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 5.x

Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x

2010 年 6 月 7 日

Text Part Number: OL-19797-01-J

【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、米国シスコシステムズ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。

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 5.x

CONTENTS

新機能と変更された機能

この章では、『*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 5.x*』に記載されている新機能および変更された機能について、リリース固有の情報を示します。このマニュアルの最新バージョンは、次のシスコ Web サイトから入手できます。
http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/interfaces/configuration/guide/if_cli.html

Cisco NX--OS Release 5.x の追加情報を確認するには、『*Cisco Nexus 7000 Series NX-OS Release Notes, Release 5.x*』を参照してください。リリース ノートは、次のシスコ Web サイトから入手できます。
http://www.cisco.com/en/US/partner/products/ps9402/prod_release_notes_list.html

表 1 では、『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 5.x』における新機能および変更された機能を要約し、その参照先を示しています。

表 1　Cisco NX--OS Release 5.x の新機能および変更された機能

機能	説明	変更されたリリース	参照先
BFD	ネットワーク プロファイリングおよびプランニングが容易になり、再収束時間の整合性が保たれ、予測可能になります。	5.0(2)	第 5 章「双方向フォワーディング検出（BFD）の設定」
Q-in-Q トンネリング	異なるカスタマーのトラフィックを分離しておいたまま、カスタマーに Virtual LAN（VLAN; 仮想 LAN）を完全に利用させることができます。	5.0(2)	第 9 章「Q-in-Q VLAN トンネルの設定」
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)	第 7 章「vPC の設定」

はじめに

ここでは、『*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 5.x*』の対象読者、構成、および表記法について説明します。また、関連マニュアルの入手方法についても説明します。

対象読者

このマニュアルは、Cisco NX-OS デバイスの設定および維持に携わる、十分な経験を持つネットワーク管理者を対象としています。

マニュアルの構成

このマニュアルの構成は、次のとおりです。

章	説明
第 1 章「概要」	Cisco NX-OS インターフェイスの概要です。
第 2 章「基本インターフェイス パラメータの設定」	レイヤ 2 およびレイヤ 3 インターフェイスで共有する基本パラメータを設定する手順について説明します。
第 3 章「レイヤ 2 インターフェイスの設定」	レイヤ 2 スイッチング ポートをアクセス ポートまたはトランク ポートとして設定する手順について説明します。
第 4 章「レイヤ 3 インターフェイスの設定」	レイヤ 3 インターフェイスを設定する手順について説明します。
第 6 章「ポート チャネルの設定」	ポート チャネルを設定し、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。
第 7 章「vPC の設定」	Virtual Port Channels（vPC; 仮想ポート チャネル）の設定方法について説明します。
第 8 章「IP トンネルの設定」	装置で Generic Route Encapsulation（GRE）を使って IP トンネルを設定する手順について説明します。

章	説明
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 Release 4.x でサポートするインターフェイスに関する Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）Request for Comments（RFC）を示します。
付録 B「Cisco NX-OS インターフェイスの設定制限」	NX-OS Release 4.x を実行するデバイスについてシスコが認定した制限および最大制限を示します。

表記法

コマンドの説明では、次の表記法を使用しています。

表記法	説明
太字	コマンドおよびキーワードは太字で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で示しています。
[ ]	角カッコの中の要素は、省略可能です。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
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。

出力例では、次の表記法を使用しています。

`screen フォント`	スイッチに表示され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*」を意味します。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

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。

関連資料

Cisco NX-OS には、次の資料が含まれます。

リリース ノート

『*Cisco Nexus 7000 Series NX-OS Release Notes, Release 5.x*』

NX-OS コンフィギュレーション ガイド

『*Cisco Nexus 7000 Series NX-OS Getting Started with Virtual Device Contexts, Release 5.x*』
『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 5.x*』
『*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 5.x*』
『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*』
『*Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide, Release 5.x*』
『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』
『*Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 5.x*』
『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 5.x*』
『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x*』
『*Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 5.x*』
『*Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x*』
『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x*』
『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』
『*Cisco NX-OS XML Management Interface User Guide, Release 5.x*』
『*Cisco NX-OS System Messages Reference*』
『*Cisco Nexus 7000 Series NX-OS MIB Quick Reference*』

NX-OS コマンド リファレンス

『*Cisco Nexus 7000 Series NX-OS Command Reference Master Index, Release 5.x*』
『*Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference, Release 5.x*』
『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x*』
『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x*』
『*Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference, Release 5.x*』
『*Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x*』
『*Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference, Release 5.x*』
『*Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 5.x*』
『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference, Release 5.x*』
『*Cisco Nexus 7000 Series NX-OS System Management Command Reference, Release 5.x*』

その他のソフトウェアのマニュアル

『*Cisco Nexus 7000 Series NX-OS Troubleshooting Guide, Release 5.x*』

関連資料

ここでは、Cisco DCNM および Cisco DCNM が管理するプラットフォームに関する資料について説明します。

ここでは、次の内容について説明します。

Cisco DCNM マニュアル

Cisco DCNM のドキュメンテーションは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

Cisco DCNM のマニュアル セットには、次の資料が含まれます。

リリース ノート

『*Cisco DCNM Release Notes, Release 5.x*』

コンフィギュレーション ガイド

『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』

『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』

『*Cisco DCNM System Management Configuration Guide, Release 5.x*』

『*Cisco DCNM Interfaces Configuration Guide, Release 5.x*』

『*Cisco DCNM Layer 2 Switching Configuration Guide, Release 5.x*』

『*Cisco DCNM Security Configuration Guide, Release 5.x*』

『*Cisco DCNM Unicast Routing Configuration Guide, Release 5.x*』

『*Cisco DCNM Getting Started with Virtual Device Contexts, Release 5.x*』

『*Cisco DCNM Virtual Device Context Configuration Guide, Release 5.x*』

『*Cisco DCNM Web Services API Guide, Release 5.x*』

Cisco Nexus 1000V シリーズ スイッチ マニュアル

Cisco Nexus 1000V シリーズ スイッチのドキュメンテーションは、次の URL で入手できます。
http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

Cisco Nexus 1000V シリーズ スイッチのマニュアル セットには、次の資料が含まれます。

リリース ノート

『*Cisco Nexus 1000V Release Notes, Release 4.0(4)SV1(2)*』

コンフィギュレーション ガイド

『*Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(2)*』
『*Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.0(4)SV1(2)*』
『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(2)*』
『*Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(2)*』
『*Cisco Nexus 1000V License Configuration Guide, Release 4.0(4)SV1(2)*』
『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)*』
『*Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(2)*』
『*Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(2)*』

Cisco Nexus 2000 シリーズ Fabric Extender マニュアル

Cisco Nexus 2000 シリーズ Fabric Extender のドキュメンテーションは、次の URL で入手できます。
http://www.cisco.com/en/US/products/ps10110/tsd_products_support_series_home.html

Cisco Nexus 2000 シリーズ Fabric Extender のマニュアル セットには、次の資料が含まれます。

リリース ノート

『*Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes*』

コンフィギュレーション ガイド

『*Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide*』

Cisco Nexus 4000 シリーズ スイッチ マニュアル

Cisco Nexus 4000 シリーズ スイッチのドキュメンテーションは、次の URL で入手できます。
http://www.cisco.com/en/US/products/ps10596/tsd_products_support_series_home.html

Cisco Nexus 4000 シリーズ スイッチのマニュアル セットには、次の資料が含まれます。

リリース ノート

『*Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter NX-OS Release Notes, Release 4.1(2)E1(1b)*』

コンフィギュレーション ガイド

『*Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter NX-OS Configuration Guide*』

Cisco Nexus 5000 シリーズ スイッチ マニュアル

Cisco Nexus 5000 シリーズ スイッチのドキュメンテーションは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

Cisco Nexus 5000 シリーズ スイッチのマニュアル セットには、次の資料が含まれます。

リリース ノート

『*Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes, Releases 4.1(3)N1(1), 4.1(3)N1(1a), 4.1(3)N2(1), and 4.1(3)N2(1a)*』

コンフィギュレーション ガイド

『*Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide*』

『*Cisco Nexus 5000 Series NX-OS Security Configuration Guide*』

『*Cisco Nexus 5000 Series NX-OS System Management Configuration Guide*』

Cisco Nexus 7000 シリーズ スイッチ マニュアル

Cisco Nexus 7000 シリーズ スイッチのドキュメンテーションは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

Cisco Nexus 7000 シリーズ スイッチのマニュアル セットには、次の資料が含まれます。

リリース ノート

『*Cisco Nexus 7000 Series NX-OS Release Notes, Release 5.x*』

コンフィギュレーション ガイド

『*Quick Start Guide: Cisco Nexus 7000 Series NX-OS Virtual Device Context Quick Start, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 1

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。

この章では、次の内容について説明します。

インターフェイスについて

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

表 1-1 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 1-1　インターフェイスのパラメータ

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	このマニュアルの第 2 章「基本インターフェイス パラメータの設定」
レイヤ 2	レイヤ 2 アクセスおよびトランク ポート設定	このマニュアルの第 3 章「レイヤ 2 インターフェイスの設定」
	レイヤ 2 MAC、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, Release 5.x*』
	ポート セキュリティ	『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 5.x*』
レイヤ 3	メディア、IPv4 および IPv6 アドレス	このマニュアルの「レイヤ 3 インターフェイスの設定」（P.4-1）
	帯域幅、遅延、IP ルーティング、VRF	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』 『*Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 5.x*』

表 1-1　インターフェイスのパラメータ （続き）

機能	パラメータ	解説場所
ポート チャネル	チャネル グループ、LACP	このマニュアルの第 6 章「ポート チャネルの設定」
vPC	仮想ポート チャネル	このマニュアルの第 7 章「vPC の設定」
トンネル	GRE トンネリング	このマニュアルの第 8 章「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 5.x*』

ここでは、次の内容について説明します。

- 「イーサネット インターフェイス」（P.1-2）
- 「管理インターフェイス」（P.1-3）
- 「ポート チャネル インターフェイス」（P.1-3）
- 「vPC」（P.1-4）
- 「サブインターフェイス」（P.1-4）
- 「VLAN ネットワーク インターフェイス」（P.1-4）
- 「ループバック インターフェイス」（P.1-4）
- 「トンネル インターフェイス」（P.1-4）

イーサネット インターフェイス

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

ここでは、次の内容について説明します。

- 「アクセス ポート」（P.1-2）
- 「トランク ポート」（P.1-2）
- 「PVLAN ホストと混合モード ポート」（P.1-3）
- 「ルーテッド ポート」（P.1-3）

アクセス ポート

アクセス ポートは 1 つの VLAN のトラフィックを送受信します。このポートのタイプはレイヤ 2 インターフェイスだけです。アクセスポート インターフェイスの詳細については、第 3 章「レイヤ 2 インターフェイスの設定」を参照してください。

トランク ポート

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、第 3 章「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 ホストと混合モード 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 は混合モード 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 混合モード ポートにレイヤ 3 VLAN ネットワーク インターフェイスや Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）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 混合モード ポートの設定や他の PVLAN の設定の詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*』を参照してください。

ルーテッド ポート

ルーテッド ポートは、IP トラフィックを他のデバイスにルーティングできる物理ポートです。ルーテッド ポートはレイヤ 3 インターフェイスだけで、Spanning Tree Protocol（STP; スパニング ツリー プロトコル）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」（P.4-2）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、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）、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, Release 5.x*』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、第 6 章「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、サーバ、またはその他の任意のネットワーキング デバイスが可能です。それぞれのデバイスで合計 768 個の vPC を設定できます。vPC は、レイヤ 2 マルチパスを行います。vPC の詳細については、第 7 章「vPC の設定」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」（P.4-2）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」（P.4-3）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」（P.4-4）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 Point-To-Point（p2p; ポイントツーポイント）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、第 8 章「IP トンネルの設定」を参照してください。

バーチャライゼーション インターフェイス

複数の Virtual Device Context（VDC; 仮想デバイス コンテキスト）が作成できます。各 VDC は独立した論理デバイスで、インターフェイスを割り当てることができます。VDC にインターフェイスを割り当てると、正しい VDC であればそのインターフェイスだけが設定できます。VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x*』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

IP トンネルおよび vPC には Enterprise Services ライセンスが必要です。このライセンスは IP トンネルをイネーブルにするシステムごとにインストールする必要があります。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。

CHAPTER 2

基本インターフェイス パラメータの設定

この章では、Cisco Nexus 7000 シリーズ NX-OS デバイスで基本インターフェイス パラメータを設定する方法について説明します。

この章では、次の内容について説明します。

（注） レイヤ 2 インターフェイスで独自に使用するパラメータを設定するには、第 3 章「レイヤ 2 インターフェイスの設定」を参照してください（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）。レイヤ 3 インターフェイスで独自に使用するパラメータを設定するには、第 4 章「レイヤ 3 インターフェイスの設定」を参照してください（ルーテッド インターフェイス、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、IP トンネル）。

基本インターフェイス パラメータについて

ここでは、次の内容について説明します。

- 「フロー制御」（P.2-5）
- 「ポート MTU サイズ」（P.2-5）
- 「帯域幅」（P.2-6）
- 「スループット遅延」（P.2-6）
- 「管理ステータス」（P.2-6）
- 「UDLD パラメータ」（P.2-7）
- 「キャリア遅延」（P.2-9）
- 「ポート チャネル パラメータ」（P.2-9）
- 「ポート プロファイル」（P.2-10）
- 「タイム ドメイン反射率計（TDR）ケーブル診断」（P.2-12）

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 インターフェイスに説明パラメータを設定する方法については、「ポート チャネルの説明の設定」（P.6-22）を参照してください。別のインターフェイスにこのパラメータを設定する方法については、「説明の設定」（P.2-15）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 パラメータの設定手順については、「ビーコン モードの設定」（P.2-17）を参照してください。

MDIX

Medium Dependent Interface-crossover（MDI-X; メディア依存インターフェイスクロスオーバー）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 パラメータの設定手順については、「MDIX パラメータの設定」（P.2-24）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。デフォルトでは、このパラメータは 100 ミリ秒に設定されています。

注意　デバウンス タイマーをイネーブルにするとリンクアップおよび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 パラメータの設定手順については、「デバウンス タイマーの設定」（P.2-25）を参照してください。

Error Disabled

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 err-disabled ステートの場合、**errdisable detect cause** コマンドを使用して、エラーに関する情報を検索します。

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 コマンドは、300 秒後に自動回復を提供します。

errdisable recovery interval コマンドを使用して、回復期間を 30 ～ 65535 秒の範囲内で変更できます。また、特定の err-disable の原因に回復タイムアウトを設定することもできます。

その原因に対して error-disabled の回復をイネーブルにしない場合、インターフェイスは、**shutdown** および **no shutdown** コマンドが入力されるまで error-disabled ステートのままです。原因の回復をイネーブルにした場合、インターフェイスは error-disabled ステートから回復し、すべての原因がタイムアウトになったときに動作を再開できるようになります。エラーの背後にある理由を表示するには、**show interface status err-disabled** コマンドを使用します。

レート モード

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 Gbps（ギガビット/秒）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。

表 2-1 に、10 Gbps 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 2-1　　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

表 2-1　共有ポートと専用ポート （続き）

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
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, Release 5.x*』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。表 2-2 は、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の各タイプで動作する設定を示します。

表 2-2　イーサネットおよび管理インターフェイスで使用する速度およびデュプレックスモード設定

モジュールのタイプ	速度モード設定	デュプレックス モード設定	動作速度（Mb/s）	動作デュプレックス モード
32 ポート 10 ギガビット イーサネット	自動[1]	自動 [1]	10,000	全二重
48 ポート 10/100/1000 イーサネット	自動 [1]	自動 [1]	1000	全二重
			10 または 100	半二重
	1000	自動 [1] または全二重	1000	全二重
	100	自動 [1] または半二重	100	半二重
		全二重	100	全二重
	10	自動 [1] または半二重	10	半二重
		全二重	10	全二重
管理	自動 [1]	自動 [1]	1000	全二重
			10 または 100	半二重
	1000	自動 [1] または全二重	1000	全二重
	100	自動 [1] または半二重	100	半二重
		全二重	100	全二重
	10	自動 [1] または半二重	10	半二重
		全二重	10	全二重

1. デフォルト設定

ポート チャネル インターフェイスに速度モードおよびデュプレックス モードを設定する方法については、「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」（P.6-23）を参照してください。他のインターフェイスに速度モードおよびデュプレックス モードを設定する方法については、「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」（P.2-27）を参照してください。

フロー制御

1 Gbps 以上で稼動するイーサネット 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、表 2-3 を参照してください。

表 2-3　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		
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）	リンク フロー制御の状態
イネーブル	イネーブル	イネーブル
イネーブル	指定	イネーブル
イネーブル	ディセーブル	ディセーブル
指定	イネーブル	イネーブル
指定	指定	イネーブル
指定	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	指定	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手順については、「フロー制御の設定」（P.2-29）を参照してください。

ポート MTU サイズ

Maximum Transmission Unit（MTU; 最大伝送ユニット）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 サイズの設定手順については、「MTU サイズの設定」（P.2-30）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 インターフェイスに帯域幅パラメータを設定する方法については、「帯域幅と遅延の割り当て（情報目的）」（P.6-19）を参照してください。他のインターフェイスに帯域幅パラメータ設定する方法については、「帯域幅の設定」（P.2-34）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、EIGRP は、遅延設定を使用して、あるイーサネット リンクの別のイーサネット リンクに対する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 インターフェイスに帯域幅パラメータを設定する方法については、「帯域幅と遅延の割り当て（情報目的）」（P.6-19）を参照してください。他のインターフェイスにスループット遅延パラメータを設定する方法については、「スループット遅延の設定」（P.2-35）を参照してください。

管理ステータス

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 インターフェイスに管理ステータス パラメータを設定する方法については、「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」（P.6-20）を参照してください。他のインターフェイスに管理ステータス パラメータを設定する方法については、「インターフェイスのシャットダウンおよび再開」（P.2-36）を参照してください。

UDLD パラメータ

ここでは、次の内容について説明します。

UDLD の概要

シスコシステムズ独自の Unidirectional Link Detection（UDLD; 単一方向リンク検出）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。単方向リンクによって、スパニング ツリー トポロジ ループなどのさまざまな問題が発生する可能性があります。

UDLD は、レイヤ 1 プロトコルと連動し、リンクの物理的ステータスを判別するレイヤ 2 プロトコルです。レイヤ 1 では、物理シグナリングおよび障害検出が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 の検出、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できない処理を実行します。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 の検知機能が連動し、物理的および論理的な単方向接続、および他のプロトコルの誤作動を防止します。

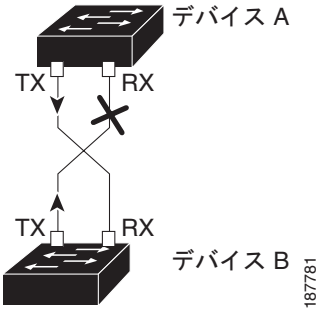
リンク上でローカル デバイスが送信したトラフィックをネイバーが受信するにもかかわらず、ネイバーから送信されたトラフィックをローカル デバイスが受信しない場合は、必ず単方向リンクが発生しています。対になっているファイバ ケーブルのどちらかの接続が切断されても、自動ネゴシエーションがアクティブである限り、リンクはアップしません。この場合、論理リンクは不確定であり、UDLD は何の処理も行いません。両方のファイバがレイヤ 1 で正常に動作していれば、レイヤ 2 の UDLD はそれらのファイバが適切に接続されているかどうか、また、適切なネイバー間でトラフィックが双方向に流れているかどうかを判別します。自動ネゴシエーションはレイヤ 1 で機能するため、このチェックは自動ネゴシエーションでは実行されません。

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。このフレームが一定の時間内にエコー バックされ、かつ特定の確認応答（エコー）がない場合は、そのリンクは単方向リンクとしてマークが付けられ、LAN ポートがシャットダウンされます。プロトコルが単方向リンクを正常に識別してディセーブルにするには、リンクの両端のデバイスが UDLD をサポートする必要があります。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）　デフォルトでは、銅線の LAN ポート上の UDLD はローカルでディセーブルに設定されており、同じタイプのメディアに不要な制御トラフィックが送信されないようになっています。

図 2-1 に、単方向リンク条件の例を示します。デバイス B は、ポート上でデバイス A から正常にトラフィックを受信しますが、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されます。

図 2-1　単方向リンク



UDLD のデフォルト設定

表 2-4 に、UDLD のデフォルト設定を示します。

表 2-4　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 ステート イネーブル（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
ツイスト ペア（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 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

デバイスとそのポートに UDLD を設定する手順については、「UDLD モードの設定」（P.2-38）を参照してください。

UDLD アグレッシブ モードおよび非アグレッシブ 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に、デフォルトの 15 秒間隔を使用する非アグレッシブ UDLD により、（デフォルトのスパニング ツリー パラメータを使用している場合）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、すみやかに単方向リンクをシャットダウンできます。

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　In-Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）中にラインカードのアップグレードが行われていて、ラインカード上の一部のポートがレイヤ 2 ポート チャネルのメンバであり、UDLD アグレッシブ モードで設定されている場合。リモート ポートのいずれかがシャットダウンされた場合、UDLD は、ローカル デバイスの対応するポートを error disabled ステートにします。これは正しい動作です。

ISSU の終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、**no shutdown** コマンドの順に実行します。

キャリア遅延

（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。VLAN ネットワーク インターフェイスの設定手順については、第 4 章「レイヤ 3 インターフェイスの設定」を参照してください。

リンクがダウン状態になり、キャリア遅延タイマーが期限切れになる前にアップ状態に戻った場合、ダウン状態は効果的にフィルタリングされ、デバイスの他のソフトウェアは、リンクダウン イベントが発生したことを認識しません。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 2 秒または 50 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。また、ポート チャネルでは、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 チャネルの設定手順については、第 6 章「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 Release 4.2(1) 以降では、多く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、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。各ポート プロファイルは、特定のタイプのインターフェイスにだけ適用できます。次のタイプを選択できます。

- 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
- トンネル

（注）　インターフェイスのタイプとしてイーサネットを選択すると、ポート プロファイルは、レイヤ 3 のデフォルト モードになります。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 1 つのインターフェイスまたは一定範囲のインターフェイスに適用すると、ポート プロファイルは継承されます。ポート プロファイルを 1 つのインターフェイスまたは一定範囲のインターフェイスに適用する（継承する）と、システムはそのポート プロファイルのすべてのコマンドをインターフェイスに適用します。さらに、1 つのポート プロファイルに別のポート プロファイルからの設定を継承させることができます。別のポート プロファイルを継承することによって、最初のポート プロファイルは、最初のポート プロファイルと矛盾しない 2 つめの継承されたポート プロファイルのすべてのコマンドを想定できます。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。

システムは、次のガイドラインに従って、インターフェイスまたは一定範囲のインターフェイスが継承したコマンドを適用します。

- 矛盾がある場合、インターフェイス モードで入力するコマンドは、ポート プロファイルのコマンドより優先されます。ただし、ポート プロファイルは、ポート プロファイル内にそのコマンドを保持します。
- port-profile コマンドがデフォルトのコマンドによって明示的に無効にされない限り、ポート プロファイルのコマンドは、インターフェイスのデフォルトのコマンドより優先されます。
- 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 プロファイルを 1 つのインターフェイスまたは一定範囲のインターフェイスに継承後、インターフェイス設定レベルで新しい値を入力することによって、個々の設定値を無効にできます。インターフェイス設定レベルで個々の設定値を削除した場合、インターフェイスは、その値を再びポート プロファイルで使用します。
- ポート プロファイルに関連付けられたデフォルトの設定はありません。

コマンドのサブセットは、指定するインターフェイスのタイプによって、ポート プロファイル コンフィギュレーション モードで使用できます。

（注）　ポート プロファイルは Session Manager で使用できません。Session Manager の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』を参照してください。

ポート プロファイルの設定をインターフェイスに適用するには、特定のポート 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、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。

1 つまたは複数のポート プロファイルを元のポート プロファイルに継承した場合、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。システムは、基盤となるポート プロファイルがイネーブルであることを想定します。

一定範囲のインターフェイスからポート プロファイルを削除すると、システムは最初にインターフェイスから設定を解除してから、ポート プロファイルの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、システムは、インターフェイスの設定をチェックし、直接入力されたインターフェイス コマンドによって無効にされた port-profile コマンドをスキップするか、コマンドをデフォルト値に戻します。

他のポート プロファイルによって継承されたポート プロファイルを削除する場合、ポート プロファイルを削除する前に、その継承を削除する必要があります。

また、ポート プロファイルを削除するインターフェイスのサブセットを、そのプロファイルを最初に適用したインターフェイスのグループから選択することもできます。たとえば、ポートプロファイルを設定し、そのポート プロファイルを継承する 10 個のインターフェイスを設定した場合、指定された 10 個のインターフェイスの一部だけからポート プロファイルを削除できます。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動作し続けます。

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、指定された一定範囲のインターフェイスの特定の設定を削除した場合、その設定もその範囲のインターフェイスのポート プロファイルだけから削除されます。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 チャネルを削除した場合、指定されたポート チャネルはポート プロファイルからも削除されます。

デバイスと同様に、オブジェクトがインターフェイスに適用されていない状態で、ポート プロファイルのオブジェクトの設定を入力できます。たとえば、Virtual Routing and Forward（VRF）インスタンスは、システムに適用しなくても設定できます。その VRF と付帯的な設定をポート プロファイルから削除しても、システムは影響を受けません。

ポート プロファイルを 1 つのインターフェイスまたは一定範囲のインターフェイスに継承し、特定の設定値を削除した後、そのポート プロファイルの設定は、指定されたインターフェイスで動作しません。

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、エラーが返されます。

ポート プロファイルをイネーブルにするか、継承するか、または修正しようとすると、チェックポイントが作成されます。ポート プロファイルの設定が失敗した場合、以前の設定にロールバックし、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（TDR）ケーブル診断

Cisco Nexus 7000 シリーズ デバイスの Cisco NX-OS Release 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組み込まれているケーブル診断機能を使用すると、リンク障害の診断のために、ケーブルを取り外して、ケーブル テスターを接続する必要がありません。ラインカード上の各ポートは、Time Domain Reflectometry（TDR; タイム ドメイン反射率計）と呼ばれる新しいテクノロジーを使用して、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 は、パルス波形信号を送信し、反射した波形の極性、振幅、および往復時間を検査することによって、導体を分析するために使用される技術です。

ケーブル内での信号の伝播速度を推定し、その反射が送信元に戻るまでの時間を測定することによって、反射点までの距離を測定できます。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。

ケーブルの障害をリモートで診断できるので、問題の根本的な原因をより早くより効果的に特定できるようになり、ユーザは接続問題にすばやく対応できます。

ライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	基本インターフェイス パラメータに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。Cisco NX-OS のライセンス スキームの詳細については、『*Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x*』を参照してください。

（注）　VDC を使用する場合は Advanced Services ライセンスが必要です。

注意事項および制約事項

次の注意事項と制約事項に従って基本インターフェイス パラメータを設定します。

- 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には、**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、表 2-2（P.2-4）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ト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。

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。

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。

ここでは、インターフェイスを指定してそれぞれの基本パラメータを設定する方法について説明します。

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。

表 2-5 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 2-5　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 モードを使用すると、同じ設定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、インターフェイス範囲コンフィギュレーション モードを終了するまで、入力するすべてのコマンド パラメータが範囲内のすべての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。ダッシュは連続するインターフェイスを区切り、カンマは連続しないインターフェイスを区切ります。連続しないインターフェイスを入力する場合、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、連続するインターフェイス範囲を設定する例を示します。

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

次に、連続しないインターフェイス範囲を設定する例を示します。

```
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にある場合にだけ（例：2/29.1-2）、サブインターフェイスを範囲内で指定できます。しかし、一定範囲のポートにある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 は入力できます。

手順の概要

1. **configure terminal**
2. **interface** *interface*

手順の詳細

	コマンド	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 1：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
	
	例 2：
	`switch(config)# interface mgmt0`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス タイプと ID を指定できます。イーサネット ポートの場合、「ethernet *slot/port*」を使用します。管理インターフェイスの場合、「mgmt0」を使用します。
		例 1 は、スロット 2、ポート 1 イーサネット インターフェイスを指定する方法です。
		例 2 は、管理インターフェイスを指定する方法です。

（注） インターフェイス タイプと ID の間に空白を追加する必要はありません（ポートまたはスロット/ポート番号）。たとえば、イーサネット スロット 4、ポート 5 のインターフェイスの場合、「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」です。

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。

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 80 字以内で、大文字と小文字は区別されます。

手順の概要

1. **configure terminal**
2. **interface** *interface*

3. **description** *text*
4. **show interface** *interface*
5. **exit**
6. **copy running-config startup-config**

手順の詳細

	コマンド	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 ethernet 2/1 switch(config-if)# switch(config)# interface mgmt0 switch(config-if)#	設定するインターフェイスを指定します。インターフェイス タイプと ID を指定できます。イーサネット ポートの場合、「ethernet *slot/port*」を使用します。管理インターフェイスの場合、「mgmt0」を使用します。 例 1 は、スロット 2、ポート 1 イーサネット インターフェイスを指定する方法です。 例 2 は、管理インターフェイスを指定する方法です。
ステップ 3	**description** *text* 例： switch(config-if)# description Ethernet port 3 on module 1. switch(config-if)#	インターフェイスの説明を指定します。説明に使用できる文字数は最大 80 文字です。
ステップ 4	**show interface** *interface* 例： switch(config)# show interface ethernet 2/1	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 5	**exit** 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 6	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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)#
```

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。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot*/*port*
3. **beacon** | {**no beacon**}
4. **show interface ethernet** *slot*/*port*
5. **exit**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	`configure terminal`
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet** *slot/port*
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**beacon** | {**no beacon**}
	
	例：
	`switch(config-if)# beacon`
	`switch(config-if)#`
		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	`show interface ethernet slot/port`
	
	例：
	`switch(config)# show interface ethernet 2/1`
		インターフェイス ステータスを表示します。ビーコン モード ステータスもあわせて表示します。

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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 モジュールの 10 GB ごとの帯域幅を 1 ポート専用にするのか同じポート グループの 4 つのポートで共有させるのかを指定できます。

ここでは、次の内容について説明します。

- 「ポート プロファイルの作成」（P.2-42）
- 「帯域幅をポート グループ内で共有」（P.2-19）

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。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot/port,* **ethernet** *slot/port,* **ethernet** *slot/port,* **ethernet** *slot/port*
3. **shutdown**
4. interface ethernet *slot/port*
5. **rate-mode dedicated**
6. no shutdown
7. **show interface ethernet** *slot/port* **capabilities**
8. **exit**
9. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet** *slot/port*, **ethernet** *slot/port*, **ethernet** *slot/port*, **ethernet** *slot/port*
	
