



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

2014 年 8 月 4 日

Cisco Systems, Inc.

www.cisco.com

シスコは世界各国 200 箇所にオフィスを開設しています。
住所、電話番号、FAX 番号は
以下のシスコ Web サイトをご覧ください。
www.cisco.com/go/offices.

**【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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任は一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco Nexus 7000 シリズ 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
© 2009–2014 Cisco Systems, Inc. All rights reserved.

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

新機能および変更された機能に関する情報

この章では、『Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x』の新機能および変更された機能に関する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 に関する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。リリースに関する追加情報については、シスコの次の Web サイトを参照してください。

<http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-release-notes-list.html>

表 1 では、『Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 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
ファブリック エクステンダ (FEX)	ファブリック エクステンダのポートには、ホスト接続に関するレイヤ 3 サポートがあり、vPC はファブリック エクステンダ (ホスト vPC) から設定できます。	5.2(1)	第 4 章「レイヤ 3 インターフェイスの設定」 第 7 章「vPC の設定」
BFD SHA1 認証	BFD パケットの SHA-1 認証をサポートします。	5.2(1)	第 5 章「双方向フォワーディング検出の設定」
デフォルト インターフェイス	複数のインターフェイス タイプの既存の設定をクリアできます。	5.2(1)	第 3 章「レイヤ 2 インターフェイスの設定」
SVI 自動ステート除外	VLAN に複数のポートがあるときに、VLAN インターフェイスのリンクアップ計算からポートを除外できます。	5.2(1)	第 3 章「レイヤ 2 インターフェイスの設定」
vPC	自動リカバリ設定のサポートを設定でき、VLAN の一貫性障害に対する MST のシステム表示機能とともに、FabricPath 設定のサポートと Cisco 2000 シリーズ ファブリック エクステンダへの vPC 接続を提供します。	5.2(1)	第 7 章「vPC の設定」
レート制限	スーパーバイザに到達するパケットのレート制限を設定します。	5.1(1)	第 2 章「基本インターフェイスパラメータの設定」

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

表 1 Cisco NX-OS Release 5.x (続き) 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
Nexus シャーシのインバンド管理	シャーシ内に F1 シリーズ モジュールのみがある場合に、Cisco Nexus 7000 スイッチのインバンド管理を設定します。	5.1(1)	第 4 章「レイヤ 3 インターフェイスの設定」
ポート チャネルの F1 シリーズ モジュールおよび M1 シリーズ モジュール	F シリーズ モジュールのポート チャネルへの 16 個のアクティブ ポートの同時バンドリングをサポートします。M シリーズ モジュールでは、最大 8 個のアクティブ ポートと 8 個のスタンバイ ポートをバンドルすることができます。	5.1(1)	第 6 章「ポート チャネルの設定」
LACP ポートチャネルの最小リンクおよび MaxBundle	LACP ポートチャネルの最小リンクおよび LACP ポートチャネル maxbundle を設定します。	5.1(1)	第 6 章「ポート チャネルの設定」
BFD	ネットワークのプロファイリングおよびプランニングを簡単にし、再コンバージェンス時間の一貫性を保ち、予測可能にします。	5.0(2)	第 5 章「双方向フォワーディング検出の設定」
Q-in-Q トンネリング	使用できる VLAN がすべて提供されながらも異なるカスタマーのトラフィックを分離することができます。	5.0(2)	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なります。	5.0(2)	第 7 章「vPC の設定」

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

はじめに

ここでは、『Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide』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。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、キーワード、およびユーザが入力するテキストは 太字 で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、 <i>イタリック体</i> 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}	必ずいずれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x y z]	いずれか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。
courier フォント	システムが表示する端末セッションおよび情報は、courier 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。



(注)

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。



ヒント

「問題解決に役立つ情報」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。



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。



ワンポイントアドバイス

「時間の節約に役立つ操作」です。記述されている操作を実行すると時間を節約できます。



警告

安全上の重要事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

これらの注意事項を保管しておいてください。



警告

このシンボルを使ったステートメントは、追加情報および規制要件または顧客要件に準拠するためのものです。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、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 (Cisco 製品資料の更新情報)*』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/c/en/us/td/docs/general/whatsnew/whatsnew.html>

『*What's New in Cisco Product Documentation (Cisco 製品資料の更新情報)*』は、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し、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をデスクトップに配信することもできます。RSS フィードは無料のサービスです。

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。

この章は、次の項で構成されています。

- 「インターフェイスに関する情報」 (P.1-1)
- 「バーチャライゼーション インターフェイス」 (P.1-5)
- 「インターフェイスのハイ アベイラビリティ」 (P.1-5)
- 「インターフェイスのライセンス要件」 (P.1-5)

インターフェイスに関する情報

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

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 パラメータ

機能	パラメータ (Parameters)	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 アクセスおよびリンク 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』
	ポート セキュリティ	『Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x』

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

表 1-1 インターフェイスパラメータ

機能	パラメータ (Parameters)	解説場所
レイヤ 3	メディア、IPv4 および IPv6 アドレス	このマニュアルの第 4 章「レイヤ 3 インターフェイスの設定」
	帯域幅、遅延、IP ルーティング、VRF	『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x』 『Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 5.x』
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 6.x』
FCoE	Cisco NX-OS リリース 5.2(1) 以降では、Cisco Nexus 7000 シリーズ スイッチ 上で Fibre Channel over Ethernet (FCoE) を実行できます。	『Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500』

この項では、次のトピックについて取り上げます。

- 「Ethernet Interfaces」 (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.1-4)
- 「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.1-5)

Ethernet Interfaces

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

この項では、次のトピックについて取り上げます。

- 「Access Ports」 (P.1-3)
- 「Trunk Ports」 (P.1-3)
- 「PVLAN ホストと無差別ポート」 (P.1-3)
- 「Routed Ports」 (P.1-3)

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

Access Ports

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

Trunk Ports

トランクポートは複数のVLANのトラフィックを送受信します。このポートのタイプはレイヤ2インターフェイスだけです。トランクポートインターフェイスの詳細については、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 ホストと無差別ポート

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

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

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

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

Routed Ports

ルーテッドポートは、IP トラフィックを他のデバイスにルーティングできる物理ポートです。ルーテッドポートはレイヤ3インターフェイスだけで、スパンニングツリープロトコル (STP) などのレイヤ2プロトコルはサポートしません。ルーテッドポートの詳細については、「ルーテッドインターフェイス」(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、簡易ネットワーク管理プロトコル (SNMP)、その他の管理エージェントを使用するリモート管理用ネットワークにデバイスを接続できます。管理ポート (mgmt0) は、自動検知であり、10/100/1000 Mb/s の速度の全二重モードで動作します。

管理インターフェイスの詳細については、『Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, 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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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、スイッチやサーバなどあらゆるネットワーク デバイスが該当します。それぞれのデバイスで合計 748 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設定の詳細については、「[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設定の詳細については、「[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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

トンネル インターフェイス

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

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

第 2 章

基本インターフェイスパラメータの設定

この章では、Cisco NX-OS デバイス上で管理されるインターフェイスの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。

この章は、次の項で構成されています。

- 「基本インターフェイスパラメータについて」 (P.2-2)
- 「ライセンス要件」 (P.2-13)
- 「注意事項と制約事項」 (P.2-13)
- 「デフォルト設定」 (P.2-15)
- 「基本インターフェイスパラメータの設定」 (P.2-15)
- 「基本インターフェイスパラメータの確認」 (P.2-55)
- 「インターフェイスカウンタのモニタリング」 (P.2-55)
- 「基本インターフェイスパラメータ設定の機能履歴」 (P.2-58)



(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)。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

基本インターフェイスパラメータについて

この項では、次のトピックについて取り上げます。

- 「説明」 (P.2-2)
- 「ビーコン」 (P.2-2)
- 「MDIX」 (P.2-3)
- 「デバウンス タイマー」 (P.2-3)
- 「Error Disabled」 (P.2-3)
- 「レート モード」 (P.2-4)
- 「速度モードとデュプレックス モード」 (P.2-4)
- 「フロー制御」 (P.2-6)
- 「ポート MTU サイズ」 (P.2-6)
- 「帯域幅」 (P.2-7)
- 「スループット遅延」 (P.2-7)
- 「管理ステータス」 (P.2-7)
- 「UDLD パラメータ」 (P.2-8)
- 「キャリア遅延」 (P.2-10)
- 「ポート チャンネルパラメータ」 (P.2-10)
- 「ポート プロファイル」 (P.2-11)
- 「タイムドメイン反射率計ケーブル診断」 (P.2-13)

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 チャンネル 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 チャンネルの説明の設定](#)」 (P.6-25) 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.2-17) 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.2-19) を参照してください。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

MDIX

メディア依存インターフェイスクロスオーバー (MDIX) 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.2-26) 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.2-27) 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 **errdisable** ステートになった場合は、**errdisable detect cause** コマンドを使用して、そのエラーに関する情報を取得してください。

特定の **error-disabled** の原因に自動 **error-disabled** 回復タイムアウトを設定し、回復期間を設定できます。

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

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

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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することも、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
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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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

Module Type	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
N7K-M132XP-12 32 ポート 10 ギガビット イーサネット	自動 ¹	自動 ¹	10,000	Full
N7K-M108X2-12L 8 ポート 10 ギガビット イーサネット	自動 ¹	自動 ¹	10,000	Full
N7K-M148GS-11 N7K-M148GS-11L 48 ポート 1 ギガビット イーサネット	自動 ¹	自動 ¹	1000	Full
N7K-M148GT-11 48 ポート 10/100/1000 イー サネット	自動 ¹	自動 ¹	1000 10 または 100	Full 半二重
	1000	自動 ¹ または 全 二重	1000	Full
	100	自動 ¹ または 半 二重	100	半二重
		Full	100	Full
	10	自動 ¹ または 半 二重	10	半二重
Full		10	Full	
管理	自動 ¹	自動 ¹	1000	Full
			10 または 100	半二重
	1000	自動 ¹ または 全 二重	1000	Full
	100	自動 ¹ または 半 二重	100	半二重
		Full	100	Full
10	自動 ¹ または 半 二重	10	半二重	
	Full	10	Full	

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.6-26)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.2-29)を参照してください。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

フロー制御

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

2つのポート間のフロー制御を有効にするには、それぞれのポートで対応する受信および送信フロー制御パラメータをイネーブルまたはディセーブルに設定します。パラメータをイネーブルに設定すると、もう一方のポートの設定とは関係なく送信または受信フロー制御機能がアクティブになります。指定したパラメータを設定すると、もう一方のポートの対応するフロー制御状態をイネーブルまたはディセーブルに設定すれば、送信または受信フロー制御機能がアクティブになります。いずれかのフロー制御状態をディセーブルに設定すると、その送信方向のフロー制御がディセーブルになります。異なるポート フロー制御状態がリンク フロー制御状態に与える影響については、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		リンク フロー制御の状態
データ受信ポート (ポーズ フレームを送信)	データ送信ポート (ポーズ フレームを受信)	
イネーブル	イネーブル	イネーブル
イネーブル	Desired	イネーブル
イネーブル	ディセーブル	ディセーブル
Desired	イネーブル	イネーブル
Desired	Desired	イネーブル
Desired	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	Desired	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.2-31) を参照してください。

ポート MTU サイズ

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

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

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。



(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 ポートを通じての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.2-32) 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、「[情報目的としての帯域幅および遅延の設定](#)」(P.6-22) 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を設定する方法については、「[帯域幅の設定](#)」(P.2-36) 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、「[情報目的としての帯域幅および遅延の設定](#)」(P.6-22) 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.2-37) 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.6-23) 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.2-38) を参照してください。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

UDLD パラメータ

この項では、次のトピックについて取り上げます。

- 「UDLD の概要」 (P.2-8)
- 「UDLD のデフォルト設定」 (P.2-9)
- 「UDLD アグレッシブ モードと非アグレッシブ モード」 (P.2-9)

UDLD の概要

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

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

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

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



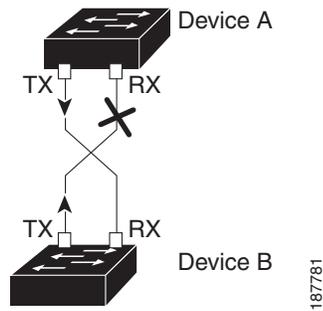
(注)

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

図 2-1 に、単一方向リンク条件の例を示します。デバイス B はこのポートでデバイス A からのトラフィックを正常に受信していますが、デバイス A は同じポート上でデバイス B からのトラフィックを受信していません。UDLD によって問題が検出され、ポートがディセーブルになります。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 イネーブル ステート (光ファイバ メディア用)	すべてのイーサネット光ファイバ LAN ポートでイネーブル
ポート別の UDLD イネーブル ステート (ツイストペア (銅製) メディア用)	すべてのイーサネット 10/100 および 1000BASE-TX LAN ポートでディセーブル
UDLD アグレッシブ モード	ディセーブル
UDLD メッセージの間隔	15 秒

デバイスとそのポートの UDLD を設定する方法については、「UDLD モードの設定」(P.2-40) を参照してください。

UDLD アグレッシブ モードと非アグレッシブ モード

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

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

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

- リンクの一方にポート スタックが生じる (送受信どちらも)
 - リンクの一部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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。



(注)

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



ヒント

ラインカードのアップグレードが In-Service Software Upgrade (ISSU) 時に実行され、ラインカードのポートの一部がレイヤ 2 ポート チャネルのメンバで、UDLD アグレッシブ モードで設定される場合。リモート ポートの 1 つがシャットダウンした場合、UDLD はローカル デバイスの対応するポートをエラー ディセーブル状態にします。これは正しい動作です。

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

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のみ設定できます。これは物理イーサネット インターフェイス、ポート チャネル、およびループバック インターフェイスには適用されません。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。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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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

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



(注)

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

ポート プロファイルをインターフェイスまたはインターフェイスの範囲にアタッチするとそのポート プロファイルが継承されます。ポート プロファイルをインターフェイスまたはインターフェイスの範囲にアタッチするか継承すると、システムがそのポート 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。また、ポート プロファイルには、別のポート プロファイルの設定を継承することができます。別のポート プロファイルを継承した場合、最初のポート プロファイルでは、それを継承した第2のポート プロファイルに含まれるすべてのコマンドは、最初のポート プロファイルとは競合していないものと見なされます。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。

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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



(注)

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

ポートプロファイル設定をインターフェイスに適用するには、そのポートプロファイルをイネーブルにする必要があります。ポートプロファイルをイネーブルにする前に、インターフェイスの範囲に対してポートプロファイルを設定および継承できます。その後、指定したインターフェイスに反映するために、この設定に対してポートプロファイルをイネーブルにします。

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

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

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

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

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

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

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

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

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

タイムドメイン反射率計ケーブル診断

Cisco Nexus 7000 シリーズ デバイスの Cisco NX-OS 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埋め込まれたケーブル診断機能により、リンク障害を診断するためにケーブルを取り外したりケーブル テスタを接続する必要はありません。ラインカード上の各ポートは、タイムドメイン反射率計 (TDR) 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 を使用して、パルス波形信号を導体に送信することで導体を分析し、反射された波形の極性、振幅およびラウンドトリップ時間を調べることができます。

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

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

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 NX-OS Licensing Guide』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。

注意事項と制約事項

基本インターフェイスパラメータの設定には次の注意事項と制約事項があります。

- 光ファイバ イーサネット ポートでは、シスコがサポートするトランシーバを使用する必要があります。シスコがサポートするトランシーバをポートに使用していることを確認するには、**show interface transceivers** コマンドを使用します。シスコがサポートするトランシーバを持つインターフェイスは、機能インターフェイスとして一覧表示されます。
- ポートはレイヤ 2 またはレイヤ 3 インターフェイスのいずれかです。両方が同時に成立することはありません。

デフォルトでは、どのポートもレイヤ 3 インターフェイスです。

レイヤ 3 インターフェイスをレイヤ 2 インターフェイスに変更するには、**switchport** コマンドを使用します。レイヤ 2 インターフェイスをレイヤ 3 インターフェイスに変更する場合は、**no switchport** コマンドを使用します。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- 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.2-5) を参照して同時に設定できる速度およびデュプレックスモードの組み合わせを確認します。
 - イーサネットポート速度を自動に設定すると、デバイスは自動的にデュプレックスモードを自動に設定します。
 - **no speed** コマンドを開始すると、デバイスは速度およびデュプレックスパラメータの両方を自動的に自動に設定します (**no speed** コマンドを入力すると、**speed auto** コマンドを入力した場合と同じ結果になります)。
 - イーサネットポート速度を自動以外の値 (10 Mb/s、100 Mb/s、1000 Mb/s など) に設定する場合は、それに合わせて接続先ポートを設定してください。接続先ポートが速度をネゴシエーションするように設定しないでください。



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



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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

デフォルト設定

表 2-5 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 2-5 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 (Parameters)	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 イネーブル ステート (光ファイバ メディア用)	すべてのイーサネット光ファイバ LAN ポートでイネーブル
銅線メディア用のポート別 UDLD イネーブル ステート	すべてのイーサネット 10/100 および 1000BASE-TX LAN ポートでディセーブル
UDLD メッセージの間隔	ディセーブル
UDLD アグレッシブ モード	ディセーブル
キャリア遅延	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

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」 (P.2-16)
- 「説明の設定」 (P.2-17)
- 「ビーコン モードの設定」 (P.2-19)
- 「帯域幅レート モードの変更」 (P.2-20)
- 「Error-Disabled ステートの設定」 (P.2-23)
- 「MDIX パラメータの設定」 (P.2-26)
- 「デバウンス タイマーの設定」 (P.2-27)

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- 「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.2-29)
- 「フロー制御の設定」(P.2-31)
- 「MTU サイズの設定」(P.2-32)
- 「帯域幅の設定」(P.2-36)
- 「スループット遅延の設定」(P.2-37)
- 「インターフェイスのシャットダウンおよび再開」(P.2-38)
- 「UDLD モードの設定」(P.2-40)
- 「キャリア遅延タイマーの設定」(P.2-43)
- 「ポート プロファイルの設定」(P.2-44)
- 「TDR ケーブル診断の実施」(P.2-52)
- 「スーパーバイザに到達するパケットのレート制限の設定」(P.2-53)

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 2-6 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 2-6 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 の場合)

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

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

次に、連続しているインターフェイス範囲の設定例を示します。

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

次に、不連続なインターフェイス範囲の設定例を示します。

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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

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	<pre>configure terminal</pre> <p>例:</p> <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<pre>interface interface</pre> <p>例 1:</p> <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre> <p>例 2:</p> <pre>switch(config)# interface mgmt0 switch(config-if)#</pre>	<p>設定するインターフェイスを指定します。インターフェイス タイプと ID を指定できます。イーサネット ポートの場合は「ethernet slot/port」を使用します。管理インターフェイスの場合は「mgmt0」を使用します。</p> <p>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。</p> <p>例 2 は、管理インターフェイスを指定する方法です。</p>



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

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**

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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	<code>configure terminal</code> 例: switch# <code>configure terminal</code> 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	<code>interface interface</code> 例: switch(config)# <code>interface ethernet 2/1</code> switch(config-if)# switch(config)# <code>interface mgmt0</code> 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 ポートの場合は「 <code>ethernet slot/port</code> 」を使用します。管理インターフェイスの場合は「 <code>mgmt0</code> 」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	<code>description text</code> 例: switch(config-if)# <code>description Ethernet port 3 on module 1.</code> switch(config-if)#	インターフェイスの説明を指定します。最大文字数は 80 文字です。
ステップ 4	<code>show interface interface</code> 例: switch(config)# <code>show interface ethernet 2/1</code>	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	<code>exit</code> 例: switch(config-if)# <code>exit</code> switch(config)#	インターフェイス モードを終了します。
ステップ 6	<code>copy running-config startup-config</code> 例: switch(config)# <code>copy running-config startup-config</code>	(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)#
```

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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	<code>configure terminal</code> 例: <code>switch# configure terminal</code> <code>switch(config)#</code>	コンフィギュレーションモードに入ります。
ステップ 2	interface ethernet slot/port 例: <code>switch(config)# interface ethernet 3/1</code> <code>switch(config-if)#</code>	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: <code>switch(config-if)# beacon</code> <code>switch(config-if)#</code>	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: <code>switch(config)# show interface ethernet 2/1</code>	ビーコンモードステータスなど、インターフェイスのステータスを表示します。
ステップ 5	exit 例: <code>switch(config-if)# exit</code> <code>switch(config)#</code>	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: <code>switch(config)# copy running-config startup-config</code>	(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)#
```

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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

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

帯域幅レート モードの変更

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

この項では、次のトピックについて取り上げます。

- 「ポート プロファイルの作成」(P.2-44)
- 「帯域幅をポート グループ内で共有」(P.2-21)

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 モードに入ります。
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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	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。

はじめる前に

同じグループのすべてのポートが同じ VDC に属している必要があります。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
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（同一ポート グループの一部でなければなりません）を指定し、インターフェイス コンフィギュレーション モードを開始します。 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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	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。この項では、次のトピックについて取り上げます。

- 「[Error Disable 検出のイネーブル化](#)」 (P.2-23)
- 「[errdisable ステート回復のイネーブル化](#)」 (P.2-24)
- 「[errdisable ステート回復間隔の設定](#)」 (P.2-25)

