の設定を保存（バッファ）し、古い VRF コンテキストから設定を削除し、保存された設定を新しい VRF コンテキストに再適用するために、クライアント/リスナーに通知を送信することによって行われます。

（注） **system vrf-member-change retain-l3-config** コマンドが有効になっている場合、レイヤ 3 設定は削除されず、保存（バッファ）されたままになります。このコマンドが有効になっていない場合（デフォルトモード）、VRF メンバーが変更されてもレイヤ 3 設定は保持されません。

レイヤ 3 設定の保持を無効にするには、**no system vrf-member-change retain-l3-config** コマンドを使用します。このモードでは、VRF メンバーが変更されてもレイヤ 3 設定は保持されません。

インターフェイスの VRF メンバーシップの変更に関する注意事項

- VRF名を変更すると、瞬間的なトラフィック損失が発生することがあります。
- **system vrf-member-change retain-l3-config** コマンドを有効にすると、インターフェイス レベルでの設定だけが処理されます。VRFの変更後にルーティングプロトコルに対応するには、ルータレベルで設定を手動で処理する必要があります。
- **system vrf-member-change retain-l3-config** コマンドは、次によるインターフェイス レベルの設定をサポートしています。
  - **ip address** やインターフェイス構成で使用可能なすべての OSPF/ISIS/EIGRP CLI などの CLI サーバーによって保持されるレイヤ 3 構成。

ループバック インターフェイス

ループバック インターフェイスは、常にアップ状態にある単独のエンドポイントを持つ仮想インターフェイスです。ループバック インターフェイスを通過するパケットはこのインターフェイスでただちに受信されます。ループバック インターフェイスは物理インターフェイスをエミュレートします。0 ～ 1023 の番号のループバック インターフェイスを最大 1024 個の設定できます。

ループバック インターフェイスを使用すると、パフォーマンスの分析、テスト、ローカル通信が実行できます。ループバック インターフェイスは、ルーティング プロトコル セッションの終端アドレスとして設定することができます。ループバックをこのように設定すると、アウトバウンドインターフェイスの一部がダウンしている場合でもルーティングプロトコルセッションはアップしたままです。

高可用性

レイヤ3インターフェイスは、ステートフル再起動とステートレス再起動をサポートします。切り替え後、Cisco NX-OS は実行時の設定を適用します。

高可用性の詳細については、「*Cisco Nexus® 3550-T* ユニキャスト ルーティングの構成」のセクションを参照してください。

DHCP クライアント

Cisco NX-OS は、SVI、物理イーサネット、および管理インターフェイス上の IPv4 アドレスと IPv6 アドレスに関して DHCP クライアントをサポートしています。**ip address dhcp** を使用して、DHCP クライアントの IP アドレスを設定できます。 または **ipv6 address dhcp** コマンドを使用します。これらのコマンドは、DHCPクライアントからDHCPサーバに要求を送信し、DHCPサーバからIPv4またはIPv6アドレスを要求します。Cisco Nexusスイッチ上のDHCPクライアントは、DHCPサーバに対して自身を識別します。DHCP サーバはこの ID を使用して、IP アドレスを DHCP クライアントに返します。

DHCP クライアントが SVI で DHCP サーバ送信ルータおよび DNS オプションによって設定されている場合、スイッチで **ip route** 0.0.0.0/0 *router-ip* および **ip name-server** *dns-ip* コマンドはスイッチで自動的に設定されます。

インターフェイスでの DHCP クライアントの使用に関する制限事項

次に、インターフェイスでの DHCP クライアントの使用に関する制限事項を示します。

- この機能は、物理イーサネット インターフェイス、管理インターフェイス、および SVI でのみサポートされます。
- この機能は、非デフォルトの Virtual Routing and Forwarding（VRF）インスタンスでサポートされます。
- **copy running-config startup-config** コマンドを入力すると、DNS サーバおよびデフォルト ルータ オプション関連の設定がスタートアップ コンフィギュレーションに保存されます。