	例：
	`switch(config)# interface ethernet 3/1, ethernet 3/3, ethernet 3/5, ethernet 3/7`
	`switch(config-if)#`
		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。
		
		次に、1 つのポートを専用モードに指定する例を示します。

	コマンド	目的
ステップ 3	**shutdown** 例： switch(config)# shutdown	ポートを管理シャットダウンします。
ステップ 4	**interface ethernet** *slot/port* 例： switch(config)# interface ethernet 3/1 switch(config)#	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	**rate-mode dedicated** 例： switch(config-if)# rate-mode dedicated switch(config-if)#	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	no shutdown 例： switch(config-if)# no shutdown	ポートを管理的にアップします。
ステップ 7	**show interface ethernet** *slot/port* **capabilities** 例： switch(config)# show interface ethernet 3/1	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	**exit** 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 9	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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。

作業を開始する前に

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。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **shutdown**
4. **interface ethernet** *slot/port*, ethernet *slot/port*, **ethernet** *slot/port*, **ethernet** *slot/port*
5. **rate-mode shared**
6. **no shutdown**
7. **show interface ethernet** *slot/port*
8. **exit**
9. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet** *slot/port*
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config)#`
		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	`shutdown`
	
	例：
	`switch(config-if)# shutdown`
		ポートを管理的にダウンさせます。

ステップ 4	**interface ethernet** *slot/port*, **ethernet** *slot/port*, **ethernet** *slot/port*, **ethernet** *slot/port*
	
	例：
	`switch(config)# interface ethernet 3/1, ethernet 3/3, ethernet 3/5, ethernet 3/7`
	`switch(config-if)#`
		設定する 4 つのイーサネット インターフェイスを指定し（同じポート グループに所属している必要があります）、インターフェイス コンフィギュレーション モードを開始します。
		
		次に、1 つのポートを専用モードに指定する例を示します。

ステップ 5	**rate-mode shared**
	
	例：
	`switch(config-if)# rate-mode shared`
	`switch(config-if)#`
		指定したポートに共有レート モードを設定します。
		
		次に、共有モードを設定する例を示します。

ステップ 6	`no shutdown`
	
	例：
	`switch(config-if)# no shutdown`
		ポートを管理的にアップします。

ステップ 7	**show interface ethernet** *slot/port* 例： `switch(config)# show interface ethernet 3/1`	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。

	コマンド	目的
ステップ 8	**exit** 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 9	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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。

ここでは、次の内容について説明します。

- 「Error Disable 検出のイネーブル化」（P.2-21）
- 「Error-Disabled 回復のイネーブル化」（P.2-22）
- 「Error-Disabled 回復間隔の設定」（P.2-23）

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。

手順の概要

1. **configure terminal**
2. **errdisable detect cause** {**acl-exception** | **all** | **link-flap** | **loopback**}
3. **shutdown**
4. **no shutdown**
5. **show interface status err-disabled**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**errdisable detect cause** {**acl-exception** | **all** | **link-flap** | **loopback**} 例： switch(config)# errdisable detect cause all switch(config)#	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。デフォルトはディセーブルです。
ステップ 3	**shutdown** 例： switch(config)# shutdown switch(config)#	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	**no shutdown** 例： switch(config)# no shutdown switch(config)#	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	**show interface status err-disabled** 例： switch(config)# 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。
ステップ 6	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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)#

Error-Disabled 回復のイネーブル化

インターフェイスを error-disabled ステートから回復させ、再びアップするアプリケーションを指定できます。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）。

手順の概要

1. **configure terminal**
2. **errdisable recovery cause** {**all** | **bpdguard** | **link-flap** | **psecure-violation** | **security-violation** | **storm-control** | **udld**}
3. **show interface status err-disabled**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**errdisable recovery cause** {**all** | **bpduguard** | **link-flap** | **psecure-violation** | **security-violation** | **storm-control** | **udld**} 例： switch(config)# errdisable recovery cause all switch(config-if)#	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 秒後にリトライします。デフォルトはディセーブルです。
ステップ 3	**show interface status err-disabled** 例： switch(config)# 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。
ステップ 4	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例では、すべての条件で error-disabled 回復をイネーブルにする方法を示します。

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

Error-Disabled 回復間隔の設定

error-disabled 回復タイマーの値を設定できます。

手順の概要

1. **configure terminal**
2. **errdisable recovery** interval *interval*
3. **show interface status err-disabled**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**errdisable recovery interval** *interval*
	
	例：
	`switch(config)# errdisable recovery interval 32`
	`switch(config-if)#`
		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	**show interface status err-disabled** 例： `switch(config)# 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。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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。

作業を開始する前に

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。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. {**mdix auto**} | {**no mdix**}
4. **show interface ethernet** *slot*/*port*
5. **exit**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface ethernet** *slot*/*port* 例： switch(config)# interface ethernet 3/1 switch(config-if)#	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	{**mdix auto**}	{**no mdix**} 例： switch(config-if)# mdix auto switch(config-if)#	ポートの MDIX 検出をイネーブルまたはディセーブルに指定します。
ステップ 4	**show interface ethernet** *slot*/*port* 例： switch(config)# show interface ethernet 3/1 switch(config-if)#	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	**exit** 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 6	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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 タイマーをイネーブルにするには、デバウンス時間をミリ秒（ms）で指定します。ディセーブルにするにはデバウンス時間を 0 に指定します。

show interface debounce コマンドを使用すると、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。

手順の概要

1. **configure terminal**
2. **interface** *ethernet slot/port*
3. **link debounce time** *milliseconds*
4. **show interface debounce**
5. **exit**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *ethernet slot/port*
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**link debounce time** *milliseconds*
	
	例：
	`switch(config-if)# link debounce time 1000`
	`switch(config-if)#`
		合計時間を指定してデバウンス タイマーをイネーブルにします（0 ～ 5000 ms）。
		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	**show interface debounce**
	
	例：
	`switch(config)# show interface debounce`
	`switch(config-if)#`
		すべてのイーサネット インターフェイスのリンク デバウンス時間を表示します。

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、イーサネット ポート 3/1 のデバウンス タイマーをイネーブルにし、デバウンス時間を 1,000 ms 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、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 モードにつては、表 2-2（P.2-4）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。

作業を開始する前に

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。

手順の概要

1. **configure terminal**
2. **interface** *interface*
3. **speed** {{**10** | **100** | **1000** | {**auto** [**10** **100** [**1000**]]}} | {**10000** | **auto**}}
4. duplex {**full** | **half** | **auto**}
5. **show interface** *interface*
6. exit
7. **copy running-config startup-config**

手順の詳細

	コマンド	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 1： switch(config)# interface ethernet 2/1 switch(config-if)# 例 2： switch(config)# interface mgmt0 switch(config-if)#	設定するインターフェイスを指定します。インターフェイス タイプと ID を指定できます。イーサネット ポートの場合、「ethernet *slot/port*」を使用します。管理インターフェイスの場合、「mgmt0」を使用します。 例 1 は、スロット 2、ポート 1 イーサネット インターフェイスを指定する方法です。 例 2 は、管理インターフェイスを指定する方法です。
ステップ 3	**speed** {{**10** | **100** | **1000** | {**auto** [**10 100** [**1000**]]}} | {**10000** | **auto**}} 例： switch(config-if)# speed 1000 switch(config-if)#	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 10,000 Mb/s（10 Gb/s）の速度を設定します。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	duplex {full | half | auto} 例： switch(config-if)# duplex full	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	**show interface** *interface* 例： switch(config)# show interface *mgmt0*	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 6	**exit** 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 7	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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性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。

作業を開始する前に

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。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **flowcontrol** {**send** | **receive**} {**desired** | **on** | **off**}
4. show interface ethernet *slot/port*
5. show interface flowcontrol
6. exit
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# config terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet** *slot*/*port*
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		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	`flowcontrol {send | receive} {desired | on | off}`
	
	例：
	`switch(config-if)# flowcontrol send on`
	`switch(config)-if#`
		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だけ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	**show interface ethernet** *slot*/*port*
	
	例：
	`switch(config)# show interface ethernet 3/1`
	`switch(config)`
		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 5	**show interface flowcontrol**
	
	例：
	`switch(config)# show interface flowcontrol`
	`switch(config)`
		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 6	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 7	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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ユニット（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 サイズは変更できますが、この値を変更した場合は、値を使用するレイヤ 2 インターフェイスもアップデートして、新しいシステム ジャンボ MTU 値を使用する必要があります。レイヤ 2 インターフェイスの MTU 値をアップデートしない場合、これらのインターフェイスはシステム デフォルト MTU（1500 バイト）を使用します。

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。

ポート モードを変更するには **switchport** コマンドを使用します。

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。

ここでは、次の内容について説明します。

- 「インターフェイス MTU サイズの設定」（P.2-31）
- 「システム ジャンボ MTU サイズの設定」（P.2-32）

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 インターフェイスとは異なるシステム ジャンボ MTU サイズを使用する場合は、「システム ジャンボ MTU サイズの設定」（P.2-32）を参照してください。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot*/*port*
3. **switchport** | {**no switchport**}
4. **mtu** *size*
5. **show interface ethernet** *slot*/*port*
6. **exit**
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface ethernet** *slot/port* 例： switch(config)# interface ethernet 3/1 switch(config-if)#	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	**switchport** | {**no switchport**} 例： switch(config-if)# no switchport switch(config-if)#	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	**mtu** *size* 例： switch(config-if)# mtu 9216 switch(config-if)#	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	**show interface ethernet** *slot/port* 例： switch(config)# show interface ethernet 2/1	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 6	**exit** 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 7	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

システム ジャンボ MTU サイズを設定するとレイヤ 2 インターフェイスの MTU サイズを指定できます。1500 ～ 9216 の偶数を指定できます。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。

手順の概要

1. **configure terminal**
2. **system jumbomtu** *size*
3. **show running-config**
4. **interface** *type slot/port*
5. **mtu** *size*
6. **exit**
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**system jumbomtu** *size*
	
	例：
	`switch(config)# system jumbomtu 8000`
	`switch(config)#`
		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	**show running-config all** 例： `switch(config)# show running-config all | include jumbomtu`	現在の動作設定を表示します。システム ジャンボ MTU サイズもあわせて表示します。

ステップ 4	**interface** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

ステップ 5	`mtu size`
	
	例：
	`switch(config-if)# mtu 1500`
	`switch(config-if)#`
		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。

ステップ 6	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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 4608
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。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot*/*port*
3. **bandwidth** *kbps*
4. **show interface ethernet** *slot*/*port*
5. **exit**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet** *slot/port*
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		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	**bandwidth** *kbps*
	
	例：
	`switch(config-if)# bandwidth 1000000`
	`switch(config-if)#`
		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	**show interface ethernet** *slot/port* 例： `switch(config)# show interface ethernet 2/1`	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。

	コマンド	目的

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot*/*port*
3. **delay** *value*
4. **show interface ethernet** *slot*/*port*
5. **exit**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet** *slot*/*port*
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**delay** *value*
	
	例：
	`switch(config-if)# delay 10000`
	`switch(config-if)#`
		遅延時間を設定します。単位は 10 マイクロ秒です。1 ～ 16777215 の情報値を設定できます。単位は 10 マイクロ秒です。

	コマンド	目的

ステップ 4	**show interface ethernet** *slot/port*
	
	例：
	`switch(config)# show interface ethernet 3/1`
	`switch(config-if)#`
		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 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、1 つのインターフェイスが別のインターフェイスより優先されるように、スループット遅延時間を設定する方法を示します。低い遅延値は高い遅延値より優先されます。次の例では、イーサネット 7/48 は 7/47 より優先されます。7/48 のデフォルト遅延は、最も高い値（16777215）に設定されている 7/47 の設定値より低くなっています。

```
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 プロトコルによってその他のネットワーク 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。

手順の概要

1. **configure terminal**
2. **interface** *interface*
3. **shutdown**
4. **show interface** *interface*
5. **no shutdown**

6. **show interface** *interface*
7. **exit**
8. **copy running-config startup-config**

手順の詳細

	コマンド	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 ethernet 2/1 switch(config-if)# switch(config)# interface mgmt0 switch(config-if)#	設定するインターフェイスを指定します。インターフェイス タイプと ID を指定できます。イーサネット ポートの場合、「ethernet *slot/port*」を使用します。管理インターフェイスの場合、「mgmt0」を使用します。 例 1 は、スロット 2、ポート 1 イーサネット インターフェイスを指定する方法です。 例 2 は、管理インターフェイスを指定する方法です。
ステップ 3	**shutdown** 例： switch(config-if)# shutdown switch(config-if)#	インターフェイスをディセーブルにします。
ステップ 4	show interface *interface* 例： switch(config-if)# show interface ethernet 2/1 switch(config-if)#	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	**no shutdown** 例： switch(config-if)# no shutdown switch(config-if)#	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	show interface *interface* 例： switch(config-if)# show interface ethernet 2/1 switch(config-if)#	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	**exit** 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 8	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

UDLD を実行するように設定されたデバイスのイーサネット インターフェイスに、ノーマルまたはアグレッシブ単方向リンク検出（UDLD）モードを設定できます。インターフェイスの UDLD モードをイネーブルにする前に、インターフェイスを含むデバイスの UDLD がイネーブルになっていることを確認する必要があります。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。

ノーマル UDLD モードを使用するには、ポートのいずれかをノーマル モードに設定し、他のポートをノーマル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。

作業を開始する前に

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。

手順の概要

1. **configure terminal**
2. **feature udld**
   no feature udld
3. **udld message-time** *seconds*
4. **udld aggressive**
5. **interface ethernet** *slot*/*port*
6. **udld** {**enable** | **disable**}
7. **show udld** [**ethernet** *slot*/*port* | **global** | **neighbors**}
8. **exit**
9. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	`configure terminal`
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**feature udld**
	
	例：
	`switch(config)# feature udld`
	`switch(config)#`
		デバイスの UDLD をイネーブルにします。

	no feature udld
	
	例：
	`switch(config)# no feature udld`
	`switch(config)#`
		デバイスの UDLD をディセーブルにします。

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

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

ステップ 5	**interface ethernet** *slot/port*
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		（任意）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 6	**udld {enable | disable}**
	
	例：
	`switch(config-if)# udld aggressive`
	`switch(config-if)#`
		（任意）指定されたインターフェイスの UDLD をイネーブルまたはディセーブルにします。

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

	コマンド	目的
ステップ 8	**exit** 例： switch(config-if-range)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 9	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

次に、イーサネット ポート 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 disable
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。

作業を開始する前に

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。

手順の概要

1. **configure terminal**
2. **interface vlan** *vlan-id*
3. **carrier-delay** {*sec* | **msec** *number*}
4. **show interface vlan** *vlan-id*
5. **exit**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	`configure terminal`
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface vlan***-id*
	
	例：
	`switch(config)# interface vlan 5`
	`switch(config-if)#`
		VLAN インターフェイス モードを開始します。

ステップ 3	**carrier-delay {***sec* **| msec** *number***}**
	
	例：
	`switch(config-if)# carrier-delay 20`
	`switch(config-if)#`
		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 2 秒または 50 ミリ秒です。

ステップ 4	**show interface vlan***-id*
	
	例：
	`switch(config-if)# show interface vlan 5`
	`switch(config-if)#`
		インターフェイスのステータスを表示します。

	コマンド	目的

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 6	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例では、VLAN 5 のキャリア遅延タイマーを 20 秒に設定する方法を示します。

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

を使用して、管理（mgmt0）イーサネット インターフェイスを設定して IP 上で接続できます。

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。

ここでは、次の内容について説明します。

- 「ポート プロファイルの作成」（P.2-42）
- 「ポート プロファイル コンフィギュレーション モードの開始とポート プロファイルの修正」（P.2-43）
- 「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」（P.2-44）
- 「特定のポート プロファイルのイネーブル化」（P.2-45）
- 「ポート プロファイルの継承」（P.2-47）
- 「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」（P.2-48）
- 「継承されたポート プロファイルの削除」（P.2-49）

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。

手順の概要

1. **configure terminal**
2. **port-profile** [**type** {**ethernet** | **interface-vlan** | **loopback** | **port channel** | **tunnel**}] *name*
3. **exit**
4. **show port-profile**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**port-profile** [**type** {**ethernet** | **interface-vlan** | **loopback** | **port channel** | **tunnel**}] *name* 例： switch(config)# port-profile type tunnel test switch(config-ppm)#	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	**exit** 例： switch(config-ppm)# exit switch(config)#	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 port-profile** 例： switch(config)# show port-profile	（任意）ポート プロファイルの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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 モードの開始とポート 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。

手順の概要

1. **configure terminal**
2. **port-profile** [**type** {**ethernet** | **interface-vlan** | **loopback** | **port channel** | **tunnel**}] *name*
3. **exit**
4. **show port-profile**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**port-profile** [**type** {**ethernet** | **interface-vlan** | **loopback** | **port channel** | **tunnel**}] *name* 例： switch(config)# port-profile type tunnel test switch(config-ppm)# no shutdown switch(config-ppm)#	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。
ステップ 3	**exit** 例： switch(config-ppm)# exit switch(config)#	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 port-profile** 例： switch(config)# show port-profile	（任意）ポート プロファイルの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

1 つのインターフェイスまたは一定範囲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。

手順の概要

1. **configure terminal**
2. **interface** [**ethernet** *slot/port* | **interface-vlan** *vlan-id* | **loopback** *number* | **port-channel** *number* | **tunnel** *number*]
3. **inherit port-profile** *name*
4. **exit**
5. **show port-profile**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **例：** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface** [**ethernet** *slot/port* | **interface-vlan** *vlan-id* | **loopback** *number* | **port channel** *number* | **tunnel** *number*] **例：** switch(config)# interface ethernet 7/3-5, 10/2, 11/20-25 switch(config-if)#	インターフェイスの範囲を選択します。
ステップ 3	**inherit port-profile** *name* **例：** switch(config-if)# inherit port-profile adam switch(config-if)#	選択されたインターフェイスに指定されたポート プロファイルを割り当てます。
ステップ 4	**exit** **例：** switch(config-ppm)# exit switch(config)#	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	**show port-profile** **例：** switch(config)# show port-profile	（任意）ポート プロファイルの設定を表示します。
ステップ 6	**copy running-config startup-config** **例：** switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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)#
```

特定のポート プロファイルのイネーブル化

ポート プロファイルの設定をインターフェイスに適用するには、特定のポート 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。

1 つまたは複数のポート プロファイルを元のポート プロファイルに継承した場合、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。システムは、基盤となるポート プロファイルがイネーブルであることを想定します。

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。

手順の概要

1. **configure terminal**
2. **port-profile** [**type** {**ethernet** | **interface-vlan** | **loopback** | **port channel** | **tunnel**}] *name*
3. **state enabled**
4. **exit**
5. **show port-profile**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**port-profile** [**type** {**ethernet** | **interface-vlan** | **loopback** | **port channel** | **tunnel**}] *name*
	
	例：
	`switch(config)# port-profile type tunnel test`
	`switch(config-ppm)# no shutdown`
	`switch(config-ppm)#`
		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	**state enabled**
	
	例：
	`switch(config-ppm)# state enabled`
	`switch(config)#`
		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	**exit**
	
	例：
	`switch(config-ppm)# exit`
	`switch(config)#`
		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	**show port-profile** 例： `switch(config)# show port-profile`	（任意）ポート プロファイルの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例では、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ます。

```
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。

手順の概要

1. **configure terminal**
2. **port-profile** *name*
3. **inherit port-profile** *name*
4. **exit**
5. **show port-profile**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**port-profile** *name*
	
	例：
	`switch(config)# port-profile test`
	`switch(config-ppm)#`
		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	**inherit port-profile** *name*
	
	例：
	`switch(config-ppm)# inherit port-profile adam`
	`switch(config-ppm)#`
		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	**exit**
	
	例：
	`switch(config-ppm)# exit`
	`switch(config)#`
		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	**show port-profile** 例： `switch(config)# show port-profile`	（任意）ポート プロファイルの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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。この作業は、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。

手順の概要

1. **configure terminal**
2. **interface** [**ethernet** *slot/port* | **interface-vlan** *vlan-id* | **loopback** *number* | **port-channel** *number* | **tunnel** *number*]
3. **no inherit port-profile** *name*
4. **exit**
5. **show port-profile**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** [**ethernet** *slot/port* | **interface-vlan** *vlan-id* | **loopback** *number* | **port channel** *number* | **tunnel** *number*]
	
	例：
	`switch(config)# interface ethernet 7/3-5, 10/2, 11/20-25`
	`switch(config-if)#`
		インターフェイスの範囲を選択します。

ステップ 3	**no inherit port-profile** *name*
	
	例：
	`switch(config-if)# no inherit port-profile adam`
	`switch(config-if)#`
		選択されたインターフェイスから指定されたポート プロファイルを削除します。

ステップ 4	**exit**
	
	例：
	`switch(config-ppm)# exit`
	`switch(config)#`
		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	**show port-profile** 例： `switch(config)# show port-profile`	（任意）ポート プロファイルの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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 から adam という名前のポート プロファイルを削除する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 7/3-5, 10/2, 11/20-25
switch(config-if)# no 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。この作業は、ポート プロファイル モードで行います。

手順の概要

1. **configure terminal**
2. **port-profile** *name*
3. **no inherit port-profile** *name*
4. **exit**
5. **show port-profile**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**port-profile** *name*
	
	例：
	`switch(config)# port-profile test`
	`switch(config-ppm)#`
		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	**no inherit port-profile** *name*
	
	例：
	`switch(config-ppm)# no inherit port-profile adam`
	`switch(config-ppm)#`
		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	**exit**
	
	例：
	`switch(config-ppm)# exit`
	`switch(config)#`
		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	目的
ステップ 5	**show port-profile** 例： switch(config)# show port-profile	（任意）ポート プロファイルの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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。

作業を開始する前に

TDR テストのガイドラインは、次のとおりです。

- TDR は最大 115 メートルの長さのケーブルをテストできます。
- ケーブルの両端で同時にテストを開始しないでください。ケーブルの両端で同時にテストを開始すると、誤ったテスト結果が得られることがあります。
- ケーブル診断テスト中にポートの設定を変更しないでください。ポートの設定を変更すると、誤ったテスト結果が得られることがあります。
- TDR テストを実行する前に、インターフェイスをダウンさせる必要があります。

手順の概要

1. **test cable-diagnostics tdr interface** *number*
2. **show interface** *number* **cable-diagnostics-tdr**

手順の詳細

	コマンド	目的
ステップ 1	**test cable-diagnostics tdr interface** *number* 例： switch# **test cable-diagnostics tdr interface ethernet 7/1**	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	**show interface** *number* **cable-diagnostics-tdr** 例： switch(config)# **show interface ethernet 7/1 cable-diagnostics-tdr**	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。

```
switch# test cable-diagnostics tdr interface ethernet 7/1
switch# show interface ethernet 7/1 cable-diagnostics-tdr

--------------------------------------------------------------------------------
Interface      Speed Pair Cable Length   Distance to fault   Channel Pair Status
-------------- ----- ---- -------------- ------------------- ------- -----------
```

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。

手順の詳細

基本的なインターフェイス設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show 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 *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を示す表を表示します。
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 vdc	現在の VDC のステータスを表示します。
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。

これらのコマンドの出力フィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x*』を参照してください。

インターフェイス カウンタの表示とクリア

Cisco NX-OS を使用して、インターフェイス カウンタを表示し、クリアできます。ここで説明する内容は、次のとおりです。

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。

手順の概要

1. **configure terminal**
2. **load-interval counters** {{**1** | **2**| **3**} *seconds*}
3. **show interface**
4. **exit**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch#`
		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	**load-interval counters** {{**1** | **2** | **3**} *seconds*}
	
	例：
	`switch(config)# load-interval counters 1 100`
	`switch(config)#`
		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 インターフェイスでは 60 秒）
		2：300 秒
		3：設定なし

ステップ 3	**show interface** *interface*
	
	例：
	`switch(config)# show interface vlan 10`
	`switch#`
		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	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		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	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例では、イーサネット ポート 3/1 に 3 つのサンプル間隔を設定する方法を示します。

```
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 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。

手順の概要

1. **clear counters** *interface*
2. **show interface**

手順の詳細

	コマンド	目的

ステップ 1	**clear counters** *interface*
	
	例：
	`switch# clear counters ethernet 2/1`
	`switch#`
		インターフェイス カウンタをクリアします。

ステップ 2	`show interface interface`
	
	例：
	`switch# show interface vlan 10`
	`switch#`
		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。

次に、イーサネット ポート 5/5 のカウンタをクリアしてリセットする例を示します。

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

デフォルト設定

表 2-6 に、基本インターフェイス パラメータのデフォルト設定を示します。

表 2-6　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	100 ミリ秒
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 ステート イネーブル（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

表 2-6　基本インターフェイス パラメータのデフォルト設定 （続き）

パラメータ	デフォルト
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	2 秒または 50 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

その他の関連資料

機能 1 の実装に関連した情報については、次を参照してください。

- 「関連資料」（P.2-54）
- 「標準規格」（P.2-54）
- 「基本インターフェイス パラメータ設定の機能履歴」（P.2-55）

関連資料

関連項目	参照先
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x*』
レイヤ 2 スイッチング	『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*』
CDP	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference, Release 5.x*』

標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

基本インターフェイス パラメータ設定の機能履歴

表 2-7 は、この機能のリリースの履歴です。

表 2-7　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
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。
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。

CHAPTER 3

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 ポートをアクセス ポートまたはトランク ポートとして設定する手順について説明します。

（注） レイヤ 2 ポートは、トランク ポート、アクセス ポート、Private VLAN（PVLAN; プライベート VLAN）ポートとして機能できます。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, Release 5.x*』を参照してください。

この章では、次の内容について説明します。

（注） SPAN 宛先インターフェイスについては、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』を参照してください。

レイヤ 2 スイッチング ポートをアクセス ポートまたはトランク ポートとして設定できます。トランクは単一のリンクを介して複数の VLAN トラフィックを伝送します。これにより、ネットワーク全体に VLAN を拡張できます。すべてのレイヤ 2 スイッチング ポートは、Media Access Control（MAC; メディア アクセス制御）アドレス テーブルを維持します。

（注） VLAN、MAC アドレス テーブル、プライベート VLAN、Spanning Tree Protocol（STP; スパニング ツリー プロトコル）については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*』を参照してください。

（注）　レイヤ 2 ポートは、トランク ポート、アクセス ポート、プライベート VLAN ポートとして機能できます。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, Release 5.x*』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）　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, Release 5.x*』を参照してください。

ここでは、次の内容について説明します。

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

アクセス インターフェイスとトランク インターフェイスについて

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 ポートには 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。

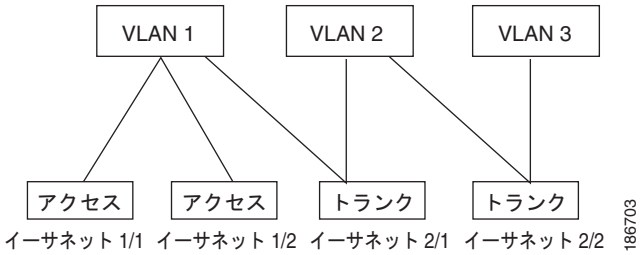
すべてのポートをレイヤ 2 ポートにするには、セットアップ スクリプトを使用するか、**system default switchport** コマンドを開始します。セットアップ スクリプトの使い方については、『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 5.x*』を参照してください。Command-Line Interface（CLI; コマンドライン インターフェイス）を使ってポートをレイヤ 2 ポートに設定するには、**switchport** コマンドを使用します。

1 つのトランクのすべてのポートは、同じ Virtual Device Context（VDC; 仮想デバイス コンテキスト）であることが必要です。VDC については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x*』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。

図 3-1 に、ネットワークでトランク ポートを使用する手順を示します。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 3-1　　トランクおよびアクセス ポートと VLAN トラフィック



（注） VLAN については『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*』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」（P.3-3）を参照してください）。

（注） レイヤ 3 インターフェイス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, Release 5.x*』を参照してください。

アクセス ポートのパフォーマンスを最適化するには、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 メッセージが表示されます。

アクセス ポートで受信するパケットのヘッダーにアクセス VLAN 値以外の 802.1Q タグがある場合、このポートは MAC 送信元アドレスを学習せずにパケットをドロップします。

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。

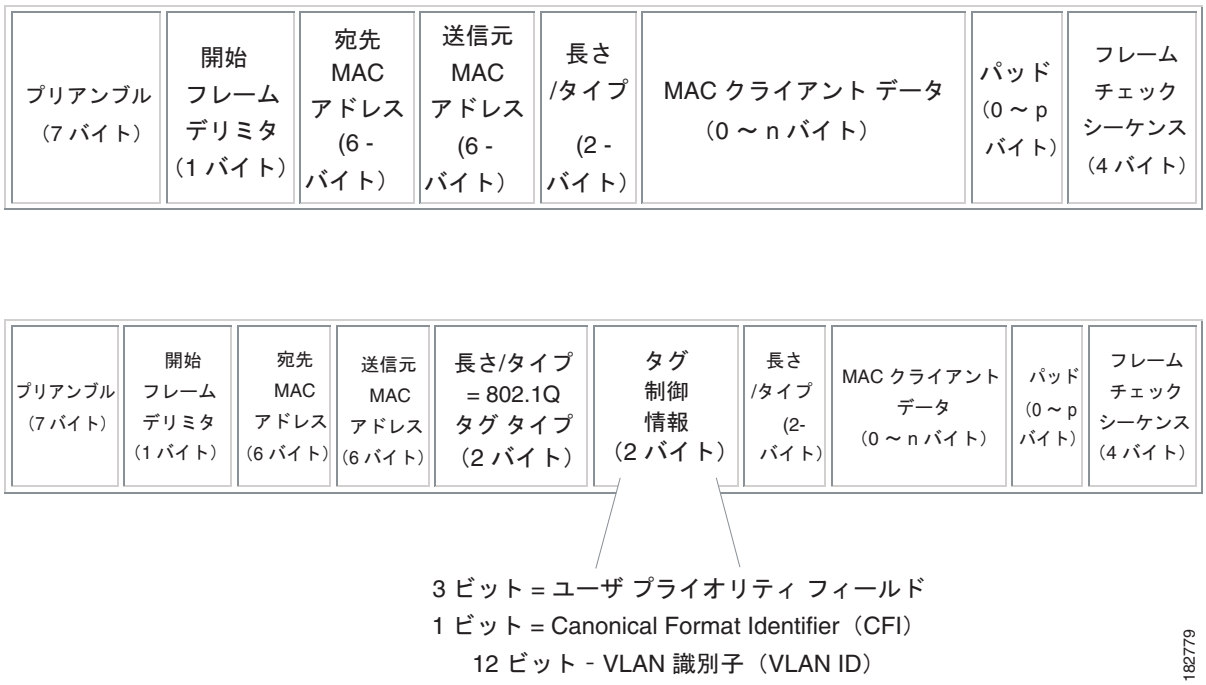
IEEE 802.1Q カプセル化

（注） VLAN の情報については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*』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 Point-To-Point（p2p; ポイントツーポイント）リンクです。トランクは単一のリンクを介して複数の VLAN トラフィックを伝送します。これにより、ネットワーク全体に VLAN を拡張できます。

