Cisco Nexus 7000 シリーズ NX-OS インターフェイス コンフィギュレーション ガイド

最終更新：2016 年 01 月 28 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

ここでは、次の項について説明します。

対象読者

このマニュアルは、Cisco Nexus デバイスのコンフィギュレーションおよびメンテナンスを担当するネットワーク管理者を対象としています。

表記法

（注） お客様のニーズを満たすためにドキュメントを更新するという継続的な取り組みの一環として、シスコでは設定タスクの文書化方法を変更しました。そのため、本ドキュメントには、従来とは異なるスタイルでの設定タスクが説明されている部分もあります。ドキュメントに新たに組み込まれるようになったセクションには、以下のセクションが含まれます。

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。

表記法	説明
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角カッコ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、角カッコで囲み、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、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコ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。角カッコ内の波カッコと縦棒は、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ません。引用符を使用すると、その引用符も含めて string とみなされます。

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、screen 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。

このマニュアルでは、次の表記法を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

Cisco Nexus 7000 シリーズ NX-OS ソフトウェアの関連資料

Cisco Nexus 7000 シリーズ NX-OS 全体のマニュアル セットは、次の URL にあります。
http://www.cisco.com/en/us/products/ps9402/tsd_products_support_series_home.html

リリース ノート

リリース ノートは、次の URL から入手できます。
http://www.cisco.com/en/US/products/ps9402/prod_release_notes_list.html

コンフィギュレーション ガイド

これらのマニュアルは、次の URL から入手できます。
http://www.cisco.com/en/US/products/ps9402/products_installation_and_configuration_guides_list.html
このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 7000 Series NX-OS Configuration Examples*』
- 『*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS IP SLAs Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS LISP Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS OTV Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide*』

- 『*Cisco Nexus 7000 Series NX-OS SAN Switching Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Quick Start*』
- 『*Cisco Nexus 7000 Series NX-OS OTV Quick Start Guide*』
- 『*Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*』
- 『*Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide*』

コマンド リファレンス

これらのマニュアルは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps9402/prod_command_reference_list.html

このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 7000 Series NX-OS Command Reference Master Index*』
- 『*Cisco Nexus 7000 Series NX-OS FabricPath Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS High Availability Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS LISP Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS OTV Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS SAN Switching Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference*』

- 『*Cisco NX-OS FCoE Command Reference for Cisco Nexus 7000 and Cisco MDS 9500*』

その他のソフトウェアのマニュアル

これらのマニュアルは、以下のランディング ページから検索できます。

http://www.cisco.com/en/us/products/ps9402/tsd_products_support_series_home.html

- 『*Cisco Nexus 7000 Series NX-OS MIB Quick Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Troubleshooting Guide*』
- 『*Cisco NX-OS Licensing Guide*』
- 『*Cisco NX-OS System Messages Reference*』
- 『*Cisco NX-OS XML Interface User Guide*』

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、または誤りや記載漏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。ciscodfa-docfeedback@cisco.com。

ご協力をよろしくお願いいたします。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『What's New in Cisco Product Documentation』を参照してください。

新しく作成された、または改訂されたシスコのテクニカル コンテンツをお手元に直接送信するには、『What's New in Cisco Product Documentation』RSS フィードをご購読ください。RSS フィードは無料のサービスです。

第 1 章

新機能および変更された機能に関する情報

新機能および変更された機能に関する情報

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *1*：新規および変更されたインターフェイス機能

機能	説明	変更されたリリース
リンク単位 BFD	ユーザがすべてのリンク アグリゲーション グループ メンバー インターフェイス（RFC 7130 で規定されている）上で個別の BFD セッションを設定できるようにするリンク単位双方向転送機能のサポートが追加されました。	7.3(0)D1(1)
vPC 用のヒットレス STP ロールの変更	vPC 用のヒットレス STP ロールの変更に対するサポートが追加されました。	7.3(0)D1(1)
非同期リンク デバウンス	デバウンス アップ リンクとデバウンス ダウン リンクに別々の値を設定するためのサポートが追加されました。	7.3(0)D1(1)

新機能および変更された機能に関する情報

機能	説明	変更されたリリース
HSPRv6 に対する BFD サポート	HSPRv6 に対する BFD サポートが追加されました。	7.3(0)D1(1)
ポート チャネル（ランダム ロード バランシング）	ポート チャネル上でのランダム ロード バランシングに対するサポートが追加されました。	7.3(0)D1(1)
イーサネット OAM	イーサネット OAM 機能を使用すると、サービスプロバイダーは MAN や WAN での接続の品質をモニタできます。サービスプロバイダーは、特定のイベントをモニタし、イベントに対しアクションを実行すること、および必要に応じて、トラブルシューティングのために特定のインターフェイスをループバック モードにすることができます。イーサネット OAM は単一の物理リンクで動作し、そのリンクの片側または両側をモニタするように設定できます。	7.3(0)D1(1)
vPC シャットダウン	ピアをシャットダウンして、デバッグ、リロード、または vPC コンプレックスからの物理的な削除のために分離し、ピア vPC スイッチがプライマリ ピアとして引き継ぐようにする **shutdown** コマンドが追加されました。	7.2(0)D1(1)
F3 上の物理ポート vPC	F3 上の物理ポート vPC に対するサポートが追加されました。	7.2(0)D1(1)
FEX 用の 1500 ホスト vPC（FEX 上の物理ポート vPC）	この機能のサポートが追加されました。	7.2(0)D1(1)
vPC 設定の同期化	vPC 設定の同期機能に対するサポートが追加されました。	7.2(0)D1(1)
F2、F2E、および F3 モジュール用の vPC 経由のレイヤ 3	この機能のサポートが追加されました。	7.2(0)D1(1)

機能	説明	変更されたリリース
FabricPath コア上のレイヤ 2 経由の BFD に対するサポート	FabricPath コア上のレイヤ 2 経由の BFD に対するサポートが追加されました。	7.2(0)D1(1)
Fabricbath コア上の SVI 経由の BFD に対するサポート	Fabricbath コア上の SVI 経由の BFD に対するサポートが追加されました。	7.2(0)D1(1)
GRE トンネル	F3 シリーズ モジュールのサポートが追加されました。	6.2(10)
トランク ポートでのネイティブ VLAN タギング	**switchport trunk native vlan tag** コマンドのサポートが追加され、**vlan dot1q tag native** コマンドに **exclude control** キーワードが追加されました。	6.2(10)
LAN シャットダウン	この機能をサポートするための **shutdown lan** コマンドが追加されました。	6.2(6)
物理ポート vPC を介した FCoE	この機能のサポートが追加されました。	6.2(6)
物理ポート vPC	vPC ピア デバイスの物理インターフェイス上の物理ポート vPC に対するサポートが追加されました。	6.2(6)
IPv6 スタティックの BFD	インターフェイス上の IPv6 スタティック ルートで BFD を設定するためのサポートが追加されました。	6.2(2a)

新機能および変更された機能に関する情報

機能	説明	変更されたリリース
FEX	Cisco ファブリック エクステンダは、キュー マッピングへのホスト インターフェイス（HIF）および DSCP 上のレイヤ 3 プロトコル隣接関係をサポートします。Cisco リリース 6.2(2) より前は、ファブリック エクステンダ（FEX）ポートをホスト接続のためのレイヤ3インターフェイスとして設定できますが、ルーティング用には設定できません。	6.2(2)
エラー ディセーブル化	エラー ディセーブル化リカバリおよび検出ランタイム情報を表示する機能が追加されました。	6.2(2)
インターフェイス ステータス エラー ポリシーの表示	ポリシー プログラミング中にエラーを受信する、インターフェイスおよび VLAN に関する情報を表示できます。	6.2(2)
インターフェイスから SNMP カウンタをクリア	インターフェイスから SNMP カウンタをクリアする機能が追加されました。	6.2(2)
SVI 自動ステートのディセーブル化	対応する VLAN にアップしているインターフェイスがない場合でも、SVI がアップしたままを許可することで SVI 自動ステート動作をディセーブルにできます。	6.2(2)
IPv6 での BFD	IPv6 での BFD のサポートが追加されました。	6.2(2)
OSPFv3 での BFD	OPSPv3 での BFD のサポートが追加されました。	6.2(2)
IS-ISv6 での BFD	IS-ISv6 での BFD のサポートが追加されました。	6.2(2)

機能	説明	変更されたリリース
非対称	F2またはF2eモジュールのハッシュ機構を非対称に変更できます（デフォルトでは対称です）。それにより、双方向転送時に発生するトラフィック ドロップを防止し、ロード バランシングを改善することができます。	6.2(2)
モード自動コマンド	特定のコマンドを同時にイネーブルにできます。	6.2(2)
マルチキャスト ロード バランス	両方の vPC パスがアップしているときに2つのピアが部分的に指定フォワーダになることを許可します。	6.1(3)
Result Bundle Hash ロード バランシング	ポート チャネル全体のロード バランシングを改善するための RBH モジュロ モードのサポートが追加されました。	6.1(3)
FEX ファブリック ポート チャネル用最少リンク数	FEX ファブリック ポート チャネルのリンクの最小数を設定する機能が追加されました。	6.1(3)
低速ドレイン デバイスの検出と輻輳回避	低速ドレイン デバイスの検出機能のサポートが追加されました。	6.1(1)
F2 シリーズおよび M2 シリーズ モジュールの BFD サポート	F2 シリーズおよび M2 シリーズ モジュールのサポートが追加されました。	6.1(1)
リリース 5.2(1) 以降変更なし。	-	-
ファブリック エクステンダ（FEX）	ファブリック エクステンダのポートには、ホスト接続に関するレイヤ 3 サポートがあり、vPC はファブリック エクステンダ（ホスト vPC）から設定できます。	5.2(1)

新機能および変更された機能に関する情報

機能	説明	変更されたリリース
BFD SHA1 認証	BFD パケットの SHA-1 認証をサポートします。	5.2(1)
デフォルト インターフェイス	複数のインターフェイス タイプの既存の設定をクリアできます。	5.2(1)
SVI 自動ステート除外	VLANに複数のポートがあるときに、VLANインターフェイスのリンクアップ計算からポートを除外できます。	5.2(1)
vPC	自動リカバリ サポートを設定し、VLAN 一貫性障害、FabricPath 設定サポートおよびCisco 2000 シリーズ ファブリック エクステンダへの vPC 接続へ MST のシステム表示を提供します。	5.2(1)
レート制限	スーパーバイザに到達するパケットのレート制限を設定します。	5.1(1)
Nexus シャーシのインバンド管理	シャーシ内に F1 シリーズ モジュールのみがある場合に、Cisco Nexus 7000 スイッチのインバンド管理を設定します。	5.1(1)
ポート チャネルの F1 シリーズ モジュールおよびM1 シリーズ モジュール	F シリーズモジュールのポート チャネルへの 16 個のアクティブ ポートの同時バンドリングをサポートします。M シリーズ モジュールでは、最大 8 個のアクティブ ポートと 8 個のスタンバイ ポートをバンドルすることができます。	5.1(1)
LACP ポートチャネルの最小リンクおよび MaxBundle	LACP ポートチャネルの最小リンクおよびLACP ポートチャネル maxbundle を設定します。	5.1(1)

機能	説明	変更されたリリース
BFD	ネットワークのプロファイリングおよびプランニングを簡単にし、再コンバージェンス時間の一貫性を保ち、予測可能にします。	5.0(2)
Q-in-Q トンネリング	使用できる VLAN がすべて提供されながらも異なるカスタマーのトラフィックを分離することができます。	5.0(2)
vPC および STP コンバージェンス	ピアが機能を停止したときのスイッチでの vPC 起動をサポート。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。	5.0(2)

新機能および変更された機能に関する情報

第 2 章

概要

この章では、Cisco NX-OS ソフトウェアでサポートするインターフェイス タイプの概要を説明します。

インターフェイスに関する情報

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。

以下の表に、インターフェイスに設定できるパラメータの情報の入手先を示します。

表 *2*：インターフェイス パラメータ

機能	パラメータ	解説場所
基本パラメータ	説明、デュプレクス、エラーディセーブル、フロー制御、MTU、ビーコン	「基本インターフェイス パラメータの設定」

機能	パラメータ	解説場所
レイヤ 2	レイヤ2アクセスおよびトランク ポート設定	「レイヤ2インターフェイスの設定」
	レイヤ2MAC、VLAN、プライベート VLAN、Rapid PVST+、Multiple Spanning Tree、スパニングツリー拡張	『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』
	ポート セキュリティ	『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x*』
レイヤ 3	メディア、IPv4 および IPv6 アドレス	「レイヤ3インターフェイスの設定」
	帯域幅、遅延、IP ルーティング、VRF	*Cisco Nexus 7000* シリーズ *NX-OS* インターフェイス コンフィギュレーション ガイド リリース *6.x* 『*Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide*』
ポート チャネル	チャネル グループ、LACP	「ポート チャネルの設定」
vPC	仮想ポート チャネル	「vPC の設定」
トンネル	GRE トンネリング	「IP トンネルの設定」
セキュリティ	Dot1X、NAC、EOU、ポート セキュリティ	『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x*』
FCoE	Cisco NX-OS Release 5.2(1) から、Cisco Nexus 7000 シリーズ スイッチ上で FCoE（Fibre Channel over Ethernet）を実行できるようになりました。	『*Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*』

Ethernet Interfaces

イーサネット インターフェイスには、アクセス ポート、トランク ポート、プライベート VLAN（PVLAN）ホスト ポートと無差別ポート、ルーテッド ポートがあります。

Access Ports

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 インターフェイスの詳細については、「レイヤ 2 インターフェイスの設定」を参照してください。

Trunk Ports

トランク ポートは複数の 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。トランク ポート インターフェイスの詳細については、「レイヤ 2 インターフェイスの設定」を参照してください。

PVLAN ホストと無差別ポート

プライベート VLAN（PVLAN）は、レイヤ 2 レベルでのトラフィック分離とセキュリティを実現します。PVLAN は 1 つのプライマリ VLAN と 1 つのセカンダリ VLAN を 1 つまたは複数組み合わせたもので、プライマリ VLAN はすべて同じです。セカンダリ VLAN には 2 種類あり、独立 VLAN とコミュニティ VLAN と呼ばれます。

独立 VLAN では、PVLAN ホストはプライマリ VLAN のホストとだけ通信します。コミュニティ VLAN では、PVLAN ホストは同じコミュニティ内の PVLAN ホスト同士およびプライマリ VLAN のホストとだけ通信し、独立 VLAN や他のコミュニティの VLAN のホストとは通信しません。コミュニティ VLAN は無差別ポートを使って PVLAN の外部と通信します。独立およびコミュニティ セカンダリ VLAN が組み合わされているにもかかわらず、プライマリ VLAN 内のすべてのインターフェイスはレイヤ 2 ドメイン 1 つだけで構成されており、必要な IP サブネットは 1 つです。

PVLAN 無差別ポートにレイヤ 3 VLAN ネットワーク インターフェイスやスイッチ仮想インターフェイス（SVI）を設定し、プライマリ PVLAN にルーティング機能を持たせることもできます。

PVLAN ホストおよび PVLAN 無差別ポートの設定および他のすべての PVLAN 設定の詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

Routed Ports

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、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。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」の項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、10/100/1000 Mb/s の速度の全二重モードで動作します。

管理インターフェイスの詳細については、『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*』を参照してください。このマニュアルにも、管理インターフェイスの IP アドレスとデフォルト IP ルーティング設定に関する情報を記載しています。

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 つ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 チャネルの設定」を参照してください。

vPC

仮想ポート チャネル（vPC）によって、2 個の異なる Cisco Nexus 7000 シリーズ デバイスを物理的に接続し、第 3 のデバイスからは 1 つのポートとして見えるリンクが実現します。第 3 のデバイスには、スイッチやサーバなどあらゆるネットワーキング デバイスが該当します。すべてのデバイス上で全部で 748 本の vPC を設定できます。vPC はレイヤ 2 マルチパッシングを提供します。vPC の詳細については、「vPC の設定」の項を参照してください。

サブインターフェイス

レイヤ 3 インターフェイスとして設定した親インターフェイスに仮想サブインターフェイスを作成できます。親インターフェイスは物理ポートでもポート チャネルでもかまいません。親インターフェイスはサブインターフェイスによって複数の仮想インターフェイスに分割されます。これらの仮想インターフェイスに IP アドレスやダイナミック ルーティング プロトコルなど固有のレイヤ3パラメータを割り当てることができます。サブインターフェイスの詳細については、「サブインターフェイス」の項を参照してください。

VLAN ネットワーク インターフェイス

VLAN ネットワーク インターフェイスは仮想のルーテッドインターフェイスで、デバイスの VLAN を同じデバイスのレイヤ 3 ルータ エンジンに接続します。レイヤ 3 内部 VLAN ルーティングが実現できるように VLAN ネットワーク インターフェイス間をルーティングできます。VLAN ネット

ワーク インターフェイスの詳細については、「VLAN インターフェイス」の項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。サブインターフェイスの詳細については、「ループバック インターフェイス」の項を参照してください。

トンネル インターフェイス

トランスポート プロトコル内部の任意のパケットは、トンネリングによってカプセル化されます。この機能は、簡単なインターフェイスを設定する仮想インターフェイスとして実装されています。トンネル インターフェイスにより、任意の標準的なポイントツーポイント（p2p）カプセル化スキームの実装に必要なサービスが提供されます。リンクごとに個別のトンネルを設定できます。詳細については、「IP トンネルの設定」を参照してください。

仮想化インターフェイス

複数の仮想デバイス コンテキスト（VDC）を作成できます。各 VDC は、インターフェイスを割り当てることのできる、独立した論理デバイスです。VDC にインターフェイスを割り当てると、現在の VDC が正しい場合のみこのインターフェイスを設定できます。VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

インターフェイスのハイ アベイラビリティ

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。ステートフル再起動はスーパーバイザ切り替え時に発生します。切り替え後、Cisco NX-OS は実行時の設定を適用します。

インターフェイスのライセンス要件

vPC には、ライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

IP トンネルには Enterprise Services ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『Cisco NX-OS Licensing Guide』を参照してください。

他のインターフェイスにはライセンスが必要ありません。

第 3 章

基本インターフェイス パラメータの設定

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

基本インターフェイス パラメータについて

レイヤ2インターフェイス（アクセス インターフェイスやトランキング インターフェイス）専用に使用されるパラメータを設定するには、「レイヤ 2 インターフェイスの設定」を参照してください。レイヤ3インターフェイス（ルーテッドインターフェイス、サブインターフェイス、VLANインターフェイス、ループバック インターフェイス、およびIPトンネル）専用に使用されるパラメータを設定するには、「レイヤ 3 インターフェイスの設定」を参照してください。

基本インターフェイス パラメータ設定の機能履歴

この表には、機能の追加や変更によるリリースの更新内容のみが記載されています。

表 *3*：基本インターフェイス パラメータ設定の機能履歴

機能名	リリース	機能情報
デバウンス リンク アップ時間	7.3(0)D1(1)	デバウンス リンクアップ時間に対するサポートが追加されました。**link debounce** {**link-up** | **time**} *milliseconds* コマンドが更新されました。
エラー ディセーブル化	6.2(2)	**show errdisable** {**detect** | **recovery**} コマンドが追加されました。
ポリシー プログラミング中のエラーを表示。	6.2(2)	ポリシープログラミング中にエラーを生成するインターフェイスおよびVLANを表示する **show interface status error policy** コマンドが追加されました。
インターフェイスから SNMP カウンタをクリア	6.2(2)	インターフェイスからSNMP値をクリアするためのオプションを提供する **snmp** キーワードを含めるための **clear counters interface** コマンドが更新されました。
インターフェイスの説明	6.2(2)	254 文字の大文字と小文字が区別される英数字の最大文字数を増やすための **description** コマンドが更新されました。
インターフェースの出力の表示拡張	6.1(1)	**show interface eth** コマンド出力が更新されました。
ポート プロファイル	4.2(1)	いくつかの設定を一定範囲のインターフェイスに同時に適用できます。

機能名	リリース	機能情報
基本インターフェイスの設定	4.0(1)	これらの機能が導入されました。

説明

イーサネット インターフェイスおよび管理インターフェイスに説明パラメータを設定して、インターフェイスにわかりやすい名前を付けることができます。それぞれのインターフェイスに独自の名前を使用すれば、複数のインターフェイスから探す場合でも必要なインターフェイスをすぐに見つけることができます。

ポートチャネルインターフェイスへの説明パラメータの設定については、「ポートチャネルの説明の設定」の項を参照してください。その他のインターフェイスへのこのパラメータの設定については、「説明の設定」の項を参照してください。

ビーコン

ビーコン モードをイネーブルにするとリンク ステート LED が緑に点滅し、物理ポートを識別できます。デフォルトでは、このモードはディセーブルです。インターフェイスの物理ポートを識別するには、インターフェイスのビーコン パラメータを有効にします。

ビーコン パラメータの設定については、「ビーコン モードの設定」の項を参照してください。

MDIX

メディア依存インターフェイスクロスオーバー（MDI-X）パラメータを使用して、デバイス間のクロスオーバー接続のイネーブル/ディセーブルを切り替えます。このパラメータは銅線インターフェイスだけに適用します。デフォルトでは、このパラメータはイネーブルです。

MDIX パラメータの設定については、「MDIX パラメータの設定」の項を参照してください。

デバウンス タイマー

デバウンス タイマーを設定するとリンク変更の通知が遅くなり、ネットワークの再設定によるトラフィック損失が減少します。デバウンスタイマーはイーサネットポートごとに個別に設定します。遅延時間はミリ秒単位で指定できます。デバウンスタイマーのリンクダウンのデフォルト値は 100 ミリ秒で、デバウンス タイマーのリンク アップのデフォルト値は 0 ミリ秒です。

Cisco NX-OS リリース 7.3(0)D1(1) 以降では、デバウンス タイマーのリンク ダウンとリンク アップで別々のデバウンス タイマー値を設定できます。リンク アップ用のデバウンス タイマーを使用すれば、システム リロード後のコンバージェンスを改善し、トラフィックのブラックホール化を回避できます。

注意 デバウンス タイマーをイネーブルにするとリンクダウン検出が遅くなり、デバウンス期間中のトラフィックが失われます。この状況は、一部のレイヤ 2 とレイヤ 3 プロトコルのコンバージェンスと再コンバージェンスに影響する可能性があります。

デバウンス タイマー パラメータの設定については、「デバウンス タイマーの設定」の項を参照してください。

エラー ディセーブル化

ポートが管理上（**no shutdown** コマンドを使用しない）イネーブルであるが、プロセスによって実行時にディセーブルになる場合、そのポートは error-disabled（err-disabled）ステートです。たとえば、UDLD が単方向リンクを検出した場合、ポートは実行時にシャットダウンされます。ただし、ポートは管理上イネーブルなので、ポート ステータスは err-disable として表示されます。ポートが err-disable ステートになると、手動で再イネーブル化する必要があります。または、自動回復を提供するタイムアウト値を設定できます。自動回復はデフォルトでは設定されておらず、デフォルトでは、err-disable の検出はすべての原因に対してイネーブルです。

インターフェイスが errdisable ステートになった場合は、**errdisable detect cause** コマンドを使用して、そのエラーに関する情報を取得してください。

特定の error-disabled の原因に自動 error-disabled 回復タイムアウトを設定し、回復期間を設定できます。**errdisable recovery cause** コマンドを使用すると、300 秒後に自動的にリカバリします。

errdisable recovery cause コマンドを使用すると、300 秒後に自動的にリカバリします。

30 ～ 65535 秒の範囲内でリカバリ期間を変更するには、**errdisable recovery interval** コマンドを使用します。特定の err-disable 原因のリカバリ タイムアウトも設定できます。

原因に対する error-disabled 回復をイネーブルにしない場合、そのインターフェイスは **shutdown** コマンドおよび **no shutdow**n コマンドが入力されるまで error-disabled ステートのままです。原因に対して回復をイネーブルにすると、そのインターフェイスの errdisable ステートは解消され、すべての原因がタイムアウトになった段階で動作を再試行できるようになります。エラーの原因を表示する場合は、**show interface status err-disabled** コマンドを使用します。

Cisco NX-OS リリース 6.2(2) 以降では、**show errdisable recovery** コマンドおよび **show errdisable detect** コマンドを使用して、errdisable リカバリおよび検出ランタイム情報を表示できます。

インターフェイス ステータス エラー ポリシー

アクセス コントロール リスト（ACL）マネージャおよび Quality of Service（QoS）マネージャなどの Cisco NX-OS ポリシー サーバは、ポリシー データベースを維持します。アクセスからトランクへのレイヤ 2 ポート モードの変更などのポリシー（入力、出力、または双方向のいずれか）は、コマンドライン インターフェイスを通じて定義されます。

ポリシーは、インターフェイス上のポリシーを設定するときにプッシュされます。インターフェイス VLAN のメンバーシップが変更したときや、ラインカードが起動すると、設定済みのすべてのポリシーが同時にプッシュされます。プッシュされるポリシーがハードウェア ポリシーと一致

するか、またそれらがポリシー プログラミング中にエラーが発生しているインターフェイスおよび VLAN を表示することを確認するには、**show interface status error policy** コマンドを入力します。

エラーをクリアし、ポリシー プログラミングが実行コンフィギュレーションを続行できるようにするには、**no shutdown** コマンドを入力します。ポリシー プログラミングが成功すると、ポートのアップが許可されます。ポリシー プログラミングが失敗した場合、設定はハードウェア ポリシーに矛盾し、ポートは error-disabled ポリシー状態になります。error-disabled ポリシー状態にとどまり、同じポートが今後アップされないように情報が保存されます。このプロセスにより、システムに不要な中断が生じるのを避けることができます。

Rate Mode

32 ポートの 10 ギガビット イーサネット モジュールでは、4 ポート単位で 10 Gb/s の帯域幅を処理します。レートモード パラメータを使用すれば、この帯域幅を 4 ポートのうちの最初のポート専用にさせることも、4 ポート全体でこの帯域幅を共有させることもできます。

以下の表に、10 Gb/s ごとの帯域幅を共有するポートのグループと、帯域幅全体を利用するために使用するグループの専用ポートを示します。

表 *4*：共有ポートと専用ポート

帯域幅を共有するポート グループ	10ギガビット イーサネットの帯域幅を専用するポート
1、3、5、7	1
2、4、6、8	2
9、11、13、15	9
10、12、14、16	10
17、19、21、23	17
18、20、22、24	18
25、27、29、31	25
26、28、30、32	26

（注） 各ポート グループのポートはすべて同じ Virtual Device Context（VDC）に属している必要があります。VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

速度モードとデュプレックス モード

速度モードとデュプレックスモードはそれぞれ、イーサネットインターフェイスおよび管理インターフェイスと相関関係にあります。デフォルトでは、これらのインターフェイスの速度およびデュプレックス モードは他のインターフェイスとそれぞれ自動ネゴシエートしますが、設定を変更することもできます。設定を変更する場合は、両方のインターフェイスで同じ速度とデュプレックス モード設定を使用するか、または少なくとも 1 つのインターフェイスで自動ネゴシエーションを使用します。

ポート チャネル インターフェイスへの速度モードとデュプレックス モードの設定については、「ポート チャネル インターフェイスへの速度とデュプレックスの設定」の項を参照してください。その他のインターフェイスへの速度とデュプレックス速度の設定については、「インターフェイス速度およびデュプレックス モードの設定」の項を参照してください。

Flow Control

1 Gb/s 以上で稼働するイーサネット ポートの受信バッファが満杯になると、フロー制御により、そのポートから送信ポートに IEEE 802.3x ポーズ フレームが送信され、指定した時間だけデータの送信を停止するよう要求されます。送信ポートは任意の速度で動作しており、ポーズ フレームを受信してデータの転送を停止することができます。

2 つのポート間のフロー制御を有効にするには、それぞれのポートで対応する受信および送信フロー制御パラメータをイネーブルまたはディセーブルに設定します。パラメータをイネーブルに設定すると、もう一方のポートの設定とは関係なく送信または受信フロー制御機能がアクティブになります。指定したパラメータを設定すると、もう一方のポートの対応するフロー制御状態をイネーブルまたはディセーブルに設定すれば、送信または受信フロー制御機能がアクティブになります。いずれかのフロー制御状態をディセーブルに設定すると、その送信方向のフロー制御がディセーブルになります。異なるポートフロー制御状態がリンク フロー制御状態に与える影響については、以下の表を参照してください。

表 *5*：リンク フロー制御上でのポート フロー制御の影響

ポート フロー制御の状態		リンク フロー制御の状態
データ受信ポート（ポーズ フレームを送信）	データ送信ポート（ポーズ フレームを受信）	
イネーブル	イネーブル	イネーブル

ポート フロー制御の状態		リンク フロー制御の状態
データ受信ポート（ポーズ フレームを送信）	データ送信ポート（ポーズ フレームを受信）	
イネーブル	必要	イネーブル
イネーブル	ディセーブル	ディセーブル
必要	イネーブル	イネーブル
必要	必要	イネーブル
必要	ディセーブル	ディセーブル
ディセーブル	イネーブル	ディセーブル
ディセーブル	必要	ディセーブル
ディセーブル	ディセーブル	ディセーブル

フロー制御パラメータの設定については、「フロー制御の設定」の項を参照してください。

ポート MTU サイズ

最大伝送単位（MTU）サイズは、イーサネット ポートで処理できる最大フレーム サイズを指定します。2 つのポート間で転送するには、どちらのポートにも同じ MTU サイズを設定する必要があります。ポートの MTU サイズを超えたフレームはドロップされます。

デフォルトではそれぞれのポートの MTU は 1500 バイトです。これはイーサネット フレームに関する IEEE 802.3 標準です。これよりも大きい MTU サイズでは、より少ないオーバーヘッドでデータをより効率的に処理できます。このようなフレームをジャンボ フレームと呼び、最大 9216 バイトまで指定できます。これもデフォルトのシステム ジャンボ MTU サイズです。

レイヤ 3 インターフェイスでは、576 ～ 9216 バイトの MTU サイズを設定できます。I/O モジュールごとに最大 64 MTU まで設定できます。

（注） グローバル LAN ポート MTU サイズは、非デフォルト MTU サイズを設定したレイヤ 3 イーサネット LAN ポートを通過するトラフィックに適用します。

レイヤ 2 ポートには、システム デフォルト（1500 バイト）またはシステム ジャンボ MTU サイズ（当初は 9216 バイト）のいずれかの MTU サイズを設定できます。

（注） システム ジャンボMTUサイズを変更すると、ポートの一部または全部に新しいシステム ジャンボ MTU サイズを指定しない限り、レイヤ 2 ポートは自動的にシステム デフォルト MTU サイズ（1500 バイト）を使用します。

MTU サイズの設定については、「MTU サイズの設定」の項を参照してください。

帯域幅

イーサネット ポートには、物理レベルで 1,000,000 Kb の固定帯域幅があります。レイヤ 3 プロトコルでは、内部メトリックが計算できるように設定した帯域幅の値が使用されます。設定した値はレイヤ 3 プロトコルで情報目的だけで使用され、物理レベルでの固定帯域幅が変更されることはありません。たとえば、Interior Gateway Routing Protocol（IGRP）ではルーティング メトリックを指定するために最小パス帯域幅が使用されますが、物理レベルの帯域幅は 1,000,000 Kb のまま変わりません。

ポートチャネル インターフェイスへの帯域幅パラメータの設定については、「情報目的としての帯域幅および遅延の設定」の項を参照してください。その他のインターフェイスへの帯域幅パラメータの設定については、「帯域幅の設定」の項を参照してください。

スループット遅延

スループット遅延パラメータの値を指定するとレイヤ 3 プロトコルで使用する値が指定できますが、インターフェイスの実際のスループット遅延は変更されません。レイヤ 3 プロトコルはこの値を使用して動作を決定します。たとえば、リンク速度などの他のパラメータが等しい場合、Enhanced Interior Gateway Routing Protocol（EIGRP）は遅延設定を使用して、他のイーサネット リンクより優先されるイーサネット リンクのプリファレンスを設定できます。設定する遅延値の単位は 10 マイクロ秒です。

ポートチャネル インターフェイスへの帯域幅パラメータの設定については、「情報目的としての帯域幅および遅延の設定」の項を参照してください。その他のインターフェイスへのスループット遅延パラメータの設定については、「スループット遅延の設定」の項を参照してください。

Administrative Status

管理ステータス パラメータはインターフェイスのアップまたはダウンを指定します。管理的にダウンしたインターフェイスはディセーブルであり、データを転送できません。管理的にアップしたインターフェイスはイネーブルであり、データを転送できます。

ポートチャネル インターフェイスへの管理ステータス パラメータの設定については、「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」の項を参照してください。その他のインターフェイスへの管理ステータス パラメータの設定については、「インターフェイスのシャットダウンおよび再開」の項を参照してください。

UDLD パラメータ

UDLD の概要

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。単方向リンクは、スパニングツリートポロジループをはじめ、さまざまな問題を引き起こす可能性があります。

UDLD は、レイヤ 1 プロトコルと協調してリンクの物理ステータスを検出するレイヤ 2 プロトコルです。レイヤ 1 では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。UDLD は、ネイバーの ID の検知、誤って接続された LAN ポートのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 とレイヤ 2 の検出が協調して動作して、物理的な単一方向接続と論理的な単一方向接続を防止し、その他のプロトコルの異常動作を防止できます。

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。対になったファイバ ケーブルのうち一方の接続が切断された場合、自動ネゴシエーションがアクティブである限り、そのリンクはアップ状態が維持されなくなります。この場合、論理リンクは不定であり、UDLD は何の処理も行いません。レイヤ 1 で両方の光ファイバが正常に動作している場合は、レイヤ 2 で UDLD が、これらの光ファイルが正しく接続されているかどうか、および正しいネイバー間でトラフィックが双方向に流れているかを調べます。自動ネゴシエーションはレイヤ 1 で動作するため、このチェックは、自動ネゴシエーションでは実行できません。

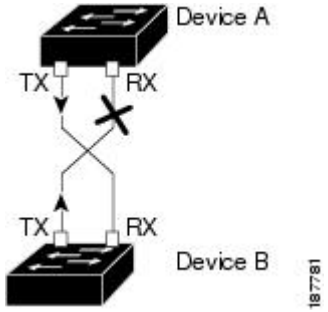
Cisco Nexus 7000 シリーズのデバイスは、UDLD をイネーブルにした LAN ポート上のネイバー デバイスに定期的にUDLDフレームを送信します。一定の時間内にフレームがエコーバックされてきて、特定の確認応答（echo）が見つからなければ、そのリンクは単一方向のフラグが立てられ、そのLANポートはシャットダウンされます。UDLDプロトコルにより単方向リンクが正しく識別されその使用が禁止されるようにするためには、リンクの両端のデバイスでUDLDがサポートされている必要があります。UDLDフレームの送信間隔は、グローバル単位でも指定されたインターフェイスにも設定できます。

（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。

以下の図は、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 *1*：単方向リンク



UDLD のデフォルト設定

表 *6*：*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）	すべてのイーサネット 10/100 および 1000BASE-TX LAN ポートでディセーブル
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

デバイスおよびそのポートへの UDLD の設定については、「UDLD モードの設定」の項を参照してください。

UDLD アグレッシブ モードと非アグレッシブ モード

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。

スパニングツリー ループを防止するため、間隔がデフォルトの 15 秒である非アグレッシブな UDLD でも、（デフォルトのスパニングツリー パラメータを使用して）ブロッキング ポートがフォワーディング ステートに移行する前に、単方向リンクをシャットダウンすることができます。

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。

ヒント ラインカードのアップグレードが In-Service Software Upgrade（ISSU）中に実行され、ラインカードのポートの一部がレイヤ 2 ポート チャネルのメンバーで UDLD アグレッシブ モードで設定されている場合、リモート ポートの 1 つがシャット ダウンされると、UDLD はローカル デバイス上の対応するポートを errdisable ステートにします。これは、正常な動作です。

ISSU の完了後にサービスを復元するには、ローカル ポートで **shutdown** コマンドと **no shutdown** コマンドを順に入力します。

Carrier Delay

（注） キャリア遅延タイマーは、VLAN ネットワーク インターフェイスでのみ設定できます。タイマーは、物理イーサネット インターフェイス、ポート チャネル、およびループバック インターフェイスでは設定できません。VLAN ネットワーク インターフェイスの設定については、「レイヤ 3 インターフェイスの設定」を参照してください。

リンクがダウンし、キャリア遅延タイマーが切れる前に回復した場合、ダウン状態は効率的にフィルタリングされ、デバイス上の他のソフトウェアによってリンクダウン イベントの発生が認識されることはありません。大きなキャリア遅延タイマーでは、検出されるリンクアップ/リンクダウン イベントが少なくなります。キャリア遅延時間を 0 に設定すると、デバイスは発生する各リンクアップ/リンクダウン イベントを検出します。

ほとんどの環境では、短い遅延時間は長い遅延時間より良好です。選択する正確な値は、リンク停止の性質およびこれらのリンクがネットワークで持続すると予想される時間によって異なります。データ リンクが短い停止の影響を受ける場合（特に、これらの停止時間がIPルーティングの収束にかかる時間より短い場合）、長いキャリア遅延の値を設定し、これらの短い停止によってルーティング テーブルで不要な問題が発生するのを防ぐ必要があります。ただし、停止がさらに長くなる傾向がある場合、停止を早く検出し、IP ルート収束が早く始まり早く終わるように、さらに短いキャリア遅延時間を設定できます。

デフォルトのキャリア遅延時間は 100 ミリ秒です。

ポート チャネル パラメータ

ポート チャネルは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構成します。1 つのポート チャネルに最大 8 つの個別インターフェイスをバンドルして、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。

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。

変更した設定をポート チャネルに適用すると、そのポート チャネルのインターフェイス メンバにもそれぞれ変更が適用されます。

ポート チャネルおよびポート チャネルの設定については、「ポート チャネルの設定」を参照してください。

ポート プロファイル

Cisco Nexus 7000 シリーズ デバイスの Cisco NX-OS リリース 4.2(1) 以降では、たくさんのインターフェイス コマンドを含むポート プロファイルを作成して、そのポート プロファイルを一定範囲のインターフェイスに適用できます。ポート プロファイルはそれぞれ特定のタイプのインターフェイスにだけ適用できます。次のインターフェイスから選択できます。

- イーサネット
- VLAN ネットワーク インターフェイス
- ループバック
- ポート チャネル
- Tunnel

インターフェイス タイプにイーサネットまたはポート チャネルを選択する場合、ポート プロファイルはデフォルト モードになります。デフォルト モードはレイヤ 3 です。ポート プロファイルをレイヤ 2 モードに変更するには、**switchport** コマンドを入力します。

ポート プロファイルをインターフェイスまたはインターフェイスの範囲にアタッチするときにポートプロファイルを継承します。ポートプロファイルをインターフェイスまたはインターフェイスの範囲にアタッチ、または継承する場合、そのポート プロファイルのすべてのコマンドがインターフェイスに適用されます。また、ポートプロファイルには、別のポートプロファイルの設定を継承することができます。別のポートプロファイルを継承すると、最初のポートプロファイルは、2 番目の継承されたポート プロファイルのコマンドのすべてが最初のポート プロファイルと競合しないと想定できます。4 つのレベルの継承がサポートされています。任意の数のポート プロファイルで同じポート プロファイルを継承できます。

次の注意事項に従って、インターフェイスまたはインターフェイスの範囲で継承されたコマンドが適用されます。

- 競合が発生した場合は、インターフェイス モードで入力したコマンドがポート プロファイルのコマンドに優先します。しかし、ポートプロファイルはそのコマンドをポートプロファイルに保持します。
- ポートプロファイルのコマンドは、port-profile コマンドがデフォルト コマンドで明示的に上書きされていない限り、インターフェイスのデフォルト コマンドに優先します。
- 一定範囲のインターフェイスが 2 つ目のポート プロファイルを継承すると、矛盾がある場合、最初のポート プロファイルのコマンドが 2 つ目のポート プロファイルのコマンドを無効にします。
- ポート プロフィルをインターフェイスまたはインターフェイスの範囲に継承した後、インターフェイス コンフィギュレーション レベルで新しい値を入力して、個々の設定値を上書きできます。インターフェイス コンフィギュレーション レベルで個々の設定値を削除すると、インターフェイスではポート プロファイル内の値が再度使用されます。
- ポート プロファイルに関連したデフォルト設定はありません。

指定するインターフェイス タイプにより、コマンドのサブセットが port-profile コンフィギュレーション モードで使用できます。

（注） Session Manager にポート プロファイルは使用できません。Session Manager については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』を参照してください。

ポートプロファイル設定をインターフェイスに適用するには、そのポートプロファイルをイネーブルにする必要があります。ポートプロファイルをイネーブルにする前に、そのポートプロファイルを一定範囲のインターフェイスに設定し、継承できます。その後、指定されたインターフェイスで設定が実行されるように、そのポート プロファイルをイネーブルにします。

元のポート プロファイルに 1 つ以上のポート プロファイルを継承する場合、最後に継承されたポート プロファイルだけをイネーブルにする必要があります。こうすれば、その前までのポート プロファイルがイネーブルにされたと見なされます。

ポート プロファイルをインターフェイスの範囲から削除する場合、まずインターフェイスからコンフィギュレーションを取り消して、ポートプロファイルリンク自体を削除します。また、ポートプロファイルを削除すると、インターフェイスコンフィギュレーションが確認され、直接入力された interface コマンドで無効にされた port-profile コマンドをスキップするか、それらのコマンドをデフォルト値に戻します。

他のポート プロファイルにより継承されたポート プロファイルを削除する場合は、そのポート プロファイルを削除する前に継承を無効にする必要があります。

また、ポート プロファイルを元々適用していたインターフェイスのグループの中から、そのプロファイルを削除するインターフェイスを選択することもできます。たとえば、1 つのポート プロファイルを設定した後、10個のインターフェイスに対してそのポートプロファイルを継承するよう設定した場合、その 10 個のうちいくつかのインターフェイスからのみポート プロファイルを削除することができます。ポート プロファイルは、適用されている残りのインターフェイスで引き続き動作します。

インターフェイスコンフィギュレーションモードを使用して指定したインターフェイスの範囲の特定のコンフィギュレーションを削除する場合、そのコンフィギュレーションもそのインターフェイスの範囲のポート プロファイルからのみ削除されます。たとえば、ポート プロファイル内にチャネル グループがあり、インターフェイス コンフィギュレーション モードでそのポート チャネルを削除する場合、指定したポートチャネルも同様にポートプロファイルから削除されます。

デバイスの場合と同様、オブジェクトをインターフェイスに適用せずに、そのオブジェクトのコンフィギュレーションをポート プロファイルに入力できます。たとえば、仮想ルーティングおよび転送（VRF）インスタンスをシステムに適用しなくても、設定できます。その VRF と関連するコンフィギュレーションをポート プロファイルから削除しても、システムに影響はありません。

インターフェイスまたはインターフェイスの範囲のポート プロファイルを継承し、特定の設定値を削除した後、その port-profile コンフィギュレーションは指定のインターフェイスでは動作しません。

ポート プロファイルを誤ったタイプのインターフェイスに適用しようとすると、システムによりエラーが返されます。

ポート プロファイルをイネーブル化、継承、または変更しようとすると、システムによりチェックポイントが作成されます。ポート プロファイル設定が正常に実行されなかった場合は、システムによりその前の設定までロールバックされ、エラーが返されます。ポート プロファイルは部分的にだけ適用されることはありません。

タイム ドメイン反射率計ケーブル診断

Cisco Nexus 7000 シリーズ デバイスの Cisco NX-OS リリース 5.0(2) および最新世代のラインカードの導入以降では、高価なサードパーティ製機器を使用せずに、ケーブル診断を実施できます。ラインカードに直接埋め込まれたケーブル診断機能により、リンク障害を診断するためにケーブルを取り外したりケーブル テスタを接続する必要はありません。ラインカード上の各ポートは、タイム ドメイン反射率計（TDR）を使用して、単独でケーブルの問題を検出し、これらの問題をスイッチ ソフトウェアにレポートできます。

TDR を使用して、パルス波形信号を導体に送信することで導体を分析し、反射された波形の極性、振幅およびラウンドトリップ時間を調べることができます。

ケーブル内の信号の伝播速度を予測し、その反射が送信元に戻るまでにかかる時間を測定することで、反射ポイントまでの距離を測定することが可能です。また、元のパルスの極性および振幅をその反射率と比較することによって、異なるタイプの障害（たとえば、開いたペアまたは短絡したペア）を区別できます。

リモートでケーブル障害を診断できるようにすることで、問題の根本原因を迅速かつ効率的に特定でき、接続問題に対する迅速な対応をユーザに提供できるようになりました。

インターフェイスのライセンス要件

vPC には、ライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

IP トンネルには Enterprise Services ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『Cisco NX-OS Licensing Guide』を参照してください。

他のインターフェイスにはライセンスが必要ありません。

注意事項と制約事項

基本インターフェイス パラメータの設定には次の注意事項と制約事項があります。

- 光ファイバ イーサネット ポートでは、シスコがサポートするトランシーバを使用する必要があります。シスコがサポートするトランシーバをポートに使用していることを確認するには、**show interface transceivers** コマンドを使用します。シスコがサポートするトランシーバを持つインターフェイスは、機能インターフェイスとして一覧表示されます。
- 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。

  デフォルトでは、どのポートもレイヤ 3 インターフェイスです。

  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には、**switchport** コマンドを使用します。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は、**no switchport** コマンドを使用します。
- ローカル ポートにフロー制御を設定する場合は、次の点に注意します。
  - リモート ポート送信パラメータの設定手順が不明の場合にポーズ フレームを受信するには、ローカル ポート受信パラメータを指定済みに設定します。
  - リモート ポート送信パラメータがイネーブルまたは指定済みである場合にポーズ フレームを受信するには、ローカル ポート受信パラメータをイネーブルに設定します。

- 受信したポーズ フレームを無視するには、ローカル ポート受信パラメータをディセーブルに設定します。
- リモート ポート受信パラメータの設定手順が不明の場合にポーズ フレームを送信するには、ローカル ポート送信パラメータを指定済みに設定します。
- リモート ポート受信パラメータがイネーブルまたは指定済みである場合にポーズ フレームを送信するには、ローカル ポート送信パラメータをイネーブルに設定します。
- ポーズ フレームを送信しないようにするには、ローカル ポート送信パラメータをディセーブルに設定します。

- 通常、イーサネット ポート速度およびデュプレックス モード パラメータは自動に設定し、システムがポート間で速度およびデュプレックス モードをネゴシエートできるようにします。これらのポートのポート速度およびデュプレックス モードを手動で設定する場合は、次の点について考慮してください。
  - イーサネットまたは管理インターフェイスに速度およびデュプレックス モードを設定する前に、速度モードとデュプレックス モード, （20 ページ） を参照して同時に設定できる速度およびデュプレックス モードの組み合わせを確認します。
  - イーサネット ポート速度を自動に設定すると、デバイスは自動的にデュプレックス モードを自動に設定します。
  - **no speed** コマンドを開始すると、デバイスは速度およびデュプレックス パラメータの両方を自動的に自動に設定します（**no speed** コマンドを入力すると、**speed auto** コマンドを入力した場合と同じ結果になります）。
  - イーサネット ポート速度を自動以外の値（10 Mb/s、100 Mb/s、1000 Mb/s など）に設定する場合は、それに合わせて接続先ポートを設定してください。接続先ポートが速度をネゴシエーションするように設定しないでください。

（注） 接続先ポートが自動以外の値に設定されている場合、デバイスはイーサネット ポート速度およびデュプレックス モードを自動的にネゴシエートできません。

- デバウンス タイマー リンク アップは、F3 シリーズ ライン カードでのみサポートされます。

注意 イーサネット ポート速度およびデュプレックス モードの設定を変更すると、インターフェイスがシャットダウンされてから再びイネーブルになる場合があります。

デフォルト設定

表 7: 基本インターフェイス パラメータのデフォルト設定

パラメータ	デフォルト
説明	ブランク
ビーコン	ディセーブル
デバウンス タイマー リンク ダウン	イネーブル100 ミリ秒
デバウンス タイマー リンク アップ	ディセーブル
帯域幅	インターフェイスのデータ レート
スループット遅延	100 マイクロ秒
管理ステータス	シャットダウン
MTU	1500 バイト
UDLD グローバル	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
銅線メディア用のポート別 UDLD イネーブル ステート	すべてのイーサネット 10/100 および 1000BASE-TX LAN ポートでディセーブル
UDLD メッセージの間隔	ディセーブル
UDLD アグレッシブ モード	ディセーブル
キャリア遅延	100 ミリ秒
エラー ディセーブル	ディセーブル
エラー ディセーブル回復	ディセーブル
エラー ディセーブル回復間隔	300 秒
リンクのデバウンス	イネーブル
ポート プロファイル	ディセーブル

基本インターフェイス パラメータの設定

基本インターフェイス パラメータの設定

インターフェイスを設定する場合、パラメータを設定する前にインターフェイスを指定する必要があります。

設定するインターフェイスの指定

同じタイプの 1 つ以上のインターフェイスのパラメータを設定する前に、インターフェイスのタイプと ID を指定する必要があります。

以下の表に、イーサネット インターフェイスおよび管理インターフェイスを指定するために使用するインターフェイス タイプと ID を示します。

表 *8*: 設定するインターフェイスの識別に必要な情報

インターフェイス タイプ	ID
イーサネット	I/O モジュールのスロット番号およびモジュールのポート番号
管理	0（ポート 0）

インターフェイス範囲コンフィギュレーション モードを使用して、同じコンフィギュレーション パラメータを持つ複数のインターフェイスを設定できます。インターフェイス範囲コンフィギュレーション モードを開始すると、このモードを終了するまで、入力したすべてのコマンド パラメータが、その範囲内の全インターフェイスに適用されます。

ダッシュ（-）とカンマ（,）を使用して、一定範囲のインターフェイスを入力します。ダッシュは連続しているインターフェイスを区切り、カンマは不連続なインターフェイスを区切ります。不連続なインターフェイスを入力するときは、各インターフェイスのメディア タイプを入力する必要があります。

次に、連続しているインターフェイス範囲の設定例を示します。

```
switch(config)# interface ethernet 2/29-30
switch(config-if-range)#
```

次に、不連続なインターフェイス範囲の設定例を示します。

```
switch(config)# interface ethernet 2/29, ethernet 2/33, ethernet 2/35
switch(config-if-range)#
```

サブインターフェイスが同じポート上の場合にだけ、範囲でサブインターフェイスを指定できます（たとえば、2/29.1-2）。ただし、ポートの範囲でサブインターフェイスを指定できません。たとえば、2/29.2-2/30.2 は入力できません。2 つのサブインターフェイスを個別に指定できます。たとえば、2/29.2、2/30.2 を入力できます。

（注） インターフェイス コンフィギュレーション モードの場合、コマンドを入力するとこのモードに指定したインターフェイスが設定されます。

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)# **interface***interface*	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 タイプと ID を指定できます。イーサネット ポートの場合は、「ethernet slot / port」を使用します。管理インターフェイスの場合は、「mgmt0」を使用します。 （注） インターフェイス タイプと ID（ポートまたはスロット/ポート番号）の間にスペースを追加する必要はありません。たとえば、イーサネット スロット 4、ポート 5 インターフェイスの場合は、「ethernet 4/5」または「ethernet4/5」と指定できます。管理インターフェイスは「mgmt0」または「mgmt 0」となります。

説明の設定

イーサネットおよび管理インターフェイスの説明を文字で設定します。使用できるのは英数字254字以内で、大文字と小文字は区別されます。

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)# **interface***interface*	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 タイプと ID を指定できます。イーサネット ポートの場合は、「ethernet slot/port」を使用します。管理インターフェイスの場合は、「mgmt0」を使用します。

	コマンドまたはアクション	目的
ステップ 3	switch(config-if)# **description***text*	インターフェイスの説明を指定します。最大文字数は 254 文字です。
ステップ 4	switch(config-if)# **exit**	インターフェイス モードを終了します。
ステップ 5	switch(config)# **show interface***interface*	（任意） インターフェイス ステータスを表示します。説明パラメータもあわせて表示します。
ステップ 6	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。

次に、モジュール 3 のイーサネット ポート 24 にインターフェイスの説明を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/24
switch(config-if)# description server1
switch(config-if)#
```

Cisco NX-OS リリース 6.1 以降では、**show interface eth** コマンドの出力は、次の例に示すように拡張されます。

```
switch# show interface eth 2/1
Ethernet2/1 is down (SFP not inserted)
admin state is down, Dedicated Interface
Hardware: 1000 Ethernet, address: 0026.9814.0ec1 (bia f866.f23e.0de8)
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, medium is broadcast
auto-duplex, auto-speed
Beacon is turned off
Auto-Negotiation is turned on
Input flow-control is off, output flow-control is off
Auto-mdix is turned off
Switchport monitor is off
EtherType is 0x8100
EEE (efficient-ethernet) : n/a
Last link flapped never
Last clearing of "show interface" counters never
0 interface resets
30 seconds input rate 0 bits/sec, 0 packets/sec
30 seconds output rate 0 bits/sec, 0 packets/sec
```

ビーコン モードの設定

イーサネット ポートのビーコン モードをイネーブルにして LED を点滅させ、物理的な位置を確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	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 ethernet***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)# {**beacon** | **no beacon**}	ビーコン モードをイネーブルにします。またはビーコンモードをディセーブルにします。デフォルト モードはディセーブルです。
ステップ 4	switch(config)# **show interface ethernet***slot/port*	（任意） ビーコン モード ステートなど、インターフェイスのステータスを表示します。
ステップ 5	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。

次に、イーサネット ポート 3/1 のビーコン モードをイネーブルにする例を示します。

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

次に、イーサネット ポート 3/1 のビーコン モードをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# no beacon
switch(config-if)#
```

帯域幅レート モードの変更

32 ポート 10 ギガビット イーサネット モジュール上の 10 Gb ごとの帯域幅が、1 つのポートに専用であるか、または同一ポート グループ内の 4 つのポートで共有されるかを指定できます。

1 ポート専用帯域幅

帯域幅を 1 つのポート専用にする場合、最初にそのグループの 4 つのポートを管理シャットダウンしてレート モードを専用に変更し、専用ポートを管理的にアップ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	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 ethernet***slot/port*, **ethernet***slot/port*, **ethernet***slot/port*, **ethernet***slot/port*	設定するイーサネット 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	switch(config-if)# **shutdown**	ポートを管理シャットダウンします。
ステップ 4	switch(config)# **interface ethernet***slot/port*	インターフェイスのグループで最初のイーサネット インターフェイスを指定します。
ステップ 5	switch(config-if)# **rate-mode dedicated**	10 GB の全帯域幅を 1 つのポート専用にします。帯域幅を専用にすると、以後のポートのサブコマンドはすべて専用モードになります。
ステップ 6	switch(config-if)# **no shutdown**	ポートを管理的にアップします。
ステップ 7	switch(config-if)# **show interface ethernet***slot/port***capabilities**	（任意） 現在のレート モードを含むインターフェイス情報を表示します。
ステップ 8	switch(config-if)# **exit**	インターフェイス モードを終了します。
ステップ 9	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。

次に、ポート 4/17、4/19、4/21、4/23 を含むグループでイーサネット ポート 4/17 の専用モードを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 4/17, ethernet 4/19, ethernet 4/21, ethernet 4/23
switch(config-if)# shutdown
switch(config-if)# interface ethernet 4/17
switch(config-if)# rate-mode dedicated
switch(config-if)# no shutdown
switch(config-if)#
```

帯域幅をポート グループ内で共有

10 GB の帯域幅を 32 ポート 10 ギガビット イーサネット モジュールのポート グループ（4 ポート）で共有できます。帯域幅を共有するには、専用ポートを管理的にダウンさせて帯域幅を共有するポートを指定し、レート モードを共有に変更してからポートを管理的にアップします。

はじめる前に

同じグループのすべてのポートが同じ VDC に属し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	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 ethernet***slot/port*	インターフェイスのグループで最初のイーサネット インターフェイスを指定します。
ステップ 3	switch(config-if)# **shutdown**	ポートを管理シャットダウンします。
ステップ 4	switch(config)# **interface ethernet***slot/port*, **ethernet***slot/port*, **ethernet***slot/port*, **ethernet***slot/port*	設定する 4 つのイーサネット インターフェイス（同一ポート グループの一部でなければなりません）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 5	switch(config-if)# **rate-mode shared**	指定したポートに共有レート モードを設定します。
ステップ 6	switch(config-if)# **no shutdown**	ポートを管理的にアップします。
ステップ 7	switch(config-if)# **show interface ethernet***slot/port*	（任意） 現在のレート モードを含むインターフェイス情報を表示します。
ステップ 8	switch(config-if)# **exit**	インターフェイス モードを終了します。
ステップ 9	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。

次に、ポート 4/17、4/19、4/21、4/23 を含むグループでイーサネット ポート 4/17 の共有モードを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 4/17
switch(config-if)# shutdown
switch(config)# interface ethernet 4/17, ethernet 4/19, ethernet 4/21, ethernet 4/23
switch(config-if)# rate-mode shared
switch(config-if)# no shutdown
switch(config-if)#
```

Error-Disabled ステートの設定

インターフェイスが error-disabled ステートに移行する理由を表示し、自動回復を設定できます。

Error-Disable 検出のイネーブル化

アプリケーションでの error-disable 検出をイネーブルにできます。その結果、原因がインターフェイスで検出された場合、インターフェイスは error-disabled ステートとなり、リンクダウン ステートに類似した動作ステートとなります。

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)# **errdisable detect cause** {**acl-exception** | **all** | **link-flap** | **loopback**}	インターフェイスを error-disabled ステートにする条件を指定します。デフォルトではイネーブルになっています。
ステップ 3	switch(config)# **shutdown**	インターフェイスを管理的にダウンさせます。インターフェイスを error-disabled ステートから手動で回復させるには、最初にこのコマンドを入力します。
ステップ 4	switch(config)# **no shutdown**	インターフェイスを管理的にアップし、error-disabled ステートから手動で回復させるインターフェイスをイネーブルにします。
ステップ 5	switch(config)# **show interface status err-disabled**	（任意） error-disabled インターフェイスに関する情報を表示します。
ステップ 6	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。

次の例では、すべての場合で error-disabled 検出をイネーブルにする方法を示します。

```
switch(config)# errdisable detect cause all
switch(config)#
```

errdisable ステート回復のイネーブル化

インターフェイスが error-disabled ステートから回復して再びアップ状態になるようにアプリケーションを設定することができます。回復タイマーを設定しない限り、300 秒後にリトライします（**errdisable recovery interval** コマンドを参照）。

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)# **errdisable recovery cause** {**all** | **bpduguard** | **link-flap** | **psecure-violation** | **security-violation** | **storm-control** | **udld**}	インターフェイスが error-disabled ステートから自動的に回復する条件を指定すると、デバイスはインターフェイスを再びアップします。デバイスは 300 秒待機してからリトライします。デフォルトではディセーブルになっています。
ステップ 3	switch(config)# **show interface status err-disabled**	（任意） error-disabled インターフェイスに関する情報を表示します。
ステップ 4	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。

次に、すべての条件下で error-disabled リカバリをイネーブルにする例を示します。

```
switch(config)# errdisable recovery cause all
switch(config)#
```

errdisable ステート回復間隔の設定

error-disabled 回復タイマーの値を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# **errdisable recovery interval***interval*	インターフェイスが error-disabled ステートから回復する間隔を指定します。有効範囲は 30 ～ 65535 秒で、デフォルトは 300 秒です。
ステップ 3	switch(config)# **show interface status err-disabled**	（任意） error-disabled インターフェイスに関する情報を表示します。
ステップ 4	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。

次の例では、error-disabled 回復タイマーが回復の間隔を 32 秒に設定するように設定する方法を示します。

```
switch(config)# errdisable recovery interval 32
switch(config)#
```

MDIX パラメータの設定

接続のタイプ（クロスオーバーまたはストレート）を他の銅線イーサネット ポート専用にする必要がある場合は、ローカル ポートの Medium Dependent Independent Crossover（MDIX）パラメータをイネーブルにします。デフォルトでは、このパラメータはイネーブルです。

はじめる前に

リモート ポートの MDIX 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	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 ethernet***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)# {**mdix auto** | **no mdix**}	ポートの MDIX 検出をイネーブルまたはディセーブルにするかどうかを指定します。

	コマンドまたはアクション	目的
ステップ 4	switch(config-if)# **show interface ethernet***slot/port***capabilities**	（任意） インターフェイス ステータスを表示します。MDIX ステータスもあわせて表示します。
ステップ 5	switch(config-if)# **exit**	インターフェイス モードを終了します。
ステップ 6	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。

次に、イーサネット ポート 3/1 の MDIX をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# mdix auto
switch(config-if)#
```

次に、イーサネット ポート 3/1 の MDIX をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# no mdix
switch(config-if)#
```

デバウンス タイマーの設定

イーサネット ポートのデバウンス タイマーは、デバウンス時間をミリ秒単位（ms）で指定することによりイネーブル化でき、デバウンス時間に 0 を指定することによりディセーブル化できます。

show interface debounce コマンドを使用すれば、すべてのイーサネット ポートのデバウンス時間を表示できます。

手順

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 ethernet***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)# **link debounce [link-up | time]***milliseconds*
指定された時間（0 ～ 5000 ミリ秒）のデバウンス リンク アップまたはダウン タイマーを有効にします。**link debounce link-up** コマンドのデフォルト値は 0 です。デバウンス リンク アップ タイマー値は 100 ミリ秒に設定することをお勧めします。

（注） **link-up** キーワードが指定されていない **link debounce** コマンドは、リンク ダウン デバウンス時間を参照します。

（注） **link debounce link-up** コマンドは、ユーザによって設定された過去の値をすべてオーバーライドします。

0 ミリ秒を指定すると、デバウンス タイマーはディセーブルになります。

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

ステップ 5 （任意） switch(config)# **show interface debounce**
イーサネット インターフェイスすべてのリンク デバウンス時間を示します。

ステップ 6 （任意） 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。

次に、リンク ダウン デバウンス タイマーを有効にして、イーサネット ポート 3/1 に対して 1000 ミリ秒に設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# link debounce time 1000
switch(config-if)#
```

次に、デバウンス リンク アップ タイマーを有効にして、イーサネット ポート 3/1 のデバウンス時間を 1000 ミリ秒に設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# link debounce link-up time 1000
switch(config-if)#
```