スイッチをリロードするとき、この設定が適切ではない場合は、この設定を削除しなければならない可能性があります。

- スイッチで設定できる DNS サーバは最大 6 つです。これは、スイッチの制限です。この最大数には、DHCP クライアントによって設定される DNS サーバと手動で設定される DNS サーバが含まれます。

  スイッチで 7 つ以上の DNS サーバが設定されている場合、DNS オプション セットによって SVI の DHCP オファーを取得すると、IP アドレスは SVI に割り当てられません。

- Cisco Nexus 3550-T スイッチは、最大 10 の IPv4 DHCPクライアントをサポートします。
- DHCP リレーの設定と DHCP クライアントの設定には互換性がなく、同じスイッチではサポートされません。インターフェイスでDHCPクライアントを設定する前にDHCP リレーの設定を削除する必要があります。
- VLAN で DHCP スヌーピングが有効になっている場合、その VLAN の SVI が DHCP クライアントによって設定されているときは、DHCP スヌーピングが SVI DHCP クライアントで実行されません。
- IPv4 DHCPクライアントを設定する場合は、 **ipv4 address use-link-local-only** コマンドで設定します。 これは **ipv4 address dhcp** コマンドを使用します。

レイヤ 3 インターフェイスの前提条件

レイヤ 3 インターフェイスには次の前提条件があります。

- IP アドレッシングおよび基本設定を熟知している。IP アドレッシングの詳細については、「*Cisco Nexus® 3550-T* ユニキャスト ルーティングの構成」のセクションを参照してください。

レイヤ 3 インターフェイスの注意事項および制約事項

レイヤ 3 インターフェイスの構成には次の注意事項と制約事項があります：

- レイヤ 3 インターフェイスをレイヤ 2 インターフェイスに変更する場合、Cisco NX-OS はインターフェイスをシャットダウンしてインターフェイスを再度イネーブルにし、レイヤ 3 固有の構成をすべて削除します。
- レイヤ 2 インターフェイスをレイヤ 3 インターフェイスに変更する場合、Cisco NX-OS はインターフェイスをシャットダウンしてインターフェイスを再度イネーブルにし、レイヤ 2 固有の構成をすべて削除します。
- IP アンナンバード インターフェイスはサポートされていません。
- SVI のマルチキャストおよび/または、ブロードキャスト カウンターはサポートされていません。

- SVI とサブインターフェイスの両方のカウンタのコントロールプレーン SVI/SI トラフィックはサポートされません。
- **internal** 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。

（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。

デフォルト設定

次の表に、レイヤ 3 インターフェイス パラメータのデフォルト設定を示します。

表 *11 :* レイヤ *3* インターフェイスのデフォルト パラメータ

パラメータ	デフォルト
管理ステート	閉じる

レイヤ 3 インターフェイスの設定

ルーテッド インターフェイスの設定

任意のイーサネット ポートをルーテッド インターフェイスとして設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	**interface ethernet** *slot/port*
	例：
	`switch(config)# interface ethernet 1/2`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	**no switchport** **例：** `switch(config-if)# no switchport`	そのインターフェイスを、レイヤ3インターフェイスとして設定します。

	コマンドまたはアクション	目的
ステップ 4	[**ip address**] 例： `switch(config-if)# ip address 192.0.2.1/8`	• このインターフェイスの IP アドレスを設定します。IP アドレスの詳細については、「*Cisco Nexus® 3550-T* ユニキャスト ルーティングの構成」のセクションを参照してください。
ステップ 5	**show interfaces** 例： `switch(config-if)# show interfaces ethernet 1/2`	（任意）レイヤ 3 インターフェイスの統計情報を表示します。

ステップ 6	**no shutdown**
	例：
	`switch#`
	`switch(config-if)# int e1/2`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーに対応するインターフェイスのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）この設定の変更を保存します。