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**

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
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。デフォルトではイネーブルになっています。
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)#
```

errdisable ステート回復のイネーブル化

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

手順の概要

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
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 秒待機してからリトライします。デフォルトではディセーブルになっています。
ステップ 3	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。

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

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

errdisable ステート回復間隔の設定

error-disabled 回復タイマーの値を設定できます。

手順の概要

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
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。

はじめる前に

リモート ポートの MDIX をイネーブルにする必要があります。

手順の概要

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**

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
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するかどうかを指定します。
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 タイマーは、デバウンス時間をミリ秒単位 (ms) で指定することによりイネーブル化でき、デバウンス時間に 0 を指定することによりディセーブル化できます。

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
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)#	指定した時間 (0 ~ 5000 ミリ秒) でデバウンス タイマーをイネーブルにします。 0 ミリ秒を指定すると、デバウンス タイマーはディセーブルになります。
ステップ 4	show interface debounce 例: switch(config)# show interface debounce switch(config-if)#	イーサネット インターフェイスすべてのリンク デバウンス時間を示します。
ステップ 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、デバウンス タイマーをイネーブルにして、イーサネット ポート 3/1 のデバウンス時間を 1000 ミリ秒に設定する例を示します。

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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

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

インターフェイス速度およびデュプレックス モードの設定

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

イーサネット インターフェイスおよび管理インターフェイスに同時に設定できる速度およびデュプレックス モードについては、[表 2-2 \(P.2-5\)](#) を参照してください。



(注)

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

はじめる前に

リモート ポートの速度設定はローカル ポートへの変更をサポートします。ローカル ポートを固有の速度で使用するには、リモート ポートにも同じ速度を設定するか、ローカル ポートがその速度を自動ネゴシエートするように設定する必要があります。

手順の概要

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`

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 ポートの場合は「ethernet slot/port」を使用します。管理インターフェイスの場合は「mgmt0」を使用します。 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、速度を 10,000 Mb/s (10 Gb/s) に設定します。または、ポートがリンクの他の 10 ギガビット イーサネットポートの速度と自動ネゴシエートするように設定します。 管理インターフェイスでは、速度を 1000 Mb/s に設定します。あるいはポートがその速度と自動ネゴシエートするように設定します。
ステップ 4	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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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

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

フロー制御の設定

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

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



(注)

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

はじめる前に

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

手順の概要

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**

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
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のみ送信設定を指定できます。受信設定は任意の速度で動作するポートに設定できます。
ステップ 4	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単位 (MTU) サイズを設定できます。レイヤ 3 インターフェイスでは、576 ~ 9216 バイトの MTU を設定できます (偶数値にする必要があります)。レイヤ 2 インターフェイスでは、システム デフォルト MTU (1500 バイト) またはシステム ジャンボ MTU サイズ (デフォルト サイズは 9216 バイト) の MTU を設定できます。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。



(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。

switchport コマンドを使用して、ポート モードを変更できます。

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

この項では、次のトピックについて取り上げます。

- 「インターフェイス MTU サイズの設定」(P.2-33)
- 「システム ジャンボ MTU サイズの設定」(P.2-34)

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.2-34) 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**

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

手順の概要

1. `configure terminal`
2. `system jumbomtu size`
3. `show running-config all`
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	<code>configure terminal</code> 例: <code>switch# configure terminal</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>system jumbomtu size</code> 例: <code>switch(config)# system jumbomtu 8000</code> <code>switch(config)#</code>	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	<code>show running-config all</code> 例: <code>switch(config)# show running-config all </code> <code>include logfile</code>	現在の稼働設定を表示します。システム ジャンボ MTU サイズもあわせて表示します。
ステップ 4	<code>interface type slot/port</code> 例: <code>switch(config)# interface ethernet 2/1</code> <code>switch(config-if)#</code>	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	<code>mtu size</code> 例: <code>switch(config-if)# mtu 1500</code> <code>switch(config-if)#</code>	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	<code>exit</code> 例: <code>switch(config-if)# exit</code> <code>switch(config)#</code>	インターフェイス モードを終了します。
ステップ 7	<code>copy running-config startup-config</code> 例: <code>switch(config)# copy running-config startup-config</code>	(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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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

帯域幅の設定

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

手順の概要

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 モードに入ります。
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。
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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	コマンド	目的
ステップ 6	<pre>copy running-config startup-config</pre> <p>例： switch(config)# copy running-config startup-config</p>	(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	<pre>configure terminal</pre> <p>例： switch# configure terminal switch(config)#</p>	コンフィギュレーション モードに入ります。
ステップ 2	<pre>interface ethernet slot/port</pre> <p>例： switch(config)# interface ethernet 3/1 switch(config-if)#</p>	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	<pre>delay value</pre> <p>例： switch(config-if)# delay 10000 switch(config-if)#</p>	遅延時間を 10 マイクロ秒単位で指定します。1 ~ 16777215 の範囲の情報値を 10 マイクロ秒単位で設定できます。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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

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



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

インターフェイスのシャットダウンおよび再開

イーサネットまたは管理インターフェイスはシャットダウンして再起動できます。インターフェイスはシャットダウンするとディセーブルになり、すべてのモニタ画面にはダウン状態で表示されます。この情報は、すべてのダイナミック ルーティング プロトコルを通じて、他のネットワーク サーバに伝達されます。シャットダウンしたインターフェイスはどのルーティング アップデートにも含まれません。インターフェイスを再開するには、デバイスを再起動する必要があります。

手順の概要

1. **configure terminal**
2. **interface interface**
3. **shutdown**
4. **show interface interface**

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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	<code>configure terminal</code> 例: <code>switch# configure terminal</code> <code>switch(config)#</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface</code> 例: <code>switch(config)# interface ethernet 2/1</code> <code>switch(config-if)#</code> <code>switch(config)# interface mgmt0</code> <code>switch(config-if)#</code>	設定するインターフェイスを指定します。インターフェイス タイプと ID を指定できます。イーサネット ポートの場合は「 <code>ethernet slot/port</code> 」を使用します。管理インターフェイスの場合は「 <code>mgmt0</code> 」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	<code>shutdown</code> 例: <code>switch(config-if)# shutdown</code> <code>switch(config-if)#</code>	インターフェイスをディセーブルにします。
ステップ 4	<code>show interface interface</code> 例: <code>switch(config-if)# show interface</code> <code>ethernet 2/1</code> <code>switch(config-if)#</code>	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	<code>no shutdown</code> 例: <code>switch(config-if)# no shutdown</code> <code>switch(config-if)#</code>	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	<code>show interface interface</code> 例: <code>switch(config-if)# show interface</code> <code>ethernet 2/1</code> <code>switch(config-if)#</code>	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	<code>exit</code> 例: <code>switch(config-if)# exit</code> <code>switch(config)#</code>	インターフェイス モードを終了します。
ステップ 8	<code>copy running-config startup-config</code> 例: <code>switch(config)# copy running-config</code> <code>startup-config</code>	(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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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

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

UDLD モードの設定

単一方向リンク検出 (UDLD) を実行するように設定されているデバイス上のイーサネット インターフェイスには、ノーマル モードまたはアグレッシブ モードの UDLD を設定できます。インターフェイスの UDLD モードをイネーブルにするには、そのインターフェイスを含むデバイス上で UDLD を事前にイネーブルにしておく必要があります。UDLD は他方のリンク先のインターフェイスおよびそのデバイスでもイネーブルになっている必要があります。

表 2-7 に、異なるインターフェイスで UDLD をイネーブルおよびディセーブルにする CLI 詳細を示します。

表 2-7 異なるインターフェイスで UDLD をイネーブルおよびディセーブルにする CLI 詳細

説明	ファイバポート	銅線またはファイバ以外のポート
デフォルト設定	イネーブル	ディセーブル
enable UDLD コマンド	no udld disable	udld enable
disable UDLD コマンド	udld disable	no udld enable

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

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

はじめる前に

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

手順の概要

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}**

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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	<code>configure terminal</code> 例： <code>switch# configure terminal</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>feature udld</code> 例： <code>switch(config)# feature udld</code> <code>switch(config)#</code>	デバイスの UDLD をイネーブルにします。
	<code>no feature udld</code> 例： <code>switch(config)# no feature udld</code> <code>switch(config)#</code>	デバイスの UDLD をディセーブルにします。
ステップ 3	<code>udld message-time seconds</code> 例： <code>switch(config)# udld message-time 30</code> <code>switch(config)#</code>	(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	<code>udld aggressive</code> 例： <code>switch(config)# udld aggressive</code> <code>switch(config)#</code>	(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	<code>interface ethernet slot/port</code> 例： <code>switch(config)# interface ethernet 3/1</code> <code>switch(config-if)#</code>	(任意) 設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	<code>udld {enable disable}</code> 例： <code>switch(config-if)# udld enable</code> <code>switch(config-if)#</code>	(任意) 指定した銅線ポートの UDLD をイネーブルにしたり、指定したファイバポートの UDLD をディセーブルにします。 銅線ポートの UDLD をイネーブルにするには、コマンドは <code>udld enable</code> となります。ファイバポートで UDLD をイネーブルにするには、コマンドは <code>no udld disable</code> となります。 (詳細については、表 2-7を参照してください)。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	コマンド	目的
ステップ 7	<pre>show udld [ethernet slot/port global neighbors]</pre> <p>例: switch(config)# show udld switch(config)#</p>	(任意) UDLD のステータスを表示します。
ステップ 8	<pre>exit</pre> <p>例: switch(config-if-range)# exit switch(config)#</p>	インターフェイス モードを終了します。
ステップ 9	<pre>copy running-config startup-config</pre> <p>例: switch(config)# copy running-config startup-config</p>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

次に、デバイスの UDLD をイネーブルにする例を示します。

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

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

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

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

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

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

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

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

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

キャリア遅延タイマーの設定

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



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

はじめる前に

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

手順の概要

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 モードに入ります。
ステップ 2	interface <i>vlan-id</i> 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 {<i>sec</i> <i>msec number</i>} 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 <i>vlan-id</i> 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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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

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

ポート プロファイルの設定

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

この項では、次のトピックについて取り上げます。

- 「ポート プロファイルの作成」 (P.2-44)
- 「ポート プロファイル コンフィギュレーション モードの開始およびポート プロファイルの修正」 (P.2-45)
- 「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.2-46)
- 「特定のポート プロファイルのイネーブル化」 (P.2-47)
- 「ポート プロファイルの継承」 (P.2-49)
- 「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.2-50)
- 「継承されたポート プロファイルの削除」 (P.2-51)

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**

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
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 モードの開始およびポート プロファイルの修正

ポート プロファイル コンフィギュレーション モードを開始し、ポート プロファイルを修正できます。ポート プロファイルを修正するには、ポート プロファイル コンフィギュレーション モードを開始する必要があります。

手順の概要

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**

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
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

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

手順の概要

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**

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
ステップ 2	interface [ethernet slot/port interface-vlan vlan-id loopback number port channel number tunnel number] 例： switch(config)# interface ethernet7/3-5, ethernet10/2, ethernet11/20-25 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)#	指定したポート プロファイルを、選択したインターフェイスに割り当てます。
ステップ 4	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 ethernet7/3-5, ethernet10/2, ethernet11/20-25
switch(config-if)# inherit port-profile adam
switch(config-if)#
```

特定のポート プロファイルのイネーブル化

ポート プロファイル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。

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

ポート プロファイルをイネーブルまたはディセーブルにするには、ポート プロファイル コンフィギュレーション モードを開始する必要があります。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
ステップ 2	port-profile [type {ethernet interface-vlan loopback port channel tunnel}] <i>name</i> 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。

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

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
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)#
```

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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	<code>configure terminal</code> 例: switch# configure terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	<code>interface [ethernet slot/port interface-vlan vlan-id loopback number port channel number tunnel number]</code> 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	<code>no inherit port-profile name</code> 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	<code>exit</code> 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	<code>show port-profile</code> 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	<code>copy running-config startup-config</code> 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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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	<code>configure terminal</code> 例: switch# configure terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	<code>port-profile name</code> 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	<code>no inherit port-profile name</code> 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	<code>exit</code> 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	<code>show port-profile</code> 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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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

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

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

TDR ケーブル診断の実施

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

はじめる前に

TDR テストの注意事項は次のとおりです。

- TDR では、最大で 115 m の長さのケーブルをテストできます。
- このテストは、ケーブルの両端で同時に開始しないでください。ケーブルの両端でテストを同時に開始すると、テストの結果が不正確になる可能性があります。
- どのケーブル診断テストの場合でも、テストの実行中にポートのコンフィギュレーションを変更しないでください。変更すると、テスト結果が不正確になる可能性があります。
- 関連するポート グループのすべてのポートを、TDR テスト実行前にシャット ダウンする必要があります。

手順の概要

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	<pre>test cable-diagnostics tdr interface number</pre> <p>例:</p> <pre>switch# test cable-diagnostics tdr interface ethernet 7/1</pre>	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	<pre>show interface number cable-diagnostics-tdr</pre> <p>例:</p> <pre>switch(config)# show interface ethernet 7/1 cable-diagnostics-tdr</pre>	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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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

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

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

```
n7000# show interface ethernet 3/12 cable-diagnostics-tdr
```

```
-----
Interface      Speed Pair Cable Length   Distance to fault   Channel Pair Status
-----
Eth3/12        1000 ---  N/A                N/A                 Pair A  Terminated
              ---  N/A                N/A                 Pair B  Terminated
              ---  N/A                N/A                 Pair C  Terminated
              ---  N/A                N/A                 Pair D  Terminated
```

スーパーバイザに到達するパケットのレート制限の設定



(注)

Cisco NX-OS リリース 5.1 以降では、スーパーバイザ モジュールに到達するパケットのレート制限をデバイスでグローバルに設定できます。詳細については、『Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 5.X』を参照してください。

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

手順の概要

1. **configure terminal**
2. **[no] rate-limit cpu direction {input | output | both} pps packets action log**
3. (任意) **exit**
4. (任意) **show system internal pktmgr interface ethernet slot/port**
5. (任意) **copy running-config startup-config**

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
ステップ 2	[no] rate-limit cpu direction {input output both} pps packets action log 例: switch(config)# interface ethernet 1/1 switch(config-if)# rate-limit cpu direction both pps 1000 action log	特定のインターフェイスのスーパーバイザ モジュールに到達するパケットのレート制限を設定します。着信または発信パケットのレートが設定済みレート制限を超過した場合、デバイスはシステム メッセージを記録しますが、パケットをドロップしません。範囲は 1 ~ 100000 です。デフォルトレートは 10000 です。
ステップ 3	exit 例: switch(config-if)# exit switch(config)#	(任意) インターフェイス モードを終了します。
ステップ 4	show system internal pktmgr interface ethernet slot/port 例: switch# show system internal pktmgr interface ethernet 4/1	(任意) 特定のインターフェイスのスーパーバイザ モジュールに到達するパケットのインバウンドおよびアウトバウンドのレート制限の設定を表示します。
ステップ 5	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。



(注)

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

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

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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
<code>show cdp</code>	CDP ステータスを表示します。
<code>show interface interface</code>	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。
<code>show interface interface</code>	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。
<code>show interface brief</code>	インターフェイスの状態表を表示します。
<code>show interface switchport</code>	レイヤ 2 ポートのステータスを表示します。
<code>show interface status err-disabled</code>	error-disabled インターフェイスに関する情報を表示します。
<code>show vdc</code>	現在の VDC のステータスを表示します。
<code>show udld interface</code>	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。
<code>show udld-global</code>	現在のデバイスの UDLD ステータスを表示します。
<code>show port-profile</code>	ポート プロファイルに関する情報を表示します。
<code>show system internal pktmgr internal ethernet slot/port</code>	特定のインターフェイスのスーパーバイザ モジュールに到達するパケットのインバウンドおよびアウトバウンドのレート制限の設定を表示します。

これらのコマンド出力のフィールドの詳細については、『Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, 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モニタリング

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。ここでは、次の内容について説明します。

- 「[インターフェイス統計情報の表示](#)」(P.2-56)
- 「[インターフェイスカウンタのクリア](#)」(P.2-57)

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 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 <code>{{1 2 3} seconds}</code> 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 インターフェイスの場合は 60 秒) 2 : 300 秒 3 : 未設定
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。

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

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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#
```

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.2-58)
- 「標準」 (P.2-58)
- 「基本インターフェイスパラメータ設定の機能履歴」 (P.2-58)

■ 基本インターフェイスパラメータ設定の機能履歴

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

関連資料

関連項目	マニュアルタイトル
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

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

基本インターフェイスパラメータ設定の機能履歴

表 2-8 に、この機能のリリース履歴を示します。

表 2-8 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
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。
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。

レイヤ 2 インターフェイスの設定



(注) Cisco リリース 5.2 以降では、Cisco Nexus 7000 シリーズのデバイスは FabricPath レイヤ 2 インターフェイスをサポートします。FabricPath の機能およびインターフェイスの詳細については、『*Cisco Nexus 7000 Series NX-OS FabricPath Command Reference, Release 5.x*』を参照してください。

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



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

- トランク ポート
- アクセス ポート
- プライベート VLAN ポート (プライベート VLAN の詳細については、『*Cisco DCNM Layer 2 Switching Configuration Guide, Release 5.x*』を参照してください)
- FabricPath ポート (FabricPath の詳細については、『*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide, Release 5.x*』および『*Cisco DCNM FabricPath Configuration Guide, Release 5.x*』を参照してください)。

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



(注) FabricPath 機能の設定の詳細については、『*Cisco DCNM FabricPath 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、またはプライベート VLAN ポートとして機能させることができます。

この章は、次の項で構成されています。

- 「[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](#)」 (P.3-2)
- 「[レイヤ 2 ポート モードのライセンス要件](#)」 (P.3-8)

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- 「ライセンス 2 インターフェイスの前提条件」 (P.3-8)
- 「注意事項と制約事項」 (P.3-8)
- 「デフォルト設定」 (P.3-10)
- 「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」 (P.3-10)
- 「インターフェイス コンフィギュレーションの確認」 (P.3-23)
- 「レイヤ 2 インターフェイスのモニタリング」 (P.3-24)
- 「アクセス ポートおよびトランク ポートの設定例」 (P.3-24)
- 「その他の参考資料」 (P.3-25)
- 「レイヤ 2 インターフェイス設定の機能履歴」 (P.3-26)



(注) SPAN 宛先インターフェイスの設定については、『*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 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張することができます。すべてのレイヤ 2 スイッチング ポートは、メディア アクセス コントロール (MAC) アドレス テーブルを維持します。



(注) VLAN、MAC アドレス テーブル、プライベート VLAN、およびスパンニングツリー プロトコルの詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*』を参照してください。



(注) レイヤ 2 ポートは、トランク ポート、アクセス ポート、またはプライベート VLAN ポートとして機能させることができます。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。

この項では、次のトピックについて取り上げます。

- 「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」 (P.3-3)
- 「IEEE 802.1Q カプセル化」 (P.3-4)
- 「アクセス VLAN」 (P.3-5)
- 「トランク ポートのネイティブ VLAN ID」 (P.3-6)
- 「ネイティブ VLAN トラフィックのタギング」 (P.3-6)
- 「許容 VLAN」 (P.3-6)

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- 「High Availability (高可用性)」 (P.3-7)
- 「仮想化のサポート」 (P.3-7)
- 「デフォルト インターフェイス」 (P.3-7)
- 「SVI 自動ステート除外」 (P.3-7)



(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。

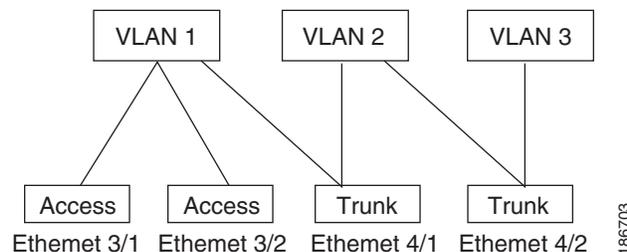
セットアップ スクリプトを使用するか、**system default switchport** コマンドを入力して、すべてのポートをレイヤ 2 ポートにできます。セットアップ スクリプトの使い方については、『Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 5.x』を参照してください。CLI を使用して、ポートをレイヤ 2 ポートとして設定するには、**switchport** コマンドを使用します。

1 つのトランク内のポートはすべて、同じ仮想デバイス コンテキスト (VDC) に配置されている必要があります。VDC 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。

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 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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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.3-4）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。

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、チャンネルグループ化はディセーブルになります。ホストを割り当てると、割り当てたポートがパケット転送を開始する時間が短縮されます。

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

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

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

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

IEEE 802.1Q カプセル化



(注)

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

複数の VLAN に接続するトランク ポートのトラフィックを正しく配信するために、デバイスは IEEE 802.1Q カプセル化（タギング方式）を使用します。この方式では、フレーム ヘッダーに挿入したタグが使用されます（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 のトラフィックを区別することができます。また、カプセル化された VLAN タグにより、トランクは同じ VLAN 上のネットワークの端から端までトラフィックを移動させます。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

図 3-2 802.1Q タグなしヘッダーと 802.1Q タグ付きヘッダー

Preamble (7 -bytes)	Start Frame Delimiter (1 -byte)	Dest. MAC Address (6 - bytes)	Source MAC Address (6 - bytes)	Length / Type (2 - bytes)	MAC Client Data (0 -n bytes)	Pad (0 -p bytes)	Frame Check Sequence (4 -bytes)
------------------------	--	---	--	------------------------------------	---------------------------------	------------------------	--

Preamble (7-bytes)	Start Frame Delimiter (1-byte)	Dest. MAC Address (6-bytes)	Source MAC Address (6-bytes)	Length/Type = 802.1Q Tag Type (2-byte)	Tag Control Information (2-bytes)	Length /Type (2- bytes)	MAC Client Data (0-n bytes)	Pad (0-p bytes)	Frame Check Sequence (4-bytes)
-----------------------	---	--------------------------------------	---------------------------------------	---	--	----------------------------------	-----------------------------------	-----------------------	---