次に、イーサネット ポート 3/1 のデバウンス タイマーをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# link debounce time 0
switch(config-if)#
```

インターフェイス速度およびデュプレックス モードの設定

インターフェイス速度とデュプレックス モードは相関関係にあります。このため、両方のパラメータを同時に設定する必要があります。

イーサネット インターフェイスおよび管理インターフェイスに同時に設定できる速度およびデュプレックス モードについては、速度モードとデュプレックス モード, （20 ページ） を参照してください。

（注） 指定するインターフェイス速度はインターフェイスで使用するデュプレックス モードに影響を与えます。このため、デュプレックス モードを設定する前に速度を設定する必要があります。自動ネゴシエーションの速度を設定する場合、デュプレックス モードは自動的に自動ネゴシエーションに設定されます。速度を 10 または 100 Mb/s に指定すると、ポートでは半二重モードを使用するように自動的に設定されますが、全二重モードを指定することもできます。1000 Mb/s（1 Gb/s）以上の速度に設定すると、自動的に全二重モードが使用されます。

はじめる前に

リモート ポートの速度設定はローカル ポートへの変更をサポートします。ローカル ポートを固有の速度で使用するには、リモート ポートにも同じ速度を設定するか、ローカル ポートがその速度を自動ネゴシエートするように設定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	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***interface*	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 タイプと ID を指定できます。イーサネット ポートの場合は、「ethernet slot / port」を使用します。管理インターフェイスの場合は、「mgmt0」を使用します。
ステップ 3	switch(config-if)# **speed** {{**10** | **100** | **1000** | {**auto** [**10** **100** [**1000**]]}} | {**10000** | **auto**}}	48 ポート 10/100/1000 モジュールのイーサネット ポートでは 10 Mb/s、100 Mb/s、1000 Mb/s の速度を設定します。またはポートの速度を同じリンクの他の 10/100/1000 ポートと自動ネゴシエートするように設定します。 32 ポート 10 ギガビット イーサネット モジュールのイーサネット ポートでは、速度を 10,000 Mb/s（10 Gb/s）に設定します。または、ポートがリンクの他の 10 ギガビット イーサネット ポートの速度と自動ネゴシエートするように設定します。 管理インターフェイスでは、速度を 1000 Mb/s に設定します。あるいはポートがその速度と自動ネゴシエートするように設定します。
ステップ 4	switch(config-if)# **duplex** {**full** | **half** | **auto**}	全二重モード、半二重モード、自動ネゴシエート モードを指定します。
ステップ 5	switch(config-if)# **exit**	インターフェイス 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	switch(config)# **show interface***interface*	（任意） インターフェイス ステータスを表示します。速度およびデュプレックス モード パラメータもあわせて表示します。
ステップ 7	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。

次に、スロット 3 の 48 ポート 10/100/1000 モジュールのイーサネット ポート 1 の速度を 1000 Mb/s に設定し、全二重モードに設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# speed 1000
switch(config-if)# duplex full
switch(config-if)#
```

フロー制御の設定

1 Gb/s 以上で動作するイーサネット ポートの場合、フロー制御ポーズ フレームを送受信するポートの機能をイネーブルまたはディセーブルにできます。1 Gb/s 未満で動作するイーサネット ポートの場合、ポーズ フレームを受信するポートの機能だけをイネーブルまたはディセーブルにできます。

ローカルポートのフロー制御をイネーブルにすると、リモートポートでのフロー制御設定にかかわらずローカルポートでのフレームの送受信を完全にイネーブルにするか、リモートポートで指定して使用する設定をローカルポートで使用するように設定します。ローカルおよびリモートポートのフロー制御をどちらもイネーブルにする、一方のポートのフロー制御を指定して設定する、あるいはこの 2 つの状態を組み合わせて設定する場合、それらのポートではフロー制御がイネーブルです。

（注） 10 Gb/s で動作するポートの場合、状態を指定してパラメータを送受信できません。

はじめる前に

必要なフロー制御に対応する設定がリモートポートにあることを確認します。ローカルポートからフロー制御ポーズフレームを送信するには、リモートポートの受信パラメータがオンまたは指定になっていることを確認します。ローカル ポートでフロー制御ポーズ フレームを受信するには、リモート ポートの送信パラメータがオンまたは指定になっていることを確認します。フロー制御を使用しない場合は、リモート ポートの送信パラメータおよび受信パラメータをオフにします。

手順

	コマンドまたはアクション	目的
ステップ 1	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 ethernet***slot/port*	イーサネット インターフェイスにスロット番号およびポート番号を指定し、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)# **flowcontrol** {**send** | **receive**} {**desired** | **on** | **off**}	ポートのフロー制御設定を指定します。1000 Mb/s 以上で動作するポートにのみ送信設定を指定できます。受信設定は任意の速度で動作するポートに設定できます。
ステップ 4	switch(config-if)# **exit**	インターフェイス モードを終了します。
ステップ 5	switch(config)# **show interface ethernet***slot/port*	（任意） インターフェイス ステータスを表示します。フロー制御パラメータもあわせて表示します。
ステップ 6	switch(config)# **show interface flowcontrol**	（任意） すべてのイーサネット ポートのフロー制御状態を表示します。
ステップ 7	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。

次に、イーサネット ポート 3/1 を設定してフロー制御ポーズ フレームを送信する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# flowcontrol send on
switch(config-if)#
```

MTU サイズの設定

レイヤ 2 およびレイヤ 3 イーサネット インターフェイスの最大伝送単位（MTU）サイズを設定できます。レイヤ 3 インターフェイスでは、576 ～ 9216 バイトの MTU を設定できます（偶数値にする必要があります）。レイヤ 2 インターフェイスでは、システム デフォルト MTU（1500 バイト）またはシステム ジャンボ MTU サイズ（デフォルト サイズは 9216 バイト）の MTU を設定できます。

（注） システム ジャンボ MTU のサイズを変更できますが、その値を変更すると、その値を使用するレイヤ 2 インターフェイスが新しいシステム ジャンボ MTU 値に自動的に変更します。

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 コマンドを使用して、ポート モードを変更できます。

ポート モードをレイヤ 2 に変更した後でレイヤ 3 に戻ってレイヤ 3 インターフェイスを設定するには、**no switchport** コマンドを使って再びポート モードを変更します。

インターフェイス MTU サイズの設定

レイヤ 3 インターフェイスでは、576 ～ 9216 バイトの MTU サイズを設定できます。

レイヤ 2 インターフェイスでは、すべてのレイヤ 2 インターフェイスをデフォルト MTU サイズ（1500 バイト）またはシステム ジャンボ MTU サイズ（デフォルト サイズは 9216 バイト）を使用するように設定できます。

レイヤ 2 インターフェイスに別のシステム ジャンボ MTU サイズを使用する必要がある場合は、「システム ジャンボ MTU サイズの設定」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	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 ethernet***slot/port*	設定するイーサネット 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	switch(config-if)# {**switchport** | **no switchport**}	レイヤ 2 またはレイヤ 3 を使用するように指定します。
ステップ 4	switch(config-if)# **mtu***size*	レイヤ 2 インターフェイスでは、デフォルト MTU サイズ（1500）またはシステム ジャンボ MTU サイズ（システム ジャンボ MTU サイズを変更していない場合は 9216）を指定します。 レイヤ 3 インターフェイスでは、576 ～ 9216 の任意の偶数を指定します。
ステップ 5	switch(config-if)# **exit**	インターフェイス 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	switch(config)# **show interface ethernet***slot/port*	（任意） インターフェイス ステータスを表示します。MTU サイズもあわせて表示します。
ステップ 7	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。

次に、レイヤ 2 イーサネット ポート 3/1 にデフォルト MTU サイズ（1500）を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# switchport
switch(config-if)# mtu 1500
switch(config-if)#
```

システム ジャンボ MTU サイズの設定

レイヤ 2 インターフェイスのジャンボ MTU サイズ、レイヤ 2 インターフェイス、およびサブインターフェイスを設定するには、次の作業を実行します。システム ジャンボ MTU サイズを設定しない場合、デフォルトは 9216 バイトです。

ポート チャネル サブインターフェイスでジャンボ MTUを設定する場合は、最初に基本インターフェイスで MTU 9216 を有効にしてから、サブインターフェイスでそれを再設定する必要があります。ジャンボ MTU を基本インターフェイスで有効にする前にサブインターフェイスで有効にすると、次のエラー メッセージがコンソールに表示されます。

```
switch(config)# int po 502.4
switch(config-subif)# mtu 9216
ERROR: Incompatible MTU values
```

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)# **system jumbomtu** *size*	システム ジャンボ MTU サイズを指定します。1500 ～ 9216 の偶数を使用します。
ステップ 3	switch(config)# **show running-config all**	（任意） 現在の稼働設定を表示します。システム ジャンボ MTU サイズもあわせて表示します。

	コマンドまたはアクション	目的
ステップ 4	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。 ジャンボ MTU 用のポート チャネル サブ インターフェイスを有効にする場合は、最初に「mtu 9216」を使用して基本インターフェイスを有効にしてから、「mtu 9216」を使用して MTU サイズをサポートするそれぞれのサブ インターフェイスを設定します。誤った順序で実行した場合は、ジャンボ MTU サポートが有効になりません。
ステップ 5	switch(config-if)# **mtu** *size*	レイヤ 2 インターフェイスでは、デフォルト MTU サイズ（1500）または以前指定したシステム ジャンボ MTU サイズを指定します。 レイヤ 3 インターフェイスでは、576 ～ 9216 の任意の偶数サイズを指定します。 （注） レイヤ 3 ポート チャネル サブインターフェイスのジャンボ MTU をイネーブルにするには、まず **mtu 9216** コマンドを使用して基本（親）インターフェイスをイネーブルにし、続いてこの MTU サイズをサポート対象とする各サブインターフェイスに **mtu 9216** コマンドを設定します。逆の順序（まずサブインターフェイス、次に基本インターフェイス）でコマンドを設定すると、「Incompatible MTU values」のメッセージが表示されます。
ステップ 6	switch(config-if)# **exit**	インターフェイス モードを終了します。
ステップ 7	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。

次に、システム ジャンボ MTU を 8000 バイトに設定し、以前ジャンボ MTU サイズに設定したインターフェイスの MTU に変更する例を示します。

```
switch# configure terminal
switch(config)# system jumbomtu 8000
switch(config)# show running-config
switch(config)# interface ethernet 2/2
switch(config-if)# switchport
switch(config-if)# mtu 8000
switch(config-if)#
```

帯域幅の設定

イーサネット インターフェイスの帯域幅を設定できます。物理レベルでは 1 GB の変更不可能な帯域幅を使用しますが、レベル 3 プロトコルには 1 ～ 10,000,000 Kb の値を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	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 ethernet***slot/port*	設定するイーサネット 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	switch(config-if)# **bandwidth***kbps*	情報用としてのみ 1 ～ 10,000,000 の値を帯域幅に指定します。
ステップ 4	switch(config-if)# **exit**	インターフェイス モードを終了します。
ステップ 5	switch(config)# **show interface ethernet***slot/port*	（任意） インターフェイス ステータスを表示します。帯域幅の値もあわせて表示します。
ステップ 6	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。

次に、イーサネット スロット 3 ポート 1 インターフェイス帯域幅パラメータに情報用の値 1,000,000 Kb を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# bandwidth 1000000
switch(config-if)#
```

スループット遅延の設定

イーサネットインターフェイスのインターフェイス スループット遅延を設定できます。実際の遅延時間は変わりませんが、1 ～ 16777215 の情報値を設定できます。単位は 10 マイクロ秒です。

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)# **interface ethernet***slot/port*	設定するイーサネット 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	switch(config-if)# **delay***value*	遅延時間を 10 マイクロ秒単位で指定します。1 ～ 16777215 の範囲の情報値を 10 マイクロ秒単位で設定できます。
ステップ 4	switch(config-if)# **exit**	インターフェイス モードを終了します。
ステップ 5	switch(config)# **show interface ethernet***slot/port*	（任意） インターフェイス ステータスを表示します。スループット遅延時間もあわせて表示します。
ステップ 6	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。

次に、あるインターフェイスが別のインターフェイスに優先するように、スループット遅延時間を設定する例を示します。低い遅延値が高い値に優先します。この例では、イーサネット 7/48 は 7/47 よりも優先されます。7/48 のデフォルトの遅延は、最大値（16777215）に設定されている 7/47 の設定値より小さいです。

```
switch# configure terminal
switch(config)# interface ethernet 7/47
switch(config-if)# delay 16777215
switch(config-if)# ip address 192.168.10.1/24
switch(config-if)# ip router eigrp 10
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# interface ethernet 7/48
switch(config-if)# ip address 192.168.11.1/24
switch(config-if)# ip router eigrp 10
switch(config-if)# no shutdown
switch(config-if)#
```

（注） feature eigrp コマンドを実行して、最初に EIGRP 機能がイネーブルであることを確認する必要があります。

インターフェイスのシャットダウンおよび再開

イーサネットまたは管理インターフェイスはシャットダウンして再起動できます。インターフェイスはシャットダウンするとディセーブルになり、すべてのモニタ画面にはダウン状態で表示されます。この情報は、すべてのダイナミック ルーティング プロトコルを通じて、他のネットワーク サーバに伝達されます。シャットダウンしたインターフェイスはどのルーティング アップデートにも含まれません。インターフェイスを再開するには、デバイスを再起動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	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***interface*	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 タイプと ID を指定できます。イーサネット ポートの場合は、「ethernet slot / port」を使用します。管理インターフェイスの場合は、「mgmt0」を使用します。
ステップ 3	switch(config-if)# **shutdown**	インターフェイスをディセーブルにします。
ステップ 4	switch(config-if)# **show interface***interface*	（任意） インターフェイス ステータスを表示します。管理ステータスもあわせて表示します。
ステップ 5	switch(config-if)# **no shutdown**	インターフェイスを再びイネーブルにします。
ステップ 6	switch(config-if)# **show interface***interface*	（任意） インターフェイス ステータスを表示します。管理ステータスもあわせて表示します。
ステップ 7	switch(config-if)# **exit**	インターフェイス モードを終了します。
ステップ 8	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。

次に、イーサネット ポート 3/1 の管理ステータスをディセーブルからイネーブルに変更する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

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 モードまたはアグレッシブ 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。

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。

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	イネーブル	ディセーブル
enable UDLD コマンド	**no udld disable**	**udld enable**
disable UDLD コマンド	**udld disable**	**no udld enable**

ノーマル UDLD モードを使用するには、ポートの 1 つをノーマル モードに設定し、他方のポートをノーマル モードまたはアグレッシブ モードに設定する必要があります。アグレッシブ UDLD モードを使用するには、両方のポートをアグレッシブ モードに設定する必要があります。

デフォルトでは、48 ポート 10/100/1000 イーサネット モジュール ポートでは UDLD がディセーブルですが、32 ポート 10 ギガビット イーサネット モジュール ポートではノーマル UDLD モードがイネーブルです。

はじめる前に

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	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 udld**	デバイスの UDLD をイネーブルにします。 **no feature udld** はデバイスの UDLD をディセーブルにします。
ステップ 3	switch(config)# **udld message-time***seconds*	（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。

	コマンドまたはアクション	目的
		（注） インターフェイス レベル タイマーは、双方向 UDLD ステータスが検出された場合にのみ変更します。それ以外の場合、タイマーは 7 秒のままで、変更できません。
ステップ 4	switch(config)# **udld aggressive**	（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	switch(config)# **interface ethernet***slot/port*	（任意） 設定するイーサネット 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	switch(config-if)# **udld** {**enable** | **disable**}	（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。詳細については、上記の表を参照してください。
ステップ 7	switch(config-if)# **exit**	インターフェイス モードを終了します。
ステップ 8	switch(config)# **show udld** [**ethernet***slot/port* | **global** | **neighbors**]	（任意） UDLD のステータスを表示します。
ステップ 9	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。

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)#
```

次の例は、ファイバインターフェイスのアグレッシブ UDLD モードをイネーブルにする方法を示しています。

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

次に、銅インターフェイス イーサネット 3/1 のアグレッシブ UDLD モードをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature udld
switch(config)# udld aggressive
switch(config)# interface ethernet 3/1
switch(config-if-range)# udld enable
switch(config-if-range)#
```

次に、イーサネット ポートの 3/1 の UDLD をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
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
```

キャリア遅延タイマーの設定

キャリア遅延タイマーは、すべてのリンクダウン/リンクアップ イベントがデバイスの他のソフトウェアによって検出されない時間を設定します。長いキャリア遅延時間を設定すると、記録されるリンクダウン/リンクアップ イベントは少なくなります。キャリア遅延時間を 0 に設定すると、デバイスは各リンクダウン/リンクアップ イベントを検出します。

（注） キャリア遅延タイマーは、VLAN ネットワーク インターフェイスでだけ設定できます。このタイマーを他のインターフェイス モードで設定できません。

はじめる前に

VLAN インターフェイス モードであることを確認します。キャリア遅延タイマーは、他のインターフェイス モードで設定できません。

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 vlan***vlan-id*	VLAN インターフェイス モードを開始します。
ステップ 3	switch(config-if)# **carrier-delay** {**sec** | **msec number**}	キャリア遅延タイマーを設定します。0 ～ 60 秒または 0 ～ 1000 ミリ秒の時間を設定できます。デフォルトは 100 ミリ秒です。
ステップ 4	switch(config-if)# **exit**	インターフェイス モードを終了します。
ステップ 5	switch(config)# **show interface***vlan-id*	（任意） インターフェイスのステータスを表示します。
ステップ 6	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。

次に、VLAN 5 に対してキャリア遅延タイマーを 20 秒に設定する例を示します。

```
switch# configure terminal
switch(config)# interface vlan 5
switch(config-if)# carrier-delay 20
switch(config-if)#
```

ポート プロファイルの設定

いくつかの設定パラメータを一定範囲のインターフェイスに同時に適用できます。範囲内のすべてのインターフェイスが同じタイプである必要があります。また、1 つのポート プロファイルから別のポート プロファイルに設定を継承することもできます。システムは 4 つのレベルの継承をサポートしています。

ポート プロファイルの作成

デバイスにポート プロファイルを作成できます。各ポート プロファイルは、タイプにかかわらず、ネットワーク上で一意の名前を持つ必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# **port-profile** [**type** {**ethernet** | **interface-vlan** | **loopback** | **port channel** | **tunnel**}] *name*	指定されたタイプのインターフェイスのポート プロファイルを作成して命名し、ポート プロファイル 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	switch(config-ppm)# **exit**	ポート プロファイル 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	switch(config)# **show port-profile**	（任意） ポート プロファイル設定を表示します。
ステップ 5	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。

次の例では、トンネル インターフェイスに test という名前のポート プロファイルを作成する方法を示します。

```
switch# configure terminal
switch(config)# port-profile type tunnel test
switch(config-ppm)#
```

ポート プロファイル コンフィギュレーション モードの開始およびポート プロファイルの修正

ポート プロファイル コンフィギュレーション モードを開始し、ポート プロファイルを修正できます。ポート プロファイルを修正するには、ポート プロファイル コンフィギュレーション モードを開始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	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)# **port-profile** [**type** {**ethernet** | **interface-vlan** | **loopback** | **port channel** | **tunnel**}] *name*	指定されたポート プロファイルのポート プロファイル コンフィギュレーション モードを開始し、プロファイルの設定を追加または削除します。

	コマンドまたはアクション	目的
ステップ 3	switch(config-ppm)# **exit**	ポート プロファイル 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	switch(config)# **show port-profile**	（任意） ポート プロファイル設定を表示します。
ステップ 5	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。

次に、指定されたポート プロファイルのポート プロファイル コンフィギュレーション モードを開始し、すべてのインターフェイスを管理的にアップする例を示します。

```
switch# configure terminal
switch(config)# port-profile type tunnel test
switch(config-ppm)# no shutdown
switch(config-ppm)#
```

一定範囲のインターフェイスへのポート プロファイルの割り当て

単独のインターフェイスまたはある範囲に属する複数のインターフェイスにポート プロファイルを割り当てることができます。すべてのインターフェイスが同じタイプである必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	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** [**ethernet***slot/port* | **interface-vlan***vlan-id* | **loopback***number* | **port-channel***number* | **tunnel***number*]	インターフェイスの範囲を選択します。
ステップ 3	switch(config-if)# **inherit port-profile***name*	指定したポートプロファイルを、選択したインターフェイスに割り当てます。
ステップ 4	switch(config-ppm)# **exit**	ポートプロファイ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	switch(config)# **show port-profile**	（任意） ポート プロファイル設定を表示します。

	コマンドまたはアクション	目的
ステップ 6	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。

次に、イーサネット インターフェイス 7/3 ～ 7/5、10/2、および 11/20 ～ 11/25 に adam という名前のポート プロファイルを割り当てる例を示します。

```
switch# configure terminal
switch(config)# interface ethernet7/3-5, ethernet10/2, ethernet11/20-25
switch(config-if)# inherit port-profile adam
switch(config-if)#
```

特定のポート プロファイルのイネーブル化

ポートプロファイル設定をインターフェイスに適用するには、そのポートプロファイルをイネーブルにする必要があります。ポートプロファイルをイネーブルにする前に、そのポートプロファイルを一定範囲のインターフェイスに設定し、継承できます。その後、指定されたインターフェイスで設定が実行されるように、そのポート プロファイルをイネーブルにします。

元のポート プロファイルに 1 つ以上のポート プロファイルを継承する場合、最後に継承されたポート プロファイルだけをイネーブルにする必要があります。こうすれば、その前までのポート プロファイルがイネーブルにされたと見なされます。

ポートプロファイルをイネーブルまたはディセーブルにするには、ポートプロファイル コンフィギュレーション モードを開始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	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)# **port-profile** [**type** {**ethernet** | **interface-vlan** | **loopback** | **port channel** | **tunnel**}] *name*	指定されたタイプのインターフェイスのポートプロファイルを作成して命名し、ポートプロファイル 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	switch(config-ppm)# **state enabled**	そのポート プロファイルをイネーブルにします。
ステップ 4	switch(config-ppm)# **exit**	ポートプロファイル 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 5	switch(config)# **show port-profile**	（任意） ポート プロファイル設定を表示します。
ステップ 6	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。

次の例は、ポート プロファイル コンフィギュレーション モードを開始し、ポート プロファイルをイネーブルにする方法を示したものです。

```
switch# configure terminal
switch(config)# port-profile type tunnel test
switch(config-ppm)# state enabled
switch(config-ppm)#
```

ポート プロファイルの継承

ポート プロファイルを既存のポート プロファイルに継承できます。システムは 4 つのレベルの継承をサポートしています。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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)#**port-profile***name*	指定されたポート プロファイルに対して、ポート プロファイル 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	switch(config-ppm)# **inherit port-profile***name*	別のポート プロファイルを既存のポート プロファイルに継承します。元のポート プロファイルは、継承されたポート プロファイルのすべての設定を想定します。
ステップ 4	switch(config-ppm)# **exit**	ポート プロファイル 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	switch(config)# **show port-profile**	（任意） ポート プロファイル設定を表示します。

	コマンドまたはアクション	目的
ステップ 6	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。

次の例では、adam という名前のポート プロファイルを test という名前のポート プロファイルに継承する方法を示します。

```
switch# configure terminal
switch(config)# port-profile test
switch(config-ppm)# inherit port-profile adam
switch(config-ppm)#
```

一定範囲のインターフェイスからのポート プロファイルの削除

プロファイルを適用した一部またはすべてのインターフェイスから、ポート プロファイルを削除できます。この設定は、インターフェイス コンフィギュレーション モードで行います。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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** [**ethernet***slot/port* | **interface-vlan***vlan-id* | **loopback***number* | **port-channel***number* | **tunnel***number*]	インターフェイスの範囲を選択します。
ステップ 3	switch(config-if)# **inherit port-profile***name*	指定したポートプロファイルを、選択したインターフェイスに割り当てます。
ステップ 4	switch(config-if)# **exit**	ポートプロファイル 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	switch(config)# **show port-profile**	（任意） ポート プロファイル設定を表示します。
ステップ 6	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。

次に、イーサネット インターフェイス 7/3 ～ 7/5、10/2、および 11/20 ～ 11/25 に adam という名前のポート プロファイルを割り当てる例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 7/3-5, 10/2, 11/20-25
switch(config-if)# inherit port-profile adam
switch(config-if)#
```

継承されたポート プロファイルの削除

継承されたポート プロファイルを削除できます。この設定は、ポート プロファイル モードで行います。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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)# **port-profile***name*	指定されたポートプロファイルに対して、ポート プロファイル 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	switch(config-ppm)# **inherit port-profile***name*	このポートプロファイルから継承されたポートプロファイルを削除します。
ステップ 4	switch(config-ppm)# **exit**	ポート プロファイル 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	switch(config)# **show port-profile**	（任意） ポート プロファイル設定を表示します。
ステップ 6	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。

次の例では、adam という名前の継承されたポート プロファイルを test という名前のポート プロファイルから削除する方法を示します。

```
switch# configure terminal
switch(config)# port-profile test
switch(config-ppm)# no inherit port-profile adam
switch(config-ppm)#
```

TDR ケーブル診断の実施

高価なサードパーティ製機器を使用せずに、ケーブル診断を実施できます。ラインカード上の各ポートは、TDR診断を使用して、単独でケーブルの問題を検出し、これらの問題をスイッチ ソフトウェアにレポートできます。

はじめる前に

TDR テストの注意事項は次のとおりです。

- TDR では、最大で 115 m の長さのケーブルをテストできます。
- このテストは、ケーブルの両端で同時に開始しないでください。ケーブルの両端でテストを同時に開始すると、テストの結果が不正確になる可能性があります。
- どのケーブル診断テストの場合でも、テストの実行中にポートのコンフィギュレーションを変更しないでください。変更すると、テスト結果が不正確になる可能性があります。
- 関連するポート グループのすべてのポートを、TDR テスト実行前にシャット ダウン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	switch# **test cable-diagnostics tdr interface***number*	指定されたインターフェイスでTDRテストを開始します。インターフェイスで以前に shutdown コマンドが実行されている必要があります。
ステップ 2	switch# **show interface***number***cable-diagnostics-tdr**	（任意） 指定されたインターフェイスのTDRテスト結果を表示します。

次の例では、特定のインターフェイスでTDRテストを行う方法を示します。この例では、イーサネット 3/1 はケーブルが 1 つ喪失しており、イーサネット 3/12 のケーブルと接続は良好です。

```
switch(config)# interface ethernet 3/1-12
switch(config-if-range)# shutdown
switch# test cable-diagnostics tdr interface ethernet 3/1
switch# test cable-diagnostics tdr interface ethernet 3/12
switch# show interface ethernet 3/1 cable-diagnostics-tdr


--------------------------------------------------------------------------------
Interface     Speed  Pair Cable Length   Distance to fault Channel   Pair Status
------------- ----- ---- -------------- ------------------- ------- -----------
Eth3/1        auto    ---     N/A        1 +/- 2 m           Pair A   Open
              auto    ---     N/A        1 +/- 2 m           Pair B   Open
              auto    ---     N/A        1 +/- 2 m           Pair C   Open
              auto    ---     N/A        1 +/- 2 m           Pair D   Open
```

```
n7000# show interface ethernet 3/12 cable-diagnostics-tdr
-------------------------------------------------------------------------------
Interface     Speed  Pair Cable Length   Distance to fault Channel   Pair Status
------------- ----- ---- -------------- ------------------ ------- -----------
Eth3/12         1000  ---  N/A               N/A             Pair A  Terminated
                      ---  N/A               N/A             Pair B  Terminated
                      ---  N/A               N/A             Pair C  Terminated
                      ---  N/A               N/A             Pair D  Terminated
```

スーパーバイザに到達するパケットのレート制限の設定

Cisco NX-OS リリース 5.1 以降では、スーパーバイザ モジュールに到達するパケットのレート制限をデバイスでグローバルに設定できます。詳細については、『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide*』を参照してください。

特定のインターフェイスのスーパーバイザ モジュールに到達するパケットのレート制限も設定できます。

（注） 着信または発信パケットのレートが設定済みレート制限を超過した場合、デバイスはシステム メッセージを記録しますが、パケットをドロップしません。

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)# [**no**] **rate-limit cpu direction** {**input** | **output** | **both**} **pps***packets***action log**	特定のインターフェイスのスーパーバイザ モジュールに到達するパケットのレート制限を設定します。着信または発信パケットのレートが設定済みレート制限を超過した場合、デバイスはシステム メッセージを記録しますが、パケットをドロップしません。範囲は 1 ～ 100000 です。デフォルト レートは 10000 です。
ステップ 3	switch(config-ppm)# **exit**	ポート プロファイル 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 system internal pktmgr interface ethernet***slot/port*	（任意） 特定のインターフェイスのスーパーバイザ モジュールに到達するパケットのインバウンドおよびアウトバウンドのレート制限の設定を表示します。
ステップ 5	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。

次に、特定のインターフェイスのスーパーバイザ モジュールに到達するパケットのレート制限を設定する例を示します。

```
switch# rate-limit cpu direction both pps 1000 action log
switch# show system internal pktmgr interface ethernet 4/9
Ethernet4/9, ordinal: 44
SUP-traffic statistics: (sent/received)
Packets: 528 / 0
Bytes: 121968 / 0
Instant packet rate: 0 pps / 0 pps
Packet rate limiter (Out/In): 1000 pps / 1000 pps
Average packet rates(1min/5min/15min/EWMA):
Packet statistics:
Tx: Unicast 0, Multicast 528
Broadcast 0
Rx: Unicast 0, Multicast 0
Broadcast 0
```

基本インターフェイス パラメータの確認

基本インターフェイス パラメータは、値を表示して確認します。パラメータ値を表示してカウンタのリストをクリアすることもできます。

（注） システムには、作業中の VDC に割り当てられているポートだけが表示されます。

コマンド	目的
show cdp	CDP ステータスを表示します。
show interface *interface*	1 つまたはすべてのインターフェイスに設定されている状態を表示します。
show interface brief	インターフェイスの状態表を表示します。
show interface switchport	レイヤ 2 ポートのステータスを表示します。
show interface status err-disabled	error-disabled インターフェイスに関する情報を表示します。
show interface status error policy [**detail**]	ハードウェア ポリシーと矛盾するインターフェイスおよび VLAN のエラーを表示します。 **detail** コマンドを使用すると、エラーを生成するインターフェイスの詳細が表示されます。
show vdc	現在の VDC のステータスを表示します。

コマンド	目的
show udld*interface*	現在のインターフェイスまたはすべてのインターフェイスの UDLD ステータスを表示します。
show udld-global	現在のデバイスの UDLD ステータスを表示します。
show port-profile	ポート プロファイルに関する情報を表示します。
show system internal pktmgr internal ethernet*slot/port*	特定のインターフェイスのスーパーバイザ モジュールに到達するパケットのインバウンドおよびアウトバウンドのレート制限の設定を表示します。
show errdisable {**recovery** | **detect**}	errdisable リカバリおよび検出ランタイム情報を表示します。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』を参照してください。

インターフェイス カウンタのモニタリング

インターフェイス統計情報の表示

インターフェイスでの統計情報の収集に、最大 3 つのサンプリング間隔を設定できます。

（注） F2 シリーズ I/O モジュールは VLAN 単位の統計情報はサポートしません。したがって、show interface コマンドは、スイッチ仮想インターフェイス（SVI）の VLAN 単位の Rx/Tx カウンタまたは統計情報を表示しません。

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)# **load-interval counters** {{**1** | **2** | **3**} *seconds*}	ビットレートおよびパケットレートの統計情報を収集する最大 3 つのサンプリング間隔を設定します。各カウンタのデフォルト値は、次のとおりです。 • 1：30 秒（VLAN ネットワーク インターフェイスの場合は 60 秒） • 2：300 秒 • 3：未設定
ステップ 3	switch(config)# **show interface***interface*	（任意） インターフェイス ステータスを表示します。カウンタもあわせて表示します。
ステップ 4	switch(config)# **exit**	ポート プロファイル 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	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。

次に、イーサネット ポート 3/1 の 3 種類のサンプリング間隔を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# load-interval counter 1 60
switch(config-if)# load-interval counter 2 135
switch(config-if)# load-interval counter 3 225
switch(config-if)#
```

インターフェイス カウンタのクリア

clear counters interface コマンドを使用して、イーサネットおよび管理インターフェイス カウンタをクリアできます。この作業は、コンフィギュレーション モードまたはインターフェイス コンフィギュレーション モードで実行できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **clear counters interface** {**all** [snmp] | **ethernet***slot/port* [**snmp**] | **loopback***number* | **mgmt***number* | **port channel***channel-number* | **tunnel***tunnel-number* | **vlan***vlan-number*}	インターフェイス カウンタをクリアします。

	コマンドまたはアクション	目的
ステップ 2	switch# **show interface***interface*	（任意） インターフェイスのステータスを表示します。
ステップ 3	switch# **show interface** [**ethernet***slot/port* | **port-channel***channel-number*] **counters**	（任意） インターフェイス カウンタを表示します。

次に、イーサネット ポート 5/5 の簡易ネットワーク管理プロトコル（SNMP）カウンタをクリアする例を示します。

```
switch# clear counters interface ethernet 5/5 snmp
switch#
```

関連資料

関連項目	マニュアル タイトル
『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/interfaces/command/reference/if_cmds.html
『*Interfaces Configuration Guide, Cisco DCNM for LAN*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/dcnm/interfaces/configuration/guide/if_dcnm.html
『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/system_management/configuration/guide/sm_nx_os_cg.html
『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/high_availability/configuration/guide/b_Cisco_Nexus_7000_Series_NX-OS_High_Availability_and_Redundancy_Guide.html
『*Cisco Nexus 2000 Series NX-OS Fabric Extender Software Configuration Guide for Cisco Nexus 7000 Series Switches, Release 6.x*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus2000/sw/configuration/guide/rel_6_1/b_Cisco_Nexus_2000_Series_NX-OS_Fabric_Extender_Software_Configuration_Guide_Release_6-x.html
『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/virtual_device_context/configuration/guide/b-7k-Cisco-Nexus-7000-Series-NX-OS-Virtual-Device-Context-Configuration-Guide.html
『*Cisco NX-OS Licensing Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/licensing/guide/b_Cisco_NX-OS_Licensing_Guide.html

関連項目	マニュアル タイトル
VLAN、MAC アドレス テーブル、プライベート VLAN、およびスパニング ツリー プロトコル。 『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/layer2/configuration/guide/b_Cisco_Nexus_7000_Series_NX-OS_Layer_2_Switching_Configuration_Guide.html
『*Cisco Nexus 7000 Series NX-OS FabricPath Command Reference*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/fabricpath/command/reference/fp_cmd_book.html
『*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/fabricpath/configuration/guide/b-Cisco-Nexus-7000-Series-NX-OS-FP-Configuration-Guide-6x.html
『Cisco Nexus 7000 Series NX-OS Release Notes』	http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-release-notes-list.html

第 4 章

レイヤ 2 インターフェイスの設定

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

レイヤ 2 インターフェイスの設定の機能履歴

この表には、機能の追加や変更によるリリースの更新内容のみが記載されています。

表 *9*：レイヤ *2* インターフェイスの設定の機能履歴

機能名	リリース	機能情報
トランク ポートでのネイティブ VLAN タギング	6.2(10)	**switchport trunk native vlan tag** コマンドのサポートが追加され、**vlan dot1q tag native** コマンドに **exclude control** キーワードが追加されました。

レイヤ 2 インターフェイスの設定

機能名	リリース	機能情報
インターフェイスおよび vlan のポリシー エラーの表示	6.2(2)	ハードウェア ポリシーと矛盾するインターフェイスおよびVLANのエラーを表示する **show interface status error policy** コマンドが追加されました。
インターフェイスから SNMP カウンタをクリア	6.2(2)	インタフェースからSNMP値をクリアするためのオプションを提供する **snmp** キーワードを含めるための **clear counters interface** コマンドが更新されました。
SVI 自動ステートのディセーブル化	6.2(2)	対応する VLAN 内にアップ状態のインターフェイスがない場合でもSVIをアップ状態に保持するための **no autostate** コマンドが追加されました。
低速ドレイン デバイスの検出と輻輳回避	6.1(1)	低速ドレインデバイスの検出および輻輳回避の設定が追加されました。
デフォルト インターフェイス	5.2(1)	複数のインターフェイスの設定をクリアするための **default interface** コマンドが追加されました。
SVI 自動ステート除外	5.2(1)	ポートの状態がSVIのアップまたはダウン状態に影響しないようにするための **switchport autostate exclude** コマンドが追加されました。
インターフェイス統計情報の3つの設定可能なサンプリング間隔	4.2(1)	**load-interval** コマンドが追加されました。

レイヤ 2 インターフェイスの設定

この章では、レイヤ 2 スイッチング ポートを、Cisco NX-OS デバイスでのアクセス ポートまたはトランク ポートとして設定する方法について説明します。

（注） Cisco リリース 5.2 以降では、Cisco Nexus 7000 シリーズのデバイスは FabricPath レイヤ 2 インターフェイスをサポートします。FabricPath 機能およびインターフェイスの詳細については、『*Cisco Nexus 7000 Series NX-OS FabricPath Command Reference*』を参照してください。

Cisco NX-OS リリース 5.1 以降では、レイヤ 2 ポートは次のいずれかとして機能できます。

- トランク ポート
- アクセス ポート
- プライベート VLAN ポート（プライベート VLAN の詳細については、『*Cisco DCNM Layer 2 Switching Configuration Guide*』を参照）
- FabricPath ポート（FabricPath については、『Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide』および『*Cisco DCNM FabricPath Configuration Guide*』を参照）

Cisco NX-OS リリース 5.2(1) 以降では、レイヤ 2 ポートは、共有インターフェイスとしても機能できます。共有インターフェイスとしてアクセス インターフェイスを設定できません。共有インターフェイスについては、『*Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*』を参照してください。

レイヤ 2 ポートは、トランク ポート、アクセス ポート、またはプライベート VLAN ポートとして機能します。

（注） Cisco NX-OS リリース 6.1 以降では、低速ドレイン デバイスの検知と輻輳回避メカニズムは、Fabric Channel over Ethernet（FCoE）トラフィックを伝送する F シリーズ I/O モジュールでサポートされます。Cisco Nexus 7000 シリーズ プラットフォームでの低速ドレイン デバイスの検出と輻輳回避の詳細については、「低速ドレイン デバイスの検出と輻輳回避の設定」の項を参照してください。

レイヤ 2 スイッチング ポートは、アクセス ポートまたはトランク ポートとして設定できます。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。すべてのレイヤ 2 スイッチング ポートは、メディア アクセス コントロール（MAC）アドレス テーブルを維持します。

（注） レイヤ 2 ポートは、トランク ポート、アクセス ポート、またはプライベート VLAN ポートとして機能します。プライベート VLAN の詳細については、『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。

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。

アクセスおよびトランク インターフェイス

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、デバイスのポートはすべてレイヤ 3 ポートです。

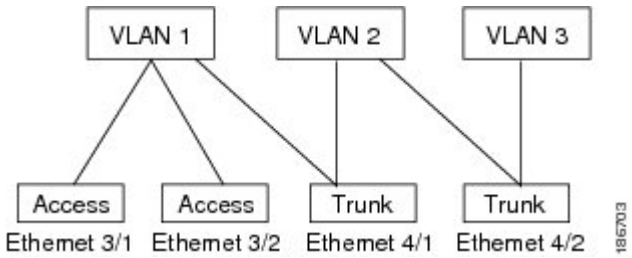
セットアップ スクリプトを使用するか、**system default switchport** コマンドを入力して、すべてのポートをレイヤ 2 ポートにできます。セットアップ スクリプトの使用については、『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x*』を参照してください。CLI を使用して、ポートをレイヤ 2 ポートとして設定するには、**switchport** コマンドを使用します。

1 つのトランク内のポートはすべて、同じ仮想デバイス コンテキスト（VDC）に配置されている必要があります。VDC については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

同じトランクのすべてのポートが同じ VDC であることが必要です。トランク ポートは異なる VDC の VLAN のトラフィックを伝送できません。

以下の図は、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



VLAN ついては、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』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）。

（注） レイヤ 3 インターフェイスでのサブインターフェイスについては、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

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

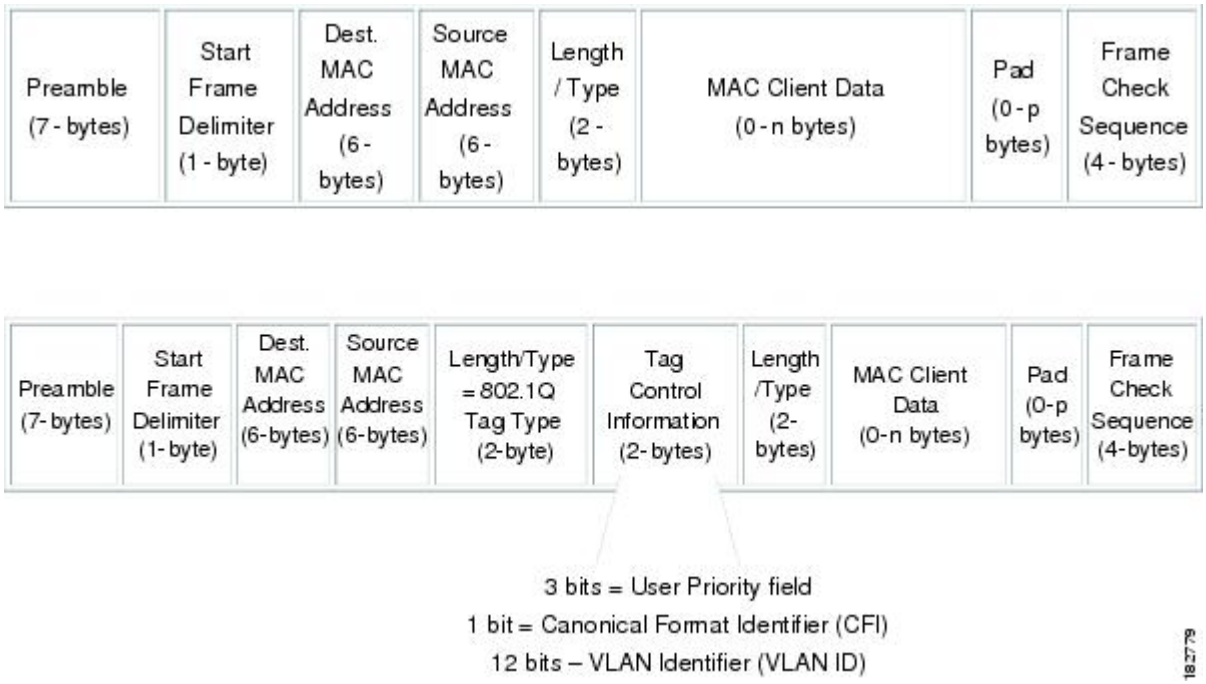
（注） VLAN については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

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（以下の図を参照）。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

（注） アクセス VLAN を割り当て、プライベート VLAN のプライマリ VLAN としても動作させると、そのアクセス VLAN に対応するすべてのアクセス ポートが、プライベート VLAN モードのプライマリ VLAN 向けのすべてのブロードキャスト トラフィックを受信するようになります。

（注） プライベート VLAN の詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

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。

（注） Fibre Channel over Ethernet（FCoE）VLAN をイーサネット トランク スイッチポートのネイティブ VLAN として使用できません。

ネイティブ VLAN トラフィックのタギング

シスコのソフトウェアは、トランク ポートで IEEE 802.1Q 標準をサポートします。タグなしトラフィックがトランク ポートを通過するには、パケットにタグがない VLAN を作成する必要があります（またはデフォルト VLAN を使用することもできます）。タグなしパケットはトランク ポートとアクセス ポートを通過できます。

ただし、デバイスを通過するすべてのパケットに 802.1Q タグがあり、トランクのネイティブ VLAN の値と一致する場合はタギングが取り除かれ、タグなしパケットとしてトランク ポートから出力されます。トランク ポートのネイティブ VLAN でパケットのタギングを保持したい場合は、この点が問題になります。

トランク ポートのすべてのタグなしパケットをドロップし、ネイティブ VLAN ID と同じ 802.1Q の値付きでデバイスに届くパケットのタグを保持するようにデバイスを設定できます。この場合も、すべての制御トラフィックはネイティブ VLAN を通過します。この設定はグローバルです。デバイスのトランク ポートは、ネイティブ VLAN のタギングを保持する場合と保持しない場合があります。

Cisco NX-OS リリース 6.2(10) 以降では、ポート レベルで **switchport trunk native vlan tag** コマンドを使用することで、制御パケットおよびデータ パケットにタグ付けするかどうかを指定できます。たとえば、**switchport trunk native vlan tag exclude control** コマンドを使用すれば、制御パケットをタグ付けせず、データ パケットをタグ付けすることができます。

（注） ポート レベルの設定が適用されると、ネイティブ VLAN タギングのグローバル設定はそのポートでは有効になりません。グローバル設定よりもポート レベルの設定が優先されます。

switchport trunk native vlan tag コマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』を参照してください。

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。

STP の詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

Cisco リリース 5.2 以降では、内部使用に予約されている VLAN のブロックを変更できます。予約されている VLAN の変更の詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』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、トンネル、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設定済みパラメータを消去できます。

（注） 最大 8 ポートがデフォルト インターフェイスに選択できます。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。

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。

SVI 自動ステート除外

一般的に、VLAN インターフェイスに複数のポートがある場合、VLAN 内のすべてのポートがダウンすると、SVI はダウン状態になります。SVI 自動ステート除外機能を使用して、SVI が同じ VLAN に属する場合でも、SVI のステータス（アップまたはダウン）を定義すると同時に特定のポートおよびポート チャネルを除外することができます。たとえば、除外されたポートまたはポート チャネルがアップ状態であり、別のポートが VLAN 内でダウン状態である場合でも、SVI 状態はダウンに変更されます。

（注） SVI 自動ステート除外機能は、スイッチド物理イーサネット ポートおよびポート チャネルに対してのみ使用できます。

SVI 自動ステートのディセーブル化

デバイスのインバンド管理にも SVI を使用できます。具体的には、自動ステートのディセーブル化機能を設定して、対応する VLAN 内にアップ状態のインターフェイスがない場合でも SVI をアップ状態に保持することができます。この機能は、システム（すべての SVI 向け）または個々の SVI に対し設定できます。

ハイ アベイラビリティ

ソフトウェアは、レイヤ 2 ポートのハイ アベイラビリティをサポートします。

（注） ハイ アベイラビリティ機能の詳細については、『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

仮想化のサポート

デバイスは仮想デバイス コンテキスト（VDC）をサポートします。

同じトランクのすべてのポートが同じ VDC であることが必要です。トランク ポートは異なる VDC の VLAN のトラフィックを伝送できません。

（注） VDC およびリソースの割り当ての詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

インターフェイスのライセンス要件

vPC には、ライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

IP トンネルには Enterprise Services ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『Cisco NX-OS Licensing Guide』を参照してください。

他のインターフェイスにはライセンスが必要ありません。

レイヤ2インターフェイスの前提条件

ライセンス 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。
- 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。

レイヤ2インターフェイスの注意事項および制約事項

VLAN トランキングには次の設定上の注意事項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。
- 他社製の 802.1Q デバイスでは、すべての VLAN に対してスパニングツリー トポロジを定義するスパニングツリーのインスタンス（Mono Spanning Tree）が 1 つしか維持されません。802.1Q トランクを介してシスコ製スイッチを他社製のスイッチに接続すると、他社製のスイッチの Mono Spanning Tree とシスコ製スイッチのネイティブ VLAN スパニングツリーが組み合わされて、Common Spanning Tree（CST）と呼ばれる単一のスパニングツリー トポロジが形成されます。
- 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。

- トランク ポートで 802.1X をイネーブルにしようとすると、エラー メッセージが表示され、802.1X はイネーブルになりません。802.1x 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
- アクセス ポートまたはトランク ポートでネイティブ VLAN を変更すると、インターフェイスがフラップされます。これは予想された動作です。

レイヤ 2 インターフェイスのデフォルト設定

表 *10*：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、4048 ～ 4094
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	イネーブル

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。

（注） トランクのすべての VLAN は同じ VDC であることが必要です。

レイヤ 2 アクセス ポートとしての VLAN インターフェイスの設定

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。

はじめる前に

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	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*} | {**port-channel***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)# **switchport mode** {**access** | **trunk**}	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** コマンドを使用します。
ステップ 4	switch(config-if)# **switchport access vlan***vlan-id*	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	switch(config-if)# **exit**	インターフェイス モードを終了します。
ステップ 6	switch(config)# **exit**	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 7	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 8	switch# **show interface status error policy** [**detail**]	（任意） ポリシープログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。

	コマンドまたはアクション	目的
		エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ 9	switch# **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 10	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。

次に、イーサネット 3/1 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 3/1
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。

（注） ポートチャネルインターフェイスについては、「ポート チャネルの設定」および『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

はじめる前に

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	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)# **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	switch(config-if)# **exit**	インターフェイス モードを終了します。
ステップ 5	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 6	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	switch# **show interface status error policy** [**detail**]	（任意） ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ 8	switch# **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	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。

次に、イーサネット 3/1 をレイヤ 2 アクセス ポートとして設定し、PortFast をイネーブルにしてポート チャネルをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
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」の項を参照）。

（注） デバイスは 802.1Q カプセル化だけをサポートします。

はじめる前に

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	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*} | {**port-channel***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)# **switchport mode** {**access** | **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。特定のトランク上で特定の VLAN だけを許可す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	switch(config-if)# **exit**	インターフェイス モードを終了します。
ステップ 5	switch(config)# **exit**	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	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	switch# **show interface status error policy** [**detail**]	（任意） ポリシープログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ 8	switch# **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	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。

次に、イーサネット 3/1 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 3/1
switch(config-if)# switchport mode trunk
switch(config-if)#
```

802.1Q トランク ポートのネイティブ VLAN の設定

ネイティブ VLAN を 802.1Q トランク ポートに設定できます。このパラメータを設定しないと、トランク ポートは、デフォルト VLAN をネイティブ VLAN ID として使用します。

（注） イーサネット インターフェイスのネイティブ VLAN として FCoE VLAN を設定できません。

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*} | {**port-channel***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)# **switchport trunk native vlan***vlan-id*	802.1Q トランクのネイティブ VLAN を設定します。指定できる範囲は 1 ～ 4094 です（ただし、内部使用に予約されている VLAN は除きます）。デフォルト値は VLAN 1 です。
ステップ 4	switch(config-if)# **exit**	インターフェイス モードを終了します。
ステップ 5	switch(config)# **exit**	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 6	switch# **show vlan**	VLAN のステータスおよび情報を表示します。
ステップ 7	switch# **show interface status error policy** [**detail**]	（任意） ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ 8	switch# **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	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。

次に、ネイティブ VLAN をイーサネット 3/1 に設定し、レイヤ 2 トランク ポートを VLAN5 に設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# switchport trunk native vlan 5
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。

switchport trunk allowed vlan*vlan-list* コマンドは、指定したポートの現在の VLAN リストを新しいリストと置き換えます。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には、設定をペーストする前に **terminal dont-ask** コマンドを使用して、メッセージの表示をディセーブルにできます。

はじめる前に

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。

Cisco リリース 5.2 以降では、内部使用に予約されている VLAN のブロックを変更できます。予約されている VLAN の変更の詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』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	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*} | {**port-channel***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)# **switchport trunk allowed vlan** {*vlan-list* | **add***vlan-list* | **all** | **except***vlan-list* | **none** | **remove***vlan-list*}	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。VLAN 3968 ～ 4047 は、内部で使用するデフォルトで予約されている VLAN です。デフォルトでは、すべてのトランク インターフェイスですべての VLAN が許可されます。Cisco リリース 5.2(1) 以降では、デフォルトの予約済み VLAN は 3968 ～ 4094 で、予約済み VLAN のブロックを変更できます。詳細については、『*Cisco Nexus*

	コマンドまたはアクション	目的
		7000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。 （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	switch(config-if)# **exit**	インターフェイス モードを終了します。
ステップ 5	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 6	switch# **show vlan**	VLAN のステータスおよび情報を表示します。
ステップ 7	switch# **show interface status error policy** [**detail**]	（任意） ポリシープログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ 8	switch# **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	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。

次に、VLAN 15 ～ 20 をイーサネット 3/1、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 3/1
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、ポートチャネル、およびトンネル インターフェイスなどの複数インターフェイスの既存コン

フィギュレーションを消去できます。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	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)# **default interface***int-if* [**checkpoint***name*]	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** キーワードを使用して、設定を消去する前にインターフェイスの実行コンフィギュレーションのコピーを保存します。
ステップ 3	switch(config)# **exit**	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	switch# **show interface**	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	switch# **show interface status error policy** [**detail**]	（任意） ポリシープログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ 6	switch# **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。

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 3/1 checkpoint test8
.......Done
switch(config)#
```

SVI 自動ステート除外の設定

イーサネットインターフェイスまたはポート チャネルに SVI 自動ステート除外機能を設定できます。自動ステート除外オプションを使用して、ポートが SVI 計算を稼働または停止したり、それを選択したポートでイネーブルのすべての VLAN に適用するのをイネーブルまたはディセーブルにすることができます。また、自動ステートが除外されたインターフェイスから VLAN を除外するには、SVI 自動ステート除外 VLAN 機能を使用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	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*} | {**port-channel***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)# **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ます。
ステップ 4	switch(config-if)# [**no**] **switchport autostate exclude**	VLAN に複数のポートがあるときに、VLAN インターフェイスのリンクアップ計算からポートを除外します。 デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。
ステップ 5	switch(config-if)# [**no**] **switchport autostate exclude vlan***vlan id*	自動ステート除外インターフェイスから vlan または vlan のセットを除外します。これにより、システムの中断を最小限に抑えることができます。 デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。
ステップ 6	switch(config-if)# **exit**	インターフェイス モードを終了します。
ステップ 7	switch(config)# **exit**	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。

	コマンドまたはアクション	目的
ステップ 8	switch# **show running-config interface** {{**type***slot/port*} | {**port-channel***number*}	（任意） 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。
ステップ 9	switch# **show interface status error policy** [**detail**]	（任意） ポリシープログラミング中にエラーを生成するインターフェイスおよびVLANが表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ 10	switch# **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 11	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。

次に、Cisco NX-OS デバイスで VLAN インターフェイスのリンクアップ計算からポートを除外する例を示します。

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

次に、自動除外インターフェイスから VLAN を除外する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# switchport
switch(config-if)# switchport autostate exclude
switch(config-if)# switchport autostate exclude vlan 10
```

システムの SVI 自動ステートのディセーブル化の設定

SVI 自動ステートのディセーブル化機能を設定して、対応する VLAN 内にアップ状態のインターフェイスがない場合でも SVI をアップ状態に保持することができます。システム全体にこの機能を設定するには、次の手順を使用します。

はじめる前に

システム全体にこの機能を設定する前に、正しい VDC にいることを確認します。VDC の変更は **switchto vdc** コマンドを使用します。

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)# **system default interface-vlan no autostate**	デバイスに対するデフォルトの自動ステート動作をディセーブルにします。
ステップ 3	switch# **show interface status error policy** [**detail**]	（任意） ポリシープログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ 4	switch# **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	switch# **show running-config** [**all**]	（任意） 実行コンフィギュレーションを表示します。 デフォルト情報および設定情報を表示するには、**all** キーワードを使用します。

次に、Cisco NX-OS デバイス上でデフォルトの自動ステート動作をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# system default interface-vlan no autostate
switch(config)# show running-config
```

SVI 単位の SVI 自動ステートのディセーブル化の設定

個々の SVI 上で SVI 自動ステートのイネーブル化またはディセーブル化を設定できます。SVI レベルの設定は、その特定の SVI に対するシステムレベルの SVI 自動ステート設定より優先されます。

はじめる前に

SVI レベルでこの機能を設定する前に、正しい VDC にいることを確認します。VDC の変更は **switchto vdc** コマンドを使用します。

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)# **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	switch(config)# **interface vlan***vlan-id*	VLAN インターフェイスを作成し、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 ～ 4094 です。
ステップ 4	switch(config-if)# [**no**] **autostate**	デフォルトでは、指定されたインターフェイスの SVI 自動ステート機能をイネーブルにします。 デフォルト設定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 5	switch(config-if)# **exit**	インターフェイス コンフィギュレーション モードを終了します。
ステップ 6	switch(config)#**show running config-interface vlan***vlan-id*	（任意） 特定の VLAN インターフェイスの実行コンフィギュレーションを表示します。
ステップ 7	switch(config)# **show interface status error policy** [**detail**]	（任意） ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ 8	switch(config)# **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

	コマンドまたはアクション	目的
		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	switch(config)# **show startup-config interface vlan***vlan id*	（任意） スタートアップ コンフィギュレーションの VLAN 設定を表示します。

次に、個々の SVI 上でデフォルトの自動ステート動作をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature interface-vlan
switch(config)# interface vlan10
witch(config-if)# no autostate
```

ネイティブ VLAN トラフィックにタグを付けるためのデバイス設定

802.1Q トランク インターフェイスを使用する場合、ネイティブ VLAN ID の値と一致しすべてのタグなしトラフィックをドロップするタグで開始するすべてのパケットに対するタギングを維持できます（この場合もインターフェイスの制御トラフィックは伝送されます）。この機能はデバイス全体に当てはまります。デバイスの VLAN を指定して当てはめることはできません。

vlan dot1q tag native グローバル コマンドを使用すると、デバイスのすべてのトラフィックですべてのネイティブ VLAN ID インターフェイスの動作を変更できます。

（注） あるデバイス上で 802.1Q タギングをイネーブルにし、別のデバイスではディセーブルにすると、デバイス上のトラフィックはすべてドロップされ、この機能はディセーブルになります。この機能はデバイスごとに独自に設定する必要があります。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。VDC が異なっていても同じ VLAN 名と ID を使用できるので、正しい VDC で作業していることを確認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	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)# **vlan dot1q tag native**	802.1Q トランキング ネイティブ VLAN ID インターフェイスの動作を変更します。このインターフェイスは、ネイティブ VLAN ID の値と一致して、すべての非タグ付きトラフィックをドロップするタグを使って入るすべてのパケットのタギングを維持します。この場合も、制御トラフィックはネイティブ VLAN を通過します。デフォルトではディセーブルになっています。
ステップ 3	switch(config)# **exit**	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	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 5	switch# **show interface status error policy** [**detail**]	（任意） ポリシー プログラミング中にエラーを生成するインターフェイスおよびVLANが表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ 6	switch# **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	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。

次に、802.1Q トランク インターフェイスのネイティブ VLAN の動作を変更してタグ付きパケットを維持し、すべての非タグ付きトラフィックをドロップする例を示します（制御トラフィックは除く）。

```
switch# configure terminal
switch(config)# vlan dot1q tag native
switch#
```

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。

ストレージ VDC でファイバ チャネルにシステム デフォルトのポート モードを設定する方法については、『*Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*』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	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)# **system default switchport** [**shutdown**]	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） **system default switchport shutdown** コマンドを発行すると、**no shutdown** を使って設定されていないすべての FEX HIF が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** を使って FEX HIF を設定します。
ステップ 3	switch(config)# **exit**	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	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	switch# **show interface status error policy** [**detail**]	（任意） ポリシー プログラミング中にエラーを生成するインターフェイスおよびVLANが表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ 6	switch# **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	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。

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)#
```

低速ドレイン デバイスの検出と輻輳回避の設定

Fibre Channel over Ethernet（FCoE）でのエンド デバイス間のデータ トラフィックは、リンク レベルおよび各ホップをベースとしたフロー制御を使用します。低速デバイスがファブリックに接続されている場合、エンド デバイスは、設定されたレートでフレームを受け入れません。低速デバイスの存在がリンクのトラフィック輻輳の原因となります。トラフィックの輻輳は、宛先デバイスに低速ドレインが発生していない場合でも、トラフィックに同一のスイッチ間リンク（ISL）を使用するファブリック内の無関係のフローに影響を与えます。

Cisco NX-OS リリース 6.1 以降では、低速ドレイン デバイスの検出と輻輳回避は、FCoE トラフィックを伝送する F シリーズ I/O モジュールでサポートされます。機能拡張は、主に低速ドレイン デバイスに接続されるエッジ ポートにあり、エッジ ポート内の輻輳状態を最小限に抑えます。

一度低速ドレイン デバイスがネットワーク上で検出されると、エッジ ポートに対するフレーム タイムアウト値を小さな値に設定し、設定したしきい値を使用するすべてのパケットに対しタイムアウト ドロップを強制できます。フレーム タイムアウト値を小さくすることにより、エッジ ポートで実際にタイムアウトになる時間より早くパケットがドロップされるため、ファブリックに影響する低速ドレイン状態が軽減されます。デフォルトのタイムアウト値は 500 ミリ秒です。この機能は、ISL のバッファ領域を空にし、低速ドレイン状態が発生していない他の無関係なフローが使用できるようにします。

組み込みイベント マネージャ（EEM）システム ポリシー __ori_mac_edge_pause（F1 I/O モジュールの場合）または __clm_sw_edge_port_pause（F2 /I/O モジュールの場合）を上書きしようとすると、デフォルト アクションとデフォルトの syslog も表示されます。action err-disable を指定して、この条件が発生する不良ポートを隔離することを推奨します。

次は、F1 I/O モジュールの EEM システム ポリシーを上書きする出力例です。

```
event manager applet my_eem_policy override __ori_mac_edge_pause
description "my_f1_Pause_eem_policy"
event policy-default count 1 time 2
action 1.0 cli switchto vdc storage
action 2.0 cli eth-port-manager internal-errdisable $interface $cause $SYSERR
```

輻輳フレーム タイムアウト値の設定

デフォルトの輻輳フレーム タイムアウト値は 500 ミリ秒です。ISL に対してはデフォルト設定を保持し、エッジ ポートに対してはデフォルト値を超えない値を設定することを推奨します。フレームが設定された輻輳フレーム タイムアウトよりも長い時間スイッチ内にある場合、それはドロップされ、ISL 内のバッファ領域が空になり、輻輳が緩和されます。

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# [**no**] **system default interface congestion timeout***milliseconds***mode** {**core** | **edge**}	デバイスに対する新しい輻輳フレーム タイムアウト値（ミリ秒）およびポート モードを設定します。 輻輳のタイムアウトの範囲は 100 ～ 1000 ミリ秒です。
ステップ 3	switch# **system default interface congestion mode** {**core** | **edge**}	デバイスに対するデフォルトの輻輳フレーム タイムアウト値（ミリ秒）およびポート モードを設定します。 輻輳のタイムアウトの範囲は 100 ～ 1000 ミリ秒です。
ステップ 4	switch# **show logging onboard flow-control request-timeout**	（任意） タイムスタンプ情報を使用してモジュールごとの送信元/宛先ペアに対する要求タイムアウトを表示します。

エッジ ポートに対し低い値のタイムアウト値（たとえば 100 または 200 ミリ秒）を設定すると、エッジ ポートの輻輳を軽減できます。輻輳が発生すると、それらのポートのパケットはすぐにタイムアウトします。500 ミリ秒のデフォルト タイムアウトに戻すには、**no system default interface congestion timeout***milliseconds***mode** {**core** | **edge**} command（または）**system default interface congestionmode** {**core** | **edge**} を使用します。

（注） 輻輳フレーム タイムアウト設定は、vdc に対してローカルで、vdc によって所有されているポート（エッジ/コア）上でのみ有効です。

（注） デフォルト設定をコア ポートに使用し、ファブリック エッジ ポートに 500 ミリ秒を超えない輻輳フレーム タイムアウト値を設定します。輻輳フレーム タイムアウト値の推奨される範囲は 100 ～ 200 ミリ秒です。

次に、スーパーバイザ CLI のタイムスタンプ情報を使用してモジュールごとの送信元/宛先ペアに対する要求タイムアウトを表示する例を示します。

```
SUP CLI:
switch# show logging onboard flow-control request-timeout
----------------------------
Module: 2
----------------------------
-------------------------------------------------------------------------------
| Dest |     Source |   Events   |   Timestamp    |  Timestamp      |
| Intf |       Intf |    Count   |     Earliest   |   Latest        |
-------------------------------------------------------------------------------
|fc4/3 |eth2/1,eth2/2 | 1736|11/14/2002-00:40:07|11/14/2002-00:57:22|
-------------------------------------------------------------------------------
|fc4/3 |eth2/1,eth2/2 | 3477|11/13/2002-23:23:27|11/14/2002-00:00:48|
-------------------------------------------------------------------------------
|fc4/3 |eth2/1,eth2/2 | 4298|11/13/2002-22:31:40|11/13/2002-23:18:00|
-------------------------------------------------------------------------------
|fc4/3 |eth2/1,eth2/2 | 9690|11/13/2002-04:54:50|11/13/2002-07:31:58|
```