例

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

コマンド	目的
switchport 例： `switch(config-if)# switchport`**`switchport`**	インターフェイスをレイヤ 2 インターフェイスとして設定し、このインターフェイス上のレイヤ 3 固有の設定を削除します。

- 次に、ルーテッド インターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# copy running-config startup-config
```

インターフェイスのデフォルト設定がルーテッドされます。レイヤ 2 にインターフェイスを設定するには、**switchport** を入力します コマンドを使用します。レイ

ヤ 2 インターフェイスをルーテッド インターフェイスに変更する場合は、**no switchport** コマンドを入力します。

VLAN インターフェイスの設定

VLAN インターフェイスを作成して内部 VLAN ルーティングを行うことができます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**feature interface-vlan** 例： `switch(config)# feature interface-vlan`	VLANインターフェイスモードをイネーブルにします。

ステップ 3	**interface vlan** *number*
	例：
	`switch(config)# interface vlan 10`
	`switch(config-if)#`
		VLANインターフェイスを作成します。number の範囲は 1 ～ 4094 です。

ステップ 4	[**ip address** *ip-address/length*] 例： `switch(config-if)# ip address 192.0.2.1/8`	• この VLAN インターフェイスの IP アドレスを設定します。IP アドレスの詳細については、「*Cisco Nexus® 3550-T* ユニキャスト ルーティングの構成」のセクションを参照してください。
ステップ 5	**show interface vlan** *number* 例： `switch(config-if)# show interface vlan 10`	（任意）レイヤ3インターフェイスの統計情報を表示します。

ステップ 6	**no shutdown**
	例：
	`switch(config)# int e1/3`
	`switch(config)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーに対応するインターフェイスのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

例

次に、VLAN インターフェイスを作成する例を示します。

```
switch# configure terminal
switch(config)# feature interface-vlan
switch(config)# interface vlan 10
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# copy running-config startup-config
```

VRF メンバーシップ変更時のレイヤ 3 保持の有効化

次の手順により、インターフェイスの VRF メンバーシップを変更する際にレイヤ 3 設定を保持できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーションモードに入ります。

ステップ 2	**system vrf-member-change retain-l3-config**
	例：
	`switch(config)# system vrf-member-change retain-l3-config`
	`Warning: Will retain L3 configuration when vrf member change on interface.`
		VRF メンバーシップ変更時のレイヤ 3 保持を有効化します。
		（注）
		レイヤ3設定の保持を無効にするには、**no system vrf-member-change retain-l3-config** コマンドを使用します。

ループバック インターフェイスの設定

ループバック インターフェイスを設定して、常にアップ状態にある仮想インターフェイスを作成できます。

始める前に

ループバック インターフェイスの IP アドレスが、ネットワークの全ルータで一意であ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：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface loopback** *instance*
	例：
	`switch(config)# interface loopback 0`
	`switch(config-if)#`
		ループバック インターフェイスを作成します。範囲は 0 ー 1023 です。

ステップ 3	[**ip address** *ip-address/length*] 例： `switch(config-if)# ip address 192.0.2.1/8`	• このインターフェイスの IP アドレスを設定します。IP アドレスの詳細については、「*Cisco Nexus® 3550-T* ユニキャスト ルーティングの構成」のセクションを参照してください。
ステップ 4	**show interface loopback** *instance* 例： `switch(config-if)# show interface loopback 0`	（任意）ループバック インターフェイスの統計情報を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

例

次に、ループバック インターフェイスを作成する例を示します。

```
switch# configure terminal
switch(config)# interface loopback 0
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# copy running-config startup-config
```

VRF へのインターフェイスの割り当て

VRF にレイヤ 3 インターフェイスを追加できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** *interface-type number*
	例：
	`switch(config)# interface loopback 0`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	**vrf member** *vrf-name* 例： `switch(config-if)# vrf member RemoteOfficeVRF`	このインターフェイスを VRF に追加します。
ステップ 4	**ip address** *ip-prefix/length* 例： `switch(config-if)# ip address 192.0.2.1/16`	このインターフェイスの IP アドレスを設定します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。
ステップ 5	**show vrf** [*vrf-name*] **interface** *interface-type number* 例： `switch(config-vrf)# show vrf Enterprise interface loopback 0`	（任意）VRF 情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

例

次に、VRF にレイヤ 3 インターフェイスを追加する例を示します。