3 bits = User Priority field
1 bit = Canonical Format Identifier (CFI)
12 bits – VLAN Identifier (VLAN ID)

182779

アクセス VLAN



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



(注) プライベート VLAN の詳細については、『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, 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（アクセスポート）用に VLAN を設定しないと、そのインターフェイスはデフォルトの VLAN（VLAN1）のトラフィックだけを伝送します。

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

アクセスポートは、アクセス VLAN 値のほかに 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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

トランク ポートのネイティブ VLAN ID

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



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

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



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

ネイティブ VLAN トラフィックのタグging

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 ポートを通るできます。

ただし、デバイスを通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グging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 でパケットのタグging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 のタグging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 に対してトラフィックを送受信します。各トランク上では、すべての VLAN ID が許可されます。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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。



(注) STP に関する詳細情報については、『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x』を参照してください。



(注) Cisco リリース 5.2 以降では、内部使用に予約されている VLAN のブロックを変更できます。予約済み VLAN の変更の詳細については、『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x』を参照してください。

High Availability (高可用性)

ソフトウェアは、レイヤ 2 ポートのハイアベイラビリティをサポートします。



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

仮想化のサポート

デバイスは仮想デバイス コンテキスト (VDC) をサポートします。

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



(注) VDC と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。

デフォルト インターフェイス

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



(注) 最大 8 ポートがデフォルト インターフェイスに選択できます。デフォルトのインターフェイス機能は、管理インターフェイスに対しサポートされていません。それはデバイスが到達不能な状態になる可能性があるためです。

SVI 自動ステート除外

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。



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

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
Cisco 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。Cisco NX-OS のライセンス スキームの詳細については、『Cisco NX-OS Licensing Guide』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。

ライセンス2 インターフェイスの前提条件

ライセンス2 インターフェイスには次の前提条件があります。

- デバイスにログインしている。
- **switchport mode** コマンドを使用する前に、ポートをレイヤ2 ポートとして設定する必要があります。デフォルトでは、デバイスのすべてのポートはレイヤ3 ポートです。

注意事項と制約事項

VLAN トランキングには次の設定上の注意事項と制限事項があります。

- ポートはレイヤ2 またはレイヤ3 インターフェイスのいずれかです。両方が同時に成立することはありません。
- レイヤ3 ポートをレイヤ2 ポートに変更する場合またはレイヤ2 ポートをレイヤ3 ポートに変更する場合は、レイヤに依存するすべての設定は失われます。アクセスまたはトランク ポートをレイヤ3 ポートに変更すると、アクセス VLAN、ネイティブ VLAN、許容 VLAN などの情報はすべて失われます。
- アクセス リンクを持つデバイスには接続しないでください。アクセス リンクにより VLAN が区分されることがあります。
- 802.1Q トランクを介してシスコ デバイスを接続するときは、802.1Q トランクのネイティブ VLAN がトランク リンクの両端で同じであることを確認してください。トランクの一端のネイティブ VLAN と反対側の端のネイティブ VLAN が異なると、スパニングツリー ループの原因になります。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- ネットワーク上のすべての VLAN についてスパン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 上のスパンニングツリーをディセーブルにすると、スパンニングツリーのループが発生する場合があります。802.1Q トランクのネイティブ VLAN のスパン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。スパン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 のスパンニングツリーをディセーブルにする必要があります。スパンニングツリーをディセーブルにする前に、ネットワークに物理ループがないことを確認してください。
- 802.1Q トランクを介して2台のシスコ デバイスを接続すると、トランク上で許容される VLAN ごとにスパンニングツリーブリッジプロトコル データ ユニット (BPDU) が交換されます。トランクのネイティブ VLAN 上の BPDU は、タグなしの状態です。予約済み IEEE 802.1D スパンニングツリー マルチキャスト MAC アドレス (01-80-C2-00-00-00) に送信されます。トランクの他のすべての VLAN 上の BPDU は、タグ付きの状態です。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 に対してスパンニングツリー トポロジを定義するスパン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switchを他社製のswitchに接続すると、他社製のswitchの Mono Spanning Tree とシスコ製のswitchのネイティブ VLAN スパン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ンニングツリー トポロジが形成されます。
- シスコ デバイスは、トランクのネイティブ VLAN 以外の VLAN にある SSTP マルチキャスト MAC アドレスに BPDU を伝送します。したがって、他社製のデバイスではこれらのフレームが BPDU として認識されず、対応する VLAN のすべてのポート上でフラッドングされます。他社製の 802.1Q クラウドに接続された他のシスコ デバイスは、フラッドングされたこれらの BPDU を受信します。BPDU を受信すると、Cisco スイッチは、他社製の 802.1Q デバイス クラウドにわたって、VLAN 別のスパンニングツリー トポロジを維持できません。シスコ デバイスを隔てている他社製の 802.1Q クラウドは、802.1Q トランクを介して他社製の 802.1Q クラウドに接続されたすべてのデバイス間の単一のブロードキャスト セグメントとして処理されます。
- シスコ デバイスを他社製の 802.1Q クラウドに接続するすべての 802.1Q トランク上で、ネイティブ VLAN が同じであることを確認します。
- 他社製の特定の 802.1Q クラウドに複数のシスコ デバイスを接続する場合は、すべての接続に 802.1Q トランクを使用する必要があります。シスコ デバイスを他社製の 802.1Q クラウドにアクセス ポート経由で接続することはできません。この場合、シスコ製のアクセス ポートはスパンニングツリー「ポート不一致」状態になり、トラフィックはポートを通過しません。
- トランク ポートをポート チャネル グループに含めることができますが、そのグループのトランクはすべて同じ設定にする必要があります。グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。パラメータの設定を変更すると、許容 VLAN やトランク ステータスなど、デバイスのグループのすべてのポートにその設定を伝えます。たとえば、ポート グループのあるポートがトランクになるのを中止すると、すべてのポートがトランクになるのを中止します。
- トランク ポートで 802.1X をイネーブルにしようとする、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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 (Parameters)	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
管理状態	閉じる

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

この項では、次のトピックについて取り上げます。

- ・「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」(P.3-10)
- ・「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」(P.3-11)
- ・「アクセス ホスト ポートの設定」(P.3-12)
- ・「トランク ポートの設定」(P.3-14)
- ・「802.1Q トランク ポートのネイティブ VLAN の設定」(P.3-15)
- ・「トランキング ポートの許可 VLAN の設定」(P.3-16)
- ・「デフォルト インターフェイスの設定」(P.3-18)
- ・「SVI 自動ステート除外の設定」(P.3-19)
- ・「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」(P.3-21)
- ・「システムのデフォルト ポート モードをレイヤ 2 に変更」(P.3-22)



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

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 である必要があります。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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

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

はじめる前に

レイヤ2 インターフェイスを設定することを確認します。

手順の概要

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. (任意) `show interface`
7. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例: <code>switch# configure terminal</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>interface {{type slot/port}} {{port-channel number}}</code> 例: <code>switch(config)# interface ethernet 3/1</code> <code>switch(config-if)#</code>	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	<code>switchport mode {access trunk}</code> 例: <code>switch(config-if)# switchport mode access</code>	インターフェイスを、非トランキング、タグなし、シングル VLAN レイヤ2 インターフェイスとして設定します。アクセスポートは、1つの VLAN のトラフィックだけを伝送できます。デフォルトでは、アクセスポートは VLAN1 のトラフィックを伝送します。異なる VLAN のトラフィックを伝送するようにアクセスポートを設定するには、 <code>switchport access vlan</code> コマンドを使用します。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	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、エンド ステーション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。

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



(注) ポートチャネル インターフェイスの詳細については『第 6 章「ポート チャネルの設定」』を、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。スパンニングツリー プロトコルの詳細について。

はじめる前に

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例： switch# <code>configure terminal</code> switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	<code>interface type slot/port</code> 例： switch(config)# <code>interface ethernet 3/1</code> 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	<code>switchport host</code> 例： switch(config-if)# <code>switchport host</code>	インターフェイスをアクセス ホスト ポートとして設定します。このポートはただちに、スパニングツリー フォワーディング ステートに移行し、このインターフェイスのポート チャネル動作をディセーブルにします。 (注) このコマンドは端末だけに適用します。
ステップ 4	<code>exit</code> 例： switch(config-if)# <code>exit</code> switch(config)#	インターフェイス モードを終了します。
ステップ 5	<code>show interface</code> 例： switch# <code>show interface</code>	(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	<code>copy running-config startup-config</code> 例： switch(config)# <code>copy running-config startup-config</code>	(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)#
```

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

トランク ポートの設定

レイヤ 2 ポートをトランク ポートとして設定できます。トランク ポートは、1 つの VLAN の非タグ付きパケットと、複数の VLAN のカプセル化されたタグ付きパケットを伝送します（カプセル化の詳細については、「IEEE 802.1Q カプセル化」(P.3-4) 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。

はじめる前に

トランク ポートを設定する前に、レイヤ 2 インターフェイスを設定することを確認します。

手順の概要

1. **configure terminal**
2. **interface** {type slot/port | port-channel number}
3. **switchport mode** {access | trunk}
4. **exit**
5. (任意) **show interface**
6. (任意) **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 モードに入ります。
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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	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 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。



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

手順の概要

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
ステップ 2	interface { <i>type slot/port</i> 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 <i>vlan-id</i> 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。指定できる範囲は 1 ~ 4094 です (ただし、内部使用に予約されている VLAN は除きます)。デフォルト値は VLAN 1 です。
ステップ 4	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 VLAN5 に設定する例を示します。

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

トランキング ポートの許可 VLAN の設定

特定のトランク ポートで許可される VLAN の ID を指定できます。



(注) **switchport trunk allowed vlan** *vlan-list* コマンドは、指定したポートの現在の VLAN リストを新しいリストと置き換えます。その結果、新しいリストが適用される前に確認を求められます。副作用として、大規模設定のコピーと貼り付けを行うと、CLI が他のコマンドを受け入れる前に確認のため待機することになるため、障害が発生する場合があります。この問題を回避するには、設定をペーストする前に **terminal dont-ask** コマンドを使用して、メッセージの表示をディセーブルにできます。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

はじめる前に

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



(注) Cisco リリース 5.2 以降では、内部使用に予約されている VLAN のブロックを変更できます。予約済み VLAN の変更の詳細については、『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x』を参照してください。

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. (任意) **show vlan**
6. (任意) **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 モードに入ります。
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 インターフェイスの許可 VLAN を設定します。デフォルトでは、トランク インターフェイス上のすべての VLAN (1 ~ 3967 および 4048 ~ 4094) が許可されます。VLAN 3968 ~ 4047 は、内部で使用するデフォルトで予約されている VLAN です。デフォルトでは、すべてのトランク インターフェイスですべての VLAN が許可されます。Cisco リリース 5.2(1) 以降では、デフォルトの予約済み VLAN は 3968 ~ 4094 で、予約済み VLAN のブロックを変更できます。詳細については、『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x』を参照してください。 (注) 内部で割り当て済みの VLAN を、トランク ポート上の許可 VLAN として追加することはできません。内部で割り当て済みの VLAN を、トランク ポートの許可 VLAN として登録しようとする、メッセージが返されます。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	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、VLAN 15 ~ 20 をイーサネット 3/1、レイヤ 2 トランク ポートの許容 VLAN リストに追加する例を示します。

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

デフォルト インターフェイスの設定

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



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

手順の概要

1. **configure terminal**
2. **default interface int-if [checkpoint name]**
3. **exit**
4. (任意) **show interface**

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
ステップ 2	default interface int-if [checkpoint name] 例： switch(config)# default interface ethernet 3/1 checkpoint test8	インターフェイスの設定を削除しデフォルトの設定を復元します。? サポートされているインターフェイスを表示します。 checkpoint キーワードを使用して、設定を消し去ってしまう前にインターフェイスの実行コンフィギュレーションを保存します。
ステップ 3	exit 例： switch(config)# exit switch#	コンフィギュレーション モードを終了します。
ステップ 4	show interface 例： switch# show interface	(任意) インターフェイスのステータスと内容を表示します。

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

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

SVI 自動ステート除外の設定

イーサネット インターフェイスまたはポート チャネルに SVI 自動ステート除外機能を設定できます。

自動ステート除外オプションを使用して、ポートが SVI 計算を稼働または停止したり、それを選択したポートでイネーブルのすべての VLAN に適用するのをイネーブルまたはディセーブルにすることができます。

手順の概要

1. **configure terminal**
2. **interface** *{{type slot/port}} | {{port-channel number}}*
3. **switchport**
4. **switchport autostate exclude**
5. **exit**
6. (任意) **show running-config interface**
7. (任意) **copy running-config startup-config**

■ 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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
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 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ます。
ステップ 4	switchport autostate exclude 例: switch(config-if)# switchport autostate exclude	VLAN に複数のポートがあるときに、VLAN インターフェイスのリンクアップ計算からポートを除外します。 デフォルト設定に戻すには、このコマンドの no 形式を使用します。
ステップ 5	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 running-config interface {{type slot/port} {port-channel number}} 例: switch(config)# show running-config interface ethernet 3/1	(任意) 指定されたインターフェイスに関する設定情報を表示します。
ステップ 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、Cisco NX-OS デバイスで VLAN インターフェイスのリンクアップ計算からポートを除外する例を示します。

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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グging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 タグging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。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。VDC が異なっても同じ VLAN 名と ID を使用できるので、正しい VDC で作業していることを確認する必要があります。

手順の概要

1. **configure terminal**
2. **vlan dot1q tag native**
3. **exit**
4. (任意) **show vlan**
5. (任意) **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 モードに入ります。
ステップ 2	vlan dot1q tag native 例： switch(config)# vlan dot1q tag native	802.1Q トランキング ネイティブ VLAN ID インターフェイスの動作を変更します。このインターフェイスは、ネイティブ VLAN ID の値と一致しすべての非タグ付きトラフィックをドロップするタグを使って開始するすべてのパケットのタグgingを維持します。この場合も、制御トラフィックはネイティブ VLAN を通過します。デフォルトではディセーブルになっています。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	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 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、すべての非タグ付きトラフィックをドロップする例を示します (制御トラフィックは除く)。

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

システムのデフォルト ポート モードをレイヤ2に変更

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

システムのデフォルト ポート モードをストレージ VDC のファイバチャネルに設定する詳細については、『Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500』を参照してください。

手順の概要

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
ステップ 2	system default switchport [shutdown] 例: switch(config-if)# system default switchport	システムのすべてのインターフェイスに対するデフォルトのポート モードをレイヤ 2 アクセスポート モードに設定します。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。
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)#
```

インターフェイスコンフィギュレーションの確認

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

コマンド	目的
show interface ethernet slot/port [brief counters debounce description flowcontrol mac-address status transceiver]	インターフェイス設定を表示します。
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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

コマンド	目的
<code>show running-config interface ethernet slot/port</code>	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。
<code>show running-config interface port-channel slot/port</code>	指定されたポートチャネル インターフェイスに関するコンフィギュレーション情報を表示します。

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。

レイヤ2 インターフェイスのモニタリング

レイヤ2 インターフェイスを表示するには、次のコマンドを使用します。

コマンド	目的
<code>clear counters [interface]</code>	カウンタをクリアします。
<code>load- interval {interval seconds {1 2 3}}</code>	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。
<code>show interface counters [module module]</code>	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。
<code>show interface counters detailed [all]</code>	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。
<code>show interface counters errors [module module]</code>	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。

アクセスポートおよびトランクポートの設定例

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

```
switch# configure terminal
switch(config)# interface ethernet 2/30
switch(config-if)# switchport
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 5
switch(config-if)#
```

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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)#
```

その他の参考資料

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.3-25)
- 「標準」 (P.3-26)
- 「管理情報ベース (MIB)」 (P.3-26)

関連資料

関連項目	マニュアル タイトル
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』
VDC	『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x』
ライセンス	『Cisco NX-OS Licensing Guide』
リリース ノート	『Cisco Nexus 7000 Series NX-OS Release Notes, Release 5.x』

■ レイヤ2 インターフェイス設定の機能履歴

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

管理情報ベース (MIB)

MIB	MIB のリンク
<ul style="list-style-type: none"> • BRIDGE-MIB • IF-MIB • CISCO-IF-EXTENSION-MIB • ETHERLIKE-MIB 	<p>MIB を検索およびダウンロードするには、次の URL にアクセスしてください。</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>

レイヤ2 インターフェイス設定の機能履歴

表 3-2 に、この機能のリリース履歴を示します。

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の3つの設定可能なサンプリング間隔	4.2(1)	load-interval コマンドが追加されました。
デフォルト インターフェイス	5.2(1)	複数のインターフェイスの設定をクリアするための default interface コマンドが追加されました。
SVI 自動ステート除外	5.2(1)	ポートの状態が SVI のアップまたはダウン状態に影響しないようにするための switchport autostate exclude コマンドが追加されました。

レイヤ 3 インターフェイスの設定

この章では、Cisco NX-OS デバイスのレイヤ 3 インターフェイスを設定する方法について説明します。

この章は、次の項で構成されています。

- 「レイヤ 3 インターフェイスについて」 (P.4-1)
- 「レイヤ 3 インターフェイスのライセンス要件」 (P.4-5)
- 「注意事項と制約事項」 (P.4-6)
- 「デフォルト設定値」 (P.4-6)
- 「ライセンス 3 インターフェイスの前提条件」 (P.4-5)
- 「レイヤ 3 インターフェイスの設定」 (P.4-6)
- 「レイヤ 3 インターフェイス設定の確認」 (P.4-17)
- 「レイヤ 3 インターフェイスのモニタリング」 (P.4-18)
- 「レイヤ 3 インターフェイスの設定例」 (P.4-19)
- 「関連項目」 (P.4-19)
- 「その他の参考資料」 (P.4-19)
- 「レイヤ 3 インターフェイス設定の機能履歴」 (P.4-20)

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せん。

共有インターフェイスをレイヤ 3 インターフェイスとして設定することはできません。共有インターフェイスについては、『Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500』を参照してください。

Cisco Release 5.2(1) 以降では、ファブリック エクステンダ (FEX) ポートをホスト接続のためのレイヤ 3 インターフェイスとして設定できますが、ルーティング用には設定できません。ファブリック エクステンダに関する詳細については、『Configuring the Cisco Nexus 2000 Series Fabric Extender』を参照してください。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

この項では、次のトピックについて取り上げます。

- 「ルーテッド インターフェイス」 (P.4-2)
- 「サブインターフェイス」 (P.4-2)
- 「VLAN インターフェイス」 (P.4-3)
- 「ループバック インターフェイス」 (P.4-4)
- 「トンネル インターフェイス」 (P.4-4)
- 「High Availability (高可用性)」 (P.4-5)
- 「仮想化のサポート」 (P.4-5)

ルーテッド インターフェイス

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

すべてのイーサネット ポートは、デフォルトでルーテッド インターフェイスです。このデフォルト動作を変更するには、CLI セットアップ スクリプトまたは **system default switchport** コマンドを使用します。

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

Cisco リリース 4.2(1) からスタティック Media Access Control (MAC) アドレスをレイヤ3 インターフェイスに割り当てられます。デフォルトでは、レイヤ3 インターフェイスの MAC アドレスは、割り当て先の VDC の MAC アドレスです。MAC アドレスの設定方法の詳細については、『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 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。

- 入力パケット数/秒
- 出力パケット数/秒
- 入力バイト数/秒
- 出力バイト数/秒

サブインターフェイス

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

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

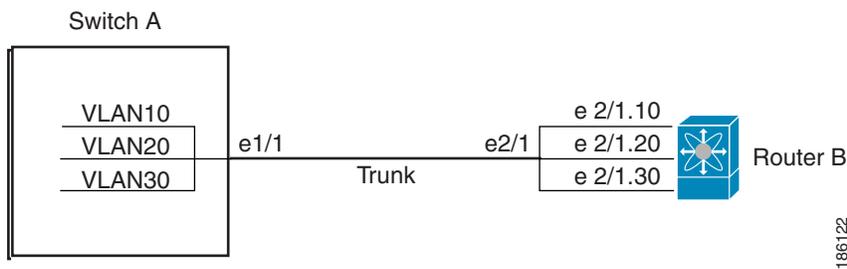
サブインターフェイスの名前は、親インターフェイスの名前（たとえば Ethernet 2/1）+ピリオド（.）+そのインターフェイス独自の番号です。たとえば、イーサネット インターフェイス 2/1 に Ethernet 2/1.1 というサブインターフェイスを作成できます。この場合、.1 はそのサブインターフェイスを表します。

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

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

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

設定の前に VLAN ネットワーク インターフェイス機能をイネーブルにする必要があります。Cisco NX-OS リリース 4.2 から、システムは機能のディセーブル化の前に自動的にチェックポイントを作成するため、このチェックポイントにロールバックできます。ロールバック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 と同じ VDC に VLAN ネットワーク インターフェイスを設定する必要があります。



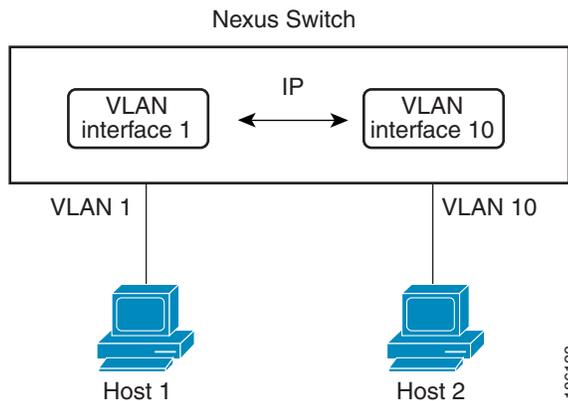
(注) VLAN 1 の VLAN インターフェイスは削除できません。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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



(注)

シャーシ内の F1 シリーズ モジュールを使用して、Cisco Nexus 7000 シリーズ スイッチでインバンド管理のための VLAN インターフェイスを設定できます。

ループバック インターフェイス

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

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

トンネル インターフェイス

Cisco NX-OS は、IP トンネルとしてトンネル インターフェイスをサポートします。IP トンネルを使うと、同じレイヤまたは上位層プロトコルをカプセル化して、2 台のルータ間で作成されたトンネルを通じて IP の結果を転送できます。IP トンネルの詳細については、第 8 章「IP トンネルの設定」を参照してください。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

High Availability（高可用性）

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

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。

仮想化のサポート

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

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

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

VDC については『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, 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 NX-OS Licensing Guide』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 ライセンスがインストールされており、VDC を設定している場合は目的の VDC が入力されている（『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x』を参照）。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- 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

注意事項と制約事項

レイヤ3 インターフェイスの設定には次の注意事項と制約事項があります。

- レイヤ3 インターフェイスをレイヤ2 インターフェイスに変更する場合、Cisco NX-OS はインターフェイスをシャットダウンしてインターフェイスを再度イネーブルにし、レイヤ3 固有の設定をすべて削除します。
- レイヤ2 インターフェイスをレイヤ3 インターフェイスに変更する場合、Cisco NX-OS はインターフェイスをシャットダウンしてインターフェイスを再度イネーブルにし、レイヤ2 固有の設定をすべて削除します。
- Cisco Nexus 2000 ファブリック エクステンダは、そのポートに接続されたデバイスでルーティング プロトコルの隣接に参加できません。直接ルートだけがサポートされます。これは、次のサポートされる接続例両方に適用されます。
 - レイヤ2 モードのファブリック エクステンダ単一ポートまたはポートチャネルを有する SVI。
 - レイヤ3 モードのファブリック エクステンダのポートまたはポートチャネル。
- レイヤ3 のルータ インターフェイスとサブインターフェイスは、F1 I/O モジュールでは設定できません。
- F2 シリーズ I/O モジュールは VLAN 単位の統計情報はサポートしません。したがって、show interface コマンドは、スイッチ仮想インターフェイス (SVI) の VLAN 単位の Rx/Tx カウンタまたは統計情報を表示しません。



(注)

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

デフォルト設定値

表 4-1 は、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です。

表 4-1 レイヤ3 インターフェイスのデフォルト パラメータ

パラメータ (Parameters)	デフォルト
管理ステータス	閉じる

レイヤ3 インターフェイスの設定

この項では、次のトピックについて取り上げます。

- 「ルーテッド インターフェイスの設定」 (P.4-7)
- 「サブインターフェイスの設定」 (P.4-9)

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- 「インターフェイスでの帯域幅の設定」 (P.4-10)
- 「VLAN インターフェイスの設定」 (P.4-11)
- 「Nexus シャーシでのインバンド管理の設定」 (P.4-13)
- 「ループバック インターフェイスの設定」 (P.4-14)
- 「VRF へのインターフェイスの割り当て」 (P.4-15)

ルーテッド インターフェイスの設定

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

はじめる前に

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

手順の概要

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. (任意) `show interfaces`
6. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例: switch# <code>configure terminal</code> switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	<code>interface ethernet slot/port</code> 例: switch(config)# <code>interface ethernet 2/1</code> 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	<code>no switchport</code> 例: switch(config-if)# <code>no switchport</code>	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 に固有の設定をすべて削除します。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	コマンド	目的
ステップ 4	ip address <i>ip-address/length</i> 例: switch(config-if)# ip address 192.0.2.1/8	このインターフェイスの IP アドレスを設定します。IP アドレスの詳細については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x』を参照してください。
	ipv6 address <i>ipv6-address/length</i> 例: switch(config-if)# ipv6 address 2001:0DB8::1/8	このインターフェイスの IPv6 アドレスを設定します。IPv6 アドレスの詳細については、『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 メディアをポイント ツー ポイントまたはブロードキャストのどちらかとして設定するには、**medium** コマンドを使用します。

コマンド	目的
medium { broadcast p2p } 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のどちらかとして設定します。



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

レイヤ 3 インターフェイスをレイヤ 2 インターフェイスに変換するには、**switchport** コマンドを使用します。

コマンド	目的
switchport 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
```