次に、モジュール CLI のタイムスタンプ情報を使用してモジュールごとの送信元/宛先ペアに対する要求タイムアウトを表示する例を示します。

```
Module CLI:
module--x# show logging onboard flow-control request-timeout
-------------------------------------------------------------------------------
| Dest |     Source |   Events   |   Timestamp    |  Timestamp      |
| Intf |       Intf |    Count   |     Earliest   |   Latest        |
-------------------------------------------------------------------------------
|fc4/3 |eth2/1,eth2/2 | 1736|11/14/2002-00:40:07|11/14/2002-00:57:22|
-------------------------------------------------------------------------------
|fc4/3 |eth2/1,eth2/2 | 3477|11/13/2002-23:23:27|11/14/2002-00:00:48|
-------------------------------------------------------------------------------
|fc4/3 |eth2/1,eth2/2 | 4298|11/13/2002-22:31:40|11/13/2002-23:18:00|
-------------------------------------------------------------------------------
|fc4/3 |eth2/1,eth2/2 | 9690|11/13/2002-04:54:50|11/13/2002-07:31:58|
```

ポーズ フレーム タイムアウト値の設定

Cisco NX-OS 6.1 以降では、ポートのポーズ フレーム タイムアウト値をイネーブルまたはディセーブルにできます。システムは一時停止状態についてポートを定期的にチェックし、ポートが設定された期間に継続的な一時停止状態にある場合は、ポートのポーズ フレーム タイムアウトをイネーブルにします。この状況は、出力でドロップされるポートに接続するすべてのフレームで発生します。この機能により ISL リンクのバッファ領域が空になり、同じリンクを使用する他の無関係のフロー上のファブリックの減速と輻輳を軽減できます。

一時停止状態がポートでクリアされたりポートがフラップすると、システムはその特定のポート上のポーズ フレーム タイムアウトをディセーブルにします。

ポーズ フレーム タイムアウトはデフォルトでイネーブルになっています。ISL に対してはデフォルト設定を保持し、エッジ ポートに対してはデフォルト値を超えない値を設定することを推奨します。

低速ドレイン デバイスの動作から迅速にリカバリするには、ポーズ フレーム タイムアウト値を設定する必要があります。それは、フレームが輻輳したタイムアウトのスイッチにあるかどうかにかかわらず、低速ドレインに直面しているエッジ ポート内のすべてのフレームがドロップされるためです。このプロセスにより、ISL 内の輻輳がすぐにクリアされます。輻輳を完全にクリアするには、輻輳フレーム タイムアウト値を設定する代わりにポーズ フレーム タイムアウト値を設定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	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# **system default interface pause timeout***milliseconds***mode** {**core** | **edge**}	デバイスに対する新しいポーズ フレーム タイムアウト値（ミリ秒）およびポート モードを設定します。
ステップ 3	switch# **system default interface pause mode** {**core** | **edge**}	デバイスに対するデフォルトのポーズフレーム タイムアウト値（ミリ秒）およびポート モードを設定します。 輻輳のタイムアウトの範囲は 100 ～ 500 ミリ秒です。
ステップ 4	switch# **no system default interface pause timeout***milliseconds***mode** {**core** | **edge**}	デバイスに対するポーズ フレーム タイムアウトをディセーブルにします。
ステップ 5	switch# **no system default interface pause mode** {**core** | **edge**}	デバイスに対するデフォルトのポーズフレーム タイムアウトをディセーブルにします。
ステップ 6	switch# **show logging onboard flow-control pause-event** [**module***x*]	1 インターフェイス 1 モジュールごとの一時停止イベントの総数を表示します。
ステップ 7	switch# **show logging onboard flow-control pause-count** [**module***x*] [*last mm minutes*] [*last hh hours*] [*last dd days*]	（任意） タイムスタンプ情報を使用して 1 インターフェイス 1 モジュールごとのポーズ カウンタを表示します。
ステップ 8	switch# **show logging onboard flow-control timeout-drops** [**module***x*] [*last mm minutes*] [*last hh hours*] [*last dd days*]	（任意） タイムスタンプ情報を使用して 1 インターフェイス 1 モジュールごとのタイムアウト ドロップを表示します。

エッジ ポート上のポーズ フレーム タイムアウト値を無効にするには、**no system default interface pause timeout***milliseconds***mode** {**core** | **edge**} コマンドを使用します。デフォルトのポーズ タイムアウト値は 500 ミリ秒です。

一時停止イベントの例

次に、スーパーバイザ CLI に関する 1 インターフェイス 1 モジュールごとの一時停止イベントの総数を表示する例を示します。

```
SUP CLI:
switch# show logging onboard flow-control pause-event module 2
----------------------------
Module: 2
----------------------------
------------------------------------------------------------------------------
STATISTICS INFORMATION FOR DEVICE ID 137 DEVICE Orion MAC Driver
------------------------------------------------------------------------------
                           |           | Time Stamp      |In|Port
Error Stat Counter Name    | Count     |MM/DD/YY HH:MM:SS|st|Range
                           |           |                 |Id|
------------------------------------------------------------------------------
SW PL0 pause event VL3     |0x4e45b    |06/18/03 05:27:50 |00|1
SW PL0 pause event VL3     |0x4e1a0    |06/18/03 05:25:50 |00|1
SW PL0 pause event VL3     |0x4dee5    |06/18/03 05:23:50 |00|1
SW PL0 pause event VL3     |0x4dc2a    |06/18/03 05:21:50 |00|1
```

次に、モジュール CLI に関する 1 インターフェイス 1 モジュールごとの一時停止イベントの総数を表示する例を示します。

```
Module CLI:
module-2# show logging onboard flow-control pause-event
------------------------------------------------------------------------------
STATISTICS INFORMATION FOR DEVICE ID 137 DEVICE Orion MAC Driver
------------------------------------------------------------------------------
                           |           | Time Stamp      |In|Port
Error Stat Counter Name    | Count     |MM/DD/YY HH:MM:SS|st|Range
                           |           |                 |Id|
------------------------------------------------------------------------------
SW PL0 pause event VL3     |0x4e45b    |06/18/03 05:27:50|00|1
SW PL0 pause event VL3     |0x4e1a0    |06/18/03 05:25:50|00|1
SW PL0 pause event VL3     |0x4dee5    |06/18/03 05:23:50|00|1
SW PL0 pause event VL3     |0x4dc2a    |06/18/03 05:21:50|00|1
SW PL0 pause event VL3     |0x4d96f    |06/18/03 05:19:50|00|1
```

ポーズ カウンタの例

次に、スーパーバイザ CLI に関するタイムスタンプ情報を使用した 1 インターフェイス 1 モジュールごとのポーズ カウンタを表示する例を示します。

```
SUP CLI:
switch# show logging onboard flow-control pause-count
------------------------------------------------------------------------------
STATISTICS INFORMATION FOR DEVICE ID 137 DEVICE Orion MAC Driver
------------------------------------------------------------------------------
                                   |           | Time Stamp      |In|Port
Error Stat Counter Name            | Count     |MM/DD/YY HH:MM:SS|st|Range
                                   |           |                 |Id|
------------------------------------------------------------------------------
GD Received pause transitions of XO|0x984       |06/17/03 14:23:59|00|1
FF-XON UP3                         |           |                 |  |
GD Received pause transitions of XO|0x41f       |06/17/03 14:21:59|00|1
FF-XON UP3                         |           |                 |  |
```

次に、モジュール CLI に関するタイムスタンプ情報を使用した 1 インターフェイス 1 モジュールごとのポーズ カウンタを表示する例を示します。

```
Module CLI:
module-2# show logging onboard flow-control pause-count
------------------------------------------------------------------------------
STATISTICS INFORMATION FOR DEVICE ID 137 DEVICE Orion MAC Driver
------------------------------------------------------------------------------
                                   |           | Time Stamp      |In|Port
Error Stat Counter Name            | Count     |MM/DD/YY HH:MM:SS|st|Range
```

```
                                  |           |                 |Id|
-------------------------------------------------------------------------------
GD Received pause transitions of XO|0x984 |06/17/03 14:23:59|00|1
FF-XON UP3                         |      |                 |  |
GD Received pause transitions of XO|0x41f |06/17/03 14:21:59|00|1
FF-XON UP3                         |      |                 |  |
```

タイムアウト ドロップの例

次に、スーパーバイザCLIに関するタイムスタンプ情報を使用した1インターフェイス1モジュールごとのタイムアウト ドロップを表示する例を示します。

```
SUP CLI:
switch# show logging onboard flow-control timeout-drops
switch# show logging onboard flow-control timeout-drops
----------------------------
Module: 2
----------------------------
-------------------------------------------------------------------------------
STATISTICS INFORMATION FOR DEVICE ID 137 DEVICE Orion MAC Driver
-------------------------------------------------------------------------------
                                  |           | Time Stamp      |In|Port
Error Stat Counter Name           | Count     |MM/DD/YY HH:MM:SS|st|Range
                                  |           |                 |Id|
-------------------------------------------------------------------------------
ORI_EB_CNT_P0_SF_TIMESTAMP_DROP   |0x100e     |11/14/02 00:45:43|00|1
ORI_EB_CNT_P0_SF_TIMESTAMP_DROP   |0xfd2      |11/14/02 00:43:42|00|1
Module CLI:
```

次に、モジュールCLIに関するタイムスタンプ情報を使用した1インターフェイス1モジュールごとのタイムアウト ドロップを表示する例を示します。

```
module-2# show logging onboard flow-control timeout-drops
-------------------------------------------------------------------------------
STATISTICS INFORMATION FOR DEVICE ID 137 DEVICE Orion MAC Driver
-------------------------------------------------------------------------------
                                  |           | Time Stamp      |In|Port
Error Stat Counter Name           | Count     |MM/DD/YY HH:MM:SS|st|Range
                                  |           |                 |Id|
-------------------------------------------------------------------------------
ORI_EB_CNT_P0_SF_TIMESTAMP_DROP   |0x100e     |11/14/02 00:45:43|00|1
ORI_EB_CNT_P0_SF_TIMESTAMP_DROP   |0xfd2      |11/14/02 00:43:42|00|1
```

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 interface status error policy [**detail**]	ハードウェア ポリシーと矛盾するインターフェイスおよび VLAN のエラーを表示します。 **detail** コマンドを使用すると、エラーを生成するインターフェイスの詳細が表示されます。
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。

これらのコマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』を参照してください。

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 {**interval***seconds* {**1** | **2** | **3**}}	Cisco Nexus 7000 シリーズ デバイスの Cisco NX-OS Release 4.2(1) から、3 種類のサンプリング間隔をビットレートおよびパケットレートの統計情報に設定します。

コマンド	目的
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、マルチキャストを、出力パケットおよびバイトとともに表示します。
show interface counters errors [**module***module*]	エラー パケットの数を表示します。

これらのコマンドについては、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』を参照してください。

アクセス ポートおよびトランク ポートの設定例

ここでは、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 2/30
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 2/35
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
switch(config)# vlan dot1q tag native
switch(config)#
```

関連資料

関連項目	マニュアル タイトル
『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/interfaces/command/reference/if_cmds.html
『*Interfaces Configuration Guide, Cisco DCNM for LAN*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/dcnm/interfaces/configuration/guide/if_dcnm.html

関連項目	マニュアル タイトル
『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/system_management/configuration/guide/sm_nx_os_cg.html
『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/high_availability/configuration/guide/b_Cisco_Nexus_7000_Series_NX-OS_High_Availability_and_Redundancy_Guide.html
『*Cisco Nexus 2000 Series NX-OS Fabric Extender Software Configuration Guide for Cisco Nexus 7000 Series Switches, Release 6.x*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus2000/sw/configuration/guide/rel_6_1/b_Cisco_Nexus_2000_Series_NX-OS_Fabric_Extender_Software_Configuration_Guide_Release_6-x.html
『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/virtual_device_context/configuration/guide/b-7k-Cisco-Nexus-7000-Series-NX-OS-Virtual-Device-Context-Configuration-Guide.html
『*Cisco NX-OS Licensing Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/licensing/guide/b_Cisco_NX-OS_Licensing_Guide.html
VLAN、MAC アドレス テーブル、プライベート VLAN、およびスパニング ツリー プロトコル。 『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/layer2/configuration/guide/b_Cisco_Nexus_7000_Series_NX-OS_Layer_2_Switching_Configuration_Guide.html
『*Cisco Nexus 7000 Series NX-OS FabricPath Command Reference*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/fabricpath/command/reference/fp_cmd_book.html
『*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/fabricpath/configuration/guide/b-Cisco-Nexus-7000-Series-NX-OS-FP-Configuration-Guide-6x.html
『Cisco Nexus 7000 Series NX-OS Release Notes』	http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-release-notes-list.html

MIB

MIB	MIB のリンク
• BRIDGE-MIB • IF-MIB • CISCO-IF-EXTENSION-MIB • ETHERLIKE-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

第 5 章

レイヤ 3 インターフェイスの設定

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

レイヤ 3 インターフェイスの機能履歴

この表には、機能の追加や変更によるリリースの更新内容のみが記載されています。

機能名	リリース	機能情報
ポリシー プログラミング中のエラーを表示。	6.2(2)	ポリシープログラミング中にエラーを生成するインターフェイスおよびVLANを表示する show interface status error policy コマンドが追加されました。
インターフェイスから SNMP カウンタをクリア	6.2(2)	インタフェースからSNMP値をクリアするためのオプションを提供するキーワード **snmp** を含めるため **clear counters interface** コマンドが更新されました。
FEX	6.2(2)	Cisco ファブリック エクステンダは、キュー マッピングへのホスト インターフェイス（HIF）および DSCP 上のレイヤ 3 プロトコル隣接関係をサポートします。 （注） Cisco リリース 6.2(2) より前は、ファブリック エクステンダ（FEX）ポートをホスト接続のためのレイヤ 3 インターフェイスとして設定できますが、ルーティング用には設定できません。
サブインターフェースの出力の表示拡張	6.1(1)	**show interface eth** コマンド出力が更新されました。
インターフェイス統計情報の 3 つの設定可能なサンプリング間隔	4.2(1)	load-interval コマンドが追加されました。
レイヤ 3 インターフェイス	4.0(1)	この機能が導入されました。

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 および IPv6 パケットをスタティック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。

共有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することはできません。共有インターフェイスについては、『*Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*』を参照してください。

Cisco NX-OS リリース 6.2(2) 以降のリリースでは、Cisco ファブリック エクステンダがキュー マッピングへのホスト インターフェイス（HIF）および DSCP 上のレイヤ 3 プロトコル隣接関係をサポートします。Cisco リリース 6.2(2) より前は、ファブリック エクステンダ（FEX）ポートをホスト接続のためのレイヤ 3 インターフェイスとして設定できますが、ルーティング用には設定できません。ファブリック エクステンダの詳細については、『Configuring the Cisco Nexus 2000 Series Fabric Extender』を参照してください。ファブリック エクステンダの詳細については、『*Configuring the Cisco Nexus 2000 Series Fabric Extender*』を参照してください。

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。このデフォルト動作を変更するには、CLI セットアップ スクリプトまたは **system default switchport** コマンドを使用します。

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。

Cisco リリース 4.2(1) からスタティック Media Access Control（MAC）アドレスをレイヤ 3 インターフェイスに割り当てられます。デフォルトでは、レイヤ 3 インターフェイスの MAC アドレスは、割り当て先の仮想デバイス コンテキスト（VDC）の MAC アドレスです。MAC アドレスの設定については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

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 チャネルの設定」を参照してください。

ルーテッドインターフェイスおよびサブ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
- 入力バイト数/秒
- 出力バイト数/秒

サブインターフェイス

レイヤ 3 インターフェイスとして設定した親インターフェイスに仮想サブインターフェイスを作成できます。親インターフェイスは物理ポートでもポート チャネルでもかまいません。

親インターフェイスはサブインターフェイスによって複数の仮想インターフェイスに分割されます。これらの仮想インターフェイスに IP アドレスやダイナミック ルーティング プロトコルなど固有のレイヤ 3 パラメータを割り当てることができます。各サブインターフェイスの IP アドレスは、親インターフェイスの他のサブインターフェイスのサブネットとは異なります。

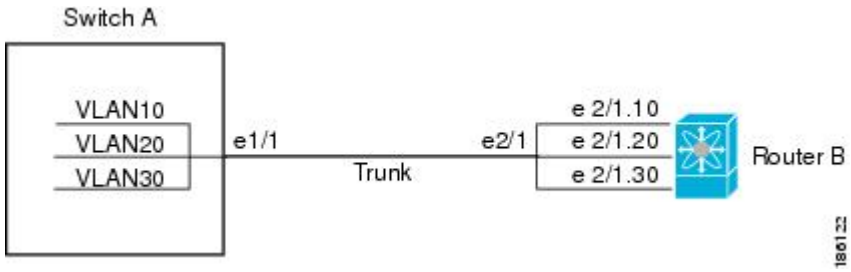
サブインターフェイスの名前は、親インターフェイスの名前（たとえば Ethernet 2/1）+ ピリオド（.）+そのインターフェイス独自の番号です。たとえば、イーサネット インターフェイス 2/1 に Ethernet 2/1.1 というサブインターフェイスを作成できます。この場合、.1 はそのサブインターフェイスを表します。

Cisco NX-OS では、親インターフェイスがイネーブルの場合にサブインターフェイスがイネーブルになります。サブインターフェイスは、親インターフェイスには関係なくシャットダウンできます。親インターフェイスをシャットダウンすると、関連するサブインターフェイスもすべてシャットダウンされます。

サブインターフェイスを使用すると、親インターフェイスがサポートするそれぞれの仮想ローカル エリア ネットワーク（VLAN）に独自のレイヤ 3 インターフェイスを実現できます。この場合、親インターフェイスは別のデバイスのレイヤ 2 トランキング ポートに接続します。サブインターフェイスを設定したら 802.1Q トランキングを使って VLAN ID に関連付けます。

以下の図は、インターフェイス E 2/1 のルータ B に接続するスイッチのトランク ポートを示しています。このインターフェイスには 3 つのサブインターフェイスがあり、トランキング ポートに接続する 3 つの VLAN にそれぞれ関連付けられています。

図 *4* : *VLAN* のサブインターフェイス



VLAN の詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

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イネーブルにすると、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。Cisco NX-OS リリース 4.2 から、システムは機能のディセーブル化の前に自動的にチェックポイントを作成するため、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 7000 Series NX-OS System Management Configuration Guide*』を参照してください。

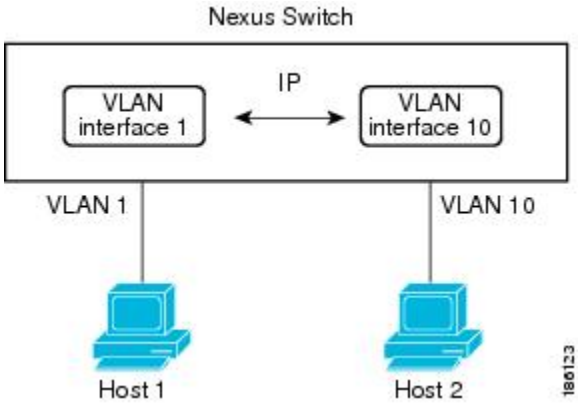
VLAN と同じ VDC に VLAN ネットワーク インターフェイスを設定する必要があります。

（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 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

以下の図は、デバイス上の 2 つの VLAN に接続されている 2 つのホストを示しています。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 *5*：*VLAN* インターフェイスによる *2* つの *VLAN* の接続



（注） シャーシ内に F1 シリーズ モジュールがある Cisco Nexus 7000 シリーズ デバイスでインバンド管理のための VLAN インターフェイスを設定できます。

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。VDC ごとに最大 1024 のループバック インターフェイスが設定できます。VDC には 0 ～ 1023 の番号が付いています。

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。

トンネル インターフェイス

Cisco NX-OS は、IP トンネルとしてトンネル インターフェイスをサポートします。IP トンネルを使うと、同じレイヤまたは上位層プロトコルをカプセル化して、2 台のルータ間で作成されたトンネルを通じて IP の結果を転送できます。IP トンネルの詳細については、「IP トンネルの設定」を参照してください。

レイヤ 3 インターフェイスのハイ アベイラビリティ

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。

ハイ アベイラビリティの詳細については、『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

レイヤ 3 インターフェイスの仮想化サポート

レイヤ 3 インターフェイスは、仮想ルーティング/転送（VRF）インスタンスをサポートします。VRF は仮想化デバイス コンテキスト（VDC）内にあります。特に別の VDC や VRF を設定しない限り、デフォルトでは、Cisco NX-OS のデフォルトの VDC およびデフォルトの VRF が使用されます。ある VDC に設定されたレイヤ 3 論理インターフェイス（VLAN インターフェイス、ループバック）は、同じ番号を持つ別の VDC に設定されたレイヤ 3 論理インターフェイスとは区別されます。たとえば、VDC 1 のループバック 0 は VDC 2 のループバック 0 とは異なります。

VDC ごとに最大 1024 のループバック インターフェイスを設定できます。

このインターフェイスは VRF に関連付けることができます。VLAN インターフェイスの場合、VLAN と同じ VDC に設定する必要があります。

VDC については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を、VRF でのインターフェイスの設定については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

（注） そのインターフェイスに IP アドレスを設定する前に、インターフェイスを VRF に割り当てる必要があります。

インターフェイスのライセンス要件

vPC には、ライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

IP トンネルには Enterprise Services ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『Cisco NX-OS Licensing Guide』を参照してください。

他のインターフェイスにはライセンスが必要ありません。

レイヤ 3 インターフェイスの前提条件

ライセンス 3 インターフェイスには次の前提条件があります。

- VDC を設定する場合は、アドバンスド サービス ライセンスをインストールし、目的の VDC を入力している（『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照）。
- IP アドレッシングおよび基本設定を熟知している。IP アドレッシングについては、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

注意事項と制約事項

レイヤ 3 インターフェイスの設定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 固有の設定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 固有の設定をすべて削除します。
- Cisco Nexus 2000 ファブリック エクステンダは、ポートに接続されたデバイスとのルーティング プロトコルの隣接に参加できません。スタティックな直接ルートだけがサポートされます。この制限事項は、サポートされる接続例両方に適用されます。

- レイヤ 2 モードのファブリック エクステンダ単一ポートまたはポート チャネルを有する SVI。
- レイヤ 3 モードのファブリック エクステンダ ポートまたはポート チャネル。

- レイヤ 3 ルータ インターフェイスおよびサブインターフェイスは、F1 I/O モジュールでは設定できません。
- F2 シリーズ I/O モジュールは VLAN 単位の統計情報はサポートしません。したがって、show interface コマンドは、スイッチ仮想インターフェイス（SVI）の VLAN 単位の Rx/Tx カウンタまたは統計情報を表示しません。

（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。

レイヤ 3 インターフェイスのデフォルト設定

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
管理状態	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。

はじめる前に

正しい VDC を使用していることを確認します（または switchto vdc コマンドを使用します）。

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。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **interface ethernet***slot/port*	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)# **no switchport**	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、このインターフェイス上のレイヤ 2 固有の設定を削除します。
ステップ 4	switch(config-if)# **ip address***ip-address/length* オプション: **ipv6 address** *ipv6-address/length* 説明: このインターフェイスの IPv6 アドレスを設定します。	このインターフェイスの IP アドレスを設定します。IP アドレスおよび IPv6 アドレスの詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。
ステップ 5	switch(config-if)# **show interfaces**	（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	switch# **show interface status error policy** [**detail**]	（任意） ポリシープログラミング中にエラーを生成するインターフェイスおよびVLANが表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ 7	switch# **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	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。

インターフェイス メディアをポイント ツー ポイントまたはブロードキャストのどちらかとして設定するには、medium コマンドを使用します。

コマンド	目的
medium {**broadcast** | **p2p**}	インターフェイス メディアをポイント ツー ポイントまたはブロードキャストのどちらかとして設定します。

デフォルト設定はbroadcastであり、この設定はどのshowコマンドにも表示されません。ただし、**p2p** に設定を変更した場合、**show running-config** コマンドを入力すると、この設定が表示されます。

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換するには、**switchport** コマンドを使用します。

コマンド	目的
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 2/1
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** コマンドを入力します。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。

サブインターフェイスの設定

ルーテッド インターフェイスまたはルーテッド インターフェイスで作成したポート チャネルに 1 つまたは複数のサブインターフェイスを設定できます。

はじめる前に

親インターフェイスをルーテッド インターフェイスとして設定します。

「ルーテッド インターフェイスの設定」の項を参照してください。

このポート チャネル上にサブインターフェイスを作成するには、ポート チャネル インターフェイスを作成します。

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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)# **interface ethernet***slot/port*	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 address***ip-address/length* **オプション**: **ipv6 address** *ipv6-address/length* **説明**: このインターフェイスの IPv6 アドレスを設定します。	このインターフェイスの IP アドレスを設定します。IP アドレスおよび IPv6 アドレスの詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。
ステップ 4	switch(config-if)# **encapsulation dot1q***vlan-id*	サブインターフェイス上の IEEE 802.1Q VLAN カプセル化を設定します。範囲は 2 ～ 4093 です。
ステップ 5	switch(config-if)# **show interfaces**	（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	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。

次に、サブ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 ethernet 2/1.1
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# encapsulation dot1Q 33
switch(config-if)# copy running-config startup-config
```

Cisco NX-OS リリース 6.1 以降では、**show interface eth** コマンドの出力が、次の例に示すように、サブインターフェイスに対し拡張されます。

```
switch# show interface ethernet 1/2.1
Ethernet1/2.1 is down (Parent Interface Admin down)
admin state is down, Dedicated Interface, [parent interface is Ethernet1/2]
Hardware: 40000 Ethernet, address: 0023.ac67.9bc1 (bia 4055.3926.61d4)
Internet Address is 10.10.10.1/24
MTU 1500 bytes, BW 40000000 Kbit, DLY 10 usec
```

```
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation 802.1Q Virtual LAN, Vlan ID 11, medium is broadcast
Auto-mdix is turned off
EtherType is 0x8100
L3 in Switched:
  ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
L3 out Switched:
  ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
```

インターフェイスでの帯域幅の設定

ルーテッドインターフェイス、ポートチャネル、またはサブインターフェイスに帯域幅を設定できます。上位層プロトコルは帯域幅パラメータを使用してパス コストを計算します。サブインターフェイスの帯域幅は、次のいずれかの方法で設定できます。

- 明示的：サブインターフェイスの帯域幅を直接設定します。
- 継承：サブインターフェイスが固有の値として、つまり親インターフェイスの帯域幅を親インターフェイスから継承するように帯域幅を設定します。

サブインターフェイスの帯域幅を設定しない場合、または親インターフェイスの帯域幅を継承しない場合、サブインターフェイスの帯域幅は次の方法で決定されます。

- 親インターフェイスがアップしている場合、サブインターフェイスの帯域幅は親インターフェイスの動作速度と同じです。ポートの場合、サブインターフェイスの帯域幅は設定されているリンク速度またはネゴシエート対象のリンク速度です。ポートチャネルの場合、サブインターフェイスの帯域幅は、ポート チャネルの各メンバのリンク速度の集合です。
- 親インターフェイスがダウンしている場合、サブインターフェイスの帯域幅は親インターフェイスのタイプによって異なります。
  - ポート チャネル サブインターフェイスの場合、サブインターフェイスの帯域幅は 100 Mb/s です。
  - 1 Gb/s イーサネット ポートの場合、サブインターフェイスの帯域幅は 1 Gb/s です。
  - 10 Gb/s イーサネット ポートの場合、サブインターフェイスの帯域幅は 10 Gb/s です。

インターフェイスの帯域幅を設定するには、インターフェイス モードで次のコマンドを使用します。

コマンド	目的
帯域幅	ルーテッド インターフェイス、ポート チャネル、またはサブインターフェイスに帯域幅パラメータを設定します。

親インターフェイスから帯域幅を継承するようにサブインターフェイスを設定するには、インターフェイス モードで次のコマンドを使用します。

コマンド	目的
bandwidth inherit [*value*]	設定された帯域幅の値を継承するように、このインターフェイスのすべてのサブインターフェイスを設定します。値を設定しない場合、サブインターフェイスは親インターフェイスの帯域幅を継承します。指定できる範囲は 1 ～ 10000000（KB 単位）です。

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。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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)#**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	switch(config)# **interface vlan***number*	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	switch(config-if)# **ip address***ip-address/length* オプション：**ipv6 address** *ipv6-address/length* 説明：このインターフェイスの IPv6 アドレスを設定します。	このインターフェイスの IP アドレスを設定します。IP アドレスおよび IPv6 アドレスの詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

	コマンドまたはアクション	目的
ステップ 5	switch(config-if)# **show interface vlan***number*	（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	switch(config-if)# **show interface status error policy** [**detail**]	（任意） ポリシー プログラミング中にエラーを生成するインターフェイスおよびVLANが表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ 7	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	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。

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
```

Nexus シャーシでのインバンド管理の設定

シャーシ内に F1 シリーズ モジュールのみがある場合に、Cisco Nexus 7000 シリーズ デバイスでインバンド管理のための VLAN インターフェイスを設定できます。

注意 F1 シリーズ モジュールのインバンド管理には専用の VLAN を使用することを推奨します。インバンド管理に使用している VLAN 上でデータ トラフィックを実行しないでください。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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)#**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	switch(config)# **interface vlan***number*	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	switch(config-if)# **no shutdown**	インターフェイスを管理上のアップ状態にします（インターフェイスをイネーブルまたはディセーブルにします）。
ステップ 5	switch(config-if)# **management**	VLAN インターフェイスの IP アドレスへのインバンド管理アクセスを許可します。
ステップ 6	switch(config-if)# **ip address***ip-address/length*	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 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。
ステップ 7	switch(config-if)# **show interface vlan***number*	（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 8	switch(config-if)# **show interface status error policy** [**detail**]	（任意） ポリシープログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ 9	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 10	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。

次に、Cisco Nexus 7000 シャーシでインバンド管理を作成する例を示します。

```
switch# configure terminal
switch(config)# feature interface-vlan
switch(config)# interface vlan 5
switch(config-if)# no shutdown
switch(config-if)# management
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# copy running-config startup-config
```

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。

はじめる前に

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。

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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)# **interface loopback***instance*	ループバック インターフェイスを作成します。範囲は 0 ～ 1023 です。
ステップ 3	switch(config-if)# **ip address***ip-address/length* **オプション**：**ipv6 address***ipv6-address/length* **説明**：このインターフェイスの IPv6 アドレスを設定します。	このインターフェイスの IP アドレスを設定します。IP アドレスおよび IPv6 アドレスの詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

	コマンドまたはアクション	目的
ステップ 4	switch(config-if)# **show interfaces loopback***instance*	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	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。

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 192.0.2.100/8
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。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

VRF 用のインターフェイスを設定した後で、トンネル インターフェイスに IP アドレスを割り当てます。

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)# **interface***interface-type number*	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)# **vrf member** *vrf-name*	このインターフェイスを VRF に追加します。
ステップ 4	switch(config-if)# **ip address***ip-address/length*	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 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

	コマンドまたはアクション	目的
ステップ 5	switch(config-if)# **show vrf** [*vrf-name*] **interface***interface-type number*	（任意） VRF 情報を表示します。
ステップ 6	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。

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
```

レイヤ 3 インターフェイス設定の確認

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 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 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***private-vlan mapping**	VLAN インターフェイスのプライベート VLAN 情報を表示します。
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 interface status error policy [**detail**]	ハードウェア ポリシーと矛盾するインターフェイスおよび VLAN のエラーを表示します。 **detail** コマンドを使用すると、エラーを受信するインターフェイスおよび VLAN の詳細を表示できます。

レイヤ 3 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
load- interval {**interval***seconds* {**1** | **2** | **3**}}	Cisco Nexus 7000 シリーズ デバイスの Cisco NX-OS Release 4.2(1) から、3 種類のサンプリング間隔をビットレートおよびパケットレートの統計情報に設定します。VLAN ネットワーク インターフェイスでの範囲は 60 ～ 300 秒であり、レイヤ インターフェイスでの範囲は 30 ～ 300 秒です。
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*slot/port***counters 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*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*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 ethernet*slot/port.number***counters**	サブインターフェイスの統計情報（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。
show interface port-channel*channel-id.number***counters**	ポート チャネル サブインターフェイスの統計情報（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。
show interface loopback*number***counters**	ループバック インターフェイスの入力および出力カウンタ（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。

コマンド	目的
show interface loopback*number***counters 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 loopback*number***counters errors**	ループバック 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 vlan*number***counters**	VLAN インターフェイスの入力および出力カウンタ（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。
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。

これらのコマンドについては、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』を参照してください。

関連資料

関連項目	マニュアル タイトル
『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/interfaces/command/reference/if_cmds.html
『*Interfaces Configuration Guide, Cisco DCNM for LAN*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/dcnm/interfaces/configuration/guide/if_dcnm.html
『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/system_management/configuration/guide/sm_nx_os_cg.html
『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/high_availability/configuration/guide/b_Cisco_Nexus_7000_Series_NX-OS_High_Availability_and_Redundancy_Guide.html

関連項目	マニュアル タイトル
『*Cisco Nexus 2000 Series NX-OS Fabric Extender Software Configuration Guide for Cisco Nexus 7000 Series Switches, Release 6.x*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus2000/sw/configuration/guide/rel_6_1/b_Cisco_Nexus_2000_Series_NX-OS_Fabric_Extender_Software_Configuration_Guide_Release_6-x.html
『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/virtual_device_context/configuration/guide/b-7k-Cisco-Nexus-7000-Series-NX-OS-Virtual-Device-Context-Configuration-Guide.html
『*Cisco NX-OS Licensing Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/licensing/guide/b_Cisco_NX-OS_Licensing_Guide.html
VLAN、MAC アドレス テーブル、プライベート VLAN、およびスパニング ツリー プロトコル。 『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/layer2/configuration/guide/b_Cisco_Nexus_7000_Series_NX-OS_Layer_2_Switching_Configuration_Guide.html
『*Cisco Nexus 7000 Series NX-OS FabricPath Command Reference*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/fabricpath/command/reference/fp_cmd_book.html
『*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/fabricpath/configuration/guide/b-Cisco-Nexus-7000-Series-NX-OS-FP-Configuration-Guide-6x.html
『Cisco Nexus 7000 Series NX-OS Release Notes』	http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-release-notes-list.html

MIB

MIB	MIB のリンク
• IF-MIB • CISCO-IF-EXTENSION-MIB • ETHERLIKE-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

第 6 章

双方向フォワーディング検出の設定

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

BFD の機能の履歴

この表には、機能の追加や変更によるリリースの更新内容のみが記載されています。

表 *12*：基本インターフェイス パラメータ設定の機能履歴

機能名	リリース	機能情報
M3 上の BFD FSA オフロード	7.3(0)DX(1)	M3 ライン カード上の BFD FSA オフロードに対するサポートが追加されました。
HSRPv6 に対する BFD サポート	7.3(0)D1(1)	HSRPv6 上の BFD に対するサポートが追加されました。
リンク単位の効率化に対処するための BFD 拡張機能	7.3(0)D1(1)	BFD アドレス リンク単位効率化に対する拡張機能として、すべての LAG メンバー インターフェイス上で個別の BFD セッションを設定するためのサポートが追加されました。
アンナンバード インターフェイス上の BFD	7.2(1)D1(1)	アンナンバード インターフェイス上で BFD を設定するためのサポートが追加されました。
F3 上の BFD FSA オフロード	7.2(1)D1(1)	F3 ライン カード上の BFD ACP オフロードに対するサポートが追加されました。
FabricPath コア上のレイヤ 2 経由の BFD に対するサポート	7.2(0)D1(1)	FabricPath コア上のレイヤ 2 経由の BFD に対するサポートが追加されました。
Fabricbath コア上の SVI 経由の BFD に対するサポート	7.2(0)D1(1)	Fabricbath コア上の SVI 経由の BFD に対するサポートが追加されました。
IPv6 スタティック ルートでの BFD	6.2(2a)	インターフェイス上のすべての IPv6 スタティック ルートで BFD を設定するためのサポートが追加されました。
BFD 相互運用性	6.2(2)	Cisco NX-OS ソフトウェアおよび Cisco IOS ソフトウェアで BFD 相互運用性を設定するためのサポートが追加されました。
IPv6 での BFD	6.2(2)	IPv6 での BFD のサポートが追加されました。
OSPFv3 での BFD	6.2(2)	OPSPv3 での BFD のサポートが追加されました。

機能名	リリース	機能情報
IS-ISv6 での BFD	6.2(2)	IS-ISv6 での BFD のサポートが追加されました。
M2 および F2 モジュール上での BFD	6.1(1)	M2 および F2 モジュールのサポートに関する注記が追加されました。
BFD 認証	5.2(1)	キー付き SHA-1 認証は BFD パケットでサポートされます。
VRRP 用 BFD	5.2(1)	VRRP の BFD のサポートが追加されました。
BFD	5.0(2)	この機能が導入されました。

BFD に関する情報

BFDは、メディアタイプ、カプセル化、トポロジ、およびルーティングプロトコルの転送パス障害を高速で検出するように設計された検出プロトコルです。BFD を使用することで、さまざまなプロトコルの Hello メカニズムにより、変動速度ではなく一定速度で転送パス障害を検出できます。BFD はプロファイリングおよびプランニングを簡単にし、再コンバージェンス時間の一貫性を保ち、予測可能にします。

BFD は 2 台の隣接デバイス間のサブセカンド障害を検出し、BFD の負荷の一部を、サポートされるモジュール上のデータ プレーンに分散できるため、プロトコル hello メッセージよりも CPU を使いません。

非同期モード

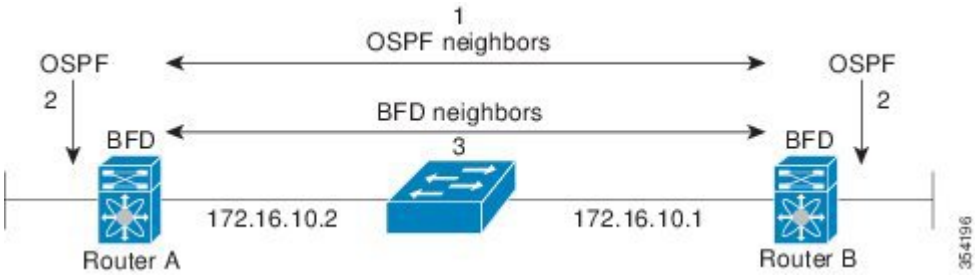
Cisco NX-OS は、BFD 非同期モードをサポートします。BFD 非同期モードでは、2 個の隣接するデバイス間で BFD 制御パケットが送信され、デバイス間の BFD ネイバー セッションがアクティベートされ、維持されます。両方のデバイス（または BFD ネイバー）で BFD を設定できます。インターフェイスおよび適切なプロトコルで一度 BFD がイネーブルになると、Cisco NX-OS は BFD セッションを作成し、BFD セッション パラメータをネゴシエートし、BFD 制御パケットをネゴシエートされた間隔で各 BFD ネイバーに送信し始めます。BFD セッション パラメータは、次のとおりです。

- 目的の最小送信間隔：このデバイスが BFD Hello メッセージを送信する間隔。
- 必要最小受信間隔：このデバイスが別の BFD デバイスからの BFD Hello メッセージを受け付ける最小間隔。

- 検出乗数：転送パスの障害を検出するまでに喪失した、別の BFD デバイスからの BFD Hello メッセージの数。

以下の図に、BFDセッションがどのように確立されているかを示します。この図は、OSPF と BFD を実行する 2 台のルータがある単純なネットワークを示します。OSPF がネイバーを検出すると（1）、OSPF 隣接ルータで BFD ネイバー セッションを開始する要求が、ローカル BFD プロセスに送信されます（2）。OSPF ネイバー ルータとの BFD ネイバー セッションが確立されました（3）。

図 *6*： *BFD* ネイバー関係の確立



障害検出

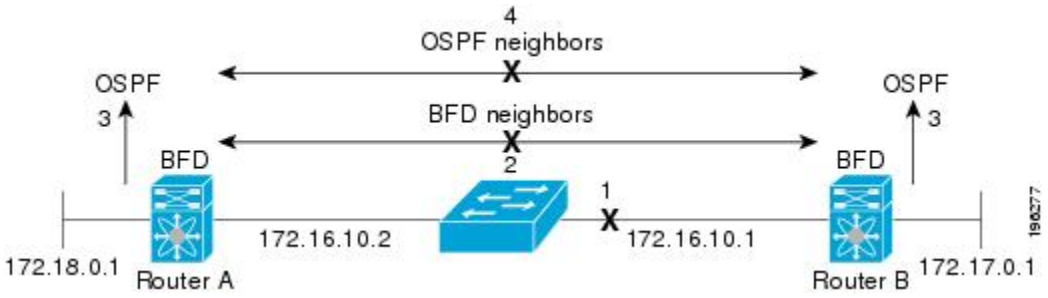
一度 BFD セッションが確立され、タイマー ネゴシエーションが終了すると、BFD ネイバーは、より速い速度の場合を除き IGP Hello プロトコルと同じ動作をする BFD 制御パケットを送信し、活性度を検出します。BFD は障害を検出しますが、プロトコルが障害の発生したピアをバイパスするための処置を行う必要があります。

BFDは転送パスに障害を検出したとき、障害検出通知をBFD対応プロトコルに送信します。ローカル デバイスは、プロトコル再計算プロセスを開始してネットワーク全体の収束時間を削減できます。

以下の図に、ネットワークで障害が発生した場合を示します（1）。OSPF ネイバー ルータでの BFD ネイバー セッションが停止されます（2）。BFD はローカル OSPF プロセスに BFD ネイバーに接続できなくなったことを通知します（3）。ローカル OSPF プロセスは OSPF ネイバー関係を解除します（4）。代替パスが使用可能な場合、ルータはただちにそのパスでコンバージェンスを開始します。

（注） BFD 障害検出は 1 秒未満で行われます。これは OSPF Hello メッセージが同じ障害を検出するより高速です。

図 *7*：***OSPF*** ネイバー関係の解除



分散型動作

Cisco NX-OS は、BFD をサポートする互換性のあるモジュールへ BDF 動作を配布できます。このプロセスで、BFD パケット処理の CPU の負荷を、BFD ネイバーに接続された各モジュールへオフロードします。すべての BFD セッションはモジュール CPU 上で行われます。BFD 障害が検出されたときに、モジュールはスーパーバイザに通知します。

BFD エコー機能

BFD エコー機能は、転送エンジンからリモート BFD ネイバーにエコー パケットを送信します。BFD ネイバーは検出を実行するために同じパスに沿ってエコーパケットを返送します。BFD ネイバーは、エコー パケットの実際の転送に参加しません。エコー機能および転送エンジンが検出の処理を行います。BFD はエコー機能がイネーブルになっている場合に非同期セッションの速度を低下させ、2 台の BFD ネイバー間で送信される BFD 制御パケット数を減らすために、slow timer を使用できます。また、転送エンジンは、リモート システムを含めないでリモート（ネイバー）システムの転送パスをテストするので、パケット間遅延の変動が少なくなり、障害検出時間が短縮されます。

BFD ネイバーの両方がエコー機能を実行している場合、エコー機能には非対称性がありません。

（注） ユニキャスト リバース パス転送チェック（uRPF）はデフォルトではディセーブルです。これを BFD のあるインターフェイス機能でイネーブルにする必要がある場合は、BFD エコー機能がディセーブルになっている必要があります。

セキュリティ

Cisco NX-OS は BFD パケットを隣接する BFD ピアから受信したことを確認するためにパケットの存続可能時間（TTL）値を使用します。すべての非同期およびエコー要求パケットの場合、BFD ネイバーは TTL 値を 255 に設定し、ローカル BFD プロセスは着信パケットを処理する前に TTL 値を 255 として確認します。エコー応答パケットの場合、BFD は TTL 値を 254 に設定します。

Cisco NX-OS リリース 5.2 以降では、BFD パケットの SHA-1 認証を設定できます。

ハイ アベイラビリティ

BFD は、ステートレス リスタートと In-Service Software Upgrade（ISSU）をサポートします。ISSU を使用すると、転送に影響を与えることなく、ソフトウェアをアップグレードできます。リブートまたはスーパーバイザ スイッチオーバー後に、Cisco NX-OS が実行コンフィギュレーションを適用し、BFD がただちに制御パケットを BFD ピアに送信します。

仮想化のサポート

BFD は、仮想ルーティングおよび転送（VRF）インスタンスをサポートしています。VRF は仮想化デバイス コンテキスト（VDC）内にあります。特に別の VDC や VRF を設定しない限り、デフォルトでは、Cisco NX-OS のデフォルトの VDC およびデフォルトの VRF が使用されます。詳細については、『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide』を参照してください。

BFD 相互運用性

この機能は、Cisco IOS ソフトウェア、Cisco NX-OS ソフトウェアおよび Cisco IOS XR ソフトウェア間の BFD 相互運用性を実現します。

F3 ライン カードおよび M3 ライン カード上の BFD ACP オフロード

F3 ライン カード上の BFD ファブリック サービス アクセラレータ（FSA）オフロードを使用すれば、F3 ライン カード上のネットワーク プロセッサ ユニットに対する非同期およびエコー BFD 送信（Tx）および受信（Rx）のオフロードを実現できます。F3 ライン カード上の BFD FSA オフロード機能は、ルーティング テーブルを再計算するために迅速な障害検出パケットまたはメッセージをルーティング プロトコルに送信することにより、スケールを改善し、ネットワーク全体の収束時間を短縮します。**bfd hw-offload-module module-name** コマンドを使用して、各 VDC の F3 ライン カード上の BFD FSA オフロードを明示的に有効にする必要があります。この機能を無効にするには、**no bfd hw-offload-module module-name** コマンドを使用します。この機能は、その特定の VDC 内のライン カード上でホストされているアクティブな BFD セッションが存在しない場合にのみ有効にできます。

BFD FSA オフロード機能は、Cisco Nexus 7000 シリーズ リリース 7.3(0)DX(1) の M3 ライン カードで導入されます。

FSA への BFD セッションのオフロードは、F3 ライン カード上ではデフォルトで無効になっており、M3 ライン カード上ではデフォルトで有効になっています。セッションが FSA にオフロードされた場合は、BFD セッションが 15 ms で動作できます。

アンナンバード インターフェイス上の BFD

シスコ ユニファイド ファブリックは、相互接続を備えた 1024 個のリーフからなる 32 個のスパインをサポートする必要があります。32 スパイン Vinci Fabric では、1 つのリーフに 32 個のレイヤ 3 リンク（スパインごとに 1 つずつ）が割り当てられます。同様に、各スピネットに 1024 個のレイヤ 3 リンク（リーフごとに 1 つずつ）が割り当てられます。通常、スパインとリーフ上の各レイヤ 3 リンクには同数の IP アドレスが必要なため、割り当てと管理が複雑になります。この複雑さを軽減するために、これらのリンク 3 レイヤは指定されたループバック インターフェイスから IP アドレスを抽出します。このようなレイヤ 3 リンクは「アンナンバード リンク」と呼ばれます。これらのレイヤ 3 アンナバード リンクは、それぞれのルータの MAC アドレスに関連付けられます。BFD がこれらのリンク上の迅速な障害検出に使用されます。これには、アンナンバード インターフェイス経由の BFD に対するサポートが不可欠です。

OSPF プロトコルと IS-IS プロトコルのどちらかを使用して、スパインとリーフ間のレイヤ 3 接続を提供することができます。

次の BFD サブ機能がアンナンバード インターフェイス上で適用されます。

- **アドレス ファミリのサポート**

  BFD クライアントは、IPv4 アドレスまたは IPv6 アドレスのいずれかを使用して BFD をブートストラップすることができます。

- **エコーのサポート**

  デフォルトで、エコー機能が IPv4 BFD セッションと IPv6 BFD セッションの両方でサポートされます。ただし、BFD IPv6 セッションがリンクローカル アドレスを使用してブートストラップされた場合は、エコーはサポートされません。

- **アンナンバード ポート チャネル経由の BFD セッション**

  論理モード セッションとリンク単位モード セッションの両方がサポートされます。デフォルトで、ポート チャネル上の設定なしで、BFD セッションが論理モードになります。

次の設定は、アンナンバード インターフェイスでサポートされません。

- スイッチ仮想インターフェイス（SVI）は、アンナンバードと見なされません。
- スパインとリーフの同じセット間のマルチパス リンクはサポートされません。
- サブ インターフェイスはアンナンバードと見なされないため、サブ インターフェイスの最適化はサポートされません。

リンク単位の効率化に対処するための BFD 拡張機能

リンク単位の効率化機能に対処するための双方向転送（BFD）拡張機能を使用すれば、すべてのリンク集約グループ（LAG）メンバーインターフェイス（RFC 7130 で規定されている）上で個別の BFD セッションを設定することができます。

この拡張機能により、BFD セッションはポート チャネルの各メンバー リンク上で動作します。BFD がリンク障害を検出すると、そのメンバー リンクが転送テーブルから削除されます。BFD セッションは個別のポートチャネルインターフェイス上で作成されるため、このメカニズムが迅速な障害検出を可能にします。

ユーザは、メイン ポート チャネル インターフェイス経由で RFC 7130 BFD を設定できます。このインターフェイスでは、メンバーごとに 1 つずつのマイクロ BFD セッションを使用することによる LAG 経由の帯域幅モニタリングが実行されます。メンバー ポートのいずれかがダウンすると、そのポートが転送テーブルから削除されます。これにより、そのメンバー上のトラフィックのブラックホール化が回避されます。

マイクロ BFD セッションは、LACP ベースのポート チャネルと非 LACP ベースのポート チャネルの両方でサポートされます（ポート チャネルのメンバー リンク上で動作する BFD セッションは「マイクロ BFD セッション」と呼ばれます）。

マイクロ BFD セッションの設定方法の詳細については、「マイクロ *BFD* セッションの設定」のトピックを参照してください。

インターフェイスのライセンス要件

vPC には、ライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

IP トンネルには Enterprise Services ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『Cisco NX-OS Licensing Guide』を参照してください。

他のインターフェイスにはライセンスが必要ありません。

BFD の前提条件

BFD には、次の前提条件があります。

- BFD 機能をイネーブルにする必要があります。
- BFD をイネーブルにする任意のクライアント プロトコルでは、そのクライアント プロトコルの BFD をイネーブルにします。
- BFD 対応インターフェイスでインターネット制御メッセージ プロトコル（ICMP）リダイレクト メッセージをディセーブルにします。

- デフォルト VDC の同一 IP の送信元および宛先アドレスの IP パケット検証チェックをディセーブルにします。
- 設定作業とともに一覧表示されているその他の詳細な前提条件を参照してください。
- Cisco NX-OS リリース 6.2(2) 以降では、IPv6 の BFD がサポートされます。
- BFD の Intermediate System-to-Intermediate System（IS-IS）IPv6 クライアントを設定するには、IS-IS がすべてのルータで実行している必要があります。さらに、BFD セッションの基本パラメータは BFD ネイバーに対して BFD セッションを実行するインターフェイス上で設定する必要があります。
- Cisco IOS ソフトウェア、Cisco NX-OS ソフトウェア、および Cisco IOS XR ソフトウェアの間で BFD の相互運用性をイネーブルにするには、エコー モードで BFD を使用します。さらに、BFD の一部であるすべてのインターフェイス、およびピア デバイスでも **no ip redirect** コマンドを設定します。

注意事項と制約事項

BFD 設定時の注意事項と制約事項は次のとおりです。

- BFD は BFD バージョン 1 をサポートします。
- Cisco NX-OS リリース 6.2(2) 以降のリリースでは、BFD は IPv4 と IPv6 をサポートします。
- BFD は、インターフェイスごとのアドレス ファミリ（IPv4 または IPv6）1 つにつき 1 セッションだけサポートします。
- BFD は、シングルホップ BFD をサポートします。
- ボーダー ゲートウェイ プロトコル（BGP）の BFD は、シングルホップ External BGP（EBGP）および Internal BGP（iBGP）ピアをサポートしています。
- BFD は、Cisco NX-OS リリース 5.2 以降ではキー付き SHA-1 認証をサポートします。
- BFD は、次のレイヤ 3 インターフェイスをサポートします。物理インターフェイス、ポートチャネル、サブインターフェイス、および VLAN インターフェイス。
- BFD はレイヤ 3 隣接情報に応じて、レイヤ 2 のトポロジ変更を含むトポロジ変更を検出します。レイヤ 3 隣接情報が使用できない場合、VLAN インターフェイス（SVI）の BFD セッションはレイヤ 2 トポロジのコンバージェンス後に稼働しない可能性があります。
- BFD は、単一のインターフェイス上の同一サブネット内の複数の IPv6 ネクスト ホップのモニタリングをサポートしていません。
- 2 台のデバイス間のスタティック ルート上の BFD については、両方のデバイスが BFD をサポートする必要があります。デバイスの一方または両方が BFD をサポートしていない場合、スタティック ルートはルーティング情報ベース（RIB）でプログラミングされません。
- BFD は、BFD マルチホップをサポートしません。iBGP 用に BFD を設定する場合は、接続先のインターフェイスで BGP ネイバーの **update-source** コマンドを設定する必要があります。

- ポート チャネル設定の制限事項
  - BFD で使用されるレイヤ 3 ポート チャネルでは、ポート チャネルの LACP をイネーブルにする必要があります。BFD リンク単位は、EIGRP、ISIS、および OSPF クライアントでのみサポートされます。

    （注） ポート チャネル上で BFD リンク単位を設定するには、インターフェイスをシャットダウンして、リンク単位を設定してから、再度、ポート チャネルを起動する必要があります。

  - SVI のセッションで使用されるレイヤ 2 ポート チャネルでは、ポート チャネルの LACP をイネーブルにする必要があります。

- SVI の制限事項
  - ASIC リセットにより他のポートのトラフィックが中断されます。このイベントは、その他のポートの SVI セッションがフラップする原因になることがあります。ASIC がリセットする既存のトリガーには、VDC をリロードしている VDC 間のポート移動があります。また、キャリア インターフェイスが仮想ポート チャネル（vPC）の場合、BFD は SVI インターフェイスではサポートされません。
  - トポロジを変更すると（たとえば、VLAN へのリンクの追加または削除、レイヤ 2 ポート チャネルからのメンバの削除など）、SVI セッションが影響を受ける場合があります。SVIセッションはダウンした後、トポロジディスカバリの終了後に起動する場合があります。

    （注） SVIのセッションがフラップしないようにし、トポロジを変更する必要がある場合は、変更を加える前に BFD 機能をディセーブルにして、変更後、BFD を再度イネーブルにできます。また、大きな値（たとえば、5秒）になるように BFD タイマーを設定し、上記のイベントの完了後に高速なタイマーに戻すこともできます。

- N7K-F132XL-15 モジュール上でのみメンバー ポートがある VLAN インターフェイスを通した BFD はサポートされません。N7K-F132XL-15 モジュール上でのみメンバー ポートを持ついずれかの VLAN を通した BFD をディセーブルにする必要があります。

  （注） （たとえば、OSPF から）ルータ レベルで BFD をイネーブルにすると、N7K-F132XL-15 ラインカードを通した BFD セッションは発生しません。OSPF などのルーティング プロトコルについては、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

- 分散レイヤ 3 ポート チャネルで BFD エコー機能を設定した場合、メンバー モジュールをリロードすると、そのモジュールでホストされた BFD セッションがフラップされ、そのためパケット損失が発生します。
- レイヤ 2 スイッチを間に入れずに BFD ピアを直接接続する場合、代替策として BFD per-link を使用できます。

（注） BFD per-link モードとサブインターフェイス最適化をレイヤ 3 ポート チャネルで同時に使用することはサポートされていません。

- BFD エコー機能は、IPv6 リンクローカル アドレスを使用する場合、サポートされません。
- IPv4 と IPv6 上の HSRP が BFD でサポートされます。
-
- HSRP BFD ALL-INTERFACE が設定されている場合は、すべてのインターフェイス上のすべての IPv4 および IPv6 HSRP グループが自動的に BFD をサポートします。
- BFD は、エニーキャスト HSRP ではサポートされません。
- サポートされている Cisco NX-OS デバイスのラインカードによって生成される BFD パケットは COS 6/DSCP CS6 とともに送信されます。BFD パケットの DSCP/COS 値は、ユーザが設定可能な値ではありません。
- BFD アドレス リンク単位の制限：
  - BFD セッションを実行している 2 台のスイッチ（ピア デバイス）間で直接接続されたポート チャネル インターフェイスでのみサポートします。
  - On モードと LACP モードの両方でレイヤ 3 ポート チャネル インターフェイスをサポートします。
  - レイヤ 3 機能を備えたすべてのライン カードをサポートします。
  - IPv6 はサポートされていません。
  - ファブリック ポート チャネルはサポートされません。
  - vPC はサポートされていません。
  - ポート チャネル経由の仮想スイッチ インターフェイスはサポートされません。
  - ストレージ VDC はサポートされません。
  - エコー機能は、マイクロ BFD セッションではサポートされません。
  - RFC 7130 リンクは、独自のリンクおよび BFD 論理リンクとともに設定できません。
  - RFC 7130 がメイン ポート チャネル インターフェイス上で設定され、論理 BFD がサブインターフェイス上で設定されている場合は、論理 BFD セッションのアグレッシブ タイマーを RFC 7130 BFD セッションより短くする必要があります。

- マイクロ BFD セッションは、ポート チャネル サブインターフェイスではサポートされません。
- FEX インターフェイス（HIF）ポートはサポートされません。
- IEFT-BFD がポート チャネル インターフェイス上で有効になっている場合は、ポート チャネルの動作状態は、セッションを確立可能な最小のマイクロ BFD セッション メンバーに依存します。ポートチャネルをアップにするために必要なリンクの最小数が満たされていない場合は、ポート チャネル インターフェイスがダウンします。その結果、ポート チャネル サブインターフェイスと論理 BFD セッションもダウンします。
- LACP ポート チャネルのメンバーがホット スタンバイ状態で、アクティブ リンクの 1 つで BFD 障害が発生した場合は、ホット スタンバイ リンクが直接起動しない可能性があります。BFD 障害が発生したアクティブ リンクがダウンすると、ホット スタンバイ メンバーがアクティブになります。このシナリオでは、ホットスタンバイが起動する前にポート チャネルがダウンする可能性があります。
- BFD リンク単位は、BFD ではサポートされません。これは、EIGRP、OSPF、および ISIS でのみサポートされます。

デフォルト設定

表 *13*：デフォルトの *BFD* パラメータ

パラメータ	デフォルト
BFD 機能	ディセーブル
必要最小受信間隔	50 ミリ秒
目的の最小送信間隔	50 ミリ秒
検出乗数	3
エコー機能	イネーブル
モード	非同期
ポート チャネル	論理モード（送信元/宛先ペアのアドレスごとに 1 セッション）。
slow timer	2000 ミリ秒
サブインターフェイスの最適化	ディセーブル

BFD の設定

設定階層

グローバル レベル、およびインターフェイスまたはサブインターフェイス レベルで BFD を設定できます（物理インターフェイスとポート チャネルの場合）。インターフェイスまたはサブインターフェイスの設定はグローバル設定よりも優先されます。サポートされているインターフェイス上で、サブインターフェイス レベルの設定は、サブインターフェイスの最適化がイネーブルになっていない限りインターフェイスまたはポート チャネル設定よりも優先されます。詳細については、「サブインターフェイスの BFD の最適化」の項を参照してください。

（注） BFD per-link モードとサブインターフェイス最適化をレイヤ 3 ポート チャネルで同時に使用することはサポートされていません。

ポート チャネルのメンバである物理ポートについては、メンバ ポートはマスター ポート チャネルの BFD 設定を継承します。メンバ ポート サブインターフェイスは、サブインターフェイスの最適化がイネーブルになっていない限りマスター ポート チャネルの BFD 設定より優先することができます。

BFD 設定のタスク フロー

BFD の設定には、次の作業を行います。

ステップ 1： BFD 機能の有効化, （141 ページ）

ステップ 2：グローバルな BFD パラメータの設定, （142 ページ）またはインターフェイスでの BFD の設定, （144 ページ）

ステップ 3： IPv6 用の BFD の設定, （149 ページ）

BFD 機能の有効化

デバイス VDC 内のインターフェイスおよびプロトコルで BFD を設定する前に、BFD 機能をイネーブルにする必要があります。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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)# **feature bfd**	BFD 機能をイネーブルにします。
ステップ 3	switch(config)# **show feature | include bfd**	（任意） イネーブルおよびディセーブルにされた機能を表示します。
ステップ 4	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。

no feature bfd コマンドを使用して、BFD 機能をディセーブルにし、関連するコンフィギュレーションをすべて削除します。

コマンド	目的
no feature bfd	BFD機能をディセーブルにして、関連するすべての設定を削除します。

グローバルな BFD パラメータの設定

デバイスのすべての BFD セッションの BFD セッション パラメータを設定できます。BFD セッション パラメータは、スリーウェイ ハンドシェイクの BFD ピア間でネゴシエートされます。

インターフェイスでこれらのグローバルなセッション パラメータを上書きするには、「インターフェイスでの BFD の設定」を参照してください。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

BFD 機能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	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)# **bfd interval***mintx***min_rx***msec***multiplier***value*	デバイスのすべての BFD セッションの BFD セッション パラメータを設定します。インターフェイスで BFD セッション パラメータを設定することにより、このコマンドでこれらの値を無効にすることができます。*mintx* および *msec* の範囲は 15 ～ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ～ 50 です。乗数のデフォルトは 3 です。 （注） *mintx* 引数の値が 15 ミリ秒に設定されていたとしても、セッション上で **bfd hw-offload-module** コマンドが有効になっていない場合は、設定は適用されず、セッションがデフォルト タイマー値の 50 ミリ秒で機能します。
ステップ 3	switch(config)# **bfd slow-timer** [*interval*]	エコー機能で使用される slow timer を設定します。この値はエコー機能がイネーブルの場合、BFD が新しいセッションを開始する速度および非同期セッションが BFD 制御パケットに使用する速度を決定します。slow-timer 値は新しい制御パケット間隔として使用されますが、エコー パケットは設定された BFD 間隔を使用します。エコー パケットはリンク障害検出に使用されますが、低速の制御パケットは BFD セッションを維持します。指定できる範囲は 1000 ～ 30000 ミリ秒です。デフォルトは 2000 です。
ステップ 4	switch(config-if)# **bfd echo-interface loopback***interface number*	双方向フォワーディング検出（BFD）のエコー フレームに使用するインターフェイスを設定します。このコマンドは、指定されたループバック インターフェイスで設定されるアドレスに、エコー パケットの送信元アドレスを変更します。指定できるインターフェイス番号の範囲は 0 ～ 1023 です。
ステップ 5	switch(config)# **show running-config bfd**	（任意） BFD の実行コンフィギュレーションを表示します。

	コマンドまたはアクション	目的
ステップ 6	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。

インターフェイスでの BFD の設定

インターフェイスのすべてのBFDセッションのBFDセッションパラメータを設定できます。BFDセッションパラメータは、スリーウェイ ハンドシェイクのBFD ピア間でネゴシエートされます。

この設定は、設定されたインターフェイスのグローバル セッション パラメータより優先されます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