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（図 3-2 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 間でトラフィック分離を維持できます。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 3-2　802.1Q 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 ポートも、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, Release 5.x*』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 モードのポート用またはアクセス 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）のトラフィックを伝送します。

VLAN のアクセス ポート メンバ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 値のほかに 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 MAC アドレスを学習せずに、そのパケットをドロップします。

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 は、トランク ポートのネイティブ VLAN ID と呼ばれます。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る*必要があります*。

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。

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。

許容 VLAN

デフォルトでは、トランク ポートは、すべての VLAN へのトラフィックを送信し、すべての VLAN からのトラフィックを受信します。各トランク上では、すべての VLAN ID が許可されます。ただし、この包括的なリストから VLAN を削除すれば、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 の収束時に問題が発生する可能性があります。VLAN1 を削除すると、そのポート上で VLAN1 のデータ トラフィックはすべてブロックされますが、制御トラフィックは通過し続けます。

（注）　パーティションの詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*』を参照してください。

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 アベイラビリティの詳細については、『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x*』を参照してください。

バーチャライゼーションのサポート

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, Release 5.x*』を参照してください。

レイヤ 2 ポート モードのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
NX-OS	レイヤ 2 ポート モードに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 のライセンス スキームの詳細については、『*Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x*』を参照してください。

（注）　VDC を使用する場合は Advanced Services ライセンスが必要です。

VLAN トランキングの前提条件

アクセスまたはトランク スイッチポート モードでポートを設定するには、次の前提条件が必要です。

- デバイスにログオンしていること。
- ポートをレイヤ 2 ポートとして設定した後で **switchport mode** コマンドを使用すること。デフォルトでは、デバイスのすべてのポートはレイヤ 3 ポートです。

注意事項および制約事項

次に示す設定時の注意事項および制約事項は、802.1Q トランクを使用するときに適用され、ネットワークのトランキングの構築方法が多少制限されます。802.1Q トランクを使用するときは、これらの制約事項に注意してください。

- 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製の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 と他端のネイティブ 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。
- ネットワーク上の各 VLAN のスパニング ツリーをディセーブルにせずに 802.1Q トランクのネイティブ VLAN 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 台のシスコ製のスイッチを接続すると、トランク上で許容される VLAN ごとにスパニング ツリー Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）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。トランク上の他の全 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の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 とシスコ製の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。
- シスコ製のスイッチは、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製のデバイスは、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、シスコ製のスイッチは、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。シスコ製の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。

- シスコ製の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製の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。シスコ製の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する場合、すべてのポートはグループに追加する最初のポートのパラメータ セットのとおりになります。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 をイネーブルにしたポートをトランク モードに変更しようとしても、ポートのモードは変更されません。

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

ここでは、次の内容について説明します。

（注）　Cisco IOS CLI を熟知している場合は、この機能の Cisco NX-OS コマンドと使用する Cisco IOS コマンドが異なる場合もある点に注意してください。

アクセスおよびトランク インターフェイスの設定に関する注意事項

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 LAN 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、タグなしの 1 つの VLAN だけのパケットを伝送します。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 VLAN1 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。

作業を開始する前に

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。

手順の概要

1. **configure terminal**
2. **interface** {{*type slot/port*} | {**port-channel** *number*}}
3. **switchport mode** {**access** | **trunk**}
4. **switchport access vlan** *vlan-id*
5. **exit**
6. **show interface**
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** {{*type slot/port*}	{**port-channel** *number*}}
		
		例：
		`switch(config)# interface ethernet 3/1`
		`switch(config-if)#`
			設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**switchport mode** {**access**	**trunk**} 例： `switch(config-if)# switchport mode access`	インターフェイスを、非トランキング、タグなし、シングル VLAN レイヤ 2 インターフェイスとして設定します。アクセス ポートは、1 つの VLAN のトラフィックだけを伝送できます。デフォルトでは、アクセス ポートは VLAN1 のトラフィックを伝送します。アクセス ポートが、異なる VLAN のトラフィックを伝送するように設定するには、**switchport access vlan** コマンドを使用します。

	コマンド	目的
ステップ 4	**switchport access vlan** *vlan-id* 例： `switch(config-if)# switchport access vlan 5`	このアクセス ポートでトラフィックを伝送する VLAN を指定します。このコマンドを入力しない場合、アクセス ポートは VLAN1 のトラフィックだけを伝送します。アクセス ポートがトラフィックを伝送する VLAN を*変更する場合*は、このコマンドを使用します。

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		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	**show interface** 例： `switch# show interface`	（任意）インターフェイスのステータスと内容を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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、端末に接続されたインターフェイスだけに適用する必要があります。

端末に接続したアクセス ポートのパフォーマンスを最適化するには、そのポートを同時にアクセス ポートとして指定します。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 インターフェイスの詳細については、第 6 章「ポート チャネルの設定」および『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*』を参照してください。スパニング ツリー プロトコルの詳細について。

作業を開始する前に

必ず、端末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してください。

手順の概要

1. **configure terminal**
2. **interface** *type slot/port*
3. **switchport host**
4. **exit**
5. **show interface**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

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

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

ステップ 5	**show interface** 例： `switch# show interface`	（任意）インターフェイスのステータスと内容を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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 のタグなしパケットと、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」（P.3-3）を参照してください）。

（注）　デバイスは 802.1Q カプセル化だけをサポートします。

作業を開始する前に

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。

手順の概要

1. **configure terminal**
2. **interface** {*type slot/port* | **port-channel** *number*}
3. **switchport mode** {**access** | **trunk**}
4. **exit**
5. **show interface**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface** {*type slot/port*	**port-channel** *number*} 例： switch(config)# interface ethernet 3/1 switch(config-if)#	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode** {**access**	**trunk**} 例： switch(config-if)# switchport mode 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	**exit** 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。

	コマンド	目的
ステップ 5	**show interface** 例： switch# show interface	（任意）インターフェイスのステータスと内容を表示します。
ステップ 6	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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場合、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。

手順の概要

1. **configure terminal**
2. **interface** {*type slot/port* | **port-channel** *number*}
3. **switchport trunk native vlan** *vlan-id*
4. **exit**
5. **show vlan**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface** {*type slot/port* | **port-channel** *number*} 例： switch(config)# interface ethernet 3/1 switch(config-if)#	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport trunk native vlan** *vlan-id* 例： switch(config-if)# switchport trunk native vlan 5	802.1Q トランクのネイティブ VLAN を設定します。有効範囲は 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 VLAN1 です。

	コマンド	目的

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

ステップ 5	**show vlan** 例： `switch# show vlan`	（任意）VLAN のステータスと内容を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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 VLAN 5 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 ポートで許可される VLAN の ID を指定できます。

作業を開始する前に

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

手順の概要

1. **configure terminal**
2. **interface** {**ethernet** *slot/port* | **port-channel** *number*}
3. **switchport trunk allowed vlan** {*vlan-list* | **add** *vlan-list* | **all** | **except** *vlan-list* | **none** | **remove** *vlan-list*}
4. **exit**
5. **show vlan**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** {**ethernet** *slot/port* | **port-channel** *number*} **例：** `switch(config)# interface ethernet 3/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport trunk allowed vlan** {*vlan-list* **add** *vlan-list* | **all** |**except** *vlan-list* | **none** | **remove** *vlan-list*} **例：** `switch(config-if)# switchport trunk allowed vlan add 15-20#`	トランク インターフェイスに許容 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）を許可します。VLAN 3968 ～ 4047 は、内部利用のためにデフォルトで予約されている VLAN です。この VLAN グループは設定可能です。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。 **（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 としては追加できません。内部で割り当てた VLAN を許容 VLAN として表示しようとすると、エラー メッセージが表示されます。

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

ステップ 5	**show vlan** **例：** `switch# show vlan`	（任意）VLAN のステータスと内容を表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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)#
```

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ン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）　あるデバイスの 802.1Q タギングでイネーブルにし、別のデバイスではディセーブルにすると、この機能をディセーブルにしたデバイスのトラフィックはすべてドロップされます。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。

作業を開始する前に

正しい VDC を開始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）。異なる VDC にも VLAN 名と ID を作成できるので、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。

手順の概要

1. **configure terminal**
2. **vlan dot1q tag native**
3. **exit**
4. **show vlan**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**vlan dot1q tag native** 例： `switch(config)# vlan dot1q tag native`	802.1Q トランクのネイティブ 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タグなしトラフィックを *ドロップ*するタグを使って開始す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。デフォルトはディセーブルです。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 4	**show vlan** 例： switch# show vlan	（任意）VLAN のステータスと内容を表示します。
ステップ 5	**copy running-config startup-config** 例： switch# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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、すべてのタグなし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#
```

デフォルト ポート モードのレイヤ 2 への変更

デフォルト ポート モードをレイヤ 2 アクセス ポートに設定できます。

手順の概要

1. **configure terminal**
2. **system default switchport** [**shutdown**]
3. **exit**
4. **show interface brief**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**system default switchport** [**shutdown**] 例： switch(config-if)# switchport trunk allowed vlan add 15-20#	システムのすべてのインターフェイスのデフォルト 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。
ステップ 3	**exit** 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。

	コマンド	目的
ステップ 4	**show interface brief** **例：** `switch# show interface brief`	（任意）インターフェイスのステータスと内容を表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、システム ポートをデフォルトでレイヤ 2 アクセス ポートに設定する例を示します。

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

インターフェイス設定の確認

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、次の作業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。
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性能に関する情報を表示します。
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。

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, Release 5.x*』を参照してください。

統計情報の表示とクリア

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、次の作業のいずれかを行います。

コマンド	目的
clear counters [*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。
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, Release 5.x*』を参照してください。

デフォルト設定

表 3-1 に、デバイスのアクセスおよびトランク ポート モード パラメータのデフォルト設定を示します。

表 3-1　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
許容 VLAN	1 ～ 3967、4048 ～ 4094
アクセス VLAN ID	VLAN1
ネイティブ VLAN ID	VLAN1
ネイティブ VLAN ID タギング	ディセーブル
管理ステート	Shut

アクセスおよびトランク ポート モードの設定例

次に、レイヤ 2 アクセス インターフェイスを設定し、このインターフェイスにアクセス VLAN 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)#
```

その他の関連資料

アクセスおよびトランク ポート モードの実装に関する追加情報については、次の項を参照してください。

- 「関連資料」（P.3-21）
- 「標準規格」（P.3-21）
- 「管理情報ベース（MIB）」（P.3-22）

関連資料

関連項目	参照先
レイヤ 3 インターフェイスの設定	第 4 章「レイヤ 3 インターフェイスの設定」
ポート チャネル	第 6 章「ポート チャネルの設定」
VLAN、プライベート VLAN、STP	『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x*』
インターフェイス	『*Cisco DCNM Interfaces Configuration Guide, Release 5.x*』
システム管理	『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』
ハイ アベイラビリティ	『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x*』
仮想デバイス コンテキスト（VDC）	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x*』
ライセンス	『*Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x*』
リリース ノート	『*Cisco Nexus 7000 Series NX-OS Release Notes, Release 5.x*』

標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

管理情報ベース（MIB）

管理情報ベース（MIB）	MIB リンク
• BRIDGE-MIB • IF-MIB • CISCO-IF-EXTENSION-MIB • ETHERLIKE-MIB	Management Information Base（MIB; 管理情報ベース）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

レイヤ 2 インターフェイス設定の機能履歴

表 3-2 は、この機能のリリースの履歴です。

表 3-2　レイヤ 2 インターフェイス設定の機能履歴

機能名	リリース	機能情報
レイヤ 2 インターフェイス	4.0(1)	この機能が導入されました。
インターフェイス統計情報に設定可能な 3 種類のサンプリング間隔	4.2(1)	**load-interval** コマンドが追加されました。

CHAPTER 4

レイヤ 3 インターフェイスの設定

この章では、Cisco Nexus 7000 シリーズ デバイスのレイヤ 3 インターフェイスを設定する手順について説明します。

この章では、次の内容について説明します。

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。

ここでは、次の内容について説明します。

ルーテッド インターフェイス

ポートをレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスとして設定できます。ルーテッド インターフェイスは、IP トラフィックを他のデバイスにルーティングできる物理ポートです。ルーテッド インターフェイスはレイヤ 3 インターフェイスだけで、Spanning Tree Protocol（STP; スパニング ツリー プロトコル）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、Command-Line Interface（CLI; コマンドライン インターフェイス）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、レイヤ 3 インターフェイスの MAC アドレスは、レイヤ 3 インターフェイスが割り当てられた Virtual Device Context（VDC; 仮想デバイス コンテキスト）の MAC アドレスです。MAC パラメータの設定手順については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*』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、第 6 章「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。

- 毎秒入力パケット数
- 毎秒出力パケット数
- 毎秒入力バイト数
- 毎秒出力バイト数

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。

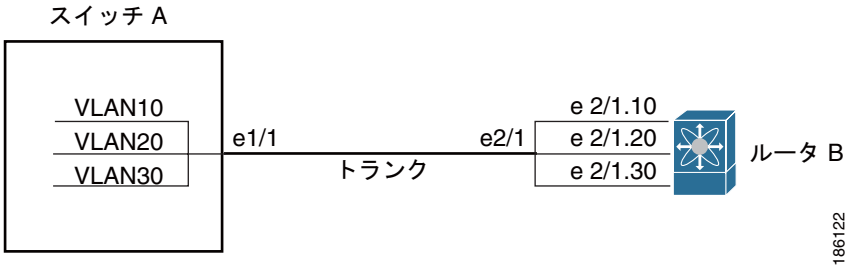
サブインターフェイスの名前は、親インターフェイスの名前（たとえば Ethernet 2/1）+ ピリオド（.）+ そのインターフェイス独自の番号です。たとえば、イーサネット インターフェイス 2/1 に Ethernet 2/1.1 というサブインターフェイスを作成できます。この場合、.1 はそのサブインターフェイスを表します。

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 Virtual Local Area Network（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。

図 4-1 に、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キング ポートを示します。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 4-1　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, Release 5.x*』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 Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）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。1 つの VLAN には 1 つの VLAN インターフェイスだけを関連付けできます。ただし、VLAN 同士をルーティングする場合や管理 Virtual Routing and Forwarding（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、VLAN に VLAN インターフェイスを設定する必要があります。VLAN インターフェイスの作成をイネーブルにすると、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 Release 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。コールバックとチェックポイントについては、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』を参照してください。

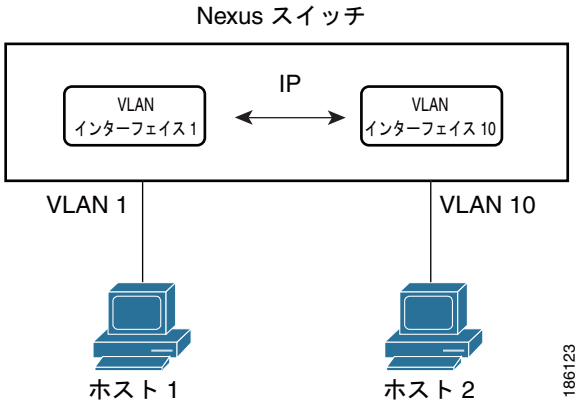
VLAN インターフェイスを VLAN と同じ VDC に設定する必要があります。

（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 アドレスと 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, Release 5.x*』を参照してください。

図 4-2 に、2 つの VLAN に 2 つのホストが接続しているデバイスを示します。VLAN ごとに VLAN インターフェイスを設定し、VLAN 間の IP ルーティングを使ってホスト 1 とホスト 2 を通信させることができます。VLAN 1 は VLAN インターフェイス 1 のレイヤ 3 で、VLAN 10 は VLAN インターフェイス 10 のレイヤ 3 で通信します。

図 4-2　VLAN インターフェイスに接続した 2 つの VLAN



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レイヤ 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、第 8 章「IP トンネルの設定」を参照してください。

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, Release 5.x*』を参照してください。

バーチャライゼーションのサポート

レイヤ 3 インターフェイスは、Virtual Routing and Forwarding（VRF; 仮想ルーティング/転送）インスタンスをサポートします。VRF は Virtual Device Context（VDC; 仮想デバイス コンテキスト）内に存在します。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, Release 5.x*』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, Release 5.x*』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。

レイヤ 3 インターフェイスのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	レイヤ 3 インターフェイスに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。Cisco NX-OS のライセンス スキームの詳細については、『*Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x*』を参照してください。

ライセンス 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。

- Advanced Services ライセンスをインストールしており、該当する VDC を開始している（VDC を設定する場合は、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x*』を参照してください）。
- IP アドレッシングおよび基本設定を熟知している。IP アドレッシングの詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。

注意事項および制約事項

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。

（注）　Cisco IOS CLI を熟知している場合は、この機能の Cisco NX-OS コマンドと使用する Cisco IOS コマンドが異なる場合もある点に注意してください。

レイヤ 3 インターフェイスの設定

ここでは、次の内容について説明します。

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。

作業を開始する前に

正しい VDC を開始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）。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **no switchport**
4. **ip address** *ip-address/length*
   または
   ipv6 address *ipv6-address/length*
5. **show interfaces**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet** *slot/port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**no switchport** 例： `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	**ip address** *ip-address/length* 例： `switch(config-if)# ip address 192.0.2.1/8`	このインターフェイスに IP アドレスを設定します。IP アドレッシングの詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。
	ipv6 address *ipv6-address/length* 例： `switch(config-if)# ipv6 address 2001:0DB8::1/8`	このインターフェイスに IPv6 アドレスを設定します。IPv6 アドレッシングの詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。
ステップ 5	**show interfaces** 例： `switch(config-if)# show interfaces ethernet 2/1`	（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	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）この設定の変更を保存します。

インターフェイス メディアを Point-To-Point（p2p; ポイントツーポイント）またはブロードキャストに設定するには、**medium** コマンドを使用します。

コマンド	目的
medium {**broadcast** | **p2p**} 例： `switch(config-if)# medium 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に設定します。

（注）　デフォルトの設定は、**medium** であり、この設定はどの **show** コマンドでも表示されません。しかし、**p2p** に設定を変更した場合は、**show running config** コマンドを入力したときにこの設定を表示できます。

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 **例：** `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、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はルーテッドです。レイヤ 2 のインターフェイスを設定する場合は、**switchport** コマンドを入力します。次に、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。

作業を開始する前に

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」（P.4-6）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 を開始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）。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot/port.number*
3. **ip address** *ip-address/length*
   または
   ipv6 address *ipv6-address/length*
4. **encapsulation dot1q** *van-id*
5. **show interfaces**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface ethernet** *slot/port.number* 例： switch(config)# interface ethernet 2/1.1 switch(config-subif)#	サブインターフェイスを作成し、サブインターフェイス コンフィギュレーション モードを開始します。*number* の範囲は 1 ～ 4094 です。
ステップ 3	**ip address** *ip-address/length* 例： switch(config-subif)# ip address 192.0.2.1/8	このサブインターフェイスに IP アドレスを設定します。IP アドレッシングの詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。
	ipv6 address *ipv6-address/length* 例： switch(config-subif)# ipv6 address 2001:0DB8::1/8	このサブインターフェイスに IPv6 アドレスを設定します。IPv6 アドレッシングの詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。
ステップ 4	**encapsulation dot1Q** *vlan-id* 例： switch(config-subif)# encapsulation dot1Q 33	（任意）サブインターフェイスに IEEE 802.1Q VLAN カプセル化を設定します。有効値の範囲は 2 ～ 4093 です。
ステップ 5	**show interfaces** 例： switch(config-subif)# show interfaces ethernet 2/1.1	（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	**copy running-config startup-config** 例： switch(config-subif)# copy running-config startup-config	（任意）この設定の変更を保存します。

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
```

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。上位レイヤ 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
bandwidth **例：** `switch(config-if)# bandwidth 100000`	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。

サブインターフェイスを設定して親インターフェイスの帯域幅を継承させるには、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*] **例：** `switch(config-if)# bandwidth inherit 100000`	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が設定した帯域幅を継承するように設定します。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。有効値の範囲は 1 ～ 10,000,000 キロバイトです。

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。

作業を開始する前に

正しい VDC を開始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）。

手順の概要

1. **configure terminal**
2. **feature interface-vlan**
3. **interface vlan** *number*

4. **ip address** *ip-address/length*
   または
   ipv6 address *ipv6-address/length*
5. **show interface vlan** *number*
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**feature interface-vlan** 例： **switch(config)# feature interface-vlan**	ループバック インターフェイスを作成します。有効な範囲は 0 ～ 1023 です。

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

ステップ 4	**ip address** *ip-address/length* 例： `switch(config-if)# ip address 192.0.2.1/8`	この VLAN インターフェイスに IP アドレスを設定します。IP アドレッシングの詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。
	ipv6 address *ipv6-address/length* 例： `switch(config-if)# ipv6 address 2001:0DB8::1/8`	この VLAN インターフェイスに IPv6 アドレスを設定します。IPv6 アドレッシングの詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。
ステップ 5	**show interface vlan** *number* 例： `switch(config-if)# show interface vlan 10`	（任意）レイヤ 3 インターフェイスの統計情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

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
```

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。

作業を開始する前に

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 を開始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）。

手順の概要

1. **configure terminal**
2. **interface loopback** *instance*
3. **ipv4 address** *ip-address*
   または
   ipv6 address
4. **show interfaces loopback** *instance*
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

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

ステップ 3	**ip address** *ip-address/length* 例： `switch(config-if)# ip address 192.0.2.100/8`	このインターフェイスに IP アドレスを設定します。IP アドレッシングの詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。
	ipv6 address *ipv6-address/length* 例： `switch(config-if)# ipv6 address 2001:0DB8::18/8`	このインターフェイスに IPv6 アドレスを設定します。IPv6 アドレッシングの詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。
ステップ 4	**show interfaces loopback** *instance* 例： `switch(config-if)# show interfaces loopback 0`	（任意）ループバック インターフェイスの統計情報を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

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
```

インターフェイスの VRF への割り当て

VRF にレイヤ 3 インターフェイスを追加できます。

作業を開始する前に

正しい VDC を開始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 にインターフェイスを設定してから、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。

手順の概要

1. **configure terminal**
2. **interface** *interface-type number*
3. **vrf member** *vrf-name*
4. **ip-address** *ip-prefix/length*
5. **show vrf** [*vrf-name*] **interface** *interface-type number*
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *interface-type number*
	
	例：
	`switch(config)# interface loopback 0`
	`switch(config-if)#`
		インターフェイス 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	**vrf member** *vrf-name* 例： `switch(config-if)# vrf member RemoteOfficeVRF`	このインターフェイスを VRF に追加します。
ステップ 4	**ip address** *ip-prefix/length* 例： `switch(config-if)# ip address 192.0.2.1/16`	このインターフェイスに 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 に割り当ててから実行します。

	コマンド	目的
ステップ 5	**show vrf** [*vrf-name*] **interface** *interface-type number* **例：** `switch(config-vrf)# show vrf Enterprise interface loopback 0`	（任意）VRF の内容を表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）この設定の変更を保存します。

次に、レイヤ 3 インターフェイスを VRF に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 インターフェイスの設定の確認

レイヤ 3 設定情報を確認するには、次のコマンドを使用します。

コマンド	目的
show interface ethernet *slot/port*	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状態を表示します。
show interface ethernet *slot/port* **capabilities**	レイヤ 3 インターフェイスの能力（ポート タイプ、速度、デュプレックス）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、デュプレックスを表示します。
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。

コマンド	目的
show interface loopback *number* **brief**	ループバック インターフェイスの動作状態を表示します。
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状態を表示します。
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 プライベート VLAN の情報を表示します。
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。

レイヤ 3 インターフェイス統計情報の表示

レイヤ 3 統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
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 インターフェイスの範囲は、60 ～ 300 秒であり、レイヤ インターフェイスの範囲は 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 ビットおよび 64 ビットのパケットおよびバイト カウンタを、エラーを含めて追加できます。
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**	Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）Management Information Base（MIB; 管理情報ベース）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。このカウンタはクリアできません。
show interface ethernet *slot/port.number* **counters**	サブ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)。

コマンド	目的
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 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 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 ビットおよび 64 ビットのパケットおよびバイト カウンタを、エラーを含めて追加できます。
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 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。このカウンタはクリアできません。

これらのコマンドについては、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x*』を参照してください。

レイヤ 3 インターフェイスの設定例

次に、イーサネット サブインターフェイスを設定する例を示します。

```
interface ethernet 2/1.10
       description Layer 3 for VLAN 10
       encapsulation dot1q 10
       ip address 192.0.2.1/8
```

次に、VLAN インターフェイスを設定する例を示します。

```
interface vlan 100
 ipv6 address 33:0DB::2/8
```

次に、ループバック インターフェイスを設定する例を示します。

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

関連項目

レイヤ 3 インターフェイスの詳細については、次の項目を参照してください。

- 第 6 章「ポート チャネルの設定」
- 『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』

デフォルト設定

表 4-1 に、レイヤ 3 インターフェイス パラメータのデフォルト設定を示します。

表 4-1　デフォルトのレイヤ 3 インターフェイス パラメータ

パラメータ	デフォルト
管理ステート	Shut

その他の関連資料

レイヤ 3 インターフェイスの実装に関する追加情報については、次の項を参照してください。

- 「関連資料」（P.4-18）
- 「管理情報ベース（MIB）」（P.4-18）
- 「標準規格」（P.4-18）

関連資料

関連項目	参照先
コマンド構文	『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x*』
IP	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』の「Configuring IP」の章
VLAN	『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*』の「Configuring VLANs」の章

管理情報ベース（MIB）

管理情報ベース（MIB）	MIB リンク
• IF-MIB • CISCO-IF-EXTENSION-MIB • ETHERLIKE-MIB	Management Information Base（MIB; 管理情報ベース）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

標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

レイヤ 3 インターフェイス設定の機能履歴

表 4-2 は、この機能のリリースの履歴です。

表 4-2　レイヤ 3 インターフェイス設定の機能履歴

機能名	リリース	機能情報
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。
インターフェイス統計情報に設定可能な 3 種類のサンプリング間隔	4.2(1)	**load-interval** コマンドが追加されました。

CHAPTER 5

双方向フォワーディング検出（BFD）の設定

この章では、Cisco NX-OS デバイスで Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）を設定する方法について説明します。

この章では、次の内容について説明します。

BFD について

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 によって、ネットワーク プロファイリングおよびプランニングが容易になり、再収束時間の整合性が保たれ、予測可能になります。

BFD は、2 個の隣接するデバイス間のサブセカンド障害検出を行います。さらに、BFD の負荷の一部をサポート モジュールのデータ プレーンに分散できるため、プロトコル Hello メッセージに比べて CPU への集中を緩和できます。

ここでは、次の内容について説明します。

- 「セキュリティ」（P.5-4）
- 「ハイ アベイラビリティ」（P.5-4）
- 「バーチャライゼーションのサポート」（P.5-4）

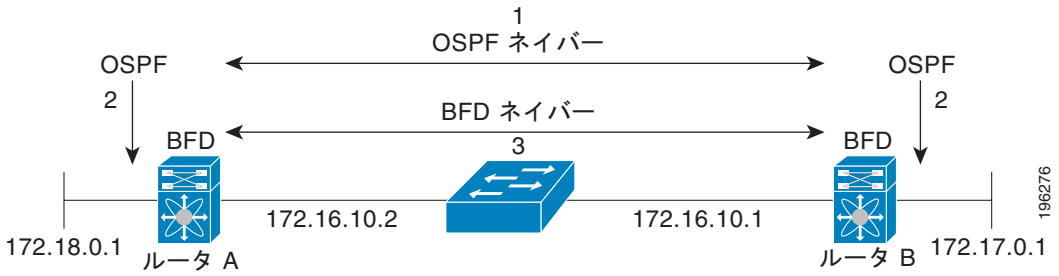
非同期モード

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（つまり BFD ネイバー）に BFD を設定します。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 パラメータには次の項目が含まれます。

- 指定最小転送間隔：デバイスが予期する BFD Hello メッセージの送信間隔。
- 必要最小受信間隔:デバイスが別の BFD デバイスから BFD Hello メッセージを受信できる最少間隔。
- 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。

図 5-1 に BFD セッション確立方法を示します。図では、OSPF と BFD を実行する 2 個のルータがある単純なネットワークを示しています。OSPF がネイバーを検出したとき（1）、ローカル BFD プロセスに要求を送信して、OSPF ネイバー ルータと BFD ネイバー セッションを開始します（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 5-1　　BFD ネイバー関係の確立



BFD 障害検出

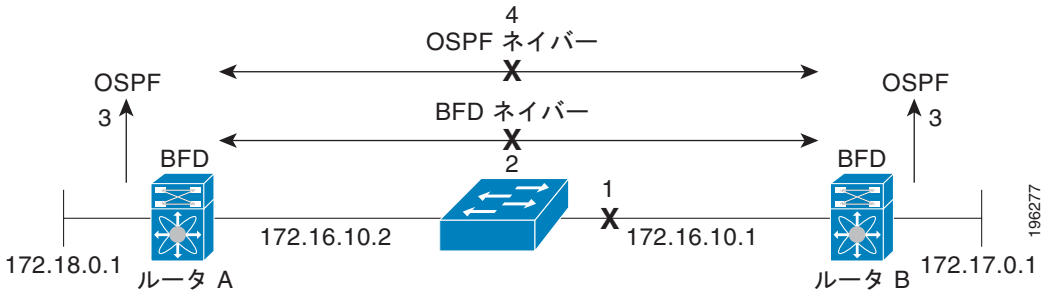
一度 BFD セッションが確立され、タイマー ネゴシエーションが終了すると、BFD ネイバーは、より速い速度の場合を除き IGP Hello プロトコルと同じ動作をする BFD 制御パケットを送信し、活性度を検出します。BFD は障害を検出しますが、プロトコルが障害の発生したピアをバイパスするための処置を行う必要があります。

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。

図 5-2 は、ネットワークで障害が発生したとき（1）に何が起こるかを示しています。OSPF ネイバー ルータとの BFD ネイバー セッションが終了されます（2）。BFD はローカル OSPF プロセスに BFD ネイバーが到達可能では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 ネイバー関係を終了します（4）。代替パスが利用できる場合は、ルータはすぐにコンバージェンスを開始します。