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

インターフェイスのデフォルト設定がルーテッドされます。レイヤ2にインターフェイスを設定するには、**switchport** コマンドを入力します。レイヤ2 インターフェイスをルーテッド インターフェイスに変更する場合は、**no switchport** コマンドを入力します。

サブインターフェイスの設定

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

はじめる前に

親インターフェイスをルーテッド インターフェイスとして設定します。

「ルーテッド インターフェイスの設定」(P.4-7) を参照してください。

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

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

手順の概要

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 vlan-id**
5. (任意) **show interfaces**
6. (任意) **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 モードに入ります。
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 <i>number</i> の範囲は 1 ~ 4094 です。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	コマンド	目的
ステップ 3	ip address <i>ip-address/length</i> 例: switch(config-subif)# ip address 192.0.2.1/8	このサブインターフェイスの IP アドレスを設定します。IP アドレスの詳細については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x』を参照してください。
	ipv6 address <i>ipv6-address/length</i> 例: switch(config-subif)# ipv6 address 2001:0DB8::1/8	このサブインターフェイスの IPv6 アドレスを設定します。IPv6 アドレスの詳細については、『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 <i>vlan-id</i> 例: switch(config-subif)# encapsulation dot1Q 33	サブインターフェイス上の IEEE 802.1Q VLAN カプセル化を設定します。範囲は 2 ~ 4093 です。
ステップ 5	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。上位層プロトコルは帯域幅パラメータを使用してパス コストを計算します。サブインターフェイスの帯域幅は、次のいずれかの方法で設定できます。

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

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

- 親インターフェイスがアップしている場合、サブインターフェイスの帯域幅は親インターフェイスの動作速度と同じです。ポートの場合、サブインターフェイスの帯域幅は設定されているリンク速度またはネゴシエート対象のリンク速度です。ポート チャネルの場合、サブインターフェイスの帯域幅は、ポート チャネルの各メンバのリンク速度の集合です。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- 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 チャンネル 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 チャンネル、またはサブインターフェイスに帯域幅パラメータを設定します。

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

コマンド	目的
bandwidth inherit [value] 例： switch(config-if)# bandwidth inherit 100000	設定された帯域幅の値を継承するように、このインターフェイスのすべてのサブインターフェイスを設定します。値を設定しない場合、サブインターフェイスは親インターフェイスの帯域幅を継承します。指定できる範囲は 1 ~ 10000000 (KB 単位) です。

VLAN インターフェイスの設定

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

はじめる前に

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

手順の概要

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. (任意) **show interface vlan number**
6. (任意) **copy running-config startup-config**

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
ステップ 2	feature interface-vlan 例: switch(config)# feature interface-vlan	VLAN インターフェイス モードをイネーブルにします。
ステップ 3	interface vlan number 例: Switch(config)# interface vlan 10 switch(config-if)#	VLAN インターフェイスを作成します。 <i>number</i> の範囲は 1 ~ 4094 です。
ステップ 4	ip address ip-address/length 例: switch(config-if)# ip address 192.0.2.1/8	この VLAN インターフェイスの IP アドレスを設定します。IP アドレスの詳細については、『Cisco Nexus 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 インターフェイスの IPv6 アドレスを設定します。IPv6 アドレスの詳細については、『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
```

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

Nexus シャーシでのインバンド管理の設定

シャーシ内に F1 シリーズ モジュールのみがある場合に、Cisco Nexus 7000 シリーズ スイッチでインバンド管理のための VLAN インターフェイスを作成できます。



注意

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

はじめる前に

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

手順の概要

1. `configure terminal`
2. `feature interface-vlan`
3. `interface vlan number`
4. `no shutdown`
5. `management`
6. `ip address ip-address/length`
7. (任意) `show interface vlan number`
8. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例： <code>switch# configure terminal</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>feature interface-vlan</code> 例： <code>switch(config)# feature interface-vlan</code>	ループバック インターフェイスを作成します。指定できる範囲は 0 ~ 1023 です。
ステップ 3	<code>interface vlan number</code> 例： <code>Switch(config)# interface vlan 10</code> <code>switch(config-if)#</code>	VLAN インターフェイスを作成します。 <i>number</i> の範囲は 1 ~ 4094 です。 (注) VLAN を設定し、インターフェイスを追加します。
ステップ 4	<code>no shutdown</code> 例： <code>switch(config-if)# no shutdown</code>	インターフェイスを管理上のアップ状態にします（インターフェイスをイネーブルまたはディセーブルにします）。
ステップ 5	<code>management</code> 例： <code>switch(config-if)# management</code>	VLAN インターフェイスの IP アドレスへのインバンド管理アクセスを許可します。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	コマンド	目的
ステップ 6	<pre>ip address ip-address/length</pre> <p>例: switch(config-if)# ip address 192.0.2.1/8</p>	この VLAN インターフェイスの IP アドレスを設定します。IP アドレスの詳細については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x』を参照してください。
ステップ 7	<pre>show interface vlan number</pre> <p>例: switch(config-if)# show interface vlan 10</p>	(任意) レイヤ 3 インターフェイスの統計情報を表示します。
ステップ 8	<pre>copy running-config startup-config</pre> <p>例: switch(config-if)# copy running-config startup-config</p>	(任意) この設定の変更を保存します。

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

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

ループバック インターフェイスの設定

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

はじめる前に

ループバック インターフェイスの IP アドレスが、ネットワークの全ルータで一意であることを確認します。

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

手順の概要

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
ステップ 2	interface loopback instance 例： switch(config)# interface loopback 0 switch(config-if)#	ループバック インターフェイスを作成します。指定できる範囲は 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の IP アドレスを設定します。IP アドレスの詳細については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, 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	
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
```

VRF へのインターフェイスの割り当て

VRF にレイヤ 3 インターフェイスを追加できます。

はじめる前に

正しい VDC を使用していることを確認します (または **switchto vdc** コマンドを使用します)。VRF 用のインターフェイスを設定した後で、トンネル インターフェイスに IP アドレスを割り当てます。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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. (任意) **show vrf [vrf-name] interface interface-type number**
6. (任意) **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 モードに入ります。
ステップ 2	interface interface-type number 例: switch(config)# interface loopback 0 switch(config-if)#	インターフェイス 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の IP アドレスを設定します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。
ステップ 5	show vrf [vrf-name] interface interface-type number 例: switch(config-vrf)# show vrf Enterprise interface loopback 0	(任意) VRF 情報を表示します。
ステップ 6	copy running-config startup-config 例: switch(config)# copy running-config startup-config	(任意) この設定の変更を保存します。

次に、VRF にレイヤ 3 インターフェイスを追加する例を示します。

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

レイヤ3 インターフェイス設定の確認

レイヤ3 の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
<code>show interface ethernet slot/port</code>	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。
<code>show interface ethernet slot/port brief</code>	レイヤ3 インターフェイスの動作ステータスを表示します。
<code>show interface ethernet slot/port capabilities</code>	レイヤ3 インターフェイスの機能（ポート タイプ、速度、およびデュプレックスを含む）を表示します。
<code>show interface ethernet slot/port description</code>	レイヤ3 インターフェイスの説明を表示します。
<code>show interface ethernet slot/port status</code>	レイヤ3 インターフェイスの管理ステータス、ポート モード、速度、およびデュプレックスを表示します。
<code>show interface ethernet slot/port.number</code>	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。
<code>show interface port-channel channel-id.number</code>	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。
<code>show interface loopback number</code>	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。
<code>show interface loopback number brief</code>	ループバック インターフェイスの動作ステータスを表示します。
<code>show interface loopback number description</code>	ループバック インターフェイスの説明を表示します。
<code>show interface loopback number status</code>	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。
<code>show interface vlan number</code>	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。
<code>show interface vlan number brief</code>	VLAN インターフェイスの動作ステータスを表示します。
<code>show interface vlan number description</code>	VLAN インターフェイスの説明を表示します。
<code>show interface vlan number private-vlan mapping</code>	VLAN インターフェイスのプライベート VLAN 情報を表示します。
<code>show interface vlan number status</code>	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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

レイヤ3 インターフェイスのモニタリング

レイヤ3 統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
<code>load- interval {interval seconds {1 2 3}}</code>	Cisco Nexus 7000 シリーズ デバイスの Cisco NX-OS Release 4.2(1) から、3 種類のサンプリング間隔をビットレートおよびパケットレートの統計情報に設定します。VLAN ネットワーク インターフェイスでの範囲は 60 ~ 300 秒であり、レイヤ インターフェイスでの範囲は 30 ~ 300 秒です。
<code>show interface ethernet slot/port counters</code>	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)。
<code>show interface ethernet slot/port counters brief</code>	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。
<code>show interface ethernet slot/port counters detailed [all]</code>	レイヤ3 インターフェイスの統計情報を表示します。オプションとして、32 ビットと 64 ビットのパケットおよびバイト カウンタ (エラーを含む) をすべて含めることができます。
<code>show interface ethernet slot/port counters errors</code>	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。
<code>show interface ethernet slot/port counters snmp</code>	SNMP MIB から報告されたレイヤ3 インターフェイス カウンタを表示します。これらのカウンタはクリアできません。
<code>show interface ethernet slot/port.number counters</code>	サブインターフェイスの統計情報 (ユニキャスト、マルチキャスト、およびブロードキャスト) を表示します。
<code>show interface port-channel channel-id.number counters</code>	ポート チャネル サブインターフェイスの統計情報 (ユニキャスト、マルチキャスト、およびブロードキャスト) を表示します。
<code>show interface loopback number counters</code>	ループバック インターフェイスの入力および出力カウンタ (ユニキャスト、マルチキャスト、およびブロードキャスト) を表示します。
<code>show interface loopback number counters detailed [all]</code>	ループバック インターフェイスの統計情報を表示します。オプションとして、32 ビットと 64 ビットのパケットおよびバイト カウンタ (エラーを含む) をすべて含めることができます。
<code>show interface loopback number counters errors</code>	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。
<code>show interface vlan number counters</code>	VLAN インターフェイスの入力および出力カウンタ (ユニキャスト、マルチキャスト、およびブロードキャスト) を表示します。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

コマンド	目的
<code>show interface vlan number counters detailed [all]</code>	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)。
<code>show interface vlan number counters snmp</code>	SNMP MIB から報告された VLAN インターフェイス カウンタを表示します。これらの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』

その他の参考資料

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.4-20)
- 「[管理情報ベース \(MIB\)](#)」 (P.4-20)
- 「[標準](#)」 (P.4-20)

■ レイヤ3 インターフェイス設定の機能履歴

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

関連資料

関連項目	マニュアル タイトル
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』内の「IP の設定」の章
VLAN	『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x』内の「VLAN の設定」の章

管理情報ベース (MIB)

MIB	MIB のリンク
<ul style="list-style-type: none"> IF-MIB CISCO-IF-EXTENSION-MIB ETHERLIKE-MIB 	<p>MIB を検索およびダウンロードするには、次の URL にアクセスしてください。</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

レイヤ3 インターフェイス設定の機能履歴

表 4-2 に、この機能のリリース履歴を示します。

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
インターフェイス統計情報の3つの設定可能なサンプリング間隔	4.2(1)	load-interval コマンドが追加されました。
レイヤ3 インターフェイス	4.0(1)	この機能が導入されました。

双方向フォワーディング検出の設定

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

この章は、次の項で構成されています。

- 「BFD について」 (P.5-1)
- 「BFD のライセンス要件」 (P.5-4)
- 「BFD の前提条件」 (P.5-4)
- 「注意事項と制約事項」 (P.5-5)
- 「デフォルト設定値」 (P.5-6)
- 「BFD の設定」 (P.5-6)
- 「BFD 設定の確認」 (P.5-26)
- 「BFD のモニタ」 (P.5-26)
- 「BFD の設定例」 (P.5-26)
- 「その他の関連資料」 (P.5-27)
- 「BFD の機能の履歴」 (P.5-27)

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 はプロファイリングおよびプランニングを簡単にし、再コンバージェンス時間の一貫性を保ち、予測可能にします。

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

この項では、次のトピックについて取り上げます。

- 「非同期モード」 (P.5-2)
- 「BFD の障害検出」 (P.5-2)
- 「分散型動作」 (P.5-3)
- 「BFD エコー機能」 (P.5-3)

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- 「セキュリティ」(P.5-4)
- 「High Availability (高可用性)」(P.5-4)
- 「仮想化のサポート」(P.5-4)

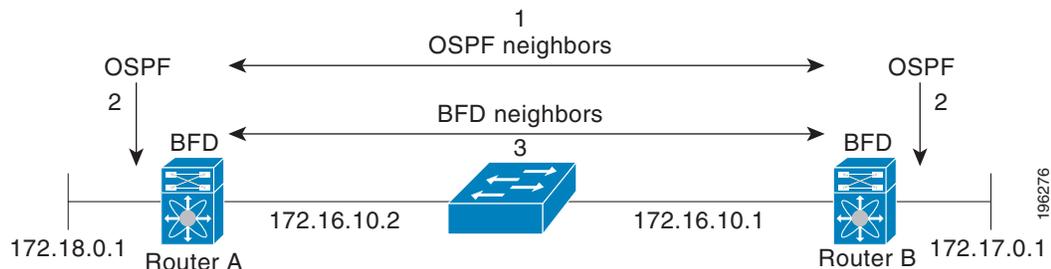
非同期モード

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（または BFD ネイバー）で BFD を設定できます。インターフェイスおよび適切なプロトコルで一度 BFD がイネーブルになると、Cisco NX-OS は BFD セッションを作成し、BFD セッションパラメータをネゴシエートし、BFD 制御パケットをネゴシエートされた間隔で各 BFD ネイバーに送信し始めます。BFD セッションパラメータは、次のとおりです。

- 目的の最小送信間隔：このデバイスが BFD Hello メッセージを送信する間隔。
- 必要最小受信間隔：このデバイスが別の BFD デバイスからの BFD Hello メッセージを受け付ける最小間隔。
- 検出乗数：転送パスの障害を検出するまでに喪失した、別の BFD デバイスからの BFD Hello メッセージの数。

図 5-1 に BFD セッション確立方法を示します。この図は、OSPF と BFD を実行する 2 台のルータがある単純なネットワークを示します。OSPF がネイバーを検出すると (1)、OSPF 隣接ルータで BFD ネイバーセッションを開始する要求が、ローカル BFD プロセスに送信されます (2)。OSPF ネイバルルータとの 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 の障害検出

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。

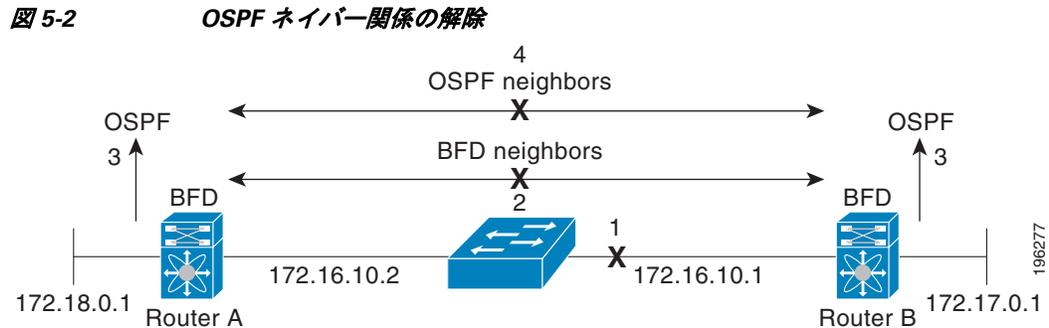
BFD は転送パスに障害を検出したとき、障害検出通知を BFD 対応プロトコルに送信します。ローカル デバイスは、プロトコル再計算プロセスを開始してネットワーク全体の収束時間を削減できます。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

図 5-2 に、ネットワーク (1) で障害が発生した場合を示します。OSPF ネイバー ルータでの BFD ネイバー セッションが停止されます (2)。BFD はローカル OSPF プロセスに BFD ネイバーに接続できなくなったことを通知します (3)。ローカル OSPF プロセスは OSPF ネイバー関係を解除します (4)。代替パスが使用可能な場合、ルータはただちにそのパスでコンバージェンスを開始します。



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



分散型動作

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

BFD エコー機能

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

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



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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

セキュリティ

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

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

High Availability (高可用性)

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

仮想化のサポート

BFD は、仮想ルーティングおよび転送 (VRF) インスタンスをサポートしています。VRF は仮想化デバイス コンテキスト (VDC) 内にあります。デフォルトでは、特に別の VDC および VRF を設定しない限り、Cisco NX-OS によりデフォルト VDC およびデフォルト 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 にはライセンスは不要です。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 NX-OS Licensing Guide』を参照してください。

BFD の前提条件

BFD には、次の前提条件があります。

- BFD 機能をイネーブルにする必要があります (「BFD 機能のイネーブル化」(P.5-7) を参照)。
- BFD をイネーブルにする任意のクライアント プロトコルでは、そのクライアント プロトコルの BFD をイネーブルにします。「ルーティング プロトコルに対する BFD サポートの設定」(P.5-15) 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 メッセージをディセーブルにします。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- デフォルト VDC の同一 IP の送信元および宛先アドレスの IP パケット検証チェックをディセーブルにします。
- 設定作業とともに一覧表示されているその他の詳細な前提条件を参照してください。