BFD 機能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	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***int-if*	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。**?** 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。
ステップ 3	switch(config)# **bfd interval***mintx***min_rx***msec***multiplier***value*	デバイスのすべての BFD セッションの BFD セッション パラメータを設定します。インターフェイスで BFD セッション パラメータを設定することにより、このコマンドでこれらの値を無効にすることができます。*mintx* および *msec* の範囲は 15 ～ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ～ 50 です。乗数のデフォルトは 3 です。

	コマンドまたはアクション	目的
		（注） *mintx* 引数の値が 15 ミリ秒に設定されていたとしても、セッション上で **bfd hw-offload-module** コマンドが有効になっていない場合は、設定は適用されず、セッションがデフォルト タイマー値の 50 ミリ秒で機能します。
ステップ 4	switch(config-if)# **bfd authentication keyed-sha1 keyid***id***key***ascii_key*	（任意） インターフェイスですべての BFD セッションの SHA-1 認証を設定します。ascii_key 文字列は BFD ピア間で共有する秘密キーです。id 値は、0 ～ 255 の数字で、この特定の ascii_key に割り当てられます。BFDパケットは、複数のアクティブ キーでの使用が許可されている id でキーを指定します。 インターフェイスの SHA-1 認証をディセーブルにするには、コマンドの **no** 形式を使用します。
ステップ 5	switch(config-if)# **show running-config bfd**	（任意） BFDの実行コンフィギュレーションを表示します。
ステップ 6	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。

ポート チャネルの BFD の設定

ポート チャネルのすべての BFD セッションの BFD セッション パラメータを設定できます。パーリンク モードがレイヤ 3 ポート チャネルに使用される場合、BFD により、ポート チャネルの各リンクのセッションが作成され、集約結果がクライアント プロトコルへ提供されます。たとえば、ポート チャネルの 1 つのリンクの BFD セッションが稼働している場合、OSPF などのクライアント プロトコルにポート チャネルが稼働していることが通知されます。BFD セッション パラメータは、スリーウェイ ハンドシェイクの BFD ピア間でネゴシエートされます。

この設定は、設定されたポートチャネルのグローバルセッションパラメータより優先されます。ポート チャネルのメンバ ポートはメンバ ポートのサブインターフェイス レベルで BFD パラメータを設定しない限り、ポート チャネルの BFD セッション パラメータを継承します。その場合、サブインターフェイス最適化がイネーブルにされていなければ、メンバポートサブインターフェ

イスはサブインターフェイス BFD コンフィギュレーションを使用します。詳細については、「サブインターフェイスの BFD の最適化」の項を参照してください。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

BFD 機能をイネーブルにします。

BFD をイネーブルにする前に、ポート チャネルの Link Aggregation Control Protocol（LACP）がイネーブルにされ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	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 port-channel***number*	ポート チャネル コンフィギュレーション モードを開始します。**?** キーワードを使用して、サポートされる数値の範囲を表示します。
ステップ 3	switch(config-if)# **bfd per-link**	ポート チャネルのリンクごとに BFD セッションを設定します。
ステップ 4	switch(config-if)# **bfd interval***mintx***min_rx***msec***multiplier***value*	デバイスのすべての BFD セッションの BFD セッションパラメータを設定します。インターフェイスで BFD セッション パラメータを設定することにより、このコマンドでこれらの値を無効にすることができます。*mintx* および *msec* の範囲は 15 ～ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ～ 50 です。乗数のデフォルトは 3 です。 （注） *mintx* 引数の値が 15 ミリ秒に設定されていたとしても、セッション上で **bfd hw-offload-module** コマンドが有効になっていない場合は、設定は適用されず、セッションがデフォルト タイマー値の 50 ミリ秒で機能します。
ステップ 5	switch(config-if)# **bfd authentication keyed-sha1 keyid***id***key***ascii_key*	（任意） インターフェイスですべての BFD セッションの SHA-1 認証を設定します。ascii_key 文字列は BFD ピア間で共有する秘密キーです。id 値は、0 ～ 255 の数字で、この特定の ascii_key に割り当てられます。BFD パケットは、複数

	コマンドまたはアクション	目的
		のアクティブ キーでの使用が許可されている id でキーを指定します。 インターフェイスの SHA-1 認証をディセーブルにするには、コマンドの **no** 形式を使用します。
ステップ 6	switch(config-if)# **show running-config bfd**	（任意） BFD の実行コンフィギュレーションを表示します。
ステップ 7	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。

BFD エコー機能の設定

BFDモニタ対象リンクの一端または両端でBFDエコー機能を設定できます。エコー機能は設定された slow timer に基づいて必要最小受信間隔を遅くします。RequiredMinEchoRx BFD セッション パラメータは、エコー機能がディセーブルの場合、ゼロに設定されます。slow timerは、エコー機能がイネーブルの場合、必要最小受信間隔になります。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

BFD 機能をイネーブルにします。

BFD セッション パラメータを設定します。

インターネット制御メッセージ プロトコル（ICMP）のリダイレクト メッセージが BFD 対応インターフェイスでディセーブルであることを確認します。インターフェイスで**no ip redirects** コマンドを使用します。

同一の送信元アドレスおよび宛先アドレスを調べる IP パケット検証チェックがディセーブルになっていることを確認します。デフォルト VDC では **no hardware ip verify address identical** コマンドを使用します。このコマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』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	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)# **bfd slow-timer***echo-interval*	エコー機能で使用される slow timer を設定します。この値は BFD が新しいセッションを開始する速度を決定し、BFD エコー機能がイネーブルの場合に非同期セッションの速度を低下させるために使用されます。この値は、エコー機能がイネーブルの場合、必要最小受信間隔より優先されます。指定できる範囲は 1000 ～ 30000 ミリ秒です。デフォルトは 2000 です。
ステップ 3	switch(config)# **interface***int-if*	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。**?** 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。
ステップ 4	switch(config-if)# **bfd echo**	エコー機能をイネーブルにします。デフォルトではイネーブルになっています。
ステップ 5	switch(config-if)# **show running-config bfd**	（任意） BFD の実行コンフィギュレーションを表示します。
ステップ 6	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。

サブインターフェイスの BFD の最適化

サブインターフェイスでBFDを最適化できます。BFDにより、設定されているすべてのサブインターフェイスのセッションが作成されます。BFD により、設定されている最小の VLAN ID を持つサブインターフェイスがマスター サブインターフェイスとして設定され、そのサブインターフェイスは親インターフェイスのBFDセッションパラメータを使用します。残りのサブインターフェイスは slow timer を使用します。最適化されたサブインターフェイス セッションでエラーが検出されると、BFD により、その物理インターフェイスのすべてのサブインターフェイスがダウンとマークされます。

（注） ハードウェア オフロード機能が有効になっているときは、サブインターフェイスの数が 750 未満の場合にのみ **bfd optimize subinterface** コマンドを設定します。そうしなければ、BFDセッションが確立されません。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

BFD 機能をイネーブルにします。

BFD セッション パラメータを設定します。

これらのサブインターフェイスが別の Cisco NX-OS デバイスに接続するようにしてください。この機能は、Cisco NX-OS でだけサポートされます。

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)# **interface***int-if*	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。**?** 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。
ステップ 3	switch(config-if)# **bfd optimize subinterface**	BFD 対応インターフェイスのサブインターフェイスを最適化します。デフォルトではディセーブルになっています。
ステップ 4	switch(config-if)# **show running-config bfd**	（任意） BFD の実行コンフィギュレーションを表示します。
ステップ 5	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。

IPv6 用の BFD の設定

IPv6 に対するグローバル BFD パラメータの設定

BFD パラメータを設定する場合は、IPv4 または IPv6 アドレス ファミリを指定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# **bfd** [**ipv4** | **ipv6**] **interval** [*interval***min_rx interval multiplier***interval-multiplier*	BFD セッション パラメータを、デバイスのすべての BFD セッションに対しミリ秒単位で設定します。

IPv6 に対するインターフェイス BFD パラメータごとの設定

はじめる前に

BFD をデバイスで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	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***number*	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。**?** 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。
ステップ 3	switch(config-if)# **bfd** [**ipv4** | **ipv6**] **interval** [*interval***min_rx interval multiplier***interval-multiplier*	BFD セッション パラメータを、デバイスのすべての BFD セッションに対しミリ秒単位で設定します。
ステップ 4	switch(config-if)# **bfd** [**ipv4** | **ipv6**] **authentication keyed-sha1 keyid***id***key***ascii_key*	（任意） 指定されたアドレス ファミリのすべての BFD セッションに対する Secure Hash Algorithm 1（SHA-1）認証を設定します。

IPv6 スタティック ルートでの BFD の設定

インターフェイス上のすべての IPv6 スタティック ルートに対する BFD を設定できます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

BFD がスタティック ルートの両端のデバイスでイネーブルになっていることを確認します。

BFD セッション パラメータを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# **vrf context***vrf-name*	VRF コンフィギュレーション モードを開始して、IPv6 スタティック ルートで BFD を設定します。 • ルートが BFD 追跡される VRF を指定します。
ステップ 3	switch(config-vrf)# **ipv6 route***route interface* {*nh-address* | *nh-prefix*}	IPv6 スタティック ルートを作成します。 • ルート引数に IPv6 アドレスを指定します。 • **?** 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。 • このスタティック ルートのネクスト ホップ（nh）アドレスまたはプレフィックスを指定します。
ステップ 4	switch(config-vrf)# **ipv6 route static bfd***network-interface* {*nh-address* | *nh-prefix*}	このインターフェイスとネクストホップの組み合わせ上のすべての IPv6 スタティック ルートに対し BFD をイネーブルにします。 • **?** 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。 • このスタティック ルートのネクスト ホップ（nh）アドレスまたはプレフィックスを指定します。
ステップ 5	switch(config-vrf)# **show bfd neighbors**	（任意） BFD ネイバーに関する情報を表示します。
ステップ 6	switch(config-vrf)# **show ipv6 route static**	（任意） スタティック ルートを表示します。

	コマンドまたはアクション	目的
ステップ 7	switch(config-vrf)# **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。

次に、2 台の BFD ネイバー間の IPv6 スタティック ルート上で BFD を設定する例を示します。

```
switch(config)# vrf context red
switch(config-vrf)# ipv6 route 1::5/64 ethernet 3/1 2::2
switch(config-vrf)# ipv6 route static bfd ethernet 3/1 2::2 <===Enables BFD on static
routes for the interface/next hop combination.
```

IPv6 に対する BFD エコー モードの設定

BFD エコー機能は、IPv6 リンクローカル アドレスを持つデバイスではサポートされません。

エコー機能はデフォルトでイネーブルになっています。IPv4、IPv6、またはすべてのアドレス ファミリでディセーブルにできます。

手順

	コマンドまたはアクション	目的
ステップ 1	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***int-if*	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。**?** 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。
ステップ 3	switch(config-if)# **bfd** [**ipv4** | **ipv6**] **echo**	指定されたアドレスに対するエコー機能をイネーブルにします。デフォルトではイネーブルになっています。 指定されたアドレス ファミリに対するエコー機能をディセーブルにするには、コマンドの **no** 形式を使用します。

IPv6 に対する BFD エコー インターフェイスの設定

すべてのエコー フレームの発信元アドレスとしてループバック インターフェイスを設定するには、このタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	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 loopback** **number**	ループバック インターフェイスを作成し、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 address***ip-address mask*	インターフェイスの IP アドレスを設定します。
ステップ 4	switch(config-if)# **ipv6 address***{ipv6-address / prefix-length | prefix-name sub-bits / prefix-length}*	すべてのエコー フレームの発信元アドレスとして IPv6 アドレスを設定します。

IPv6 に対する BFD スロータイマーの設定

エコー モードはデフォルトでイネーブルになっています。スロータイマー値を設定し、アドレス ファミリに対するエコー モードをディセーブルまたは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	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***int-if*	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。**?** 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。
ステップ 3	switch(config-if)# **bfd** [**ipv4** | **ipv6**] **slow-timer**[*interval*]	指定したアドレス ファミリに対するエコー機能で使用するために、slow timer をミリ秒単位で設定します。

ルーティング プロトコルに対する BFD サポートの設定

BGP での BFD の設定

Border Gateway Protocol（BGP）用に BFD を設定できます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

BFD 機能をイネーブルにします。

BFD セッション パラメータを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# **router bgp***as-number*	BGP をイネーブルにして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。
ステップ 3	switch(config-router)# **neighbor** {*ip-address* | *ipv6-address*} **remote-as***as-number*	リモート BGP ピアの IPv4 アドレスまたは IPv6 アドレスおよび AS 番号を設定します。ip-address の形式は x.x.x.x です。ipv6-address の形式は A:B::C:D です。
ステップ 4	switch(config-router-neighbor)# **bfd**	この BGP ピアの BFD をイネーブルにします。
ステップ 5	switch(config-router-neighbor)# **show running-config bfd**	（任意） BFD の実行コンフィギュレーションを表示します。
ステップ 6	switch(config-router-neighbor)# **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。

EIGRP 上の BFD の設定

Enhanced Interior Gateway Routing Protocol（EIGRP）の BFD を設定できます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

BFD 機能をイネーブルにします。

BFD セッション パラメータを設定します。

EIGRP 機能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	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)# **router eigrp***instance-tag*	インスタンス タグを設定して、新しい EIGRP プロセスを作成します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。 AS 番号であると認められていない *instance-tag* を設定する場合は、autonomous-system コマンドを使用して AS 番号を明示的に設定する必要があります。そうしないと、この EIGRP インスタンスはシャットダウン状態のままになります。
ステップ 3	switch(config-router-neighbor)# **bfd**	（任意） すべての EIGRP インターフェイスの BFD をイネーブルにします。
ステップ 4	switch(config-router-neighbor)# **interface***int-if*	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。**?** 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。
ステップ 5	switch(config-if)# **ip eigrp***instance-tag***bfd**	（任意） EIGRP インターフェイスで BFD をイネーブルまたはディセーブルにします。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。 デフォルトではディセーブルになっています。
ステップ 6	switch(config-if)# **show ip eigrp** [**vrf***vrf-name*] [**interfaces***if*]	（任意） EIGRP に関する情報を表示します。*vrf-name* には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。

	コマンドまたはアクション	目的
ステップ 7	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。

OSPF での BFD の設定

Open Shortest Path First バージョン 2（OSPFv2）で BFD を設定できます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

BFD 機能をイネーブルにします。

BFD セッション パラメータを設定します。

OSPF 機能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	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)# **router ospf***instance-tag*	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
ステップ 3	switch(config-router)# **bfd**	（任意） すべての OSPFv2 インターフェイスの BFD をイネーブルにします。
ステップ 4	switch(config-router)# **interface***int-if*	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。**?** 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。
ステップ 5	switch(config-if)# **ip ospf bfd**	（任意） OSPFv2 インターフェイスで BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。

	コマンドまたはアクション	目的
ステップ 6	switch(config-if)# **show ip ospf** [**vrf***vrf-name*] [**interfaces***if*]	（任意） OSPF に関する情報を表示します。*vrf-name* には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。
ステップ 7	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。

OSPFv3 での BFD の設定

BFD は、IPv6 ネットワークのリンクステート ルーティング プロトコルである Open Shortest Path First バージョン 3（OSPFv3）をサポートします。

OSPFv3 に対する BFD サポートをイネーブルにするには、2 つの方法があります。

- ルータ コンフィギュレーション モードで bfd コマンドを入力して、OSPFv3 がルーティングしているすべてのインターフェイスに対して BFD をイネーブルにできます。インターフェイス コンフィギュレーション モードで **ospfv3 bfd disable** コマンドを入力して、個々のインターフェイス上で BFD サポートをディセーブルにできます。
- インターフェイス コンフィギュレーション モードで **ospfv3 bfd** コマンドを入力して、OSPFv3 がルーティングしているインターフェイスのサブセットに対して BFD をイネーブルにできます。

（注） OSPF は、FULL ステートの OSPF ネイバーに対する BFD セッションを開始するだけです。

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)# **interface***int-if*	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。**?** 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。
ステップ 3	switch(config-if)# **bfd interval***mintx***min_rx***msec***multiplier***value*	デバイスのすべての BFD セッションの BFD セッション パラメータを設定します。インターフェイスで BFD セッション パラメータを設定

	コマンドまたはアクション	目的
		することにより、このコマンドでこれらの値を無効にすることができます。*mintx* および *msec* の範囲は 15 ～ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ～ 50 です。乗数のデフォルトは 3 です。 （注） *mintx* 引数の値が 15 ミリ秒に設定されていたとしても、セッション上で **bfd hw-offload-module** コマンドが有効になっていない場合は、設定は適用されず、セッションがデフォルトタイマー値の 50 ミリ秒で機能します。
ステップ 4	switch(config-if)# **end**	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。

すべてのインターフェイスでの OSPFv3 に対する BFD の設定

はじめる前に

OSPFv3 は、参加しているすべてのデバイスで実行されている必要があります。BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定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	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)# **router ospfv3***process-id*	OSFPv3 ルーティング プロセスを設定します。
ステップ 3	switch(config-router)# **bfd**	ルーティング プロセスに参加するすべてのインターフェイスに対して BFD をイネーブルにします。
ステップ 4	switch(config-router)# **exit**	EXEC モードに戻すには、このコマンドを 2 回入力します。

	コマンドまたはアクション	目的
ステップ 5	switch# **show bfd neighbors** [**details**]	既存の BFD 隣接関係の詳細なリストを表示します。
ステップ 6	switch# **show ospfv3** [*process-id*]	OSPFv3 ルーティング プロセスに関する一般的な情報を表示します。

1 つ以上のインターフェイスでの OSPFv3 に対する BFD の設定

はじめる前に

OSPFv3 は、参加しているすべてのデバイスで実行されている必要があります。BFD セッションをBFDネイバーに対して実行するインターフェイスで、BFDセッションの基本パラメータを設定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	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***int-if*	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。**?** 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。
ステップ 3	switch(config-if)# **ospfv3 bfd** [**disable**]	OSPFv3 ルーティング プロセスに関連付けられた 1 つ以上のインターフェイスに対して、インターフェイスごとに BFD をイネーブルにします。
ステップ 4	switch(config-if)# **exit**	EXEC モードに戻すには、このコマンドを 2 回入力します。
ステップ 5	switch# **show bfd neighbors** [**details**]	既存の BFD 隣接関係の詳細なリストを表示します。
ステップ 6	switch# **show ospfv3** [*process-id*]	OSPFv3 ルーティング プロセスに関する一般的な情報を表示します。

IS-IS での BFD の設定

Intermediate System-to-Intermediate System（IS-IS）プロトコル用に BFD を設定できます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

BFD 機能をイネーブルにします。

BFD セッション パラメータを設定します。

IS-IS 機能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	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)# **router isis***instance-tag*	instance tag を設定して、新しい IS-IS インスタンスを作成します。
ステップ 3	switch(config-router)# **bfd**	（任意） すべての IS-IS インターフェイスの BFD をイネーブルにします。
ステップ 4	switch(config-router)# **interface***int-if*	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。**?** 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。
ステップ 5	switch(config-if)# **isis bfd**	（任意） IS-IS インターフェイスで BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 6	switch(config-if)# **show isis** [**vrf***vrf-name*] [**interfaces***if*]	（任意） IS-IS に関する情報を表示します。*vrf-name* には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。
ステップ 7	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。

IS-ISv6 での BFD の設定

BFD で登録されたプロトコルとして IS-IS で BFD サポートが設定される場合、IS-IS が BFD から転送パスの検出障害メッセージを受信します。IS-IS に対する BFD サポートは、ルータ アドレス ファミリ コンフィギュレーション モードまたはインターフェイス コンフィギュレーション モードで設定できます。IS-IS IPv6は、シングルトポロジ モードで実行します。

IS-IS BFD は、シングルトポロジ モードに同時隣接している IPv4 と IPv6 の両方をサポートします。BFD が IPv4 と IPv6 の両方にイネーブルの場合、IS-IS は BFD に 2 つの BFD セッション作成要求を送信します。シングルトポロジ モードでは、IS-IS 隣接状態は、両方のBFD セッションがアップした場合にのみ実行できます。BFDセッションのいずれかがダウンすると、関連する IS-IS 隣接状態もまたダウンします。

IS-IS BFD IPv6 がインターフェイスでディセーブルの場合、IS-IS は隣接デバイスから IPv6 の関連 BFD セッションを削除します。IS-IS 隣接エントリを削除すると、すべての BFD セッションも削除されます。IS-IS は、次のいずれかのイベントが発生したときに要求した各 BFD セッションを削除するように BFD に要求します。

- IS-IS インスタンスが削除または設定解除される。
- IS-IS 隣接エントリが削除される。
- IS-IS BFD がアドレス ファミリのネクスト ホップ インターフェイスでディセーブルになる。

インターフェイスでの IS-IS IPv6 クライアント サポートの設定

IS-IS は、次の条件がすべて満たされると、インターフェイスと隣接デバイスの IPv6 アドレスに対する BFD セッションを要求します。

- IS-IS 隣接エントリが存在する。
- アドレス ファミリ識別子（AFI）固有のピア インターフェイス アドレスが認識されている。
- IS-IS BFD がインターフェイスでその AFI に対してイネーブルになっている。
- IS-IS がローカル インターフェイスでその AFI に対してイネーブルになっている。
- 隣接デバイスが RFC 6213 をサポートしている場合、BFD が指定されたネットワーク層プロトコル識別子（NLPID）に対しイネーブルになっている必要がある。

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***int-if*	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。**?**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。
ステップ 3	switch(config-if)# **isis ipv6 bfd**	IS-IS に設定されている特定のインターフェイスで BFD IPv6 をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	switch(config-if)# **end**	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 5	switch(config)# **show isis interface***type number*	（任意） IS-IS に関するインターフェイス情報を表示します。

すべてのインターフェイスでの BFD の IS-IS IPv6 クライアント サポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	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)# **router isis***process-id*	IS-IS ルーティング プロトコルをイネーブルにし、ルータ 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-router)# **metric-style transition**	（任意） 新しいスタイル、タイプ、長さ、値オブジェクト（TLV）のみを生成し受け入れるように、IS-IS を実行しているデバイスを設定します。
ステップ 4	switch(config-router)# **address-family ipv6 unicast**	標準の IPv6 アドレス プレフィックスを使用する IS-IS ルーティング セッションを設定するアドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	switch(config-router-af)# **bfd**	ルーティング プロセスに参加するすべてのインターフェイスに対して BFD をイネーブルにします。
ステップ 6	switch(config-router-af)# **end**	アドレス ファミリ 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	switch(config)# **show isis** [*process-id*]	（任意） IS-IS に関するインターフェイス情報を表示します。

特定のインターフェイスでの FabricPath BFD の設定

はじめる前に

BFD 機能をイネーブルにします。

BFD セッション パラメータを設定します。

feature-set fabricpath コマンドを入力すると、ISIS 機能がデフォルトで有効になります。

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)# **[no] bfd fabricpath encap-ce**	ユーザが、セッション単位で L2BFD フレームのカプセル化モードを選択できるようにします。コマンドを有効にすると、Fabricpath カプセル化を使用せずにフレームが送信されます。デフォルト モードは、Fabricpath カプセル化を使用してフレームが送信されます。
ステップ 3	switch(config-if)# **fabricpath isis bfd**	インターフェイス上で FabricPath BFD をイネーブルにします。

この例では、特定のインターフェイス上で FabricPath BFD を設定する方法を示します。

```
switch# configure terminal
switch(config)# [no] bfd fabricpath encap-ce
switch(config-if)# fabricpath isis bfd
```

すべての IS-IS インターフェイスでの FabricPath BFD の設定

はじめる前に

正しい VRF を使用していることを確認します。

BFD 機能をイネーブルにします。

BFD セッション パラメータを設定します。

feature-set fabricpath コマンドを入力すると、ISIS 機能がデフォルトで有効になります。

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)# **fabricpath domain default**	グローバル FabricPath レイヤ 2 Intermediate System to Intermediate System（IS-IS）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-fabricpath-isis)# **bfd**	すべての IS-IS インターフェイス上で FabricPath BFD をイネーブルにします。

この例では、すべての IS-IS インターフェイス上で FabricPath BFD を設定する方法を示します。

```
switch# configure terminal
switch(config)# fabricpath domain default
switch(config-fabricpath-isis)# bfd
```

HSRP での BFD の設定

Hot Standby Router Protocol（HSRP）用に BFD を設定できます。アクティブおよびスタンバイの HSRP ルータは BFD を介して相互に追跡しています。スタンバイ HSRP ルータ上の BFD がアクティブ HSRP ルータが動作していないことを検知すると、スタンバイ HSRP はこのイベントをアクティブ タイマー失効として取り扱いアクティブ HSRP ルータとして役割を引き継ぎます。

show hsrp bfd-sessions コマンドは、すべてのインターフェイスの HSRP BFD セッション情報を表示するために使用します。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

BFD 機能をイネーブルにします。

BFD セッション パラメータを設定します。

HSRP 機能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	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)# **hsrp bfd all-interfaces**	（任意） HSRP インターフェイスですべての BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 3	switch(config)# **interface***int-if*	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。**?** 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。
ステップ 4	switch(config-if)# **hsrp bfd**	（任意） HSRP インターフェイスで BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 5	switch(config-if)# **show running-config hsrp**	（任意） HSRP の実行コンフィギュレーションを表示します。
ステップ 6	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。

VRRP での BFD の設定

仮想ルータ冗長プロトコル（VRRP）の BFD を設定できます。アクティブおよびスタンバイの VRRP ルータは BFD を介して相互に追跡しています。スタンバイ VRRP ルータ上の BFD がアクティブ VRRP ルータが動作していないことを検知すると、スタンバイ VRRP はこのイベントをアクティブ タイマー失効として取り扱いアクティブ VRRP ルータとして役割を引き継ぎます。

show vrrp detail では、このイベントが BFD@Act-down または BFD@Sby-down として表示されます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

BFD 機能をイネーブルにします。

BFD セッション パラメータを設定します。

VRRP 機能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	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***int-if*	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。**?** 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。
ステップ 3	switch(config-if)# **vrrp***group-no*	VRRP グループ番号を指定します。
ステップ 4	switch(config-if)# **vrrp bfd***address*	VRRP インターフェイスで BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 5	switch(config-if)# **show running-config vrrp**	（任意） VRRP の実行コンフィギュレーションを表示します。
ステップ 6	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。

PIM での BFD の設定

PIM（Protocol Independent Multicast）プロトコルの BFD を設定できます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

BFD 機能をイネーブルにします。

PIM 機能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	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 pim bfd**	PIM の BFD をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **interface***int-if*	（任意） 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。**?** 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。
ステップ 4	switch(config-if)# **ip pim bfd-instance** [**disable**]	PIM インターフェイスの BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 5	switch(config-if)# **show running-config pim**	（任意） PIM の実行コンフィギュレーションを表示します。
ステップ 6	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。

スタティック ルートでの BFD の設定

インターフェイスのスタティック ルータの BFD を設定できます。仮想ルーティングおよび転送（VRF）インスタンス内のスタティック ルートでの BFD を任意で設定できます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

BFD 機能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	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)# **vrf context***vrf-name*	（任意） VRF 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-vrf)# **ip route***route interface* {*nh-address* | *nh-prefix*}	スタティック ルートを作成します。**?** キーワードを使用して、サポートされているインターフェイスを表示します。

	コマンドまたはアクション	目的
ステップ 4	switch(config-vrf)# **ip route static bfd interface** {*nh-address* | *nh-prefix*}	インターフェイスのすべてのスタティック ルートの BFD をイネーブルにします。**?** 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。
ステップ 5	switch(config-vrf)# **show ip route static** [**vrf***vrf-name*]	（任意） スタティック ルートを表示します。
ステップ 6	switch(config-vrf)# **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。

MPLS TE 高速再ルーティングの BFD 設定

MPLS トラフィック エンジニアリング（TE）はBFDを使用して、ノード障害の検出を高速化し、転送パス障害の検出時間を短縮します。MPLS TE 高速再ルーティングの BFD は、トンネルで高速再ルーティングをイネーブルにすると自動的に設定されます。詳細については、『*Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide*』の「Configuring MPLS TE Fast Reroute Link and Node Protection」の章を参照してください。

インターフェイスにおける BFD のディセーブル化

グローバルまたは VRF レベルで BFD がイネーブルになっているルーティング プロトコルのインターフェイスで BFD を選択的にディセーブルにできます。

インターフェイスでBFDをディセーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドのいずれかを使用します。

コマンド	目的
ip eigrp*instance-tag***bfd disable**	EIGRP インターフェイスで BFD をディセーブルにします。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
ip ospf bfd disable	OSPFv2 インターフェイスで BFD をディセーブルにします。
isis bfd disable	IS-IS インターフェイスで BFD をディセーブルにします。

アンナンバード インターフェイスでの BFD の設定

アンナンバードインターフェイス経由でBFDをセットアップする基本的なスイッチ設定の一部を以下に示します。

1. アンナンバードのイーサネット インターフェイスを設定します。
2. アンナンバード インターフェイスの IP アドレスが抽出されるループバック インターフェイスを設定します。
3. ルータ上で IS-IS または VRF を使用した OSPF を設定します。

手順

ステップ 1 アンナンバードのイーサネット インターフェイス上で ISIS を設定する手順を以下に示します。

a) 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。
switch# **configure terminal**

b) 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。
switch(config)# **interface ethernet***slot* / *port*

c) インターフェイス メディアをポイントツーポイントとして設定します。
switch(config-if)# **medium p2p**

d) ループバック インターフェイス上で IP 処理を有効にします。
switch(config-if)# **ip unnumbered***instance*

e) 複数のレベルでルーティングのコストを計算するための IS-IS メトリックを設定します。
switch(config-if)# **isis metric** {*metric-value* | **maximum**} [**level-1** | **level-2**]

f) 隣接関係のタイプを設定します。
switch(config-if)# **isis circuit-type** [**level-1** | **level-1-2** | **level-2-only**]

g) 設定されたインターフェイス上でIS-IS ルーティング プロセスを IP 用に設定し、エリア指示子をルーティング プロセスにアタッチします。
switch(config-if)#**ip router isis***area-tag*

h) BFD の有効化
switch(config-if)#**isis bfd***instance*

i) コンフィギュレーション モードを終了します。
switch(config-if)#**end**

ステップ 2 アンナンバード インターフェイスの IP アドレスが抽出されるループバック インターフェイスを設定する手順を以下に示します。

a) ループバック インターフェイスを作成し、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。
switch(config)# **interface loopback***instance*

b) このループバック インターフェイスの IP アドレスを設定します。

switch(config-if)#**ip address***address*

c) 設定されたインターフェイス上でIS-ISルーティング プロセスをIP用に設定し、エリア指示子をルーティング プロセスにアタッチします。
switch(config-if)#**ip router isis***area-tag*

アンナンバード インターフェイス上の BFD の設定例

次の例では、ISISプロトコルを使用したアンナンバードイーサネットインターフェイス上でBFDを設定する方法を示します。

```
interface Ethernet1/2
  medium p2p
  ip unnumbered loopback1
  isis metric 10 level-1
  isis circuit-type level-1
  ip router isis 100
  isis bfd
  no shutdown
router isis 100
  net 49.0001.0000.0000.000a.00
  is-type level-1
    address-family ipv6 unicast
```

次の例では、OSPF と VRF を使用したアンナンバード インターフェイス経由で BFD を設定する方法を示します。

```
vrf context vrf3
interface Ethernet1/14
  medium p2p
  vrf member vrf3
  ip unnumbered loopback1
  ip router ospf 10 area 0.0.0.0
  no shutdown

interface loopback1
  vrf member vrf3
  ip address 10.1.1.2/32
line vty
router ospf 10
  bfd
  vrf vrf3
  bfd
```

BFD 相互運用性の設定

ポイントツーポイント リンク内の Cisco NX-OS デバイスの BFD 相互運用性の設定

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***int-if*	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。**?** 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。
ステップ 3	switch(config-if)# **ip ospf bfd**	OSPFv2 インターフェイスで BFD をイネーブルにします。デフォルトではディセーブルになっています。 サポートされている任意のプロトコルの BFD をイネーブルにできます。
ステップ 4	switch(config-if)# **no ip redirect**	デバイスがリダイレクトを送信しないようにします。
ステップ 5	switch(config-if)# **bfd interval***mintx***min_rx***msec***multiplier***value***	デバイスのすべての BFD セッションの BFD セッションパラメータを設定します。インターフェイスで BFD セッションパラメータを設定することにより、このコマンドでこれらの値を無効にすることができます。*mintx* および *msec* の範囲は 15 ～ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ～ 50 です。乗数のデフォルトは 3 です。 （注） *mintx* 引数の値が 15 ミリ秒に設定されていたとしても、セッション上で **bfd hw-offload-module** コマンドが有効になっていない場合は、設定は適用されず、セッションがデフォルト タイマー値の 50 ミリ秒で機能します。
ステップ 6	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、EXEC モードに戻ります。

スイッチ仮想インターフェイス内の Cisco NX-OS デバイスの BFD 相互運用性の設定

BFDは、L3スイッチ上に設定されたスイッチ仮想インターフェイスでサポートされます。このような2つのスイッチを接続するポートは、次のモードで接続できます。

- トランク：このような2つのデバイスのポートは従来のイーサネットを使用して接続し、トランク モードで設定することができます。
- ファブリック：このような2つのデバイスのポートはファブリック パス コアを使用して接続し、FabricPath モードで設定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	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***int-if*	ダイナミック スイッチ仮想インターフェイス（SVI）を作成します。
ステップ 3	switch(config-if)# **bfd interval***mintx***min_rx***msec***multiplier***value*	デバイスのすべてのBFDセッションのBFDセッション パラメータを設定します。インターフェイスでBFDセッションパラメータを設定することにより、このコマンドでこれらの値を無効にすることができます。*mintx* および *msec* の範囲は 15 ～ 999 ミリ秒で、デフォルトは50です。乗数の範囲は1 ～ 50です。乗数のデフォルトは 3 です。 （注） *mintx* 引数の値が 15 ミリ秒に設定されていたとしても、セッション上で **bfd hw-offload-module** コマンドが有効になっていない場合は、設定は適用されず、セッションがデフォルト タイマー値の 50 ミリ秒で機能します。
ステップ 4	switch(config-if)# **no ip redirect**	デバイスがリダイレクトを送信しないようにします。
ステップ 5	switch(config-if)# **ip address***ip-address/length*	このインターフェイスの IP アドレスを設定します。
ステップ 6	switch(config-if)# **ip ospf bfd**	OSPFv2 インターフェイスで BFD をイネーブルにします。デフォルトではディセーブルになっています。

	コマンドまたはアクション	目的
ステップ 7	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、EXECモードに戻ります。
ステップ 8	switch(config)# **interface***int-if*	上記手順に従って設定された別のスイッチに接続するポートを設定します。
ステップ 9	次のいずれかを実行します。 • switch(config-if)# **switchport mode trunk** • switch(config-if)# **switchport mode fabricpath**	インターフェイスが、従来のイーサネット トランク ポートまたはファブリック パス ポートとして設定されます。
ステップ 10	switch(config-if)# **end**	特権 EXEC モードに戻ります。

論理モードの Cisco NX-OS デバイスの BFD 相互運用性の設定

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 number.subinterface-id*	ポート チャネル コンフィギュレーション モードを開始します。**?** キーワードを使用して、サポートされる数値の範囲を表示します。
ステップ 3	switch(config-if)# **bfd interval***mintx***min_rx***msec***multiplier***value*	デバイスのすべての BFD セッションの BFD セッション パラメータを設定します。インターフェイスで BFD セッション パラメータを設定することにより、このコマンドでこれらの値を無効にすることができます。*mintx* および *msec* の範囲は 15 ～ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ～ 50 です。乗数のデフォルトは 3 です。

	コマンドまたはアクション	目的
		（注） *mintx* 引数の値が 15 ミリ秒に設定されていたとしても、セッション上で **bfd hw-offload-module** コマンドが有効になっていない場合は、設定は適用されず、セッションがデフォルトタイマー値の 50 ミリ秒で機能します。
ステップ 4	switch(config-if)# **no ip redirect**	デバイスがリダイレクトを送信しないようにします。
ステップ 5	switch(config-if)# **ip ospf bfd**	OSPFv2 インターフェイスで BFD をイネーブルにします。デフォルトではディセーブルになっています。
ステップ 6	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、EXEC モードに戻ります。

Cisco Nexus 7000 シリーズ デバイスでの BFD 相互運用性の確認

次に、Cisco Nexus 7000 シリーズ デバイス上で BFD 相互運用性を確認する例を示します。

```
switch# show bfd neighbors details
OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int
Vrf
10.1.1.1 10.1.1.2 1140850707/2147418093 Up 6393(4) Up Vlan2121
default
Session state is Up and using echo function with 50 ms interval
Local Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: None
MinTxInt: 50000 us, MinRxInt: 2000000 us, Multiplier: 3
Received MinRxInt: 2000000 us, Received Multiplier: 4
Holdown (hits): 8000 ms (0), Hello (hits): 2000 ms (108)
Rx Count: 92, Rx Interval (ms) min/max/avg: 347/1996/1776 last: 1606 ms ago
Tx Count: 108, Tx Interval (ms) min/max/avg: 1515/1515/1515 last: 1233 ms ago
Registered protocols: ospf
Uptime: 0 days 0 hrs 2 mins 44 secs
Last packet: Version: 1 - Diagnostic: 0
State bit: Up - Demand bit: 0
Poll bit: 0 - Final bit: 0
Multiplier: 4 - Length: 24
My Discr.: 2147418093 - Your Discr.: 1140850707
Min tx interval: 2000000 - Min rx interval: 2000000
Min Echo interval: 1000 - Authentication bit: 0
Hosting LC: 10, Down reason: None, Reason not-hosted: None

switch# show bfd neighbors details
OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int
Vrf
10.0.2.1 10.0.2.2 1140850695/131083 Up 270(3) Up Po14.121
default
Session state is Up and not using echo function
Local Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: None
MinTxInt: 50000 us, MinRxInt: 50000 us, Multiplier: 3
Received MinRxInt: 100000 us, Received Multiplier: 3
```

```
Holdown (hits): 300 ms (0), Hello (hits): 100 ms (3136283)
Rx Count: 2669290, Rx Interval (ms) min/max/avg: 12/1999/93 last: 29 ms ago
Tx Count: 3136283, Tx Interval (ms) min/max/avg: 77/77/77 last: 76 ms ago
Registered protocols: ospf
Uptime: 2 days 21 hrs 41 mins 45 secs
Last packet: Version: 1 - Diagnostic: 0
State bit: Up - Demand bit: 0
Poll bit: 0 - Final bit: 0
Multiplier: 3 - Length: 24
My Discr.: 131083 - Your Discr.: 1140850695
Min tx interval: 100000 - Min rx interval: 100000
Min Echo interval: 0 - Authentication bit: 0
Hosting LC: 8, Down reason: None, Reason not-hosted: None
```

F3 および M3 ライン カード上の BFD ACP オフロードの確認

BFD 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show running-config bfd	実行 BFD コンフィギュレーションを表示します。
show startup-config bfd	次のシステム起動時に適用される BFD コンフィギュレーションを表示します。
show bfd neighbors	BFD ネイバーに関する情報を表示します。
show bfd neighbors neighbors	BFD ネイバーに関する詳細情報を表示します。

次の例では、F3 および M3 ライン カード上の BFD ACP オフロード機能を確認する方法を示します。出力には、オフロードされたセッションの横にアスタリスク（*）記号が表示されます。

```
switch# show bfd neighbors

OurAddr   NeighAddr  LD/RD       RH/RS   Holdown(mult) State  Int   Vrf
*10.2.2.2   10.2.2.1   1124073477/1  Up      N/A(3)        Up     Eth1/45   default

10.1.1.2   10.1.1.1    1124073478/1   Down    N/A(3)        Down   Eth1/46  default

*10.3.3.2  10.3.3.1    1124073479/1   Up      N/A(3)        Up     Eth1/47  default

10.4.4.2   10.4.4.1    1124073480/1   Down    N/A(3)        Down   Eth1/48  default
```

次の例では、F3 および M3 ライン カード上の BFD ACP オフロードを確認する方法を示します。出力には、特定のセッションがオフロードされたことを示すフィールドが表示されます。

```
switch# show bfd neighbors details

OurAddr   NeighAddr LD/RD                RH/RS  Holdown(mult) State Int     Vrf
*10.2.2.1  10.2.2.2   1107296257/1124073474 Up    4880(3)       Up    Eth1/2  default

Session state is Up and using echo function with 50 ms interval
Local Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: None
MinTxInt: 50000 us, MinRxInt: 2000000 us, Multiplier: 3
Received MinRxInt: 2000000 us, Received Multiplier: 3
Holdown (hits): 6000 ms (0), Hello (hits): 2000 ms (1142)
```

```
Rx Count: 1139, Rx Interval (ms) min/max/avg: 0/5132/1693 last: 1119 ms ago
Tx Count: 1142, Tx Interval (ms) min/max/avg: 1689/1689/1689 last: 1120 ms ago
Registered protocols:  hsrp_engine
Uptime: 0 days 0 hrs 32 mins 3 secs
Last packet: Version: 1                - Diagnostic: 0
             State bit: Up             - Demand bit: 0
             Poll bit: 0               - Final bit: 0
             Multiplier: 3             - Length: 24
             My Discr.: 1124073474     - Your Discr.: 1107296257
             Min tx interval: 50000    - Min rx interval: 2000000
             Min Echo interval: 50000  - Authentication bit: 0
Hosting LC: 1, Down reason: None, Reason not-hosted: None, Offloaded: Yes
```

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』を参照してください。

マイクロ BFD セッションの設定

ポート チャネル インターフェイスの設定

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

BFD機能をイネーブルにします。詳細については、次のサイトを参照してください。BFD機能の有効化, （141 ページ）

手順

ステップ 1 インターフェイス ポート チャネルを設定します。
switch(config)# **interface port-channel** *port-number*

ポート チャネル コンフィギュレーション モードを開始します。**?** キーワードを使用して、サポートされる数値の範囲を表示します。

ステップ 2 レイヤ 3 ポート チャネルとしてインターフェイスを設定します。
switch(config)# **no switchport**

次の作業

- BFD 開始タイマーの設定
- IETF リンク単位 BFD の有効化

（オプション）BFD 開始タイマーの設定

手順

ポート チャネルの BFD 開始タイマーを設定します。

switch(config)# **interface port-channel** *port-number*

（注） デフォルト値は無限（つまり、タイマーが作動していない状態）です。開始タイマーが動作するためには、ポート チャネル BFD 設定を完了する前（つまり、port-channel bfd track-member-link と port-channel bfd destination をアクティブ メンバーとのレイヤ 3 ポート チャネル インターフェイス用に設定する前）に開始タイマー値を設定します。

次の作業

- IETF リンク単位 BFD の有効化
- BFD 宛先 IP アドレスの設定

IETF リンク単位 BFD の有効化

手順

ポート チャネル インターフェイス上で IETF BFD を有効にします。
switch(config-if)# **port-channel bfd track-member-link**

次の作業

- BFD 宛先 IP アドレスの設定
- マイクロ BFD セッション設定の確認

BFD 宛先アドレスの設定

手順

メンバー リンク上の BFD セッションに使用される IPv4 アドレスを設定します。
switch(config-if)# **port-channel bfd destination** *ip-address*

次の作業

- マイクロ BFD セッション設定の確認

（オプション）マイクロ BFD セッション設定の確認

マイクロ BFD セッション設定を確認するには、次のコマンドを任意の順序で使用します。

手順

ステップ 1 ポート チャネルとポート チャネル メンバーの動作状態を表示します。
switch# **show port-channel summary**

ステップ 2 ポート チャネル メンバー上のマイクロ BFD セッションを表示します。
switch# **show bfd neighbors**

ステップ 3 ポート チャネル インターフェイスの BFD セッションと、メンバーの関連するマイクロ BFD セッションを表示します。
switch# **show bfd neighbors details**

ステップ 4 BFD のテクニカル サポート情報を表示します。
switch# **show tech-support bfd**

ステップ 5 イーサネット ポート マネージャ、イーサネット ポートチャネル マネージャ、および LACP のテクニカル サポート情報を表示します。
switch# **show tech-support lacp all**

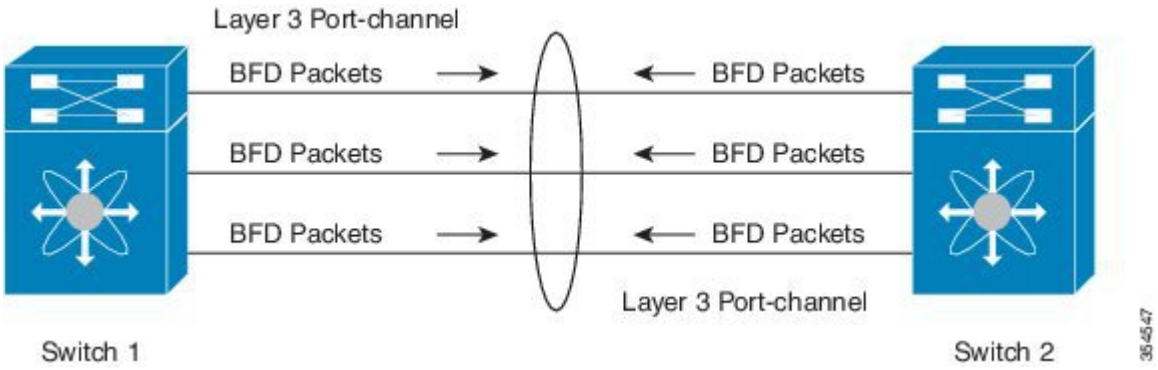
ステップ 6 ポート チャネル インターフェイスの実行コンフィギュレーション情報を表示します。
switch# **show running-config interface port-channel** *port-channel-number*

例：マイクロ BFD セッションの設定

マイクロ BFD セッションの設定

この例では、次のトポロジを使用しています。

図 *8*：マイクロ *BFD* セッションの設定



スイッチ 1 のサンプル設定

```
feature bfd
configure terminal
```

```
    interface port-channel 10
       port-channel bfd track-member-link
       port-channel bfd destination 10.1.1.2
       port-channel bfd start 60
       ip address 10.1.1.1/24
```

スイッチ 2 のサンプル設定

```
feature bfd
configure terminal
     interface port-channel 10
           port-channel bfd track-member-link
           port-channel bfd destination 10.1.1.1
           port-channel bfd start 60
             ip address 10.1.1.2/24
```

マイクロ BFD セッション設定の確認

次に、**show port-channel summary** コマンドの出力結果を示します。

下記に表示される出力にはフィールドの説明も表示されます。

```
switch(config-if-range)# show port-channel summary

Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
10    Po10(RD)    Eth      NONE    Eth7/26(b)   Eth7/27(b) Eth7/28(b)
```

次に、**show bfd neighbors detail** コマンドの出力結果を示します。

出力にはフィールドの説明も表示されます。

```
switch(config-if-range)# show bfd neighbors detail


OurAddr   NeighAddr   LD/RD         RH/RS  Holdown(mult)  State    Int   Vrf
10.1.1.1  10.1.1.2    1107296277/0  Down    N/A(3)        Down    Po10  default
Session state is Down and not using echo function
Local Diag: 1, Demand mode: 0, Poll bit: 0, Authentication: None
MinTxInt: 0 us, MinRxInt: 0 us, Multiplier: 0
Received MinRxInt: 0 us, Received Multiplier: 0
Holdown (hits): 0 ms (0), Hello (hits): 0 ms (0)
Rx Count: 0, Rx Interval (ms) min/max/avg: 0/0/0 last: 0 ms ago
Tx Count: 0, Tx Interval (ms) min/max/avg: 0/0/0 last: 0 ms ago
Registered protocols:  eth_port_channel
Downtime: 0 days 0 hrs 0 mins 4 secs
Last packet: Version: 0               - Diagnostic: 0
             State bit: AdminDown     - Demand bit: 0
             Poll bit: 0              - Final bit: 0
             Multiplier: 0            - Length: 24
             My Discr.: 0             - Your Discr.: 0
             Min tx interval: 0       - Min rx interval: 0
             Min Echo interval: 0     - Authentication bit: 0
Hosting LC: 0, Down reason: Control Detection Time Expired, Reason not-hosted: SUCCESS,
Offloaded: No
Parent session, please check port channel config for member info
```

BFD 設定の確認

BFD 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show running-config bfd	実行 BFD コンフィギュレーションを表示します。
show startup-config bfd	次のシステム起動時に適用される BFD コンフィギュレーションを表示します。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』を参照してください。

BFD のモニタ

BFD 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 bfd neighbors [**application***name*] [**details**]	BGP や OSPFv2 などのサポートされるアプリケーションの BFD に関する情報を表示します。
show bfd neighbors [**interface***int-if*] [**details**]	インターフェイスの BGP セッションに関する情報を表示します。
show bfd neighbors [**dest-ip***ip-address*] [**src-ip***ip-address*][**details**]	インターフェイス上の指定された BGP セッションに関する情報を表示します。
show bfd neighbors [**vrf***vrf-name*] [**details**]	VRF の BFD に関する情報を表示します。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』を参照してください。

BFD の設定例

次に、デフォルト BFD セッション パラメータを使用した、Ethernet 2/1 上の OSPFv2 の BFD 設定例を示します。

```
feature bfd
feature ospf
router ospf Test1
interface ethernet 2/1
```

```
  ip ospf bfd
  no shutdown
```

次に、デフォルト BFD セッション パラメータを使用した、EIGRP インターフェイスの BFD 設定例を示します。

```
feature bfd
feature eigrp
bfd interval 100 min_rx 100 multiplier 4
router eigrp Test2
 bfd
```

関連資料

関連項目	マニュアル タイトル
『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/interfaces/command/reference/if_cmds.html
『*Interfaces Configuration Guide, Cisco DCNM for LAN*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/dcnm/interfaces/configuration/guide/if_dcnm.html
『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/system_management/configuration/guide/sm_nx_os_cg.html
『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/high_availability/configuration/guide/b_Cisco_Nexus_7000_Series_NX-OS_High_Availability_and_Redundancy_Guide.html
『*Cisco Nexus 2000 Series NX-OS Fabric Extender Software Configuration Guide for Cisco Nexus 7000 Series Switches, Release 6.x*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus2000/sw/configuration/guide/rel_6_1/b_Cisco_Nexus_2000_Series_NX-OS_Fabric_Extender_Software_Configuration_Guide_Release_6-x.html
『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/virtual_device_context/configuration/guide/b-7k-Cisco-Nexus-7000-Series-NX-OS-Virtual-Device-Context-Configuration-Guide.html
『*Cisco NX-OS Licensing Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/licensing/guide/b_Cisco_NX-OS_Licensing_Guide.html
VLAN、MAC アドレス テーブル、プライベート VLAN、およびスパニング ツリー プロトコル。 『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/layer2/configuration/guide/b_Cisco_Nexus_7000_Series_NX-OS_Layer_2_Switching_Configuration_Guide.html

関連項目	マニュアル タイトル
『*Cisco Nexus 7000 Series NX-OS FabricPath Command Reference*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/fabricpath/command/reference/fp_cmd_book.html
『*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/fabricpath/configuration/guide/b-Cisco-Nexus-7000-Series-NX-OS-FP-Configuration-Guide-6x.html
『Cisco Nexus 7000 Series NX-OS Release Notes』	http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-release-notes-list.html

RFC

RFC	タイトル
RFC 5880	双方向フォワーディング検出（*BFD*）
RFC 5881	『*BFD for IPv4 and IPv6 (Single Hop)*』

第 7 章

ポート チャネルの設定

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

ポート チャネルの設定

この章では、ポート チャネルを設定し、Cisco NX-OS デバイスでポート チャネルをより有効に利用するために Link Aggregation Control Protocol（LACP）を適用して設定する手順を説明します。

Cisco NX-OS リリース 5.1(1) 以降では、ポート チャネルに F1 シリーズ モジュールまたは M1 シリーズ モジュールを使用することができますが、単一のポート チャネルで F1 モジュールのメンバ ポートを M1 モジュールのポートと組み合わせることはできません。単一のスイッチでは、物理スイッチ上のすべてのポートチャネルメンバー間で、ポートチャネルの互換性パラメータが同一である必要があります。

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。ポートチャネリングはまた、Mシリーズモジュールおよびこれらの物理インターフェイス全体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。

（注） Cisco NX-OS リリース 5.1 以降では、F シリーズ モジュールのポート チャネルに最大 16 個のアクティブ リンクをバンドルすることができます。

ポート チャネル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。共有インターフェイスの詳細については、『*Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*』を参照してください。

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 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 アドレスを追加してレイヤ 3 ポート チャネルにサブインターフェイスを作成できます。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。

Cisco NX-OS Release 4.2 から、ポート セキュリティをポート チャネルに適用できますポート セキュリティについては、『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide*』を参照してください。ポートチャネル内のすべてのポートは、同じ仮想デバイス コンテキスト（VDC）にある必要があります。VDC にまたがってポート チャネルを設定す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設定」を参照してください。

変更した設定をポート チャネルに適用すると、そのポート チャネルのメンバ インターフェイスにもそれぞれ変更が適用されます。たとえば、スパニングツリー プロトコル（STP）パラメータ

をポート チャネルに設定すると、Cisco NX-OS ソフトウェアはこれらのパラメータをポート チャネルのそれぞれのインターフェイスに適用します。

（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。

サブインターフェイスが論理ポート チャネル インターフェイスの一部であっても、レイヤ 3 ポート チャネルにサブインターフェイスを作成できます。ポート チャネル サブインターフェイスの詳細については、「サブインターフェイス」の項を参照してください。

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」の項を参照してください。

ポート チャネル設定の機能履歴

この表には、機能の追加や変更によるリリースの更新内容のみが記載されています。

機能名	リリース	機能情報
M3 シリーズモジュール上の GPRS トンネリング プロトコル（GTP）ロード バランシングのサポート	7.3(0)DX(1)	M3 モジュールを使用した GTP トラフィックのポート チャネルと ECMP のロードバランシングが改善されました。
ランダム ロード バランス（ポート チャネル）	7.3(0)D1(1)	ポート チャネル上でのランダム ロード バランシングに対するサポートが追加されました。ポートチャネル全体のロード バランシングを改善するために、**random** キーワードが **port-channel load-balance** コマンドに追加されました。
インターフェイスおよび VLAN のポリシー エラーの表示	6.2(2)	**show interface status error policy** コマンドが追加されました。
F2 または F2e モジュールでの双方向フロー時のトラフィック ドロップの回避	6.2(2)	ポート チャネル全体のロード バランシングを改善するために、**asymmetric** キーワードが **port-channel load-balance** コマンドに追加されました。

機能名	リリース	機能情報
Result Bundle Hash ロード バランシング	6.1(3)	ポート チャネル全体のロード バランシングを改善するための RBH モジュロ モードのサポート。
FEX ファブリック ポート チャネル用最少リンク数	6.1(3)	この機能が導入されました。
ポート チャネル ハッシュ分散	6.1(1)	ポート チャネル ハッシュ分散の固定およびアダプティブ モードのサポート。
F2 モジュールのロードバランシングのサポート	6.0(1)	ポートチャネル全体のロードバランシングに対する F2 モジュールのサポートが追加されました。
ポート チャネル	5.2(1)	サポートが 528 ポート チャネルに増加されました。
LACP の最少リンクおよび Maxbundle	5.1(1)	この機能が導入されました。
ポート チャネル	4.2(1)	サポートが 256 ポート チャネルに増加されました。
ポート チャネル	4.0(1)	この機能が導入されました。

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、M シリーズ モジュール上の最大 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。

（注） Cisco NX-OS リリース 5.1 以降では、F シリーズ モジュールのポート チャネルに最大 16 個のアクティブ ポートを同時にバンドルすることができます。

最大 8 つのポートをスタティック ポート チャネルにバンドルできます。集約プロトコルは使用しません。M シリーズ モジュールでは、M シリーズ モジュールの最大 8 個のアクティブ ポートと最大 8 個のスタンバイ ポート、および F シリーズ モジュールの最大 16 個のポートをバンドルすることができます。

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スタティック 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 チャネルの設定」の項を参照）。

（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」の項を参照）。集約プロトコルを使わずにスタティック 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 をイネーブルにしない限り変更できません（「ポート チャネル モード」の項を参照）。

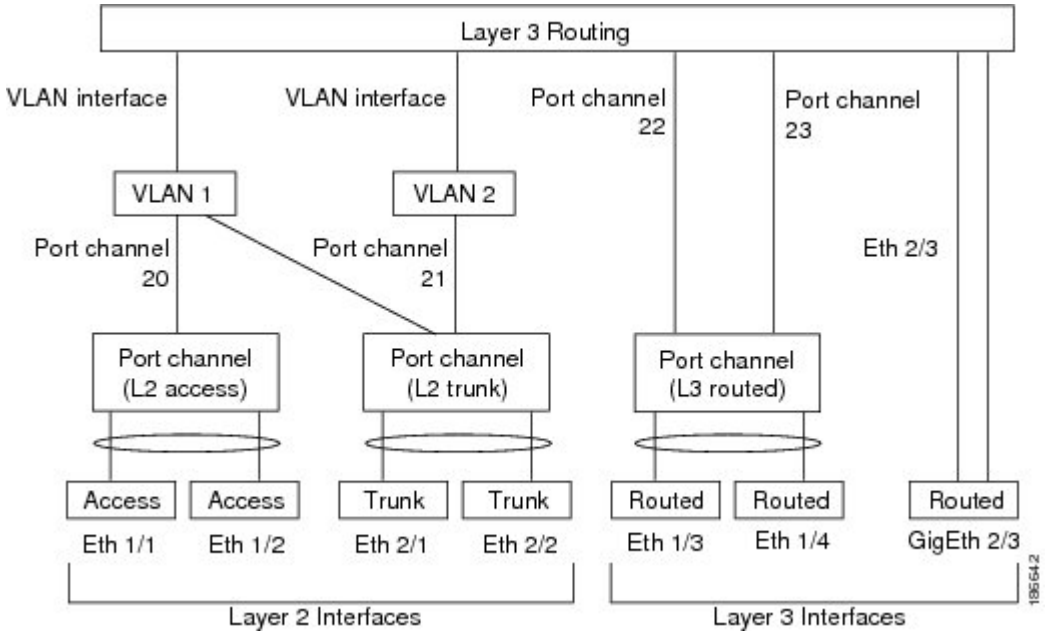
ポート チャネル インターフェイスを作成すると、ポート チャネルを直接作成できます。またはチャネル グループを作成して個別ポートをバンドルに集約させることができます。インターフェイスをチャネル グループに関連付けると、ポート チャネルがない場合は対応するポート チャネルが自動的に作成されます。この場合、ポート チャネルは最初のインターフェイスのレイヤ 2 またはレイヤ 3 設定を行います。最初にポート チャネルを作成することもできます。この場合は、Cisco NX-OS ソフトウェアがポート チャネルと同じチャネル番号の空のチャネル グループを作成してデフォルト レイヤ 2 またはレイヤ 3 設定を行い、互換性も設定します（「互換性要件」の項を参照）。ポート チャネル サブインターフェイスの作成および削除の詳細については、「レイヤ 3 インターフェイスの設定」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 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

以下の図に、ポート チャネル インターフェイスを示します。

図 *9*：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り、場合によってはサブインターフェイスもあります。

Cisco NX-OS Release 4.2(1) から、スタティック MAC アドレスを使用してレイヤ 3 ポート チャネルを設定できます。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 チャネルでのスタティック MAC アドレスの設定については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』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 ポートの設定については、「レイヤ 2 インターフェイスの設定」を、レイヤ 3 インターフェイスおよびサブインターフェイスの設定については、「レイヤ 3 インターフェイスの設定」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
- Duplex
- フロー制御
- IP アドレス：IPv4 および IPv6
- 最大伝送単位（MTU）
- 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。

- （リンク）速度性能
- Access VLAN
- 許可 VLAN リスト
- レート モードのチェック。
- 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
- レイヤ 3 ポート：サブインターフェイスは不可
- MTU サイズ
- メディア タイプ、銅線またはファイバ
- Module Type
- ネットワーク層
- ポート モード
- SPAN：SPAN の始点または宛先ポートは不可
- 速度設定

- ストーム制御
- タグ付きまたは非タグ付き
- トランク ネイティブ VLAN

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には、**show port-channel compatibility-parameters** 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（v4 および v6）
- MAC address
- スパニングツリー プロトコル
- NAC
- サービス ポリシー
- アクセス コントロール リスト（ACL）

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
- デバウンス
- UDLD
- MDIX
- レート モード
- シャットダウン
- SNMP トラップ

ポート チャネル インターフェイスにサブインターフェイスを設定し、ポート チャネルのメンバ ポートを削除すると、ポート チャネル サブインターフェイスの設定はメンバ ポートに伝わりません。

（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 モードについては、「LACP マーカー レスポンダ」の項を参照してください。

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、IP アドレス、またはレイヤ 4 ポート番号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およびポート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、デバイス全体または指定したモジュール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。モジュールごとの設定は、デバイス全体のロードバランシング設定よりも優先されます。デバイス全体に 1 つのロードバランシング モードを、指定したモジュールに別のモードを、さらに別の指定したモジュールに別の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。

（注） 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 アドレスです。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。チャネルグループ バンドルのインターフェイス間でロード バランシング方式を設定するには、**port-channel load-balance** コマンドを使用します。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方式は src-dst-ip です。このコマンドの追加情報については、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』を参照してください。

F1 シリーズ モジュールは、MAC アドレスに基づく非 IP トラフィックのロード バランシングはサポートしません。F1 シリーズ モジュールのポートがポート チャネルで使用され、非 IP トラフィックがポート チャネルで送信されると、レイヤ 2 トラフィックが故障する場合があります。Cisco NX-OS リリース 6.0(1) 以降では、ロード バランシングは F2 モジュールをサポートします。

次のいずれかの方式を使用するようにデバイスを設定し、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 MAC アドレス
- 送信元 MAC アドレス
- 送信元および宛先 MAC アドレス
- 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 TCP/UDP ポート番号
- 宛先 TCP/UDP ポート番号
- 送信元および宛先 TCP/UDP ポート番号

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。

（注） 仮想デバイス コンテキスト（VDC）ごとにポート チャネルを使用してロード バランシングを設定できません。この機能を設定する場合はデフォルト VDC であることが必要です。別の VDC からこの機能を設定しようとすると、システムはエラーを表示します。

ロードバランシングは、VDC とは無関係に、システム全体または特定のモジュールによって設定できます。ポートチャネルのロードバランシングは、すべての VDC にわたるグローバル設定です。

入トラフィックがマルチプロトコル ラベル スイッチング（MPLS）の場合、ソフトウェアはパケットの IP アドレスのラベルの下位部分を参照します。

マルチキャスト トラフィックは、ユニキャスト トラフィックと同じポート チャネル ロード バランシング設定を継承します。これは、システム全体のロード バランシング設定とモジュール固有のロード バランシング設定の両方に適用されます。

（注） Cisco IOS を実行しているデバイスは、 **port-channel hash-distribution** コマンドの入力により単一のメンバーで障害が発生した場合に、ASIC のメンバー ポートの動作を最適化することができます。Cisco Nexus 7000 シリーズ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であれ、モジュール単位であれ、**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。このコマンドについては、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』を参照してください。

Cisco NX-OS リリース 6.1(3) は、Cisco Nexus 7000 M シリーズ I/O XL モジュールと F シリーズ モジュールのポートチャネル メンバーのロード バランシングを改善するための新しい Result Bundle Hash（RBH）モードをサポートします。新しい RBH モジュロ モードでは、RBH の結果は、実際のポートチャネル メンバー数に基づきます。