```
switch# configure terminal
switch(config)# interface loopback 0
switch(config-if)# vrf member RemoteOfficeVRF
switch(config-if)# ip address 209.0.2.1/16
switch(config-if)# copy running-config startup-config
```

インターフェイスでの DHCP クライアントの設定

管理インターフェイスで DHCP クライアントの IPv4 アドレスを構成できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル構成モードを開始します。
ステップ 2	switch(config)# **interface ethernet** *type slot/port* | **mgmt** *mgmt-interface-number* |	物理イーサネット インターフェイス、管理インターフェイスを作成します。
ステップ 3	switch(config-if)# [**no**] [**ip** | **ipv4] address dhcp**	DHCP サーバに IPv4 アドレスを要求します。 取得されたいずれかのアドレスを削除するには、このコマンドの **no** 形式を使用します。
ステップ 4	設定を保存します。	

レイヤ 3 インターフェイス設定の確認

レイヤ 3 の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show interface ethernet *slot/port*	レイヤ3インターフェイスの設定情報、ステータス、カウンタ（インバウンドおよびアウトバウンドパケット レートおよびバイト レートの、5 分間指数減少移動平均を含む）を表示します。
show interface ethernet *slot/port* **brief**	レイヤ 3 インターフェイスの動作ステータスを表示します。
show interface ethernet *slot/port* **capabilities**	レイヤ 3 インターフェイスの機能（ポート タイプ、速度、およびデュプレックスを含む）を表示します。
show interface ethernet *slot/port* **description**	レイヤ 3 インターフェイスの説明を表示します。
show interface ethernet *slot/port* **status**	レイヤ3インターフェイスの管理ステータス、ポート モード、速度、およびデュプレックスを表示します。

コマンド	目的
show interface ethernet *slot/port.number*	サブインターフェイスの設定情報、ステータス、カウンタ（インバウンドおよびアウトバウンドパケット レートおよびバイト レートが 5 分間に指数関数的に減少した平均値を含む）を表示します。
show interface port-channel *channel-id.number*	ポートチャネル サブインターフェイスの設定情報、ステータス、カウンタ（インバウンドおよびアウトバウンドパケット レートおよびバイト レートの、5 分間指数減少移動平均を含む）を表示します。
show interface loopback *number*	ループバック インターフェイスの設定情報、ステータス、カウンタを表示します。
show interface loopback *number* **brief**	ループバック インターフェイスの動作ステータスを表示します。
show interface loopback *number* **description**	ループバック インターフェイスの説明を表示します。
show interface loopback *number* **status**	ループバック インターフェイスの管理ステータスおよびプロトコル ステータスを表示します。
show interface vlan *number*	VLAN インターフェイスの設定情報、ステータス、カウンタを表示します。
show interface vlan *number* **brief**	VLAN インターフェイスの動作ステータスを表示します。
show interface vlan *number* **description**	VLANインターフェイスの説明を表示します。
show interface vlan *number* **status**	VLAN インターフェイスの管理ステータスおよびプロトコル ステータスを表示します。
show ip interface brief	インターフェイス アドレスとインターフェイス ステータス（ナンバード/アンナンバード）を表示します。
show ip route	OSPF または ISIS を介して取得されたルートを表示します（最適なユニキャストおよびマルチキャスト ネクストホップのアドレスが含まれる）。

レイヤ 3 インターフェイスのモニタリング

レイヤ 3 統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
show interface ethernet *slot/port* **counters**	レイヤ 3 インターフェイスの統計情報を表示します（ユニキャスト、マルチキャスト、ブロードキャスト）。
show interface ethernet *slot/port* **counters brief**	レイヤ 3 インターフェイスの入力および出力カウンタを表示します。
show interface ethernet errors *slot/port* **detailed** [**all**]	レイヤ 3 インターフェイスの統計情報を表示します。オプションとして、32 ビットと 64 ビットのパケットおよびバイト カウンタ（エラーを含む）をすべて含めることができます。
show interface ethernet errors *slot/port* **counters errors**	レイヤ 3 インターフェイスの入力および出力エラーを表示します。
show interface ethernet errors *slot/port* **counters snmp**	SNMP MIB から報告されたレイヤ 3 インターフェイス カウンタを表示します。
show interface loopback *number* **detailed** [**all**]	ループバック インターフェイスの統計情報を表示します。オプションとして、32 ビットと 64 ビットのパケットおよびバイト カウンタ（エラーを含む）をすべて含めることができます。
show interface vlan *number* **counters detailed** [**all**]	VLAN インターフェイスの統計情報を表示します。オプションとして、レイヤ 3 パケットおよびバイト カウンタをすべて含めることができます（ユニキャストおよびマルチキャスト）。
show interface vlan *number* **counters snmp**	SNMP MIB から報告された VLAN インターフェイス カウンタを表示します。

レイヤ 3 インターフェイスの設定例

次に、ループバック インターフェイスを設定する例を示します。