（注）　BFD 障害検出は、サブセカンド タイムで発生し、同じ障害を OSPF Hello メッセージよりも高速で検出できます。

図 5-2　　OSPF ネイバー関係の終了



分散モード

Cisco NX-OS は、BFD 動作を互換モジュールに分散できます。このプロセスは、BFD パケット処理の CPU 負荷を BFD ネイバーに接続された各モジュールに移します。すべての BFD セッション トラフィックはモジュール CPU で発生します。BFD 障害が検出されたとき、モジュールはスーパーバイザに通知します。

BFD 分散モードは、次の Cisco Nexus 7000 シリーズ モジュールでサポートされます。

- Cisco Nexus 7000 シリーズ 48 ポート 10/100/1000 イーサネット モジュール（N7K-M148GT-11）
- Cisco Nexus 7000 シリーズ 32 ポート 10 ギガビット イーサネット モジュール、80Gbps ファブリック（N7K-M132XP-12）
- Cisco Nexus 7000 シリーズ 8 ポート 10 ギガビット イーサネット モジュール、80Gbps ファブリック

（注）　その他のすべてのモジュールは、スーパーバイザか、または別のサポート モジュールを使用して、BFD パケット処理を行います。

BFD エコー モード

BFD エコー モードは、エコー パケットを転送エンジンからリモート BFD ネイバーに送信します。BFD ネイバーは、検出を行う目的でエコー パケットを同じパスを通じて送り返します。BFD ネイバーは実際のエコー パケットの転送には関与しません。エコー機能および転送エンジンは、検出プロセスに責任を持ちます。BFD は、スロー タイマーを使用することで、2 個の BFD ネイバー間で送信される BFD 制御パケットの数を削減できます。また、転送エンジンはリモート システムに影響を与えることなく、リモート（ネイバー）システム上の転送パスをテストします。このため、インターパケット遅延の変動は小さくなり、障害検出は高速になります。

エコー モードは、両方の BFD ネイバーがエコー モードを実行する場合、非対照ではありません。

セキュリティ

Cisco NX-OS は、パケット Time to Live（TTL; 存続可能時間）値を使用して、BFD パケットが隣接する BFD ピアから送信されたことを確認します。すべての非同期要求パケットおよびエコー要求パケットに対して、BFD ネイバーは TTL 値を 255 に設定し、ローカル BFD プロセスは受信パケットの処理の前に TTL 値が 255 であることを確認します。エコー応答パケットの場合、BFD は TTL 値を 254 に設定します。

ハイ アベイラビリティ

BFD は、ステートレスな再起動、および In-Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）をサポートします。ISSU では、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 スイッチオーバーの後に、Cisco DC-OS は実行コンフィギュレーションを適用し、BFD はすぐに制御パケットを BFD ピアに送信します。

バーチャライゼーションのサポート

BFD は Virtual Routing and Forwarding（VRF; 仮想ルーティング / 転送）インスタンスをサポートします。VRF は仮想デバイス コンテキスト（VDC）内に存在します。VDC や VRF を特別に設定しない限り、デフォルトでは、Cisco DC-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, Release 5.x*』を参照してください。

BFD のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	BFD に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。Cisco NX-OS のライセンス スキームの詳細については、『*Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x*』を参照してください。

BFD の前提条件

BFD を使用するには、次の前提条件を満たしている必要があります。

- BFD 機能をイネーブルにする必要があります（「BFD 機能のイネーブル化」（P.5-6）を参照）。
- BFD をイネーブルにする必要のあるすべてのクライアント プロトコルに対して、BFD をイネーブルにします。「ルーティング プロトコルの BFD サポートの設定」（P.5-13）を参照してください。
- BFD 対応インターフェイスで Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）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 の同一の IP 送信元アドレスと IP 宛先アドレスのパケット検証チェックをディセーブルにします。
- 詳細な前提条件については、設定タスクを参照してください。

注意事項および制約事項

BFD には、次の注意事項と制約事項があります。

- BFD バージョン 1 をサポートしています。
- IPv4 をサポートしています。
- シングルホップ BFD をサポートしています。
- Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）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。
- レイヤ 3 インターフェイスである、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 インターフェイスをサポートします。
- BFD は、レイヤ 3 隣接情報によって、レイヤ 2 トポロジ変化を含むトポロジ変化を検出しています。レイヤ 3 隣接情報が利用できない場合、VLAN インターフェイス（Switched Virtual Interface（SVI; スイッチ仮想インターフェイス））上の BFD セッションは、レイヤ 2 トポロジの収束後にアップになりません。

デフォルト設定

表 5-1 は、各 BFD パラメータに対するデフォルト設定を示します。

表 5-1　デフォルト 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
指定最小転送間隔	50 ミリ秒
検出乗数	3
エコー モード	イネーブル
モード	非同期
ポート チャネル	論理モード（発信元 - 宛先ペア アドレスごとに 1 セッション）
スロー タイマー	2000 ミリ秒
サブインターフェイス最適化	ディセーブル

BFD の設定

ここでは、次の内容について説明します。

- 「ポート チャネル上での BFD の設定」（P.5-9）
- 「BFD エコー モードの設定」（P.5-11）
- 「サブインターフェイス上での BFD の最適化」（P.5-12）
- 「ルーティング プロトコルの BFD サポートの設定」（P.5-13）

階層の設定

グローバル レベル、VRF レベル、インターフェイス レベル、ポート チャネル レベル、またはサブインターフェイス レベル（物理インターフェイスおよびポート チャネルの場合）で BFD を設定できます。VRF コンフィギュレーションは、グローバル コンフィギュレーションより優先されます。インターフェイス コンフィギュレーションまたはポート チャネル コンフィギュレーションは、VRF コンフィギュレーションまたはグローバル コンフィギュレーションより優先されます。サポートされるインターフェイスでは、サブインターフェイス最適化がイネーブルにされない限り、サブインターフェイス レベル コンフィギュレーションは、インターフェイス コンフィギュレーションまたはポート チャネル コンフィギュレーションより優先されます。詳細については、「サブインターフェイス上での BFD の最適化」（P.5-12）を参照してください。

ポート チャネルのメンバである物理ポートの場合、メンバ ポートはマスター ポート チャネルの BFD コンフィギュレーションを継承します。サブインターフェイス最適化がイネーブルにされない限り、メンバ ポート サブインターフェイスは、マスター ポート チャネルの BFD コンフィギュレーションより優先されます。

BFD 設定のタスク フロー

BFD を設定するには、次の作業を行います。

ステップ 1　「BFD 機能のイネーブル化」。

ステップ 2　「グローバル BFD パラメータの設定」または「インターフェイス上での BFD の設定」。

ステップ 3　「ルーティング プロトコルの BFD サポートの設定」。

BFD 機能のイネーブル化

デバイス（VDC）のインターフェイスまたはプロコル上で 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。

作業を開始する前に

正しい VDC を開始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）。

手順の概要

1. **configure terminal**
2. **feature bfd**
3. **show feature | include bfd**

4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**feature bfd** 例： `switch(config)# feature bfd`	BFD 機能をイネーブルにします。
ステップ 3	**show feature | include bfd** 例： `switch(config)# show feature | include bfd`	（任意）イネーブルにされた機能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	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）この設定の変更を保存します。

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 例： `switch(config)# no feature bfd`	BFD 機能をディセーブルにして、関連するコンフィギュレーションをすべて削除します。

グローバル 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、BFD ピア間においてスリーウェイ ハンドシェイクでネゴシエートされます。

これらのインターフェイス上のグローバル セッション パラメータを無効にするには、「インターフェイス上での BFD の設定」（P.5-8）を参照してください。

作業を開始する前に

正しい VDC を開始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 機能のイネーブル化」（P.5-6）を参照してください。

手順の概要

1. **configure terminal**
2. **bfd interval** *mintx* **min_rx** *msec* **multiplier** *value*

3. **bfd slow-timer** [*interval*]
4. **show running-config bfd**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**bfd interval** *mintx* **min_rx** *msec* **multiplier** *value* 例： switch(config)# bfd interval 50 min_rx 50 multiplier 3	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と、これらの値より優先されます。*mintx* および *msec* の範囲は 50 ～ 999 ミリ秒で、デフォルトは 50 です。乗数（multiplier）の範囲は 1 ～ 50 です。乗数のデフォルトは 3 です。
ステップ 3	**bfd slow-timer** [*interval*] 例： switch(config)# bfd slow-timer 2000.	スロー タイマーを設定します。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	**show running-config bfd** 例： switch(config)# show running-config bfd	（任意）BFD 実行コンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

インターフェイス上での 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、BFD ピア間においてスリーウェイ ハンドシェイク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。

作業を開始する前に

正しい VDC を開始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 機能のイネーブル化」（P.5-6）を参照してください。

手順の概要

1. **configure terminal**
2. **interface** *int-if*
3. **bfd interval** *mintx* **min_rx** *msec* **multiplier** *value*

4. **show running-config bfd**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *int-if*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`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	**bfd interval** *mintx* **min_rx** *msec* **multiplier** *value* 例： `switch(config-if)# bfd interval 50 min_rx 50 multiplier 3`	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 パラメータを設定します。これは、グローバル BFD セッション パラメータより優先されます。*mintx* および *msec* の範囲は 50 ～ 999 ミリ秒で、デフォルトは 50 です。乗数（multiplier）の範囲は 1 ～ 50 です。乗数のデフォルトは 3 です。
ステップ 4	**show running-config bfd** 例： `switch(config-if)# show running-config bfd`	（任意）BFD 実行コンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

ポート チャネル上での 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。ポート チャネルの各リンクに対して BFD はセッションを作成し、集約結果をクライアント プロトコルに提供します。たとえば、ポート チャネル上のあるリンクの BFD セッションがアップであるとき、BFD は OSPF などのクライアント プロトコルにポート チャネルがアップであることを通知します。BFD セッション パラメータは、BFD ピア間においてスリーウェイ ハンドシェイク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、サブインターフェイス レベル BFD パラメータをメンバ ポート上で設定しない限り、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上での BFD の最適化」（P.5-12）を参照してください。

作業を開始する前に

正しい VDC を開始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 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。

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」（P.5-6）を参照してください。

手順の概要

1. **configure terminal**
2. **interface port-channel** *number*
3. **bfd per-link**
4. （任意）**bfd interval** *mintx* **min_rx** *msec* **multiplier** *value*
5. **show running-config bfd**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface port-channel** *number*
	
	例：
	`switch(config)# interface port-channel 2`
	`switch(config-if)#`
		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、サポートされる数字の範囲を表示します。

ステップ 3	**bfd per-link** 例： `switch(config-if)# bfd per-link`	ポート チャネルの各リンクに BFD セッションを設定します。
ステップ 4	**bfd interval** *mintx* **min_rx** *msec* **multiplier** *value* 例： `switch(config-if)# bfd interval 50 min_rx 50 multiplier 3`	（任意）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 パラメータを設定します。これは、グローバル BFD セッション パラメータより優先されます。*mintx* および *msec* の範囲は 50 ～ 999 ミリ秒で、デフォルトは 50 です。乗数（multiplier）の範囲は 1 ～ 50 です。乗数のデフォルトは 3 です。
ステップ 5	**show running-config bfd** 例： `switch(config-if)# show running-config bfd`	（任意）BFD 実行コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

BFD エコー モードの設定

BFD モニタ対象リンクの一方または両方の端に BFD エコー モードを設定できます。エコー モードは設定されたスロー タイマーに基づいて必要最小受信間隔をスロー ダウンします。エコー モードがディセーブルにされている場合、RequiredMinEchoRx BFD セッション パラメータはゼロに設定されます。エコー モードがイネーブルにされている場合、スロー タイマーが必要最小受信間隔になります。

作業を開始する前に

正しい VDC を開始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 機能のイネーブル化」（P.5-6）を参照してください。

BFD セッション パラメータを設定します。「グローバル BFD パラメータの設定」（P.5-7）または「インターフェイス上での BFD の設定」（P.5-8）を参照してください。

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 メッセージがディセーブルにされていることを確認します。インターフェイス上で **no ip redirects** コマンドを使用します。

同一の IP 送信元アドレスと IP 宛先アドレスのパケット検証チェックがディセーブルにされていることを確認します。デフォルト VDC で **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, Release 5.x*』を参照してください。

手順の概要

1. **configure terminal**
2. **bfd slow-timer** *echo-interval*
3. **interface** *int-if*
4. **bfd echo**
5. **show running-config bfd**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**bfd slow-timer** *echo-interval* 例： `switch(config)# bfd slow-timer 2000`	エコー モードで使用されるスロー タイマーを設定します。エコー モードがイネーブルにされているとき、この値は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	**interface** *int-if*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`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。

	コマンド	目的
ステップ 4	**bfd echo** 例： `switch(config-if)# bfd echo`	BFD エコー モードをイネーブルにします。デフォルトはイネーブルです。
ステップ 5	**show running-config bfd** 例： `switch(config-if)# show running-config bfd`	（任意）BFD 実行コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

サブインターフェイス上での BFD の最適化

サブインターフェイス上で最適化できます。BFD は、設定されたすべてのサブインターフェイスに対してセッションを作成します。BFD は、最小の VLAN ID が設定されたサブインターフェイスをマスター サブインターフェイスとして設定し、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。その他のサブインターフェイスはスロー タイマーを使用します。最適化されたサブインターフェイス セッションがエラーを検出した場合、BFD は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をダウンとしてマークします。

作業を開始する前に

正しい VDC を開始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 機能のイネーブル化」（P.5-6）を参照してください。

BFD セッション パラメータを設定します。「グローバル BFD パラメータの設定」（P.5-7）または「インターフェイス上での BFD の設定」（P.5-8）を参照してください。

これらのサブインターフェイスが別の Cisco NX-OS デバイスに接続されていることを確認します。この機能は Cisco NX-OS だけでサポートされています。

手順の概要

1. **configure terminal**
2. **interface** *int-if*
3. **bfd optimize subinterface**
4. **show running-config bfd**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *int-if*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`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	**bfd optimize subinterface** **例：** `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。デフォルトはディセーブルです。
ステップ 4	**show running-config bfd** **例：** `switch(config-if)# show running-config bfd`	（任意）BFD 実行コンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

ルーティング プロトコルの BFD サポートの設定

ここでは、次の内容について説明します。

BGP 上での BFD の設定

ボーダー ゲートウェイ プロトコル（BGP）の BFD を設定できます。

作業を開始する前に

正しい VDC を開始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 機能のイネーブル化」（P.5-6）を参照してください。

BFD セッション パラメータを設定します。「グローバル BFD パラメータの設定」（P.5-7）または「インターフェイス上での BFD の設定」（P.5-8）を参照してください。

BGP 機能をイネーブルにします。詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。

手順の概要

1. **configure terminal**
2. **router bgp** *as-number*
3. **neighbor** {*ip-address* | *ipv6-address*} **remote-as** *as-number*
4. **bfd**
5. **show running-config bgp**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**router bgp** *as-number*
	
	例：
	`switch(config)# router bgp 64496`
	`switch(config-router)#`
		BGP をイネーブルにし、AS 番号をローカル BGP スピーカーに割り当てます。AS 番号は、16 ビット整数または 32 ビット整数（xx.xx の形式で、上位 16 ビット 10 進数と下位 16 ビット 10 進数から形成される）が可能です。

ステップ 3	**neighbor** {*ip-address* | *ipv6-address*} **remote-as** *as-number*
	
	例：
	`switch(config-router)# neighbor 209.165.201.1 remote-as 64497`
	`switch(config-router-neighbor)#`
		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	**bfd** 例： `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	**show running-config bgp** 例： `switch(config-router-neighbor)# show running-config bgp`	（任意）BGP 実行コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-router-neighbor)# copy running-config startup-config`	（任意）この設定の変更を保存します。

EIGRP 上での BFD の設定

Enhanced Interior Gateway Routing Protocol（EIGRP）での BFD の設定

作業を開始する前に

正しい VDC を開始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 機能のイネーブル化」（P.5-6）を参照してください。

BFD セッション パラメータを設定します。「グローバル BFD パラメータの設定」（P.5-7）または「インターフェイス上での BFD の設定」（P.5-8）を参照してください。

EIGRP 機能をイネーブルにします。詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。

手順の概要

1. **configure terminal**
2. **router eigrp** *instance-tag*
3. **bfd**
4. **interface** *int-if*
5. {**ip** | **ipv6**} **eigrp** *instance-tag* **bfd**
6. **show** {**ip** | **ipv6**} **eigrp** [**vrf** *vrf-name*] [**interfaces** *if*]
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**router eigrp** *instance-tag*
	
	例：
	`switch(config)# router eigrp Test1`
	`switch(config-router)#`
		設定されたインスタンス タグを持つ新しい 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 番号として適切ではない*インスタンス タグ*を設定する場合、**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。AS 番号を明示的に設定しない場合、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	**bfd** 例： `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。

	コマンド	目的

ステップ 4	**interface** *int-if*
	
	例：
	`switch(config-router-neighbor)# interface ethernet 2/1`
	`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	{**ip** | **ipv6**} **eigrp** *instance-tag* **bfd** **例：** `switch(config-if)# ip eigrp Test1 bfd`	（任意）EIGRP 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。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。 デフォルトはディセーブルです。
ステップ 6	**show** {**ip** | **ipv6**} **eigrp** [**vrf** *vrf-name*] [**interfaces** *if*] **例：** `switch(config-if)# show ip eigrp`	（任意）EIGRP に関する情報を表示します。vrf-name には最大 32 文字の英数字を使用できます。大文字と小文字を区別します。
ステップ 7	**copy running-config startup-config** **例：** `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

OSPF 上での BFD の設定

Open Shortest Path First version 2（OSPFv2）の BFD を設定できます。

作業を開始する前に

正しい VDC を開始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 機能のイネーブル化」（P.5-6）を参照してください。

BFD セッション パラメータを設定します。「グローバル BFD パラメータの設定」（P.5-7）または「インターフェイス上での BFD の設定」（P.5-8）を参照してください。

OSPF 機能をイネーブルにします。詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。

手順の概要

1. **configure terminal**
2. **router ospf** *instance-tag*
3. **bfd**
4. **interface** *int-if*
5. **if ospf bfd**
6. **show ip ospf** [**vrf** ***vrf-name***] [**interface** ***if***]
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *instance-tag* 例： switch(config)# router ospf 201 switch(config-router)#	設定されたインスタンス タグを持つ新しい OSPFv2 インスタンスを作成します。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。
ステップ 3	**bfd** 例： 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	**interface** *int-if* 例： switch(config-router)# interface ethernet 2/1 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	**ip ospf bfd** 例： switch(config-if)# ip ospf 201 bfd	（任意）OSPFv2 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。デフォルトはディセーブルです。
ステップ 6	**show ip ospf** [**vrf** *vrf-name*] [**interface** *if*] 例： switch(config-if)# show ip ospf	（任意）OSPF に関する情報を表示します。vrf-name には最大 32 文字の英数字を使用できます。大文字と小文字を区別します。
ステップ 7	**copy running-config startup-config** 例： switch(config-if)# copy running-config startup-config	（任意）この設定の変更を保存します。

IS-IS での BFD の設定

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

作業を開始する前に

正しい VDC を開始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 機能のイネーブル化」（P.5-6）を参照してください。

BFD セッション パラメータを設定します。「グローバル BFD パラメータの設定」（P.5-7）または「インターフェイス上での BFD の設定」（P.5-8）を参照してください。

IS-IS 機能をイネーブルにします。詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。

手順の概要

1. **configure terminal**
2. **router isis** *instance-tag*
3. **bfd**
4. **interface** *int-if*
5. **isis bfd**
6. **show isis**
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**router isis** *instance-tag*
	
	例：
	`switch(config)# router isis Enterprise`
	`switch(config-router)#`
		設定された*インスタンス タグ*を持つ新しい IS-IS インスタンスを作成します。

ステップ 3	**bfd** 例： `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	**interface** *int-if*
	
	例：
	`switch(config-router)# interface ethernet 2/1`
	`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	**isis bfd** 例： `switch(config-if)# isis bfd`	（任意）IS-IS 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。デフォルトはディセーブルです。
ステップ 6	**show isis** [**vrf** *vrf-name*] [**interface** *if*] 例： `switch(config-if)# showisis`	（任意）IS-IS に関する情報を表示します。vrf-name には最大 32 文字の英数字を使用できます。大文字と小文字を区別します。
ステップ 7	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

インターフェイス上での BFD のディセーブル化

グローバル レベルまたは VRF レベルで BFD がイネーブルにされているルーティング プロトコルに対し、選択的にインターフェイス上の BFD をディセーブルにできます。

インターフェイス上で 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うちのいずれかを使用します。

コマンド	目的
{**ip** | **ipv6**} **eigrp** *instance-tag* **bfd disable** **例：** `switch(config-if)# ip eigrp Test1 bfd disable`	EIGRP インターフェイス上で 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 **例：** `switch(config-if)# ip ospf 201 bfd disable`	OSPFv2 インターフェイス上で BFD をディセーブルにします。
isis bfd disable **例：** `switch(config-if)# isis bfd disable`	IS-IS インターフェイス上で BFD をディセーブルにします。

ホットスタンバイ ルータ プロトコル（HSRP）での BFD の設定

Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）の BFD を設定できます。アクティブ HSRP ルータおよびスタンバイ HSRP ルータは、BFD を通じてお互いをトラッキングします。スタンバイ HSRP ルータの BFD が、アクティブ HSRP ルータがダウンしていることを検出した場合、スタンバイ HSRP ルータは、このイベントをアクティブ タイム満了として処理し、アクティブ HSRP ルータを引き継ぎます。

show hsrp 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。

作業を開始する前に

正しい VDC を開始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 機能のイネーブル化」（P.5-6）を参照してください。

BFD セッション パラメータを設定します。「グローバル BFD パラメータの設定」（P.5-7）または「インターフェイス上での BFD の設定」（P.5-8）を参照してください。

HSRP 機能をイネーブルにします。詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。

手順の概要

1. **configure terminal**
2. **interface** *int-if*
3. **hsrp bfd**
4. **show running-config hsrp**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface** *int-if* 例： switch(config)# interface ethernet 2/1 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	**hsrp bfd** 例： switch(config-if)# hsrp bfd	（任意）HSRP 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。デフォルトはディセーブルです。
ステップ 4	**show running-config hsrp** 例： switch(config-if)# show running-config hsrp	（任意）HSRP 実行コンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config** 例： switch(config-if)# copy running-config startup-config	（任意）この設定の変更を保存します。

Protocol Independent Multicast（PIM）上での BFD の設置

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

作業を開始する前に

正しい VDC を開始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 機能のイネーブル化」（P.5-6）を参照してください。

PIM 機能をイネーブルにします。詳細については、『*Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 5.x*』を参照してください。

手順の概要

1. **configure terminal**
2. **ip pim bfd**
3. **interface** *if-type*
4. **ip pim bfd-instance** [**disable**]（任意）
5. **show running-config pim**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**ip pim bfd** 例： switch(config)# ip pim bfd	PIM の BFD をイネーブルにします。
ステップ 3	**interface** *int-if* 例： switch(config)# interface ethernet 2/1 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	**ip pim bfd-instance** [**disable**] 例： switch(config-if)# ip pim bfd-instance	（任意）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。デフォルトはディセーブルです。
ステップ 5	**show running-config pim** 例： switch(config)# show running-config pim	（任意）PIM 実行コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

スタティック ルータ上での 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。オプションで Virtual Routing and Forwarding（VRF; 仮想ルーティング/転送）インスタンス内のスタティック ルータの BFD を設定できます。

作業を開始する前に

正しい VDC を開始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 機能のイネーブル化」（P.5-6）を参照してください。

手順の概要

1. **configure terminal**
2. **vrf context** *vrf-name*（任意）
3. **ip route** *route* **interface** *if* {*nh-address* | *nh-prefix*}
4. **ip route static bfd** *interface* {*nh-address* | *nh-prefix*}
5. **show ip route static** [**vrf** *vrf-name*]
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**vrf context** *vrf-name* 例： switch(config)# vrf context Red switch(config-vrf)#	（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	**ip route** *route interface* {*nh-address* | *nh-prefix*} 例： switch(config-vrf)# ip route 192.0.2.1 ethernet 2/1 192.0.2.4	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、サポートされるインターフェイスを表示します。
ステップ 4	**ip route static bfd** *interface* {*nh-address* | *nh-prefix*} 例： switch(config-vrf)# ip route static bfd ethernet 2/1 192.0.2.4	インターフェイス上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	**show ip route static**[**vrf** *vrf-name*] 例： switch(config-vrf)# show ip route static vrf Red	（任意）スタティック ルートを表示します。
ステップ 6	**copy running-config startup-config** 例： switch(config-vrf)# copy running-config startup-config	（任意）この設定の変更を保存します。

BFD 設定の確認

BFD 設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show 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。

これらのコマンドの出力フィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x*』を参照してください。

BFD のモニタ

BFD ステータス情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show 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**]	インターフェイス上の 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。