対称ハッシュ

ポートチャネル上のトラフィックを効率的にモニタするには、ポートチャネルに接続された各インターフェイスがフォワードとリバースの両方のトラフィック フローを受信することが不可欠です。通常、フォワードとリバースのトラフィック フローが同じ物理インターフェイスを使用する保証はありません。ただし、ポート チャネルで対称ハッシュを有効にすると、双方向トラフィックが同じ物理インターフェイスを使用するように強制され、ポート チャネルの各物理インターフェイスが効果的に一連のフローにマッピングされます。

対称ハッシュが有効になっている場合、ハッシュに使用されるパラメータ（送信元と宛先の IP アドレスなど）は、ハッシュ アルゴリズムに入る前に標準化されます。このプロセスにより、パラメータがリバースされる（フォワード トラフィックの送信元がリバース トラフィックの宛先になる）場合にハッシュ出力が同じになることが保証されます。このため、同じインターフェイスが選択されます。

対称ハッシュをサポートするのは、次のロードバランシング アルゴリズムのみです。

- src ip
- dst ip rotate
- dst ip
- src ip rotate

- src-dst ip
- src ip-l4port
- dst ip-l4port rotate
- dst ip-l4port
- src ip-l4port rotate
- src-dst ip-l4port-vlan
- dst ip-vlan
- src ip-vlan rotate
- src-dst ip-vlan
- src l4port
- dst l4port rotate
- dst l4port
- src l4port rotate
- src-dst l4port
- src mac
- dst mac rotate
- dst mac
- src mac rotate
- src-dst mac

ランダム ロード バランシング（ポート チャネル）

ポート チャネル上のランダム ロード バランシングは、IP-UDP パケット経由の GPRS トンネリング プロトコル（GTP）のポート リンク帯域幅使用率を改善するソフトウェア ソリューションです。既存の M1、M2、F1、F2、および F2e ライン カード ハードウェアはランダム ロード バランシングを実行する機能を備えていないため、このソフトウェア ソリューションがロードバランシングとポート チャネル帯域幅の最適化を支援します。ランダム ロードバランシングは、F3 シリーズ ライン カードでのみサポートされます。また、ランダム ロード バランシングは、すべてのトラフィック タイプに適用可能で、レイヤ 3 トラフィックの出力ポートで効果的です。Cisco NX-OS ソフトウェアは、多項式スキームを使用することにより、ポート チャネル内のすべてのインターフェイス上ですべてのトラフィックのランダム ロード バランシングを実行します。

LACP

LACP では、最大 16 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。最大 8 個のインターフェイスをアクティブにでき、最大 8 個のインターフェイスを M シリーズ モジュールでスタンバイ状態にできます。

Cisco NX-OS リリース 5.1 以降では、F シリーズ モジュールのポート チャネルに最大 16 個のアクティブ リンクをバンドルすることができます。

LACP の概要

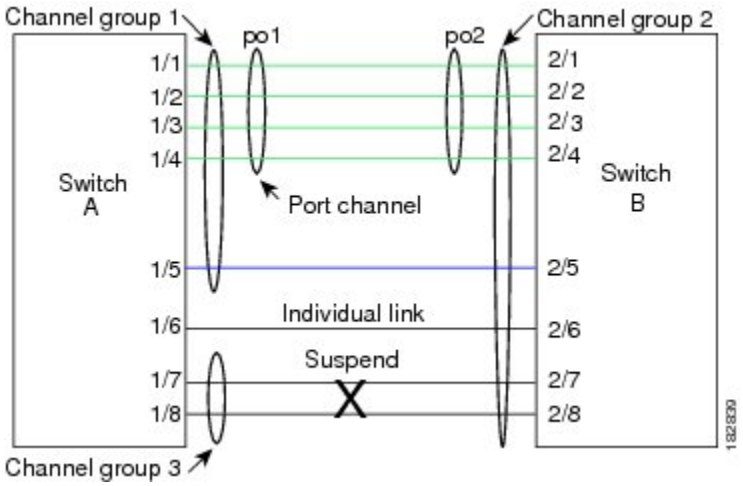
（注） LCAP は、使用する前にイネーブルにする必要があります。デフォルトでは、LACP はディセーブルです。

LACP のイネーブル化については、「LACP のイネーブル化」の項を参照してください。

Cisco NX-OS リリース 4.2 以降では、システムは機能のディセーブル化の前に自動的にチェックポイントを作成するため、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 7000 Series NX-OS System Management Configuration Guide*』を参照してください。

以下の図に、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方法を示します。

図 *10*：個別リンクをポート チャネルに組み込む



LACP では、最大 16 のインターフェイスを 1 つのチャネル グループにバンドルできます。チャネル グループのインターフェイスが 8 つよりも多い場合、残りのインターフェイスは、M シリーズ モジュール上のこのチャネル グループに関連付けられたポート チャネルのホット スタンバイとなります。

Cisco NX-OS リリース 5.1 以降では、F シリーズ モジュールのポート チャネルに最大 16 個のアクティブ リンクをバンドルすることができます。

（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いずれかのチャネル 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。

チャネル モード	説明
passive	LACP モード。ポートをパッシブ ネゴシエーション ステートにします。ポートは受信した LACP パケットには応答しますが、LACP ネゴシエーションは開始しません。
active	LACP モード。ポートをアクティブ ネゴシエーション ステートにします。ポートはLACPパケットを送信して、他のポートとのネゴシエーションを開始します。
on	すべてのスタティック ポート チャネル（LACP を実行していない）がこのモードです。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。 チャネルで LACP をイネーブルにするには、そのチャネルのインターフェイスでチャネル モードを active または passive に設定します。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。 デフォルトのポート チャネル モードは on 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、ポートは LACP ポート チャネルを形成できます。

- active モードのポートは、active モードの別のポートとともにポート チャネルを正しく形成できます。
- active モードのポートは、passive モードの別のポートとともにポート チャネルを形成できます。
- passive モードのポート同士ではポート チャネルを構成できません。これは、どちらのポートもネゴシエーションを開始しないためです。
- on モードのポートは LACP を実行しておらず、active または passive モードの別のポートとともにポート チャネルを形成できません。

LACP ID パラメータ

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。

システム ID は VDC ごとに異なります。

（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 マーカー レスポンダ

ポートチャネルを使用すればデータ トラフィックを動的に再配布できます。この再配布により、リンクが削除または追加されたり、ロードバランシング スキームが変更されることもあります。トラフィック フローの途中でトラフィックが再配布されると、フレームの秩序が乱れる可能性があります。

LACP は Marker Protocol を使って、再配布によってフレームが重複したり順番が入れ替わらないようにします。Marker Protocol は、所定のトラフィック フローのすべてのフレームがリモート エンドで正しく受信すると検出します。LACP は ポート チャネル リンクごとに Marker PDUS を送信します。リモート システムは、Marker PDU よりも先にこのリンクで受信されたすべてのフレームを受信すると、Marker PDU に応答します。リモート システムは次に Marker Responder を送信します。ポート チャネルのすべてのメンバ リンクの Marker Responder を受信したローカル システムは、トラフィック フローのフレームを正しい順序で再配分します。ソフトウェアは Marker Responder だけをサポートします。

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

以下の表に、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。

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	16	8

LACP 互換性の拡張

相互運用性の解決、およびLACPプロトコル収束の高速化のために複数の新しいコマンドがリリース 4.2(3) に追加されました。

Cisco Nexus 7000 シリーズのデバイスが非 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、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。これらの状況を解決するために、**lacp graceful-convergence** コマンドが追加されました。

デフォルトで、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。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。**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。

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。

Cisco NX-OS リリース 5.1 では、最小リンクおよび maxbundle 機能の導入により、LACP ポート チャネル動作がさらに改善し、1 台の管理対象インターフェイスの帯域幅が増加します。

LACP ポート チャネルの最少リンク数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 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 ポート数の上限を定義します。
- 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。

ファブリック エクステンダへの LACP オフロード

Cisco Nexus 7000 シリーズ デバイスのコントロール プレーンの負荷を軽減するために、Cisco NX-OS は、ファブリック エクステンダ CPU へのリンク レベルのプロトコル処理をオフロードする機能を適用します。この機能は、ファブリック エクステンダで設定された LACP ポート チャネルが少なくとも 1 つあると、デフォルトで LACP によってサポートされます。

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 レートを設定するには、「LACP 高速タイマー レートの設定」の項を参照してください。

ISSU およびステートフル スイッチオーバーは、LACP 高速タイマーでは保証できません。

FEX ファブリック ポート チャネルのリンクの最小数

デュアルホーム接続のホスト（アクティブ/スタンバイ）のネットワーク構成では、ファブリック ポート チャネルのリンクの最小数をサポートするように Cisco Nexus 2000 シリーズ ファブリック エクステンダ（FEX）を設定できます。

ファブリック ポート チャネル リンクの数が指定されたしきい値を下回ると、ホスト側の FEX インターフェイスがダウンし、ホストと FEX 間の接続の NIC スイッチオーバーが可能になります。FEX インターフェイスのスタンバイ FEX への自動リカバリは、ファブリック ポート チャネル リンクの数が指定したしきい値に到達するとトリガーされます。

仮想化のサポート

メンバー ポートと他のポート チャネルに関連する設定は、ポート チャネルとメンバー ポートを持つ仮想デバイス コンテキスト（VDC）で設定します。各 VDC で 1 ～ 4096 の番号を使ってポート チャネルに番号を設定できます。異なる VDC に同じポート チャネル番号を使用できます。たとえば、VDC1 にポート チャネル 100 を設定し、VDC2 の別のポート チャネルにも 100 を設定できます。

ただし、LACP システム ID は VDC ごとに異なります。LACP の詳細については、「LACP の概要」の項を参照してください。

（注） VDC およびリソース割り当ての詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

1 つのポート チャネルのすべてのポートは同じ VDC に置く必要があります。LACP を使用する場合、8 つすべてのアクティブ ポートと 8 つすべてのスタンバイ ポートは同じ VDC であることが必要です。ポート チャネルは 1 つの VDC から始まり（そのチャネルのすべてのポートが同じ VDC）、別の VDC のポート チャネルに対応します（この場合もそのチャネルのすべてのポートは同じ VDC）。

（注） ポートチャネリング ロード バランシング モードは、単一のモジュールまたはモジュール全体で動作します。デフォルト VDC のポート チャネルを使用するロード バランシングを設定する必要があります。指定した VDC のポート チャネルを使用してロード バランシングを設定することはできません。ロードバランシングの詳細については、「ポート チャネルを使用したロード バランシング」の項を参照してください。

ハイ アベイラビリティ

ポート チャネルは、複数のポートのトラフィックをロード バランシングすることでハイ アベイラビリティを実現します。物理ポートが故障した場合、ポート チャネルのメンバがアクティブであればポート チャネルは引き続き動作します。モジュール間の設定が共通しているため、異なるモジュールのポートをバンドルして、モジュール故障時にも動作するポート チャネルを作成できます。

ポート チャネルは、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。ステートフル再起動はスーパーバイザ切り替え時に発生します。切り替え後、Cisco NX-OS ソフトウェアは実行時の設定を適用します。

動作しているポート数が設定された最小リンク数を下回った場合、ポート チャネルはダウンします。

（注） ハイ アベイラビリティ機能の詳細については、『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

インターフェイスのライセンス要件

vPC には、ライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

IP トンネルには Enterprise Services ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『Cisco NX-OS Licensing Guide』を参照してください。

他のインターフェイスにはライセンスが必要ありません。

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。
- 必要に応じて、Advanced Services ライセンスをインストールし、特定の VDC を開始します。
- チャネル グループのすべてのポートが同じ VDC にある必要があります。
- 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。互換性要件の詳細については、「互換性要件」の項を参照してください。
- デフォルト VDC のロード バランシングを設定すること。

注意事項と制約事項

ポート チャネリング設定時の注意事項および制約事項は、次のとおりです。

- 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 パラメータの設定」を参照）。
- 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。互換性要件の詳細については、「互換性要件」の項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。
- ポートチャネルにポートを追加する前に、ポートセキュリティ情報をそのポートから削除しておく必要があります。同様に、チャネル グループのメンバであるポートにポートセキュリティ情報を追加できません。
- ポート チャネル グループに属するポートはプライベート VLAN ポートとして設定しないでください。ポートがプライベート VLAN の設定に含まれている間は、そのポート チャネルの設定は非アクティブになります。

- チャネル メンバ ポートを発信元または宛先 SPAN ポートにできません。
- F1 および M1 シリーズのラインカードからのポートを同一のポート チャネルに設定できません。ポートが互換性要件を満たしていないためです。
- M1 および M2 シリーズのラインカードからのポートを同一のポート チャネルに設定できません。
- F2e および F3 シリーズのラインカードからのポートを同一のポート チャネルに設定できません。ポートが互換性要件を満たしていないためです。
- Cisco NX-OS リリース 5.1 以降では、最大 16 個のアクティブ リンクを F1 シリーズ ライン カードのポート チャネルにバンドルすることができます。
- F1 シリーズ モジュールは、MAC アドレスに基づく非 IP トラフィックのロード バランシングはサポートしません。F1 シリーズ モジュールのポートがポート チャネルで使用され、非 IP トラフィックがポート チャネルで送信されると、レイヤ 2 トラフィックが故障する場合があります。
- F シリーズと XL タイプの M シリーズ モジュールのみが RBH モジュロ モードをサポートします。
- ポート チャネル上のランダム ロード バランシングは、F3 シリーズ ライン カードでのみサポートされます。ポート チャネルの両側が F3 ライン カードだけであることを確認します。

デフォルト設定

表 *14*：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
RBH モジュロ モード	ディセーブル
LACP	ディセーブル
Channel mode	on
LACP システム プライオリティ	32768

パラメータ	デフォルト
LACP ポート プライオリティ	32768
LACP の最小リンク	1
Maxbundle	16
FEX ファブリック ポート チャネル用最少リンク数	1
ランダム ロード バランシング（ポート チャネル）	ディセーブル

ポート チャネルの設定

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。

はじめる前に

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。

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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)# **interface port-channel***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。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	switch(config-if)# **show port-channel summary**	ポート チャネル情報を表示します。
ステップ 4	switch(config-if)# **show interface status error policy** [**detail**]	（任意） ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーが

	コマンドまたはアクション	目的
		ハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ 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 6	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。

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*	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。

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にインターフェイス設定がどのように変わるかの詳細については、「互換性要件」の項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。

はじめる前に

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。

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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	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 port-channel***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。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	switch(config-if)# **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	switch(config-if)# **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	switch(config-if)# **switchport trunk** {**allowed vlan***vlan-id* | **native***vlan-id*}	（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。
ステップ 6	switch(config-if)# **channel-group***channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]	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。 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。 （注） force オプションは、ポートにポート チャネルの他のメンバーとの QoS ポリシーの不一致がある場合に失敗します。
ステップ 7	switch(config-if)# **show interface***type slot/port*	（任意） 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 8	switch(config-if)# **show interface status error policy** [**detail**]	（任意） ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ 9	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 10	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。

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	チャネル グループからポートを削除します。

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。また、既存のレイヤ 3 ポート チャネルにサブインターフェイスを追加できます。

はじめる前に

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。

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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	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 port-channel***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。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	switch(config-if)# **no 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	switch(config-if)# **channel-group***channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]	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。 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	switch(config-if)# **show interface***type slot/port*	（任意） インターフェイス情報を表示します。
ステップ 6	switch(config-if) **show interface status error policy** [**detail**]	（任意） ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。

	コマンドまたはアクション	目的
		エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ **7**	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**	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。

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	チャネル グループからポートを削除します。

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)# no 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	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 port-channel***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	switch(config-if)# **bandwidth***value*	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 ～ 80,000,000 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	switch(config-if)# **delay***value*	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。 （注） Cisco リリース 4.2(1) より前は、デフォルトの遅延値が 100 マイクロ秒でした。
ステップ 5	switch(config-if)# **exit**	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	switch(config)# **show interface port-channel***channel-number*	（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 7	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。

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上ダウンします。

手順

	コマンドまたはアクション	目的
ステップ 1	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 port-channel***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	switch(config-if)# **shutdown** | **no shutdown**	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。 **no shutdown** コマンドはインターフェイスを開きます。インターフェイスは管理的にアップとなります。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	switch(config-if)# **exit**	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	switch# **show interface port-channel***channel-number*	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	switch# **show interface status error policy** [**detail**]	（任意） ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ 7	switch# **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	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。

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	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 port-channel***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。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	switch(config-if)# **description**	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	switch(config-if)# **exit**	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	switch(config-if)# **show interface port-channel***channel-number*	（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	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。

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
```

ポート チャネル インターフェイスへの速度とデュプレックスの設定

ポート チャネル インターフェイスに速度とデュプレックスを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	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 port-channel***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	switch(config-if)# **speed** {**10** | **100** | **1000** | **auto**}	ポートチャネル インターフェイスの速度を設定します。デフォルトの自動ネゴシエーションは自動です。
ステップ 4	switch(config-if)# **duplex** {**auto** | **full** | **half**}	ポート チャネル インターフェイスのデュプレックスを設定します。デフォルトの自動ネゴシエーションは自動です。
ステップ 5	switch(config-if)# **exit**	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	switch# **show interface port-channel***channel-number*	（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 7	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。

次に、ポート チャネル 2 に 100 Mb/s を設定する例を示します。

```
switch# configure terminal
switch (config)# interface port-channel 2
switch(config-if)# speed 100
```

フロー制御の設定

1 Gb 以上で動作するポート チャネル インターフェイスのフロー制御ポーズ パケットの送信および受信機能をイネーブルまたはディセーブルにできます。より低速で動作するポートチャネルインターフェイスでは、ポートチャネルインターフェイスのポーズパケット受信機能だけをイネーブルまたはディセーブルにできます。

（注） この設定が正しく動作するには、フロー制御リンクのローカルおよびリモート エンドの両方で一致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	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 port-channel***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	switch(config-if)# **flowcontrol** {**receive** | **send**} {**desired** | **off** | **on**}	フロー制御パラメータを設定して、ポート チャネル インターフェイスのポーズ パケットを送信および受信します。デフォルトは [desired] です。
ステップ 4	switch(config-if)# **exit**	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	switch# **show interface port-channel***channel-number*	（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	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。

次に、ポート チャネル グループ 2 にポート チャネル インターフェイスを設定してポーズ パケットを送信および受信する例を示します。

```
switch# configure terminal
switch(config)# interface port-channel 2
switch(config-if)# flowcontrol receive on
switch(config-if)# flowcontrol send on
```

ポート チャネルを使ったロード バランシングの設定

VDC アソシエーションにかかわらず、ポート チャネルのロードバランシング アルゴリズムを設定し、デバイス全体または 1 のモジュールだけに適用できます。モジュールベースのロード バランシングは、デバイスベースのロード バランシングに優先します。

はじめる前に

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。

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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)# [**no**] **port-channel load-balance***method* {**dst ip** | **dst ip-l4port-vlan** | **dst ip-vlan** | **dst mac** | **dst l4port** | **dst ip-l4port** | **src-dst ip** | **src-dst mac** | **src-dst l4port** | **src-dst ip-l4port** | **src-dst ip-vlan** | **src-dst ip-l4port-vlan** | **src ip** | **src ip-l4port-vlan** | **src ip-l4port** | **src ip-vlan** | **src mac** | **src l4port** | **hash-modulo** [**force**]} [**gtp-teid**] [**module***module-number* | **fex** {*fex-range* | **all**}] [**asymmetric**] [**rotate***rotate*]	デバイスまたはモジュールのロード バランシング アルゴリズムを指定します。指定可能なアルゴリズムはデバイスによって異なります。レイヤ 3 のデフォルトは IPv4 と IPv6 の両方で **src-dst ip** で、非 IP のデフォルトは **src-dst mac** です。 （注） **asymmetric** キーワードは、**src-dst ip** コマンドおよび F2 または F2e モジュールでのみ有効です。F2 または F2e モジュールはデフォルトで対称になるため、**asymmetric** キーワードにより双方向フロー時に発生するトラフィック ドロップを防止します。F2 または F2e モジュールをイネーブルにする必要があるという警告メッセージが表示されます。これにより、ロードバランシングが改善し、システムの中断を回避できます。 デフォルトのシステム設定（対称）に戻るには、**no port-channel load-balance src-dst mac asymmetric** コマンドを使用します。 （注） モジュールベースの設定がすでに存在する場合は、それがデフォルトのシステム設定よりも優先されます。 システム レベルの設定（対称）に戻るには、モジュール レベルで **no port-channel load-balance src-dst mac asymmetric module** コマンドを使用します。 （注） **module**、**asymmetric**、および **rotate** の各キーワードは、**hash-modulo** コマンドに使用できません。 **gtp-teid** キーワードが GTP ヘッダー フィールドを含むパケット内で指定された場合は、選択されるポート チャネル メンバーが、MAC アドレス、IP アドレス、L4 ポートなどのすでに指定されたパケット ヘッダー フィールドだけでなく、32 ビット トンネル エンドポイント ID（TEID）ヘッダー フィールドにも依存します。パケットは、TEID ヘッダー フィールドがポート チャネル ロード バランシングで使用されるように M3 モジュール上のポートに入る必要があります。 **gtp-teid** キーワードがパケット内で指定された場合は、そのパケットの TEID ヘッダー フィールドがポート チャネル メンバーの選択で使用されます。ただし、パケットに IPv4 または IPv6 ヘッダー フィールド、宛先ポート 2152 の UDP ヘッダー

	コマンドまたはアクション	目的
		フィールド、プロトコル タイプ 1 の GTP バージョン 1 ヘッダーフィールドが、この順で含まれている場合に限られます。他のすべての GTP ヘッダー フィールドは、GTP 制御メッセージと見なされます。GTP エンドポイント間のネットワーク上の GTP 制御メッセージの並べ替えを回避するために、NX-OS は、チャネル メンバーの選択に GTP 制御メッセージの TEID ヘッダー フィールドを含めません。 （注） **gtp-teid** キーワードは、M3 モジュール上でのみサポートされ、他のモジュールの動作に影響を与えません。
ステップ 3	**show port-channel load-balance**	（任意） ポート チャネル ロードバランシング アルゴリズムを表示します。
ステップ 4	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。

非 IP トラフィック用の src-dst mac と IP トラフィック用の src-dst ip のデフォルトのロードバランシング アルゴリズムを復元するには、**no port-channel load-balance** コマンドを使用します。

コマンド	目的
no port-channel load-balance	デフォルトのロード バランシング アルゴリズムを復元します。

次に、モジュール 5 のポート チャネルに発信元 IP ロードバランシングを設定する例を示します。

```
switch# configure terminal
switch(config)# port-channel load-balance src-ip-l4port module 5
```

次の例では、スイッチ 1 とスイッチ 2 に接続されたポート チャネルの対称ポート チャネル ロード バランシングのためのさまざまな組み合わせを設定する方法を示します。

次の設定の組み合わせに示すものと同じ **rotate** *rotate-value* を使用してください。

```
 ! Configure port-channel hash distribution at the global level!

switch1(config)# port-channel hash-distribution fixed
Switch2(config)# port-channel hash-distribution fixed


! Configure symmetric port-channel load balancing combinations on both
switch1 and switch2 of a port channel.!

!Combination 1!
```

```
switch1(config)# port-channel load-balance src ip
Switch2(config)# port-channel load-balance dst ip rotate 4

!Combination 2!

switch1(config)# port-channel load-balance dst ip
Switch2(config)# port-channel load-balance src ip rotate 4

!Combination 3!

switch1(config)# port-channel load-balance src ip-l4port
Switch2(config)# port-channel load-balance dst ip-l4port rotate 6

!Combination 4!

switch1(config)# port-channel load-balance dst ip-l4port
Switch2(config)# port-channel load-balance src ip-l4port rotate 6

!Combination 5!

switch1(config)# port-channel load-balance src ip-l4port vlan
Switch2(config)# port-channel load-balance dst ip-l4port rotate 8

!Combination 6!

switch1(config)# port-channel load-balance dst ip-l4port vlan
Switch2(config)# port-channel load-balance src ip-l4port rotate 8

!Combination 7!

switch1(config)# port-channel load-balance src ip-vlan
Switch2(config)# port-channel load-balance dst ip-vlan rotate 8

!Combination 8!

switch1(config)# port-channel load-balance dst ip-vlan
Switch2(config)# port-channel load-balance src ip-vlan rotate 8

!Combination 9!

switch1(config)# port-channel load-balance src l4port
Switch2(config)# port-channel load-balance dst l4port rotate 2

!Combination 10!

switch1(config)# port-channel load-balance dst l4port
Switch2(config)# port-channel load-balance src l4port rotate 2

!Combination 11!

switch1(config)# port-channel load-balance src mac
Switch2(config)# port-channel load-balance dst mac rotate 6

!Combination 12!

switch1(config)# port-channel load-balance dst mac
Switch2(config)# port-channel load-balance src mac rotate 6
```

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。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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)# **feature lacp**	デバイスの LACP をイネーブルにします。
ステップ 3	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。

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。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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)# **interface port-channel***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	switch(config-if)# **channel-group***number***mode** {**active** | **on** | **passive**}	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。 デフォルトのポート チャネル モードは on です。
ステップ 4	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	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。

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

Cisco NX-OS リリース 5.1 では、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。

はじめる前に

適切なポートチャネル 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	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 port-channel***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	switch(config-if)# **lacp min-links***number*	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、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。指定できる範囲は 1 ～ 16 です。
ステップ 4	switch(config-if)# **show running-config interface port-channel***number*	（任意） ポートチャネル最少リンク数コンフィギュレーションを表示します。

デフォルトのポートチャネル最小リンク設定を復元するには、**no lacp min-links** コマンドを使用します。

コマンド	目的
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。

次に、モジュール 3 のポート チャネル 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)# lacp min-links 3
```

LACP ポートチャネル MaxBundle の設定

Cisco NX-OS リリース 5.1 では、LACP 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。

はじめる前に

適切なポートチャネル 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	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 port-channel***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	switch(config-if)# **lacp max-bundle***number*	ポートチャネル インターフェイスを指定して、max-bundle 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。 ポート チャネルの max-bundle のデフォルト値は 16 です。指定できる範囲は 1 ～ 16 です。 （注） デフォルト値は 16 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	switch(config-if)# **show running-config interface port-channel***number*	（任意） ポートチャネル最少リンク数コンフィギュレーションを表示します。

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	デフォルトのポートチャネル max-bundle 設定を復元します。

次に、モジュール 3 のポート 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)# 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。In-Service Software Upgrade（ISSU）およびステートフル スイッチオーバー（SSO）は、LACP 高速レート タイマーではサポートされません。

はじめる前に

LACP 機能がイネーブルになっていることを確認します。

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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)# **interface port-channel***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	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。 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。

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。

複数の VDC のシステム プライオリティ値を同じ設定に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	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)# **lacp system-priority***priority*	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。 （注） VDC ごとに LACP システム ID が異なります。これは、この設定値に MAC アドレスが追加されるためです。
ステップ 3	switch(config)# **show lacp system-identifier**	（任意） LACP システム識別子を表示します。
ステップ 4	switch(config)# **show running-config interface port-channel***number*	（任意） ポートチャネル最少リンク数コンフィギュレーションを表示します。

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。

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 port-channel***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	switch(config-if)# **lacp port-priority***priority*	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。
ステップ 4	switch(config-if)# **show running-config interface port-channel***number*	（任意） ポートチャネル最少リンク数コンフィギュレーションを表示します。

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 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） コマンドが実行される前に、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。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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	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 port-channel***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	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	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	switch(config-if)# **no shutdown**	ポート チャネルを管理的にアップします。
ステップ 6	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。

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	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 port-channel***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。

	コマンドまたはアクション	目的
ステップ 3	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	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	switch(config-if)# **no shutdown**	ポート チャネルを管理的にアップします。
ステップ 6	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。

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。このプロセスによって、サーバの中には起動に失敗するものがあります。そのようなサーバは、LACP が論理的にポートを稼働状態にしていることを必要とするからです。

（注） エッジ ポートで lacp suspend-individual コマンドを入力するだけです。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。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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	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)# **interface port-channel***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	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	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	switch(config-if)# **no shutdown**	ポート チャネルを管理的にアップします。
ステップ 6	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。

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	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 port-channel***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	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	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。

	コマンドまたはアクション	目的
ステップ 5	switch(config-if)# **no shutdown**	ポート チャネルを管理的にアップします。
ステップ 6	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。

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
```

ポート チャネル ハッシュ分散の設定

Cisco NX-OS リリース 6.1(1) 以降、ハッシュ分散のアダプティブおよび固定設定は、グローバル レベルおよびポートチャネル レベルの両方でサポートされます。このオプションは、メンバがアップまたはダウンしたときに Result Bundle Hash（RBH）分散の変化を最小限に抑えることにより、トラフィックの中断を最小限に抑えます。このため、変化のない RBH 値にマッピングされているフローが同じリンクを流れ続けるようになります。ポートチャネル レベルの設定はグローバル設定よりも優先されます。デフォルト設定はグローバルに適応し、各ポート チャネルの設定がないので、ISSU 中に変更はありません。コマンドが適用されたときにポートはフラップされず、設定は次のメンバー リンクの変更イベントで有効になります。どちらのモードも RBH モジュールまたは非モジュール スキームで動作します。

この機能がサポートされない下位バージョンへの ISSD 時には、固定モード コマンドがグローバルに使用されている場合や、ポートチャネル レベルの設定がある場合は、この機能を無効にする必要があります。

グローバル レベルでのポート チャネル ハッシュ分散の設定

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)# **no port-channel hash-distribution** {**adaptive** | **fixed**}	グローバル レベルでポート チャネル ハッシュ分散を指定します。 デフォルトはアダプティブ モードです。

	コマンドまたはアクション	目的
		コマンドは、次のメンバー リンク イベント（link down/up/no shutdown/shutdown）まで有効になりません。Do you want to continue (y/n) ? [yes]
ステップ 3	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。

次に、グローバル レベルでハッシュ分散を設定する例を示します。

```
switch# configure terminal
switch(config)# no port-channel hash-distribution fixed
```

ポート チャネル レベルでのポート チャネル ハッシュ分散の設定

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 port-channel** {*channel-number* | *range*}	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)# **no port-channel hash-distribution** {**adaptive** | **fixed**}	グローバル レベルでポート チャネル ハッシュ分散を指定します。 デフォルトはアダプティブ モードです。 コマンドは、次のメンバー リンク イベント（link down/up/no shutdown/shutdown）まで有効になりません。Do you want to continue (y/n) ? [yes]
ステップ 4	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。

次に、グローバル レベル コマンドとしてハッシュ分散を設定する例を示します。

```
switch# configure terminal
switch(config)# no port-channel hash-distribution fixed
```

RBH モジュロ モードの設定

RBH モジュロ モードをイネーブルにすると、すべてのポート チャネルがフラップされます。

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)# **port-channel load-balance hash-modulo**	RBH モジュロ モードをイネーブルにします。このコマンドはすべてのポート チャネルを再初期化するため、続行するか、続行しないかのオプションがあります。 （注） このコマンドは、現在のシステム全体のモジュール タイプが M1 シリーズ モジュールを含む場合に拒否されます。システム全体の設定から M1 シリーズ モジュール タイプを削除するには、**system module-type f1, f2, m1xl, m2xl** コマンドを入力します。
ステップ 3	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。

次に、RBH モジュロ モードをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# port-channel load-balance hash-modulo
```

FEX ファブリック ポート チャネルの最小リンクの設定

Cisco NX-OS リリース 6.1(3) 以降では、FEX ファブリック ポート チャネルのリンクの最小数を設定して、一定数の FEX ファブリック ポートチャネル メンバ ポートがダウンすると、FEX のホスト側のインターフェイスが中断するようにできます。

はじめる前に

適切なポートチャネル 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	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 port-channel***number*	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	switch(config-if)# **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	switch(config-if)# **switchport mode fex-fabric**	外部ファブリック エクステンダをサポートするように、ポート チャネルを設定します。
ステップ 5	switch(config-if)# [**no**] **port-channel min-links***number*	FEX ファブリック ポート チャネルのリンクの最小数を設定します。指定できる範囲は 1 ～ 16 です。
ステップ 6	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 7	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。

次に、FEX ファブリック ポート チャネルのリンクの最小数を設定する例を示します。

```
switch# configure terminal
switch(config)# interface port-channel 100
switch(config-if)# switchport
switch(config-if)# switchport mode fex-fabric
switch(config-if)# port-channel min-links 3
switch(config-if)# show port-channel summary
Flags: D - Down P - Up in port-channel (members) I - Individual
H - Hot-standby (LACP only) s - Suspended r - Module-removed
S - Switched R - Routed U - Up (port-channel)
M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port- Type Protocol Member Ports Channel
--------------------------------------------------------------------------------
101 Po101(SM) Eth NONE Eth10/46(P) Eth10/47(P) Eth10/48(P)
```

ランダム ロード バランスの設定

ポート チャネル上でのランダム ロード バランスの設定

手順

ステップ 1 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。
switch# **configure terminal**

ステップ 2 インターフェイス ポート チャネルを設定します。
switch(config)# **interface port-channel** *port-channel-number*

ステップ 3 ポート チャネル インターフェイスのランダム ロード バランスを設定します。ランダム ロード バランス機能を無効にするには、次のコマンドの **no** 形式を使用します。
switch(config-if)# **egress port-channel load-balance random**

（注） これにより、デフォルトのシステムまたはモジュール全体のポート チャネル ロード バランス設定がオーバーライドされます。入力トラフィックのランダム ロード バランシングを設定するには、レイヤ 3 上のスイッチ仮想インターフェイス（SVI）で **egress port-channel load-balance random** コマンドを設定します。

次の作業

- ランダム ロード バランス設定の確認

インターフェイス上でのランダム ロード バランスの設定

手順

ステップ 1 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。
switch# **configure terminal**

ステップ 2 ポート チャネル インターフェイスを設定します。
switch(config)# **interface** *interface-name*

ステップ 3 インターフェイスのランダム ロード バランスを設定します。ランダム ロード バランス機能を無効にするには、次のコマンドの **no** 形式を使用します。
switch(config-if)# **egress port-channel load-balance random**

（注） 入力レイヤ 3 インターフェイスまたはポート チャネル インターフェイスは、レイヤ 2 またはレイヤ 3 出力インターフェイスとポート チャネル インターフェイス上で、ランダム ロード バランスを実行します。

単一の物理インターフェイスでのランダム ロード バランスの設定は、トラフィックが入力レイヤ 3 インターフェイスに入って、ポート チャネル インターフェイスから出るシナリオに有効です。

次の作業

- ランダム ロード バランス設定の確認

VLAN のランダム ロード バランスの設定

手順

ステップ 1 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。
switch# **configure terminal**

ステップ 2 VLAN を設定します。
switch(config)# **vlan** *vlan-id*

ステップ 3 VLAN コンフィギュレーション モードを開始します。
switch(config-vlan)# **vlan configuration** *vlan-id*

ステップ 4 VLAN のランダム ロード バランスを設定します。ランダム ロード バランス機能を無効にするには、次のコマンドの **no** 形式を使用します。
switch(config-if)# **egress port-channel load-balance random**

（注） ランダム ロード バランスは、VLAN 上のすべてのレイヤ 2 入力インターフェイスに適用されます。入力インターフェイスは、すべてのレイヤ 2 またはレイヤ 3 ポート チャネル出力インターフェイス上でランダム ロード バランスを実行します。

次の作業

- ランダム ロード バランス設定の確認

SVI のランダム ロード バランスの設定

手順

ステップ 1 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。

switch# **configure terminal**

ステップ 2 スイッチ仮想インターフェイス（SVI）を設定します。
switch(config)# **vlan** *vlan-range*

ステップ 3 VLAN コンフィギュレーション モードを開始します。
switch(config)# **vlan configuration** *vlan-range*

ステップ 4 入力トラフィック用の SVI のランダム ロード バランスを設定します。ランダム ロード バランス機能を無効にするには、次のコマンドの **no** 形式を使用します。
switch(config-vlan-config)# **egress port-channel load-balance random**

次の作業

- ランダム ロード バランス設定の確認

例：ランダム ロード バランスの設定

ポート チャネル上でのランダム ロード バランスの設定

次の例では、ポート チャネル インターフェイス上でランダム ロード バランスを設定する方法を示します。

```
configure terminal
    interface port-channel 44
       egress port-channel load-balance random
```

インターフェイス上でのランダム ロード バランスの設定

次の例では、物理インターフェイス上でランダム ロード バランスを設定する方法を示します。

```
configure terminal
    interface Ethernet6/1
       egress port-channel load-balance random
```

VLAN のランダム ロード バランスの設定

次の例では、VLAN 上でランダム ロード バランスを設定する方法を示します。

```
configure terminal
    vlan 100
       vlan configuration 100
         egress port-channel load-balance random
```

スイッチ仮想インターフェイスのランダム ロード バランスの設定

次の例では、入力トラフィック用のスイッチ仮想インターフェイス（SVI）上でランダム ロード バランスを設定する方法を示します。

```
configure terminal
    vlan 2-10
    vlan configuration 2-10
       egress port-channel load-balance random
```

ポート チャネル設定の確認

ポート チャネル設定情報を表示する場合は、次のコマンドを使用します。

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。
load-interval {**interval***seconds* {**1** | **2** | **3**}}	Cisco Nexus 7000 シリーズ デバイスの Cisco NX-OS Release 4.2(1) から、3 種類のサンプリング間隔をビットレートおよびパケットレートの統計情報に設定します。
show port-channel compatibility-parameters	ポート チャネルに追加するためにメンバ 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 [**interfaceport-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。

コマンド	目的
show interface status error policy [**detail**]	ハードウェア ポリシーと矛盾するインターフェイスおよび VLAN のエラーを表示します。 **detail** コマンドを使用すると、エラーを受信するインターフェイスおよびVLANの詳細を表示できます。

これらのコマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』を参照してください。

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。
load-interval {**interval***seconds* {**1** | **2** | **3**}}	Cisco Nexus 7000 シリーズ デバイスの Cisco NX-OS Release 4.2(1) から、3 種類のサンプリング間隔をビットレートおよびパケットレートの統計情報に設定します。
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。
show interface counters errors [**module***module*]	エラー パケットの数を表示します。
show lacp counters	LACP の統計情報を表示します。

これらのコマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』を参照してください。

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 2/5
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
『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/interfaces/command/reference/if_cmds.html
『*Interfaces Configuration Guide, Cisco DCNM for LAN*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/dcnm/interfaces/configuration/guide/if_dcnm.html
『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/system_management/configuration/guide/sm_nx_os_cg.html
『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/high_availability/configuration/guide/b_Cisco_Nexus_7000_Series_NX-OS_High_Availability_and_Redundancy_Guide.html

関連項目	マニュアル タイトル
『*Cisco Nexus 2000 Series NX-OS Fabric Extender Software Configuration Guide for Cisco Nexus 7000 Series Switches, Release 6.x*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus2000/sw/configuration/guide/rel_6_1/b_Cisco_Nexus_2000_Series_NX-OS_Fabric_Extender_Software_Configuration_Guide_Release_6-x.html
『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/virtual_device_context/configuration/guide/b-7k-Cisco-Nexus-7000-Series-NX-OS-Virtual-Device-Context-Configuration-Guide.html
『*Cisco NX-OS Licensing Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/licensing/guide/b_Cisco_NX-OS_Licensing_Guide.html
VLAN、MAC アドレス テーブル、プライベート VLAN、およびスパニング ツリー プロトコル。 『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/layer2/configuration/guide/b_Cisco_Nexus_7000_Series_NX-OS_Layer_2_Switching_Configuration_Guide.html
『*Cisco Nexus 7000 Series NX-OS FabricPath Command Reference*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/fabricpath/command/reference/fp_cmd_book.html
『*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/fabricpath/configuration/guide/b-Cisco-Nexus-7000-Series-NX-OS-FP-Configuration-Guide-6x.html
『Cisco Nexus 7000 Series NX-OS Release Notes』	http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-release-notes-list.html

標準

標準	タイトル
IEEE 802.3ad	—

MIB

MIB	MIB のリンク
• IEEE8023-LAG-CAPABILITY • CISCO-LAG-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

第 8 章

vPC の設定

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

vPC の設定機能の履歴

この表には、機能の追加や変更によるリリースの更新内容のみが記載されています。

表 *15*：*vPC* の設定機能の履歴

機能名	リリース	機能情報
M3 モジュール上の vPC サポート	7.3(0)DX(1)	M3 モジュール上の vPC に対するサポートが追加されました。
ヒットレス vPC ロールの変更	7.3(0)D1(1)	トラフィック フローに影響を与えずに vPC ロールを切り替えるためのサポートが追加されました。
vPC シャットダウン	7.2(0)D1(1)	ピアをシャットダウンして、デバッグ、リロード、または vPC コンプレックスからの物理的な削除のために分離し、ピア vPC スイッチがプライマリ ピアとして引き継ぐようにする **shutdown** コマンドが追加されました。
F3 上の物理ポート vPC	7.2(0)D1(1)	F3 上の物理ポート vPC に対するサポートが追加されました。
FEX 用の 1500 ホスト vPC（FEX 上の物理ポート vPC）	7.2(0)D1(1)	FEX 用の 1500 ホスト vPC（FEX 上の物理ポート vPC）に対するサポートが追加されました。
vPC 設定の同期化	7.2(0)D1(1)	vPC 設定同期機能は、あるスイッチの設定を別の類似スイッチに自動的に同期します。
F2E および F3 モジュール用の vPC 経由のレイヤ 3	7.2(0)D1(1)	この機能のサポートが追加されました。
F2 上の物理ポート vPC	6.2(6)	F2 上の物理ポート vPC に対するサポートが追加されました。
LAN シャットダウン	6.2(6)	この機能をサポートするための **shutdown lan** コマンドが追加されました。
物理ポート vPCs を介した FCoE	6.2(6)	この機能のサポートが追加されました。

機能名	リリース	機能情報
物理ポート vPC	6.2(6)	vPC ピアデバイスの物理インターフェイス上の物理ポート vPC に対するサポートが追加されました。
vPC	6.2(2)	vPC の特定のコマンドを同時にイネーブルにするための **mode auto** コマンドが追加されました。
vPC	6.1(3)	両方の vPC パスがアップしているときに 2 つのピアが部分的に指定フォワーダになることを許可する **multicast load-balance** コマンドが追加されました。
vPC	5.2(1)	サポートが 528 vPC にまで増えました。
vPC	5.2(1)	vPC で障害が発生したときに vPC セカンダリデバイスの孤立ポートを一時停止するための **vpc orphan-ports suspend** コマンドが追加されました。
vPC	5.2(1)	停電後に vPC リカバリのスピードと信頼性を高めるための **auto-recovery** コマンドが追加されました。**reload restore** コマンドが非推奨になりました。
vPC	5.2(1)	矛盾した設定の VLAN だけが一時停止されるように VLAN 単位整合性検査が追加されました。
vPC	5.2(1)	矛盾した設定がピア間で検出されたときに、vPC プライマリ デバイスがトラフィックを転送することを可能にする **graceful consistency-check** コマンドが追加されました。
vPC	5.0(2)	一対の vPC スイッチがレイヤ 2 トポロジ内で 1 つの STP ルートとして現れることを可能にする **peer-switch** コマンドが追加されました。

機能名	リリース	機能情報
vPC	5.0(2)	vPC スイッチ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する **reload restore** コマンドが追加されました。
vPC	4.2(1)	リロード後にルーティング テーブルが収束できるまで vPC セカンダリ デバイスの稼働を遅延させるための **delay restore** コマンドが追加されました。
vPC	4.2(1)	vPC ピア リンクに障害が発生しても、確実に VLAN インターフェイスが稼働したままになるようにするために、**dual-active exclude interface-vlan** コマンドが追加されました。
vPC	4.2(1)	確実にすべてのパケットがデバイスのゲートウェイ MAC アドレスを使用するようにするために、**peer-gateway** コマンドが追加されました。
vPC	4.2(1)	サポートが 256 vPC にまで増えました。
vPC	4.1(4)	サポートが 192 vPC にまで増えました。
vPC	4.1(2)	これらの機能が導入されました。

vPC の設定

この章では、Cisco NX-OS デバイス上で仮想ポート チャネル（vPC）を設定する方法を説明します。

（注） Cisco NX-OS リリース 5.1(1) 以降では、vPC は FabricPath と相互運用するように機能強化されました。FabricPath ネットワークで vPC を設定するには、『*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*』を参照してください。

Cisco NX-OS リリース 5.1(1) 以降では、個々のスイッチの vPC ピア リンクに対し F シリーズ モジュールでは 10 ギガビット イーサネット（10GE）インターフェイス以上を、または M シリーズ モジュールでは 10 ギガビット イーサネット インターフェイス以上を使用できますが、F モジュール上のメンバ ポートを M モジュール上のポートと組み合わせて単一スイッチ上の単一ポート チャ

ネルにすることはできません。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。共有インターフェイスの詳細については、『*Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*』を参照してください。

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 ポートでも同じでなければならないので、シャーシごとに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

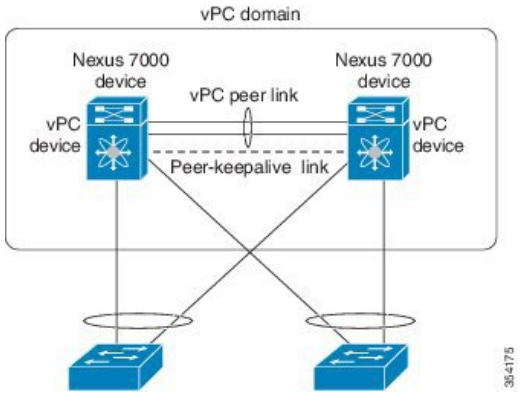
仮想ポート チャネル（vPC）は、物理的には 2 台の異なる Cisco Nexus 7000 シリーズ デバイスに接続されているリンクを、第 3 のデバイスには単一のポートに見えるようにします。第 3 のデバイスは、スイッチ、サーバ、ポートチャネルをサポートするその他の任意のネットワーキング デバイスのいずれでもかまいません。vPC は、ノード間の複数の並列パスを可能にし、トラフィックのロード バランシングを可能にすることによって、冗長性を作り、バイセクショナルな帯域幅を増やすレイヤ 2 マルチパスを提供できます。

vPC+

仮想ポート チャネル（vPC+）は、CE のみを実行する仮想ポート チャネル（vPC）の拡張です。vPC+ ドメインにより、クラシカル イーサネット（CE）の vPC ドメインと Cisco FabricPath クラウドが相互運用でき、また FabricPath とレイヤ 3 境界でファースト ホップ ルーティング プロトコル（FHRP）のアクティブ-アクティブ機能が提供されます。vPC+ ドメインは、FabricPath デバイスがイネーブルの Cisco Nexus 7000 シリーズが 1 つの vPC+ を形成し、FabricPath ネットワークのその他のデバイスに接続する固有の仮想スイッチとなることを可能にします。vPC+ の詳細については、『*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*』を参照してください。

（注） 同じ VDC には、vPC+ ドメインと vPC ドメインを設定できません。

図 *11*：*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。vPC ドメインは単一の仮想デバイス コンテキスト（VDC）に関連付けられるため、同じ 1 つの vPC ドメインに所属するすべての vPC インターフェイスが同一 VDC 内で定義されていなければなりません。配置した各 VDC に、独立した vPC ピア リンクとピアキープアライブ リンクのインフラストラクチャがなくてはなりません。vPC ピア（ドメインが同じ 2 台の vPC ピア デバイス）を同じ物理デバイスの 2 つの VDC 内に統合することは、サポートされていません。vPC ピア リンクは、リンクの両エンドに少なくとも 10 ギガバイト イーサネット ポートを使用しなければならず、そうなっていないとリンクが形成されません。

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 内のポート チャネル（vPC ピア リンク チャネルを含む）を設定した場合は、F シリーズ ライン カードで 16 個のアクティブ リンクをサポートし、M シリーズ ライン カードで 1 ポート チャネルあたり 8 個のアクティブ リンクをサポートできます。LACP を使用して vPC のポート チャネル（vPC ピア リンク チャネルを含む）を設定した場合は、F シリーズ カードで 1 ポート チャネルあたり 8 個のアクティブ リンクと 8 個のスタンバイ リンクをサポートできます。（LACP と vPC の使用の詳細については、「その他の機能との vPC の相互作用」の項を参照）。

lacp graceful-convergence コマンドを使用して、ポート チャネルの Link Aggregation Control Protocol（LACP）グレースフル コンバージェンスを設定できます。管理上ダウン状態にあるポート チャネル インターフェイスでのみ、このコマンドを使用できます。管理上アップ状態にあるポート チャネルの LACP グレースフル コンバージェンスは設定できず、ディセーブルにすることもできません。

lacp suspend-individual コマンドを使用して、ポート チャネル上の LACP ポートの一時停止を有効にできます。ポート チャネルでピア ポートから LACP ブリッジ プロトコル データ ユニット（BPDU）を LACP が受け取っていない場合、その LACP ではポートを一時的な動作停止状態に設定します。これによって、サーバの中には起動に失敗するものがあります。そのようなサーバは、LACP が論理的にポートを稼働状態にしていることを必要とするからです。

（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。

Cisco NX-OS リリース 4.2 以降では、システムは機能のディセーブル化の前に自動的にチェックポイントを作成するため、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 7000 Series NX-OS System Management Configuration Guide*』を参照してください。

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。

専用ポート モードで 2 つ以上の 10 ギガビット イーサネット ポートを使用することにより、1 台の Cisco Nexus 7000 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。正しいハードウェアをイネーブルにしており、Cisco NX-OS リリース 4.1(5) 以降の vPC を実行していることを確認するには、show hardware feature-capability 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 7000 シリーズ シャーシで、再度 2 つ以上の 10 ギガビット イーサネット ポートを専用モードで使用して、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。正しいモジュールを使用していないと、システムからエラー メッセージが表示されます。

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

Cisco NX-OS リリース 4.2 以降では、すべての vPC ピア リンクおよびコアに面したインターフェイスを 1 つのモジュール上で設定しなければならない場合、コアへのレイヤ 3 リンクに関連付けられているトラック オブジェクトおよび両方の vPC ピア デバイス上の vPC ピア リンク上のすべてのリンクを設定してください。いったんこの機能を設定したら、プライマリ vPC ピア デバイスに障害が発生した場合には、プライマリ vPC ピア デバイス上のすべての vPC リンクを、システムが自動的に停止します。システムが安定するまでは、このアクションにより、すべての vPC トラフィックが強制的にセカンダリ vPC ピア デバイスに送られます。

トラック オブジェクトを作成し、コアおよび vPC ピア リンクに接続されているプライマリ vPC ピア デバイス上のすべてのリンクにそのオブジェクトを適用できます。track interface コマンドについては、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

vPC ドメインには、両方の vPC ピア デバイス、vPC ピアキープアライブ リンク、vPC ピア リンク、および vPC ドメイン内にあってダウンストリーム デバイスに接続されているすべてのポート チャネルが含まれます。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） 常にすべての vPC デバイスを両方の vPC ピア デバイスに、ポート チャネルを使用して接続してください。

vPC の用語

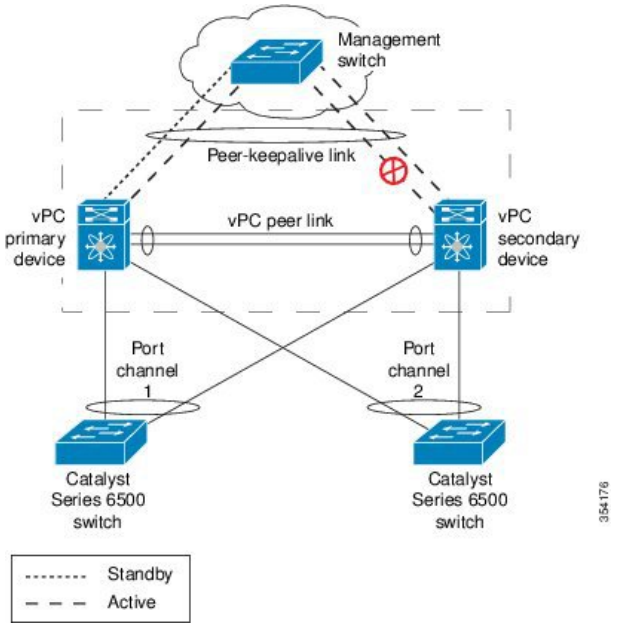
vPC で使用される用語は、次のとおりです。

- 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。両エンドが 10 ギガバイト イーサネット インターフェイス上になくてはなりません。
- vPC メンバ ポート：vPC に属するインターフェイス。
- ホスト vPC ポート：vPC に属するファブリック エクステンダのホスト インターフェイス。
- vPC ドメイン：このドメインには、両方の vPC ピア デバイス、vPC ピアキープアライブ リンク、vPC 内に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 7000 シリーズのデバイスをモニタします。ピアキープアライブ リンクは、vPC ピア デバイス間での設定可能なキープアライブ メッセージの定期的な送信を行います。

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

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

図 *12*：*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

vPC ピア リンクは、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です。リンクの両エンドが、10 ギガビット イーサネット インターフェイス上になくてはなりません。

- 両方の vPC ピア スイッチにコントロール プレーン情報を同期します（vPC 状態、一貫性パラメータ、MAC アドレスなど）。
- ローカル vPC がダウンしたとき、vPC ピア スイッチにデータ パケットを転送します。

- 同一の物理 Cisco Nexus 7000 デバイス上の 2 つの VDC 間の単一 vPC ドメインはサポートされません。

（注） vPC ピア リンクを設定する場合は、あらかじめピアキープアライブ リンクを設定しておく必要があります。設定しておかないと、ピア リンクは機能しません（vPC ピアキープアライブ リンクと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）。

vPC ピア リンクは、2 つのデバイスを vPC ピアとして設定するように設定できます。vPC ピア リンクを設定するためには、モジュールを使用する必要があります。

vPC ピア リンクを設定する場合は、専用ポート モードを使用することを推奨します。専用ポート モードについては、「基本インターフェイス パラメータの設定」を参照してください。

Cisco NX-OS リリース 6.2 での vPC ピア リンクと I/O モジュールのサポート

F2e VDC を設定できます。2 台の vPC ピア デバイスの VDC タイプは、F2 シリーズ モジュールおよび F2e シリーズ モジュールが同じ VDC またはシステムで使用されるときに一致している必要があります。同じトポロジの F2 シリーズ モジュールおよび F2e シリーズ モジュールについては、F2 シリーズ モジュールに関連している機能のみが適用されます。

Cisco NX-OS リリース 6.2(2) への ISSU 後、F2 VDC は F2e シリーズ モジュールの有無に関係なく、F2 F2e VDC に自動的に変更されます。

以下の表に、Cisco NX-OS リリース 6.2 で vPC ピア リンクの両側でサポートされる I/O モジュールを示します。

表 *16*：*Cisco NX-OS* リリース *6.2* 以降で *vPC* ピア リンクの両側でサポートされる *I/O* モジュールの組み合わせ

vPC プライマリ	vPC セカンダリ
M1 I/O モジュール	M1 I/O モジュール
M2 I/O モジュール	M2 I/O モジュール
M3 I/O モジュール	M3 I/O モジュール
F2 I/O モジュール	F2 I/O モジュール
F2 I/O モジュール	F2e I/O モジュール
F2e I/O モジュール	F2e I/O モジュール
F2e I/O モジュール	F2 I/O モジュール
F3 I/O モジュール	F3 I/O モジュール

Cisco NX-OS リリース 6.1 およびそれ以前のリリースでの vPC ピア リンクと I/O モジュールのサポート

Cisco NX-OS リリース 6.1 およびそれ以前のリリースでは、vPC ピア リンクの一方の側の同一 I/O モジュールのみがサポートされます。vPC ピア リンクの一方の側で異なる I/O モジュールを使用している場合はサポートされません。ポート チャネルの同じ側で I/O モジュールを混在している場合もサポートされません。上の表に、vPC ピア リンクの両側でサポートされる I/O モジュールを示します。

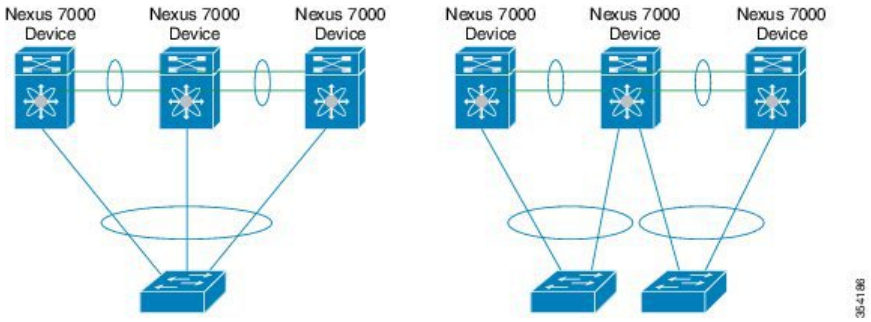
ポート チャネルの使用中は、両側で同じライン カードを使用することをお勧めします。

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、以下の図を参照してください。

図 *13*：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。

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

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

両方の vPC ピア リンク デバイスおよびダウンストリーム デバイスで、任意の標準ロードバランシング スキームを設定できます（ロード バランシングについては、第 6 章の「ポート チャネルの設定」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、7-30 ページの「CFSoE」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 については、7-30 ページの「CFSoE」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。

（注） 独立した VRF を作成して設定し、その vPC ピアキープアライブ リンクのための VRF 内の各 vPC ピア デバイス上でレイヤ 3 ポートを設定することを推奨します。ピアキープアライブのデフォルト ポートとデフォルト VRF は、管理ポートと管理 VRF です。

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、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。
  - ポート チャネルが vPC ピア リンクとして指定されている場合は、spanning-tree port type network コマンドが追加されるため、ポート チャネルが Bridge Assurance ポートになります。
  - 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 デバイスからのレイヤ 3 接続を設定します。
- HSRP アクティブ：vPC ピア デバイス上でホットスタンバイ ルータ プロトコル（HSRP）と VLAN インターフェイスを使用する場合は、プライマリ vPC ピア デバイスを HSRP アクティブの最も高いプライオリティで設定します。セカンダリ デバイスを HSRP スタンバイになる

ように設定し、各 vPC デバイスの VLAN インターフェイスが同じ管理/動作モードにあることを確認します（vPC および HSRP の詳細については、「vPC ピア リンクとルーティング」の項を参照）。

単方向リンク検出（UDLD）の設定では、次の留意点に注意してください。

- LACP がポート チャ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。

UDLD の設定については、「UDLD モードの設定」の項を参照してください。

vPC ピア リンクのレイヤ 3 バックアップ ルートの設定

HSRP や PIM などのアプリケーションに 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。また、vPC ピア デバイスからのルーティングに VLAN ネットワーク インターフェイスを使用できます。

（注） 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」を参照してください。

Cisco NX-OS リリース 6.2(2) 以降では、vPC ピア リンクが M シリーズ モジュールと F2e シリーズ モジュールを持つ混在シャーシ内の F2e シリーズ モジュール上にある場合、vPC ピア リンクを介してレイヤ 3 バックアップ ルーティング パスを使用しないでください。代わりに追加のスイッチ間ポート チャネルを使用して専用のレイヤ 3 バックアップ ルーティング パスを配置します。

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。

Cisco NX-OS リリース 4.2(1) 以降では、指定した VLAN インターフェイスが vPC ピア リンクに障害が発生しても vPC セカンダリ デバイス上で停止しないようにすることができるようになりました。

この機能を設定するには、**dual-active exclude interface-vlan** コマンドを使用します。

（注） Cisco NX-OS リリース 7.2(0)D1(1) 以降では、vPC ドメインにレイヤ 3 デバイスを接続している場合に、vPC ピア リンク上でも伝送される VLAN を使用したルーティング プロトコルのピアリングはサポートされません。vPC ピア デバイスおよび汎用レイヤ 3 デバイスの間でルーティング プロトコルの隣接関係が必要な場合は、相互接続に物理的にルーティングされたインターフェイスを使用する必要があります。vPC ピアゲートウェイ機能の使用では、この要件は変わりません。

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。

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独立した VRF に関連付けることを推奨します。独立した VRF を設定しなかった場合は、デフォルトで管理 VRF と管理ポートが使用されます。vPC ピアキープアライブ メッセージの送受信にピア リンク自体を使用することはしないでください。VRF 設定の詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

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。ホールドタイムアウト値とタイムアウト値を同時に設定できます。

ホールドタイムアウト値：ホールドタイムアウト値の範囲は、3 ～ 10 秒の間で、3 秒がデフォルト値です。このタイマーは、vPC ピア リンクが停止した時点で開始します。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。

タイムアウト値よりも小さいホールドタイムアウト値を設定すると、vPC システムは、ホールドタイムアウト期間の vPC ピアキープアライブ メッセージを無視して、タイムアウト期間のリマインダのメッセージを考慮します。キープアライブ メッセージがこの期間に受信されない場合は、vPC セカンダリ デバイスがプライマリ デバイスのロールを引き継ぎます。たとえば、ホールドタイムアウト値が 3 秒で、タイムアウト値が 5 秒の場合、最初の 3 秒間の vPC キープアライブ メッセージは無視され（スーパーバイザの障害がピア リンク障害の後、数秒間処理されるとき、など）、キープアライブ メッセージは、残り 2 秒のタイムアウト期間が考慮されます。この期間が過ぎて、キープアライブ メッセージがない場合は、vPC セカンダリ デバイスはプライマリ デバイスとして引き継がれます。

タイムアウト値：タイムアウト値の範囲は 3 ～ 20 秒の間で、デフォルト値は 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。ホールドタイムアウト値以下にタイムアウト値を設定する場合、タイムアウト継続期間はホールドタイムアウト期間後に開始されます。たとえば、タイムアウト値が 3 秒で、ホールドタイムアウト値が 5 秒の場合、タイムアウト期間は 5 秒後に開始されます。

（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。

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。次に、インターフェイスを信頼できるポートとして設定する例を示します。

```
(config)# class-map type qos match-all trust-map
(config-cmap-qos)# match cos 4-7

(config)# policy-map type qos ingresspolicy
(config-pmap-qos)# class trust-map

(config)# interface Ethernet8/11
(config-if)# service-policy type qos input ingresspolicy
```

信頼できるポートおよび優先順位の設定の詳細については、『*Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide*』を参照してください。

vPC ピア ゲートウェイ

Cisco NX-OS リリース 4.2(1) 以降では、vPC ピア デバイスを、vPC ピア デバイスの MAC アドレスを送信先とす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るようになりました。

この機能を設定するには、**peer-gateway** コマンドを使用します。

（注） Cisco NX-OS リリース 6.2(2) 以降では、mode auto コマンドを使用して、この機能を自動的にイネーブルにすることができます。このコマンドの使用に関する詳細については、「特定の vPC コマンドの自動イネーブル化」の項を参照してください。

一部のネットワーク接続ストレージ（NAS）デバイスまたはロードバランサは、特定のアプリケーションのパフォーマンスを最適化するのに役立つ機能を備えている場合があります。これらの機能により、同じサブネットにローカルに接続されていないホストから送信された要求に応答するときに、デバイスはルーティング テーブルのルックアップを回避できます。このようなデバイスは、一般的な HSRP ゲートウェイではなく、送信元の Cisco Nexus 7000 シリーズ デバイスや Cisco Nexus 7700 シリーズ デバイスの MAC アドレスを使用して、トラフィックに応答する場合があります。この動作は、一部の基本的なイーサネット RFC 標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、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。