注意事項と制約事項

BFD 設定時の注意事項と制約事項は次のとおりです。

- BFD は BFD バージョン 1 をサポートします。
- BFD は IPv4 をサポートします。
- BFD は、シングルホップ BFD をサポートします。
- ボーダー ゲートウェイ プロトコル (BGP) の BFD は、シングルホップ External BGP (EBGP) および Internal BGP (iBGP) ピアをサポートしています。
- BFD は、Cisco NX-OS リリース 5.2 以降ではキー付き SHA-1 認証をサポートします。
- BFD は、次のレイヤ 3 インターフェイスをサポートします。物理インターフェイス、ポート チャネル、サブインターフェイス、および VLAN インターフェイス。
- BFD はレイヤ 3 隣接情報に応じて、レイヤ 2 のトポロジ変更を含むトポロジ変更を検出します。レイヤ 3 隣接情報が使用できない場合、VLAN インターフェイス (SVI) の BFD セッションはレイヤ 2 トポロジのコンバージェンス後に稼働しない可能性があります。
- ポート チャネル設定の制限事項
 - BFD で使用されるレイヤ 3 ポート チャネルでは、ポート チャネルの LACP をイネーブルにする必要があります。
 - SVI のセッションで使用されるレイヤ 2 ポート チャネルでは、ポート チャネルの LACP をイネーブルにする必要があります。
- SVI の制限事項
 - ASIC リセットにより他のポートのトラフィックが中断されます。このイベントは、その他のポートの SVI セッションがフラップする原因になることがあります。ASIC がリセットする既存のトリガーには、VDC をリロードしている VDC 間のポート移動があります。また、キャリア インターフェイスが仮想ポート チャネル (vPC) の場合、BFD は SVI インターフェイスではサポートされません。
 - トポロジを変更すると (たとえば、VLAN へのリンクの追加または削除、レイヤ 2 ポート チャネルからのメンバの削除など)、SVI セッションが影響を受ける場合があります。SVI セッションはダウンした後、トポロジ ディスカバリの終了後に起動する場合があります。



ヒント

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

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。



(注) (たとえば、OSPF から) ルータレベルで BFD をイネーブルにすると、N7K-F132XL-15 ラインカードを通した BFD セッションは発生しません。OSPF およびその他のルーティングプロトコルについては、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x』を参照してください。

- 分散レイヤ 3 ポート チャンネルで BFD エコー機能を設定した場合、メンバー モジュールをリロードすると、そのモジュールでホストされた BFD セッションがフラップされ、そのためパケット損失が発生します。

レイヤ 2 スイッチを間に入れずに BFD ピアを直接接続する場合、代替策として BFD per-link モードを使用できます。



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

- IPv4 に対する HSRP は、BFD でサポートされます。IPv6 に対する HSRP は、BFD でサポートされていません。
- サポートされている Cisco NX-OS デバイス ラインカードによって生成される BFD パケットは COS 6/DSCP CS6 とともに送信されます。BFD パケットの DSCP/COS 値は、ユーザが設定可能な値ではありません。

デフォルト設定値

表 5-1 に、BFD パラメータのデフォルト設定を示します。

表 5-1 デフォルトの BFD パラメータ

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

BFD の設定

この項では、次のトピックについて取り上げます。

- 「設定階層」(P.5-7)
- 「BFD 設定のタスク フロー」(P.5-7)

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- 「BFD 機能のイネーブル化」 (P.5-7)
- 「グローバルな BFD パラメータの設定」 (P.5-8)
- 「インターフェイスでの BFD の設定」 (P.5-9)
- 「ポート チャネルの BFD の設定」 (P.5-11)
- 「BFD エコー機能の設定」 (P.5-12)
- 「サブインターフェイスの BFD の最適化」 (P.5-14)
- 「ルーティング プロトコルに対する BFD サポートの設定」 (P.5-15)

設定階層

グローバル レベル、およびインターフェイスまたはサブインターフェイス レベルで BFD を設定できます (物理インターフェイスとポート チャネルの場合)。インターフェイスまたはサブインターフェイスの設定は、グローバル コンフィギュレーションよりも優先されます。サポートされているインターフェイス上で、サブインターフェイス レベルの設定は、サブインターフェイスの最適化がイネーブルになっていない限りインターフェイスまたはポート チャネル設定よりも優先されます。詳細については、「サブインターフェイスの BFD の最適化」 (P.5-14) を参照してください。



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

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

BFD 設定のタスク フロー

BFD の設定には、次の作業を行います。

- ステップ 1 BFD 機能のイネーブル化。
- ステップ 2 グローバルな BFD パラメータの設定またはインターフェイスでの BFD の設定。
- ステップ 3 ルーティング プロトコルに対する BFD サポートの設定。

BFD 機能のイネーブル化

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

はじめる前に

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

手順の概要

1. `configure terminal`
2. `feature bfd`
3. (任意) `show feature | include bfd`
4. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例: switch# <code>configure terminal</code> switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	<code>feature bfd</code> 例: switch(config)# <code>feature bfd</code>	BFD 機能をイネーブルにします。
ステップ 3	<code>show feature include bfd</code> 例: switch(config)# <code>show feature include bfd</code>	(任意) イネーブルおよびディセーブルにされた機能を表示します。
ステップ 4	<code>copy running-config startup-config</code> 例: switch(config)# <code>copy running-config startup-config</code>	(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
<code>no feature bfd</code> 例: switch(config)# <code>no feature bfd</code>	BFD 機能をディセーブルにして、関連するすべての設定を削除します。

グローバルな BFD パラメータの設定

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

インターフェイスのグローバルなセッション パラメータを無効にするには、「[インターフェイスでの BFD の設定](#)」(P.5-9) を参照してください。

はじめる前に

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

BFD 機能をイネーブルにします。「[BFD 機能のイネーブル化](#)」(P.5-7) を参照してください。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

手順の概要

1. `configure terminal`
2. `bfd interval mintx min_rx msec multiplier value`
3. `bfd slow-timer [interval]`
4. (任意) `show running-config bfd`
5. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例: <code>switch# configure terminal</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>bfd interval <i>mintx</i> <i>min_rx</i> <i>msec</i> <i>multiplier</i> <i>value</i></code> 例: <code>switch(config)# bfd interval 50 min_rx 50 multiplier 3</code>	デバイスのすべての BFD セッションの BFD セッションパラメータを設定します。インターフェイスで BFD セッションパラメータを設定することにより、これらの値を無効にすることができます。 <i>mintx</i> および <i>msec</i> の範囲は 50 ~ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ~ 50 です。乗数のデフォルトは 3 です。
ステップ 3	<code>bfd slow-timer [<i>interval</i>]</code> 例: <code>switch(config)# bfd slow-timer 2000.</code>	エコー機能で使用される slow timer を設定します。この値はエコー機能がイネーブルの場合、BFD が新しいセッションを開始する速度および非同期セッションが BFD 制御パケットに使用する速度を決定します。slow-timer 値は新しい制御パケット間隔として使用されますが、エコーパケットは設定された BFD 間隔を使用します。エコーパケットはリンク障害検出に使用されますが、低速の制御パケットは BFD セッションを維持します。指定できる範囲は 1000 ~ 30000 ミリ秒です。デフォルトは 2000 です。
ステップ 4	<code>show running-config bfd</code> 例: <code>switch(config)# show running-config bfd</code>	(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	<code>copy running-config startup-config</code> 例: <code>switch(config)# copy running-config startup-config</code>	(任意) この設定の変更を保存します。

インターフェイスでの BFD の設定

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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

はじめる前に

正しい VDC を使用していることを確認します（または `switchto vdc` コマンドを使用します）。BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」(P.5-7) 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. (任意) `bfd authentication keyed-sha1 keyid id key ascii_key`
5. (任意) `show running-config bfd`
6. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例: <code>switch# configure terminal</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>interface int-if</code> 例: <code>switch(config)# interface ethernet 2/1</code> <code>switch(config-if)#</code>	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。? サポートされているインターフェイスを表示します。
ステップ 3	<code>bfd interval mintx min_rx msec multiplier value</code> 例: <code>switch(config-if)# bfd interval 50</code> <code>min_rx 50 multiplier 3</code>	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。これはグローバルな BFD セッション パラメータより優先されます。 <i>mintx</i> および <i>msec</i> の範囲は 50 ~ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ~ 50 です。乗数のデフォルトは 3 です。
ステップ 4	<code>bfd authentication keyed-sha1 keyid id key ascii_key</code> 例: <code>switch(config-if)# bfd authentication</code> <code>keyed-sha1 keyid 1 ascii_key cisco123</code>	(任意) インターフェイス上のすべての BFD セッションの SHA-1 認証を設定します。 <i>ascii_key</i> 文字列は BFD ピア間で共有される秘密キーです。0 ~ 255 の数値の <i>id</i> 値が、この特定の <i>ascii_key</i> に割り当てられます。BFD パケットは <i>id</i> でキーを指定し、複数のアクティブ キーが使用できます。インターフェイスの SHA-1 認証をディセーブルにするには、コマンドの no 形式を使用します。
ステップ 5	<code>show running-config bfd</code> 例: <code>switch(config-if)# show running-config</code> <code>bfd</code>	(任意) BFD 実行コンフィギュレーションを表示します。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	コマンド	目的
ステップ 6	<pre>copy running-config startup-config</pre> <p>例： switch(config-if)# copy running-config startup-config</p>	(任意) この設定の変更を保存します。

ポート チャネルの BFD の設定

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

この設定は、設定されたポート チャネルのグローバル セッション パラメータより優先されません。ポート チャネルのメンバポートはメンバポートのサブインターフェイス レベルで BFD パラメータを設定しない限り、ポート チャネルの BFD セッション パラメータを継承します。その場合、サブインターフェイス最適化がイネーブルにされていないならば、メンバポート サブインターフェイスはサブインターフェイス BFD コンフィギュレーションを使用します。詳細については、「サブインターフェイスの BFD の最適化」(P.5-14) を参照してください。

はじめる前に

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

BFD 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.5-7) 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. (任意) `bfd authentication keyed-sha1 keyid id key ascii_key`
6. (任意) `show running-config bfd`
7. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<pre>configure terminal</pre> <p>例： switch# configure terminal switch(config)#</p>	コンフィギュレーション モードに入ります。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	コマンド	目的
ステップ 2	<code>interface port-channel number</code> 例: <code>switch(config)# interface port-channel 2</code> <code>switch(config-if)#</code>	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ている番号の範囲を表示します。
ステップ 3	<code>bfd per-link</code> 例: <code>switch(config-if)# bfd per-link</code>	ポート チャネルのリンクごとに BFD セッションを設定します。
ステップ 4	<code>bfd interval mintx min_rx msec multiplier value</code> 例: <code>switch(config-if)# bfd interval 50</code> <code>min_rx 50 multiplier 3</code>	(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。これはグローバルな 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	<code>bfd authentication keyed-sha1 keyid id key ascii_key</code> 例: <code>switch(config-if)# bfd authentication</code> <code>keyed-sha1 keyid 1 ascii_key cisco123</code>	(任意) インターフェイス上のすべての BFD セッションの SHA-1 認証を設定します。ascii_key 文字列は BFD ピア間で共有される秘密キーです。0 ~ 255 の数値の id 値が、この特定の ascii_key に割り当てられます。BFD パケットは id でキーを指定し、複数のアクティブ キーが使用できます。 インターフェイスの SHA-1 認証をディセーブルにするには、コマンドの no 形式を使用します。
ステップ 6	<code>show running-config bfd</code> 例: <code>switch(config-if)# show running-config</code> <code>bfd</code>	(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 7	<code>copy running-config startup-config</code> 例: <code>switch(config-if)# copy running-config</code> <code>startup-config</code>	(任意) この設定の変更を保存します。

BFD エコー機能の設定

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

はじめる前に

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

BFD 機能をイネーブルにします。「[BFD 機能のイネーブル化](#)」(P.5-7) 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。(「[グローバルな BFD パラメータの設定](#)」(P.5-8) または「[インターフェイスでの BFD の設定](#)」(P.5-9) を参照)。

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

同一の送信元アドレスおよび宛先アドレスを調べる IP パケット検証チェックがディセーブルになっていることを確認します。デフォルト VDC では **no hardware ip verify address identical** コマンドを使用します。このコマンドの詳細については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, 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. (任意) **show running-config bfd**
6. (任意) **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 モードに入ります。
ステップ 2	bfd slow-timer echo-interval 例： switch(config)# bfd slow-timer 2000	エコー機能で使用される slow timer を設定します。この値は BFD が新しいセッションを開始する速度を決定し、BFD エコー機能がイネーブルの場合に非同期セッションの速度を低下させるために使用されます。この値は、エコー機能がイネーブルの場合、必要最小受信間隔より優先されます。指定できる範囲は 1000 ~ 30000 ミリ秒です。デフォルトは 2000 です。
ステップ 3	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。? サポートされているインターフェイスを表示します。
ステップ 4	bfd echo 例： switch(config-if)# bfd echo	エコー機能をイネーブルにします。デフォルトではイネーブルになっています。
ステップ 5	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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

サブインターフェイスの BFD の最適化

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

はじめる前に

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

BFD 機能をイネーブルにします。「[BFD 機能のイネーブル化](#)」(P.5-7) 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。（「[グローバルな BFD パラメータの設定](#)」(P.5-8) または「[インターフェイスでの BFD の設定](#)」(P.5-9) を参照）。

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例: <code>switch# configure terminal</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>interface int-if</code> 例: <code>switch(config)# interface ethernet 2/1</code> <code>switch(config-if)#</code>	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。? サポートされているインターフェイスを表示します。
ステップ 3	<code>bfd optimize subinterface</code> 例: <code>switch(config-if)# bfd optimize</code> <code>subinterface</code>	BFD 対応インターフェイスのサブインターフェイスを最適化します。デフォルトではディセーブルになっています。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	コマンド	目的
ステップ 4	<pre>show running-config bfd</pre> <p>例： switch(config-if)# show running-config bfd</p>	(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	<pre>copy running-config startup-config</pre> <p>例： switch(config-if)# copy running-config startup-config</p>	(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に対する BFD サポートの設定

この項では、次のトピックについて取り上げます。

- 「BGP での BFD の設定」 (P.5-15)
- 「EIGRP 上での BFD の設定」 (P.5-16)
- 「OSPF での BFD の設定」 (P.5-18)
- 「IS-IS での BFD の設定」 (P.5-19)
- 「HSRP での BFD の設定」 (P.5-20)
- 「VRRP での BFD の設定」 (P.5-21)
- 「Protocol Independent Multicast (PIM) 上での BFD の設置」 (P.5-23)
- 「スタティックルートでの BFD の設定」 (P.5-24)
- 「MPLS TE 高速再ルーティングの BFD 設定」 (P.5-25)
- 「インターフェイスにおける BFD のディセーブル化」 (P.5-25)

BGP 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。

はじめる前に

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

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」 (P.5-7) 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。「グローバルな BFD パラメータの設定」 (P.5-8) または「インターフェイスでの BFD の設定」 (P.5-9) を参照。

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`

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

5. (任意) `show running-config bgp`
6. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例: <code>switch# configure terminal</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>router bgp as-number</code> 例: <code>switch(config)# router bgp 64496</code> <code>switch(config-router)#</code>	BGP をイネーブルにして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による <code>xx.xx</code> という形式です。
ステップ 3	<code>neighbor {ip-address ipv6-address} remote-as as-number</code> 例: <code>switch(config-router)# neighbor 209.165.201.1 remote-as 64497</code> <code>switch(config-router-neighbor)#</code>	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。 <code>ip-address</code> の形式は <code>x.x.x.x</code> です。 <code>ipv6-address</code> の形式は <code>A::B::C:D</code> です。
ステップ 4	<code>bfd</code> 例: <code>switch(config-router-neighbor)# bfd</code>	この BGP ピアの BFD をイネーブルにします。
ステップ 5	<code>show running-config bgp</code> 例: <code>switch(config-router-neighbor)# show running-config bgp</code>	(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	<code>copy running-config startup-config</code> 例: <code>switch(config-router-neighbor)# copy running-config startup-config</code>	(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 BFD を設定できます。

はじめる前に

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

BFD 機能をイネーブルにします。「[BFD 機能のイネーブル化](#)」(P.5-7) 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。「[グローバルな BFD パラメータの設定](#)」(P.5-8) または「[インターフェイスでの BFD の設定](#)」(P.5-9) を参照。

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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

手順の概要

1. `configure terminal`
2. `router eigrp instance-tag`
3. `bfd`
4. `interface int-if`
5. (任意) `ip eigrp instance-tag bfd`
6. (任意) `show ip eigrp [vrf vrf-name] [interfaces if]`
7. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例: <code>switch# configure terminal</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>router eigrp instance-tag</code> 例: <code>switch(config)# router eigrp Test1</code> <code>switch(config-router)#</code>	インスタンス タグを設定して、新しい EIGRP プロセスを作成します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。 AS 番号であると認められていない <code>instance-tag</code> を設定する場合は、 <code>autonomous-system</code> コマンドを使用して AS 番号を明示的に設定する必要があります。そうしないと、この EIGRP インスタンスはシャットダウン状態のままになります。
ステップ 3	<code>bfd</code> 例: <code>switch(config-router-neighbor)# bfd</code>	(任意) すべての EIGRP インターフェイスの BFD をイネーブルにします。
ステップ 4	<code>interface int-if</code> 例: <code>switch(config-router-neighbor)#</code> <code>interface ethernet 2/1</code> <code>switch(config-if)#</code>	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。? サポートされているインターフェイスを表示します。
ステップ 5	<code>ip eigrp instance-tag bfd</code> 例: <code>switch(config-if)# ip eigrp Test1 bfd</code>	(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。 デフォルトではディセーブルになっています。
ステップ 6	<code>show ip eigrp [vrf vrf-name] [interfaces if]</code> 例: <code>switch(config-if)# show ip eigrp</code>	(任意) EIGRP に関する情報を表示します。 <code>vrf-name</code> には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	コマンド	目的
ステップ 1	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 での BFD の設定

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

はじめる前に

正しい VDC を使用していることを確認します (または **switchto vdc** コマンドを使用します)。BFD 機能をイネーブルにします。「[BFD 機能のイネーブル化](#)」(P.5-7) 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。(「[グローバルな BFD パラメータの設定](#)」(P.5-8) または「[インターフェイスでの BFD の設定](#)」(P.5-9) を参照)。

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. (任意) **if ospf bfd**
6. (任意) **show ip ospf [vrf vrf-name] [interface if]**
7. (任意) **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 モードに入ります。
ステップ 2	router ospf instance-tag 例: switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
ステップ 3	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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	コマンド	目的
ステップ 4	interface <i>int-if</i> 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。? サポートされてい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。デフォルトではディセーブルになっています。
ステップ 6	show ip ospf [<i>vrf vrf-name</i>] [interface <i>if</i>] 例： switch(config-if)# show ip ospf	(任意) OSPF に関する情報を表示します。 <i>vrf-name</i> には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。
ステップ 7	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) プロトコルで BFD を設定できます。

はじめる前に

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

BFD 機能をイネーブルにします。「[BFD 機能のイネーブル化](#)」(P.5-7) 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。「[グローバルな BFD パラメータの設定](#)」(P.5-8) または「[インターフェイスでの BFD の設定](#)」(P.5-9) を参照。

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. (任意) **isis bfd**
6. (任意) **show isis** [*vrf vrf-name*] [**interface** *if*]
7. (任意) **copy running-config startup-config**

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
ステップ 2	router isis instance-tag 例: switch(config)# router isis Enterprise switch(config-router)#	<i>instance tag</i> を設定して、新しい IS-IS インスタンスを作成します。
ステップ 3	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。? サポートされてい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。デフォルトではディセーブルになっています。
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。 <i>vrf-name</i> には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。
ステップ 7	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。

HSRP での BFD の設定

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

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

はじめる前に

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

BFD 機能をイネーブルにします。「[BFD 機能のイネーブル化](#)」(P.5-7) 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。「[グローバルな BFD パラメータの設定](#)」(P.5-8) または「[インターフェイスでの BFD の設定](#)」(P.5-9) を参照)。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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. `hsrp bfd all-interfaces`
3. `interface int-if`
4. (任意) `hsrp bfd`
5. (任意) `show running-config hsrp`
6. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例： switch# configure terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 1	<code>hsrp bfd all-interfaces</code> 例： switch# hsrp bfd all-interfaces	(任意) すべての HSRP インターフェイスで BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 2	<code>interface int-if</code> 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。? サポートされているインターフェイスを表示します。
ステップ 3	<code>hsrp bfd</code> 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。デフォルトではディセーブルになっています。
ステップ 4	<code>show running-config hsrp</code> 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	<code>copy running-config startup-config</code> 例： switch(config-if)# copy running-config startup-config	(任意) この設定の変更を保存します。

VRRP での BFD の設定

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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

はじめる前に

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

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」(P.5-7) 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。（「グローバルな BFD パラメータの設定」(P.5-8) または 「インターフェイスでの BFD の設定」(P.5-9) を参照）。

VRRP 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. `vrrp bfd`
4. (任意) `show running-config vrrp`
5. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例： <code>switch# configure terminal</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>interface int-if</code> 例： <code>switch(config)# interface ethernet 2/1</code> <code>switch(config-if)#</code>	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。? サポートされているインターフェイスを表示します。
ステップ 3	<code>vrrp bfd</code> 例： <code>switch(config-if)# vrrp bfd</code>	VRRP インターフェイスで BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 4	<code>show running-config vrrp</code> 例： <code>switch(config-if)# show running-config vrrp</code>	(任意) VRRP 実行コンフィギュレーションを表示します。
ステップ 5	<code>copy running-config startup-config</code> 例： <code>switch(config-if)# copy running-config startup-config</code>	(任意) この設定の変更を保存します。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