これらのコマンドの出力フィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x*』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
```

その他の関連資料

BFD の実装に関する詳細は、次の各項を参照してください。

- 「関連資料」（P.5-24）
- 「RFC」（P.5-24）
- 「BFD 機能の履歴」（P.5-24）

関連資料

関連項目	参照先
BFD コマンド	詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。

RFC

RFC	タイトル
draft-ietf-bfd-base-09.txt	『*Bidirectional Forwarding Detection*』（バージョン 1）
draft-ietf-bfd-multihop-06.txt	『*BFD for Multihop Paths*』
draft-ietf-bfd-v4v6-1hop9-.txt	『*BFD for IPv4 and IPv6 (Single Hop)*』

BFD 機能の履歴

表 5-2 は、この機能のリリースの履歴です。

表 5-2　BFD 機能の履歴

機能名	リリース	機能情報
BFD	5.0(2)	この機能が導入されました。

CHAPTER 6

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 Nexus 7000 シリーズ NX-OS 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。

この章では、次の内容について説明します。

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。また、ポート チャネルでは、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 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 セキュリティの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 5.x*』を参照してください）。

ポート チャネルのすべてのポートが同じ Virtual Device Context（VDC; 仮想デバイス コンテキスト）であることが必要です。複数の VDC にポート チャネルを設定できません。デバイスごとに最大 256 のポート チャネルを設定できます。

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手順については、第 3 章「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、Spanning Tree Protocol（STP; スパニング ツリー プロトコル）パラメータをポート チャネルに設定すると、Cisco DC-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」（P.4-2）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。

LACP については「LACP の概要」（P.6-8）を参照してください。

ここでは、次の内容について説明します。

ポート チャネル

ポート チャネルは物理リンクをチャネル グループにバンドルして単一の論理リンクを作成し、最大 8 つの物理リンクからなる集約帯域幅を実現します。ポート チャネルのメンバ ポートが故障すると、それまでに故障したリンクで伝送されたトラフィックはポート チャネルに残っている他のメンバ ポートに切り替えます。

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。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」（P.6-13）を参照）。

（注）　デバイスのポート チャネルは Port Aggregation Protocol（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」（P.6-4）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」（P.6-9）を参照）。

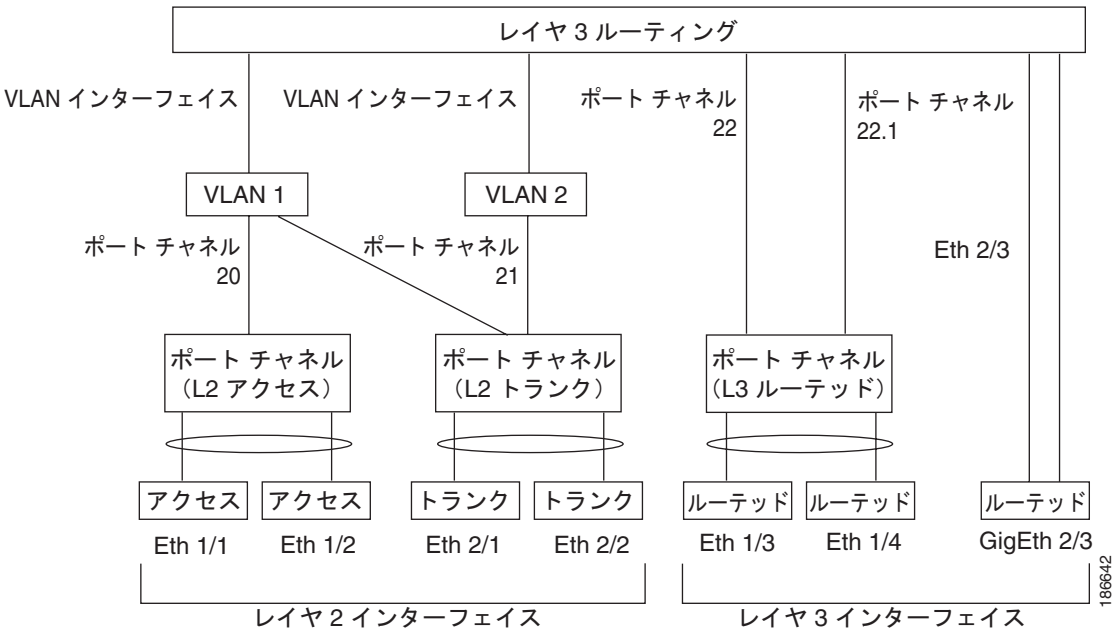
ポート チャネル インターフェイスを作成すると、ポート チャネルを直接作成できます。またはチャネル グループを作成して個別ポートをバンドルに集約させることができます。インターフェイスをチャネル グループに関連付けると、ポート チャネルがない場合は対応するポート チャネルが自動的に作成されます。この場合、ポート チャネルは最初のインターフェイスのレイヤ 2 またはレイヤ 3 設定を行います。最初にポート チャネルを作成することもできます。この場合は、Cisco DC-OS ソフトウェアがポート チャネルと同じチャネル番号の空のチャネル グループを作成してデフォルト レイヤ 2 またはレイヤ 3 設定を行い、互換性も設定します（「互換性要件」（P.6-4）を参照）。ポート チャネル サブインターフェイスの作成と削除の詳細については、第 4 章「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、そのポートのチャネルが有効であれば、ポート チャネルはアップしています。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

図 6-1 に、ポート チャネル インターフェイスを示します。

図 6-1　　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 Media Access Control（MAC; メディア アクセス制御）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 アドレス設定については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*』を参照してください。

レイヤ 2 ポートにアクセスまたはトランク モードを設定する手順については、第 3 章「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 インターフェイスとサブインターフェイスを設定する手順については、第 4 章「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：情報目的で設定します。上位レベルプロトコルで使用されます。
- 遅延：情報目的で設定します。上位レベルプロトコルで使用されます。
- 説明
- デュプレックス
- フロー制御
- IP アドレス：IPv4 と IPv6 です。
- Maximum Transmission Unit（最大伝送ユニット ; MTU）（MTU の設定については、第 2 章「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）
- 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、ソフトウェアは特定のインターフェイス アトリビュートをチェックし、インターフェイスがチャネル グループと互換性があることを確認します。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 DC-OS ソフトウェアはインターフェイスの多数の動作アトリビュートをチェックしてから、その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容します。

互換性チェックの対象となる動作属性は次のとおりです。

- ネットワーク レイヤ
- （リンク）速度性能
- 速度設定
- デュプレックス性能
- デュプレックス設定
- ポート モード
- アクセス VLAN

- トランク ネイティブ VLAN
- タグ付きまたはタグなし
- 許可 VLAN リスト
- MTU サイズ
- SPAN：SPAN の始点または宛先ポートは不可
- レイヤ 3 ポート：サブインターフェイスは不可
- ストーム制御
- フロー制御性能
- フロー制御設定

Cisco DC-OS ソフトウェアが使用する互換性チェックの全リストを確認するには、**show port-channel compatibility-parameters** コマンドを使用します。

チャネル モード セットを **on** に設定したインターフェイスだけをスタティック ポート チャネルに追加できます。また、チャネル モードを **active** または **passive** に設定したインターフェイスだけを、LACP を実行するポート チャネルに追加できます（ポート チャネル モードの詳細については、「LACP Marker Responder」（P.6-10）を参照してください）。これらの属性は、個々のメンバ ポートに設定できます。設定するメンバ ポートのアトリビュート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 アドレス
- スパニング ツリー プロトコル
- NAC
- サービス ポリシー
- Quality of Service（QoS; サービス品質）
- Access Control List（ACL; アクセス コントロール リスト）

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 チャネルを使ったロード バランシング

Cisco DC-OS ソフトウェアは、フレームのアドレスを数値にハッシュしてチャネルのリンクを 1 つ選択することで、ポート チャネルの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。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 バランシングは、MAC アドレス、IP アドレスを使用します。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 バランシング設定に優先されます。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 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、送信元および宛先 MAC アドレスです。

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

- 宛先 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） 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することはできません。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 Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）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。

ポート チャネルを使用するロード バランシング アルゴリズムは、マルチキャスト トラフィックには適用されません。設定したロード バランシング アルゴリズムにかかわらず、マルチキャスト トラフィックは次の方式を使用してポート チャネルのロード バランシングを行います。

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

（注） Cisco IOS を実行するデバイスは、単一メンバの障害時に、**port-channel hash-distribution** コマンドを実行することで、メンバ ポートの ASIC の動作を最適化できました。Cisco Nexus 7000 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 ethernet** 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せん。

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 つのインターフェイスをアクティブに、最大 8 つのインターフェイスをスタンバイ ステートにできます。

ここでは、次の内容について説明します。

- 「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」（P.6-11）
- 「LACP 互換性の拡張」（P.6-11）

LACP の概要

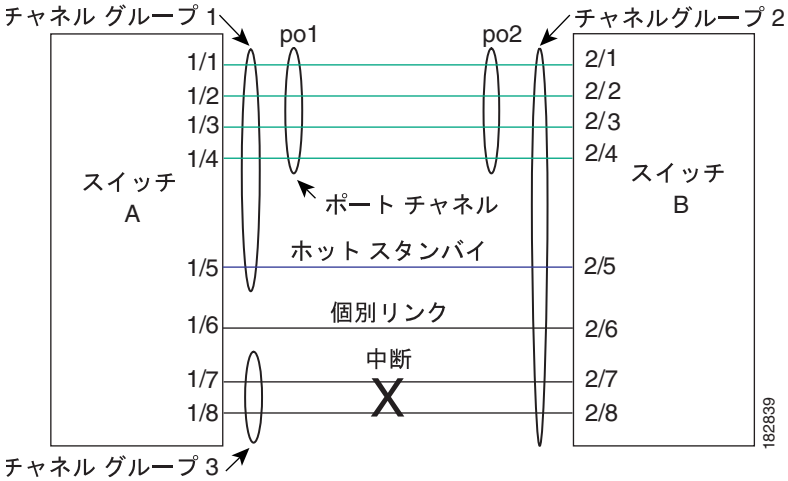
（注）　LCAP は、使用する前に イネーブルにする必要があります。デフォルトでは、LACP はディセーブルです。

LACP をイネーブルにする手順については「LACP のイネーブル化」（P.6-27）を参照してください。

Cisco NX-OS Release 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。コールバックとチェックポイントについては、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』を参照してください。

図 6-2 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 6-2　　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、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。

（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 設定が有効な場合は LACP をディセーブルにできません。

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** に設定して、各チャネルの LACP をイネーブルにします。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** 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。

表 6-1 で、各チャネル モードについて説明します。

表 6-1　ポート チャネルの個別リンクのチャネル モード

チャネル モード	説明
passive	LACP 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。 各チャネルで 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。そのため、LACP チャネル グループには参加しません。 デフォルト 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、**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。
- **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

ここでは、LACP パラメータについて次の内容を説明します。

LACP システム プライオリティ

LACP を実行するどのシステムにも LACP システム プライオリティ値があります。このパラメータのデフォルトの値である 32768 を適用することも、1 ～ 65535 の値を設定することもできます。LACP はシステム プライオリティに MAC アドレスを使用してシステム ID を形成します。また、他のデバイスとのネゴシエーション中にもシステム プライオリティを使用します。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 のシステム 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。

LCAP 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。LACP ポート プライオリティに、デフォルト値である 32768 を適用することも、1 ～ 65535 の値を設定することもできます。LACP はポート番号とともにポート プライオリティを使用して、ポート ID を形成します。

互換性のあるすべてのポートを集約できない制限がある場合、LACP はポート プライオリティを使用して、スタンバイ モードにする必要があるポートを決定し、アクティブ モードにすべきポートを指定します。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。管理キーは、他のポートと集約されるポートの機能を定義します。他のポートと集約されるポート機能は、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 Marker Responder

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

表 6-2 に、LACP がイネーブルのポート チャネルとスタティック ポート チャネルの主な相違点を示します。

表 6-2　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

設定	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	適用不可
リンクのチャネル モード	次のいずれかです。 • Active • Passive	On だけ
チャネルの最大リンク数	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 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ときに、サーバの起動に失敗する原因になることがあります。**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。

バーチャライゼーションのサポート

メンバ 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 ポートを持つ Virtual Device Context（VDC; 仮想デバイス コンテキスト）で設定します。すべての VDC 間に最大 256 のポート チャネルを設定できます。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」（P.6-8）を参照してください。

（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, Release 5.x*』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と VLAN は同じ VDC であることが必要です。LACP を使用する場合、最大 8 つのアクティブ ポートと最大 8 つのスタンバイ ポートは同じ VDC であることが必要です。ポート チャネルはグローバルに作成されるので、ポート チャネルにメンバ ポートを設定する前に、それぞれの VDC に割り当てるメンバ ポートを確認する必要があります。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 チャネルを使ったロード バランシング」（P.6-6）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 DC-OS ソフトウェアは実行時の設定を適用します。

（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, Release 5.x*』を参照してください。

ポート チャネリングのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	ポート チャネリングに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 のライセンス スキームの詳細については、『*Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x*』を参照してください。

ただし、VDC を使用する場合は Advanced Services ライセンスが必要です。

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。

- デバイスにログオンしていること。
- 必要に応じて Advanced Services ライセンスをインストールし、必要な VDC を開始すること。

- チャネル グループのすべてのポートが同じ VDC であること。
- シングル ポート チャネルのすべてのポートは、レイヤ 2 またはレイヤ 3 ポートであること。
- シングル ポート チャネルのすべてのポートが、互換性の要件を満たしていること。互換性の要件の詳細については、「互換性要件」（P.6-4）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。

注意事項および制約事項

ポート チャネリングには次の注意事項と制約事項があります。

- 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。
- 冗長スーパーバイザ エンジン上のポートも含め、すべてのモジュール上のすべてのイーサネット ポートは、ポート チャネル（最大 8 つのアクティブ ポートを持つ）をサポートします。これらのポートは、物理的に隣接しているポートでなくても、また同じモジュール上のポートでなくてもかまいません。
- 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 （共有および専用ポートについては、第 2 章「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）。
- 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。
- STP では、ポート チャネル バンドルはシングル ポートと見なされます。この場合のポート コストは、そのチャネルに割り当てられているすべての設定されたポート コストの合計です。
- 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。

ポート チャネルの設定

ここでは、次の内容について説明します。

- 「ポート チャネルの説明の設定」（P.6-22）
- 「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」（P.6-23）
- 「フロー制御の設定」（P.6-24）
- 「ポート チャネルを使ったロード バランシングの設定」（P.6-25）
- 「LACP のイネーブル化」（P.6-27）
- 「LACP ポート チャネル ポート モードの設定」（P.6-28）
- 「LACP システム プライオリティの設定」（P.6-29）
- 「LACP ポート プライオリティの設定」（P.6-30）
- 「LACP グレースフル コンバージェンス」（P.6-31）
- 「LACP の個別一時停止のディセーブル化」（P.6-34）

（注）　ポート チャネル インターフェイスに MTU を設定する手順については、第 2 章「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。ポート チャネル インターフェイスに IPv4 および IPv6 アドレスを設定する手順については、第 4 章「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）　Cisco IOS CLI を熟知している場合は、この機能の Cisco NX-OS コマンドと使用する Cisco IOS コマンドが異なる場合もある点に注意してください。

ポート チャネルの作成

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

作業を開始する前に

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 を開始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）。

手順の概要

1. **configure terminal**
2. **interface port-channel** *channel-number*
3. **show port-channel summary**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface port-channel** *channel-number*
	
	例：
	`switch(config)# interface port-channel 1`
	`switch(config-if)`
		設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。指定できる範囲は 1 ～ 4096 です。Cisco DC-OS ソフトウェアは、チャネル グループがない場合はそれを自動的に作成します。

ステップ 3	**show port-channel summary** **例：** `switch(config-router)# show port-channel summary`	（任意）ポート チャネルに関する情報を表示します。
ステップ 4	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

次に、ポート チャネルを作成する例を示します。

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

ポート チャネルを削除したときのインターフェイス コンフィギュレーションの変化について詳しくは、「互換性要件」（P.6-4）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。

作業を開始する前に

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 を開始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。

手順の概要

1. **configure terminal**
2. **interface** *type slot/port*
3. **switchport**
4. **switchport mode trunk**
5. **switchport trunk** {**allowed vlan** *vlan-id* | **native** *vlan-id*}
6. **channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]
7. **show interface** *type slot/port*
8. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)`
		チャネル グループに追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

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

	コマンド	目的

ステップ 6	**channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]
	
	例：
	`switch(config-if)# channel-group 5`
	
	例：
	`switch(config-if)# channel-group 5 force`
		チャネル グループのポートを変更し、モードを設定します。channel-number の範囲は 1 ～ 4096 です。ポート チャネルがない場合は、このチャネル グループに関連付けられたポート チャネルが作成されます。すべてのスタティック ポート チャネル インターフェイスは、**on** モードに設定されます。すべての LACP 対応ポート チャネルインターフェイスを **active** または **passive** に設定する必要があります。デフォルト モードは、**on** です。
		
		（任意）一部の設定に互換性がないインターフェイスをチャネルに追加します。強制されるインターフェイスは、チャネル グループと同じ速度、デュプレックス、およびフロー制御設定を持っている必要があります。

ステップ 7	**show interface** *type slot/port* **例：** `switch(config-router)# show interface port channel 5`	（任意）インターフェイスの内容を表示します。
ステップ 8	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

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。

作業を開始する前に

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 を開始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。

手順の概要

1. **configure terminal**
2. **interface** *type slot/port*
3. **no switchport**
4. **channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]
5. **show interface** *type slot/port*
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)`
		チャネル グループに追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

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

ステップ 4	**channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]
	
	例：
	`switch(config-if)# channel-group 5`
	
	例：
	`switch(config-if)# channel-group 5 force`
		チャネル グループのポートを変更し、モードを設定します。channel-number の範囲は 1 ～ 4096 です。ポート チャネルがない場合、Cisco DC-OS ソフトウェアにより、このチャネル グループに関連付けられたポート チャネルが作成されます。
		
		（任意）一部の設定に互換性がないインターフェイスをチャネルに追加します。強制されるインターフェイスは、チャネル グループと同じ速度、デュプレックス、およびフロー制御設定を持っている必要があります。

	コマンド	目的
ステップ 5	**show interface** *type slot/port* 例： `switch(config-router)# show interface ethernet 1/4`	（任意）インターフェイスの内容を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

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
```

次に、レイヤ 3 ポート チャネル インターフェイスを作成して IP アドレスを割り当てる例を示します。

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

帯域幅と遅延の割り当て（情報目的）

ポート チャネルの帯域幅は、そのチャネルのアクティブ リンク数の合計で決まります。

ポート チャネル インターフェイスの帯域幅と遅延を情報目的で設定します。

手順の概要

1. **configure terminal**
2. **interface port-channel** *channel-number*
3. **bandwidth** *value*
4. **delay** *value*
5. **exit**
6. **show interface port-channel** *channel-number*
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。

ステップ 2	**interface port-channel** *channel-number*
	
	例：
	switch(config)# interface port-channel 2
	switch(config-if)
		設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**bandwidth** *value* 例： switch(config-if)# bandwidth 60000000 switch(config-if)#	帯域幅を指定します。これは情報目的で使用します。有効値の範囲は 1 ～ 80,000,000 Kbps です。デフォルト値はチャネル グループのアクティブ インターフェイスの合計によって異なります。
ステップ 4	**delay** *value* 例： switch(config-if)# delay 10000 switch(config-if)#	スループット遅延を指定します。これは情報目的で使用します。有効値の範囲は 1 ～ 16,777,215 で、単位は 10 マイクロ秒です。デフォルト値は 10 マイクロ秒です。 **（注）** Cisco リリース 4.2(1) よりも前は、デフォルト値は 100 マイクロ秒でした。
ステップ 5	**exit** 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了し、コンフィギュレーション モードに戻ります。
ステップ 6	**show interface port-channel** *channel-number* 例： switch(config-router)# show interface port-channel 2	（任意）指定したポート チャネルのインターフェイス情報を表示します。
ステップ 7	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、情報用にポート チャネル 5 の帯域幅および遅延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。

手順の概要

1. **configure terminal**
2. **interface port-channel** *channel-number*
3. **shutdown | no shutdown**
4. **exit**
5. **show interface port-channel** *channel-number*
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface port-channel** *channel-number*
	
	例：
	`switch(config)# interface port-channel 2`
	`switch(config-if)`
		設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**shutdown**
	
	例：
	`switch(config-if)# shutdown`
	`switch(config-if)#`
		インターフェイスをシャットダウンします。トラフィックは通過せず、インターフェイスは管理ダウン状態になります。デフォルトは no shutdown です。

	no shutdown
	
	例：
	`switch(config-if)# no shutdown`
	`switch(config-if)#`
		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 no shutdown なしです。

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

ステップ 5	**show interface port-channel** *channel-number* 例： `switch(config-router)# show interface port-channel 2`	（任意）指定したポート チャネルのインターフェイス情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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。

手順の概要

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

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface port-channel** *channel-number*
	
	例：
	`switch(config)# interface port-channel 2`
	`switch(config-if)`
		設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**description**
	
	例：
	`switch(config-if)# description engineering`
	`switch(config-if)#`
		ポート チャネル インターフェイスに説明を追加できます。説明は 80 字以内で行います。デフォルトでは、説明は表示されません。説明を表示する場合はあらかじめこのパラメータを設定する必要があります。

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

ステップ 5	**show interface port-channel** *channel-number* 例： `switch(config-router)# show interface port-channel 2`	（任意）指定したポート チャネルのインターフェイス情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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。

手順の概要

1. **configure terminal**
2. **interface port-channel** *channel-number*
3. **speed** {**10** | **100** | **1000** | **auto**}
4. **duplex** {**auto** | **full** | **half**}
5. **exit**
6. **show interface port-channel** *channel-number*
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface port-channel** *channel-number*
	
	例：
	`switch(config)# interface port-channel 2`
	`switch(config-if)`
		設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**speed** {**10** | **100** | **1000** | **auto**}
	
	例：
	`switch(config-if)# speed auto`
	`switch(config-if)#`
		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 auto です。

ステップ 4	**duplex** {**auto** | **full** | **half**}
	
	例：
	`switch(config-if)# speed auto`
	`switch(config-if)#`
		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 auto です。

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

	コマンド	目的
ステップ 6	**show interface port-channel** *channel-number* 例： switch(config-router)# show interface port-channel 2	（任意）指定したポート チャネルのインターフェイス情報を表示します。
ステップ 7	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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。1 Gb よりも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）　この設定がリンクのローカルおよびリモート エンドの両方で一致しなければ、フロー制御が正しく動作しません。

手順の概要

1. **configure terminal**
2. **interface port-channel** *channel-number*
3. **flowcontrol** {**receive** | **send**} {**desired** | **off** | **on**}
4. **exit**
5. **show interface port-channel** *channel-number*
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。

ステップ 2	**interface port-channel** *channel-number*
	
	例：
	switch(config)# interface port-channel 2
	switch(config-if)
		設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**flowcontrol** {**receive** | **send**} {**desired** | **off** | **on**} 例： switch(config-if)# flowcontrol send desired switch(config-if)#	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、ディセーブルです。
ステップ 4	**exit** 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了し、コンフィギュレーション モードに戻ります。
ステップ 5	**show interface port-channel** *channel-number* 例： switch(config-router)# show interface port-channel 2	（任意）指定したポート チャネルのインターフェイス情報を表示します。
ステップ 6	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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 VDC との関連付けにかかわらず 1 のモジュールだけに適用します。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。

作業を開始する前に

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 を開始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）。

手順の概要

1. **configure terminal**
2. **port-channel load-balance ethernet** {**dest-ip-port** | **dest-ip-port-vlan** | **destination-ip-vlan** | **destination-mac** | **destination-port** | **source-dest-ip-port** | **source-dest-ip-port-vlan** | **source-dest-ip-vlan** | **source-dest-mac** | **source-dest-port** | **source-ip-port** | **source-ip-port-vlan** | **source-ip-vlan** | **source-mac** | **source-port**} [*module-number*]
3. **show port-channel load-balance**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**port-channel load-balance ethernet** {**dest-ip-port** | **dest-ip-port-vlan** | **destination-ip-vlan** | **destination-mac** | **destination-port** | **source-dest-ip-port** | **source-dest-ip-port-vlan** | **source-dest-ip-vlan** | **source-dest-mac** | **source-dest-port** | **source-ip-port** | **source-ip-port-vlan** | **source-ip-vlan** | **source-mac** | **source-port**} [module-*number*]
	
	例：
	`switch(config)# port-channel load-balance ethernet source-destination-mac`
	`switch(config)#`
		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。有効範囲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 および IPv6 の **source-dest-ip**、非 IP のデフォルトは **source-dest-mac** です。

ステップ 3	**show port-channel load-balance** 例： `switch(config-router)# 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	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

no port-channel load-balance ethernet を使用してデフォルトのロード バランシング アルゴリズム（非 IP トラフィック用の source-dest-mac、および IP トラフィック用の source-dest-ip）を復元します。

コマンド	目的
no port-channel load-balance ethernet **例：** `switch(config)# no port-channel load-balance ethernet`	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 ethernet source-ip-port module 5
```

LACP のイネーブル化

LACP はデフォルトでディセーブルです。LACP 設定を開始する前に 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。

作業を開始する前に

正しい VDC を開始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）。

手順の概要

1. **configure terminal**
2. **feature lacp**
3. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 2	**feature lacp** 例： switch(config)# feature lacp	デバイスの LACP をイネーブルにします。
ステップ 3	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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 モードを使えば、LACP でリンクを許容できます。

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。

作業を開始する前に

正しい VDC を開始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）。

手順の概要

1. **configure terminal**
2. **interface** *type slot/port*
3. **channel-group** *number* **mode** {**active** | **on** | **passive**}
4. **show port-channel summary**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。

ステップ 2	**interface** *type slot/port*
	
	例：
	switch(config)# interface ethernet 1/4
	switch(config-if)
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**channel-group** *number* **mode** {**active** | **on** | **passive**} 例： switch(config-if)# channel-group 5 mode active	ポート チャネルのリンクのポート モードを指定します。LACP をイネーブルにしたら、各リンクまたはチャネル全体を active または passive に設定します。 関連する集約プロトコルを使用せずにポート チャネルを実行する場合、ポート チャネル モードは常に on です。 デフォルトのポート チャネル モードは on です。
ステップ 4	**show port-channel summary** 例： switch(config-if)# show port-channel summary	（任意）ポート チャネルの概要を表示します。
ステップ 5	**copy running-config startup-config** 例： switch(config-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 システム プライオリティの設定

LACP のシステム 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。

作業を開始する前に

LACP をイネーブルにします。

正しい VDC を開始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）。

手順の概要

1. **configure terminal**
2. **lacp system-priority** *priority*
3. **show lacp system-identifier**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**lacp system-priority** *priority* 例： switch(config)# lacp system-priority 40000	LACP で使用するシステム プライオリティを設定します。有効範囲は 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	**show lacp system-identifier** 例： switch(config-if)# show lacp system-identifier	LACP システム ID を表示します。
ステップ 4	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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。

作業を開始する前に

LACP をイネーブルにします。

正しい VDC を開始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）。

手順の概要

1. **configure terminal**
2. **interface** *type slot/port*
3. **lacp port-priority** *priority*
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。

ステップ 2	**interface** *type slot/port*
	
	例：
	switch(config)# interface ethernet 1/4
	switch(config-if)
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**lacp port-priority** *priority* 例： switch(config-if)# lacp port-priority 40000.	LACP で使用するポート プライオリティを設定します。有効範囲は 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	**copy running-config startup-config** 例： switch(config-if)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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。

（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。

作業を開始する前に

LACP をイネーブルにします。

正しい VDC を開始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）。

手順の概要

1. **configure terminal**
2. **interface port-channel** *number*

3. **shutdown**
4. **no lacp graceful-convergence**
5. **no shutdown**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。

ステップ 2	**interface port-channel** *number*
	
	例：
	switch(config)# interface port-channel 1
	switch(config-if)
		設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**shutdown** 例： switch(config-if) shutdown	ポート チャネルを管理シャットダウンします。
ステップ 4	**no lacp graceful-convergence** 例： switch(config-if)# no lacp graceful-convergence	ポート チャネルの LACP グレースフル コンバージェンスをディセーブルにします。
ステップ 5	**no shutdown** 例： switch(config-if) no shutdown	ポート チャネルを管理的にアップします。
ステップ 6	**copy running-config startup-config** 例： switch(config-if)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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 コンバージェンスを再度イネーブルにする

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。

手順の概要

1. **configure terminal**
2. **interface port-channel** *number*
3. **shutdown**
4. **lacp graceful-convergence**
5. **no shutdown**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface port-channel** *number*
	
	例：
	`switch(config)# interface port-channel 1`
	`switch(config-if)`
		設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**shutdown** 例： `switch(config-if) shutdown`	ポート チャネルを管理シャットダウンします。

ステップ 4	**lacp graceful-convergence**
	
	例：
	`switch(config-if)# lacp`
	`graceful-convergence`
		ポート チャネルの LACP グレースフル コンバージェンスをイネーブルにします。

ステップ 5	**no shutdown** 例： `switch(config-if) no shutdown`	ポート チャネルを管理的にアップします。

ステップ 6	**copy running-config startup-config**
	
	例：
	`switch(config-if)# copy running-config`
	`startup-config`
		（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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。これが、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ときに、サーバの起動に失敗する原因になることがあります。個別の利用のために動作を調整できます。

（注）　エッジ ポートで **lacp suspend-individual** コマンドを実行するだけです。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。

作業を開始する前に

LACP をイネーブルにします。

正しい VDC を開始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）。

手順の概要

1. **configure terminal**
2. **interface port-channel** *number*
3. **shutdown**
4. **no lacp suspend-individual**
5. **no shutdown**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface port-channel** *number*
	
	例：
	`switch(config)# interface port-channel 1`
	`switch(config-if)`
		設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**shutdown** 例： `switch(config-if) shutdown`	ポート チャネルを管理シャットダウンします。
ステップ 4	**no lacp suspend-individual** 例： `switch(config-if)# no lacp suspend-individual`	ポート チャネルで LACP 個別ポートの一時停止動作をディセーブルにします。

	コマンド	目的
ステップ 5	**no shutdown** 例： 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	**copy running-config startup-config** 例： switch(config-if)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、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動作を再度イネーブルにできます。

手順の概要

1. **configure terminal**
2. **interface port-channel** *number*
3. **shutdown**
4. **lacp suspend-individual**
5. **no shutdown**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。

ステップ 2	**interface port-channel** *number*
	
	例：
	switch(config)# interface port-channel 1
	switch(config-if)
		設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**shutdown** 例： switch(config-if) shutdown	ポート チャネルを管理シャットダウンします。

	コマンド	目的
ステップ 4	**lacp suspend-individual** 例： `switch(config-if)# lacp suspend-individual`	ポート チャネルで LACP 個別ポートの一時停止動作をイネーブルにします。
ステップ 5	**no shutdown** 例： `switch(config-if) no shutdown`	ポート チャネルを管理的にアップします。
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、ポート チャネルで LACP 個別ポートの一時停止動作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 チャネルの設定の確認

次のコマンドを使用すると、ポート チャネル構成情報を表示することができます。

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 [**interface port-channel** *channel-number*]	1 つ以上のポート チャネル インターフェイスの集約状態を表示します。
show port-channel load-balance	ポート チャネルで使用するロード バランシングのタイプを表示します。
show port-channel summary	ポート チャネル インターフェイスのサマリーを表示します。
show port-channel traffic	ポート チャネルのトラフィック統計情報を表示します。
show port-channel usage	使用済みおよび未使用のチャネル番号の範囲を表示します。
show lacp {**counters** [**interface port-channel** *channel-number*] | [**interface** *type*/*slot*] | **neighbor** [**interface port-channel** *channel-number*] | **port-channel** [**interface port-channel** *channel-number*] | **system-identifier**]]}	LACP の情報を表示します。
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情報を表示します。

このコマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x*』を参照してください。

統計情報の表示

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。

これらのコマンドについては、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x*』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 DC-OS ソフトウェアによって、ポート チャネルは自動的に作成されます。