（注） Cisco NX-OS リリース 5.1(3) 以降では、VLAN インターフェイスが vPC ピア デバイスのレイヤ 3 バックアップ ルーティングに使用され、F1 ラインカードがピア リンクとして使用される場合は、peer-gateway exclude-vlan vlan-number コマンドを実行して VLAN をピアゲートウェイ機能から除外する必要があります（イネーブルの場合）。バックアップ ルートの詳細については、「vPC ピア リンクのレイヤ 3 バックアップ ルートの設定」の項を参照してください。

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

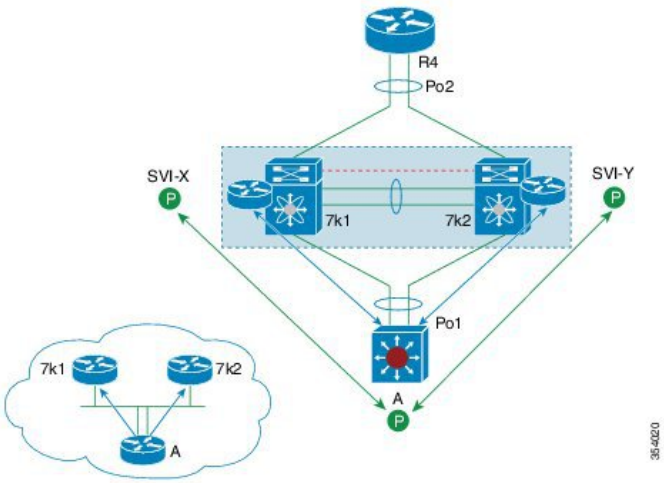
F2E および F3 モジュール用の vPC 経由のレイヤ 3

このセクションでは、F2E および F3 モジュール機能用の vPC 経由のレイヤ 3 と、その設定方法について説明します。Cisco NX-OS リリース 7.2(0)D1(1) 以降では、レイヤ 3 デバイスが vPC コンプレックス内の両方の vPC ピア間のピアリング隣接関係を形成できます。すべての vPC ピアが同じ VLAN を使用する必要があります。ピア リンク経由で送信されるトラフィックの TTL はデクリメントしません。F2E および F3 モジュール機能用の vPC 経由のレイヤ 3 を設定する前に、ピア ゲートウェイ機能を有効にする必要があります。ピア ゲートウェイ機能を使用すれば、vPC ピア（SVI X）（下の図を参照）が他のピア（SVI-Y）の代わりにパケットを転送することができます。この機能は、ピア リンク経由のトラフィックを回避することで帯域幅を節約します。別のレイヤ 3 リンクを使用せずに、レイヤ 3 デバイスと vPC ピア間のピア隣接関係をセットアップすることができます。ブリッジド トラフィックとルーテッド トラフィックの両方が同じリンク経由で流れることができます。

レイヤ 3 デバイスと vPC ピア間のルーティング隣接関係は、非 vPC VLAN なしで形成されます。隣接関係は vPC VLAN 上で形成されます。レイヤ 3 デバイスと vPC ピア間のルーティング隣接関係は、vPC ピア間のレイヤ 3 スイッチ間リンクなしで形成されます。隣接関係は vPC ピア リンク上で形成されます。すべてのトラフィックに対してリンクまたはデバイスでエラーが発生すると、

コンバージェンスが早まります。vPC ループ回避メカニズムはすべてのトラフィックで使用できます。

図 *14* : *vPC* 経由のレイヤ *3* ソリューション



Cisco NX-OS リリース 7.2(0)D1(1) での VPC 経由のレイヤ 3 のサポート

次の図は、Cisco NX-OS リリース 7.2(0)D1(1) での VPC 経由のレイヤ 3 のサポートを示しています。

図 *15*：サポート：*vPC* 相互接続を介したピアリング。ルータは両方の *vPC* ピアとピアリングします。

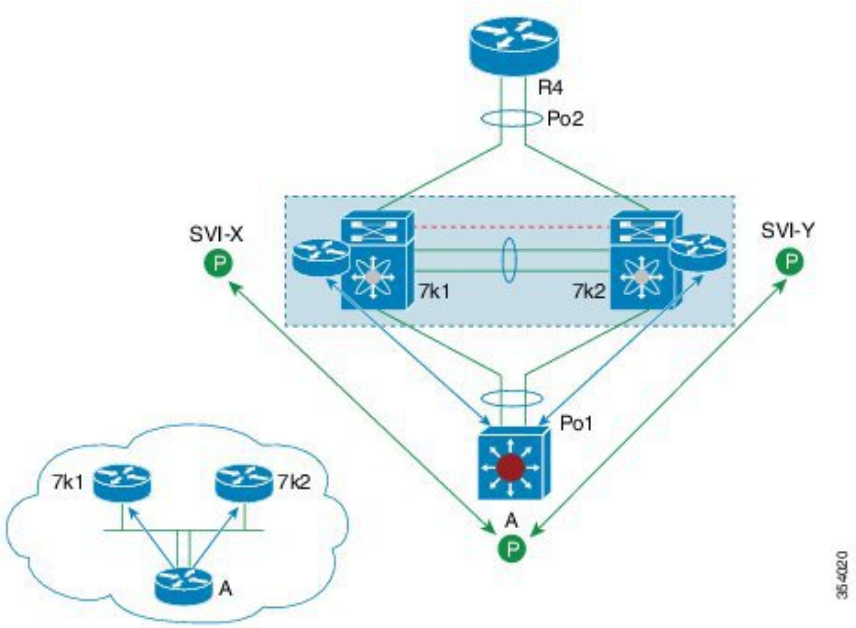


図 *16*：サポート：*vPC VLAN* を使用した *STP* 相互接続を介したピアリング。ルータは両方の *vPC* ピアとピアリングします。

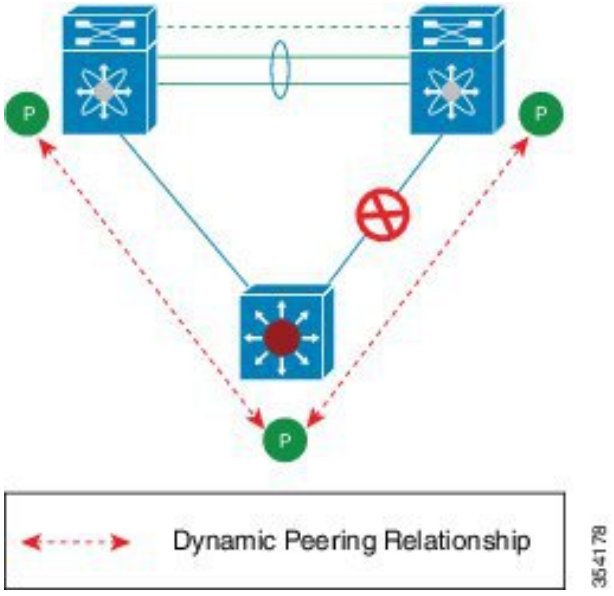


図 *17*：サポート：両方の *vPC* ピアと孤立デバイスとのルート ピアリング。

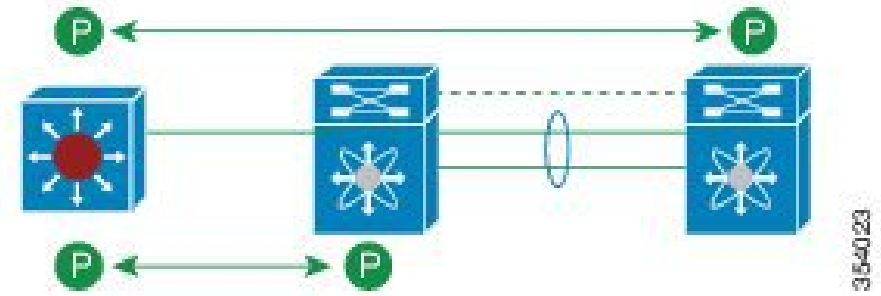


図 *18*：サポート：*vPC* 相互接続を介したピアリング。各 *Nexus* デバイスが *2* 台の *vPC* ピアとピアリングします。

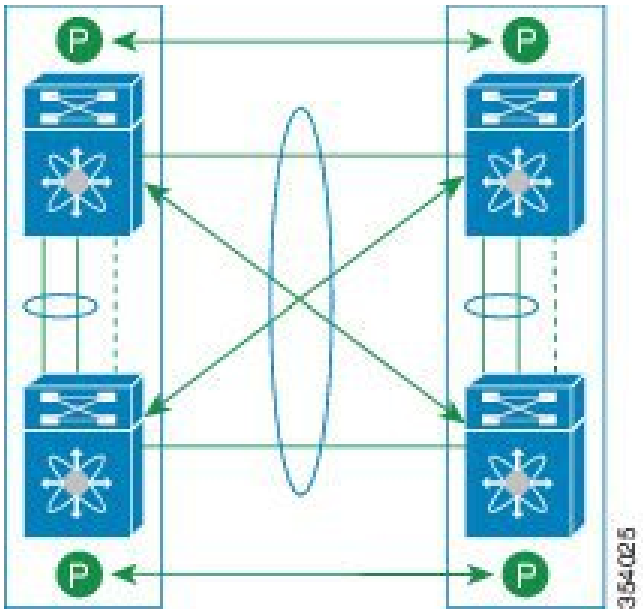
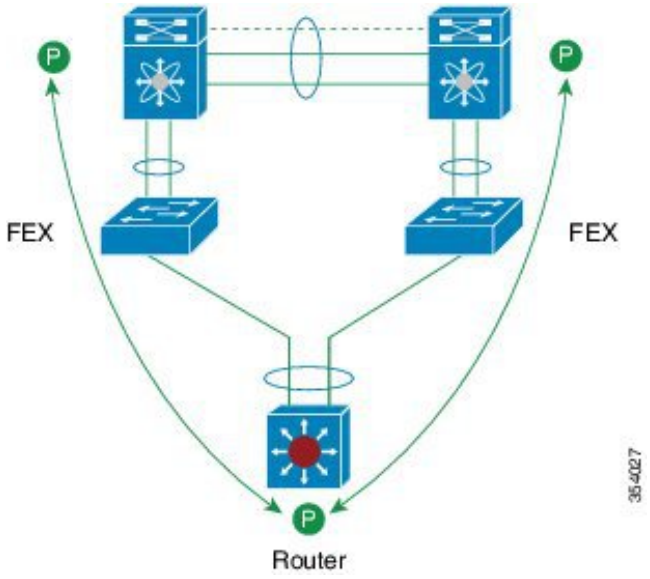


図 *19*：サポート：*FEX vPC* ホスト インターフェイスを介した *vPC* ピアとのピアリング



FEX は、Straight Through トポロジで Nexus に接続します。ルータは、衛星ポート経由で両方の Nexus ボックスとピアリングします。FEX アクティブ - アクティブ モード vPC での vPC を介したレイヤ 3 はサポートされません。

図 *20*：未サポート：不等レイヤ *3* メトリックを使用した *vPC* インターフェイスを介したピアリング

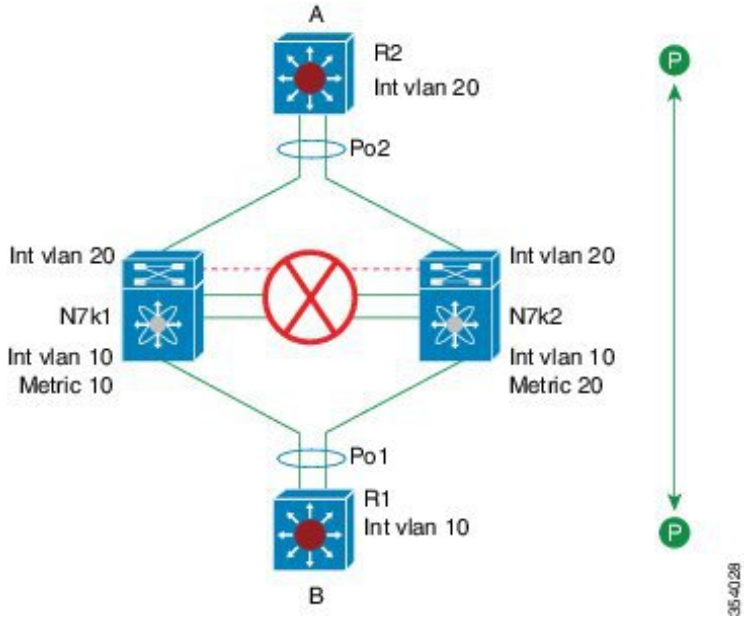
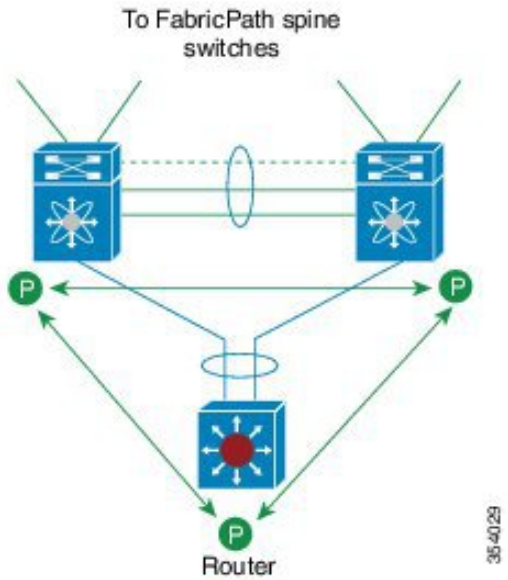


図 *21*：未サポート：*Cisco NX-OS 7.2(0)D1(1)* での *vPC+* を介したピアリング



vPC+ インターフェイスを介した vPC ピアとのピアリングはサポートされません。

図 *22*：未サポート：***vPC+ VLAN*** を使用した ***vPC+*** ピアと ***STP*** 相互接続とのピアリング

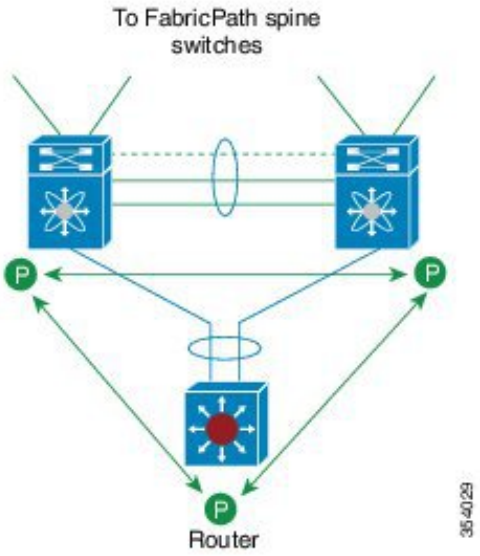


図 *23*：未サポート：両方の ***vPC+*** ピアと孤立デバイスとのルート ピアリング

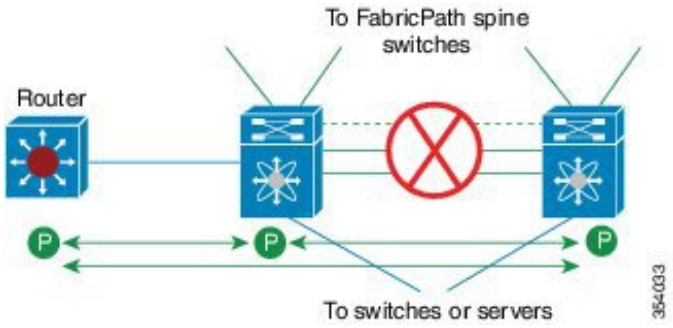
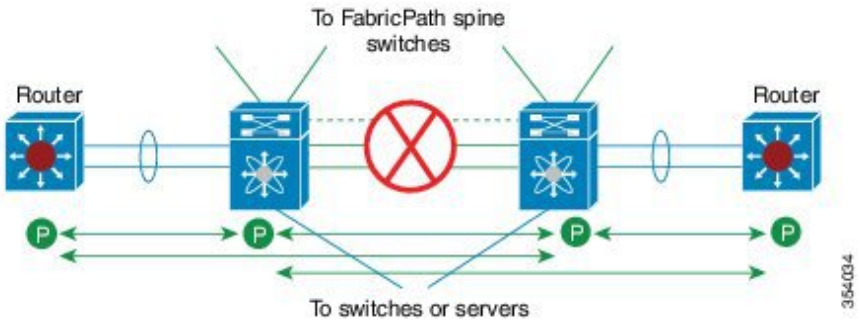


図 *24*：未サポート：***PC*** 相互接続を介したピアリングと ***vPC VLAN*** を使用して ***vPC+*** ピア リンクを介したピアリング



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コンフィギュレーション 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。VDC につき設定できる vPC ドメインは、1 つだけです。

各デバイス上で、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設定する必要があります。各デバイス上でピア 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、静的にしか設定できません。各 vPC ピア デバイス上の vPC 内のすべてのポートが、同じ VDC 内になくてはなりません。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設定できます。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。

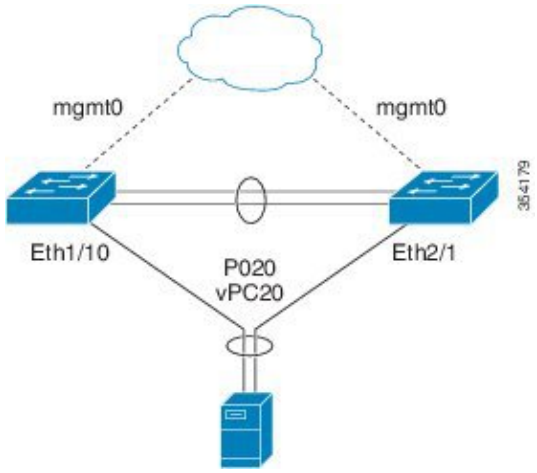
vPC MAC テーブルの表示の詳細については、「CFSoE」の項を参照してください。vPC ドメインを作成した後は、Cisco NX-OS ソフトウェアによって vPC ドメインのシステム プライオリティが作成されます。vPC ドメインに特定のシステム プライオリティを設定することもできます。

（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

以下の図は、Cisco Nexus 7000 シリーズのデバイス 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ている基本設定を示しています。

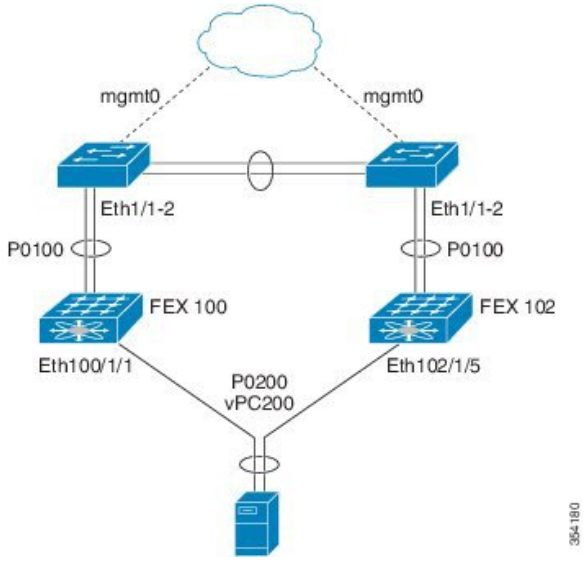
図 *25*：スイッチ *vPC* トポロジ



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 Eth2/1 がメンバ ポートとしてあります。

Cisco NX-OS リリース 5.2(1) 以降では、以下の図に示すように、ファブリック エクステンダ（FEX）を通してピア デバイスから vPC を設定できます。

図 *26*：*FEX Straight-Through* トポロジ（ホスト *vPC*）



この図では、各 FEX は Cisco Nexus 7000 シリーズ デバイスがあるシングル ホーム接続（Straight-Through FEX トポロジ）です。この FEX 上のホスト インターフェイスはポート チャネルとして設定され、それらのポート チャネルは vPC として設定されています。Eth100/1/1 および Eth102/1/5 は、PO200 のメンバーとして設定され、PO200 は vPC 200 に対し設定されます。

どちらのトポロジでも、ポート チャネル P020 および P0200 をピア スイッチ上でまったく同じように設定する必要があります。その後、設定の同期を使用して vPC スイッチの設定を同期します。FEX ポートの設定の詳細については、『*Configuring the Cisco Nexus 2000 Series Fabric Extender*』を参照してください。

物理ポート vPC

物理ポート vPC は、vPC ピア デバイスの物理インターフェイスに設定された vPC です。物理ポート vPC は、ダウンストリーム デバイスに任意で Link Aggregation Control Protocol（LACP）を実行できます。物理ポート vPC は F2 モジュールと F2E モジュールでサポートされます。vPC 設定はメンバー ポートに直接適用されます。また、vPC を使用して設定された物理インターフェイス上で LACP プロトコルを有効にすることもできます。Cisco NX-OS 7.2(0)D1(1) 以降では、物理ポート vPC が F3 モジュールと FEX モジュールでもサポートされます。

F2、F3、および FEX 用の物理ポート vPC

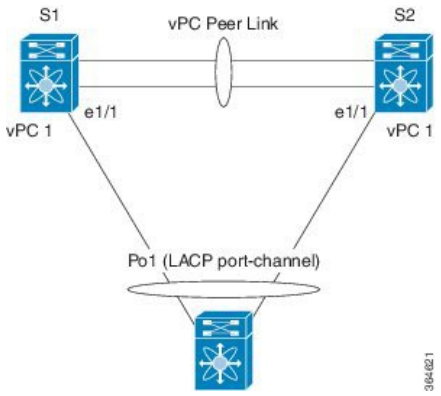
ここでは、F2、F3、および FEX モジュール用の物理ポート VPC について説明します。

F2、F3、および FEX 用の物理ポート VPC 機能には、次のようなメリットがあります。

- ユーザが vPC 設定を有効にするためのポート チャネルを作成しない簡易設定が使用できます。vPC 設定はメンバー ポートに直接適用されます。
- vPC のレグごとに 1 つずつの 10 ギガビット イーサネット ポート、40 ギガビット イーサネット ポート、または 100 ギガビット イーサネット ポートを備えた vPC セットアップをサポートします。このようなケースでの vPC セットアップ用のポート チャネルの作成は最適ではありません。この機能は、インターフェイスが 1 つしかないポート チャネル vPC に最適です。
- 拡張性が向上するため、将来的にさらに多くの物理ポートをサポートできます。
- ポート チャネルではなく、物理ポートに関するアカウンティング ログとシステム ログを提供します。
- 大規模な FEX セットアップをサポートします。この機能は、インターフェイスが 1 つしかないポート チャネル vPC に最適です。
- ポート チャネル構造から設定と導入を分離することにより、vPC の制限を広げます。
- vPC 上の物理ポートの FCoE サポートを拡張する拡張機能が追加されるため、既存の FCoE サポート用の構造を維持しながら、イーサネット トラフィックのマルチパシングが可能になります。

（注） 物理ポート vPC+ を設定する前に、**fabricpath multicast load-balance** コマンドを有効にする必要があります。この要件は標準の前面パネルと FEX ポートに適用されます。

図 *27*：物理ポート *vPC* のトポロジ



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、「CFSoE」の項を参照）。

（注） 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するには、**show vpc consistency-parameters** コマンドを入力します。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 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」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） 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するには、**show vpc consistency-parameters** コマンドを入力します。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）
- チャネル単位のリンク速度
- チャネル単位のデュプレックス モード
- 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
- 最大伝送単位（MTU）

次のパラメータが、Cisco NX-OS リリース 6.2(6) で物理ポート vPC に対し追加されました。

- ネイティブ VLAN
- ポート モード
- インターフェイス タイプ
- VLAN xLT マッピング
- vPC カード タイプ
- 共有モード

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** コマンドおよび **show vpc consistency-parameters** コマンドを入力して、syslog メッセージをチェックします。

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。ピア リンクの片方のデバイスだけで設定されている VLAN は、vPC またはピア リンクを使用してトラフィックを通過させることはしません。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
- Quality of Service（QoS）の設定とパラメータ
- STP インターフェイス設定：
  - BPDU Filter
  - BPDU ガード
  - コスト
  - リンク タイプ
  - プライオリティ
  - VLAN（Rapid PVST+）
- ポート セキュリティ
- Cisco Trusted Security（CTS）
- ポート セキュリティ
- Cisco Trusted Security（CTS）
- ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピング
- ネットワーク アクセス コントロール（NAC）
- ダイナミック ARP インスペクション（DAI）
- IP ソース ガード（IPSG）
- インターネット グループ管理プロトコル（IGMP）スヌーピング
- ホット スタンバイ ルーティング プロトコル（HSRP）
- プロトコルに依存しないマルチキャスト（PIM）
- ゲートウェイ ロード バランシング プロトコル（GLBP）
- 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

Cisco NX-OS リリース 5.2(1) より前のリリースでは、整合性検査により一致しなければならないパラメータのリストからパラメータの不一致が検出されると、vPC ピア リンクと vPC は稼働できません。vPC がすでに確立された後にパラメータの不一致が設定された場合は、vPC は一時停止モードに移動し、vPC にトラフィックは流れません。

Cisco NX-OS リリース 5.2(1) 以降では、グレースフルな整合性検査機能を設定でき、不一致が作動中の vPC で導入されたときに、セカンダリ ピア デバイス上のリンクのみを中断できます。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。

この機能を設定するには、**graceful consistency-check** コマンドを使用します。

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。NX-OS リリース 5.2(1) より前のリリースでは、有効な VLAN の設定がピア デバイス間で矛盾している場合は、vPC の確立や一時停止モードへの移動はできません。

Cisco NX-OS リリース 5.2(1) 以降では、vPC は動作可能なままで、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。STP ポート タイプの詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

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。

vPC シャットダウン

vPC シャットダウン機能は、ユーザが vPC コンプレックスからスイッチを分離してからデバッグ、リロード、または物理的に削除することができるようにするため、vPC コンプレックス内のピア vPC スイッチを通過する vPC トラフィックは影響を受けません。

ユーザが **shutdown** コマンドを実行すると、MCEC モジュール（MCECM）がアウトオブバンド（OOB）キープアライブ メッセージの送信を停止して、すべての vPC ポート、SVI、およびピア リンクをダウンさせます。ダウンしているピア リンクとキープアライブ メッセージの非可用性を検出すると、ピア vPC スイッチがプライマリ ピアを引き継ぎます。キープアライブ メッセージが受信されないため、ピア vPC スイッチはフラップ後も vPC ピア リンクを起動しません。ピア リンクがダウンしているため、孤立 vPC スイッチはすべての vPC をダウンしたままにします。vPC 孤立ポートは、設定された孤立ポートを一時停止します。

ユーザがこのコマンドの **no** 形式を実行すると、スイッチがネットワーク トラフィックの中断を最小限に抑えながら、vPC コンプレックスに復帰します。このコマンドの **no** 形式を実行すると、キープアライブが開始され、ピア リンクが起動し、すべての vPC が順に起動します。

プライマリ スイッチ上で実行された場合は、**shutdown** コマンドのデュアル アクティブ ステータスが確立されます。

vPC **shutdown** コマンドを実行すると、孤立ポートの接続が解除されます。

Cisco NX-OS サービスは、永続ストレージ サービス（PSS）に **shutdown** コマンドを保存します。このコマンドはスイッチのリロード時に復元されます。**shutdown** コマンドは vPC 設定として保存されます。スタートアップ コンフィギュレーションにコピーされた場合は、vPC 設定と一緒に **shutdown** コマンドが再度実行されます。**shutdown** コマンドはスイッチのリロード時に復元されます。

vPC Shutdown コマンド後の vPC スイッチ間のバージョンの互換性

デバッグ後または ISSU 後に起動した孤立 vPC ピア スイッチの vPC オペレーティング バージョンが、ピア スイッチと異なる可能性があります。**no shutdown** コマンドが適用された場合は、vPC ピア リンクが、一方のバージョンがもう一方のバージョンより低い 2 台のスイッチを使用して起動します。

vPC シャットダウン時の STP の役割

STP は、ロール スイッチオーバーが発生したときに、新しいプライマリ vPC ピアが現在の状態を継承するようにポート状態を vPC ピアと同期します。MCECM がロール変更を検出して STP に通知するのに 6 秒以上かかった場合は、vPC 上で送信される STP ブリッジ プロトコル データ ユニット（BPDU）がタイムアウトします。これを回避するために、両方の vPC スイッチが vPC ポート経由で BPDU を送信するように、STP ピア スイッチ機能を設定することをお勧めします。

FEX アクティブ - アクティブ モードのスイッチに対する vPC Shutdown コマンド

デュアルホーム FEX が vPC 内で接続されているスイッチ上で **shutdown** コマンドを設定すると、FEX がそのスイッチ上でオフラインになります。孤立スイッチの ISSU は、FEX 上のソフトウェア イメージを更新しません。FEX アクティブ - アクティブ用に各スイッチを分離してアップグレードすることによって ISSU を実行するために、vPC **shutdown** コマンドを使用することはできません。

ピア 1 とピア 2 が関与する次の FEX アクティブ - アクティブ シナリオについて考えます。

- 非アクティブ ピアであるピア 2 は、VPC shutdown コマンドなどによってオフラインになっています。
- アクティブ ピアのピア 1 上で ISSU が実行され、ソフトウェア イメージがバージョン アップされています。

FEX アクティブ - アクティブを含むすべてのライン カードとリモート ライン カードのソフトウェア イメージがバージョン アップされています。これは、FEX アクティブ - アクティブが非アクティブ ピアでオフラインになっているためです。

その後、非アクティブ ピアが VPC no shutdown コマンドでオンラインになったときに、このピアは引き続き下位バージョンのソフトウェア イメージを実行することになります。このようなケースでは、FEX アクティブ - アクティブのステータスがこのピア内の AA バージョン不一致とオフラインの間で切り替わります。これは、両方のピアが別々のバージョンのソフトウェア イメージを実行しているためです。この状況を回避するには、ピア 2 が上位バージョンのソフトウェア イメージにアップグレードされるまで、ピア 2 を起動しない、または、VPC shutdown コマンドを実行しないようにする必要があります。

vPC シャットダウン時のレイヤ 2 MCECM の役割

no shutdown コマンドを実行すると、Multichassis EtherChannel Module（MCECM）がキープアライブ メッセージを停止して、ピア リンクをダウンさせます。vPC ピア スイッチが 5 秒以内にキープアライブ メッセージを受信しなかった場合は、プライマリ ロールを引き受けます。

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。

単一モジュール上での vPC ピア リンクとコアへのリンクの設定

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

Cisco NX-OS リリース 4.2 以降では、すべての vPC ピア リンクとコアに面するインターフェイスを単一モジュール上で設定しなければならない場合は、両方の vPC ピア デバイス上のすべての vPC ピア リンク上の、およびコアへのレイヤ 3 リンクに関連付けられているトラック オブジェクトとトラック リストをコマンドラインインターフェイスを使用して設定してください。トラック リスト上のすべてのトラッキング対象オブジェクトが停止した場合、システムは次のように動作するため、この設定を使用すれば、その特定のモジュールが停止した場合のトラフィックのドロップを避けることができます。

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

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

コアに対するすべてのリンクおよびすべての vPC ピア リンクを含むトラック リストを、そのオブジェクトとして作成する必要があります。このトラック リストの指定した vPC ドメインに対して、トラッキングをイネーブルにします。この同じ設定を他方の vPC ピア デバイスにも適用します。オブジェクト トラッキングおよびトラック リストの設定については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

オブジェクト トラッキングの設定については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

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

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

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

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

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

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

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

ステップ 3：このトラック オブジェクトを vPC ドメインに追加します。

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

ステップ 4：トラック オブジェクトを表示します。

```
switch# show vpc brief
Legend:
       (*) - local vPC is down, forwarding via vPC peer-link
vPC domain id                     : 1
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
vPC role                          : secondary
Number of vPCs configured         : 52
Track object                      : 44
vPC Peer-link status
---------------------------------------------------------------------
id    Port   Status  Active vlans
--    ----   ------  --------------------------------------------------
1     Po100   up      1-5,140
vPC status
----------------------------------------------------------------------
id    Port  Status Consistency Reason                     Active vlans
--    ---- ------   ----------- -------------------------- ------------
1      Po1   up      success    success                     1-5,140
```

次に、オブジェクト トラッキングに関する情報を表示する例を示します。

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

その他の機能との vPC の相互作用

vPC と LACP

LACP は、vPC ドメインのシステム MAC アドレスを使用して、vPC の LACP Aggregation Group（LAG）ID を形成します（LAG-ID および LACP については、第 6 章の「ポート チャネルの設定」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。

M シリーズ モジュールおよび LACP では、vPC ピア リンクは、16 個の LACP インターフェイス（8 個のアクティブ リンクと 8 個のホット スタンバイ リンク）をサポートします。ダウンストリーム vPC チャネル上では、8 個のアクティブ リンクと 8 個のホット スタンバイ リンクとで、16 個の LACP リンクを設定できます。LACP を使用せずにポート チャネルを設定する場合は、各チャネルに 8 個のリンクしか持てません。F シリーズのライン カードでは、vPC ピア リンクとダウンストリーム vPC チャネルは最高 16 個のアクティブな LACP リンクをサポートします。ポート チャネルが LACP を使用して設定されていなくても、各チャネルに 16 個のリンクを設定できます。

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。

ポート チャネルが vPC ピア リンクとして指定されている場合は、spanning-tree port type network コマンドが追加されるため、ポート チャネルが Bridge Assurance ポートになります。vPC ピア リンク上では STP 拡張機能を一切有効にしないことをお勧めします。STP 拡張がすでに設定されている場合、その拡張が vPC ピア リンクの問題の原因となることはありません。

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

STP 拡張機能および PVST シミュレーションについては、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

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 については、7-30 ページの「CFSoE」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 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 Filter
- 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。

この機能がイネーブルになっている場合は、show spanning-tree コマンドで vPC に関する情報を表示できます。例については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

（注） ダウンストリームデバイスのポートは、STPエッジポートとして設定することを推奨します。スイッチに接続されているすべてのホスト ポートを STP エッジ ポートとして設定してくださいSTP ポート タイプの詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

（注） トランスペアレント モードの適応型セキュリティ アプライアンス（ASA）を使用して Nexus 7000 ピア スイッチ上で 2 つの VLAN をブリッジすると、スイッチがどちらかの VLAN を STP ディスピュートにします。これを回避するには、ポート上でピア スイッチまたは STP を無効にします。

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 Release 5.0(2) に追加されました。この機能は、一対の Cisco Nexus 7000 シリーズ 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ことを可能にします。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。ピア リンク障害は、南北のトラフィックには影響がありませんが、東西のトラフィックが失われます。

STP 拡張機能および Rapid PVST+ については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

vPC ピア リンクの指定フォワーダ

リリース 6.0 以降では、Cisco NX-OS により、vPC パスの両方がアップしたときに 2 つのピアが部分的に指定フォワーダとなるよう制御する方法が提供されます。この制御がイネーブルの場合、各ピアを（ハードウェアに応じて）RBH/FTAG の分離セットに対するマルチデスティネーションのサウスバウンド パケット用の指定フォワーダにすることができます。指定フォワーダは、vPC ごとにネゴシエートされます。この制御は、vPC ドメイン モードで設定された **fabricpath multicast load-balance** コマンドでイネーブルになります。

次に例を示します。

```
switch(config)# vpc domain 1
switch(config-vpc-domain)# fabricpath multicast load-balance
```

（注） Cisco NX-OS リリース 6.2(2) 以降では、この機能は **mode auto** コマンドが使用されると自動的にイネーブルになります。このコマンドの使用に関する詳細については、「特定の vPC 機能の自動イネーブル化」の項を参照してください。

（注） F2 シリーズ モジュールのみがマルチキャスト ロード バランシングをサポートします。F1 シリーズ モジュールでは、設定はサポートされますが、ロード バランシングは発生しません。

（注） **fabricpath multicast load-balance** コマンドは、FEX ポートと vPC+ を設定するのに必要となります。

vPC の指定フォワーダのイネーブル化の詳細については、『*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*』を参照してください。

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 リリース 4.2(6) に追加されました。**ip arp synchronize** および **ipv6 nd synchronize** コマンドをイネーブルにし、vPC ピア間のアドレス テーブルのコンバージェンスの高速化をサポートする必要があります。このコンバージェンスにより、ピア リンク ポート チャネルがフラップしたり、vPC ピアがオンラインに戻るときに、IPv4 の場合は ARP テーブルの復元でまたは IPv6 の場合は ND テーブルの復元で発生する遅延を解消できます。

（注） Cisco NX-OS リリース 6.2(2) 以降では、mode auto コマンドを使用して、この機能を自動的にイネーブルにすることができます。このコマンドの使用については、「特定の vPC コマンドの自動イネーブル化」の項を参照してください。

vPC マルチキャスト：PIM、IGMP、および IGMP スヌーピング

（注） Nexus 7000 シリーズ デバイスの Cisco NX-OS ソフトウェアは、vPC での Product Independent Multicast（PIM）、Source-Specific Multicast（SSM）または双方向（PIM）をサポートしません。Cisco NX-OS ソフトウェアは、vPC での PIM Any Source Multicast（ASM）を完全にサポートします。

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

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

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

次のシナリオで、ごくわずかなトラフィック損失が観察される場合があります。

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

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

vPC およびマルチキャストで情報を表示するコマンドについては、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』を参照してください。

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

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

（注） vPC VLAN（vPC ピア リンクで伝送される VLAN）とダウンストリーム vPC が接続されたレイヤ 3 デバイス間の PIM ネイバー関係はサポートされません。それによりマルチキャスト パケットのドロップが生じる場合があります。PIM ネイバー関係がダウンストリーム レイヤ 3 デバイスで必要な場合、物理レイヤ 3 インターフェイスを vPC インターフェイスの代わりに使用する必要があります。

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） 次のコマンドは、vPC モードでサポートされていません。

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

マルチキャストの詳細については、『*Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide*』を参照してください。

マルチキャスト PIM デュアル DR（プロキシ DR）

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

Cisco NX-OS vPC 実装（非 F2 モード）では、PIM はデュアル指定ルータ（DR）モードで動作します。つまり、vPC デバイスが vPC SVI の発信インターフェイス（OIF）上の DR である場合、そのピアは自動的にプロキシ DR ロールを引き継ぎます。IGMP は、OIF が DR である場合、OIF（レポートはその OIF で学習されます）をフォワーディングに追加します。デュアル DR では、両方の vPC デバイスには、次の例に示すように、vPC SVI OIF に対して同一のエントリ (*,G) があります。

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

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

IP PIM PRE-BUILD SPT

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

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

(S,G)
  oif1 (mrib)

VPC Device2:
------------
```

```
(*,G)
  oif1 (igmp)

(S,G)
NULL
```

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

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

F2 モジュールの VPC ピア リンクによる PIM DUAL DR および IP PIM PRE-BUILD SPT

F2 モードでの vPC 実装では、ハードウェアの制限により、PIM デュアル DR モードはディセーブルです。その結果、PIM DR だけが OIF を追加し、その状態は次の例に示されます。

```
Case 1: One OIF
===============
VPC Device1 (say this is PIM DR on oif1):
-----------------------------------------
(*,G)
  oif1 (igmp)

VPC Device2:
------------
(*,G) will not be created.
```

送信元トラフィックが受信されると、vPC デバイス 1 のみが (S,G) ルートを追加します。

```
VPC Device1 (say this is PIM DR on oif1):
-----------------------------------------
(*,G)
  oif1 (igmp)
(S,G)
  oif1 (mrib)

VPC Device2:
------------
(*, G) will not be created.
(S, G) will not be created.
```

この場合（F2 モード）、**ip pim pre-build-spt** コマンドを入力しても、対応する (S,G) ルートが最初の場所に作成されないので、値は追加されません。

```
Case 2: Two OIFs
================
VPC Device1 (say this is PIM DR on oif1):
-----------------------------------------
(*,G)
  oif1 (igmp)

VPC Device2 (say this is PIM DR on oif2):
-----------------------------------------
```

```
(*,G)
  oif2 (igmp)
```

送信元トラフィックが受信されると、次の例に示すように、関連する OIF が (S,G) ルートにより継承されます。

```
VPC Device1 (say this is PIM DR on oif1):
----------------------------------------
(*,G)
  oif1 (igmp)

(S,G)
  oif1 (mrib)

VPC Device1 (say this is PIM DR on oif2):
----------------------------------------
(*,G)
  oif2 (igmp)

(S,G)
  oif2 (mrib)
```

F2 モジュールを使用した vPC ピア リンクの場合は、**ip pim pre-build-spt** コマンドを入力する必要はありません。これは、関連するルートに NULL でない oiflist があるため PIM が (S,G) ジョインをアップストリームに送信するためです。

（注） vPC 機能が F2 モードでイネーブルになっている場合は、**ip pim pre-build-spt** コマンドを入力しないでください。

vPC ピア リンクとルーティング

ファースト ホップ ルーティング プロトコル（FHRP）は、vPC と相互運用します。ホット スタンバイ ルーティング プロトコル（HSRP）、ゲートウェイ ロードバランシング プロトコル（GLBP）、および仮想ルータ冗長プロトコル（VRRP）のすべてが、vPC と相互運用できます。すべてのレイヤ 3 デバイスを両方の vPC ピア デバイスにデュアル接続することを推奨します。

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

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

さらに、if-hsrp コンフィギュレーション モードで priority コマンドを使用して、vPC ピア リンク上でイネーブルになっているグループの状態がスタンバイになっているか、またはリッスン状態になっている場合のフェールオーバーのしきい値を設定できます。インターフェイスがアップまたはダウンするのを防ぐために下限および上限しきい値を設定できます。

VRRP は、vPC ピア デバイス上で実行されている場合に HSRP とよく似た動作を示します。VRRP は、HSRP を設定したのと同じ方法で設定してください。GLBP については、両方の vPC ピア デバイス上のフォワーダがトラフィックを転送します。

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

Cisco NX-OS リリース 4.2(1) 以降では、**delay restore** コマンドを使用して、ピアの隣接関係が確立され VLAN インターフェイスが再びアップ状態になるまで vPC の再稼働を遅延させるための復元タイマーを設定することができます。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。この機能を設定するには、delay restore コマンドを使用します。

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

FHRP とルーティングの詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

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、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** コマンドと **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。

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

CFS は、TCP/IP を介したデータも転送します。IP 経由の CFS の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』を参照してください。

（注） CFS リージョンはサポートされていません。

vPC および孤立ポート

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

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、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。Cisco NX-OS リリース 5.2(1) 以降では、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。

物理ポート vPC を介した Fibre Channel over Ethernet

物理ポート仮想ポート チャネル（vPC）を介した Fibre Channel over Ethernet（FCoE）機能は、vPC インターフェイスへの物理イーサネット インターフェイスの共有モデルを拡張します。

vPC レグを形成する各イーサネット インターフェイスは、ストレージ仮想デバイス コンテキスト（VDC）とイーサネット VDC 間で共有されます。共有イーサネット インターフェイスは、FCoE および LAN トラフィックの両方を伝送します。相互に排他的な FCoE と LAN VLAN は、vPC レグ上のトラフィックを伝送するために割り当てられます。FCoE トラフィックは FCoE VLAN により伝送され、LAN トラフィックは LAN VLAN により伝送されます。

シャットダウン LAN

特定の設定およびネットワーク パラメータは、物理ポート vDC が動作するようにピア スイッチ間で一貫している必要があります。ネットワーク（タイプ 1）に影響を与える不一致が検出され

た場合、セカンダリ vPC レグ（アクセス スイッチとホスト間の物理リンク）が停止します。物理ポート vPC を介した FCoE を使用すると、vPC レグは FCoE リンクと LAN リンクが両方ダウンするように FCoE および LAN トラフィックの両方を伝送します。シャットダウン LAN 機能を使用することで、イーサネット インターフェイス上の LAN VLAN のみをシャットダウンまたは起動することができます。

停電後の vPC リカバリ

データセンターの停電時には、vPC を含む両方の Cisco Nexus 7000 シリーズ デバイス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。しかし、Cisco NX-OS リリースによっては、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。

リロードでの復元

（注） Cisco NX-OS リリース 5.2(1) 以降では、**reload restore** コマンドおよびメソッドが非推奨となっています。**auto-recovery** コマンドおよびメソッドを使用することを推奨します。

Cisco NX-OS リリース 5.0(2) 以降では、ピアがオンラインになれなかった場合に、reload restore コマンドを使用して vPC サービスを復元するように Cisco Nexus 7000 シリーズ デバイスを設定できるようになりました。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、Cisco NX-OS ソフトウェアは、ユーザによる設定可能なタイマーを開始します（デフォルトは 240 秒）。ピア リンク ポートが物理的に稼働し始めるか、ピアキープアライブが機能し始めたら、タイマーは停止し、デバイスはピアの隣接が形成されるのを待ちます。

ピアキープアライブ パケットもピア リンク アップ パケットも受信できないままタイマーが切れると、Cisco NX-OS ソフトウェアは、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 ロールのマスターとしても機能します。

自動リカバリ

Cisco NX-OS リリース 5.2(1) 以降では、ピアがオンラインになれなかった場合に、**auto-recovery** コマンドを使用して vPC サービスを復元するように Cisco Nexus 7000 シリーズ デバイスを設定できるようになりました。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、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 ロールのマスターとしても機能します。

Cisco NX-OS リリース 6.2(2) 以降では、**mode auto** コマンドを使用して、この機能を自動的にイネーブルにすることができます。このコマンドの使用については、「特定の vPC コマンドの自動イネーブル化」の項を参照してください。

Cisco NX-OS リリース 7.2(0)D1(1) 以降では、プライマリ ピアがダウンして、15 個のキープアライブ メッセージが失われた場合に、セカンダリ デバイスがプライマリ ロールを引き継ぎます。

Cisco NX-OS リリース 7.2(0)D1(1) 以降では、**auto-recovery** コマンドを設定することにより、セカンダリ ピアがプライマリ ピアから 15 個のキープアライブを受信できなかった場合に、プライマリ ピアを引き継ぐようにできます。スイッチがリロードすると、自動回復機能タイマーが起動して、ピア スイッチが応答しなかった場合に、プライマリ STP ロールを引き継ぎます。

vPC shutdown コマンドを設定すると、自動回復機能がブロックされます。

Cisco NX-OS リリース 6.2.(2) 以降では、初期ブート中に自動回復機能が起動するように、論理ピア リンクをダウンさせ、ピア キープアライブ メッセージを受信しないようにする必要があります。以前のリリースでは、ピア キープアライブ メッセージが受信されずに物理ピア リンクがアップ ステータスに設定されていた場合に、自動回復機能が起動しませんでした。

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。

ハイ アベイラビリティ

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

ハイ アベイラビリティ機能の詳細については、『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

ヒットレス vPC ロールの変更

vPC ヒットレス 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ためのフレームワークを提供します。vPC ロールの交換は、vPC ドメインに属しているデバイスのロール プライオリティ値に基づいて行われます。**vpc role preempt** コマンドを実行すると、ロール プライオリティの低い 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。

ヒットレス vPC ロールの変更に関するユース ケース シナリオ

ヒットレス vPC ロールの変更機能は、次のシナリオで使用できます。

- ロール変更の要求：vPC ドメイン内のピア 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：デバイスがリロード後に起動し、ロールが定義されている場合は、ヒットレス vPC ロールの変更機能を使用してロールを復元することができます。たとえば、リロード後にプライマリ デバイスが稼働可能なセカンダリのロールを引き継ぎ、セカンダリ デバイスが稼働可能なプライマリのロールを引き継いだ場合は、**vpc role preempt** コマンドを使用して、vPC ピアのロールを元の定義済みのロールに変更できます。

（注） **vpc role preempt** コマンドを設定する前に、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。**vpc role preempt** コマンドを設定する前に、vpc domain コマンドで **no port-channel limit** を設定します。

- 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（稼働可能な）プライマリのままですが、vPC セカンダリ スイッチがプライマリ スイッチ候補になり、その vPC メンバー ポートを稼働状態にします。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 設定の同期化

仮想ポート チャネル（vPC）トポロジでは、ピア スイッチの設定を同じにする必要があります。そのため、両方のピア スイッチ上の設定を繰り返す必要があります。この処理では、設定ミスや漏れによるエラーが発生する場合があります。これは、設定の不一致によるその他のサービス障害につながる可能性があります。設定の同期では、1 台のスイッチを設定し、自動的にピア スイッチで設定を同期することによって、これらの問題を排除します。

vPC トポロジでは、すべての Cisco Nexus 7000 シリーズ スイッチの一部のパラメータを一致させる必要があります。vPC 整合性検査は、両方の Cisco Nexus 7000 シリーズ スイッチが同じ設定

（Type1 または Type 2）を持つことを確認するために使用できます。設定が一致しない場合は、グローバル（スパニングツリーポートモードなど）、ポートレベル（速度、デュプレックス、またはチャネルグループ タイプなど）、またはポート チャネル インターフェイスであるかどうかに応じて、両方のピア スイッチで vPC が中断ステートになったり、VLAN がブロッキング ステートになったりする可能性があります。その結果、1 つのスイッチの設定がまったく同じようにピア スイッチにコピーされていることを確認する必要があります。

設定の同期は、ネットワーク内のスイッチのペア間の設定を同期させることができます。設定の同期と vPC は、独立した 2 つの機能であり、設定の同期では、vPC 整合性検査は除外されません。チェックが続行されます。設定の不一致がある場合は、vPC は中断ステートになります。

FEX アクティブ/アクティブ セットアップ：

- すべてのホスト インターフェイス（HIF）ポートが内部 vPC にマップされます。
- vPC Config-Sync 機能は、内部 vPC 作成通知をリッスンして、HIF ポート設定のマージをトリガーします。
- マージが成功すれば、以降のすべての HIF 設定がピア スイッチと同期されます。
- マージが失敗した場合は、HIF のステータスが「同期が外れたピア」としてマークされ、インターフェイスの設定が同期されません。

（注）

vPC ピア リンクを設定して、稼働状態にする必要があります。

同期するコマンドを選択することはできません。

vPC 設定の同期のメリット

設定の同期の利点は次のとおりです。

- スイッチ間の設定を同期させるためのメカニズムが提供されます。
- ピア間で接続が確立されると、設定がマージされます。
- コマンドの相互排他機能が提供されます。
- 既存のセッションおよびポートのプロファイル機能がサポートされています。
- ユーザの操作が最小限で済みます。
- ユーザ エラーの可能性が最小限に抑えられます。

vPC 設定の同期をサポートするコマンド

次のコマンドのタイプが設定の同期に使用できます。

（注） **show vpc config-sync cli syntax** コマンドは、設定の同期に使用可能なすべてのコマンドを列挙します。同期するコマンドを選択することはできません。

- タイプ 1 設定：
  - グローバル設定
  - vPC メンバー ポート チャネル設定
- vPC 設定

（注） 設定は vPC ピア スイッチのどちらかで行うことができます。

インターフェイスのライセンス要件

vPC には、ライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

IP トンネルには Enterprise Services ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『Cisco NX-OS Licensing Guide』を参照してください。

他のインターフェイスにはライセンスが必要ありません。

注意事項と制約事項

vPC 設定時の注意事項と制限事項は次のとおりです。

- vPC 上の IPv6 マルチキャストはサポートされません。
- vPC 経由のルーティングは、F2E モジュールと F3 モジュールでのみサポートされます。
- vPC ピアは、アップグレードまたはダウングレードプロセス中にのみ、異なるバージョンの NX-OS ソフトウェアを稼働できます。
- アップグレードまたはダウングレード期間以外で異なるバージョンを実行する vPC ピアはサポートされません。
- 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。
- これらを設定する前に、vPC を有効にします。

- システムが vPC ピア リンクを形成するには、その前にピア キープアライブ リンクとピア キープアライブ メッセージを設定します。
- vPC に入れられるのは、レイヤ 2 ポート チャネルだけです。
- 両方の vPC ピア デバイスを設定します。設定は片方のデバイスから他方へ送信されません。
- マルチレイヤ（バックツーバック）vPC を設定するために、それぞれの vPC に一意の vPC ドメイン ID を割り当てます。
- 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 および SSM 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、または IPSG はサポートされていません。
- DHCP リレーはサポートされます。
- CFS リージョンはサポートされていません。
- ポート チャネル上でのポート セキュリティは、サポートされていません。
- 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。
- この目的には VLAN ネットワーク インターフェイスを使用するよりも、vPC ピア デバイスからのルーティングのためのレイヤ 3 リンクを別途設定してください。
- 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。
- vPC を使用する場合は、FHRP（HSRP、VRRP、GLBP）にデフォルトのタイマーを使用し、PIM 設定を行うことを推奨します。アグレッシブ タイマーを vPC 設定で使用すると、コンバージェンス時間のメリットがありません。
- vPC ピア リンク VLAN トラフィックを伝送するすべての非 vPC インターフェイス（ポート チャネルまたはイーサネット）上で **vpc orphan-ports suspend** コマンドを設定します。vPC シャットダウン中に、vPC マネージャが、**vpc orphan-ports suspend** 設定を使用して、vPC インターフェイス、vPC インターフェイス VLAN、および非 vPC インターフェイスをダウンさせます。
- vPC 環境で open shortest path first（OSPF）を設定する場合は、コア スイッチ上でルータ コンフィギュレーション モードで次のタイマー コマンドを使用することにより、vPC ピア リンクがシャットダウンしたときに OSPF の高速コンバージェンスを実現します。

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

  OSPF の詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。
- HSRP の BFD は、vPC 環境ではサポートされていません。

- STP ポート コストは、vPC 環境で 200 に固定されています。
- 同一の物理 Cisco Nexus 7000 デバイス上の 2 つの VDC 間の単一 vPC ドメインはサポートされません。
- ジャンボ フレームは、vPC ピア リンクではデフォルトでイネーブルです。
- FabricPath VLAN 経由のルーティング プロトコル隣接関係はサポートされません。

自動リカバリには次の制限事項と注意事項があります。

- Cisco NX-OS リリース 6.2(2) 以降のリリースでは、自動リカバリはデフォルトでイネーブルです。以前のリリースで自動リカバリをすでにイネーブルにしており、リリース 6.2(2) 以降のリリースにアップグレードする場合、自動リカバリはアップグレード後でもイネーブルのままになります。リリース 6.2(2) 以降のリリースで自動リカバリをディセーブルにする場合は、**auto-recovery disable** コマンドを使用して自動リカバリを明示的にディセーブルにする必要があります。
- Cisco NX-OS Release 6.2.(2) 以降では、初期ブート中に自動回復機能が起動するように、論理ピア リンクをダウンさせ、ピア キープアライブ メッセージを受信しないようにする必要があります。6.2.2 より前のリリースでは、ピア キープアライブ メッセージが受信されず、物理ピア リンクがアップ ステータスに設定されていた場合は、自動リカバリが起動しませんでした。

物理ポート vPC には次の注意事項と制約事項が適用されます。

- 物理ポート vPC は、Nexus F2、F2e、および F3 シリーズ モジュールでのみサポートされます。
- 物理ポート vPC は、M3 モジュールが組み込まれた VDC ではサポートされません。
- 物理ポート vPC は、Nexus F2、F2e、および F3 シリーズ モジュール上の vPC+ でのみサポートされます。
- 物理ポート vPC は、ファブリック エクステンダ（FEX）インターフェイスでサポートされます。
- Link Aggregation Control Protocol（LACP）は、vPC なしで物理ポートでイネーブルにできません。
- 同じ vPC 設定を複数の物理ポートに適用することはできません。

物理ポート vPC を介した FCoE には次の注意事項と制限事項があります。

- FCoE は、トランク ポートでのみサポートされます。
- FCoE は、共有インターフェイスでのみサポートされます。
- FCoE はポート チャネル vPC ではサポートされていません。
- 物理ポート vPC を介した FCoE は、タイプ F2 のストレージ VDC のみでサポートされます。
- 物理ポート vPC を介した FCoE は、ストレージ VDC でサポートされません。これは、物理ポート vPC 経由のレイヤ 2 マルチパシングが LAN に対してのみサポートされるためです。

- VPC+ 経由の FCoE はサポートされません。
- シャットダウン LAN 設定は、共有インターフェイスのみでサポートされます。
- リンク層検出プロトコル（LLDP）は、シャットダウン LAN のイーサネット VDC でイネーブルにする必要があります。

ヒットレス vPC ロールの変更機能には次の注意事項と制約事項が適用されます。

- vPC STP ヒットレス ロールの変更機能は、Cisco Nexus 7.3(0)D1(1) リリース以降でのみサポートされます。
- vPC ロールの変更は、ピア デバイスのどちらからでも実行できます。
- 元のセカンダリ デバイスに元のプライマリ デバイスより高いプライオリティ値を設定した場合は、ロール交換が実行できません。元のセカンダリ デバイスの値が元のプライマリ デバイスより低くなるように、どちらかの vPC デバイスのロール プライオリティを変更します。デバイスの既存のロールを表示するには、ローカル スイッチとピア スイッチ上で **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、vPC+ 上で、**fabricpath multi path load-balance** コマンドを有効にします。転送タグ（FTag）スキームが vPC+ でロール変更をシームレスに設定するために使用されます。FTag スキームが使用されることを保証するには、vPC+ 上で **fabricpath multi path load-balance** コマンドと依存関係にある **no port channel limit** コマンドを有効にする必要があります。
- vPC ヒットレス ロールの変更機能を設定する前に、vPC+ 上で **no port channel limit** コマンドを有効にします。このコマンドが有効になっていない場合は、vPC ヒットレス ロールの変更を設定できず、エラー メッセージが表示されます。両方の vPC デバイスで次のコマンドを設定します。

（注） 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** コマンドを有効にしなかった場合は、コンバージェンスの問題が発生する可能性があります。
- ピア デバイス上でタイプ 1 の不一致が発生した場合は、vPC ヒットレス ロールの変更を実行できません。

vPC の設定

vPC の設定

vPC のイネーブル化

vPC を設定して使用するには、その前に vPC 機能をイネーブルにしなければなりません。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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)# **feature vpc**	デバイス上で vPC をイネーブルにします。
ステップ 3	switch(config)# **exit**	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	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。
ステップ 5	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。

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。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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)# **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	switch(config)# **exit**	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	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。
ステップ 5	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。

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してください。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。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

vPC 機能をイネーブルに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	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)# **vpc domain***domain-id*	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	switch(config-vpc-domain)# **exit**	vpc-domain コンフィギュレーション モードを終了します。
ステップ 4	switch# **show vpc brief**	（任意） 各 vPC ドメインに関する要約情報を表示します。
ステップ 5	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。

次に、vPC ドメインを作成する例を示します。

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

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

（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。

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） vPC ピアキープアライブ リンクを使用する際は、個別の VRF インスタンスを設定して、各 vPC ピア デバイスからその VRF にレイヤ 3 ポートを接続することを推奨します。ピア リンク自体を使用して vPC ピアキープアライブ メッセージを送信しないでください。VRF の作成および設定については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。ピアキープアライブ メッセージに使用される送信元と宛先の両方の IP アドレスがネットワーク内で一意であることを確認してください。

管理ポートと管理 VRF が、これらのキープアライブ メッセージのデフォルトです。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

vPC 機能をイネーブルに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	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)# **vpc domain***domain-id*	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	switch(config-vpc-domain)# **peer-keepalive destination***ip address* [**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* | **udp-port***number* | **vrf** {*name* | **management** | **vpc-keepalive**}]	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） 独立した VRF を設定し、vPC ピアキープアライブ リンクのための VRF 内の各 vPC ピア デバイスからのレイヤ 3 ポートを使用することを推奨します。VRF の作成および設定の詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。
ステップ 4	switch(config-vpc-domain)# **exit**	vpc-domain 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 5	switch# **show vpc statistics**	（任意） キープアライブ メッセージのコンフィギュレーションに関する情報を表示します。
ステップ 6	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。

VRF 設定の詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

次の例は、vPC ピアキープアライブ 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

vPC ピア リンクを作成するには、指定した vPC ドメインのピア リンクとするポート チャネルを各デバイス上で指定します。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。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

vPC 機能をイネーブルにしていることを確認します。

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	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 port-channel***channel-number*	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。

	コマンドまたはアクション	目的
ステップ 3	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	switch(config-if)# **switchport trunk allowed vlan***vlan-list*	（任意） 許容 VLAN リストを設定します。
ステップ 5	switch(config-if)# **vpc peer-link**	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。 （注） ポート チャネルが vPC ピア リンクとして指定されている場合は、**spanning-tree port type network** コマンドが追加されるため、ポート チャネルが Bridge Assurance ポートになります。
ステップ 6	switch(config-vpc-domain)# **exit**	vpc-domain コンフィギュレーション モードを終了します。
ステップ 7	switch# **show vpc brief**	（任意） vPC ピア リンクに関する情報など、各 vPC の情報を表示します。
ステップ 8	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。

次の例は、vPC ピア リンクを設定する方法を示します。

```
switch# configure terminal
switch(config)# interface port-channel 20
switch(config-if)# switchport mode
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1-120,201-3967
switch(config-if)# vpc peer-link
switch(config-vpc-domain)# exit
switch(config)#
```

F2、F3、および FEX 上での物理ポート vPC の設定

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***namenumber*	物理ポート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	switch(config-if)# **switchport**	インターフェイスをレイヤ 2 スイッチング ポートとして設定します。
ステップ 4	switch(config-if)# **vpc***number*	vPC への選択された物理インターフェイスをダウンストリーム デバイスに接続するように設定し、インターフェイス vPC コンフィギュレーション モードを開始します。物理インターフェイスには、デバイスの任意のモジュールを使用できます。有効な範囲は 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物理インターフェイスに割り当てる vPC 番号は、両方の vPC デバイスで同じにする必要があります。
ステップ 5	switch(config-if-vpc)# **lacp mode active**	物理ポート上で LACP を有効にします。 （注） 静的モードを使用することもできます。
ステップ 6	switch(config-if-vpc)# **exit**	インターフェイス vPC コンフィギュレーション モードを終了します。
ステップ 7	switch(config-if)# **exit**	インターフェイス コンフィギュレーション モードを終了します。
ステップ 8	switch(config)# **exit**	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 9	switch# **show running-config interface***namenumber*	（任意） インターフェイスに関する情報を表示します。

次の例では、F2、F3、および FEX モジュール上で物理ポート vPC を設定する方法を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# switchport
switch(config-if)# vpc 10
switch(config-if-vpc)# lacp mode active
switch(config-if-vpc)# exit
switch(config-if)# exit
switch(config)# exit
switch# show running-config interface
```

次の例では、LACP モードを確認する方法を示します。

```
switch# show running-config interface

   Interface Ethernet1/1
   no shutdown
   Switchport
    vpc 1
      lacp mode active
```

vPC 上での VLAN の作成

vPC VLAN は、vPC メンバー ポートおよび vPC ピア リンクで許可される VLAN です。vPC 環境で多数の VLAN を設定する場合は、一度に 1 つずつの VLAN を設定するのではなく、VLAN の範囲を指定することによって、複数の VLAN を同時に設定することをお勧めします。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

vPC 機能をイネーブルに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	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)# **vlan 200-299**	200 ～ 299 の範囲で VLAN を設定して、VLAN 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-vlan)# **exit**	VLAN コンフィギュレーション モードを終了します。

次の例では、100 の VLAN を設定し、それぞれに名前を付ける方法を示します。

```
switch# configure terminal
switch(config)# vlan 200-299
switch(config-vlan)# exit
switch(config)# vlan 201
switch(config-vlan)# name finance
switch(config-vlan)# exit
switch(config)#
```