Protocol Independent Multicast (PIM) 上での BFD の設置

Protocol Independent Multicast (PIM) で BFD を設定できます。

はじめる前に

正しい VDC を使用していることを確認します (または `switchto vdc` コマンドを使用します)。BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」(P.5-7) 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. (任意) `ip pim bfd-instance [disable]`
5. (任意) `show running-config pim`
6. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例: <code>switch# configure terminal</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>ip pim bfd</code> 例: <code>switch(config)# ip pim bfd</code>	PIM の BFD をイネーブルにします。
ステップ 3	<code>interface int-if</code> 例: <code>switch(config)# interface ethernet 2/1</code> <code>switch(config-if)#</code>	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ている番号の範囲を表示します。
ステップ 4	<code>ip pim bfd-instance [disable]</code> 例: <code>switch(config-if)# ip pim bfd-instance</code>	(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。デフォルトではディセーブルになっています。
ステップ 5	<code>show running-config pim</code> 例: <code>switch(config)# show running-config pim</code>	(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	<code>copy running-config startup-config</code> 例: <code>switch(config)# copy running-config startup-config</code>	(任意) この設定の変更を保存します。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

スタティックルートでのBFDの設定

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

はじめる前に

正しいVDCを使用していることを確認します (または `switchto vdc` コマンドを使用します)。BFD機能をイネーブルにします。「[BFD機能のイネーブル化](#)」(P.5-7)を参照してください。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例: <code>switch# configure terminal</code> <code>switch(config)#</code>	コンフィギュレーションモードに入ります。
ステップ 2	<code>vrf context vrf-name</code> 例: <code>switch(config)# vrf context Red</code> <code>switch(config-vrf)#</code>	(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	<code>ip route route interface {nh-address nh-prefix}</code> 例: <code>switch(config-vrf)# ip route 192.0.2.1</code> <code>ethernet 2/1 192.0.2.4</code>	スタティックルートを作り「?」を使用します。サポートされているインターフェイスを表示します。
ステップ 4	<code>ip route static bfd interface {nh-address nh-prefix}</code> 例: <code>switch(config-vrf)# ip route static bfd</code> <code>ethernet 2/1 192.0.2.4</code>	インターフェイスのすべてのスタティックルートのBFDをイネーブルにします。? サポートされているインターフェイスを表示します。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	コマンド	目的
ステップ 5	<pre>show ip route static [vrf vrf-name]</pre> <p>例： switch(config-vrf)# show ip route static vrf Red</p>	(任意) スタティック ルートを表示します。
ステップ 6	<pre>copy running-config startup-config</pre> <p>例： switch(config-vrf)# copy running-config startup-config</p>	(任意) この設定の変更を保存します。

MPLS TE 高速再ルーティングの BFD 設定

MPLS トラフィック エンジニアリング (TE) は BFD を使用して、ノード障害の検出を高速化し、転送パス障害の検出時間を短縮します。MPLS TE 高速再ルーティングの BFD は、トンネルで高速再ルーティングをイネーブルにすると自動的に設定されます。詳細については、『Cisco Nexus 7000 Series NX-OS Multiprotocol Label Switching Configuration Guide, Release 5.x』の「Configuring MPLS TE Fast Reroute Link and Node Protection (MPLS TE 高速再ルーティングのリンクおよびノード保護の設定)」の章を参照してください。

インターフェイスにおける BFD のディセーブル化

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

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

コマンド	目的
<pre>ip eigrp instance-tag bfd disable</pre> <p>例： switch(config-if)# ip eigrp Test1 bfd disable</p>	EIGRP インターフェイスで BFD をディセーブルにします。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
<pre>ip ospf bfd disable</pre> <p>例： switch(config-if)# ip ospf 201 bfd disable</p>	OSPFv2 インターフェイスで BFD をディセーブルにします。
<pre>isis bfd disable</pre> <p>例： switch(config-if)# isis bfd disable</p>	IS-IS インターフェイスで BFD をディセーブルにします。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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

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

BFD のモニタ

BFD を表示するには、次のコマンドを使用します。

コマンド	目的
<code>show bfd neighbors [application name] [details]</code>	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。
<code>show bfd neighbors [interface int-if] [details]</code>	インターフェイスの BGP セッションに関する情報を表示します。
<code>show bfd neighbors [dest-ip ip-address] [src-ip ip-address] [details]</code>	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。
<code>show bfd neighbors [vrf vrf-name] [details]</code>	VRF の BFD に関する情報を表示します。

これらのコマンド出力のフィールドの詳細については、『Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, 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
```

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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.5-27)
- 「RFC」 (P.5-27)
- 「BFD の機能の履歴」 (P.5-27)

関連資料

関連項目	マニュアルタイトル
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
RFC 5880	双方向フォワーディング検出 (BFD)
RFC 5881	『BFD for IPv4 and IPv6 (Single Hop)』

BFD の機能の履歴

表 5-2 に、この機能のリリース履歴を示します。

表 5-2 BFD 機能の履歴

機能名	リリース	機能情報
BFD 認証	5.2(1)	キー付き SHA-1 認証は BFD パケットでサポートされます。
VRRP 用 BFD	5.2(1)	VRRP の BFD のサポートが追加されました。
BFD	5.0(2)	この機能が導入されました。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。



ポート チャンネルの設定

この章では、Cisco NX-OS デバイスにポート チャンネルをより有効的に使用するためにポート チャンネルを設定し、Link Aggregation Control Protocol (LACP) を適用して設定する方法について説明します。

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

この章は、次の項で構成されています。

- 「ポート チャンネルについて」 (P.6-1)
- 「ポート チャンネリングのライセンス要件」 (P.6-15)
- 「ポート チャンネリングの前提条件」 (P.6-15)
- 「注意事項と制約事項」 (P.6-15)
- 「デフォルト設定」 (P.6-16)
- 「ポート チャンネルの設定」 (P.6-16)
- 「ポートチャンネル設定の確認」 (P.6-42)
- 「ポート チャンネル インターフェイス コンフィギュレーションのモニタリング」 (P.6-43)
- 「ポート チャンネルの設定例」 (P.6-44)
- 「その他の関連資料」 (P.6-44)
- 「ポート チャンネル設定の機能履歴」 (P.6-45)

ポート チャンネルについて

ポート チャン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 チャンネルに最大 8つの個別アクティブ リンクをバンドルして、帯域幅と冗長性を向上させることができます。ポート チャンネリングはまた、M シリーズ モジュールおよびこれらの物理インターフェイス全体でトラフィックのロード バランシングも行います。ポート チャン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 チャンネルは動作しています。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。



(注)

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

ポートチャネルの一部になるように共有インターフェイスを設定できません。共有インターフェイスに関する詳細については、『Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500』を参照してください。

レイヤ 2 ポートチャネルに適合するレイヤ 2 インターフェイスをバンドルすれば、レイヤ 2 ポートチャネルを作成できます。レイヤ 3 ポートチャネルに適合するレイヤ 3 インターフェイスをバンドルすれば、レイヤ 3 ポートチャネルを作成できます。レイヤ 3 ポートチャネルを作成したら、ポートチャネルインターフェイスに IP アドレスを追加してレイヤ 3 ポートチャネルにサブインターフェイスを作成できます。レイヤ 2 インターフェイスとレイヤ 3 インターフェイスを同一のポートチャネルで組み合わせることはできません。

Cisco NX-OS Release 4.2 から、ポートセキュリティをポートチャネルに適用できます。ポートセキュリティの詳細については、『Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 5.X』を参照してください。

ポートチャネル内のすべてのポートは、同じ仮想デバイスコンテキスト (VDC) にある必要があります。VDC にまたがってポートチャネルを設定することはできません。

ポートチャネルをレイヤ 3 からレイヤ 2 に変更することもできます。レイヤ 2 インターフェイスの作成手順については、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、スパニングツリープロトコル (STP) パラメータをポートチャネルに設定すると、Cisco NX-OS ソフトウェアはこれらのパラメータをポートチャネルのそれぞれのインターフェイスに適用します。



(注)

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

サブインターフェイスが論理ポートチャネルインターフェイスの一部であっても、レイヤ 3 ポートチャネルにサブインターフェイスを作成できます。ポートチャネルサブインターフェイスの詳細については、「サブインターフェイス」(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。共有インターフェイスでは LACP を設定できません。

LACP については、「LACP の概要」(P.6-9) を参照してください。

この項では、次のトピックについて取り上げます。

- 「ポートチャネル」(P.6-3)
- 「ポートチャネルインターフェイス」(P.6-4)
- 「基本設定」(P.6-4)
- 「互換性要件」(P.6-5)
- 「ポートチャネルを使ったロードバランシング」(P.6-7)

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- 「LACP」 (P.6-8)
- 「仮想化のサポート」 (P.6-14)
- 「High Availability (高可用性)」 (P.6-14)

ポートチャネル

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



(注)

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

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

ただし、LACPをイネーブルにすればポートチャネルをより柔軟に使用できます。LACPを使ってポートチャネルを設定する場合とスタティックポートチャネルを使って設定する場合は、手順が多少異なります（「ポートチャネルの設定」(P.6-16)を参照）。



(注)

デバイスのポートチャネルはポート集約プロトコル (PAgP) をサポートしません。

各ポートにはポートチャネルが1つだけあります。ポートチャネルのすべてのポートには互換性があり、同じ速度とデュプレックスモードを使用します（「互換性要件」(P.6-5)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.6-10)を参照）。

ポートチャネルインターフェイスを作成すると、ポートチャネルを直接作成できます。またはチャネルグループを作成して個別ポートをバンドルに集約させることができます。インターフェイスをチャネルグループに関連付けると、ポートチャネルがない場合は対応するポートチャネルが自動的に作成されます。この場合、ポートチャネルは最初のインターフェイスのレイヤ2またはレイヤ3設定を行います。最初にポートチャネルを作成することもできます。この場合は、Cisco NX-OS ソフトウェアがポートチャネルと同じチャネル番号の空のチャネルグループを作成してデフォルトレイヤ2またはレイヤ3設定を行い、互換性も設定します（「互換性要件」(P.6-5)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)

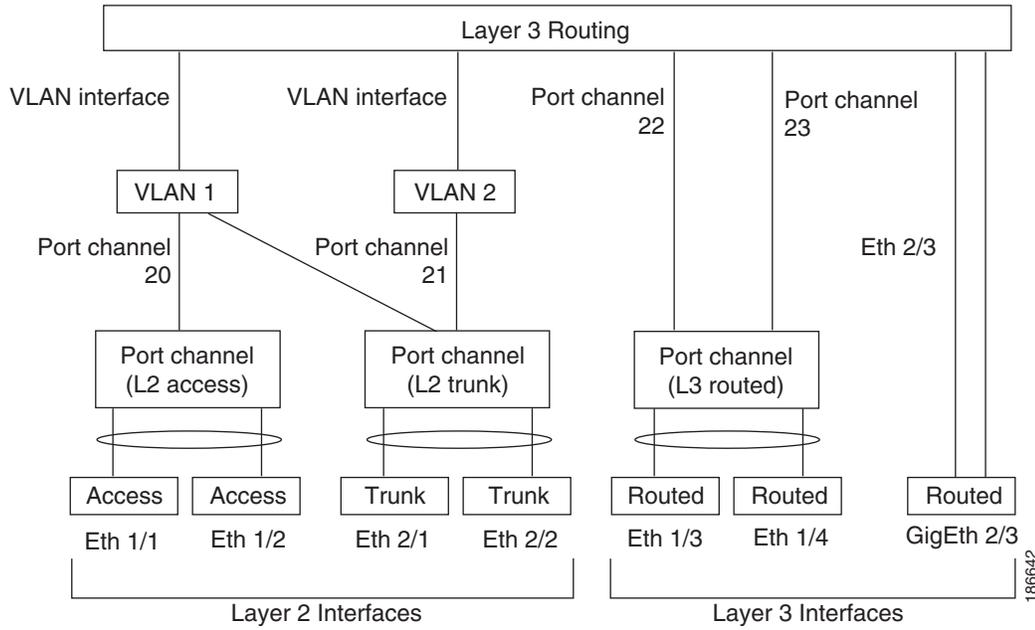
少なくともメンバポートの1つがアップしており、かつそのポートのチャネルが有効であれば、ポートチャネルは動作上アップ状態にあります。メンバポートがすべてダウンしていれば、ポートチャネルはダウンしています。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 MAC アドレスを使用してレイヤ3ポートチャネルを設定できます。この値を設定しない場合、レイヤ3ポートチャネルは、最初にアップになるチャネルメンバのルータMACを使用します。レイヤ3ポートチャネルでのスタティックMACアドレス設定については、『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：この設定は情報目的で使用します。上位レベルプロトコルで使用されます。
- 遅延：この設定は情報目的で使用します。上位レベルプロトコルで使用されます。
- 説明
- Duplex

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- フロー制御。
- IP アドレス : IPv4 および IPv6
- 最大伝送単位 (MTU)
- シャットダウン
- 速度

互換性要件

チャネルグループにインターフェイスを追加する場合、ソフトウェアは特定のインターフェイス属性をチェックし、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 NX-OS ソフトウェアはインターフェイスの多数の動作属性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。

- ネットワーク層
- (リンク) 速度性能
- 速度設定
- デュプレックス性能
- デュプレックス設定
- ポートモード
- アクセス VLAN
- トランクネイティブ VLAN
- タグ付きまたは非タグ付き
- 許可 VLAN リスト
- 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 NX-OS で使用される完全な互換性チェック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。

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

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

- (リンク) 速度性能
- 速度設定

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- 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加入すると、個々のパラメータの一部が削除され、次のようなポートチャネルの値に置き換えられます。

- 帯域幅
- 遅延
- UDP の拡張認証プロトコル
- VRF
- IP アドレス (v4 および v6)
- MAC address
- スパニングツリープロトコル
- NAC
- サービスポリシー
- アクセスコントロールリスト (ACL)

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

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

ポートチャネルインターフェイスにサブインターフェイスを設定し、ポートチャネルのメンバポートを削除すると、ポートチャネルサブインターフェイスの設定はメンバポートに伝わりません。



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

ポートチャネルモードについては、「[LACP マーカーレスポンド](#)」(P6-12) を参照してください。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

ポートチャネルを使ったロードバランシング

Cisco NX-OS ソフトウェアは、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では、MACアドレス、IPアドレス、またはレイヤ4ポート番号を使用してリンクを選択します。ポートチャネルロードバランシングは、送信元または宛先アドレスおよびポートの両方またはどちらか一方を使用します。

ロードバランシングモードを設定して、デバイス全体または指定したモジュールに設定したすべてのポートチャネルに適用することができます。モジュールごとの設定は、デバイス全体のロードバランシング設定よりも優先されます。デバイス全体に1つのロードバランシングモードを、指定したモジュールに別のモードを、さらに別の指定したモジュールに別のモードを設定できます。ポートチャネルごとにロードバランシング方式を設定することはできません。

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



(注)

レイヤ3インターフェイスのデフォルトロードバランシングモードは、発信元および宛先IPアドレスです。非IP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。



(注)

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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。



(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。

入力トラフィックがマルチプロトコルラベルスイッチング (MPLS) トラフィックの場合、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、単一メンバの障害が **port-channel hash-distribution** コマンドを実行して発生した場合にメンバーポート ASIC の動作を最適化できました。Cisco Nexus 7000 シリーズのデバイスはこの最適化をデフォルトで実行し、このコマンドを必要とせず、またサポートしません。Cisco NX-OS は、デバイス全体に対してであれ、モジュール単位であれ、**port-channel load-balance** コマンドによるポートチャネル上のロードバランシング基準のカスタマイズをサポートします。このコマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x*』を参照してください。

LACP

LACP では、最大 16 のインターフェイスを 1 つのポートチャネルに設定できます。最大 8 個のインターフェイスをアクティブにでき、最大 8 個のインターフェイスを M シリーズモジュールでスタンバイ状態にできます。

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

この項では、次のトピックについて取り上げます。

- 「LACP の概要」 (P.6-9)
- 「ポートチャネルモード」 (P.6-10)
- 「LACP ID パラメータ」 (P.6-11)
- 「LACP マーカーレスポンド」 (P.6-12)
- 「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.6-12)
- 「LACP 互換性の拡張」 (P.6-12)
- 「LACP ポートチャネルの最小リンクおよび MaxBundle」 (P.6-13)
- 「ファブリックエクステンダへの LACP オフロード」 (P.6-13)
- 「LACP 高速タイマー」 (P.6-13)

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

LACP の概要



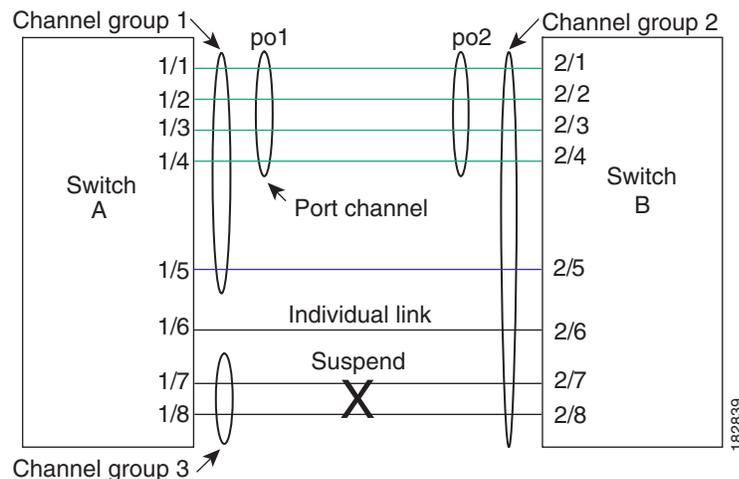
(注) LACP は、使用する前にイネーブルにする必要があります。デフォルトでは、LACP はディセーブルです。

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.6-30) を参照してください。

Cisco NX-OS リリース 4.2 以降では、システムは機能のディセーブル化の前に自動的にチェックポイントを作成するため、このチェックポイントにロールバックできます。ロールバック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、M シリーズ モジュール上のこのチャネルグループに関連付けられたポートチャネルのホットスタンバイとなります。

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



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

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

ポートチャネルモード

ポートチャネルの個別インターフェイスは、チャネルモードで設定します。スタティックポートチャネルを集約プロトコルを使用せずに実行すると、チャネルモードは常に **on** に設定されます。

デバイス上で LACP をグローバルにイネーブルにした後、各チャネルの LACP をイネーブルにします。それには、各インターフェイスのチャネルモードを **active** または **passive** に設定します。チャネルグループにリンクを追加すると、LACP チャネルグループの個別リンクにいずれかのチャネルモードを設定できます。



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

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。 チャネルで LACP をイネーブルにするには、そのチャネルのインターフェイスでチャネルモードを active または passive に設定します。LACP は、 on 状態のインターフェイスとネゴシエートする場合、LACP パケットを受信しないため、そのインターフェイスと個別のリンクを形成します。つまり、LACP チャネルグループには参加しません。 デフォルト 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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- **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」(P.6-11)
- 「LCAP ポートプライオリティ」(P.6-11)
- 「LACP 管理キー」(P.6-11)

LACP システムプライオリティ

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

システム ID は VDC ごとに異なります。



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

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。デフォルト値である 32768 をそのまま使用するか、1 ~ 65535 の範囲で値を設定できます。LACP では、ポートプライオリティおよびポート番号によりポート ID が構成されます。

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

LACP 管理キー

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

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

LACP マーカーレスポンダ

ポートチャネルを使用すればデータトラフィックを動的に再配布できます。この再配布により、リンクが削除または追加されたり、ロードバランシングスキームが変更されることもあります。トラフィックフローの途中でトラフィックが再配布されると、フレームの秩序が乱れる可能性があります。

LACP は Marker Protocol を使って、再配布によってフレームが重複したり順番が入れ替わらないようにします。Marker Protocol は、所定のトラフィックフローのすべてのフレームがリモートエンドで正しく受信すると検出します。LACP はポートチャネルリンクごとに Marker PDUS を送信します。リモートシステムは、Marker PDU よりも先にこのリンクで受信されたすべてのフレームを受信すると、Marker PDU に応答します。リモートシステムは次に Marker Responder を送信します。ポートチャネルのすべてのメンバリンクの Marker Responder を受信したローカルシステムは、トラフィックフローのフレームを正しい順序で再配分します。ソフトウェアは Marker Responder だけをサポートします。

LACP がイネーブルのポートチャネルとスタティックポートチャネルの相違点

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

構成	LACP がイネーブルのポートチャネル	スタティックポートチャネル
適用されるプロトコル	グローバルにイネーブル	N/A
リンクのチャネルモード	次のいずれか。 <ul style="list-style-type: none"> Active Passive 	On だけ
チャネルを構成する最大リンク数	16	8

LACP 互換性の拡張

相互運用性の解決、および LACP プロトコル収束の高速化のために複数の新しいコマンドがリリース 4.2(3) に追加されました。

Cisco Nexus 7000 シリーズのデバイスが非 Nexus ピアに接続されている場合、そのグレースフルフェールオーバーのデフォルトが、ディセーブルにされたポートがダウンになるための時間を遅らせる可能性があります。また、ピアからのトラフィックを喪失する原因にもなります。これらの状況を解決するために、**lacp graceful-convergence** コマンドが追加されました。

デフォルトで、ポートがピアから LACP PDU を受信しない場合、LACP はポートを中断ステータスに設定します。場合によっては、この機能は誤設定によって作成されるループの防止に役立ちますが、サーバが LACP にポートを論理的アップにするように要求するため、サーバの起動に失敗する原因になることがあります。**lacp suspend-individual** コマンドを使用して、ポートを個別の状態に設定できます。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

LACP ポートチャネルの最小リンクおよび MaxBundle

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

Cisco NX-OS リリース 5.1 では、最小リンクおよび maxbundle 機能の導入により、LACP ポートチャネル動作がさらに改善し、1 台の管理対象インターフェイスの帯域幅が増加します。

LACP ポートチャネルの MinLink 機能は次の処理を実行します。

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

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

LACP MaxBundle 機能では、次の処理が行われます。

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



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

ファブリックエクステンダへの LACP オフロード

Cisco Nexus 7000 シリーズデバイスのコントロールプレーンの負荷を軽減するために、Cisco NX-OS は、ファブリックエクステンダ CPU へのリンクレベルのプロトコル処理をオフロードする機能を適用します。この機能は、ファブリックエクステンダで設定された LACP ポートチャネルが少なくとも 1 つあると、デフォルトで LACP によってサポートされます。

LACP 高速タイマー

LACP タイマーレートを変更することにより、LACP タイムアウトの時間を変更することができます。lACP rate コマンドを使用すれば、LACP がサポートされているインターフェイスに LACP 制御パケットを送信する際のレートを設定できます。タイムアウトレートは、デフォルトのレート（30 秒）から高速レート（1 秒）に変更することができます。このコマンドは、LACP がイネーブルになっているインターフェイスでのみサポートされます。LACP 高速時間レートを設定するには、「LACP 高速タイマーレートの設定」(P.6-34) を参照してください。

ISSU およびステートフルスイッチオーバーは、LACP 高速タイマーでは保証できません。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

仮想化のサポート

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仮想デバイスコンテキスト (VDC) で設定します。各 VDC で 1 ~ 4096 の番号を使ってポートチャネルに番号を設定できます。異なる VDC に同じポートチャネル番号を使用できます。たとえば、VDC1 にポートチャネル 100 を設定し、VDC2 の別のポートチャネルにも 100 を設定できます。

ただし、LACP システム ID は VDC ごとに異なります。LACP の詳細については、「[LACP の概要](#)」(P.6-9) を参照してください。



(注) VDC と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は同じ VDC に置く必要があります。LACP を使用する場合、8 つすべてのアクティブポートと 8 つすべてのスタンバイポートは同じ VDC であることが必要です。ポートチャネルは 1 つの VDC から始まり (そのチャネルのすべてのポートが同じ VDC)、別の VDC のポートチャネルに対応します (この場合もそのチャネルのすべてのポートは同じ VDC)。



(注) ポートチャネリングロードバランシングモードは、単一のモジュールまたはモジュール全体で動作します。デフォルト VDC のポートチャネルを使用するロードバランシングを設定する必要があります。指定した VDC のポートチャネルを使用してロードバランシングを設定することはできません。ロードバランシングの詳細については、「[ポートチャネルを使ったロードバランシング](#)」(P.6-7) を参照してください。

High Availability (高可用性)

ポートチャネルは、複数のポートのトラフィックをロードバランシングすることでハイアベイラビリティを実現します。物理ポートが故障した場合、ポートチャネルのメンバがアクティブであればポートチャネルは引き続き動作します。モジュール間の設定が共通しているため、異なるモジュールのポートをバンドルして、モジュール故障時にも動作するポートチャネルを作成できます。

ポートチャネルは、ステートフル再起動とステートレス再起動をサポートします。ステートフル再起動はスーパーバイザ切り替え時に発生します。切り替え後、Cisco NX-OS ソフトウェアは実行時の設定を適用します。

Cisco NX-OS Release 5.1 以降では、動作可能なポートが設定された最小リンク数を下回った場合に、ポートチャネルがダウンします。



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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 のライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』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。

- デバイスにログインしていること。
- 必要に応じて、Advanced Services ライセンスをインストールし、特定の VDC を開始します。
- チャンネルグループのすべてのポートが同じ VDC にある必要があります。
- シングルポートチャン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ン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.6-5) を参照してください。
- デフォルト VDC のロードバランシングを設定すること。

注意事項と制約事項

ポートチャネリング設定時の注意事項および制約事項は、次のとおりです。

- 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ンネルを設定できます。
- 共有および専用ポートは同じポートチャン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ポートチャンネルでは、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ンネルを形成できます。互換性の要件の詳細については、「互換性要件」(P.6-5) を参照してください。
- STP は、設定されたポートメンバの集約帯域幅に基づいてポートチャンネルのコストを計算します。NX-OS では、このコストはそれらのポートチャンネルメンバの動作状態に基づいて動的に更新されません。
- ポートチャンネルを設定した場合、ポートチャンネルインターフェイスに適用した設定はポートチャン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 ポートチャンネルの半二重ポートは中断ステートになります。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- 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、チャン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。
- チャンネルメンバポートを発信元または宛先 SPAN ポートにできません。
- F1 および M1 シリーズのラインカードからのポートを同一のポートチャネルに設定できません。ポートが互換性要件を満たしていないためです。
- Cisco NX-OS リリース 5.1 以降では、最大 16 個のアクティブリンクを F1 シリーズラインカードのポートチャネルにバンドルすることができます。

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 (Parameters)	デフォルト
ポートチャネル	管理アップ
レイヤ 3 インターフェイスのロードバランシング方式	送信元および宛先 IP アドレス
レイヤ 2 インターフェイスのロードバランシング方式	送信元および宛先 MAC アドレス
モジュールごとのロードバランシング	ディセーブル
LACP	ディセーブル
チャンネルモード	on
LACP システムプライオリティ	32768
LACP ポートプライオリティ	32768
Minlinks	1
Maxbundle	16

ポートチャネルの設定

この項では、次のトピックについて取り上げます。

- 「ポートチャネルの作成」 (P.6-17)
- 「レイヤ 2 ポートをポートチャネルに追加」 (P.6-18)
- 「レイヤ 3 ポートをポートチャネルに追加」 (P.6-20)
- 「情報目的としての帯域幅および遅延の設定」 (P.6-22)
- 「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.6-23)
- 「ポートチャネルの説明の設定」 (P.6-25)

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- 「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.6-26)
- 「フロー制御の設定」 (P.6-27)
- 「ポートチャネルを使ったロード バランシングの設定」 (P.6-28)
- 「LACP のイネーブル化」 (P.6-30)
- 「LACP ポートチャネルポートモードの設定」 (P.6-31)
- 「LACP ポートチャネルの MinLink の設定」 (P.6-32)
- 「LACP ポートチャネル MaxBundle の設定」 (P.6-33)
- 「LACP 高速タイマーレートの設定」 (P.6-34)
- 「LACP システムプライオリティの設定」 (P.6-35)
- 「LACP ポートプライオリティの設定」 (P.6-36)
- 「LACP グレースフルコンバージェンス」 (P.6-37)
- 「LACP の個別一時停止のディセーブル化」 (P.6-40)



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

ポートチャネルの作成

チャン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。関連するチャンネルグループは自動的に作成されます。

はじめる前に

LACP ベースのポートチャネルにする場合は LACP をイネーブルにします。正しい VDC を使用していることを確認します (または `switchto vdc` コマンドを使用します)。

手順の概要

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
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。範囲は 1 ~ 4096 です。Cisco NX-OS ソフトウェアは、チャネルグループがない場合はそれを自動的に作成します。
ステップ 3	show port-channel summary 例: switch(config-router)# show port-channel summary	(任意) ポートチャネルに関する情報を表示します。
ステップ 4	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。

次の例は、ポートチャネルの作成方法を示しています。

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

ポートチャネルを削除したときのインターフェイス コンフィギュレーションの変化については、「[互換性要件](#)」(P.6-5) を参照してください。

レイヤ2ポートをポートチャネルに追加

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

はじめる前に

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

正しい VDC を使用していることを確認します（または `switchto vdc` コマンドを使用します）。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	<code>configure terminal</code> 例： <code>switch# configure terminal</code> <code>switch(config)#</code>	コンフィギュレーションモードに入ります。
ステップ 2	<code>interface type slot/port</code> 例： <code>switch(config)# interface ethernet 1/4</code> <code>switch(config-if)</code>	チャン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	<code>switchport</code> 例： <code>switch(config-if)# switchport</code>	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	<code>switchport mode trunk</code> 例： <code>switch(config-if)# switchport mode trunk</code>	(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	<code>switchport trunk {allowed vlan vlan-id native vlan-id}</code> 例： <code>switch(config-if)# switchport trunk native 3</code>	(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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	コマンド	目的
ステップ 6	<pre>channel-group channel-number [force] [mode {on active passive}]</pre> <p>例:</p> <pre>switch(config-if)# channel-group 5</pre> <p>例:</p> <pre>switch(config-if)# channel-group 5 force</pre>	<p>チャンネルグループ内にポートを設定し、モードを設定します。channel-number の指定できる範囲は 1 ~ 4096 です。ポートチャネルがない場合は、このチャンネルグループに関連付けられたポートチャンネルが作成されます。すべてのスタティックポートチャン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 対応ポートチャン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。</p> <p>(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ンネルに追加します。強制されるインターフェイスは、チャン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。</p> <p>(注) force オプションは、ポートにポートチャンネルの他のメンバーとの QoS ポリシーの不一致がある場合に失敗します。</p>
ステップ 7	<pre>show interface type slot/port</pre> <p>例:</p> <pre>switch(config-router)# show interface port channel 5</pre>	(任意) インターフェイスの内容を表示します。
ステップ 8	<pre>copy running-config startup-config</pre> <p>例:</p> <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

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

コマンド	目的
<pre>no channel-group</pre> <p>例:</p> <pre>switch(config)# no channel-group</pre>	チャン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 をチャンネルグループ 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ンネルに追加

新しいチャン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ンネルグループにレイヤ 3 ポートを追加できます。ポートチャンネルがない場合は、このチャンネルグループに関連付けられたポートチャンネルが作成されます。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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

はじめる前に

LACPベースのポートチャネルにする場合はLACPをイネーブルにします。

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

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

手順の概要

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	<code>configure terminal</code> 例： switch# configure terminal switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	<code>interface type slot/port</code> 例： switch(config)# interface ethernet 1/4 switch(config-if)	チャン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	<code>no switchport</code> 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	<code>channel-group channel-number [force] [mode {on active passive}]</code> 例： switch(config-if)# channel-group 5 例： switch(config-if)# channel-group 5 force	チャンネルグループ内にポートを設定し、モードを設定します。channel-numberの指定できる範囲は1～4096です。ポートチャネルがない場合は、Cisco NX-OSソフトウェアによってこのチャン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ンネルに追加します。強制されるインターフェイスは、チャン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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	コマンド	目的
ステップ 5	<code>show interface type slot/port</code> 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	<code>copy running-config startup-config</code> 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、チャンネルグループからポートを削除します。チャン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
	<code>no channel-group</code> 例: switch(config)# no channel-group	チャン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 モードのチャンネルグループ 6 に追加する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# channel-group 6
```