```
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
```

デフォルト設定

表 6-3 に、ポート チャネル パラメータのデフォルト設定を示します。

表 6-3　デフォルト ポート チャネル パラメータ

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

その他の関連資料

ポート チャネルの実装に関する追加情報については、次の項を参照してください。

- 「関連資料」（P.6-40）
- 「管理情報ベース（MIB）」（P.6-40）

関連資料

関連項目	参照先
レイヤ 2 インターフェイスの設定	第 3 章「レイヤ 2 インターフェイスの設定」
レイヤ 3 インターフェイスの設定	第 4 章「レイヤ 3 インターフェイスの設定」
共有および専用ポート	第 2 章「基本インターフェイス パラメータの設定」
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x*』
インターフェイス	『*Cisco DCNM Interfaces Configuration Guide, Release 5.x*』
システム管理	『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』
ハイ アベイラビリティ	『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x*』
VDC	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x*』
ライセンス	『*Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x*』
リリース ノート	『*Cisco Nexus 7000 Series NX-OS Release Notes, Release 5.x*』

標準規格

標準規格	タイトル
IEEE 802.3ad	—

管理情報ベース（MIB）

管理情報ベース（MIB）	MIB リンク
• IEEE8023-LAG-CAPABILITY • CISCO-LAG-MIB	Management Information Base（MIB; 管理情報ベース）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

ポート チャネル設定の機能履歴

表 6-4 は、この機能のリリースの履歴です。

表 6-4　ポート チャネル設定の機能履歴

機能名	リリース	機能情報
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	4.2(1)	サポートが 256 ポート チャネルに増加されました。

CHAPTER 7

vPC の設定

この章では、Cisco Nexus 7000 シリーズのデバイス上で仮想ポート チャネル（vPCs）を設定する方法を説明します。

この章では、次の内容について説明します。

（注） ポート チャネルと Link Aggregation Control Protocol（LACP）の設定の詳細については、第 6 章「ポート チャネルの設定」を参照してください。

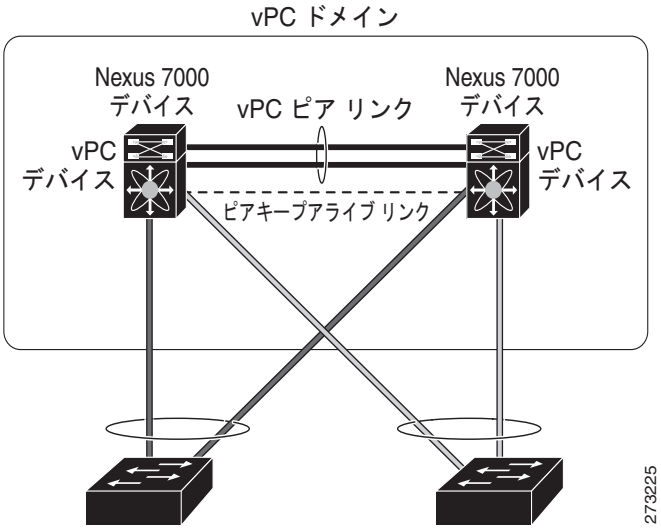
vPC について

ここでは、次の内容について説明します。

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（図 7-1 を参照してください）。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。Cisco NX-OS Release 4.1(4) から、デバイスごとに最大 256 個の vPC を設定できます。vPC は、ノード間の複数の並列パスを可能にし、トラフィックのロード バランシングを可能にすることによって、冗長性を作り、バイセクショナルな帯域幅を増やすレイヤ 2 マルチパスを提供できます。

図 7-1　　vPC のアーキテクチャ



vPC で使用できるのは、レイヤ 2 ポート チャネルだけです。vPC ドメインは単一の 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 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
- Link Aggregation Control Protocol（LACP）

LACP を使用せずに vPC（vPC ピア リンク チャネルも含めて）のポート チャネルを設定する場合は、各デバイスが、単一のポート チャネル内に最大 8 つのアクティブ リンクを持てます。LACP を使用して vPC（vPC ピア リンク チャネルも含めて）のポート チャネルを設定する場合は、各デバイスが、単一のポート チャネル内に 8 つのアクティブ リンクと 8 つのスタンバイ リンクを持つことができます（LACP と vPCs の使用方法の詳細については、「その他の機能との vPC の相互作用」（P.7-17）を参照してください）。

（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。

リリース 4.2 から、システムはこの機能をディセーブルにする前のチェックポイントを自動的に取得するようになったため、このチェックポイントにロールバックすれば機能をイネーブルにできます。ロールバックとチェックポイントについては、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』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。

1 つの Cisco Nexus 7000 シリーズ シャーシ上のポートを、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、設定することにより、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 Release 4.1(5) で始まった 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。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お勧めします。次に、もう 1 つの Cisco Nexus 7000 シリーズ シャーシで、やはり 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 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ク 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 リリース NX-OS 4.2 から、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します。**track interface** コマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』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。各デバイス上で持てる vPC ドメイン ID は 1 つだけです。

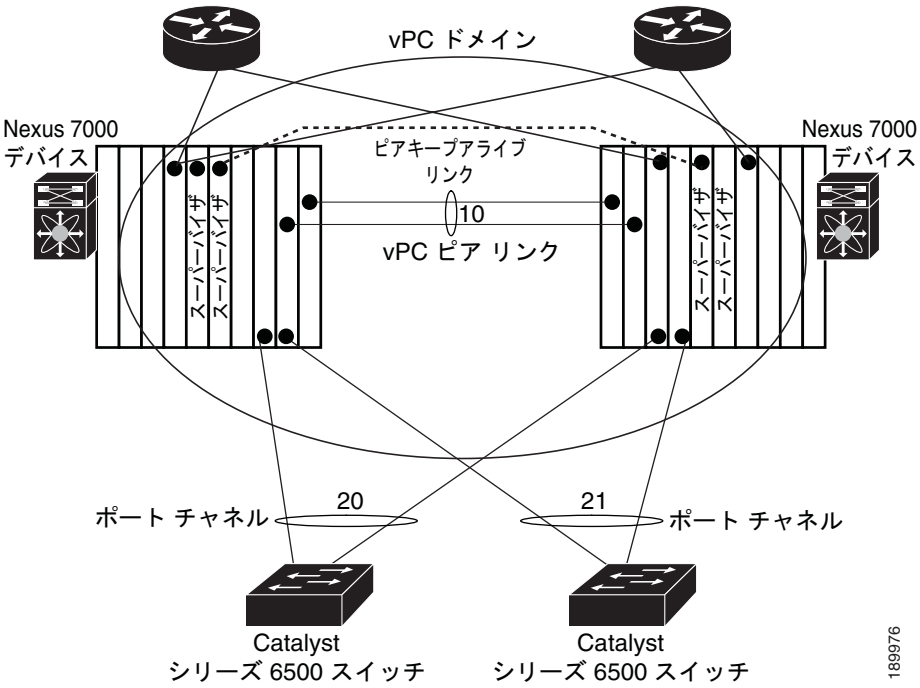
このバージョンでは、各ダウンストリーム デバイスを、単一のポート チャネルを使用して単一の vPC ドメイン ID に接続できます。

（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（図 7-2 を参照してください）は、次の利点を提供します。

- 単一のデバイスが 2 つのアップストリーム デバイスを介して 1 つのポート チャネルを使用することを可能にします。
- スパニング ツリー プロトコル（STP）のブロック ポートをなくします。
- ループフリーなトポロジを提供します。
- 利用可能なすべてのアップリンク帯域幅を使用します。
- リンクまたはデバイスに障害が発生した場合に、ファースト コンバージェンスを提供します。
- リンク レベルの復元力を提供します。
- ハイ アベイラビリティを保証します。

図 7-2　　1 つの VDC 内の vPC インターフェイス



VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x*』を参照してください。

vPC の用語

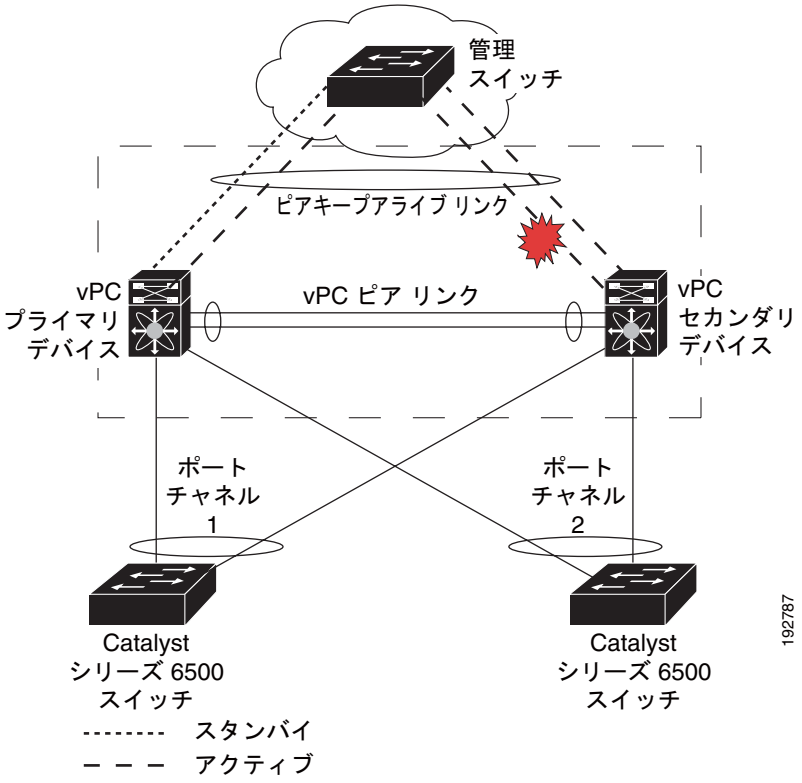
vPCs で使用される用語は、次のとおりです。

- 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 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しなければならない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 デバイスを監視します。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 VRF に関連付けることをお勧めします。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かなければなりません（図 7-3 を参照してください）。

図 7-3　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動しており、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：vPCs に属するインターフェイス。

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。

ここでは、vPC ピア リンクについて説明します。内容は次のとおりです。

- 「vPC ピア リンクの概要」（P.7-6）
- 「プライマリおよびセカンダリ デバイス上で手動で設定しなければならない機能」（P.7-8）
- 「レイヤ 3 接続のための VLAN インターフェイスの設定」（P.7-9）

（注）　vPC ピアリンクを設定するよりも前にピアキープアライブ リンクを設定しなければなりません。そうしないと、ピアリンクは機能しません （vPC のピアキープアライブ リンクとメッセージの詳細については、「ピアキープアライブ リンクとメッセージ」（P.7-9）を参照してください）。

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、モジュールを使用しなければなりません。

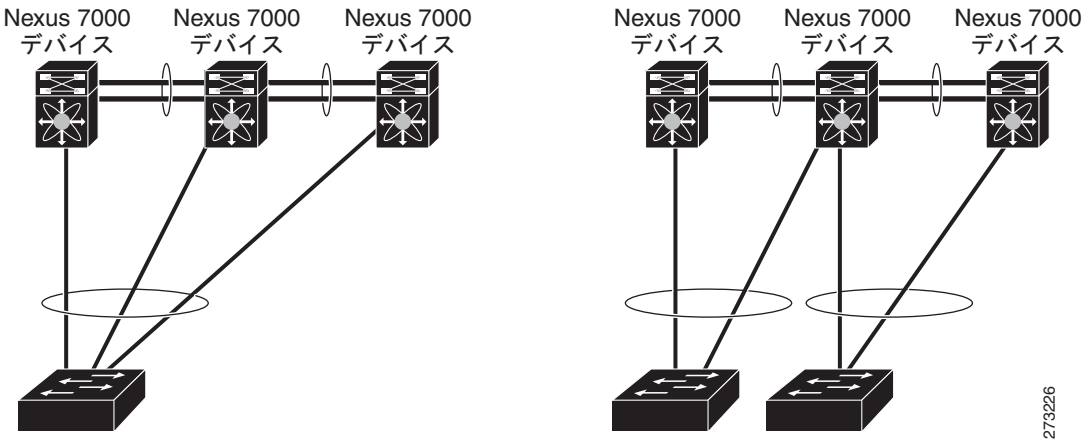
（注）　vPC ピア リンクを設定する場合は、専用ポート モードを使用することをお勧めします。専用ポート モードの詳細については、第 2 章「基本インターフェイス パラメータの設定」を参照してください。

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、図 7-4 を参照してください。

図 7-4　許可されていない vPC ピア設定



有効な設定を作成するには、まず各デバイス上でポート チャネルを設定してから、vPC ドメインを設定します。ポート チャネルを各デバイスに、同じ vPC ドメイン ID を使用してピア 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お勧めします。

（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お勧めします。

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 ピア リンクの互換パラメータ」（P.7-12）を参照してください）。各デバイスが管理プレーンから完全に独立しているため、デバイスが重要なパラメータについて互換性があることを管理者が確認しなければなりません。vPC ピア デバイスは、独立したコントロール プレーンを持っています。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しなければなりません。一貫性が必要な設定の詳細については、「vPC ピア リンクの互換パラメータ」（P.7-12）を参照してください。

vPC ピア リンクを設定すると、接続されているデバイスの片方がプライマリ デバイスになり、接続されているデバイスの他方がセカンダリ デバイスになるように、vPC ピア デバイスがネゴシエートします（「vPC の設定」（P.7-24）を参照してください）。Cisco NX-OS ソフトウェアは、最も小さい 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、以前プライマリ デバイスだったデバイスがセカンダリ デバイスになります。

いずれの vPC デバイスがプライマリ デバイスになるかを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、ネットワーク上のインターフェイスが停止してから再開します。ロール プライオリティを再度設定して片方の vPC がプライマリ デバイスになるようにしたい場合は、プライマリとセカンダリ両方の vPC デバイス上でロール プライオリティを適切な値に設定します。次に、両方のデバイス上で **shutdown** コマンドを入力して、vPC ピア リンクになっているポート チャネルをシャットダウンし、最後に、両方のデバイス上で **no shutdown** コマンドを入力して、ポート チャネルを再びイネーブルにします。

（注）　各 vPC ピア デバイスの vPC ピア リンクに対して、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お勧めします。

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 バランシングの詳細については、第 6 章「ポート チャネルの設定」を参照してください）。

設定情報は、Cisco Fabric Service over Ethernet（CFSoE）プロトコルを使用して vPC ピア リンクを流れます。（CFSoE の詳細については、「CFSoE」（P.7-21）を参照してください）。

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、「CFSoE」（P.7-21）を参照してください）。

Cisco NX-OS 4.2(1) から、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。

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動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 デバイスが稼動している場合は、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お勧めします。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 メッセージの詳細については、「ピアキープアライブ リンクとメッセージ」（P.7-9）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しなければならない機能

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しなければなりません。

- 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」（P.7-17）を参照してください。
  - Bridge Assurance がすべての vPC ピア リンク上でイネーブルになるように、vPC ピア リンク インターフェイスを STP ネットワーク ポートとして設定することをお勧めします。
  - 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 Rapid PVST+ を設定し、プライマリ デバイスがすべてのインターフェイスのルートになるように MST を設定することをお勧めします。
- 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 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 デバイスは HSRP スタンバイになるように設定します。また、同じ管理/動作モードにある各 vPC デバイス上に VLAN インターフェイスが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」（P.7-20）を参照してください）。

vPC ピア リンクの両側で Unidirectional Link Detection（UDLD; 単一方向リンク検出）を設定することをお勧めします。UDLD を設定する手順については「UDLD モードの設定」（P.2-38）を参照してください。

レイヤ 3 接続のための VLAN インターフェイスの設定

HSRP や PIM などのアプリケーションを使用するネットワークのレイヤ 3 にリンクするために、vPC ピア デバイス上の VLAN ネットワーク インターフェイスを使用できます。ただし、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 リンクを別途設定することをお勧めします。

（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方法の詳細については、第 4 章「レイヤ 3 インターフェイスの設定」を参照してください。

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

Cisco NX-OS 4.2(1) から、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）　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しなければなりません。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 ピア間の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動していないと、システムは vPC ピア リンクを稼動させることができません。

（注）　vPC ピアキープアライブ リンクを、各 vPC ピア デバイス内のレイヤ 3 インターフェイスにマッピングされている独立した VRF に関連付けることをお勧めします。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 の設定方法の詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』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。vPC ピアキープアライブ メッセージのデフォルトの間隔は、1 秒です。この間隔は、400 ミリ秒～ 10 秒の範囲内で設定可能です。

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

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

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

- ホールドタイムアウトの間は、vPC セカンダリ デバイスは、受信したキープアライブ メッセージに基づくアクションは一切行いません。これは、スーパーバイザがピア リンクの停止後数秒間の間に失敗したなどが原因で、システムが一時的なキープアライブを受信した場合に、システムがアクションを取ることを防ぐためです。
- タイムアウト中は、vPC セカンダリ デバイスは、設定された間隔が終了するまでにキープアライブ メッセージを受信できないと、vPC プライマリ デバイスになるというアクションを取ります。

キープアライブ メッセージの時間の設定方法については、「vPC の設定」（P.7-24）を参照してください。

（注）　ピアキープアライブ メッセージに使用される送信元 IP アドレスと宛先 IP アドレスの両方が、ネットワーク上で一意であり、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 から到達できることを確認してください。

Command-Line Interface（CLI; コマンドライン インターフェイス）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
```

信頼できるポートと優先順位の設定方法の詳細については、『*Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide, Release 5.x*』を参照してください。

vPC ピア ゲートウェイ

Cisco NX-OS 4.2(1) から、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。

一部の Network-Attached Atorage（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ことを目的とした機能を備えている場合があります。基本的に、こういった機能では、同じサブネットにローカルには接続されていないホストから発生した要求に応答する場合に、ルーティング テーブル ルックアップの実行が避けられます。このようなデバイスは、一般的な HSRP ゲートウェイではなく、送信元 Cisco Nexus 7000 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。このような動作は、一部の基本的なイーサネット RFC 規格と互換性がありません。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、この機能は、ピアリンクの使用を最適化し、トラフィック損失の可能性をなくします。

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、デバイスの稼動も 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場合は、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、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 リダイレクトをディセーブルにする必要があります。vPC ドメイン内でこの機能をイネーブルにすると、このような要件があることが、適切なメッセージによってユーザに通知されます。

ピアゲートウェイ vPC デバイスに到達するパケットは、その TTL がデクリメントされるため、TTL = 1 となっているパケットは TTL の失効が原因で伝送中にドロップされる可能性があります。ピアゲートウェイ機能がイネーブルになっており、パケットを TTL = 1 で送出する特定のネットワーク プロトコルが vPC VLAN 上で稼動している場合は、これを考慮する必要があります。

vPC ドメイン

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

vPC ドメインは、キープアライブ メッセージを設定するために使用したり、他の vPC ピア リンク パラメータについて、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したり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方法については、「vPC の設定」（P.7-24）を参照してください。

vPC ドメインを作成するには、まず各 vPC ピア デバイス上で、1 ～ 1000 の値を使用して vPC ドメイン ID を作成しなければなりません。vPC ドメインは、VDC ごとに 1 つだけ持つことができます。

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しなければなりません。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。可能であれば、各 vPC 内で LACP をアクティブ モードのインターフェイスと一緒に使用してポート チャネルを設定することをお勧めします。これにより、ポート チャネルのフェールオーバーが発生した場合の最適化されたスマートな回復が保証され、さらにポート チャネル自体の間での設定の不一致に対する設定チェックが提供されます。

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 で作成することをお勧めします。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 の表示の詳細については、「CFSoE」（P.7-21）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なければなりません。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 は稼動しません。

vPC ピア リンクの互換パラメータ

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お勧めします。

両方の vPC ピア デバイス上で vPC 機能をイネーブルにし、ピア リンクを設定したら、CFS メッセージによって、ローカル vPC ピア デバイス上の設定のコピーがリモート vPC ピア デバイスに提供されます。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」（P.7-21）を参照してください）。

（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 の稼動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、第 6 章「ポート チャネルの設定」を参照してください。

ここで説明する内容は、次のとおりです。

- 「同じでなければならない設定パラメータ」（P.7-12）
- 「同じにすべき設定パラメータ」（P.7-13）

同じでなければならない設定パラメータ

ここで示す設定パラメータは、vPC ピア リンクの両方のデバイスで同じように設定されていなければなりません。そうなっていないと、vPC はサスペンド モードに移行します。

（注）　vPC 内のすべてのインターフェイスで、下に示す動作パラメータおよび設定パラメータの値が同じになっていなければなりません。

（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 の稼動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
- チャネルごとのリンク速度
- チャネルごとのデュプレックス モード

- チャネルごとのトランク モード：
  - Native VLAN
  - トランク上の許可 VLAN
  - ネイティブ VLAN トラフィックのタギング
- Spanning Tree Protocol（STP; スパニング ツリー プロトコル）モード
- 多重スパニング ツリーの 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
- STP グローバル設定：
  - Bridge Assurance の設定
  - ポート タイプの設定
  - ループ ガードの設定
- STP インターフェイス設定：
  - ポート タイプの設定
  - ループ ガード
  - ルート ガード
- Maximum Transmission Unit（MTU; 最大伝送ユニット）

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しなければなりません。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; サービス品質）の設定とパラメータ
- STP インターフェイス設定：
  - BPDU フィルタ
  - BPDU ガード
  - コスト

  - リンク タイプ
  - プライオリティ
  - VLAN（Rapid PVST+）
- ポート セキュリティ
- Cisco Trusted Security（CTS）
- Dynamic Host Configuration Protocol（DHCP）スヌーピング
- Network Access Control（NAC; ネットワーク アクセス コントロール）
- Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）
- IP Source Guard（IPSG; IP ソース ガード）
- Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピング
- Hot Standby Routing Protocol（HSRP; ホット スタンバイ ルーティング プロトコル）
- Protocol Independent Multicast（PIM; プロトコル独立マルチキャスト）
- Gateway Load-Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）
- 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お勧めします。

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お勧めします。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, Release 5.x*』を参照してください。

最後に、各 vPC ピア デバイス上で作業して、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 vPC 番号を割り当てます。vPC を作成するときには、最小限のトラフィックの中断が発生します。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*。

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 デバイスに接続しなければなりません。

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。最後に、各 vPC ピア デバイス上で作業して、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 vPC 番号を割り当てます。vPC を作成するときには、最小限のトラフィックの中断が発生します。

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 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 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。

コアへのすべてのリンクとすべての vPC ピア リンクが入っているトラック リストをそのオブジェクトとして作成します。このトラック リスト用の指定した vPC ドメインの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 トラッキングとトラック リストの設定方法については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。

オブジェクト トラッキングの設定方法については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。

（注）　オブジェクトトラッキング リストを設定するときには、必ず Boolean OR を使用してください。

1 つのモジュール上で vPC ピア リンクとコアへのリンクを設定するには、次の手順を実行します。

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。

```
n7k-1(config-if)# track 35 interface ethernet 8/35 line-protocol
n7k-1(config-track)# track 23 interface ethernet 8/33 line-protocol
n7k-1(config)# track 55 interface port-channel 100 line-protocol
```

ステップ 2　Boolean OR を使用して、トラック リスト内にすべてのインターフェイスを含むトラック リストを作成します。

```
n7k-1(config)# track 44 list boolean OR
n7k-1(config-track)# object 23
n7k-1(config-track)# object 35
n7k-1(config-track)# object 55
n7k-1(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。

```
n7k-1(config)# vpc domain 1
n7k-1(config-vpc-domain)# track 44
```

ステップ 4　次の例は、**show vpc brief** コマンドを使用して、トラック オブジェクトを表示する方法を示します。

```
n7k-1# 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
```

次の例は、**show track brief** コマンドを使用して、トラック オブジェクトに関する情報を表示する方法を示します。

```
n7k-1# 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

ここでは、次の内容について説明します。

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 と LACP については、第 6 章「ポート チャネルの設定」を参照してください）。

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お勧めします。この設定により、デバイス、単方向リンク、およびマルチホップ接続の間の互換性をより簡単に検出できるようになり、実行時の変更およびリンク障害に対してダイナミックな応答が可能になります。

vPC ピア リンクは、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 インターフェイスをサポートします。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。

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お勧めします。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なければなりません。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 は稼動しません。

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「フェールセイフ」メカニズムをスパニング ツリー プロトコル（STP）が提供する必要があります。vPC を初めて稼動させたときに、STP による再コンバージェンスが発生します。STP は、vPC ピア リンクを特殊なリンクとして扱い、常に vPC ピア リンクを STP のアクティブ トポロジに含めます。

すべての vPC ピア リンク インターフェイスを STP ネットワーク ポート タイプに設定して、すべての vPC リンク上で Bridge Assurance が自動的にイネーブルになるようにすることをお勧めします。また、vPC ピア リンク上ではどの STP 拡張機能もイネーブルにしないこともお勧めします。STP 拡張がすでに設定されている場合は何も問題は発生しませんが、これらを設定する必要はありません。

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 拡張機能と PVST シミュレーションの詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*』を参照してください。

（注）　パラメータのリストは、vPC ピア リンクの両サイドの vPC ピア デバイス上で同じになるように設定しなければなりません。これらの一致していなければならない必須設定については、「vPC ピア リンクの互換パラメータ」（P.7-12）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、「CFSoE」（P.7-21）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」（P.7-9）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お勧めします。

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しなければなりません。

- 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
  - Bridge Assurance の設定
  - ポート タイプの設定
  - ループ ガードの設定
- STP インターフェイス設定：
  - ポート タイプの設定
  - ループ ガード
  - ルート ガード

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

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

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, Release 5.x*』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お勧めします。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, Release 5.x*』を参照してください）。

vPC ピア スイッチ

vPC ピア スイッチ機能は、STP コンバージェンスに関連するパフォーマンス上の問題を解決するために、Cisco NX-OS 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、次のトポロジで使用できます。

- すべてのデバイスが vPC に属する純粋なピア スイッチ トポロジ。
- その設定内に vPC デバイスと非 vPC デバイスが混在するハイブリッド ピア スイッチ トポロジ。

STP 拡張機能と Rapid PVST+ の詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*』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、PIM SSM も BIDR on vPC もサポートしていません。Cisco NX-OS ソフトウェアは、PIM ASM on vPC 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 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 とマルチキャストに関する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, Release 5.x*』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、vPC ピア デバイスの片方だけがマルチキャスト 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 デバイスでの DR 情報を同期させます。vPC モードになっているときには、IGMP についてデュアル DR という概念があります。これは、vPC モードでないときは使用できないもので、両方の vPC ピア デバイスにピア間でマルチキャスト グループ情報を維持させます。

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しなければなりません。IGMP スヌーピングは、デフォルトで有効になっています。

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, Release 5.x*』を参照してください。

vPC ピア リンクとルーティング

First Hop Routing Protocols（FHRP; ファーストホップ冗長プロトコル）は、vPC と相互運用できます。Hot Standby Routing Protocol（HSRP; ホット スタンバイ ルーティング プロトコル）、Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）、および Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）のすべてが、vPCs 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お勧めします。

（注）　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 接続をイネーブルにし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作成については、第 4 章「レイヤ 3 インターフェイスの設定」を参照してください）。

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停止したり稼動したりするのを防ぐために、低いしきい値と高い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。

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。

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、お勧めできません。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 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 アドレスを設定しなければなりません。

Cisco NX-OS 4.2(1) から、ピアの隣接が形成されて VLAN インターフェイスがバックアップされるまで vPC の再稼動を遅らせる復元タイマーを設定できるようになりました。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。

（注） データ センターが停電した場合に、vPC が正常に稼動し始める前に HSRP がイネーブルになると、トラフィック損失が発生します。vPC が安定するまでの時間を確保するために、HSRP 遅延をイネーブルにする必要があります。HSRP 遅延とプリエンプション遅延の両方をイネーブルにすると、Cisco Nexus 7000 シリーズ デバイスは、両方のタイマーの時間が切れた後にレイヤ 2 スイッチングを有効にします。

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, Release 5.x*』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示します。

Cisco Fabric Services は、TCP/IP を介したデータの転送も行います。CFS over IP の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』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。

バーチャライゼーションのサポート

（注）　1 つの VDC 内に配置した各 vPC ドメインについて、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をプロビジョニングしなければなりません。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。

1 つの 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。このバージョンのソフトウェアは、VDC ごとに 1 つの vPC しかサポートしません。各 VDC で 1 ～ 4096 の番号を使用して、vPC に番号を付けることができます。これらの vPC 番号は、別の VDC 内で再利用できます。

（注）　VDC と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, Release 5.x*』を参照してください。

リロードでの vPC の復元

データ センターの停電時には、vPC を構成する両方の Cisco Nexus 7000 シリーズ デバイスがリロードされます。まれに、ピアの片方だけが復元できることがあります。リモート ピアとのハンドシェイクが実行されないと vPC ポート チャネルは稼動できないため、通信ができず、vPC は機能できません。

Cisco NX-OS Release 5.0(2) からは、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、ユーザによる設定が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動し始めるか、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 ロールを想定します。ソフトウェアが vPC を初期化し、そのローカル ポートを稼動させ始めます。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。

vPC 復元ピア 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、一貫性チェックが実行され、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、その下位互換性により、システムは正常に機能します。

（注）　ハイアベイラビリティ機能の詳細については、『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x*』を参照してください。

vPC のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	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。Cisco NX-OS のライセンス スキームの詳細については、『*Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x*』を参照してください。

注意事項および制約事項

vPC には、次の注意事項と制約事項があります。

- 1 つの vPC のすべてのポートが、同じ VDC 内になくてはなりません。
- vPC を設定するには、まず vPC をイネーブルにしなければなりません。
- 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なければなりません。
- vPC に入れられるのは、レイヤ 2 ポート チャネルだけです。
- 両方の vPC ピア デバイスを設定しなければなりません。設定が片方のデバイスから他方へ送信されることはありません。
- マルチレイヤ（バックツーバック）vPC を設定するには、それぞれの vPC に一意の vPC ドメイン ID を割り当てなければなりません。

- 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。互換性に関する推奨事項について、「vPC ピア リンクの互換パラメータ」（P.7-12）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、IPSG はサポートされていません。DHCP リレーはサポートされています。
- 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お勧めします。
- 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 環境で OSPF を設定する場合は、vPC ピアリンクが停止した場合のファースト OSPF コンバージェンスを確保するために、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 コマンドを使用してください。

```
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, Release 5.x*』を参照してください。

vPC の設定

（注） この手順を vPC ピア リンクの両側にある両方のデバイスで使用しなければなりません。両方の vPC ピア デバイスをこの手順で設定します。

ここでは、Command-Line Interface（CLI; コマンドライン インターフェイス）を使用して vPC を設定する方法を説明します。内容は次のとおりです。

- 「vPC ピア デバイス ロールの手動での設定」（P.7-38）
- 「シングルモジュール vPC でのトラッキング機能の設定」（P.7-40）
- 「リロード復元の設定」（P.7-41）
- 「vPC ピア スイッチの設定」（P.7-43）

（注）　Cisco IOS CLI を熟知している場合は、この機能の Cisco NX-OS コマンドと使用する Cisco IOS コマンドが異なる場合もある点に注意してください。

vPC のイネーブル化

vPC を設定して使用するには、その前に vPC 機能をイネーブルにしなければなりません。

作業を開始する前に

正しい VDC を開始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）。

手順の概要

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

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**feature vpc** 例： `switch(config)# feature vpc`	デバイスの vPC をイネーブルにします。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 4	**show feature** 例： switch# show feature	（任意）デバイス上でイネーブルになっている機能を表示します。
ステップ 5	**copy running-config startup-config** 例： switch# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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)#
```

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。

作業を開始する前に

正しい VDC を開始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）。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no feature vpc** 例： switch(config)# no feature vpc	デバイスの vPC をディセーブルにします。

	コマンド	目的
ステップ 3	**exit** 例： switch(config)# exit switch#	コンフィギュレーション モードを終了します。
ステップ 4	**show feature** 例： switch# show feature	（任意）デバイス上でイネーブルになっている機能を表示します。
ステップ 5	**copy running-config startup-config** 例： switch# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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)#
```

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。

作業を開始する前に

vPC 機能がイネーブルになっていることを確認します。

正しい VDC を開始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）。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vpc domain** *domain-id* 例： switch(config)# vpc domain 5 switch(config-vpc-domain)#	デバイス上に vPC ドメインを作成し、設定目的で vpc-domain コンフィギュレーション モードを開始します。デフォルトはありません。指定できる範囲は 1 ～ 1,000 です。
ステップ 3	**exit** 例： switch(config-vpc-domain)# exit switch(config)#	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	**show vpc brief** 例： switch# show vpc brief	（任意）各 vPC ドメインに関する簡単な情報を表示します。
ステップ 5	**copy running-config startup-config** 例： switch# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例は、vPC ドメインを作成する方法を示します。

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

次の例は、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方法を示します。

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

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） システムが vPC ピア リンクを形成するには、その前に vPC ピアキープアライブ リンクを設定しなければなりません。

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）　独立した Virtual Routing and Forwarding（VRF; 仮想ルーティング/転送）インスタンスを設定し、各 vPC ピア デバイスからのレイヤ 3 ポートを vPC ピアキープアライブ リンクの VRF に入れることをお勧めします。vPC ピアキープアライブ メッセージの送信にピア リンク自体を使用することはしないでください。VRF の作成と設定の方法については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。
ピアキープアライブ メッセージの送信元と宛先両方の IP アドレスが、ネットワーク上で固有になってい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。

作業を開始する前に

vPC 機能がイネーブルになっていることを確認します。

正しい VDC を開始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）。

手順の概要

1. **configure terminal**
2. **vpc domain** *domain-id*
3. **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**}]
4. **exit**
5. **show vpc statistics**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**vpc domain** *domain-id*
	
	例：
	`switch(config)# vpc domain 5`
	`switch(config-vpc-domain)#`
		デバイス上に vPC ドメインを作成し、設定目的で vpc-domain コンフィギュレーション モードを開始します。

	コマンド	目的

ステップ 3	**peer-keepalive destination** *ipaddress* [**hold-timeout** *secs* | **interval** *msecs* {**timeout** *secs*} | {**precedence** {*prec-value* | **network** | **internet** | **critical** | **flash-override** | **flash** | **immediate** **priority** | **routine**}} | **tos** {*tos-value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal**}} |**tos-byte** *tos-byte-value*} | **source** *ipaddress* | **vrf** {*name* | **management** **vpc-keepalive**}]
	
	例：
	`switch(config-vpc-domain)# peer-keepalive destination 172.28.230.85`
	`switch(config-vpc-domain)#`
		vPC ピアキープアライブ リンクのリモート エンドの IPv4 アドレスを設定します。
		（注） vPC ピアキープアライブ リンクを設定するまでは、vPC ピア リンクは形成されません。
		
		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お勧めします。VRF の作成と設定の詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。

ステップ 4	**exit**
	
	例：
	`switch(config-vpc-domain)# exit`
	`switch(config)#`
		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	**show vpc statistics** **例：** `switch# show vpc statistics`	（任意）キープアライブ メッセージの設定に関する情報を表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

VRF の設定方法の詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』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)# feature vpc
switch(config)# vpc domain 100
switch(config-vpc-domain)# peer-keepalive destination 172.168.1.2 source 172.168.1.1 vrf
vpc-keepalive
```