F2E および F3 モジュール用の vPC 経由のレイヤ 3 の設定

はじめる前に

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

ピア リンクがアップ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	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)# **vpc domain***domain-id*	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	switch(config-vpc-domain)# **layer3 peer-router**	両方のピアとのピアリング隣接関係を形成するためレイヤ 3 デバイスをイネーブルにします。 （注） 両方のピアでこのコマンドを設定します。
ステップ 4	switch(config-vpc-domain)# **exit**	vpc-domain コンフィギュレーション モードを終了します。
ステップ 5	switch# **show vpc brief**	（任意） （任意）各 vPC ドメインに関する簡単な情報を表示します。
ステップ 6	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。

次の例では、F2、F2E、および F3 モジュールの vPC 経由のレイヤ 3 を設定する方法を示します。

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

次の例では、F2、F2E、および F3 モジュールの vPC 経由のレイヤ 3 機能が設定されているかどうかを確認する方法を示します。

```
switch# show vpc brief
vPC domain id : 1
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
Configuration consistency status : success
Per-vlan consistency status : failed
Type-2 consistency status : success
vPC role : secondary
Number of vPCs configured : 2
Peer Gateway : Enabled
Peer gateway excluded VLANs : -
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Enabled (timeout = 240 seconds)
Operational Layer3 Peer : Enabled
```

vPC ピアゲートウェイの設定

Cisco NX-OS リリース 4.2(1) とそれ以降のリリースでは、vPC ピア デバイスを、vPC ピア デバイスの MAC アドレスを送信先とす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るようになりました。

vPC ドメインにレイヤ 3 デバイスを接続した場合、vPC ピアリンク上でも送信される VLAN を使用したルーティング プロトコルのピアリンクはサポートされません。vPC ピア デバイスおよび汎用レイヤ 3 デバイスの間でルーティング プロトコルの隣接関係が必要な場合は、相互接続に物理的にルーティングされたインターフェイスを使用する必要があります。vPC ピアゲートウェイ機能の使用では、この要件は変わりません。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

vPC 機能をイネーブルに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	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)# **vpc domain***domain-id*	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	switch(config-vpc-domain)# **peer-gateway**	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。

	コマンドまたはアクション	目的
ステップ 4	switch(config-vpc-domain)# **peer-gateway exclude-vlan***backup-vlan-id*	（任意） Cisco NX-OS リリース 5.1(3) 以降では、混在シャーシ モードの中継 VLAN トラフィックのソフトウェア スイッチングを回避します。 詳細については、「vPC ピア ゲートウェイ」の項を参照してください。
ステップ 5	switch(config-vpc-domain)# **exit**	vpc-domain コンフィギュレーション モードを終了します。
ステップ 6	switch# **show vpc brief**	（任意） vPC ピア リンクに関する情報など、各 vPC の要約情報を表示します。
ステップ 7	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。

グレースフル整合性検査の設定

Cisco NX-OS リリース 5.2(1) 以降では、グレースフル整合性検査機能を設定できます。それはデフォルトでイネーブルになっています。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	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)# **vpc domain***domain-id*	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	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。

	コマンドまたはアクション	目的
		この機能をディセーブルにする場合は、このコマンドの **no** 形式を使用します。
ステップ 4	switch(config-vpc-domain)# **exit**	vpc-domain コンフィギュレーション モードを終了します。
ステップ 5	switch# **show vpc brief**	（任意） 各 vPC ドメインに関する要約情報を表示します。

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 シャットダウンの設定

Cisco NX-OS リリース 7.2(0)D1(1) 以降では、vPC コンプレックスからスイッチを分離してからデバッグ、リロード、または物理的に削除することができるシャットダウンを使用できるため、vPC コンプレックス内のピア vPC スイッチを通過する vPC トラフィックは影響を受けません。

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)# **vpc domain***domain-id*	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	switch(config-vpc-domain)# **shutdown**	ピアをシャットダウンして、デバッグ、リロード、または vPC コンプレックスからの物理的な削除のために分離し、ピア vPC スイッチがプライマリ ピアとして引き継ぐようにします。 この機能をディセーブルにする場合は、このコマンドの **no** 形式を使用します。

	コマンドまたはアクション	目的
ステップ 4	switch(config-vpc-domain)# **exit**	vPC-domain コンフィギュレーション モードを終了します。

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 1
switch(config-vpc-domain)# shutdown
switch(config-vpc-domain)# exit
switch(config)#
```

vPC Config Sync の設定

vPC 設定同期の有効化

はじめる前に

両方のピア スイッチで、同じ vPC ドメイン ID を作成する必要があります。

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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)# **vpc domain***domain-id*	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	switch(config-vpc-domain)# **config-sync**	vPC 設定同期を有効にします。 （注） このコマンドは、プライマリ スイッチとセカンダリ スイッチの両方で設定する必要があります。

次の表に、スイッチ 1 とスイッチ 2 の設定同期のプロセスを示します。

プライマリ スイッチ	セカンダリ スイッチ

`switch-1# configure terminal`
`switch-1(config)# vpc domain 300`
`switch-1(config-vpc-domain)# config-sync`
	`switch-2# configure terminal`
	`switch-2(config)# vpc domain 300`
	`switch-2(config-vpc-domain)# config-sync`

設定同期が、同じ vPC ドメイン内の両方のスイッチで有効になっています。	
`switch-1# configure terminal` `switch-1(config)# spanning-tree mode mst`	
上記の設定は、プライマリ スイッチに適用され、セカンダリ スイッチに同期されます。 設定は、両方のスイッチに正しく適用されるか、両方で失敗するかのどちらかです。	

`switch-1# show running-config`
`...`
`spanning-tree mode mst`
`...`
	`switch-2# show running-config`
	`...`
	`spanning-tree mode mst`
	`...`

	`switch-2# configure terminal` `switch-2(config)# spanning-tree port type switch-2 default`
設定は、セカンダリ スイッチに適用され、プライマリ スイッチに同期されます。 （注） 設定はどちらのスイッチにも適用できます。	

`switch-1# show running-config`
`...`
`spanning-tree port type network default`
`...`
	`switch-2# show running-config`
	`...`
	`spanning-tree port type network default`
	`...`

物理ポート vPC の設定の同期

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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)# **interface***type slot/port*	vPC 物理ポートを指定し、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	switch(config-if)# **vpc***vpc-id* [**sync** {**export** | **import**}]	ポート チャネルを vPC に移動し、インターフェイス vPC 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。 • **sync export** は、プライマリ スイッチ設定をセカンダリ スイッチにエクスポートできるようにします。 • **sync import** は、セカンダリ スイッチ設定をプライマリ スイッチにインポートできるようにします。
ステップ 4	switch(config-if)# **show running-config interface ethernet***slot/port*	（任意） 物理ポートの実行コンフィギュレーションを表示します。

非対称マッピング

次の表に、プライマリ スイッチとセカンダリ スイッチの vPC 物理ポート上の設定同期（非対称マッピング）を有効にするプロセスを示します。

プライマリ スイッチ	セカンダリ スイッチ

`switch-1# configure terminal`
`switch-1(config)# interface eth1/1`
`switch-1(config-if)# vpc 100`	

物理ポート（イーサネット 1/1）がプライマリ スイッチ上の vPC 100 ドメインに追加されます。 vPC 100 は、セカンダリ スイッチ上で設定されません。設定は、vPC 100 がセカンダリ スイッチに追加されるまで同期されません。	

	`switch-2# configure terminal`
	`switch-2(config)# interface eth2/3`
	`switch-2(config-if)# vpc 100`

セカンダリ スイッチへの vPC 100 の設定に続いて、物理ポート（セカンダリ スイッチ上のインターフェイス イーサネット 2/3 とプライマリ スイッチ上のインターフェイス イーサネット 1/1）の設定が同期されます。	

対称マッピング

次の表に、プライマリ スイッチとセカンダリ スイッチの vPC 物理ポート上の設定同期（対称マッピング）を有効にするプロセスを示します。

プライマリ スイッチ	セカンダリ スイッチ

`switch-1# configure terminal`
`switch-1(config)# interface eth1/1`
`switch-1(config-if)# vpc 100 symmetric`
	`switch-2# configure terminal`
	`switch-2(config)# interface eth1/1`

物理ポート（イーサネット 1/1）がプライマリ スイッチ上の vPC 100 ドメインに追加されます。物理ポート（イーサネット 1/1）はセカンダリ スイッチ上にもあります。 プライマリ スイッチとセカンダリ スイッチの両方の物理ポートの設定が同期され続けます。	

`switch-1# show running-config interface eth1/10`
 	
`interface ethernet1/1`
`  switchport`
`  switchport mode trunk`
`  vpc 100`
	`switch-2# show running-config interface eth1/10`
	
	`interface ethernet1/1`
	`  switchport`
	`  switchport mode trunk`
	`  vpc 100`

vPC メンバー ポート チャネルの設定の同期

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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)# **interface port-channel***channel-number*	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	switch(config-if)# **switchport**	インターフェイスをレイヤ 2 スイッチング ポートとして設定します。
ステップ 4	switch(config-if)# **vpc***vpc-id* [**sync** {**export** | **import**}]	ポート チャネルを vPC に移動し、インターフェイス vPC 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。 • **sync export** は、プライマリ スイッチ設定をセカンダリ スイッチにエクスポートできるようにします。

	コマンドまたはアクション	目的
		• **sync import** は、セカンダリ スイッチ設定をプライマリ スイッチにインポートできるようにします。
ステップ 5	switch(config-if)# **show running-config interface port-channel***channel-number*	（任意） ポート チャネルの実行コンフィギュレーションを表示します。

次の表に、プライマリ スイッチとセカンダリ スイッチのポート チャネル 10 上の設定同期を有効にするプロセスを示します。

プライマリ スイッチ	セカンダリ スイッチ

`switch-1# configure terminal`
`switch-1(config)# interface port-channel 10`
`switch-1(config-if)# switchport`
`switch-1(config-if)# vpc 10`	

ポート チャネル 10 上の設定がセカンダリ スイッチに同期されます。 （注） **vpc***number* コマンドは、プライマリ スイッチとセカンダリ スイッチのどちらかで最初に指定できます。	

	`switch-2# show running-config interface po10`
	
	`interface port-channel10`
	`  switchport`
	`  vpc 10`

設定は、セカンダリ スイッチに適用され、プライマリ スイッチに同期されます。 （注） 設定はどちらのスイッチにも適用できます。	

	`switch-2# configure terminal`
	`switch-2(config)# interface port-channel 10`
	`switch-2(config-if)# switchport mode trunk`

show running-config interface port-channel*channel-number* コマンドは、ポート チャネル 10 の設定同期が成功したことを示します。	

`switch-1# show running-config interface port-channel 10`
 	
`interface port-channel10`
`  switchport`
`  switchport mode trunk`
`  vpc 10`
	`switch-2# show running-config interface port-channel 10`
	
	`interface port-channel10`
	`  switchport`
	`  switchport mode trunk`
	`  vpc 10`

vPC 設定同期の確認

vPC 設定同期を確認するには、次のいずれかの作業を行います。

コマンド	目的
show running-config vpc-config-sync	config-sync が使用できるかどうかを表示します。
show vpc config-sync cli syntax	設定を同期可能なコマンドのリストを表示します。
show vpc config-sync database	設定同期データベースを表示します。
show vpc config-sync merge status	スイッチと各 vPC インターフェイスのマージ ステータスを表示します。
show vpc config-sync status	vPC設定同期プロセスの最後の10の操作ステータスを表示します。 • マージ ステータス（成功/失敗）を表示します。 • vPC設定同期プロセスで実行された最後のアクションとその結果を表示します。

vPC ピア リンクの設定の互換性チェック

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	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)# **show vpc consistency-parameters** {**global** | **interface port-channel***channel-number*}	（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。

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

（注） 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。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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。

vPC 機能をイネーブルに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	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 port-channel***channel-number*	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	switch(config-if)# **vpc***number*	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。有効な範囲は 1 ～ 4096 です。

	コマンドまたはアクション	目的
		（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	switch(config-vpc-domain)# **exit**	vpc-domain コンフィギュレーション モードを終了します。
ステップ 5	switch# **show vpc brief**	（任意） 各 vPC ドメインに関する要約情報を表示します。
ステップ 6	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。

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)#
```

特定の vPC コマンドの自動イネーブル化

Cisco NX-OS リリース 6.2(2) 以降では、**mode auto** コマンドを使用して次のコマンドを自動的かつ同時にイネーブルにできます。**peer-gateway**、**auto-recovery**、**fabricpath multicast load-balance**、**ip arp synchronize**、および **ipv6 nd synchronize**。

（注） Cisco NX-OS リリース 6.2(2) 以降のリリースでは、自動リカバリはデフォルトでイネーブルです。リリース 6.2(2) 以降のリリースで自動リカバリをディセーブルにする場合は、**no auto-recovery** コマンドを使用して自動リカバリを明示的にディセーブルにする必要があります。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

vPC 機能をイネーブルに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	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 vpc**	デバイス上で vPC をイネーブルにします。
ステップ 3	switch(config)# **vpc domain***domain-id*	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 4	switch(config-vpc-domain)# [**no**] **mode auto**	次のコマンドを同時にイネーブルにします。**peer-gateway**、**auto-recovery**、**fabricpath multicast load-balance**、**ip arp synchronize**、および **ipv6 nd synchronize**。 この機能をディセーブルにする場合は、このコマンドの **no** 形式を使用します。
ステップ 5	switch(config-vpc-domain)# **exit**	vpc-domain コンフィギュレーション モードを終了します。
ステップ 6	switch(config)# **exit**	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 7	switch# **show running-config vpc**	（任意） イネーブルにするコマンドを含む vPC に関する情報を表示します。
ステップ 8	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。

次のコマンドを同時にイネーブルにする例を次に示します。**peer-gateway**、**auto-recovery**、**fabricpath multicast load-balance**、**ip arp synchronize**、および **ipv6 nd synchronize**。

```
switch# configure terminal
switch# feature vpc
switch(config)# vpc domain 1
switch(config-vpc-domain)# mode auto

The following commands are executed:
peer-gateway ;
auto-recovery ;
ip arp synchronize ;
ipv6 nd synchronize ;
fabricpath multicast load-balance ;

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# show running-config vpc

!Command: show running-config vpc
!Time: Thu Feb 18 12:31:42 2013

version 6.2(2)
feature vpc

vpc domain 1
peer-gateway
auto-recovery
fabricpath multicast load-balance
ip arp synchronize
ipv6 nd synchronize
```

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。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

vPC 機能をイネーブルに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	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)# **vpc domain***domain-id*	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	switch(config-vpc-domain)# **system-mac***mac-address*	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	switch(config-vpc-domain)# **exit**	vpc-domain コンフィギュレーション モードを終了します。
ステップ 5	switch# **show vpc role**	（任意） vPC システムの 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 6	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。

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。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

vPC 機能をイネーブルに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	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)# **vpc domain***domain-id*	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。

	コマンドまたはアクション	目的
ステップ 3	switch(config-vpc-domain)# **system-priority***priority*	指定した vPC ドメインに割り当てるシステム プライオリティを入力します。指定できる値の範囲は、1 ～ 65535 です。デフォルト値は 32667 です。
ステップ 4	switch(config-vpc-domain)# **exit**	vpc-domain コンフィギュレーション モードを終了します。
ステップ 5	switch# **show vpc role**	（任意） vPC システムの MAC アドレスを表示します。
ステップ 6	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。

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。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

vPC 機能をイネーブルに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	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)# **vpc domain***domain-id*	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	switch(config-vpc-domain)# **role priority***priority*	vPC システム プライオリティに与えるロール プライオリティを入力します。指定できる値の範囲は 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	switch(config-vpc-domain)# **exit**	vpc-domain コンフィギュレーション モードを終了します。
ステップ 5	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	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。

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)#
```

シングルモジュール vPC でのトラッキング機能の設定

Cisco NX-OS Release 4.2 以降では、すべての vPC ピア リンクとコアに面するインターフェイスを単一モジュール上で設定しなければならない場合は、両方のプライマリ vPC ピア デバイス上の vPC ピア リンクのすべてのリンク上の、およびコアへのレイヤ 3 リンクに関連付けられているトラック オブジェクトとトラック リストを設定しなければなりません。いったんこの機能を設定したら、プライマリ vPC ピア デバイスに障害が発生した場合には、プライマリ vPC ピア デバイス上のすべての vPC リンクを、システムが自動的に停止します。システムが安定するまでは、このアクションにより、すべての vPC トラフィックが強制的にセカンダリ vPC ピア デバイスに送られます。

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

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

vPC 機能をイネーブルにしていることを確認します。

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

手順

	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)# **vpc domain***domain-id*	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	switch(config-vpc-domain)# **track***track-object-id*	以前に関連するインターフェイスで設定されたトラック リスト オブジェクトを vPC ドメインに追加します。オブジェクト トラッキングおよびトラック リストの設定については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。
ステップ 4	switch(config-vpc-domain)# **exit**	vpc-domain コンフィギュレーション モードを終了します。
ステップ 5	switch# **show vpc brief**	（任意） 追跡対象オブジェクトに関する情報を表示します。
ステップ 6	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。

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

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

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

停電後のリカバリの設定

停電が発生すると、vPC はピア隣接がスイッチ リロード時に形成するのを待ちます。この状況は、許容範囲内に収まらないほど長いサービスの中断に至る場合があります。Cisco Nexus 7000 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

（注） Cisco NX-OS リリース 5.2(1) 以降では、reload restore コマンドおよびこのセクションで説明されている手順が非推奨となっています。auto-recovery コマンドおよび「自動リカバリの設定」で説明されている手順を使用することを推奨します。

Cisco NX-OS リリース 5.0(2) 以降では、ピアがオンラインになれなかった場合に、reload restore コマンドを使用して vPC サービスを復元するように Cisco Nexus 7000 シリーズ デバイスを設定できるようになりました。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

vPC 機能をイネーブルに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	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)# **vpc domain***domain-id*	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	switch(config-vpc-domain)# **reload restore** [**delay***time-out*]	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。

	コマンドまたはアクション	目的
ステップ 4	switch(config-vpc-domain)# **exit**	vpc-domain コンフィギュレーション モードを終了します。
ステップ 5	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	switch# **show vpc consistency-parameters interface port-channel***number*	（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	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。

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 NX-OS リリース 5.2(1) 以降では、ピアがオンラインになれなかった場合に、**auto-recovery** コマンドを使用して vPC サービスを復元するように Cisco Nexus 7000 シリーズ デバイスを設定できるようになりました。

（注） Cisco NX-OS リリース 6.2(2) 以降のリリースでは、自動リカバリはデフォルトでイネーブルです。リリース 6.2(2) 以降のリリースで自動リカバリをディセーブルにする場合は、**no auto-recovery** コマンドを使用して自動リカバリを明示的にディセーブルにする必要があります。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

vPC 機能をイネーブルに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	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)# **vpc domain***domain-id*	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	switch(config-vpc-domain)# **auto-recovery** [**reload-delay***time*]	vPC がそのピアが機能しないことを前提として vPC を稼働させ始めるように設定し、vPC を復元するためのリロード後に待機する時間を指定します。デフォルト遅延値は 240 秒です。240 ~ 3600 秒の遅延を設定できます。 vPC をデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。
ステップ 4	switch(config-vpc-domain)# **exit**	vpc-domain コンフィギュレーション モードを終了します。
ステップ 5	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。

	コマンドまたはアクション	目的
ステップ 6	switch# **show vpc consistency-parameters interface port-channel***number*	（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	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。

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
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。Cisco NX-OS リリース 5.2(1) 以降では、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） 6.2 より前のリリースでは、すべてのメンバー ポート上で vPC orphan-port コマンドを設定し、それらをポート チャネルにバンドルします。これ以降のリリースでは、ポート チャネル インターフェイス上で直接コマンドを設定します。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

vPC 機能をイネーブルに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	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)# **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	switch(config)# **interface port-channel***channel-number*	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 4	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	switch(config-if)# **exit**	インターフェイス コンフィギュレーション モードを終了します。
ステップ 6	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。

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

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

vPC ピア スイッチの設定

Cisco Nexus 7000 シリーズ デバイスは、一対の vPC デバイスがレイヤ 2 トポロジ内で 1 つの STP ルートとして現れるように設定することができます。この項では、次のトピックについて取り上げます。

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。

（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。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

vPC 機能をイネーブルに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	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)# **vpc domain***domain-id*	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	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	switch(config-vpc-domain)# **spanning-tree vlan***vlan-range***priority***value*	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	switch(config-vpc-domain)# **exit**	vpc-domain コンフィギュレーション モードを終了します。
ステップ 6	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	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。

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)#
```

ハイブリッド vPC ピア スイッチ トポロジの設定

spanning-tree pseudo-information コマンド（詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』を参照）を使用して STP VLAN ベースのロードバランシング基準を満たすように代表ブリッジ ID を変更した後、ルート ブリッジ ID を最高のブリッジ プライオリティよりもよい値に変更することにより、ハイブリッド vPC または非 vPC ピア スイッチ トポロジを設定することができます。次に、ピア スイッチをイネーブルにします。

（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疑似ルート プライオリティが必要です。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

vPC 機能をイネーブルに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	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)# **spanning-tree pseudo-information**	スパニングツリー疑似情報を設定します。
ステップ 3	switch(config-pseudo)# **vlan***vlan-range***designated priority***value*	VLAN の指定ブリッジプライオリティを設定します。有効な値は、0 ～ 61440 の範囲内の 4096 の倍数です。
ステップ 4	switch(config-pseudo)# **vlan***vlan-range***root priority***value*	VLAN のルート ブリッジ プライオリティを設定します。有効な値は、0 ～ 61440 の範囲内の 4096 の倍数です。
ステップ 5	switch(config)# **vpc domain***domain-id*	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 6	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。

	コマンドまたはアクション	目的
		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 7	switch(config-vpc-domain)# **exit**	vpc-domain コンフィギュレーション モードを終了します。
ステップ 8	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 9	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。

次の例は、ハイブリッド 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)# spanning-tree pseudo-information
switch(config-pseudo)# vlan 1 designated priority 8192
switch(config-pseudo)# vlan 1 root priority 4096
switch(config-pseudo)# vpc domain 5
switch(config-vpc-domain)# peer-switch
switch(config-vpc-domain)# exit
switch(config)#
```

vPC の配信の有効化

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)# **vpc domain***domain-id*	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。

	コマンドまたはアクション	目的
ステップ 3	switch(config-vpc-domain)# **config-sync**	スイッチ上で vPC config-sync を有効にして、CFS を物理イーネット（CFSoE）に録します。 （注） 他の vPC アに対して **config syn** コマンドの設定を繰り返します。
ステップ 4	switch(config-vpc-domain)# **exit**	vPC-domain コンフギュレーション モードを終了します。
ステップ 5	switch(config-vpc-domain)# **vpcconfig-syncre-emerge**[**sync**{**export**|**import**}]	（オプション）現在マージが失敗した場に、ピア スイッチの設定のマージをトガーします。 （注） ローカル イッチ設定をピア スイッチに適用するには、**sync export** オションを使用できます。リモート スイッチ設定をローカル スイッチに適用するには、**sync impo** オプションを使用できます。
ステップ 6	switch(config-vpc-domain)# **vpcconfig-syncre-emergeinterfaceport-channel***channel-name*[**sync**{**export**|**import**}]	（オプション）現在マージが失敗した場に、ピア スイッチの **interface**

	コマンドまたはアクション	目的
		port-channel 設定のマージをトリガーします。 （注） ローカル **interface port-channel** *channel-number* コマンド設定をピア スイッチに適用するには、**sync export** オプションを使用できます。リモート **interface port-channel** *channel-number* コマンド設定をローカル スイッチに適用するには、**sync import** オプションを使用できます。
ステップ 7	switch(config-vpc-domain)# **vpcconfig-syncre-emergeinterface***typeslot/port*[**sync**{**export**|**import**}]	（オプション）現在のマージが失敗した場合に、ピア スイッチとの **interface ethernet** のマージをトリガーします。

	コマンドまたはアクション	目的
		（注） ローカル **interface ethernet slot/port** コマンド設定をピア スイッチに適用するには、**sync export** オプションを使用できます。リモート **interface ethernet slot/port** コマンド設定をローカル スイッチに適用するには、**sync import** オプションを使用できます。
ステップ 8	switch(config-vpc-domain)# **exit**	vPC ドメイン コンフィギュレーション モードを終了します。
ステップ 9	switch(config)# **exit**	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 10	switch(config)# **show vpc config-sync merge status**	ピア スイッチとの設定マージのステータスを表示します。

```
switch# configure terminal
switch(config)# vpc domain 1
switch(config-vpc-domain)# config-sync
switch(config-vpc-domain)# vpc config-sync re-merge sync export
switch(config)# vpc config-sync re-merge interface port-channel 1 sync export
switch(config)# vpc config-sync re-merge interface ethernet 1/1 sync export  import
```

```
switch(config)# exit
switch(config)# show vpc config-sync merge status
```

物理ポート vPC を介した FCoE の設定

この項では、次のトピックについて取り上げます。

物理ポート vPC インターフェイスの設定

イーサネット VDC に物理ポート vPC インターフェイスを設定するには、次のタスクを実行します。ピア VDC を設定するには、このタスクを繰り返してください。

はじめる前に

- vPC 機能をイネーブルにしていることを確認します。
- 必ず、ピア リンク ポート チャネルおよびポート チャネル メンバーを設定してください。
- 正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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)# **interface ethernet***slot/port-list*	イーサネット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、スロットの場合は 1 ~ 253 で、ポートの場合は 1 ～ 128 です。
ステップ 3	switch(config-if)# **switchport**	インターフェイスをレイヤ 2 スイッチング ポートとして設定します。
ステップ 4	switch(config-if)# **switchport mode trunk**	レイヤ 2 でトランキング VLAN インターフェイスを指定します。 トランク ポートは、同じ物理リンクの（トランク可能 VLAN リスト設定に基づいた）1 つまたは複数の VLAN でトラフィックを送ることができます。
ステップ 5	switch(config-if)# **switchport trunk allowed vlan***vlan-list*	トランキング インターフェイスで許可される VLAN の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 6	switch(config-if)# **spanning-tree port type network**	ネットワーク スパニング ツリー ポートとしてレイヤ 2 スイッチに接続するインターフェイスを設定します。
ステップ 7	switch(config-if)# **vpc***number*	ポート チャネルを vPC に移動し、インターフェイス vPC コンフィギュレーション モードを開始します。 number 引数の範囲は 1 ～ 4096 です。
ステップ 8	switch(config-if-vpc)# **lapc mode active**	**channel group mode active** コマンドを設定したピア リンク メンバ インターフェイスで LAPC をイネーブルにします。
ステップ 9	switch(config-if-vpc)# **no shutdown**	ポートを管理的にアップします。

次に、イーサネット VDC に物理ポートの vPC を設定する例を示します。

vPC 機能をイネーブルにします。
```
switch-eth(config)# feature vpc
```

ピア リンク PC を設定します。
```
switch-eth(config)# interface port-channel 1
switch-eth(config-if)# switchport
switch-eth(config-if)# switchport mode trunk
switch-eth(config-if)# switchport trunk allowed vlan 10-20
switch-eth(config-if)# spanning-tree port type network
switch-eth(config-if)# vpc peer-link
```

ピア リンク ポート チャネル メンバーを設定します。
```
switch-eth(config)# interface Ethernet3/21
switch-eth(config-if)# switchport
switch-eth(config-if)# switchport mode trunk
switch-eth(config-if)# switchport trunk allowed vlan 10-20
switch-eth(config-if)# channel group 1 mode active
switch-eth(config-if)# no shutdown
```

物理ポート vPC インターフェイスの設定
```
switch-eth(config)# interface Ethernet3/1
switch-eth(config-if)# switchport
switch-eth(config-if)# switchport mode trunk
switch-eth(config-if)# switchport trunk allowed vlan 10-20
switch-eth(config-if)# vpc 10
switch-eth(config-if-vpc)# lacp mode active
switch-eth(config-if-vpc)# no shutdown
```

次に、ピア VDC に物理ポート vPC を設定する例を示します。

vPC 機能をイネーブルにします。
```
switch-eth(config)# feature vpc
```

ピア リンク PC を設定します。
```
switch-eth(config)# interface port-channel 1
switch-eth(config-if)# switchport
switch-eth(config-if)# switchport mode trunk
switch-eth(config-if)# switchport trunk allowed vlan 10-20
```

```
switch-eth(config-if)# spanning-tree port type network
switch-eth(config-if)# vpc peer-link
```

ピア リンク ポート チャネル メンバーを設定します。

```
switch-eth(config)# interface Ethernet4/21
switch-eth(config-if)# switchport
switch-eth(config-if)# switchport mode trunk
switch-eth(config-if)# switchport trunk allowed vlan 10-20
switch-eth(config-if)# channel group 1 mode active
switch-eth(config-if)# no shutdown
```

物理ポート vPC インターフェイスの設定

```
switch-eth(config)# interface Ethernet4/1
switch-eth(config-if)# switchport
switch-eth(config-if)# switchport mode trunk
switch-eth(config-if)# switchport trunk allowed vlan 10-20
switch-eth(config-if)# vpc 10
switch-eth(config-if-vpc)# lacp mode active
switch-eth(config-if-vpc)# no shutdown
```

ヒットレス vPC ロールの変更の設定

はじめる前に

- vPC 機能をイネーブルにします。
- 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

ステップ 1 ヒットレス vPC ロールの変更機能を有効にします。
switch# **vpc role preempt**

ステップ 2 （オプション）ヒットレス vPC ロールの変更機能を検証します。
switch# **show vpc role**

ヒットレス vPC ロールの変更の設定

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。

```
! The following is an output from the show vpc role command before the
vPC hitless feature is configured !

switch# show vpc role

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

```
! Configure vPC hitless role change on the device!

switch# vpc role preempt

! The following is an output from the show vpc role command after the
vPC hitless feature is configured !

switch# 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
```

vPC 設定の確認

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。
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。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』を参照してください。

F2、F3、および FEX 上での物理ポート vPC の確認

コマンド	目的
show vpc brief	vPCに関する要約情報を表示します。
show lacp port-vpc summary	vPC ID、物理ポート、LACP ポートの状態の詳細などの、物理ポート VPC の LACP ステータスを表示します。
show lacp counters	ポート チャネルと物理ポート vPC インターフェイスのLACPカウンタを表示します。
show lacp counters interface*namenumber*	インターフェイス名別に、物理インターフェイスまたはポート チャネル インターフェイス上のLACPカウンタを表示します。
show lacp neighbor	ポートのLACPネイバー情報を表示します。
show lacp neighbor interface*namenumber*	物理インターフェイス上で設定されたポートのネイバーを表示します。

次に、vPC に関する要約情報を確認する例を示します。

```
switch# show vpc brief

vPC status
----------------------------------------------------------------------------------------
id   Port          Status     Consistency   Reason           Active    vlans
----------------------------------------------------------------------------------------
1    Ethernet1/1    up        success       - - - -          200-250,  900-1000
```

次に、vPC ID、物理ポート、LACP ポートの状態の詳細などの物理ポート VPC の LACP ステータスを確認する例を示します。

```
switch# show lacp port-vpc summary

Flags:         D - Down                    P - up
               s - Suspended              H - Hot-standby (LACP only)

VPC-Id                  Member Port
1                       Ethernet 1/1(P)
2                       Ethernet 1/2(H)
3                       Ethernet 1/3(s)
```

次に、ポート チャネルと物理ポート vPC インターフェイスの LACP カウンタを確認する例を示します。

```
switch# show lacp counters

                  LACPDUs         Marker      Marker Response    LACPDUs
Port              Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
--------------------------------------------------------------------------------
Ethernet2/1
Ethernet2/1        1677   1804     0      0        0      0         0

port-channel2
Ethernet2/2        1677   1808     0      0        0      0         0
```

次に、物理インターフェイス上の LACP カウンタを確認する例を示します。

```
switch# show lacp counters  interface ethernet 1/1

LACPDUs         Marker      Marker Response    LACPDUs
Port              Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
--------------------------------------------------------------------------------
Ethernet1/1
Ethernet1/1        17466  17464    0      0        0      0         0
```

次に、vPC とポート チャネル メンバーの両方として設定されたポートのネイバーを確認する例を示します。

```
switch# show lacp neighbor

Flags:  S - Device is sending Slow LACPDUs F - Device is sending Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode
Eth1/1 neighbors
Partner's information
            Partner               Partner                     Partner
Port        System ID             Port Number     Age         Flags
Eth1/1      32768,2-0-0-0-0-66    0x2402          41595       SA

            LACP Partner          Partner                     Partner
            Port Priority         Oper Key                    Port State
            32768                 0x91                        0x3d
```

次に、物理インターフェイス上で設定されたポートのネイバーを確認する例を示します。

```
switch# show lacp neighbor interface ethernet 1/1

Flags:  S - Device is sending Slow LACPDUs F - Device is sending Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode
Eth1/1 neighbor
Partner's information
            Partner               Partner                     Partner
Port        System ID             Port Number     Age         Flags
Eth1/1      32768,0-26-98-14-e-c1  0x207          13          SA

            LACP Partner          Partner                     Partner
            Port Priority         Oper Key                    Port State
            32768                 0x0                         0x3d
```

vPC のモニタリング

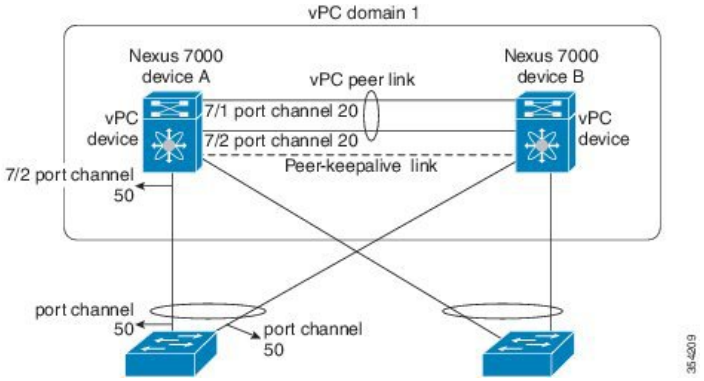
vPC 統計情報を表示するには、**show vpc statistics** コマンドを使用します。

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

図 *28*：*vPC* の設定例



ステップ 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
```

ステップ 2：（任意）ピア リンクにするインターフェイスの 1 つを専用モードに設定します。

```
switch(config)# interface ethernet 7/1, ethernet 7/3, ethernet 7/5. ethernet 7/7
switch(config-if)# shutdown
switch(config-if)# exit
switch(config)# interface ethernet 7/1
switch(config-if)# rate-mode dedicated
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)#
```

ステップ 3：（任意）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 モードに設定します。

```
switch(config)# interface ethernet 7/2, ethernet 7/4, ethernet 7/6. ethernet 7/8
switch(config-if)# shutdown
switch(config-if)# exit
switch(config)# interface ethernet 7/2
switch(config-if)# rate-mode dedicated
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)#
```

ステップ 4：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 チャネルに設定します。

```
switch(config)# interface ethernet 7/1-2
```

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

ステップ 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
```

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

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

ステップ 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
```

ステップ 8：vPC ピア リンクを設定します。

```
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)#
```

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

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

ステップ 10：設定を保存します。

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

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

関連資料

関連項目	マニュアル タイトル
『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/interfaces/command/reference/if_cmds.html
『*Interfaces Configuration Guide, Cisco DCNM for LAN*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/dcnm/interfaces/configuration/guide/if_dcnm.html
『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/system_management/configuration/guide/sm_nx_os_cg.html
『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/high_availability/configuration/guide/b_Cisco_Nexus_7000_Series_NX-OS_High_Availability_and_Redundancy_Guide.html
『*Cisco Nexus 2000 Series NX-OS Fabric Extender Software Configuration Guide for Cisco Nexus 7000 Series Switches, Release 6.x*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus2000/sw/configuration/guide/rel_6_1/b_Cisco_Nexus_2000_Series_NX-OS_Fabric_Extender_Software_Configuration_Guide_Release_6-x.html
『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/virtual_device_context/configuration/guide/b-7k-Cisco-Nexus-7000-Series-NX-OS-Virtual-Device-Context-Configuration-Guide.html
『*Cisco NX-OS Licensing Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/licensing/guide/b_Cisco_NX-OS_Licensing_Guide.html
VLAN、MAC アドレス テーブル、プライベート VLAN、およびスパニング ツリー プロトコル。 『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/layer2/configuration/guide/b_Cisco_Nexus_7000_Series_NX-OS_Layer_2_Switching_Configuration_Guide.html
『*Cisco Nexus 7000 Series NX-OS FabricPath Command Reference*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/fabricpath/command/reference/fp_cmd_book.html
『*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/fabricpath/configuration/guide/b-Cisco-Nexus-7000-Series-NX-OS-FP-Configuration-Guide-6x.html
『Cisco Nexus 7000 Series NX-OS Release Notes』	http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-release-notes-list.html

標準

標準	タイトル
IEEE 802.3ad	—

MIB

MIB	MIB のリンク
• IEEE8023-LAG-CAPABILITY • CISCO-LAG-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

第 9 章

ブレイクアウト モードのインターフェイスの設定

ブレイクアウトの機能履歴

この表には、機能の追加や変更によるリリースの更新内容のみが記載されています。

表 *17*：ブレイクアウトの機能履歴

機能名	リリース	機能情報
ブレイクアウト	6.2(6) 6.2(8)	Cisco Nexus 7000 シリーズ スイッチ上のブレイクアウト機能に対するサポートが追加されました。 Cisco Nexus 7700 シリーズ スイッチ上のブレイクアウト機能に対するサポートが追加されました。

ブレイクアウトについて

Cisco Nexus 7000 シリーズ スイッチと Cisco Nexus 7700 スイッチは、ブレイクアウト機能をサポートします。ブレイクアウトを使用すれば、40 ギガビット イーサネット ポートを 4 つの独立した論理 10 ギガビットイーサネットポートに分割することができます。ブレイクアウトは、アクティブな Twinax（7 ～ 10 m）ケーブルまたはマルチモード ファイバ ケーブル（MTP コネクタまたは MPO コネクタ付きの SR4 光ケーブル）でサポートされます。

（注） ブレイクアウト機能が設定されている場合は、対応するモジュールがリロードされ、対応するインターフェイスの設定が削除されます。

ブレイクアウト機能は次のモジュールでサポートされます。

- Cisco Nexus 7000 F3 シリーズ 12 ポート 40 ギガビット イーサネット モジュール
- Cisco Nexus 7000 M2 シリーズ 6 ポート 40 ギガビット イーサネット モジュール
- Cisco Nexus 7700 F3 シリーズ 24 ポート 40 ギガビット イーサネット モジュール

ポートでのブレイクアウトの設定

はじめる前に

正しい仮想ドメイン コンテキスト（VDC）に入っていることを確認します。**switchto vdc** コマンドを使用して必要な VDC に移動します。

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)# **interface breakout module** *slot* **port** *port-range* **map 10g-4x**	ポートのブレイクアウト機能を設定します。 • *slot*：シャーシモデル別のポートのスロット番号。 • *port-range*：ブレイクアウトを設定する単一のポートまたはポートの範囲。

	コマンドまたはアクション	目的
ステップ 3	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することで、変更を保存します。

次の例では、1 つの 40 ギガビット イーサネット ポートを 4 つの 10 ギガビット イーサネット ポートにブレイクアウトする方法を示します。

```
switch# configure terminal
switch(configure)# interface breakout module 1 port 1-12 map 10g-4x
switch(configure)# copy running-config startup-config
```

ブレイクアウト設定の削除

はじめる前に

正しい仮想ドメイン コンテキスト（VDC）に入っていることを確認します。**switchto vdc** コマンドを使用して必要な VDC に移動します。

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)# **no interface breakout module** *slot* **port** *port-range* **map 10g-4x**	ポート モジュールにおけるブレイクアウトの設定を削除して、インターフェイスを 40 ギガビット イーサネット モードの動作に戻します。 • *slot*：シャーシモデル別のモジュールのスロット番号。 （注） ブレイクアウト機能の設定時に対応するポートに使用したものと同じ *slot* モジュール値を入力します。 • *port-range*：単一のポートまたはポートの範囲。 （注） ブレイクアウト機能の設定時に対応するポートに使用したものと同じ *port-range* 値を入力します。

	コマンドまたはアクション	目的
ステップ 3	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することで、変更を保存します。

次の例では、ポート上のブレイクアウト設定を削除して、40 ギガビット イーサネット モードの動作に戻す方法を示します。

```
switch# configure terminal
switch(configure)# no interface breakout module 1 port 1-12 map 10g-4x
switch(configure)# copy running-config startup-config
```

ブレイクアウト設定の確認

ブレイクアウト設定を確認するには、次のコマンドを使用します。これらのコマンドは任意の順序で使用できます。

手順

ステップ 1 **show interface eth1/1 capabilities**
インターフェイス コンフィギュレーションに関する情報を表示します。

ステップ 2 **show interface brief**
インターフェイス設定の概要を表示します。

次に、インターフェイスのブレイクアウト設定を確認する例を示します。

```
switch# show interface ethernet 1/1 capabilities | i Breakout

Breakout capable:      yes
```

次に、インターフェイス設定の概要を表示するために使用される **show interface brief** コマンドの出力例を示します。

```
switch# show interface brief | grep 1/1

Eth1/1/1      --      eth  routed down    SFP not inserted           auto(D) --
Eth1/1/2      --      eth  routed down    SFP not inserted           auto(D) --
Eth1/1/3      --      eth  routed down    SFP not inserted           auto(D) --
Eth1/1/4      --      eth  routed down    SFP not inserted           auto(D) --
```

第 10 章

IP トンネルの設定

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

IP トンネル設定の機能履歴

この表には、機能の追加や変更によるリリースの更新内容のみが記載されています。

機能名	リリース	機能情報
GRE トンネル	7.3(0)DX(1)	M3 シリーズ モジュールのサポートが追加されました。
GRE トンネル	6.2(10)	F3 シリーズ モジュールのサポートが追加されました。
異なる VRF のトンネルとトランスポートのサポート	6.1(1)	この機能が導入されました。
デフォルト以外の VDC および VRF 内の IP トンネル	4.2(1)	この機能が導入されました。
IP トンネル	4.0(1)	この機能が導入されました。

IP トンネルについて

IP トンネルを使うと、同じレイヤまたは上位層プロトコルをカプセル化して、2 台のデバイス間で作成されたトンネルを通じて IP に結果を転送できます。

IP トンネルの概要

IP トンネルは次の 3 つの主要コンポーネントで構成されています。

- パッセンジャ プロトコル：カプセル化する必要があるプロトコル。パッセンジャ プロトコルの例には IPv4 があります。
- キャリア プロトコル：パッセンジャ プロトコルをカプセル化するために使用するプロトコル。Cisco NX-OS はキャリア プロトコルとして GRE をサポートします。
- トランスポートプロトコル：カプセル化したプロトコルを伝送するために使用するプロトコル。トランスポート プロトコルの例には IPv4 があります。

IP トンネルは IPv4 などのパッセンジャ プロトコルを使用し、このプロトコルを GRE などのキャリア プロトコル内にカプセル化します。次に、このキャリア プロトコルは IPv4 などのトランスポート プロトコルを通じてデバイスから送信されます。

対応する特性を持つトンネル インターフェイスをトンネルの両端にそれぞれ設定します。

詳細については、「IP トンネルの設定」の項を参照してください。

設定の前にトンネル機能をイネーブルにする必要があります。Cisco NX-OS リリース 4.2 から、システムは機能のディセーブル化の前に自動的にチェックポイントを作成するため、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 7000 Series NX-OS System Management Configuration Guide*』を参照してください。

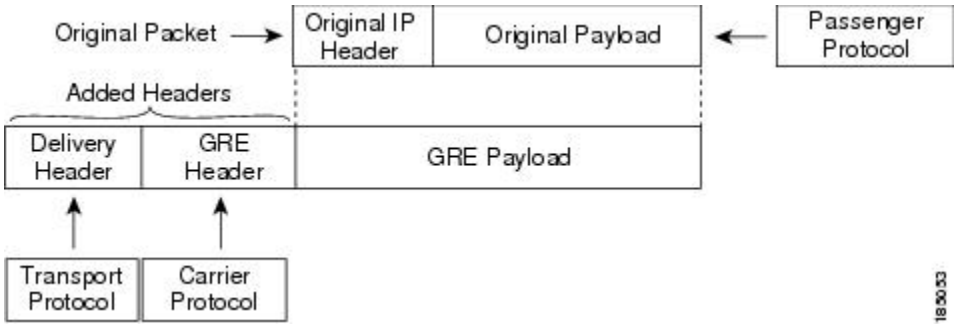
GRE トンネル

（注） Cisco NX-OS リリース 5.1(1) 以降では、ソフトウェアは GRE トンネルを通じてマルチキャスティングをサポートします。

Generic Routing Encapsulation（GRE）をさまざまなパッセンジャ プロトコルのキャリア プロトコルとして使用できます。

以下の図は、GRE トンネルの IP トンネルのコンポーネントを示しています。オリジナルのパッセンジャ プロトコル パケットは GRE ペイロードとなり、デバイスはパケットに GRE ヘッダーを追加します。次にデバイスはトランスポート プロトコル ヘッダーをパケットに追加して送信します。

図 *29* : *GRE PDU*



Path MTU Discovery

パス最大伝送単位（MTU）ディスカバリ（PMTUD）は、パケットの発信元から宛先へのパスに沿って最小 MTU を動的に決定することで、2 つのエンドポイント間のパスのフラグメンテーションを防ぎます。PMTUD は、パケットにフラグメンテーションが必要であるという情報がインターフェイスに届くと、接続に対する送信 MTU 値を減らします。

PMTUD をイネーブルにすると、インターフェイスはトンネルを通過するすべてのパケットに Don't Fragment（DF）ビットを設定します。トンネルに入ったパケットがそのパケットの MTU 値よりも小さい MTU 値を持つリンクを検出すると、リモート リンクはそのパケットをドロップし、パケットの送信元にインターネット制御メッセージプロトコル（ICMP）メッセージを返します。このメッセージには、フラグメンテーションが要求されたこと（しかし許可されなかったこと）と、パケットをドロップしたリンクの MTU が含まれています。

（注） トンネル インターフェイスの PMTUD は、トンネル エンドポイントがトンネルのパスでデバイスによって生成される ICMP メッセージを受信することを要求します。ファイアウォール接続を通じて PMTUD を使用する前に、ICMP メッセージが受信できることを確認してください。Cisco NX-OS ソフトウェアは、デフォルトで、ICMP 到達不能メッセージを無効にします。ICMP 到達不能メッセージは、**ip unreachables** インターフェイス コマンドを使用して Cisco NX-OS ソフトウェアで有効にできます。

仮想化のサポート

Cisco NX-OS リリース 4.2 以降では、非デフォルトの VDC および非デフォルトの VRF のトンネルを設定できます。ある VDC に設定されたトンネルは、同じ番号を持つ別の VDC に設定されたトンネルとは区別されます。たとえば、VDC 1 のトンネル 0 は VDC 2 のトンネル 0 とは異なります。

Cisco NX-OS リリース 6.1(1) より前の場合は、トンネル インターフェイスとトンネル トランスポートは同じ VRF にある必要があります。VDC については、『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide』を、VRF については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

ハイ アベイラビリティ

IP トンネルはステートフル再起動をサポートします。ステートフル再起動はスーパーバイザ切り替え時に発生します。切り替え後、Cisco NX-OS は実行時の設定を適用します。

インターフェイスのライセンス要件

vPC には、ライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

IP トンネルには Enterprise Services ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『Cisco NX-OS Licensing Guide』を参照してください。

他のインターフェイスにはライセンスが必要ありません。

IP トンネルの前提条件

IP トンネルには次の前提条件があります。

- IP トンネルを設定するための TCP/IP に関する基礎知識があること。

- スイッチにログインしている。
- Cisco NX-OS の Enterprise Services ライセンスをインストールしていること。
- IP トンネルを設定してイネーブルにする前にデバイスのトンネリング機能をイネーブルにしておくこと。

注意事項と制約事項

IP トンネルの設定に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS は、IETF RFC 2784 に定義されている GRE ヘッダーをサポートします。Cisco NX-OS は、トンネル キーと IETF RFC 1701 のその他のオプションをサポートしません。
- トンネルは、Cisco Nexus 7000 シリーズ プラットフォームの M シリーズのカードでのみサポートされます。
- Cisco NX-OS は、トンネル インターフェイスの Web Cache Control Protocol（WCCP）をサポートしません。
- トンネル機能は、Cisco Nexus 7000 シリーズ プラットフォームと Cisco Nexus 7700 シリーズ プラットフォーム上の M シリーズ モジュールと F3 シリーズ モジュールでのみサポートされます。
- Cisco NX-OS は、GRE トンネル キープアライブをサポートしません。

デフォルト設定

パラメータ	デフォルト
パス MTU ディスカバリ経過時間タイマー	10 分
パス MTU ディスカバリの最小 MTU	64
トンネル機能	ディセーブル

IP トンネルの設定

トンネリングのイネーブル化

IP トンネルを設定する前にトンネリング機能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	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 tunnel**	新しいトンネル インターフェイスを作成できます。 トンネルインターフェイス機能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 3	switch(config)# **show feature**	（任意） デバイス上でイネーブルされている機能に関する情報を表示します。
ステップ 4	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。

トンネル インターフェイスの作成

トンネル インターフェイスを作成して、この論理インターフェイスを IP トンネルに設定できます。

はじめる前に

Cisco NX-OS リリース 6.1 以降のリリースでは、異なる VRF でトンネル送信元およびトンネル宛先を設定できます。トンネリング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	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 tunnel***number*	新しいトンネルインターフェイスを作成します。
ステップ 3	switch(config-if)# **tunnel source** {*ip-address* | *interface-name*}	この IP トンネルの送信元アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 4	switch(config-if)# **tunnel destination** {*ip-address* | *host-name*}	この IP トンネルの宛先アドレスを設定します。
ステップ 5	switch(config-if)# **tunnel use-vrf***vrf-name*	設定された VRF をトンネルの IP 宛先アドレスの検索に使用します。
ステップ 6	switch(config-if)# **show interfaces tunnel***number*	（任意） トンネルインターフェイスの統計情報を表示します。
ステップ 7	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。

トンネル インターフェイスおよび関連するすべての設定を削除するには、**no interface tunnel** コマンドを使用します。

コマンド	目的
no interface tunnel*number*	トンネルインターフェイスおよび関連する設定を削除します。

次のオプション パラメータを設定して、インターフェイス コンフィギュレーション モードでトンネルを調整することができます。

コマンド	目的
description*string*	トンネルの説明を設定します。
mtu*value*	インターフェイスで送信される IP パケットの MTU を設定します。
tunnel ttl*value*	トンネルの存続可能時間を設定します。範囲は 1 ～ 255 です。

次に、トンネル 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 tunnel 1
switch(config-if)# tunnel source ethernet 1/2
switch(config-if)# tunnel destination 192.0.2.1
switch(config-if)# copy running-config startup-config
```

GRE トンネルの設定

トンネル インターフェイスを GRE トンネル モードに設定できます。

はじめる前に

トンネリング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	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 tunnel***number*	新しいトンネル インターフェイスを作成します。
ステップ 3	switch(config-if)# **tunnel mode gre ip**	このトンネル モードを GRE に設定します。
ステップ 4	switch(config-if)# **show interfaces tunnel***number*	（任意） トンネル インターフェイスの統計情報を表示します。
ステップ 5	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。

パス MTU ディスカバリのイネーブル化

トンネルでパス MTU ディスカバリをイネーブルにするには、**tunnel path-mtu discovery** コマンドを使用します。

コマンド	目的
tunnel path-mtu-discovery [**age-timer***min*] [**min-mtu***bytes*]	トンネル インターフェイスで Path MTU Discovery（PMTUD）をイネーブルにします。パラメータは次のとおりです。 • *mins*：分数。有効な範囲は 10 ～ 30 です。デフォルトは 10 です。 • *mtu-bytes*：認識された最小 MTU。範囲は 92 ～ 65535 です。デフォルトは 92 です。

トンネル インターフェイスへの VRF メンバーシップの割り当て

VRF にトンネル インターフェイスを追加できます。

はじめる前に

トンネリング機能がイネーブルになっていることを確認します。

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

VRF 用のインターフェイスを設定した後で、トンネル インターフェイスに IP アドレスを割り当てます。

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)# **interface tunnel***number*	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)# **vrf member***vrf-name*	このインターフェイスを VRF に追加します。
ステップ 4	switch(config-vrf)# **ip address***ip-prefix/length*	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 に割り当てた後に行う必要があります。
ステップ 5	switch(config-vrf)# **show vrf** [*vrf-name*] **interface***interface-type number*	（任意） VRF 情報を表示します。
ステップ 6	switch(config-vrf)# **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。

次に、VRF にトンネル 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 tunnel 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
```

IP トンネリングの設定例

次の例では、簡易 GRE トンネルを示します。イーサネット 1/2 は、ルータ A のトンネル送信元であり、ルータ B のトンネル宛先です。イーサネット インターフェイス 2/1 は、ルータ B のトンネル送信元であり、ルータ A のトンネル宛先です。

ルータ A：

```
feature tunnel
interface tunnel 0
  ip address 209.165.20.2/8
  tunnel source ethernet 1/2
  tunnel destination 192.0.2.2
  tunnel mode gre ip
  tunnel path-mtu-discovery 25 1500
interface ethernet1/2
  ip address 192.0.2.55/8
```

ルータ B：