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

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

情報目的としての帯域幅および遅延の設定

ポートチャネルの帯域幅は、チャンネル内のアクティブリンクの合計数によって決定されます。情報目的でポートチャネルインターフェイスに帯域幅および遅延を設定します。

手順の概要

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`

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
ステップ 2	interface port-channel channel-number 例: switch(config)# interface port-channel 2 switch(config-if)	設定するポートチャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	bandwidth value 例: switch(config-if)# bandwidth 60000000 switch(config-if)#	情報目的で使用される帯域幅を指定します。有効な範囲は 1 ~ 80,000,000 kbs です。デフォルト値はチャネルグループのアクティブ インターフェイスの合計によって異なります。
ステップ 4	delay value 例: switch(config-if)# delay 10000 switch(config-if)#	情報目的で使用されるスループット遅延を指定します。範囲は、1 ~ 16,777,215 (10 マイクロ秒単位) です。デフォルト値は 10 マイクロ秒です。 (注) Cisco リリース 4.2(1) より前は、デフォルトの遅延値が 100 マイクロ秒でした。
ステップ 5	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、ポートチャネル 5 の帯域幅および遅延の情報パラメータを設定する例を示します。

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

ポートチャネル インターフェイスのシャットダウンと再起動

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
ステップ 2	interface port-channel <i>channel-number</i> 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	シャットダウン 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 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 <i>channel-number</i> 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
```

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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	<code>configure terminal</code> 例: <code>switch# configure terminal</code> <code>switch(config)#</code>	コンフィギュレーションモードに入ります。
ステップ 2	<code>interface port-channel channel-number</code> 例: <code>switch(config)# interface port-channel 2</code> <code>switch(config-if)</code>	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	<code>description</code> 例: <code>switch(config-if)# description engineering</code> <code>switch(config-if)#</code>	ポートチャネルインターフェイスに説明を追加できます。説明に 80 文字まで使用できません。デフォルトでは、説明は表示されません。このパラメータを設定してから、出力に説明を表示する必要があります。
ステップ 4	<code>exit</code> 例: <code>switch(config-if)# exit</code> <code>switch(config)#</code>	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	<code>show interface port-channel channel-number</code> 例: <code>switch(config-router)# show interface port-channel 2</code>	(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	<code>copy running-config startup-config</code> 例: <code>switch(config)# copy running-config startup-config</code>	(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
```

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
ステップ 2	interface port-channel <i>channel-number</i> 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)# duplex 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。
ステップ 6	show interface port-channel <i>channel-number</i> 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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

次に、ポートチャネル 2 に 100 Mb/s を設定する例を示します。

```
switch# configure terminal
switch (config)# interface port-channel 2
switch(config-if)# speed 100
```

フロー制御の設定

1 Gb 以上で動作するポートチャネルインターフェイスのフロー制御ポーズパケットの送信および受信機能をイネーブルまたはディセーブルにできます。より低速で動作するポートチャネルインターフェイスでは、ポートチャネルインターフェイスのポーズパケット受信機能だけをイネーブルまたはディセーブルにできます。



(注)

この設定が正しく動作するには、フロー制御リンクのローカルおよびリモートエンドの両方で一致する必要があります。

手順の概要

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に入ります。
ステップ 2	interface port-channel <i>channel-number</i> 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 [desired] 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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	コマンド	目的
ステップ 5	<pre>show interface port-channel channel-number</pre> <p>例: switch(config-router)# show interface port-channel 2</p>	(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	<pre>copy running-config startup-config</pre> <p>例: switch(config)# copy running-config startup-config</p>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

次に、ポートチャネルグループ 2 にポートチャネルインターフェイスを設定してポーズパケットを送信および受信する例を示します。

```
switch# configure terminal
switch (config)# interface port-channel 2
switch(config-if)# flowcontrol receive on
switch(config-if)# flowcontrol send on
```

ポートチャネルを使ったロードバランシングの設定

VDC アソシエーションにかかわらず、ポートチャネルのロードバランシングアルゴリズムを設定し、デバイス全体または 1 のモジュールだけに適用できます。モジュールベースのロードバランシングは、デバイスベースのロードバランシングに優先します。

はじめる前に

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

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

手順の概要

1. `configure terminal`
2. `port-channel load-balance {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`

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例： switch# <code>configure terminal</code> switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	<code>port-channel load-balance {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}</code> [module-number] 例： switch(config)# <code>port-channel load-balance source-destination-mac</code> 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。指定可能なアルゴリズムはデバイスによって異なります。レイヤ 3 のデフォルトは IPv4 と IPv6 の両方で source-dest-ip で、非 IP のデフォルトは source-dest-mac です。
ステップ 3	<code>show port-channel load-balance</code> 例： switch(config-router)# <code>show port-channel load-balance</code>	(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	<code>copy running-config startup-config</code> 例： switch(config)# <code>copy running-config startup-config</code>	(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。

デフォルトのロードバランシング アルゴリズムである、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` を復元するには、**no port-channel load-balance** コマンドを使用します。

コマンド	目的
<code>no port-channel load-balance</code> 例： switch(config)# <code>no port-channel load-balance</code>	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 source-ip-port module 5
```

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

LACP のイネーブル化

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

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

LACP を設定する手順は次のとおりです。

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

はじめる前に

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

手順の概要

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

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
```

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

LACP ポートチャネルポートモードの設定

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

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

はじめる前に

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

手順の概要

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

次に、LACP をイネーブルにしたインターフェイスを、チャンネルグループ 5 のイーサネット インターフェイス 1/4 のアクティブ ポートチャネル モードに設定する例を示します。

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

LACP ポートチャネルの MinLink の設定

Cisco NX-OS リリース 5.1 では、LACP minlinks 機能を設定できます。最小リンクと maxbundles は LACP でのみ動作します。ただし、非 LACP ポートチャネルに対してこれらの機能の CLI コマンドを入力できますが、これらのコマンドは動作不能です。

はじめる前に

適切なポートチャネル インターフェイスであることを確認します。

手順の概要

1. `configure terminal`
2. `interface port-channel number`
3. `lACP min-links number`
4. `show running-config interface port-channel number`

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例: switch# configure terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	<code>interface port-channel number</code> 例: switch(config)# interface port-channel 3 switch(config-if)	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>lACP min-links number</code> 例: switch(config-if)# lACP min-links 3	ポートチャネル インターフェイスを指定して、最小リンクを設定し、インターフェイス コンフィギュレーション モードを開始します。 ポートチャネルの最小リンクのデフォルト値は 1 です。許容範囲は 1 ~ 16 です。
ステップ 4	<code>show running-config interface port-channel number</code> 例: switch(config-if)# show running-config interface port-channel 3	(任意) ポートチャネルの最小リンク設定を表示します。

デフォルトのポートチャネル最小リンク設定を復元するには、`no lACP min-links` コマンドを使用します。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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

次に、モジュール3のポートチャネル インターフェイスの最小リンクを設定する例を示します。

```
switch# configure terminal
switch (config)# lacp min-links 3
```

LACP ポートチャネル MaxBundle の設定

Cisco NX-OS リリース 5.1 では、LACP minlinks 機能を設定できます。最小リンクと maxbundles は LACP でのみ動作します。ただし、非 LACP ポートチャネルに対してこれらの機能の CLI コマンドを入力できますが、これらのコマンドは動作不能です。

はじめる前に

適切なポートチャネル インターフェイスであることを確認します。

手順の概要

1. **configure terminal**
2. **interface port-channel *number***
3. **lacp max-bundle *number***
4. **show running-config interface port-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)#	コンフィギュレーションモードに入ります。
ステップ 2	interface port-channel <i>number</i> 例: switch(config)# interface port-channel 3 switch(config-if)	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	コマンド	目的
ステップ 3	<pre>lACP max-bundle number</pre> <p>例: switch(config-if)# lACP max-bundle</p>	<p>ポートチャネル インターフェイスを指定して、max-bundle を設定し、インターフェイス コンフィギュレーション モードを開始します。</p> <p>ポート チャネルの max-bundle のデフォルト値は 16 です。指定できる範囲は 1 ~ 16 です。</p> <p>(注) デフォルト値は 16 ですが、ポート チャネルのアクティブ メンバ数は、pc_max_links_config およびポートチャネルで許可されている pc_max_active_members の最小数です。</p>
ステップ 4	<pre>show running-config interface port-channel number</pre> <p>例: switch(config-if)# show running-config interface port-channel 3</p>	<p>(任意) ポートチャネル max-bundle 設定を表示します。</p>

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

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

次に、モジュール 3 のポート チャネル インターフェイスの max-bundle を設定する例を示します。

```
switch# configure terminal
switch (config)# lACP max-bundle 3
```

LACP 高速タイマーレートの設定

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

はじめる前に

LACP 機能がイネーブルになっていることを確認します。

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

手順の概要

1. **configure terminal**
2. **interface type slot/port**
3. **lACP rate fast**

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	interface type slot/port 例: switch(config)# interface ethernet 1/4	設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	lACP rate fast 例: switch(config-if)# lACP rate fast	LACP がサポートされているインターフェイスに LACP 制御パケットを送信する際のレートとして高速レート (1 秒) を設定します。 タイムアウト レートをデフォルトにリセットするには、コマンドの no 形式を使用します。

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

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

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

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

LACP システム プライオリティの設定

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

複数の VDC のシステム プライオリティ値を同じ設定にすることができます。

はじめる前に

LACP をイネーブルにします。

正しい VDC を使用していることを確認します (または **switch tovdc** 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**

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例: switch# <code>configure terminal</code> switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	<code>lacp system-priority priority</code> 例: switch(config)# <code>lacp system-priority 40000</code>	LACP で使用するシステム プライオリティを設定します。指定できる範囲は 1 ~ 65535 で、値が大きいほどプライオリティは低くなります。デフォルト値は 32768 です。 (注) VDC ごとに LACP システム ID が異なります。これは、この設定値に MAC アドレスが追加されるためです。
ステップ 3	<code>show lacp system-identifier</code> 例: switch(config-if)# <code>show lacp system-identifier</code>	LACP システム識別子を表示します。
ステップ 4	<code>copy running-config startup-config</code> 例: switch(config)# <code>copy running-config startup-config</code>	(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。

はじめる前に

LACP をイネーブルにします。

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

手順の概要

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例： switch# <code>configure terminal</code> switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	<code>interface type slot/port</code> 例： switch(config)# <code>interface ethernet 1/4</code> 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	<code>lacp port-priority priority</code> 例： switch(config-if)# <code>lacp port-priority 40000</code>	LACP で使用するポート プライオリティを設定します。指定できる範囲は 1 ~ 65535 で、値が大きいほどプライオリティは低くなります。デフォルト値は 32768 です。
ステップ 4	<code>copy running-config startup-config</code> 例： switch(config-if)# <code>copy running-config startup-config</code>	(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。

はじめる前に

LACP をイネーブルにします。

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

手順の概要

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 モードに入ります。
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 コンバージェンスの再イネーブル化