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。vPC ピア リンクとして指定するレイヤ 2 ポート チャネルはトランク モードに設定し、冗長性のために各 vPC ピア デバイス上で独立したモジュール上の 2 つのポートを使用することをお勧めします。

作業を開始する前に

vPC 機能がイネーブルになっていることを確認します。

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。

正しい VDC を開始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）。

手順の概要

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

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface port-channel** *channel-number*
	
	例：
	`switch(config)# interface port-channel 20`
	`switch(config-if)#`
		このデバイスの vPC ピア リンクとして使用するポート チャネルを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**vpc peer-link**
	
	例：
	`switch(config-if)# vpc peer-link`
	`switch(config-vpc-domain)#`
		選択したポート チャネルを vPC ピア リンクとして設定し、vpc-domain コンフィギュレーション モードを開始します。

ステップ 4	**exit**
	
	例：
	`switch(config-vpc-domain)# exit`
	`switch(config)#`
		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	**show vpc brief** 例： `switch# show vpc brief`	（任意）各 vPC に関する情報を表示します。vPC ピア リンクに関する情報も表示されます。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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)# vpc peer-link
switch(config-vpc-domain)#
```

vPC ピアゲートウェイの設定

Cisco NX-OS 4.2(1) から、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。

（注）　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しなければなりません。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。

作業を開始する前に

vPC 機能がイネーブルになっていることを確認します。

正しい VDC を開始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）。

手順の概要

1. **configure terminal**
2. **interface vlan** *vpc-interface-vlan-id*
3. **no ip redirects**
4. **vpc domain** *domain-id*
5. **peer-gateway**
6. **exit**
7. **show vpc brief**
8. **copy running-config startup-config**

手順の詳細

	コマンド	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 vlan** *vpc-interface-vlan-id*
	
	例：
	`switch(config)# interface vlan 10`
	`switch(config-if)#`
		vPC VLAN 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	**no ip redirects**
	
	例：
	`switch(config-if)# no ip redirects`
	`switch(config-vpc-domain)#`
		VLAN インターフェイスでの Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）リダイレクト メッセージの送信をディセーブルにします。

	コマンド	目的

ステップ 4	**vpc domain** *domain-id*
	
	例：
	`switch(config-if)# vpc domain 5`
	`switch(config-vpc-domain)#`
		vPC ドメインがまだ存在しなかった場合はそれを作成し、vpc-domain コンフィギュレーション モードを開始します。

ステップ 5	**peer-gateway**
	
	例：
	`switch(config-vpc-domain)# peer-gateway`
	`Note:`
	`------:: Disable IP redirects on all interface-vlans of this vPC domain for correct operation of this feature ::------`
		ピアのゲートウェイ MAC アドレスを宛先とするパケットのレイヤ 3 フォワーディングをイネーブルにします。

ステップ 6	**exit**
	
	例：
	`switch(config-vpc-domain)# exit`
	`switch(config)#`
		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	**show vpc brief** 例： `switch# show vpc brief`	（任意）各 vPC に関する情報を表示します。vPC ピア リンクに関する情報も表示されます。
ステップ 8	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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 上での一貫した設定については、「vPC ピア リンクの互換パラメータ」（P.7-12）を参照してください。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**show vpc consistency-parameters** {**global** | **interface port-channel** *channel-number*} 例： switch(config)# show vpc consistency-parameters global switch(config)#	すべての vPC インターフェイスの間で一貫していなければならない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）　冗長性のために vPC ドメインのダウンストリーム ポート チャネルを 2 つのデバイスに接続することをお勧めします。

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。最後に、各 vPC ピア デバイス上で作業して、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 vPC 番号を割り当てます。vPC を作成するときには、最小限のトラフィックの中断が発生します。

作業を開始する前に

vPC 機能がイネーブルになっていることを確認します。

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。

正しい VDC を開始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）。

手順の概要

1. **configure terminal**
2. **interface port-channel** *channel-number*
3. **vpc** *number*

4. **exit**
5. **show vpc brief**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface port-channel** *channel-number* 例： switch(config)# interface port-channel 20 switch(config-if)#	ダウンストリーム デバイスに接続するために vPC に入れるポート チャネルを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**vpc** *number* 例： switch(config-if)# vpc peer-link switch(config-vpc-domain)#	選択したポート チャネルを vPC に入れてダウンストリーム デバイスに接続するように設定します。これらのポート チャネルには、デバイス内の任意のモジュールを使用できます。指定できる範囲は 1 ～ 4096 です。 **（注）** vPC ピア デバイスからダウンストリーム デバイスに接続されているポート チャネルに割り当てる vPC 番号は、*両方の* vPC デバイスで同じで*なければなりません*。
ステップ 4	**exit** 例： switch(config-vpc-domain)# exit switch(config)#	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	**show vpc brief** 例： switch# show vpc brief	（任意）vPC に関する情報を表示します。
ステップ 6	**copy running-config startup-config** 例： switch# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例は、ダウンストリーム デバイスに接続されるポート チャネルを設定する方法を示します。

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

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 MAC アドレスは手動で設定することも可能です。

作業を開始する前に

vPC 機能がイネーブルになっていることを確認します。

正しい VDC を開始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）。

手順の概要

1. **configure terminal**
2. **vpc domain** *domain-id*
3. **system-mac** *mac-address*
4. **exit**
5. **show vpc role**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**vpc domain** *domain-id*
	
	例：
	`switch(config)# vpc domain 5`
	`switch(config-vpc-domain)#`
		設定する vPC ドメインの番号を入力します。vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**system-mac** *mac-address*
	
	例：
	`switch(config-vpc-domain)# system-mac 23fb.4ab5.4c4e`
	`switch(config-vpc-domain)#`
		指定した vPC ドメインに割り当てる MAC アドレスを aaaa.bbbb.cccc の形式で入力します。

ステップ 4	**exit**
	
	例：
	`switch(config-vpc-domain)# exit`
	`switch(config)#`
		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	目的
ステップ 5	**show vpc role** 例： switch# show vpc brief	（任意）vPC システム MAC アドレスを表示します。
ステップ 6	**copy running-config startup-config** 例： switch# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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
```

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 を実行している場合は、手動で vPC システム プライオリティを設定して、vPC ピア デバイスが確実に LACP 上のプライマリ デバイスになるようにすることをお勧めします。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設定してください。これらの値が一致していないと、vPC は稼動しません。

作業を開始する前に

vPC 機能がイネーブルになっていることを確認します。

正しい VDC を開始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）。

手順の概要

1. **configure terminal**
2. **vpc domain** *domain-id*
3. **system-priority** *priority*
4. **exit**
5. **show vpc role**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vpc domain** *domain-id* 例： switch(config)# vpc domain 5 switch(config-vpc-domain)#	設定する vPC ドメインの番号を入力します。vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	**system-priority** *priority* 例： switch(config-vpc-domain)# system-priority 4000 switch(config-vpc-domain)#	指定した vPC ドメインに割り当てるシステム プライオリティを入力します。指定できる値の範囲は、1 ～ 65535 です。デフォルト値は 32667 です。
ステップ 4	**exit** 例： switch(config-vpc-domain)# exit switch(config)#	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	**show vpc role** 例： switch# show vpc role	（任意）vPC システム プライオリティを表示します。
ステップ 6	**copy running-config startup-config** 例： switch# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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
```

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 リンクの両側を設定した後に、Cisco NX-OS ソフトウェアによってプライマリ vPC ピア デバイスとセカンダリ vPC ピア デバイスが選出されます。ただし、vPC のプライマリ デバイスとして特定の vPC ピア デバイスを選出したい場合もあるでしょう。その場合、プライマリ デバイスにする vPC ピア デバイスのロール値を手動でその他の vPC ピア デバイスより低い値に設定してください。

vPC は、ロール プリエンプションはサポートしません。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 デバイスが機能上 vPC プライマリ デバイスを引き継ぎます。ただし、以前のプライマリ vPC が再び稼動し始めても、元の動作ロールは復元されません。

作業を開始する前に

vPC 機能がイネーブルになっていることを確認します。

正しい VDC を開始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）。

手順の概要

1. **configure terminal**
2. **vpc domain** *domain-id*
3. **role priority** *priority*
4. **exit**
5. **show vpc role**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**vpc domain** *domain-id*
	
	例：
	`switch(config)# vpc domain 5`
	`switch(config-vpc-domain)#`
		設定する vPC ドメインの番号を入力します。vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**role priority** *priority*
	
	例：
	`switch(config-vpc-domain)# role priority 4000`
	`switch(config-vpc-domain)#`
		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。

ステップ 4	**exit**
	
	例：
	`switch(config-vpc-domain)# exit`
	`switch(config)#`
		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	**show vpc role** 例： `switch# show vpc role`	（任意）vPC システム プライオリティを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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 4000
```

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。

作業を開始する前に

vPC 機能がイネーブルになっていることを確認します。

正しい Virtual Device Context（VDC; 仮想デバイス コンテキスト）を開始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）。

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。

手順の概要

1. **configure terminal**
2. **vpc domain** *domain-id*
3. **track** *track-object-id*
4. **exit**
5. **show vpc**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**vpc domain** *domain-id*
	
	例：
	`switch(config)# vpc domain 5`
	`switch(config-vpc-domain)#`
		設定する vPC ドメインの番号を入力します。
		vpc-domain コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**track** *track-object-id* 例： switch(config-vpc-domain)# track object 23 switch(config-vpc-domain)#	以前に関連するインターフェイスで設定されたトラックリスト オブジェクトを vPC ドメインに追加します。オブジェクト トラッキングとトラック リストの設定方法については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。
ステップ 4	**exit** 例： switch(config-vpc-domain)# exit switch(config)#	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	**show vpc brief** 例： switch# show vpc brief	（任意）トラッキング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	**copy running-config startup-config** 例： switch# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例は、以前から設定されていたトラック リストオブジェクトを vPC ピア デバイス上の vPC ドメインに入れる方法を示します。

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

リロード復元の設定

停電が発生すると、vPC は、スイッチがリロードされてピアの隣接が形成されるのを待ちます。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。

作業を開始する前に

vPC 機能がイネーブルになっていることを確認します。

正しい VDC を開始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）。

手順の概要

1. **configure terminal**
2. **vpc domain** *domain-id*
3. **reload restore** [**delay** *time-out*]
4. **exit**
5. **show running-config vpc**
6. **show vpc consistency-parameters interface port-channel** *number*
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**vpc domain** *domain-id*
	
	例：
	`switch(config)# vpc domain 5`
	`switch(config-vpc-domain)#`
		設定する vPC ドメインの番号を入力します。vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**reload restore** [**delay** *time-out*] **例：** `switch(config-vpc-domain)# reload restore`	vPC をそのピアが機能しないことを前提として vPC を稼動させるように設定します。デフォルトの遅延は 240 秒です。タイムアウト遅延は、240 ～ 3600 秒の範囲内で設定できます。 vPC を標準の動作にリセットするには、このコマンドの **no** 形式を使用します。
ステップ 4	**exit**	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	**show running-config vpc** **例：** `switch# show running-config vpc`	（任意）vPC に関する情報、特にリロード ステータスを表示します。
ステップ 6	**show vpc consistency-parameters interface port-channel** *number* **例：** `switch# show vpc consistency-parameters interface port-channel 1`	（任意）指定したインターフェイスの vPC の一貫性パラメータに関する情報を表示します。
ステップ 7	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。 **（注）**　リロード機能がイネーブルになっていることを確認するには、この手順を実行します。

次の例は、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)# 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         -    -                   -
```

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。ここでは、次の内容について説明します。

- 「純粋な vPC ピア スイッチ トポロジの設定」（P.7-43）
- 「ハイブリッド vPC ピア スイッチ トポロジの設定」（P.7-44）

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。

作業を開始する前に

vPC 機能がイネーブルになっていることを確認します。

正しい VDC を開始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）。

手順の概要

1. **configure terminal**
2. **vpc domain** *domain-id*
3. **peer-switch**
4. **spanning-tree vlan** *vlan-range* **priority** *value*
5. **exit**
6. **show spanning-tree summary**
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vpc domain** *domain-id* 例： switch(config)# vpc domain 5 switch(config-vpc-domain)#	設定する vPC ドメインの番号を入力します。 vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	**peer-switch** 例： switch(config-vpc-domain)# peer-switch	vPC スイッチ ペアがレイヤ 2 トポロジ内で 1 つの STP ルートとして現れるようにします。 ピア スイッチ vPC トポロジをディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 4	**spanning-tree vlan** *vlan-range* **priority** *value* 例： switch(config)# spanning-tree vlan 1 priority 8192	VLAN のブリッジ プライオリティを設定します。有効な値は、4096 の倍数です。デフォルト値は 32768 です。
ステップ 5	**exit**	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	**show spanning-tree summary** 例： switch# show spanning-tree summary	（任意）スパニング ツリー ポートの状態の概要を表示します。これに、vPC ピア スイッチも含まれます。
ステップ 7	**copy running-config startup-config** 例： switch# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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（『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x*』を参照してください）を使用して STP VLAN ベースのロード バランシング条件を満たすように代表ブリッジ IC 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。

作業を開始する前に

vPC 機能がイネーブルになっていることを確認します。

正しい VDC を開始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）。

手順の概要

1. **configure terminal**
2. **spanning-tree pseudo-information**
3. **vlan** *vlan-range* **designated priority** *value*
4. **vlan** *vlan-range* **root priority** *value*
5. **vpc domain** *domain-id*
6. **peer-switch**
7. **exit**
8. **show spanning-tree summary**
9. **copy running-config startup-config**

手順の詳細

	コマンド	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	**spanning-tree pseudo-information**
	
	例：
	`switch(config)# spanning-tree pseudo-information`
	`switch(config-pseudo)#`
		スパニング ツリー疑似情報を設定します。

ステップ 3	**vlan** *vlan-id* **designated priority** *priority* 例： `switch(config-pseudo)# vlan 1 designated priority 8192`	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	**vlan** *vlan-id* **root priority** *priority* 例： `switch(config-pseudo)# vlan 1 root priority 4096`	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	**vpc domain** *domain-id*
	
	例：
	`switch(config)# vpc domain 5`
	`switch(config-vpc-domain)#`
		設定する vPC ドメインの番号を入力します。vpc-domain コンフィギュレーション モードを開始します。

ステップ 6	**peer-switch** 例： `switch(config-vpc-domain)# peer-switch`	vPC スイッチ ペアがレイヤ 2 トポロジ内で 1 つの STP ルートとして現れるようにします。 ピア スイッチ vPC トポロジをディセーブルにするには、このコマンドの **no** 形式を使用します。

	コマンド	目的
ステップ 7	**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	**show spanning-tree summary** 例： switch# show spanning-tree summary	（任意）スパニング ツリー ポートの状態の概要を表示します。これに、vPC ピア スイッチも含まれます。
ステップ 9	**copy running-config startup-config** 例： switch# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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)# exit
switch(config)# vpc domain 5
switch(config-vpc-domain)# peer-switch
```

vPC 設定の確認

vPC 設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show feature	vPC がイネーブルになっているかどうかを表示します。
show vpc brief	vPC に関する簡単な情報を表示します。
show vpc consistency-parameters	すべての vPC インターフェイスの間で一貫していなければならない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。

これらのコマンドの出力フィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x*』を参照してください。

vPC 統計情報の監視

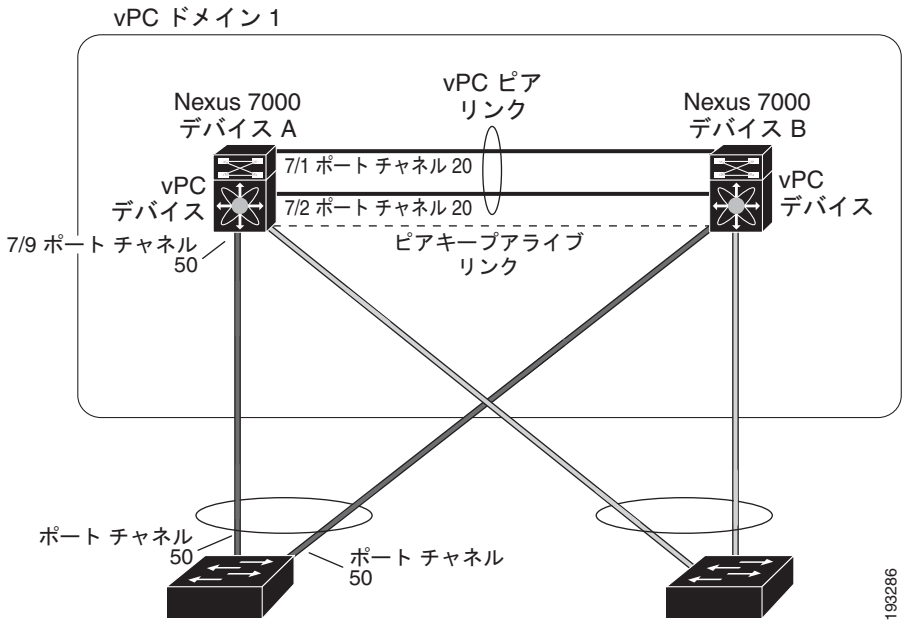
vPC 統計情報を表示するには、**show vpc statistics** コマンドを使用します。

（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、デバイス A 上で図 7-5 に示すとおりに vPC を設定する方法を示します。

図 7-5　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 VEF を作成し、レイヤ 3 インターフェイスをその VRF に追加します。

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

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)# 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。

デフォルト設定

表 7-1 に、vPC パラメータのデフォルト設定を示します。

表 7-1　デフォルト vPC パラメータ

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

その他の関連資料

vPC を実装する方法の詳細については、次の項目を参照してください。

- 「関連資料」（P.7-50）
- 「標準規格」（P.7-50）
- 「管理情報ベース（MIB）」（P.7-50）

関連資料

関連項目	参照先
ポート チャネルの設定	第 6 章「ポート チャネルの設定」
レイヤ 2 インターフェイスの設定	第 3 章「レイヤ 2 インターフェイスの設定」
レイヤ 3 インターフェイスの設定	第 4 章「レイヤ 3 インターフェイスの設定」
共有および専用ポート	第 2 章「基本インターフェイス パラメータの設定」
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x*』
インターフェイス	『*Cisco DCNM Interfaces Configuration Guide, Release 5.x*』
システム管理	『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』
ハイ アベイラビリティ	『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x*』
VDC	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x*』
リリース ノート	『*Cisco Nexus 7000 Series NX-OS Release Notes, Release 5.x*』

標準規格

標準規格	タイトル
IEEE 802.3ad	—

管理情報ベース（MIB）

管理情報ベース（MIB）	MIB リンク
• IEEE8023-LAG-CAPABILITY • CISCO-LAG-MIB	Management Information Base（MIB; 管理情報ベース）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

vPC の設定機能の履歴

表 7-2 は、この機能のリリースの履歴です。

表 7-2　vPC の設定機能の履歴

機能名	リリース	機能情報
vPC	4.1(2)	これらの機能が導入されました。
vPC	4.1(4)	サポートが 192 vPC にまで増えました。
vPC	4.2(1)	サポートが 256 vPC にまで増えました。

表 7-2　vPC の設定機能の履歴 （続き）

機能名	リリース	機能情報
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)	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動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)	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 デバイスの稼動を遅延させるための **delay restore** コマンドが追加されました。
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 を稼動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	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。

CHAPTER 8

IP トンネルの設定

この章では、Cisco Nexus 7000 シリーズ デバイスで Generic Route Encapsulation（GRE）を使って IP トンネルを設定する手順について説明します。

この章では、次の内容について説明します。

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レイヤ 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。

ここでは、次の内容について説明します。

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」（P.8-4）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 Release 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。コールバックとチェックポイントについては、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』を参照してください。

Cisco NX-OS Release 4.2 から、ある Virtual Device Context（VDC; 仮想デバイス コンテキスト）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。

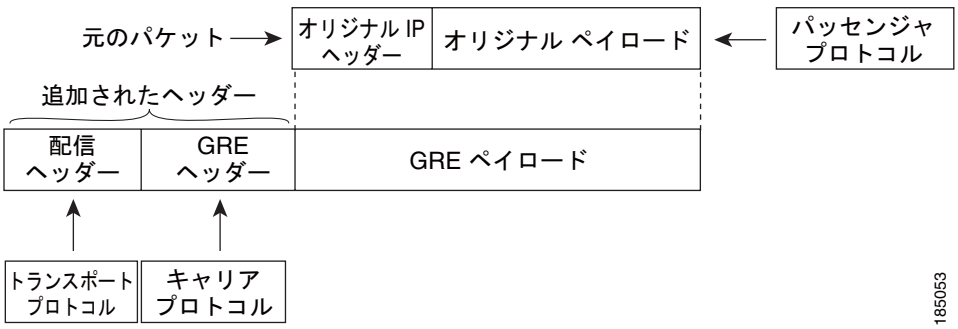
Cisco NX-OS Release 4.2 から、トンネル送信元 IP アドレスおよび宛先 IP アドレスは、同一の Virtual Routing and Forwarding（VRF; 仮想ルーティング / 転送）にある必要があります。

GRE トンネル

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。

図 8-1 に、GRE トンネルの IP トンネル コンポーネントを示します。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 8-1　GRE Protocol Data Unit（PDU）



Path MTU Discovery（PMTUD）

Path Maximum Transmission Unit（MTU; 最大伝送ユニット）Discovery（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 Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）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。

バーチャライゼーションのサポート

IP トンネルはデフォルトの Virtual Device Context（VDC; 仮想デバイス コンテキスト）およびデフォルトの Virtual Routing and Forwarding（VRF; 仮想ルーティング / 転送）インスタンスにだけ設定できます。

Cisco NX-OS Release 4.2 から、トンネル インターフェイスは Virtual Routing and Forwarding（VRF; 仮想ルーティング / 転送）インスタンスのメンバとして、および、VDC のメンバとして設定できます。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。

トンネル送信元 IP アドレスおよび宛先 IP アドレスは、同一の VRF にある必要があります。VRF がトンネル宛先の検索に何を使用するかも指定できます。この VRF は、トンネル送信元 IP アドレスの VRF と一致しなければなりません。

VDC については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x*』を、VRF については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』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。

IP トンネルのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	IP トンネルには Enterprise Services ライセンスが必要です。Cisco NX-OS ライセンス方式について、およびライセンスの取得方法と適用方法についての詳細については、『*Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x*』を参照してください。

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 オンしていること。
- 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。

注意事項および制約事項

IP トンネルには、次の注意事項と制約事項があります。

- 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 インターフェイスとトンネル転送の両方は、同一の VRF 内になければなりません。そうでない場合は、ハードウェア データ パスにエラーが発生します。

IP トンネルの設定

ここでは、次の内容について説明します。

（注） Cisco IOS CLI を熟知している場合は、この機能の Cisco NX-OS コマンドと使用する Cisco IOS コマンドが異なる場合もある点に注意してください。

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。

手順の概要

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

手順の詳細

	コマンド	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 tunnel** 例： `switch(config)# feature tunnel`	デバイスのトンネルをイネーブルにします。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show feature** 例： `switch# show feature`	（任意）デバイス上でイネーブルになっている機能を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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。

作業を開始する前に

トンネル インターフェイスとトンネル宛先の両方が、同一の VRF 内にあることが必要です。

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。

手順の概要

1. **configure terminal**
2. **interface tunnel** *number*
3. **tunnel source** {*ip-address* | *interface-name*}
4. **tunnel destination** {*ip-address* | *host-name*}
5. **tunnel use-vrf** *vrf-name*
6. **show interfaces tunnel** *number*
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface tunnel** *number*
	
	例：
	`switch(config)# interface tunnel 1`
	`switch(config-if)#`
		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	**tunnel source** {*ip-address* | *interface-name*} 例： `switch(config-if)# tunnel source ethernet 1/2`	この IP トンネルの送信元アドレスを設定します。
ステップ 4	**tunnel destination** {*ip-address* | *host-name*} 例： `switch(config-if)# tunnel destination 192.0.2.1`	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	**tunnel use-vrf** *vrf-name* 例： `switch(config-if)# tunnel vrf blue`	（任意）トンネル IP 宛先アドレスの検索に設定された VRF を使用します。
ステップ 6	**show interfaces tunnel** *number* 例： `switch(config-if)# show interfaces tunnel 1`	（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	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

トンネル インターフェイスおよびすべての関連する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* **例：** `switch(config)# no interface tunnel 1`	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。

次のパラメータを任意に設定し、インターフェイス コンフィギュレーション モードでトンネルを調整します。

コマンド	目的
description *string* **例：** `switch(config-if)# description GRE tunnel`	トンネルの説明を設定します。
mtu *value* **例：** `switch(config-if)# mtu 1400`	インターフェイス上で送信する IP パケットの MTU を設定します。
tunnel ttl *value* **例：** `switch(config-if)# tunnel ttl 100`	トンネルの Time-to-Live（TTL; 存続可能時間）値を設定します。有効な範囲は 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。

作業を開始する前に

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。

手順の概要

1. **configure terminal**
2. **interface tunnel** *number*
3. **tunnel mode gre ip**
4. **show interfaces tunnel** *number*
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface tunnel** *number* 例： switch(config)# interface tunnel 1 switch(config-if)#	トンネル 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	**tunnel mode gre ip** 例： 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	**show interfaces tunnel** *number* 例： switch(config-if)# show interfaces tunnel 1	（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	**copy running-config startup-config** 例： switch(config-if)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、トンネル インターフェイスに GRE を設定し、GRE トンネルにキープアライブを設定する方法を示します。

```
switch# configure terminal
switch(config)# interface tunnel 1
switch(config-if)# tunnel mode gre ip
switch(config-if)# copy running-config startup-config
```

Path MTU Discovery のイネーブル化

トンネルの Path MTU Discovery をイネーブルにするには、インターフェイス コンフィギュレーション モードで **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*] 例： switch(config-if)# tunnel path-mtu-discovery 25 1500	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。次のパラメータがあります。 • *mins* : 分数を指定します。有効な範囲は 10 ～ 30 です。デフォルトは 10 です。 • *mtu-bytes* : 認識される最小 MTU。有効な範囲は 92 ～ 65535 です。デフォルトは 92 です。

トンネル インターフェイスに割り当てる VRF メンバシップ

VRF にトンネル インターフェイスを追加できます。

作業を開始する前に

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 を開始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 にインターフェイスを設定してから、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。

手順の概要

1. **configure terminal**
2. **interface tunnel** *number*
3. **vrf member** *vrf-name*
4. **ip-address** *ip-prefix/length*
5. **show vrf** [*vrf-name*] **interface** *interface-type number*
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface tunnel** *number*
	
	例：
	`switch(config)# interface tunnel 0`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**vrf member** *vrf-name* 例： `switch(config-if)# vrf member RemoteOfficeVRF`	このインターフェイスを VRF に追加します。
ステップ 4	**ip address** *ip-prefix/length* 例： `switch(config-if)# ip address 192.0.2.1/16`	このインターフェイスに 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 に割り当ててから実行します。

	コマンド	目的
ステップ 5	**show vrf** [*vrf-name*] **interface** *interface-type number* **例：** `switch(config-vrf)# show vrf Enterprise interface tunnel 0`	（任意）VRF の内容を表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）この設定の変更を保存します。

次に、トンネル インターフェイスを VRF に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 トンネル設定情報の確認

IP トンネルの設定情報を表示するには、次のコマンドを使用します。

コマンド	目的
show interface 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、トランスポート、VRF）。入力および出力パケット、バイト、パケット レートを表示します。
show interface tunnel *number* **brief**	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ている説明を表示します。
show interface tunnel *number* **status**	トンネル インターフェイスの動作状態を表示します。
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。