```
feature tunnel
interface tunnel 0
  ip address 209.165.20.1/8
  tunnel source ethernet2/1
  tunnel destination 192.0.2.55
  tunnel mode gre ip
interface ethernet 2/1
ip address 192.0.2.2/8
```

IP トンネル設定の確認

IP トンネルの設定情報を確認するには、次のいずれかの作業を行います。

コマンド	目的
show interface tunnel*number*	トンネルインターフェイスの設定を表示します（MTU、プロトコル、転送、および VRF）。入力および出力パケット、バイト、およびパケット レートを表示します。
show interface brief | include Tunnel	トンネル インターフェイスの動作状態、IP アドレス、カプセル化のタイプ、MTU を表示します。
show interface tunnel*number***description**	トンネルインターフェイスに設定された説明を表示します。
show interface tunnel*number***status**	トンネルインターフェイスの動作ステータスを表示します。
show interface tunnel*number***status err-disabled**	トンネル インターフェイスの errdisable 状態を表示します。

関連資料

関連項目	マニュアル タイトル
『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/interfaces/command/reference/if_cmds.html
『*Interfaces Configuration Guide, Cisco DCNM for LAN*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/dcnm/interfaces/configuration/guide/if_dcnm.html
『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/system_management/configuration/guide/sm_nx_os_cg.html
『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/high_availability/configuration/guide/b_Cisco_Nexus_7000_Series_NX-OS_High_Availability_and_Redundancy_Guide.html
『*Cisco Nexus 2000 Series NX-OS Fabric Extender Software Configuration Guide for Cisco Nexus 7000 Series Switches, Release 6.x*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus2000/sw/configuration/guide/rel_6_1/b_Cisco_Nexus_2000_Series_NX-OS_Fabric_Extender_Software_Configuration_Guide_Release_6-x.html
『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/virtual_device_context/configuration/guide/b-7k-Cisco-Nexus-7000-Series-NX-OS-Virtual-Device-Context-Configuration-Guide.html
『*Cisco NX-OS Licensing Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/licensing/guide/b_Cisco_NX-OS_Licensing_Guide.html
VLAN、MAC アドレス テーブル、プライベート VLAN、およびスパニング ツリー プロトコル。 『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/layer2/configuration/guide/b_Cisco_Nexus_7000_Series_NX-OS_Layer_2_Switching_Configuration_Guide.html
『*Cisco Nexus 7000 Series NX-OS FabricPath Command Reference*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/fabricpath/command/reference/fp_cmd_book.html
『*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*』	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/fabricpath/configuration/guide/b-Cisco-Nexus-7000-Series-NX-OS-FP-Configuration-Guide-6x.html

関連項目	マニュアル タイトル
『Cisco Nexus 7000 Series NX-OS Release Notes』	http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-release-notes-list.html

第 11 章

Q-in-Q VLAN トンネルの設定

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

Q-in-Q トンネルおよびレイヤ 2 プロトコルのトンネリングの機能履歴

この表には、機能の追加や変更によるリリースの更新内容のみが記載されています。

表 *18* : *Q-in-Q* トンネルおよびレイヤ *2* プロトコルのトンネリングの機能履歴

機能名	リリース	機能情報
インターフェイスおよび VLAN のポリシー エラーの表示	6.2(2)	**show interface status error policy** コマンドが追加されました。
Q-in-Q VLAN トンネル	5.0(2)	この機能が導入されました。
L2 プロトコルのトンネリング	5.0(2)	この機能が導入されました。

Q-in-Q トンネルについて

この章では、Cisco NX-OS デバイス上で IEEE 802.1Q-in-Q (Q-in-Q) VLAN トンネルおよびレイヤ 2 プロトコルのトンネリングを設定する方法について説明します。

Q-in-Q VLAN トンネルを使用することで、サービス プロバイダーは第 2 の 802.1Q タグをすでにタグ付けされたフレームに追加して、カスタマーに内部使用の VLAN をすべて提供しながら、インフラストラクチャ内で異なるカスタマーのトラフィックを分離することができます。

Q-in-Q トンネリング

サービス プロバイダーのビジネス カスタマーには、多くの場合、サポートする VLAN ID および VLAN の数に固有の要件があります。同一サービスプロバイダー ネットワークのさまざまなカスタマーが必要とする VLAN 範囲は重複し、インフラストラクチャを通るカスタマーのトラフィックは混合してしまうことがあります。カスタマーごとに一意の VLAN ID 範囲を割り当てると、カスタマーの設定が制限され、802.1Q 仕様の 4096 の VLAN に関する上限を容易に超えてしまいます。

（注） Q-in-Q は、ポート チャネルおよび仮想ポート チャネル（vPC）でサポートされます。非対称リンクとしてポート チャネルを設定するには、ポート チャネル内のすべてのポートが同じトンネリング設定でなければなりません。

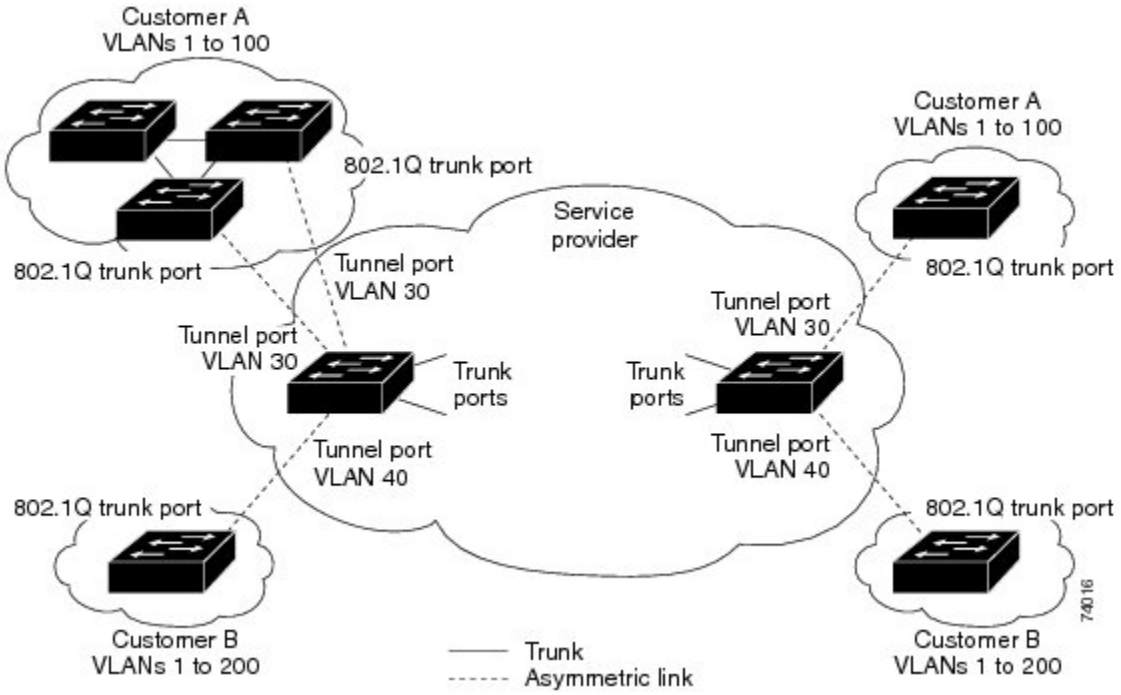
サービス プロバイダーは、802.1Q トンネリング機能を使用すると、単一の VLAN を使用して、複数の VLAN を含むカスタマーをサポートできます。同一の VLAN 上にあるように見えるときでも、サービス プロバイダー インフラストラクチャ内のカスタマーの VLAN ID を保護したり、異なるカスタマーの VLAN トラフィックを分離しておくことができます。IEEE 802.1Q トンネリングは、VLAN-in-VLAN 階層構造およびタグ付きパケットへのタギングによって、VLAN スペースを拡張します。802.1Q トンネリングをサポートするように設定されたポートは、トンネル ポートといいます。トンネリングを設定する場合、トンネリング専用の VLAN にトンネル ポートを割り

当てます。カスタマーごとに個別の VLAN が必要ですが、その VLAN はカスタマーの VLAN をすべてサポートします。

カスタマー デバイスの IEEE 802.1Q トランク ポートから、通常どおりに適切な VLAN ID でタグ付けされたカスタマー トラフィックが、サービスプロバイダー エッジ スイッチのトンネル ポートに着信します。カスタマー デバイスとエッジ スイッチの間のリンクは、一方の端が 802.1Q トランク ポート、反対側がトンネル ポートとして設定されているので、非対称リンクです。それぞれのカスタマーに固有のアクセス VLAN ID には、トンネル ポート インターフェイスを割り当てます。以下の図を参照してください。

（注） 選択的 Q-in-Q トンネリングはサポートされません。トンネル ポートに着信すべてのフレームは、Q-in-Q タギングの対象となります。

図 *30*：*802.1Q-in-Q* トンネル ポート

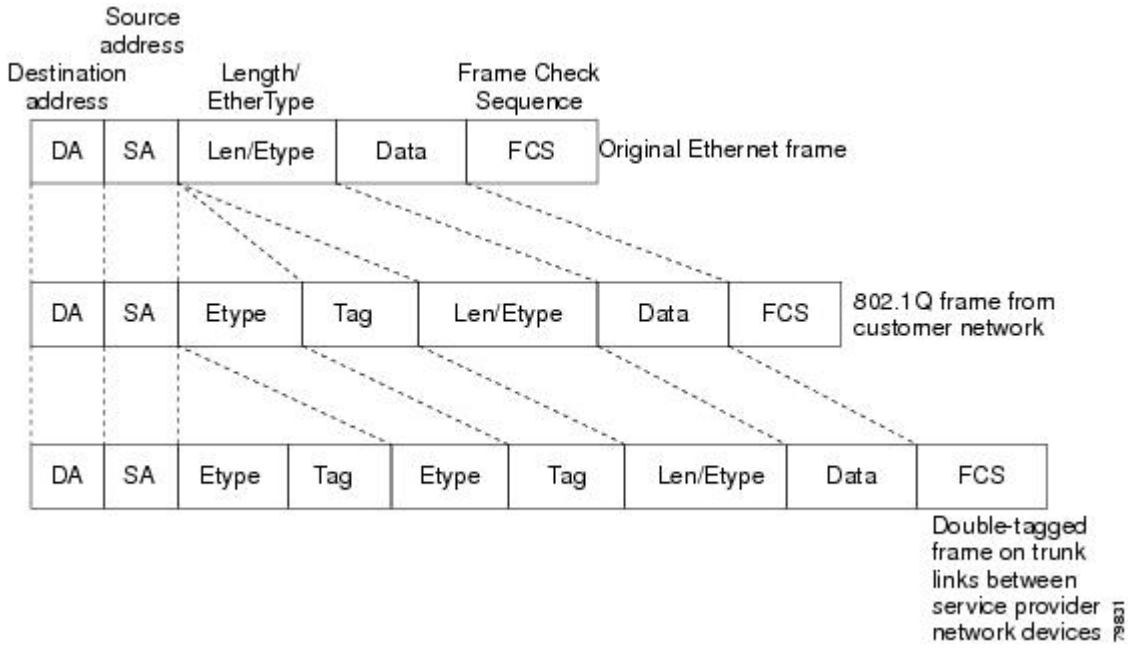


サービスプロバイダー エッジ スイッチのトンネル ポートに着信するパケット（適切な VLAN ID ですでに 802.1Q タグ付けされている）は、カスタマーに一意である VLAN ID を含む 802.1Q タグの別のレイヤでカプセル化されます。元々のカスタマーの 802.1Q タグは、カプセル化されたパケットの中に維持されます。したがって、サービスプロバイダー インフラストラクチャに着信するパケットは二重にタグ付けされます。

外部タグには、カスタマーの（サービス プロバイダーによって割り当てられた）アクセス VLAN ID が含まれます。（カスタマーによって割り当てられた）内部タグの VLAN ID は、受信トラ

フィックの VLAN です。この二重タギングは、以下の図に示すようにタグ スタック構成 Double-Q または Q-in-Q と呼ばれます。

図 *31*：タグなし、*802.1Q* タグ付き、および二重タグ付きイーサネット フレーム



この方法で、外部タグの VLAN ID スペースは内部タグの VLAN ID スペースに依存しません。単一の外部 VLAN ID は、個々のカスタマーの全体の VLAN ID スペースを表すことができます。この方法により、カスタマーのレイヤ 2 ネットワークをサービス プロバイダー ネットワーク全体に拡張して、複数のサイトに仮想 LAN インフラストラクチャを作成することも可能になります。

（注） 階層型タギング、すなわちマルチレベルの dot1q タギング Q-in-Q はサポートされていません。

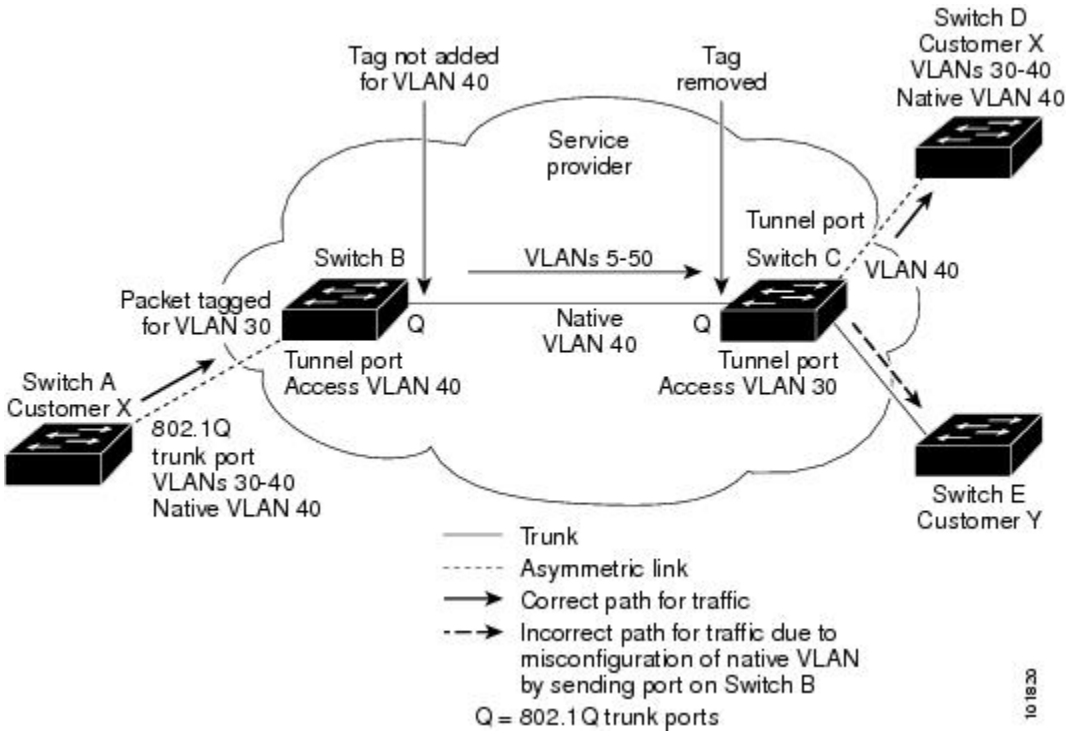
ネイティブ VLAN のリスク

エッジ スイッチで 802.1Q トンネリングを設定する場合は、サービス プロバイダー ネットワークにパケットを送信するために、802.1Q トランク ポートを使用する必要があります。ただし、サービスプロバイダー ネットワークのコアを通過するパケットは、IEEE 802.1Q トランク、ISL トランク、または非トランキング リンクで伝送される場合があります。802.1Q トランクをこれらのコア スイッチで使用する場合には、802.1Q トランクのネイティブ VLAN を、同じスイッチ上の dot1q トンネル ポートのどのネイティブ VLAN にも一致させないでください。ネイティブ VLAN 上のトラフィックが 802.1Q 送信トランク ポートでタグ付けされなくなるためです。

以下の図では、VLAN 40 は、サービスプロバイダー ネットワークの入力エッジ スイッチ（スイッチ B）において、カスタマー X からの 802.1Q トランク ポートのネイティブ VLAN として設定さ

れています。カスタマー X のスイッチ A は、VLAN 30 のタグ付きパケットを、アクセス VLAN 40 に属する、サービスプロバイダー ネットワークのスイッチ B の入力トンネル ポートに送信します。トンネル ポートのアクセス VLAN（VLAN 40）は、エッジ スイッチのトランク ポートのネイティブ VLAN（VLAN 40）と同じなので、トンネル ポートから受信したタグ付きパケットに 802.1Q タグは追加されません。パケットには VLAN 30 タグだけが付いて、サービスプロバイダー ネットワークで出力エッジ スイッチ（スイッチ C）のトランク ポートに送信され、出力スイッチ トンネルによってカスタマー Y に間違えて送信されます。

図 *32*：ネイティブ *VLAN* のリスク



ネイティブ VLAN の問題を解決する方法は 2 つあります。

- 802.1Q トランクから出るすべてのパケット（ネイティブ VLAN を含む）が、vlan dot1q tag native コマンドを使用してタグ付けされるように、エッジ スイッチを設定します。すべての 802.1Q トランクでネイティブ VLAN パケットにタグを付けるようにスイッチを設定した場合、スイッチはタグなしパケットを受信しますが、タグ付きパケットだけを送信します。

（注） **vlan dot1q tag native** コマンドは、すべてのトランク ポート上のタギング動作に影響を与えるグローバル コマンドです。

- エッジ スイッチのトランク ポートのネイティブ VLAN ID が、カスタマー VLAN 範囲に属さないようにします。たとえばトランク ポートが VLAN100 ～ 200 のトラフィックを運ぶ場合は、この範囲以外の番号をネイティブ VLAN に割り当てます。

レイヤ 2 プロトコルのトンネリングについて

サービスプロバイダー ネットワーク経由で接続される複数のサイトのカスタマーは、さまざまなレイヤ 2 プロトコルを実行して、すべてのリモート サイトおよびローカル サイトを含むようにトポロジを拡大する必要があります。スパニングツリー プロトコル（STP）が適切に稼働している必要があり、すべての VLAN で、ローカル サイトおよびサービスプロバイダー インフラストラクチャ経由のすべてのリモート サイトを含む、適切なスパニングツリーを構築する必要があります。Cisco Discovery Protocol（CDP）は、ローカルおよびリモート サイトから隣接するシスコ デバイスを検出することができる必要があり、VLAN トランキング プロトコル（VTP）は、カスタマー ネットワークのすべてのサイトを通して一貫した VLAN 設定を提供する必要があります。

プロトコル トンネリングがイネーブルになると、サービス プロバイダー インフラストラクチャの受信側にあるエッジ スイッチが、レイヤ 2 プロトコルを特別の MAC アドレスでカプセル化し、サービス プロバイダー ネットワークの端まで送信します。ネットワークのコア スイッチでは、このパケットが処理されずに通常のパケットとして転送されます。CDP、STP、または VTP のブリッジプロトコルデータユニット（BPDU）は、サービスプロバイダーインフラストラクチャを通過し、サービスプロバイダーネットワークの発信側にあるカスタマースイッチまで配信されます。同一パケットは同じ VLAN のすべてのカスタマー ポートで受信されます。

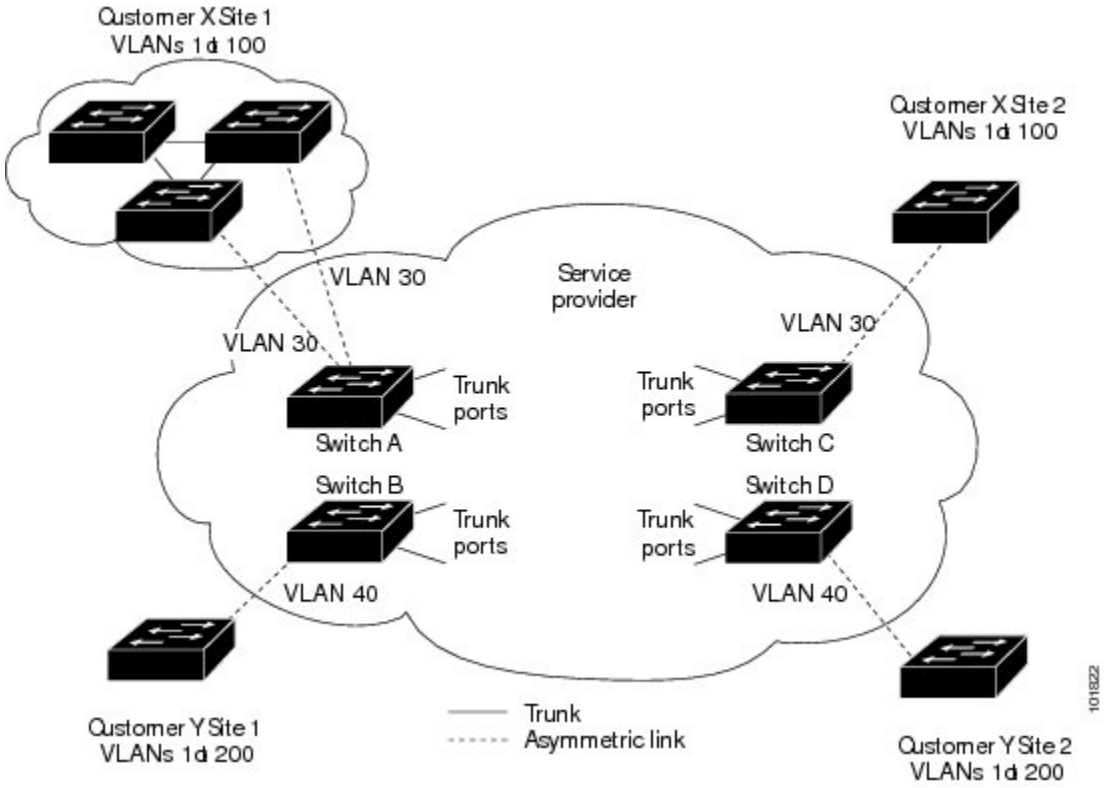
802.1Q トンネリング ポートでプロトコルのトンネリングをイネーブルにしていない場合、サービスプロバイダー ネットワークの受信側のリモート スイッチでは BPDU を受信せず、STP、CDP、802.1X、および VTP を適切に実行できません。プロトコルのトンネリングがイネーブルである場合、それぞれのカスタマー ネットワークのレイヤ 2 プロトコルは、サービスプロバイダー ネットワーク内で動作しているものから完全に区別されます。802.1Q トンネリングでサービスプロバイダーネットワークを通してトラフィックを送信する、さまざまなサイトのカスタマースイッチでは、カスタマー VLAN が完全に認識されます。

（注） レイヤ 2 プロトコルのトンネリングは、ソフトウェアで BPDU をトンネリングすることで動作します。スーパーバイザが受信する多数の BPDU により CPU の負荷が大きくなります。スーパーバイザ CPU の負荷を軽減するために、ハードウェア レート リミッタを使用する必要がある場合があります。「レイヤ 2 プロトコル トンネル ポートのレート制限の設定」の項を参照してください。

たとえば、以下の図で、カスタマー X には、サービス プロバイダー ネットワークを介して接続された同じ VLAN に 4 台のスイッチがあります。ネットワークが BPDU をトンネリングしない

と、ネットワークの遠端のスイッチは STP、CDP、802.1X、および VTP プロトコルを正しく実行できません。

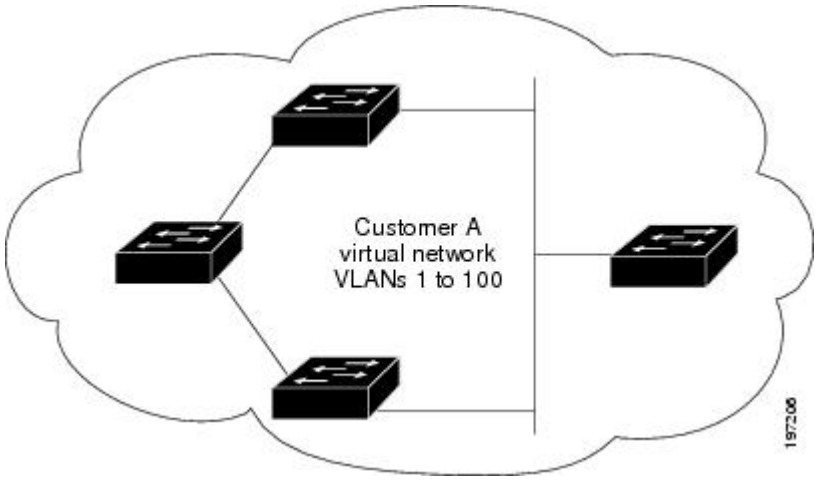
図 *33*：レイヤ *2* プロトコル トンネリング



前の例では、カスタマー X、サイト 1 のスイッチ上の VLAN で動作する STP は、カスタマー X、サイト 2 のスイッチに基づくコンバージェンス パラメータを考慮せずに、このサイトのスイッチのスパニング ツリーを構築します。

以下の図は、BPDU トンネリングがイネーブルになっていない場合の、カスタマーのネットワークでの結果トポロジを示します。

図 *34*：*BPDU* トンネリングを使用しない仮想ネットワーク トポロジ



インターフェイスのライセンス要件

vPC には、ライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

IP トンネルには Enterprise Services ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『Cisco NX-OS Licensing Guide』を参照してください。

他のインターフェイスにはライセンスが必要ありません。

注意事項と制約事項

Q-in-Q トンネリングおよびレイヤ 2 トンネリングには、次の設定に関する注意事項と制約事項があります。

- Q-in-Q トンネルは、F1 ラインカードではサポートされていません。
- サービスプロバイダー ネットワーク内のスイッチは、Q-in-Q タギングによる MTU サイズの増加に対応するように設定する必要があります。
- Q-in-Q タグ付きパケットの MAC アドレス ラーニングは、外部 VLAN（サービス プロバイダー VLAN）タグに基づいています。単一の MAC アドレスが複数の内部（カスタマー）VLAN で使用される配置においては、パケット転送の問題が発生する場合があります。

- レイヤ 3 以上のパラメータは、トンネル トラフィックでは識別できません（レイヤ 3 宛先や送信元アドレスなど）。トンネル型トラフィックはルーティングできません。
- Cisco Nexus 7000 シリーズのデバイスは、トンネル トラフィックに対する MAC レイヤ ACL/QoS（VLAN ID および送信元/宛先 MAC アドレス）のみを提供できます。
- MAC アドレスに基づくフレーム配布を使用する必要があります。
- 非対称リンクでは 1 つのポートだけがトラッキングするため、Dynamic Trunking Protocol（DTP）をサポートしません。無条件でトランクになるように、非対称リンクの 802.1Q トランク ポートを設定する必要があります。
- プライベート VLAN をサポートするように設定されたポートに 802.1Q トンネリング機能を設定することはできません。プライベート VLAN は、これらの導入には必要ではありません。
- トンネル VLAN の IGMP スヌーピングをディセーブルにする必要があります。
- コントロール プレーン ポリシング（CoPP）はサポートされません。
- ネイティブ VLAN でのタギングを維持し、タグなしトラフィックを廃棄するには、vlan dot1Q tag native コマンドを入力する必要があります。このコマンドにより、ネイティブ VLAN の設定ミスを防止できます。
- 802.1Q インターフェイスをエッジ ポートにするように手動で設定する必要があります。
- Dot1x トンネリングはサポートされていません。
- EtherType 設定が複数の Cisco Nexus デバイスで有効になるように、EPLD を新しいバージョンにアップグレードする必要があります。
- トンネル全体に STP BPDU または CDP パケットを転送するために、レイヤ 2 プロトコル機能を設定できません。

Q-in-Q トンネルおよびレイヤ 2 プロトコルのトンネリングの設定

802.1Q トンネル ポートの作成

switchport mode コマンドを使用して dot1q-tunnel ポートを作成します。

（注） **spanning-tree port type edge** コマンドを使用して、エッジ ポートに 802.1Q トンネル ポートを設定する必要があります。ポートの VLAN メンバーシップは、**switchport access vlan***vlan-id* コマンドを使用して変更されます。

dot1q-tunnel ポートに割り当てられたアクセス VLAN の IGMP スヌーピングをディセーブルにして、マルチキャスト パケットが Q-in-Q トンネルを通過できるようにする必要があります。

はじめる前に

はじめに、スイッチ ポートとしてインターフェイスを設定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	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 ethernet***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)# **switchport**	インターフェイスをレイヤ 2 スイッチング ポートとして設定します。
ステップ 4	switch(config-if)# **switchport mode dot1q-tunnel**	ポートに 802.1Q トンネルを作成します。インターフェイス モードを変更すると、ポートはダウンし、再初期化（ポート フラップ）されます。トンネル インターフェイスでは BPDU フィルタリングがイネーブルになり、CDP がディセーブルになります。
ステップ 5	switch(config-if)# **no switchport mode dot1q-tunnel**	（任意） ポートで 802.1Q トンネルをディセーブルにします。
ステップ 6	switch(config-if)# **exit**	設定モードを終了します。
ステップ 7	switch(config)# **show dot1q-tunnel** [**interface***if-range*]	（任意） dot1q-tunnel モードにあるすべてのポートを表示します。必要に応じて、表示するインターフェイスまたはインターフェイスの範囲を指定できます。
ステップ 8	switch(config)# **show interface status error policy** [**detail**]	（任意） ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN を表示します。これにより、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 9	switch(config)# **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 10	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。

次に、802.1Q トンネル ポートを作成する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 7/1
switch(config-if)# switchport
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# exit
switch(config)# exit
switch# show dot1q-tunnel
```

Q-in-Q 用の EtherType の変更

Q-in-Q カプセル化に使用するように 802.1Q EtherType 値を変更できます。

（注） 二重タグ フレームを伝送する出力トランク インターフェイス（サービス プロバイダーに接続するトランク インターフェイス）だけに EtherType を設定する必要があります。トランクの一方で EtherType を変更した場合、トランクのもう一方でも同じ値を設定する必要があります（対称構成）。

注意 設定した EtherType 値は、（Q-in-Q パケットだけではなく）インターフェイスから出るすべてのタグ付きパケットに影響します。

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。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **interface ethernet***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)# **switchport**	インターフェイスをレイヤ 2 スイッチング ポートとして設定します。
ステップ 4	switch(config-if)# **switchport dot1q ethertype***value*	ポート上の Q-in-Q トンネル用に EtherType を設定します。
ステップ 5	switch(config-if)# **no switchport dot1q ethertype**	（任意） ポートの EtherType を 0x8100 のデフォルト値にリセットします。
ステップ 6	switch(config-if)# **exit**	設定モードを終了します。
ステップ 7	switch(config)# **show interface status error policy** [**detail**]	（任意） ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN を表示します。これにより、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ 8	switch(config)# **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	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。

次に、802.1Q トンネル ポートを作成する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 7/1
switch(config-if)# switchport
switch(config-if)# switchport dot1q ethertype 0x9100
switch(config-if)# exit
switch(config)# exit
switch# show dot1q-tunnel
```

レイヤ 2 プロトコル トンネルのイネーブル化

802.1Q トンネル ポートでプロトコルのトンネリングを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	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 ethernet***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)# **switchport**	インターフェイスをレイヤ 2 スイッチング ポートとして設定します。
ステップ 4	switch(config-if)# **switchport mode dot1q-tunnel**	ポートに 802.1Q トンネルを作成します。インターフェイス モードを変更すると、ポートはダウンし、再初期化（ポート フラップ）されます。トンネル インターフェイスでは BPDU フィルタリングがイネーブルになり、CDP がディセーブルになります。
ステップ 5	switch(config-if)# **l2protocol tunnel** [**cdp** | **stp** | **vtp**]	レイヤ 2 プロトコルのトンネリングをイネーブルにします。必要に応じて、CDP、STP、または VTP トンネリングをイネーブルにできます。
ステップ 6	switch(config-if)# **no l2protocol tunnel** [**cdp** | **stp** | **vtp**]	（任意） プロトコルのトンネリングをディセーブルにします。
ステップ 7	switch(config-if)# **exit**	設定モードを終了します。
ステップ 8	switch(config)# **show interface status error policy** [**detail**]	（任意） ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN を表示します。これにより、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ 9	switch(config)# **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 10	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。

次に、802.1Q トンネル ポートでプロトコルのトンネリングをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 7/1
switch(config-if)# switchport
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# l2protocol tunnel stp
switch(config-if)# exit
switch(config)# exit
```

L2 プロトコル トンネル ポートに対するグローバル CoS の設定

トンネル ポートの入力 BPDU が指定されたクラスでカプセル化されるように、サービス クラス（CoS）の値をグローバルに指定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# **l2protocol tunnel cos***value*	すべてのレイヤ 2 プロトコルのトンネリング ポートでグローバル CoS 値を指定します。デフォルト CoS 値は 5 です。
ステップ 3	switch(config)# **no l2protocol tunnel cos**	（任意） グローバル CoS 値をデフォルト値に設定します。
ステップ 4	switch(config)# **exit**	設定モードを終了します。
ステップ 5	switch# **show interface status error policy** [**detail**]	（任意） ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN を表示します。これにより、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 6	switch# **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	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。

次に、レイヤ 2 プロトコルのトンネリングのためのグローバル CoS 値を指定する例を示します。

```
switch# configure terminal
switch(config)# l2protocol tunnel cos 6
switch(config)# exit
```

レイヤ 2 プロトコル トンネル ポートのレート制限の設定

レイヤ 2 プロトコルのトンネリング用にハードウェア レート リミッタの設定を指定できます。デフォルトは 500 パケット/秒に設定されます。ロードまたはカスタマーにトンネリングされる VLAN 数によって、カスタマーのネットワーク上の STP のエラーを回避するためにこの値を調整する必要がある場合があります。

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)# **hardware rate-limiter layer-2 l2pt***packets-per-sec*	dot1q-tunnel ポートからの着信プロトコル パケットがハードウェアにドロップされる 1 秒あたりのパケット数のしきい値を設定します。有効値は 0 ～ 30000 です。
ステップ 3	switch(config)# **no hardware rate-limiter layer-2 l2pt**	（任意） しきい値をデフォルトの毎秒 500 パケットにリセットします。

レイヤ 2 プロトコル トンネル ポートのしきい値の設定

レイヤ2プロトコルのトンネリング ポートに対するポート ドロップおよびシャットダウン値を指定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	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 ethernet***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)# **switchport**	インターフェイスをレイヤ 2 スイッチング ポートとして設定します。
ステップ 4	switch(config-if)# **switchport mode dot1q-tunnel**	ポートに 802.1Q トンネルを作成します。
ステップ 5	switch(config-if)# **l2protocol tunnel drop-threshold** [**cdp** | **stp** | **vtp**] *packets-per-sec*	廃棄される前にインターフェイスで処理できる最大パケット数を指定します。必要に応じて、CDP、STP、または VTP を指定できます。パケットの有効な値は 1 ～ 4096 です。
ステップ 6	switch(config-if)# **no l2protocol tunnel drop-threshold** [**cdp** | **stp** | **vtp**]	（任意） しきい値を 0 にリセットし、ドロップしきい値をディセーブルにします。
ステップ 7	switch(config-if)# **l2protocol tunnel shutdown-threshold** [**cdp** | **stp** | **vtp**] *packets-per-sec*	インターフェイスで処理できる最大パケット数を指定します。パケット数が超過すると、ポートは error-disabled ステートになります。必要に応じて、CDP、STP、または VTP を指定できます。パケットの有効な値は 1 ～ 4096 です。
ステップ 8	switch(config-if)# **l2protocol tunnel shutdown-threshold** [**cdp** | **stp** | **vtp**]	（任意） しきい値を 0 にリセットし、シャットダウンしきい値をディセーブルにします。
ステップ 9	switch(config-if)# **exit**	設定モードを終了します。
ステップ 10	switch(config)# **show interface status error policy** [**detail**]	（任意） ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN を表示します。これにより、ポリシーがハードウェア ポリシーと一致することを確認できます。

	コマンドまたはアクション	目的
		エラーを生成するインターフェイスの詳細を表示するには、**detail** コマンドを使用します。
ステップ 11	switch(config)# **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 12	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。

Q-in-Q 設定の確認

コマンド	目的
clear l2protocol tunnel counters [**interface***if-range*]	すべての統計情報カウンタをクリアします。インターフェイスが指定されていない場合、すべてのインターフェイスのレイヤ2プロトコル トンネル統計情報がクリアされます。
show dot1q-tunnel [**interface***if-range*]	dot1q トンネル モードのインターフェイス範囲またはすべてのインターフェイスが表示されます。
show l2protocol tunnel [**interface***if-range* | **vlan***vlan-id*]	一定範囲のインターフェイス（特定の VLAN の一部であるすべての dot1q-tunnel インターフェイスまたはすべてのインターフェイス）のレイヤ 2 プロトコル トンネル情報を表示します。
show l2protocol tunnel summary	レイヤ2プロトコル トンネルが設定されているすべてのポートのサマリーを表示します。
show running-config l2pt	現在のレイヤ2プロトコル トンネルの実行コンフィギュレーションを表示します。

コマンド	目的
show interface status error policy [**detail**]	ハードウェア ポリシーと矛盾するインターフェイスおよび VLAN のエラーを表示します。 **detail** コマンドを使用すると、エラーを受信するインターフェイスおよびVLANの詳細を表示できます。

Q-in-Q およびレイヤ 2 プロトコルのトンネリングの設定例

次に、イーサネット 7/1 に着信するトラフィックに対し Q-in-Q を処理するよう設定されたサービス プロバイダーのスイッチを示します。レイヤ 2 プロトコル トンネルが STP BPDU に対してイネーブルにされます。このカスタマーは VLAN 10（外部 VLAN タグ）に割り当てられます。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vlan 10
switch(config-vlan)# no shutdown
switch(config-vlan)# no ip igmp snooping
switch(config-vlan)# exit
switch(config)# interface ethernet 7/1
switch(config-if)# switchport
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# switchport access vlan 10
switch(config-if)# spanning-tree port type edge
switch(config-if)# l2protocol tunnel stp
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# exit
switch#
```

第 12 章

イーサネット OAM の設定

イーサネット OAM

この章では、イーサネットの運用管理および保守（OAM）の設定について説明します。

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

イーサネット OAM の機能履歴

表 *19*：イーサネット *OAM* の機能履歴

機能名	リリース	機能情報
イーサネット OAM	7.3(0)D1(1)	この機能が導入されました。

イーサネット OAM について

メトロ エリア ネットワーク（MAN）またはワイドエリア ネットワーク（WAN）テクノロジーとしてのイーサネットでは、運用管理および保守（OAM）機能の実装によって大きな恩恵が得られます。イーサネット リンク OAM 機能を使用すると、サービス プロバイダーは MAN や WAN での接続の品質をモニタできます。サービス プロバイダーは、特定のイベントをモニタし、イベントに対しアクションを実行すること、および必要に応じて、トラブルシューティングのために特定のインターフェイスをループバック モードにすることができます。イーサネット リンク OAM は単一の物理リンクで動作し、そのリンクの片側または両側をモニタするように設定できます。

イーサネット リンク OAM は次のように設定できます。

- リンク OAMプロファイルを設定し、このプロファイルを複数のインターフェイスのパラメータの設定に使用できます。
- リンク OAM は、インターフェイス上で直接設定できます。

インターフェイスでリンク OAM プロファイルも使用している場合、プロファイルで設定された特定のパラメータは、インターフェイスで直接別の値を設定することで上書きできます。

EOAMプロファイルにより、複数のインターフェイスでEOAM機能を設定するプロセスが容易になります。イーサネット OAM プロファイルおよびそのすべての機能は、他のインターフェイスから参照でき、他のインターフェイスでそのイーサネット OAM プロファイルの機能を継承できます。

個々のイーサネットリンクOAM機能は、1つのプロファイルに含めることなく、個々のインターフェイスで設定できます。このような場合、個別に設定される機能は、プロファイルの機能よりも常に優先されます。

カスタムEOAMの設定を行う望ましい方法は、イーサネットコンフィギュレーションモードで、EOAM プロファイルを作成し、個別のインターフェイスまたは複数のインターフェイスにアタッチすることです。

次の標準的なイーサネット リンク OAM 機能が、Cisco Nexus 7000 シリーズ スイッチでサポートされます。

- ネイバー探索
- リンク モニタリング
- 誤配線検出（シスコ固有）

ネイバー探索

ネイバー探索では、リンクの両端で、相手側のOAM機能を学習し、OAM ピア関係を確立できるようにします。両端でセッションを確立する前に、ピアに特定の機能が必要となる場合もあります。アクション コンフィギュレーション サブモードで **capabilities-conflict** コマンドまたは **discovery-timeout** コマンドを使用して、機能の競合が存在する場合や検出プロセスがタイムアウトした場合に実行する、特定のアクションを設定できます。

リンク モニタリング

リンク モニタリングでは、OAM ピアで、リンク品質が時間とともに低下する障害をモニタできます。リンク モニタリングをイネーブルにすると、設定したしきい値を超えた場合にアクションを実行するように OAM ピアを設定できます。

誤配線検出（シスコ固有）

誤配線検出はシスコ独自の機能で、可能性のある誤配線のケースを特定するために、すべての情報 OAMPDU の 32 ビットのベンダー フィールドを使用します。

インターフェイスのライセンス要件

vPC には、ライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

IP トンネルには Enterprise Services ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『Cisco NX-OS Licensing Guide』を参照してください。

他のインターフェイスにはライセンスが必要ありません。

イーサネット OAM の前提条件

- 適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。このコマンド リファレンスには、各コマンドに必要なタスク ID が含まれます。ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。
- スイッチ上の F3（10 ギガビット イーサネット）シリーズ モジュールまたは M2（10 ギガビット イーサネット）シリーズ モジュールを使用する必要があります。

注意事項と制約事項

イーサネット OAM の次の機能領域は、Cisco NX-OS 7000 シリーズ スイッチではサポートされません。

- Hello インターバル設定
- リモート ループバック
- イーサネット障害検出（EFD）

イーサネット OAM の設定

イーサネット OAM プロファイルの設定

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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 ethernet-link-oam** 例： `switch(config)# feature ethernet-link-oam`	イーサネット リンク OAM 機能を有効にします。

ステップ 3	**ethernet oam profile** *profile-name*
	
	例：
	`switch(config)# ethernet oam profile Profile_1`
	`switch(config-eoam)#`
		新しいイーサネット運用管理および保守（OAM）プロファイルを作成し、イーサネット OAM 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	**link-monitor**
	
	例：
	`switch(config-eoam)# link-monitor`
	`switch(config-eoam-lm)#`
		イーサネット OAM リンク モニタ コンフィギュレーション モードを開始します。

ステップ 5	**symbol-period window***window* 例： `switch(config-eoam-lm)# symbol-period window 60000`	（任意） イーサネット OAM シンボル期間エラー イベントのウィンドウ サイズをミリ秒単位で設定します。 指定できる範囲は 1000 ～ 60000 です。デフォルト値は 1000 です。
ステップ 6	**symbol-period threshold low***threshold* [**high***threshold*] 例： `switch(config-eoam-lm)# symbol-period threshold low 10000000 high 60000000`	（任意） イーサネット OAM シンボル期間エラー イベントをトリガーするしきい値をシンボル単位で設定します。上限しきい値はオプションです。下限しきい値とともにのみ設定できます。 指定できる範囲は 1 ～ 60000000 です。デフォルトの下限しきい値は 1 です。

	コマンドまたはアクション	目的
ステップ 7	**frame window***window* 例： `switch(config-eoam-lm)# frame window 60`	（任意） OAM フレーム エラー イベントのフレームのウィンドウ サイズをミリ秒単位で設定します。 指定できる範囲は 1000 ～ 60000 です。デフォルト値は 1000 です。
ステップ 8	**frame threshold low***threshold***high***threshold* 例： `switch(config-eoam-lm)# frame threshold low 10000000 high 60000000`	（任意） イーサネット OAM フレーム エラー イベントをトリガーするしきい値をシンボル単位で設定します。上限しきい値はオプションです。下限しきい値とともにのみ設定できます。 指定できる範囲は 1 ～ 12000000 です。デフォルトの下限しきい値は 1 です。
ステップ 9	**frame-period window***window* 例： `switch(config-eoam-lm)# frame-period window 60000`	（任意） イーサネット OAM フレーム期間エラー イベントのウィンドウ サイズをミリ秒単位で設定します。 指定できる範囲は 1000 ～ 60000 です。デフォルト値は 1000 です。
ステップ 10	**frame-period threshold low***threshold* [**high***threshold*] 例： `switch(config-eoam-lm)# frame-period threshold low 100 high 1000000`	（任意） イーサネット OAM フレーム期間エラー イベントをトリガーするしきい値をフレーム単位で設定します。上限しきい値はオプションです。下限しきい値とともにのみ設定できます。 指定できる範囲は 1 ～ 1000000 です。デフォルトの下限しきい値は 60000 です。 IEEE 802.3 標準では、1 つのウィンドウ内のエラー フレーム数としてしきい値超過イベントが規定されています。標準に準拠するために、フレーム期間イベントの下限しきい値と上限しきい値が 100 万フレームあたりのエラー数で測定されます。したがって、リモートの下限しきい値と上限しきい値を決定するための計算式は、(設定されたしきい値 * 受信されたブリッジ プロトコル データ ユニット（BPDU）のフレーム ウィンドウ)/1000000 になります。たとえば、受信されたフレーム ウィンドウが 300 の場合は、上限しきい値が 20000 * 300/1000000 = 6 になります。

	コマンドまたはアクション	目的
ステップ 11	**frame-seconds window***window* 例： `switch(config-eoam-lm)# frame-seconds window 900000`	（任意） OAM フレーム秒数エラーイベントのウィンドウ サイズをミリ秒単位で設定します。 指定できる範囲は 10000 ～ 900000 です。デフォルト値は 60000 です。
ステップ 12	**frame-seconds threshold low***threshold* [**high***threshold*] 例： `switch(config-eoam-lm)# frame-seconds threshold 3 threshold 900`	（任意） フレーム秒数エラーイベントをトリガーするしきい値を秒単位で設定します。上限しきい値は下限しきい値とともにのみ設定できます。 指定できる範囲は 1 ～ 900 です。デフォルト値は 1 です。
ステップ 13	**exit** 例： `switch(config-eoam-lm)# exit switch(config-eoam)#`	イーサネット OAM モードを終了します。
ステップ 14	**connection timeout***seconds* 例： `switch(config-eoam)# connection timeout 30`	イーサネット OAM セッションのタイムアウト値を（秒単位）設定します。 指定できる範囲は 2 ～ 30 です。デフォルト値は 5 です。
ステップ 15	**mode** {**active** | **passive**} 例： `switch(config-eoam)# mode passive`	イーサネット OAM モードを設定します。デフォルトは active です。
ステップ 16	**require-remote** 例： `switch(config-eoam)# require-remote switch(config-eoam-require)#`	イーサネット OAM セッションがアクティブになる前に有効にする必要がある機能を指定するために require-remote コンフィギュレーション サブモードを開始します。
ステップ 17	**mode** {**active** | **passive**} 例： `switch(config-eoam-require)# mode active`	イーサネット OAM セッションがアクティブになる前に、リモート エンドでアクティブ モードまたはパッシブ モードを設定する必要があります。
ステップ 18	**link-monitoring** 例： `switch(config-eoam-require)# link-monitoring`	イーサネット OAM セッションがアクティブになる前に、リモート エンドで link-monitoring を設定する必要があります。

	コマンドまたはアクション	目的

ステップ 19	**exit**
	
	例：
	`switch(config-eoam-require)# exit`
	`switch(config-eoam)#`
		require-remote コンフィギュレーション サブモードを終了します。

ステップ 20	**アクション**
	
	例：
	`switch(config-eoam)# action`
	`switch(config-eoam-action)#`
		イベント アクションを設定するために、アクション コンフィギュレーション サブモードを開始します。

ステップ 21	**capabilities-conflict** {**disable** | **efd** | **error-disable-interface**} 例： `switch(config-eoam-action)# capabilities-conflict disable`	機能の矛盾のイベントが発生したときにインターフェイスで実行するアクションを指定します。デフォルト アクションは、syslog エントリの作成です。 （注） デフォルトを変更する場合、プロファイルの設定を上書きし、インターフェイスのイベントが発生した場合にそれを記録するには、**log** キーワード オプションをインターフェイス イーサネット OAM コンフィギュレーション モードで使用できます。
ステップ 22	**critical-event** {**disable** | **error-disable-interface**} 例： `switch(config-eoam-action)# critical-event error-disable-interface`	重大イベント通知をリモート イーサネット OAM ピアから受信したときにインターフェイスで実行するアクションを指定します。デフォルト アクションは、syslog エントリの作成です。 （注） デフォルトを変更する場合、プロファイルの設定を上書きし、インターフェイスのイベントが発生した場合にそれを記録するには、**log** キーワード オプションをインターフェイス イーサネット OAM コンフィギュレーション モードで使用できます。
ステップ 23	**discovery-timeout** {**disable** | **efd** | **error-disable-interface**} 例： `switch(config-eoam-action)# discovery-timeout disable`	接続タイムアウトが発生したときにインターフェイスで実行するアクションを指定します。デフォルト アクションは、syslog エントリの作成です。 （注） デフォルトを変更する場合、プロファイルの設定を上書きし、インターフェイスのイベントが発生した場合にそれを記録するには、**log** キーワード オプションをインターフェイス イーサネット OAM コンフィギュレーション モードで使用できます。

	コマンドまたはアクション	目的
ステップ 24	**dying-gasp** {**disable** | **error-disable-interface**} 例： `switch(config-eoam-action)# dying-gasp error-disable-interface`	dying-gasp 通知をリモート イーサネット OAM ピアから受信したときにインターフェイスで実行するアクションを指定します。デフォルトアクションは、syslog エントリの作成です。 （注） デフォルトを変更する場合、プロファイルの設定を上書きし、インターフェイスのイベントが発生した場合にそれを記録するには、**log** キーワード オプションをインターフェイス イーサネット OAM コンフィギュレーション モードで使用できます。
ステップ 25	**high-threshold** {**error-disable-interface** | **log**} 例： `switch(config-eoam-action)# high-threshold error-disable-interface`	上限しきい値を超過した場合にインターフェイスで実行するアクションを指定します。デフォルトは上限しきい値を超過した場合、何のアクションも実行しません。 （注） デフォルトを変更する場合、プロファイルの設定を上書きし、イベントが発生した場合にインターフェイスでアクションしないようにするには、**disable** キーワード オプションをインターネットイーサネットOAM コンフィギュレーション モードで使用できます。
ステップ 26	**remote-loopback disable** 例： `switch(config-eoam-action)# remote-loopback disable`	リモートループバックのイベント発生時に処理がインターフェイスで実行されないことを指定します。デフォルトアクションは、syslogエントリの作成です。 （注） デフォルトを変更する場合、プロファイルの設定を上書きし、インターフェイスのイベントが発生した場合にそれを記録するには、**log** キーワード オプションをインターフェイス イーサネット OAM コンフィギュレーション モードで使用できます。
ステップ 27	**session-down** {**disable** | **efd** | **error-disable-interface**} 例： `switch(config-eoam-action)# session-down error-disable-interface`	イーサネット OAM セッションがダウンした場合にインターフェイスで実行するアクションを指定します。 （注） デフォルトを変更する場合、プロファイルの設定を上書きし、インターフェイスのイベントが発生した場合にそれを記録するには、**log** キーワード オプションをインターフェイス イーサネット OAM コンフィギュレーション モードで使用できます。

	コマンドまたはアクション	目的
ステップ 28	**session-up disable** 例： `switch(config-eoam-action)# session-up disable`	イーサネット OAM セッションが設定された場合にアクションがインターフェイスで実行されないことを指定します。デフォルトアクションは、syslog エントリの作成です。 （注） デフォルトを変更する場合、プロファイルの設定を上書きし、インターフェイスのイベントが発生した場合にそれを記録するには、**log** キーワード オプションをインターフェイス イーサネット OAM コンフィギュレーション モードで使用できます。
ステップ 29	**uni-directional link-fault** {**disable** | **efd** | **error-disable-interface**} 例： `switch(config-eoam-action)# uni-directional link-fault disable`	リンク障害通知をリモート イーサネット OAM ピアから受信したときにインターフェイスで実行するアクションを指定します。デフォルトアクションは、syslog エントリの作成です。 （注） デフォルトを変更する場合、プロファイルの設定を上書きし、インターフェイスのイベントが発生した場合にそれを記録するには、**log** キーワード オプションをインターフェイス イーサネット OAM コンフィギュレーション モードで使用できます。
ステップ 30	**wiring-conflict** {**disable** | **efd** | **log**} 例： `switch(config-eoam-action)# wiring-conflict disable`	配線競合イベントが発生したときにインターフェイスで実行するアクションを指定します。デフォルトはインターフェイスを errdisable ステートにします。 （注） デフォルトを変更する場合、プロファイルの設定を上書きし、イベントが発生した場合にインターフェイスを errdisable ステートにするには、**error-disable-interface** キーワード オプションをインターフェイス イーサネット OAM コンフィギュレーション モードで使用できます。
ステップ 31	**end** 例： `switch(config-eoam-action)# end`	コンフィギュレーション セッションを終了し、EXEC モードに戻ります。

インターフェイスへのイーサネット OAM プロファイルのアタッチ

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***interface*
	
	例：
	`switch(config)# interface GigabitEthernet 0/0/6/11`
	`switch(config-if)#`
		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、イーサネット インターフェイス名と rack/slot/module/port 表記を指定します。

ステップ 3	**ethernet oam**
	
	例：
	`switch(config-if)# ethernet oam`
	`switch(config-if-eoam)#`
		イーサネット OAM をイネーブルにし、インターフェイスイーサネットOAM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	**profile***profile-name* 例： `switch(config-if-eoam)# profile Profile_1`	指定されたイーサネットOAMプロファイルとその設定のすべてをインターフェイスにアタッチします。
ステップ 5	**end** 例： `switch(config-if-eoam)# end`	コンフィギュレーションセッションを終了し、EXEC モードに戻ります。

イーサネット OAM のインターフェイスでの設定およびプロファイル設定の上書き

EOAMプロファイルの使用は、共通のEOAMの設定でいくつかのインターフェイスを設定する効率的な方法です。ただし、プロファイルを使用して特定のインターフェイスの特定の機能の動作を変更する場合、プロファイル設定を上書きできます。インターフェイスに適用される特定のプロファイル設定を上書きするには、そのインターフェイスの動作を変更するようにインターフェイス イーサネット OAM コンフィギュレーション モードでこのコマンドを設定できます。

場合によっては、コマンドのデフォルト設定により、特定のキーワード オプションだけをインターフェイス イーサネット OAM コンフィギュレーション モードで使用できます。たとえば、**action** コンフィギュレーション サブモード コマンドを設定しなければ、このコマンドの複数の形式のデフォルト動作では、プロファイルが作成されインターフェイスに適用されるときに syslog エントリを作成します。したがって、**log** キーワードは、デフォルトの動作であるため、プロファ

イルのこれらのコマンドについてはイーサネット OAM 設定で使用できなくなります。ただし、プロファイルの設定でデフォルトが変更された場合、インターフェイス イーサネット OAM 設定で **log** キーワードを使用でき、特定のインターフェイスの syslog エントリの作成のアクションを保持できるようになります。

イーサネット OAM 設定をインターフェイスで設定し、プロファイルの設定を上書きするには、次の手順を実行します。

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***interface*
	
	例：
	`switch(config)# interface GigabitEthernet 0/0/6/11`
	`switch(config-if)#`
		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、イーサネットインターフェイス名と rack/slot/module/port 表記を指定します。

ステップ 3	**ethernet oam**
	
	例：
	`switch(config-if)# ethernet oam`
	`switch(config-if-eoam)#`
		イーサネット OAM をイネーブルにし、インターフェイス イーサネット OAM 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	*interface-Ethernet-OAM-command* 例： `switch(config-if-eoam)# mode passive`	イーサネット OAM コンフィギュレーション コマンドを設定し、プロファイル設定の設定を上書きします。ここで、*interface-Ethernet-OAM-command* は、インターフェイス イーサネット OAM コンフィギュレーション モードのプラットフォームでサポートされるいずれかのコマンドです。
ステップ 5	**end** 例： `switch(config-if-eoam)# end`	コンフィギュレーション セッションを終了し、EXEC モードに戻ります。

インターフェイス上でのイーサネット OAM 統計情報のクリア

すべてのイーサネット OAM インターフェイス上のパケット カウンタをクリアする場合は、**clear ethernet oam statistics** コマンドを使用します。特定のイーサネット OAM インターフェイス上のパケット カウンタをクリアする場合は、**clear ethernet oam statistics***interface* コマンドを使用します。

```
switch# clear ethernet oam statistics interface gigabitethernet 0/1/5/1
```

イーサネット OAM の設定の確認

show ethernet oam configuration コマンドを使用して、特定のインターフェイスまたはすべてのインターフェイスのイーサネット OAM 設定の値を表示します。

（注） これらの設定の一部は特定のプラットフォームでサポートされませんが、デフォルトは報告されます。Cisco Nexus 7000 シリーズ スイッチでは、次の領域がサポートされません。

- Hello インターバル設定
- リモート ループバック
- EFD

```
switch# show ethernet oam configuration interface gigabitethernet 0/0/0/0
GigabitEthernet0/0/0/0:
  Hello interval:                                          1s
  Link monitoring enabled:                                  Y
  Remote loopback enabled:                                  N
  Mib retrieval enabled:                                    N
  Uni-directional link-fault detection enabled:             N
  Configured mode:                                     Active
  Connection timeout:                                       5
  Symbol period window:                                  1000
  Symbol period low threshold:                              1
  Symbol period high threshold:                          None
  Frame window:                                          1000
  Frame low threshold:                                      1
  Frame high threshold:                                  None
  Frame period window:                                   1000
  Frame period low threshold:                               1
  Frame period high threshold:                           None
  Frame seconds window:                                 60000
  Frame seconds low threshold:                              1
  Frame seconds high threshold:                          None
  High threshold action:                                 None
  Link fault action:                                      Log
  Dying gasp action:                                      Log
  Critical event action:                                  Log
  Discovery timeout action:                               Log
  Capabilities conflict action:                           Log
  Wiring conflict action:                        Error-Disable
  Session up action:                                      Log
  Session down action:                                    Log
  Remote loopback action:                                 Log
  Require remote mode:                                 Ignore
  Require remote MIB retrieval:                             N
  Require remote loopback support:                          N
  Require remote link monitoring:                           N
```

show ethernet oam discovery コマンドは、OAM セッションのステータスを表示するために使用します。インターフェイスを指定しなかった場合は、OAMが設定されたすべてのインターフェイスの詳細が表示されます。

```
switch# show ethernet oam discovery GigabitEthernet0/0/6/11
GigabitEthernet0/0/6/11
Local client
  Administrative configuration:
    PDU revision:                         2
    Mode:                            Active
```

```
    Unidirectional support:                N
    Link monitor support:                  N
    Remote loopback support:               Y
    MIB retrieval support:                 Y
    Maximum PDU size:                   1500
    Mis-wiring detection key:         20492C

  Operational status:
    Port status:                 Operational
    Loopback status:                    None
    Interface mis-wired:                   N

Remote client
  MAC address:  0030.96fd.6bfa
  Vendor (OUI): 00.00.0C (Cisco)

  Administrative configuration:
    PDU revision:                          5
    Mode:                            Passive
    Unidirectional support:                N
    Link monitor support:                  Y
    Remote loopback support:               Y
    MIB retrieval support:                 N
    Maximum PDU size:                   1500
```

show ethernet oam statistics コマンドは、ローカルとリモートの OAM セッションの統計情報を表示するために使用します。インターフェイスを指定しなかった場合は、OAMが設定されたすべてのインターフェイスの統計情報が表示されます。

```
switch# show ethernet oam statistics
GigabitEthernet0/0/6/11
Counters
--------
  Information OAMPDU Tx            45
  Information OAMPDU Rx            42
  Unique Event Notification OAMPDU Tx         0
  Unique Event Notification OAMPDU Rx              0
  Duplicate Event Notification OAMPDU Tx           0
  Duplicate Event Notification OAMPDU Rx           0
  Loopback Control OAMPDU Tx                       0
  Loopback Control OAMPDU Rx                       3
  Variable Request OAMPDU Tx                       0
  Variable Request OAMPDU Rx                       0
  Variable Response OAMPDU Tx                      0
  Variable Response OAMPDU Rx                      0
  Organization Specific OAMPDU Tx                  0
  Organization Specific OAMPDU Rx                  0
  Unsupported OAMPDU Tx            93
  Unsupported OAMPDU Rx             0
  Frames Lost due to OAM                          12

Local event logs
----------------
  Errored Symbol Period records                    0
  Errored Frame records             0
  Errored Frame Period records           0
  Errored Frame Second records           0

Remote event logs
-----------------
  Errored Symbol Period records            0
  Errored Frame records             0
  Errored Frame Period records           0
  Errored Frame Second records                     0
```

show ethernet oam event-log コマンドは、OAM が設定されたインターフェイスの最新のイベント ログを表示するために使用します。

```
switch# show ethernet oam event-log
Wed Jan 23 06:16:46.684 PST
Local Action Taken:
    N/A    - No action needed         EFD    - Interface brought down using EFD
    None   - No action taken          Err.D  - Interface error-disabled
    Logged - System logged

GigabitEthernet0/1/0/0
================================================================================
Time                       Type           Loc'n  Action Threshold Breaching Value
-------------------------- -------------- ------ ------ --------- ---------------
Wed Jan 23 06:13:25 PST   Symbol period  Local  N/A            1               4
Wed Jan 23 06:13:33 PST   Frame          Local  N/A            1               6
Wed Jan 23 06:13:37 PST   Frame period   Local  None           9              12
Wed Jan 23 06:13:45 PST   Frame seconds  Local  N/A            1              10
Wed Jan 23 06:13:57 PST   Dying gasp     Remote Logged       N/A             N/A

GigabitEthernet0/1/0/1
================================================================================
Time                       Type           Loc'n  Action Threshold Breaching Value
-------------------------- -------------- ------ ------ --------- ---------------
Wed Jan 23 06:26:14 PST   Dying gasp     Remote Logged       N/A             N/A
Wed Jan 23 06:33:25 PST   Symbol period  Local  N/A            1               4
Wed Jan 23 06:43:33 PST   Frame period   Remote N/A            9              12
Wed Jan 23 06:53:37 PST   Critical event Remote Logged       N/A             N/A
Wed Jan 23 07:13:45 PST   Link fault     Remote EFD          N/A             N/A
Wed Jan 23 07:18:23 PST   Dying gasp     Local  Logged       N/A             N/A
```

show ethernet oam event-log interface detail コマンドは、OAM が設定された特定のインターフェイスの詳細なイベント ログを表示するために使用します。

```
switch# show ethernet oam event-log interface detail
Wed Jan 23 06:21:16.392 PST
(Scaled): For remote threshold events "Local High Threshold" is scaled for
          comparison with "Breaching Value".
          This is to account for different local and remote window sizes.

GigabitEthernet0/1/0/0
====================================================================
Event at Wed Jan 23 2013 06:26:14.62 PST:
    Type:                                                 Dying gasp
    Location:                                                 Remote
    Local Action Taken:                                 System logged
    Local Event Running Total:                                    1
Event at Wed Jan 23 2013 06:33:25.62 PST:
    Type:                            Threshold Event - Symbol period
    Location:                                                  Local
    Local Action Taken:                                No action needed
    Local Event Running Total:                                    1
    Local Window Size:                                         1000
    Local Threshold:                                              1
    Local High Threshold:                            Not configured
    Breaching Value:                                              4
    Local Error Running Total:                                    8
Event at Wed Jan 23 2013 06:43:37.73 PST:
    Type:                             Threshold Event - Frame period
    Location:                                                 Remote
    Local Action Taken:                                No action needed
    Remote Event Running Total:                                   1
    Remote Window Size:                                        1000
    Remote Threshold:                                             9
    Local High Threshold (Scaled):                   Not configured
    Breaching Value:                                             12
    Remote Error Running Total:                                  24
Event at Wed Jan 23 2013 06:53:57.12 PST:
    Type:                                               Critical event
    Location:                                                 Remote
```

```
    Local Action Taken:                                 System logged
    Local Event Running Total:                                     1
Event at Wed Jan 23 2013 07:13:57.12 PST:
    Type:                                                  Link fault
    Location:                                                  Remote
    Local Action Taken:            Interface brought down using EFD
    Local Event Running Total:                                     1
Event at Wed Jan 23 2013 07:18:57.12 PST:
    Type:                                                  Dying gasp
    Location:                                                   Local
    Local Action Taken:                                 System logged
    Local Event Running Total:                                     1
```

show ethernet oam summary コマンドは、すべてのアクティブな OAM セッションの概要を表示するために使用します。

```
switch# show ethernet oam summary
Link OAM System Summary
=======================

Profiles                                 6
Interfaces                              10
  Interface states:
    Port down                            1
    Passive wait                         1
    Active send                          1
    [Evaluating                          0]
    [Local accept                        0]
    [Local reject                        0]
    Remote reject                        1
    Operational                          6
      Loopback mode                      1
  Miswired connections                   1
Events                                  13
  Local                                  4
    Symbol error                         0
    Frame                                2
    Frame period                         1
    Frame seconds                        1
  Remote                                 9
    Symbol error                         3
    Frame                                4
    Frame period                         1
    Frame seconds                        1
```

show ethernet oam summary detail コマンドは、すべてのアクティブな OAM セッションの概要と、すべてのインターフェイスにおける最新の 10 件のイベントに関する詳細を表示するために使用します。

```
switch# show ethernet oam summary detail
Link OAM System Summary
=======================

Profiles                                 6
Interfaces                              10
  Interface states:
    Port down                            1
    Passive wait                         1
    Active send                          1
    [Evaluating                          0]
    [Local accept                        0]
    [Local reject                        0]
    Remote reject                        1
    Operational                          6
      Loopback mode                      1
  Miswired connections                   1
Events                                  13
  Local                                  4
    Symbol error                         0
    Frame                                2
    Frame period                         1
```

```
    Frame seconds                       1
  Remote                                9
    Symbol error                        3
    Frame                               4
    Frame period                        1
    Frame seconds                       1

Recent Event Logs
=================
Interface           Time                Type           Loc'n  Action
------------------- ------------------- -------------- ------ ------
Gi0/0/0/0           Jan 23 06:13:25 PST Symbol period  Local  N/A
Gi0/0/0/0           Jan 23 06:13:33 PST Frame          Local  N/A
Gi0/0/0/2           Jan 23 06:13:37 PST Frame period   Local  N/A
Gi0/0/0/1           Jan 23 06:13:45 PST Frame seconds  Local  EFD
Gi0/0/0/0           Jan 23 06:13:48 PST Dying gasp     Remote Err.D
```

イーサネット OAM の設定例

イーサネット OAM プロファイルをグローバルに設定するための設定例

```
switch# configure terminal
switch(config)# feature ethernet-link-oam
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# link-monitor
switch(config-eoam-lm)# symbol-period window 60000
switch(config-eoam-lm)# symbol-period threshold low 10000000 high 60000000
switch(config-eoam-lm)# frame window 60
switch(config-eoam-lm)# frame threshold low 10000000 high 60000000
switch(config-eoam-lm)# frame-period window 60000
switch(config-eoam-lm)# frame-period threshold low 100 high 1000000
switch(config-eoam-lm)# frame-seconds window 900000
switch(config-eoam-lm)# frame-seconds threshold 3 threshold 900
switch(config-eoam-lm)# exit
switch(config-eoam)# connection timeout 30
switch(config-eoam)# mode passive
switch(config-eoam)# require-remote
switch(config-eoam-require)# mode active
switch(config-eoam-require)# link-monitoring
switch(config-eoam-require)# exit
switch(config-eoam)# action
switch(config-eoam-action)# capabilities-conflict disable
switch(config-eoam-action)# critical-event error-disable-interface
switch(config-eoam-action)# discovery-timeout disable
switch(config-eoam-action)# dying-gasp error-disable-interface
switch(config-eoam-action)# high-threshold error-disable-interface
switch(config-eoam-action)# remote-loopback disable
switch(config-eoam-action)# session-down error-disable-interface
switch(config-eoam-action)# session-up disable
switch(config-eoam-action)# uni-directional link-fault disable
switch(config-eoam-action)# wiring-conflict disable
```

イーサネットOAMプロファイルを特定のインターフェイスに接続するための設定例

```
switch# configure terminal
switch(config)# interface GigabitEthernet 0/0/6/11
switch(config-if)# ethernet oam
switch(config-if-eoam)# profile Profile_1
```

特定のインターフェイス上でイーサネット OAM 機能を設定するための設定例

```
switch# configure terminal
switch(config)# interface GigabitEthernet 0/0/6/11
switch(config-if)# ethernet oam
switch(config-if-eoam)# link-monitor
switch(config—if-eoam-lm)# symbol-period window 60000
switch(config-if-eoam-lm)# symbol-period threshold low 10000000 high 60000000
switch(config-if-eoam-lm)# frame window 60
switch(config-if-eoam-lm)# frame threshold low 10000000 high 60000000
switch(config-if-eoam-lm)# frame-period window 60000
switch(config-if-eoam-lm)# frame-period threshold low 100 high 1000000
switch(config-if-eoam-lm)# frame-seconds window 900000
switch(config-if-eoam-lm)# frame-seconds threshold 3 threshold 900
switch(config-if-eoam-lm)# exit
switch(config-if-eoam)# connection timeout 30
switch(config-if-eoam)# mode passive
switch(config-if-eoam)# require-remote
switch(config-if-eoam-require)# mode active
switch(config-if-eoam-require)# link-monitoring
switch(config-if-eoam-require)# exit
switch(config-if-eoam)# action
switch(config-if-eoam-action)# capabilities-conflict disable
switch(config-if-eoam-action)# critical-event error-disable-interface
switch(config-if-eoam-action)# discovery-timeout disable
switch(config-if-eoam-action)# dying-gasp error-disable-interface
switch(config-if-eoam-action)# high-threshold error-disable-interface
switch(config-if-eoam-action)# remote-loopback disable
switch(config-if-eoam-action)# session-down error-disable-interface
switch(config-if-eoam-action)# session-up disable
switch(config-if-eoam-action)# uni-directional link-fault disable
switch(config-if-eoam-action)# wiring-conflict disable
```

プロファイルでイーサネットOAM機能を設定してから、インターフェイス上でその設定をオーバーライドする設定例

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# mode passive
switch(config-eoam)# action
switch(config-eoam-action)# capabilities-conflict disable
switch(config-eoam-action)# critical-event error-disable-interface
switch(config-eoam-action)# discovery-timeout disable
switch(config-eoam-action)# dying-gasp error-disable-interface
switch(config-eoam-action)# remote-loopback disable
switch(config-eoam-action)# session-down error-disable-interface
switch(config-eoam-action)# session-up disable
switch(config-eoam-action)# uni-directional link-fault disable
switch(config-eoam-action)# wiring-conflict disable
switch# configure terminal
switch(config)# interface GigabitEthernet 0/0/6/11
switch(config-if)# ethernet oam
switch(config-if-eoam)# profile Profile_1
switch(config-if-eoam)# mode active
switch(config-if-eoam)# action
switch(config-if-eoam-action)# capabilities-conflict disable
switch(config-if-eoam-action)# critical-event error-disable-interface
switch(config-if-eoam-action)# discovery-timeout disable
switch(config-if-eoam-action)# dying-gasp error-disable-interface
switch(config-if-eoam-action)# remote-loopback disable
switch(config-if-eoam-action)# session-down error-disable-interface
switch(config-if-eoam-action)# session-up disable
switch(config-if-eoam-action)# uni-directional link-fault disable
switch(config-if-eoam-action)# wiring-conflict disable
```

関連資料

関連項目	マニュアル タイトル
『Cisco NX-OS Licensing Guide』	『Cisco NX-OS Licensing Guide』
『Cisco Nexus 7000 Series NX-OS Release Notes』	『Cisco NX-OS 7000 Series Release Notes』

付 録 A

Cisco NX-OS インターフェイスがサポートする IETF RFC

Cisco NX-OS インターフェイスがサポートする IETF RFC

RFC	タイトル
RFC 1981	『Path MTU Discovery for IP version 6』
RFC 2373	『IP Version 6 Addressing Architecture』
RFC 2374	『An Aggregatable Global Unicast Address Format』
RFC 2460	『Internet Protocol, Version 6 (IPv6) Specification』
RFC 2461	『Neighbor Discovery for IP Version 6 (IPv6)』
RFC 2462	『IPv6 Stateless Address Autoconfiguration』
RFC 2463	『Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification』
RFC 2464	『Transmission of IPv6 Packets over Ethernet Networks』
RFC 2467	『Transmission of IPv6 Packets over FDDI Networks』
RFC 2472	『IP Version 6 over PPP』
RFC 2492	『IPv6 over ATM Networks』

Cisco NX-OS インターフェイスがサポートする IETF RFC

RFC	タイトル
RFC 2590	『Transmission of IPv6 Packets over Frame Relay Networks Specification』
RFC 3021	『Using 31-Bit Prefixes on IPv4 Point-to-Point Links』
RFC 3152	『Delegation of IP6.ARPA』
RFC 3162	『RADIUS and IPv6』
RFC 3513	『Internet Protocol Version 6 (IPv6) Addressing Architecture』
RFC 3596	『DNS Extensions to Support IP version 6』
RFC 4193	『Unique Local IPv6 Unicast Addresses』

付 録 B

Cisco NX-OS インターフェイスの設定制限

インターフェイスの設定制限値