```
interface loopback 3
ip address 192.0.2.2/32
```

インターフェイスのVRFメンバーシップ変更の例

- VRFメンバーシップを変更する場合はレイヤ3設定の保持を有効にします。

```
switch# configure terminal
switch(config)# system vrf-member-change retain-l3-config

Warning: Will retain L3 configuration when vrf member change on interface.
```

- レイヤ3の保持を確認します。

```
switch# show running-config | include vrf-member-change

system vrf-member-change retain-l3-config
```

- レイヤ3設定によってSVIインターフェイスをVRFの「blue」として設定します。

```
switch# configure terminal
switch(config)# show running-config interface vlan 2002

interface Vlan2002
description TESTSVI
no shutdown
vrf member blue
no ip redirects
ip address 192.168.211.2/27
ip router ospf 1 area 0.0.0.0
preempt delay minimum 300 reload 600
priority 110 forwarding-threshold lower 1 upper 110
ip 192.168.211.1
preempt delay minimum 300 reload 600
priority 110 forwarding-threshold lower 1 upper 110
```

- VRFの変更後にSVIインターフェイスを確認します。

```
switch# configure terminal
switch(config)# show running-config interface vlan 2002

interface Vlan2002
description TESTSVI
no shutdown
vrf member red
no ip redirects
ip address 192.168.211.2/27
ip router ospf 1 area 0.0.0.0
preempt delay minimum 300 reload 600
priority 110 forwarding-threshold lower 1 upper 110
ip 192.168.211.1
preempt delay minimum 300 reload 600
priority 110 forwarding-threshold lower 1 upper 110
```

（注）

- VRF を変更する場合、レイヤ 3 設定の保持は次に影響します。
  - 物理インターフェイス
  - ループバック インターフェイス
  - SVI インターフェイス
  - ポート チャネル
- VRF を変更する場合、既存のレイヤ 3 設定が削除され、再適用されます。すべてのルーティング プロトコル（OSPF/ISIS/EIGRP）が古い VRF でダウンし、新しい VRF でアップします。
- ダイレクトおよびローカル IPv4 アドレスが古い VRF から削除され、新しい VRF にインストールされます。
- VRF 変更時にトラフィック損失が発生する可能性があります。

関連資料

関連資料	マニュアル タイトル
IP	「*Cisco Nexus® 3550-T* ユニキャスト ルーティング構成」セクション
VLANs	「*Cisco Nexus® 3550-T* レイヤ *2* スイッチング構成」セクション

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。