IP トンネルの設定例

次に、簡単な GRE トンネルの例を示します。イーサネット 1/2 はルータ A のトンネル送信元およびルータ 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 のトンネル送信元およびルータ 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
```

デフォルト設定

表 8-1 に、IP トンネル パラメータのデフォルト設定を示します。

表 8-1　デフォルトの IP トンネル パラメータ

パラメータ	デフォルト
Path MTU Discovery 経過時間タイマー	10 分
Path MTU Discovery 最小 MTU	64
トンネル機能	ディセーブル

その他の関連資料

IP トンネルの実装に関する追加情報については、次の項を参照してください。

- 「関連資料」（P.8-11）
- 「標準規格」（P.8-12）

関連資料

関連項目	参照先
IP トンネル コマンド	『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x*』
IP フラグメンテーションおよび Path MTU Discovery	『*Resolve IP Fragmentation, MTU, MSS, and PMTUD Issues with GRE and IPSEC*』

標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

IP トンネル設定の機能履歴

表 8-2 は、この機能のリリースの履歴です。

表 8-2　IP トンネル設定の機能履歴

機能名	リリース	機能情報
IP トンネル	4.0(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。

CHAPTER 9

Q-in-Q VLAN トンネルの設定

ここでは、Cisco Nexus 7000 シリーズ デバイスでの 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 トンネリングの設定方法について説明します。

この章では、次の内容について説明します。

Q-in-Q トンネルについて

Q-in-Q VLAN トンネルにより、サービス プロバイダーは、既存のタグ付きフレームに第 2 の 802.1Q タグを付加することで、自社のインフラストラクチャ内の異なるカスタマーのトラフィックを分離したまま、カスタマーには内部利用のために VLAN を完全に利用させることができます。

ここでは、次の内容について説明します。

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、しばしば、サポートされる VLAN ID と VLAN の数に固有の要件があります。同一のサービス プロバイダー ネットワークを使用する異なるカスタマーが要求する VLAN 範囲が重なり、インフラストラクチャを通過するカスタマーのトラフィックが混在することもありえます。各カスタマーに一意の VLAN ID 範囲を割り当てることは、カスタマーのコンフィギュレーションを制限することになり、また、802.1Q 仕様の VLAN 制限である 4096 を容易に超えてしまいます。

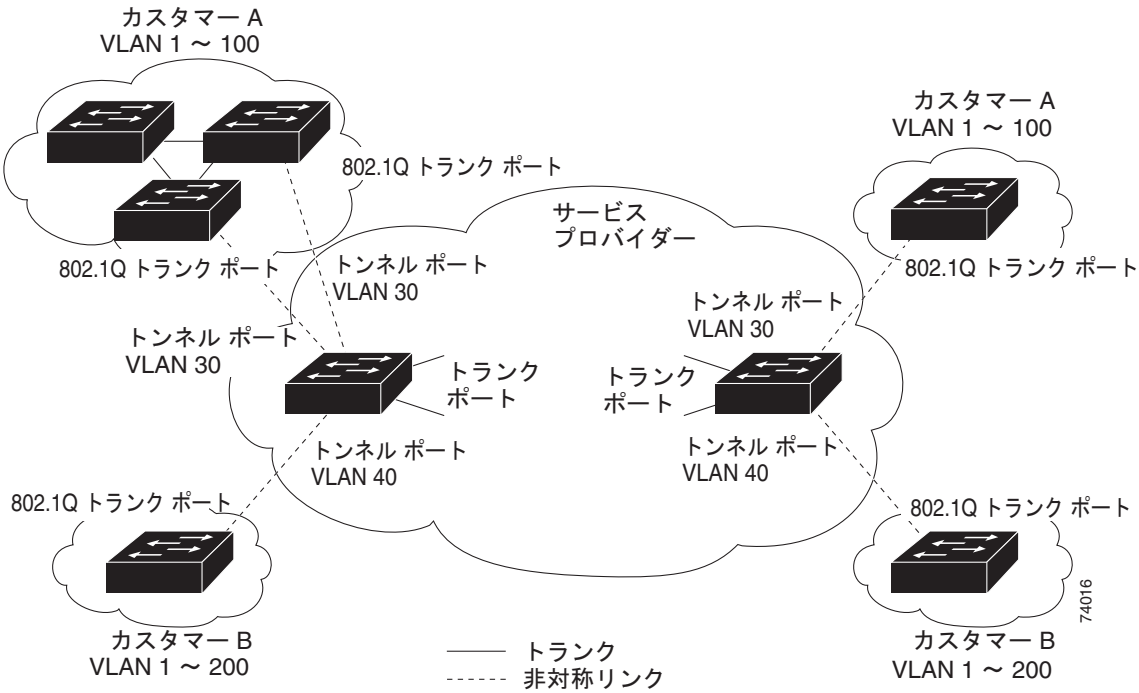
（注）　Q-in-Q は、ポート チャネルおよび Virtual Port Channel（vPC; 仮想ポート チャネル）でサポートされます。ポート チャネルを非対称リンクとして設定するには、ポート チャネルのすべてのポートが同一のトンネリング設定であることが必要です。

802.1Q トンネリング機能により、サービス プロバイダーは 1 つの VLAN を使用して、複数の VLAN を所有する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。802.1Q トンネリングは、VLAN 内 VLAN 階層構造を使用しタグ付きパケットをタグ付けして VLAN スペースを拡張します。802.1Q トンネリングをサポートとするように設定されたポートを *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は、トンネル ポートをトンネリング専用の VLAN に割り当てます。各カスタマーには個別の VLAN が 1 つ必要ですが、この VLAN はカスタマーの VLAN をすべてサポートします。

適切な VLAN ID を使用して通常の方法でタグ付けされたカスタマー トラフィックは、カスタマー デバイス上の 802.1Q トランク ポートから発信し、トンネル ポートを経由して、サービス プロバイダーのエッジ スイッチに着信します。カスタマー デバイスとエッジ スイッチの間のリンクは、一端が 802.1Q トランク ポートとして設定され、もう一端がトンネルポートとして設定されていることから、*非対象リンク*と呼ばれます。カスタマーごとに一意であるアクセス VLAN ID に、トンネル ポート インターフェイスを割り当てます。図 9-1 を参照してください。

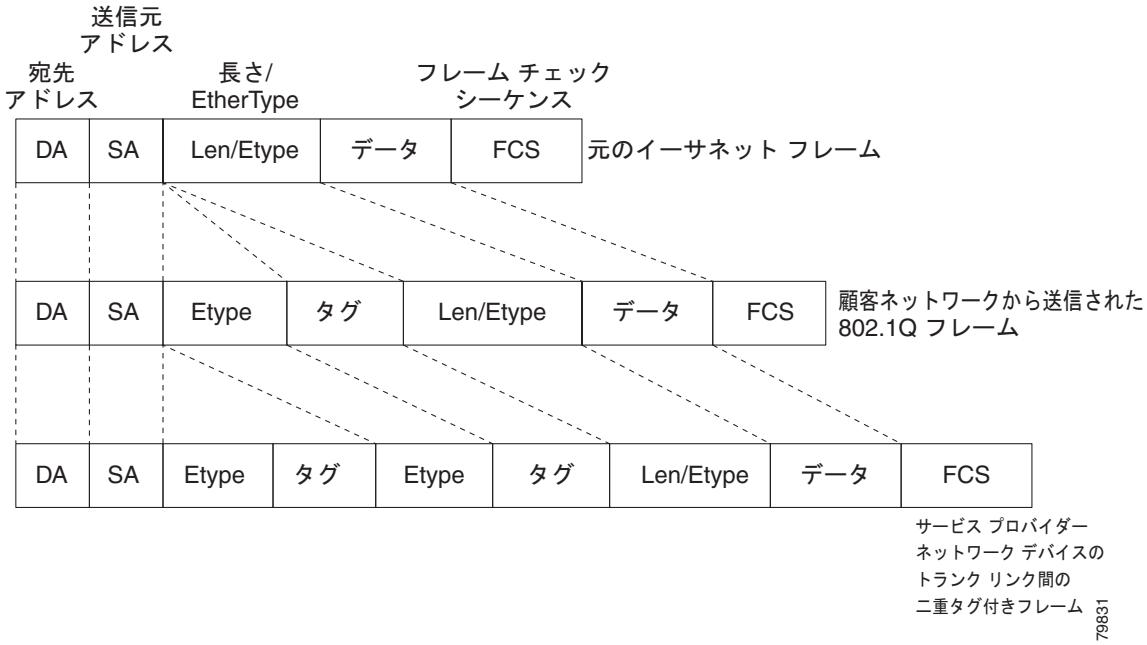
（注）　選択的 Q-in-Q トンネリングはサポートされません。トンネル ポートに入るフレームはすべて、Q-in-Q タギングされます。

図 9-1　802.1Q-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 ポートに入るパケットは適切な VLAN ID を使用して 802.1Q タグ付けされており、カスタマーに一意の 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 プロバイダーのインフラストラクチャに入るパケットは、二重にタグ付けされています。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、タグ スタック、二重 Q、または、Q-in-Q と呼ばれ、図 9-2 に示すとおりです。

図 9-2　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



この方法を使用することで、外部タグの VLAN ID スペースが、内部タグの VLAN ID スペースと無関係になります。1 つの外部 VLAN ID で、個別のカスタマーの VLAN ID スペース全体を表すことができます。この技術によって、カスタマーのレイヤ 2 ネットワークはサービス プロバイダー ネットワーク全体に広がり、複数のサイトにわたる仮想 LAN インフラストラクチャの構築が可能になります。

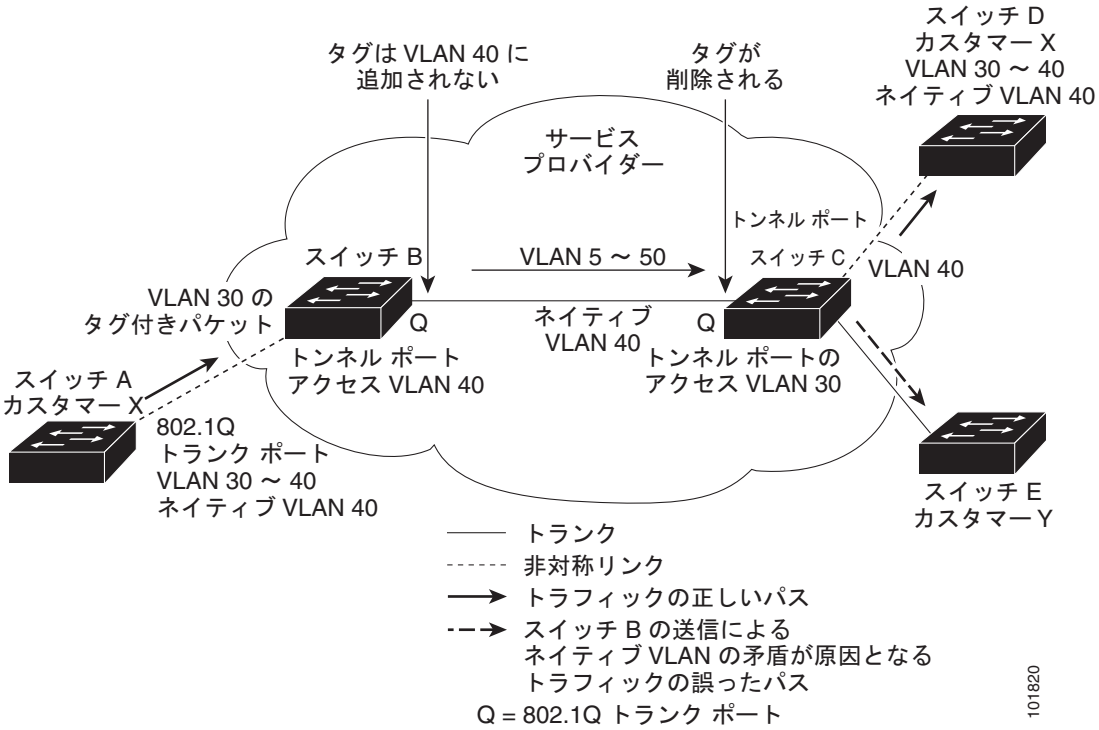
（注）　階層的タギング、つまり、マルチレベル dot1q タギング Q-in-Q はサポートされません。

ネイティブ VLAN ハザード

エッジ スイッチに 802.1Q トンネリングを設定する場合、パケットをサービス プロバイダー ネットワークに送出するために 802.1Q トランク ポートを使用する必要があります。しかし、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、802.1Q トランクや、ISL トランク、非トランキング リンクによって伝送されることがあります。これらのコア スイッチで 802.1Q トランクが使用されている場合、ネイティブ VLAN のトラフィックは 802.1Q 送信トランク ポートでタグ付けされていないため、802.1Q トランクのネイティブ VLAN は、同一のスイッチ上の dot1q トンネル ポートのネイティブ VLAN と一致してはなりません。

図 9-3 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）で接続している、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 のタグ付けされたパケットを、サービス プロバイダー ネットワーク内のアクセス VLAN 40 に属するスイッチ 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 トランク ポートのネイティブ VLAN（VLAN 40）と同じであるため、トンネル ポートから受信したタグ付けされたパケットに 802.1Q タグは付加されません。パケットは VLAN 30 タグだけを伝送したままサービス プロバイダー ネットワークを経由して出力エッジ スイッチ（スイッチ C）のトランク ポートに到達するため、出力スイッチ トンネル ポートを通じて誤ってカスタマー Y へ送出されます。

図 9-3　　ネイティブ VLAN ハザード



ネイティブ VLAN 問題を解決する方法は次の 2 つです。

- ネイティブ VLAN を含め、802.1Q トランクへ送出されるすべてのパケットがタグ付けされるように、**vlan dot1q tag native** コマンドを使用してエッジ スイッチを設定します。すべての 802.1Q トランクのネイティブ VLAN パケットにタグ付けするようにスイッチが設定されている場合、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 トランク ポートのネイティブ VLAN ID が、カスタマー VLAN 範囲内でないことを確認します。たとえば、トランク ポートが VLAN 100 ～ 200 のトラフィックを伝送するとき、ネイティブ VLAN にその範囲外の番号を割り当てます。

レイヤ 2 プロトコル トンネリングについて

サービス プロバイダー ネットワークで接続された異なるサイトを持つカスタマーは、トポロジを拡大してすべてのリモート サイトおよびローカル サイトを含めるために、さまざまなレイヤ 2 プロトコルを実行する必要があります。Spanning Tree Protocol（STP; スパニング ツリー プロトコル）を適切に実行し、すべての VLAN が、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に広がる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 サイトからネイバー シスコ デバイスを検出できる必要があります。また、VLAN Trunking Protocol（VTP）は、カスタマー ネットワークのすべてのサイト全体にわたって一貫した VLAN コンフィギュレーションを提供する必要があります。

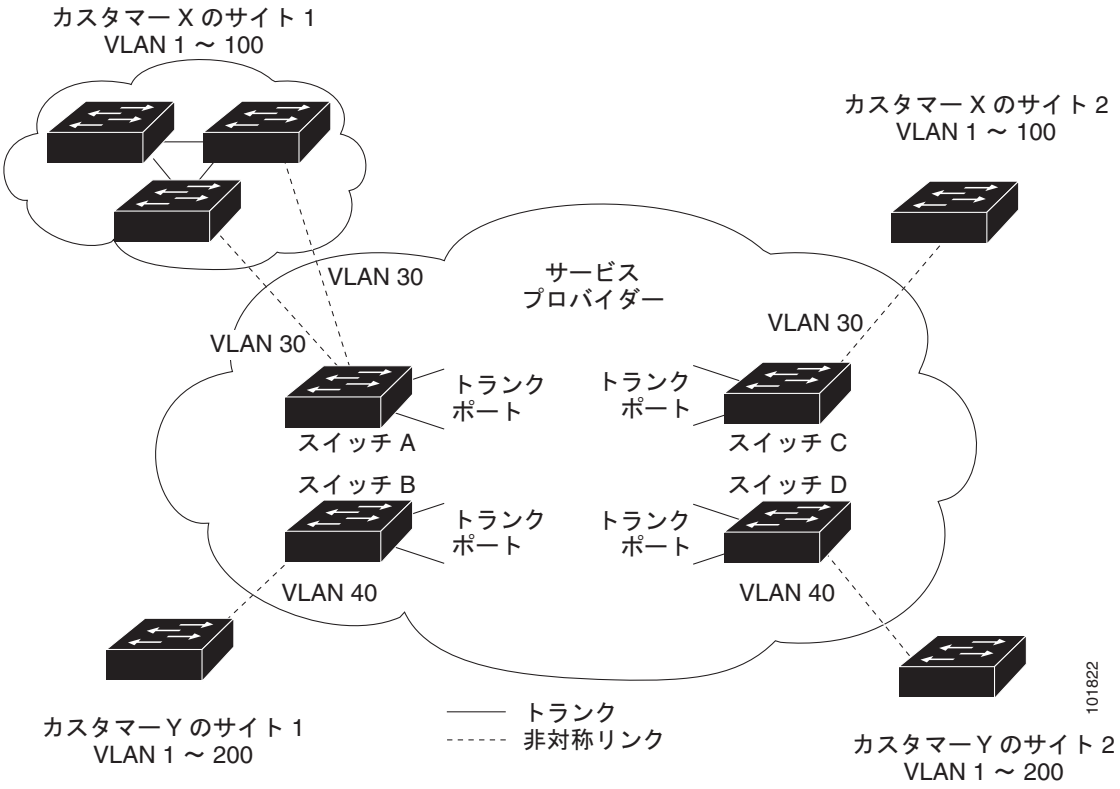
プロトコル トンネリングがイネーブルになると、サービス プロバイダー インフラストラクチャの受信側にあるエッジ スイッチが、レイヤ 2 プロトコルを特別の Media Access Control（MAC; メディア アクセス制御）アドレスでカプセル化し、サービス プロバイダー ネットワークの端まで送信します。ネットワークのコア スイッチはこれらのパケットを処理せず、通常のパケットと同様に転送します。CDP、STP、または、VTP 用の Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）は、サービス プロバイダー インフラストラクチャを経由して、サービス プロバイダー ネットワークの送信側にあるカスタマー スイッチへ配信されます。同一の VLAN にすべてのカスタマー ポートが、同一のパケットを受信します。

802.1Q トンネリング ポートでプロトコル トンネリングがイネーブルでない場合、サービス プロバイダー ネットワークの受信側の端にあるリモート スイッチは、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 トンネリングがイネーブルである場合、各カスタマー 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 ネットワーク内で実行されているプロトコルから完全に分離されます。802.1Q トンネリングを使用してサービス プロバイダー ネットワークを経由してトラフィックを送信する異なるサイトのカスタマー スイッチは、カスタマー VLAN の情報を完全に取得します。

（注）　Layer 2 プロトコル トンネリングは、ソフトウェアのトンネリング BPDU によって機能します。SUP に到着する大量の BPDU は、CPU 負荷の増大の原因となります。SUP CPU の負荷を削減するために、ハードウェア レート リミッタを使用する必要がある可能性があります。「レイヤ 2 プロトコル トンネル ポートのレート リミットの設定」（P.9-13）を参照してください。

たとえば、図 9-4 では、カスタマー X には、同一の VLAN にサービス プロバイダー ネットワークを経由して接続された 4 個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場合、ネットワークの遠端にあるスイッチは、STP、CDP、802.1X、および VTP プロトコルを正しく実行できません。

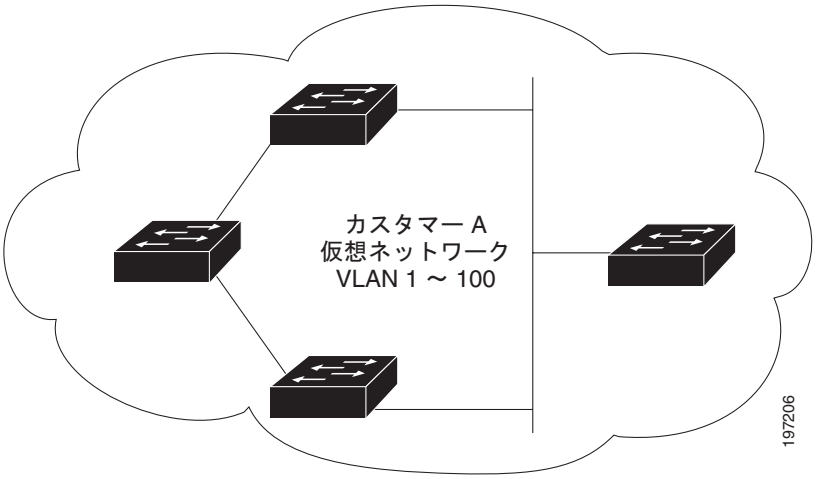
図 9-4　レイヤ 2 プロトコル トンネリング



前述の例では、カスタマー X のサイト 1 にあるスイッチ上の VLAN の STP は、そのサイトのスイッチ上に、カスタマー X のサイト 2 のスイッチに基づくコンバージェンス パラメータを考慮することなくスパニング ツリーを構築します。

図 9-5 に、BPDU トンネリングがイネーブルでない場合に、結果として得られるカスタマー ネットワークのトポロジを示します。

図 9-5　BPDU トンネリングがない場合の仮想ネットワーク トポロジ



Q-in-Q トンネルのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	802.1Q-in-Q VLAN トンネリング、および L2 プロトコル トンネリングに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。Cisco NX-OS のライセンス スキームの詳細については、『*Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x*』を参照してください。

注意事項および制約事項

Q-in-Q トンネリングおよびレイヤ 2 トンネリングには、次の注意事項と制約事項があります。

- サービス プロバイダー ネットワークのスイッチは、Q-in-Q タギングによって生じる Maximum Transmission Unit（MTU; 最大伝送ユニット）サイズの増加に対処するように設定される必要があります。
- Q-in-Q タグ付きパケットの MAC アドレス学習は、外部 VLAN（サービス プロバイダー VLAN）タグに基づきます。パケット転送問題は、1 つの MAC アドレスが複数の内部（カスタマー）VLAN にわたって使用される配置で発生します。
- レイヤ 3 以上のパラメータは、トンネル トラフィック内では識別できません（たとえば、レイヤ 3 宛先および送信元アドレス）。トンネル化された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 デバイスは、トンネル トラフィックの MAC レイヤ ACL/QoS（VLAN ID および送信元/宛先 MAC アドレス）しか実現できません。
- MAC アドレス ベースのフレーム配信を使用しなければなりません。
- 非対称リンクでは、リンク上の 1 つのポートだけがトランクになるため、Dynamic Trunking Protocol（DTP）をサポートしません。無条件に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上で、802.1Q トンネリング機能を設定できません。プライベート VLAN はこれらの配置には必要ありません。
- トンネル VLAN 上の Internet Group Management Protocol（IGMP）スヌーピングをディセーブルにする必要があります。
- Control Plane Policing（CoPP; コントロール プレーン ポリシング）はサポートされません。
- **vlan dot1Q tag native** コマンドを実行して、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ドロップする必要があります。これによって、ネイティブ VLAN の誤設定を防止できます。
- 手動で、802.1Q インターフェイスをエッジ ポートになるよう設定する必要があります。
- リリース 5.0(2) の場合、Dot1x トンネリングはサポートされません。
- 一部の Cisco Nexus デバイスに対して EtherType コンフィギュレーションを有効にするために、EPLD アップグレードを実行して、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。

Q-in-Q トンネルおよびレイヤ 2 プロトコル トンネリングの設定

ここでは、Cisco Nexus 7000 シリーズ デバイスでの Q-in-Q トンネルおよびレイヤ 2 プロトコル トンネリングの設定方法について説明します。

ここでは、次の内容について説明します。

（注）　Cisco IOS CLI を熟知している場合は、この機能の Cisco NX-OS コマンドと使用する Cisco IOS コマンドが異なる場合もある点に注意してください。

802.1Q トンネル ポートの作成

switchport mode コマンドを使用して、dot1q トンネル ポートを作成します。

（注）　リリース 5.0(2) の場合、**spanning-tree port type edge** コマンドを使用して、802.1Q トンネル ポートをエッジ ポートに設定する必要があります。ポートの VLAN メンバシップは、**switchport access vlan** *vlan-id* コマンドを使用して変更されます。

dot1q トンネル 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 パケットの Q-in-Q トンネルの通過を許可する必要があります。

作業を開始する前に

最初に、インターフェイスをスイッチポートとして設定する必要があります。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **switchport**
4. **switchport mode dot1q-tunnel**
5. **no switchport mode dot1q-tunnel**
6. **exit**
7. **show dot1q-tunnel [interface** *if-range***]**
8. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface ethernet** *slot/port* 例： switch(config)# **interface ethernet 7/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport** 例： 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	**switchport mode dot1q-tunnel** 例： 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 モードが変更されると、ポートがダウンになり、再初期化（ポート フラップ）されます。BPDU フィルタリングがイネーブルにされ、トンネル インターフェイスの CDP がディセーブルにされます。
ステップ 5	**no switchport mode** 例： switch(config-if)# **no switchport mode**	（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	**exit** 例： switch(config-if)# **exit** 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 7	**show dot1q-tunnel** [**interface** *if-range*] 例： switch# **show dot1q-tunnel**	（任意）dot1q トンネル モードのポートをすべて表示します。オプションで、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	**copy running-config startup-config** 例： switch# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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 の EtherType の変更

Q-in-Q カプセル化に使用する 802.1Q EtherType 値を変更できます。

（注） 二重タグ付き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）にだけ、EtherType を設定する必要があります。トランクの一方の EtherType を変更する場合、トランクのもう一方の端でも同じ値を設定する必要があります（対称型コンフィギュレーション）。

注意 設定する EtherType 値は、（Q-in-Q パケットだけでなく）そのインターフェイスから送出されるタグ付きパケットすべてに影響を与えます。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **switchport**
4. **switchport dot1q ethertype** *value*
5. **no switchport dot1q ethertype**
6. **exit**
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface ethernet** *slot/port* 例： switch(config)# **interface ethernet 7/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport** 例： 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	**switchport dot1q ethertype** *value* 例： switch(config-if)# **switchport dot1q ethertype 0x9100**	ポートの Q-in-Q トンネルの EtherType を設定します。
ステップ 5	**no switchport dot1q ethertype** 例： switch(config-if)# **no switchport dot1q ethertype**	（任意）ポートの EtherType をデフォルト値の 0x8100 にリセットします。

	コマンド	目的
ステップ 6	**exit** 例： switch(config-if)# **exit** 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 7	**copy running-config startup-config** 例： switch# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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 トンネリングをイネーブルにできます。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot*/*port*
3. **switchport**
4. **switchport mode dot1q-tunnel**
5. **l2protocol tunnel [cdp | stp | vtp]**
6. **no l2protocol tunnel [cdp | stp | vtp]**
7. **exit**
8. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface ethernet** *slot*/*port* 例： switch(config)# **interface ethernet 7/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**switchport** 例： `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	**switchport mode dot1q-tunnel** 例： `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	**l2protocol tunnel** [**cdp** | **stp** | **vtp**] 例： `switch(config-if)# l2protocol tunnel stp`	レイヤ 2 プロトコル トンネリングをイネーブルにします。オプションで、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	**no l2protocol tunnel** [**cdp** | **stp** | **vtp**] 例： `switch(config-if)# no l2protocol tunnel`	（任意）プロトコル トンネリングをディセーブルにします。

ステップ 7	**exit**
	
	例：
	`switch(config-if)# exit`
	`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 8	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、802.1Q トンネル ポートでプロトコル トンネリングをイネーブルにする方法を示します。

```
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 ポートのグローバル サービス クラス（CoS）の設定

トンネル ポートの入力 BPDU を指定されたクラスでカプセル化するために、Class of Service（CoS; サービス クラス）値をグローバルに指定できます。

手順の概要

1. **configure terminal**
2. **l2protocol tunnel cos** *value*
3. **no l2protocol tunnel cos**
4. **exit**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**l2protocol tunnel cos** *cos-value* 例： switch(config)# **l2protocol tunnel cos 6**	レイヤ 2 プロトコル トンネリング ポートのグローバル CoS 値を指定します。デフォルトの CoS 値は 5 です。
ステップ 3	**no l2protocol tunnel cos** 例： switch(config)# **no l2protocol tunnel cos**	（任意）グローバル CoS 値をデフォルトに設定します。
ステップ 4	**exit** 例： 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 5	**copy running-config startup-config** 例： switch# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、レイヤ 2 プロトコル トンネリングのためにグローバル 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 リミットの設定

レイヤ 2 プロトコル トンネリングのハードウェア レート リミッタ コンフィギュレーションを指定できます。デフォルトは、毎秒 500 パケットです。負荷、またはカスタマー用にトンネリングされる VLAN の数に応じて、この値を調整して、カスタマーのネットワークでの STP エラーを防止する必要があります。

手順の概要

1. **configure terminal**
2. **hardware rate-limiter layer-2 l2pt** *packets-per-sec*
3. **no hardware rate-limiter layer-2 l2pt**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**hardware rate-limiter layer-2 l2pt** *packets-per-second* 例： switch(config)# **hardware rate-limiter layer-2 l2pt 4096**	それを上回る dot1q トンネル ポートからの受信プロトコルはハードウェアでドロップされるように、1 秒あたりのパケット数のしきい値を設定します。指定できる範囲は 0 ～ 30000 です。
ステップ 3	**no hardware rate-limiter layer-2 l2pt** 例： switch(config)# **no hardware rate-limiter layer-2 l2pt**	（任意）しきい値をデフォルト値の毎秒 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 トンネリングのポートのドロップ値およびシャットダウン値を指定できます。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **switchport**
4. **switchport mode dot1q-tunnel**
5. **l2protocol tunnel drop-threshold [cdp | stp | vtp]** *packets-per-sec*
6. **no l2protocol tunnel drop-threshold [cdp | stp | vtp]**
7. **l2protocol tunnel shutdown-threshold [cdp | stp | vtp]** *packets-per-sec*
8. **no l2protocol tunnel shutdown-threshold [cdp | stp | vtp]**
9. **exit**
10. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface ethernet** *slot/port* 例： switch(config)# **interface ethernet 7/1**	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**switchport** 例： 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	**switchport mode dot1q-tunnel** 例： 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	**l2protocol tunnel drop-threshold** [**cdp** | **stp** | **vtp**] *packets-per-sec* 例： switch(config)# **l2protocol tunnel drop-threshold 3000**	ドロップ以前にインターフェイスで処理できるパケットの最大数を指定します。オプションで、CDP、STP、または VTP を指定できます。パケット数に有効な値は、1 ～ 4096 です。
ステップ 6	**no l2protocol tunnel drop-threshold** [**cdp** | **stp** | **vtp**] 例： switch(config)# **no l2protocol tunnel drop-threshold**	（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	**l2protocol tunnel shutdown-threshold** [**cdp** | **stp** | **vtp**] *packets-per-sec* 例： switch(config)# **l2protocol tunnel shutdown-threshold 3000**	インターフェイスで処理できるパケットの最大数を指定します。パケット数がこれを超えると、ポートは error-disabled 状態になります。オプションで、CDP、STP、または VTP を指定できます。パケット数に有効な値は、1 ～ 4096 です。
ステップ 8	**no l2protocol tunnel shutdown-threshold** [**cdp** | **stp** | **vtp**] 例： switch(config)# **no l2protocol tunnel shutdown-threshold**	（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	**exit** 例： 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 10	**copy running-config startup-config** 例： switch# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

設定の確認

Q-in-Q トンネルおよびレイヤ 2 プロトコル トンネリングの設定情報を表示するには、次のコマンドを使用します。

コマンド	目的
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。

コマンド	目的
show l2protocol tunnel [**interface** *if-range* | **vlan** *vlan-id*]	インターフェイス範囲、または指定された VLAN の一部またはすべてのインターフェイスのすべての dot1q トンネル インターフェイスに対してレイヤ 2 プロトコル トンネル情報が表示されます。
show l2protocol tunnel summary	レイヤ 2 プロトコル トンネル コンフィギュレーションを持つすべてのポートの要約が表示されます。
show running-config l2pt	現在のレイヤ 2 プロトコル トンネル実行コンフィギュレーションが表示されます。

設定例

次に、Ethernet 7/1 の受信トラフィックの Q-in-Q を処理するように設定されたサービス プロバイダー スイッチの例を示します。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。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#
```

Q-in-Q トンネルおよびレイヤ 2 プロトコル トンネリングの機能履歴

表 9-1 は、この機能のリリースの履歴です。

表 9-1　Q-in-Q トンネルおよびレイヤ 2 プロトコル トンネリングの機能履歴

機能名	リリース	機能情報
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 トンネリング	5.0(2)	この機能が導入されました。

APPENDIX A

Cisco NX-OS インターフェイスがサポートする IETF RFC

ここでは、Cisco Nexus 7000 シリーズ NX-OS Release 5.x でサポートするインターフェイスに関する Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）Request for Comments（RFC）を示します。

IPv6 に関する RFC の参考資料

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*』
RFC 2590	『*Transmission of IPv6 Packets over Frame Relay Networks Specification*』
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*』

APPENDIX B

Cisco NX-OS インターフェイスの設定制限

Cisco NX-OS がサポートする機能には最大設定制限があります。一部の機能については、最大値に達していない制限値をサポートする設定を検証しました。表 B-1 に、Cisco NX--OS Release 5.x が稼動するスイッチで、シスコが確認した制限値および最大制限値を示します。

表 B-1　　Cisco NX--OS Release 5.x 設定の制限値

機能	最大制限
VDC あたりの VLAN	4000
デバイスあたりのポート チャネル	256
デバイスあたりの vPC	256

INDEX

B

C

H

I

L

M

P

S

U

V

か

き

け

さ

し

す

せ

は

ひ

ふ

ほ

ま

め

ら

る

れ

ろ