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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に入ります。
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
```

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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。これによって、サーバの中には起動に失敗するものがあります。そのようなサーバは、LACP が論理的にポートを稼動状態にしていることを必要とするからです。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** コマンドを入力するだけです。このコマンドを使用する前に、ポートチャネルが管理上のダウン状態である必要があります。

はじめる前に

LACP をイネーブルにします。

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

手順の概要

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 モードに入ります。
ステップ 2	interface port-channel <i>number</i> 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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	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をディセーブルにする方法を示します。

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

LACP の個別一時停止の再イネーブル化

デフォルトの LACP 個別ポートの一時停止を再度イネーブルにできます。

手順の概要

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に入ります。
ステップ 2	interface port-channel <i>number</i> 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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

	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
```

ポートチャネル設定の確認

ポートチャネルの設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show interface port-channel <i>channel-number</i>	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 <i>channel-number</i>]	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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

コマンド	目的
show lacp { counters [interface port-channel channel-number] [interface type/slot] neighbor [interface port-channel channel-number] port-channel [interface port-channel channel-number] system-identifier]}	LACP に関する情報を表示します。
show running-config interface port-channel channel-number	ポートチャネルの実行コンフィギュレーション情報を表示します。

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

ポートチャネルインターフェイスコンフィギュレーションのモニタリング

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

コマンド	目的
clear counters interface port-channel channel-number	カウンタをクリアします。
clear lacp counters [interface port-channel channel-number]	LACP カウンタをクリアします。
load- interval { interval seconds { 1 2 3 }}	Cisco Nexus 7000 シリーズ デバイスの Cisco NX-OS Release 4.2(1) から、3 種類のサンプリング間隔をビットレートおよびパケットレートの統計情報に設定します。
show interface counters [module module]	入力および出力オクテット ユニキャストパケット、マルチキャストパケット、ブロードキャストパケットを表示します。
show interface counters detailed [all]	入力パケット、バイト、マルチキャストおよび出力パケット、バイトを表示します。
show interface counters errors [module module]	エラーパケットの数を表示します。
show lacp counters	LACP の統計情報を表示します。

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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

```
switch# configure terminal
switch (config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# no ip address
switch(config-if)# channel-group 6 mode active
switch (config)# interface ethernet 2/5
switch(config-if)# no switchport
switch(config-if)# no ip address
switch(config-if)# channel-group 6 mode active
switch (config)# interface port-channel 6
switch(config-if)# ip address 192.0.2.1/8
```

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.6-44)
- 「管理情報ベース (MIB)」(P.6-45)

関連資料

関連項目	マニュアルタイトル
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』

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

関連項目	マニュアルタイトル
VDC	『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x』
ライセンス	『Cisco NX-OS Licensing Guide』
リリースノート	『Cisco Nexus 7000 Series NX-OS Release Notes, Release 5.x』

標準

標準	タイトル
IEEE 802.3ad	—

管理情報ベース (MIB)

MIB	MIBのリンク
<ul style="list-style-type: none"> IEEE8023-LAG-CAPABILITY CISCO-LAG-MIB 	<p>MIBを検索およびダウンロードするには、次のURLにアクセスしてください。</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>

ポートチャネル設定の機能履歴

表 6-4 に、この機能のリリース履歴を示します。

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	5.2(1)	サポートが528ポートチャネルに増加されました。
Minlinks および Maxbundle	5.1(1)	この機能が導入されました。
ポートチャネル	4.2(1)	サポートが256ポートチャネルに増加されました。
ポートチャネル	4.0(1)	この機能が導入されました。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

vPC の設定

この章では、Cisco NX-OS デバイス上で仮想ポート チャンネル (vPC) を設定する方法を説明します。



(注) Cisco NX-OS リリース 5.1(1) 以降では、vPC は FabricPath と相互運用するように機能強化されました。FabricPath ネットワークで vPC を設定するには、『Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide, Release 5.x』を参照してください。

Cisco NX-OS リリース 5.1(1) 以降では、個々のスイッチの vPC ピア リンクに対し F シリーズ モジュールでは 10 Gbps イーサネット (10GE) インターフェイスを、または M シリーズ モジュールでは 10GE インターフェイスを使用できますが、F モジュール上のメンバポートを M モジュール上のポートと組み合わせて単一スイッチ上の単一ポート チャンネルにすることはできません。ポート チャンネルの互換性パラメータは、物理スイッチのすべてのポート チャンネル メンバで同じである必要があります。

vPC の一部になるように共有インターフェイスを設定できません。共有インターフェイスに関する詳細については、『Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500』を参照してください。



(注) ポート チャンネルの互換性パラメータは、両方のピアのすべての vPC メンバポートでも同じでなければならないので、シャーシごとに同じタイプのモジュールを使用する必要があります。

この章は、次の項で構成されています。

- 「vPC について」 (P.7-2)
- 「vPC のライセンス要件」 (P.7-31)
- 「注意事項と制約事項」 (P.7-31)
- 「デフォルト設定値」 (P.7-32)
- 「vPC の設定」 (P.7-33)
- 「vPC 設定の確認」 (P.7-59)
- 「vPC のモニタリング」 (P.7-59)
- 「vPC の設定例」 (P.7-60)
- 「その他の参考資料」 (P.7-62)
- 「vPC の設定機能の履歴」 (P.7-63)

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。



(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

この項では、次のトピックについて取り上げます。

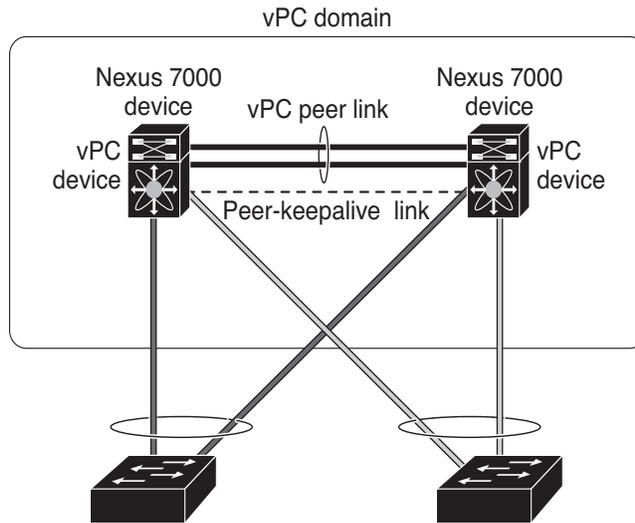
- 「vPC の概要」 (P.7-2)
- 「vPC の用語」 (P.7-5)
- 「vPC ピア リンク」 (P.7-6)
- 「ピアキープアライブ リンクとメッセージ」 (P.7-12)
- 「vPC ピア ゲートウェイ」 (P.7-13)
- 「vPC ドメイン」 (P.7-14)
- 「vPC トポロジ」 (P.7-15)
- 「vPC インターフェイスの互換パラメータ」 (P.7-16)
- 「vPC 番号」 (P.7-19)
- 「他のポート チャネルの vPC への移行」 (P.7-20)
- 「単一モジュール上での vPC ピア リンクとコアへのリンクの設定」 (P.7-20)
- 「その他の機能との vPC の相互作用」 (P.7-22)
- 「仮想化のサポート」 (P.7-29)
- 「停電後の vPC リカバリ」 (P.7-30)
- 「High Availability (高可用性)」 (P.7-31)

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 チャンネルだけです。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、そうならないとリンクが形成されません。

ポート チャンネルの設定は、次のいずれかを使用して行います。

- プロトコルなし
- リンク集約制御プロトコル (LACP)

LACP を使用せずに vPC (vPC ピア リンク チャンネルも含めて) のポート チャンネルを設定する場合は、各デバイスが、単一のポート チャンネル内に最大 8 つのアクティブ リンクを持てます。LACP を使用して vPC (vPC ピア リンク チャンネルも含めて) のポート チャンネルを設定する場合は、各デバイスが、単一のポート チャンネル内に 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 vPC 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.7-22) 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。

Cisco NX-OS リリース 4.2 以降では、システムは機能のディセーブル化の前に自動的にチェックポイントを作成するため、このチェックポイントにロールバックできます。ロールバック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。

専用モードで 2 つ以上の 10 ギガビット イーサネット ポートを使用することにより、1 台の Cisco Nexus 7000 シリーズ シャーシでポート チャンネルを設定して vPC ピア リンクを作成できます。正しいハードウェアをイネーブルにしており、Cisco NX-OS 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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

vPC ピア リンク レイヤ 2 ポート チャネルは、トランクとして設定することを推奨します。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 Cisco Nexus デバイスが第 3 のデバイスには 1 つのデバイスとして見える vPC ピア リンクが作成されます。第 3 のデバイス、またはダウンストリーム デバイスは、スイッチ、サーバ、vPC に接続された正規のポート チャネルを使用するその他の任意のネットワークング デバイスのいずれでもかまいません。正しいモジュールを使用していないと、システムからエラー メッセージが表示されます。



(注)

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

Cisco NX-OS リリース 4.2 以降では、すべての vPC ピア リンクおよびコアに面したインターフェイスを 1 つのモジュール上で設定しなければならない場合、コアへのレイヤ 3 リンクに関連付けられているトラック オブジェクトおよび両方の vPC ピア デバイス上の vPC ピア リンク上のすべてのリンクを設定してください。いったんこの機能を設定したら、プライマリ vPC ピア デバイスに障害が発生した場合には、プライマリ vPC ピア デバイス上のすべての vPC リンクを、システムが自動的に停止します。システムが安定するまでは、このアクションにより、すべての vPC トラフィックが強制的にセカンダリ vPC ピア デバイスに送られます。

トラック オブジェクトを作成し、コアおよび vPC ピア リンクに接続されているプライマリ vPC ピア デバイス上のすべてのリンクにそのオブジェクトを適用します。**track interface** コマンドについては、『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。各デバイスに設定できる vPC ドメイン ID は、1 つだけです。

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



(注)

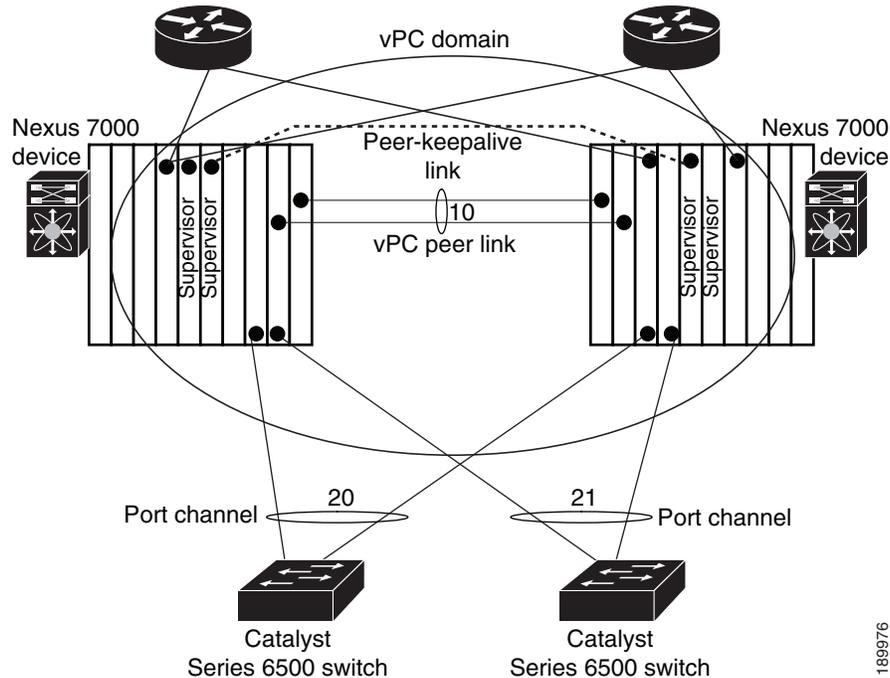
常にすべての vPC デバイスを両方の vPC ピア デバイスに、ポート チャネルを使用して接続してください。

vPC (図 7-2 を参照) には、次の利点があります。

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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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

vPC で使用される用語は、次のとおりです。

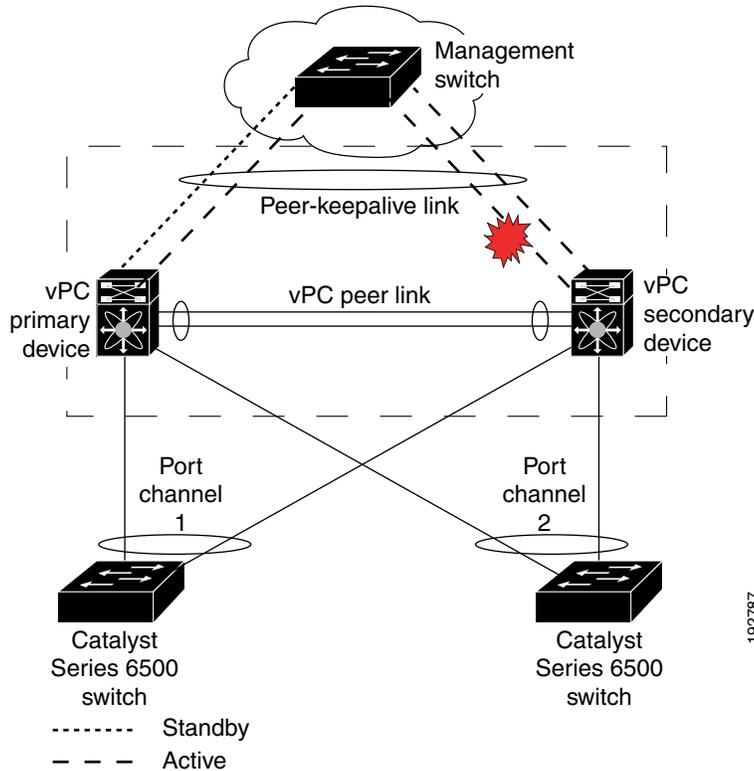
- vPC : vPC ピア デバイスとダウンストリーム デバイスの間の結合されたポート チャネル。
- vPC ピア デバイス : vPC ピア リンクと呼ばれる特殊なポート チャネルで接続されている一対のデバイスの 1 つ。
- vPC ピア リンク : vPC ピア デバイス間の状態を同期するために使用されるリンク。両エンドが 10 ギガバイト イーサネット インターフェイス上にはなりません。
- vPC メンバ ポート : vPC に属するインターフェイス。
- ホスト vPC ポート : vPC に属するファブリック エクステンダのホスト インターフェイス。
- vPC ドメイン : このドメインには、両方の vPC ピア デバイス、vPC ピアキープアライブ リンク、vPC 内においてダウンストリーム デバイスに接続されているすべてのポート チャネルが含まれます。また、このドメインは、vPC グローバルパラメータを割り当てるために使用する必要があるコンフィギュレーション モードに関連付けられています。
- vPC ピアキープアライブ リンク : ピアキープアライブ リンクは、さまざまな vPC ピア Cisco Nexus 7000 シリーズのデバイスをモニタします。ピアキープアライブ リンクは、vPC ピア デバイス間での設定可能なキープアライブ メッセージの定期的な送信を行います。

ピアキープアライブ リンクを、各 vPC ピア デバイス内のレイヤ 3 インターフェイスにマッピングされている独立した VRF に関連付けることを推奨します。独立した VRF を設定しなかった場合は、デフォルトで管理 VRF 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

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

ポートとスタンバイ管理ポートの両方に接続した管理スイッチを置く必要があります (図 7-3 を参照)。

図 7-3 vPC ピアキーブアライブ リンクの管理ポートを接続するための独立したスイッチが必要



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

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

vPC ピア リンク

vPC ピア リンクは、vPC ピア デバイス間の状態を同期するために使用されるリンクです。リンクの両エンドが、10 ギガビット イーサネット インターフェイス上にはなりません。

vPC に 2 台のスイッチで動作するスプリット コントロールプレーンが含まれているため、vPC は次のようにピア リンクを使用します。

- 両方の vPC ピア スイッチにコントロールプレーン情報を同期します (vPC 状態、一貫性パラメータ、MAC アドレスなど)。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- ローカル vPC がダウンしたとき、vPC ピア スイッチにデータ パケットを転送します。
- 同一の物理 Cisco Nexus 7000 デバイス上の 2 つの VDC 間の単一 vPC ドメインはサポートされません。

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.7-8)
- 「プライマリおよびセカンダリ デバイス上で手動で設定する必要がある機能」(P.7-10)
- 「vPC ピア リンクのレイヤ 3 バックアップ ルートの設定」(P.7-11)



(注)

vPC ピア リンクを設定する場合は、あらかじめピアキーブアライブ リンクを設定しておく必要があります。設定しておかないと、ピア リンクは機能しません (vPC のピアキーブアライブ リンクとメッセージの詳細については、「ピアキーブアライブ リンクとメッセージ」(P.7-12) 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、モジュールを使用する必要があります。



(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推奨します。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。

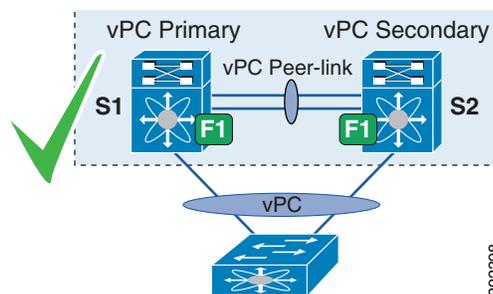
vPC ピア リンクと I/O モジュールのサポート

vPC ピア リンクの一方の側にある同一の I/O モジュールのみがサポートされます。vPC ピア リンクの一方の側で異なる I/O モジュールを使用している場合はサポートされません。ポート チャネルの同じ側で I/O モジュールを混在している場合もサポートされません。表 7-1 では、vPC ピア リンクの両側でサポートされる I/O モジュールを表示します。図 7-4 から 図 7-7 では、vPC ピア リンクの両側でサポートされる設定とサポートされない設定を表示します。

表 7-1 vPC ピア リンクの両側でサポートされる I/O モジュールの組み合わせ

vPC プライマリ	vPC セカンダリ
F1 I/O モジュール	F1 I/O モジュール
M1 I/O モジュール	M1 I/O モジュール

図 7-4 サポート対象：vPC ピア リンクの一方の側にある 2 つの F1 I/O モジュール



マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

図 7-5 サポート対象：vPC ピア リンクの一方の側にある 2 つの M1 I/O モジュール

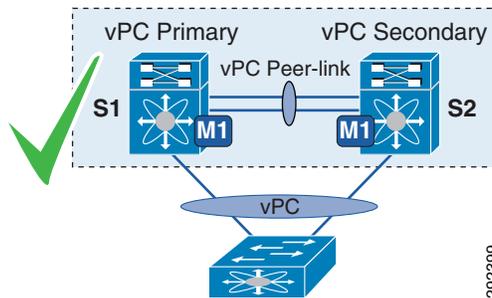


図 7-6 サポート対象外：vPC ピア リンクの一方の側にある 2 つの異なる I/O モジュール (M1 と F1)

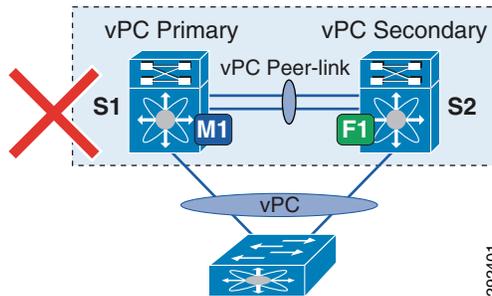
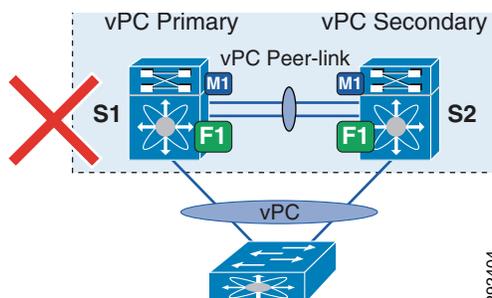


図 7-7 サポート対象外：ピア リンクの同じ側にある混在した I/O モジュール



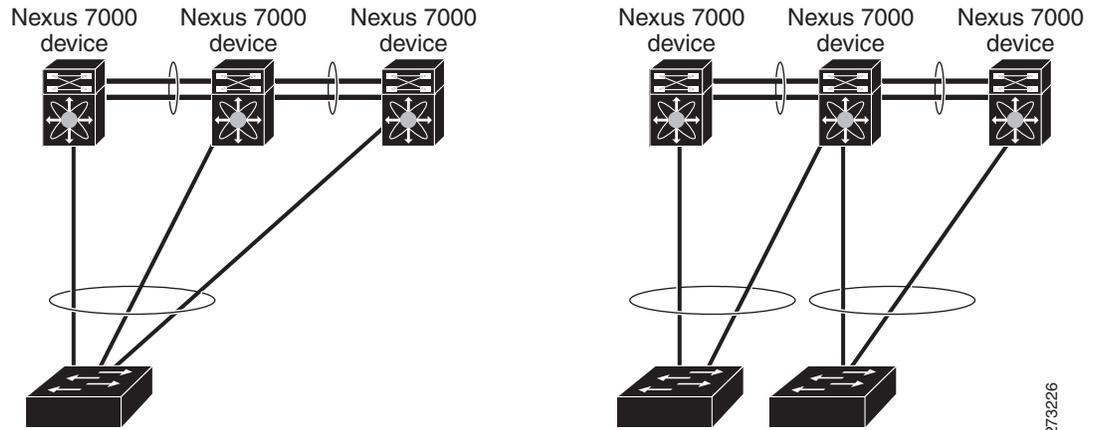
vPC ピア リンクの概要

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 7-8](#) を参照してください。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

図 7-8 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 チャンネルを設定してから、vPC ドメインを設定します。ポート チャン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 チャンネルに設定することを推奨します。



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

多くの動作パラメータおよび設定パラメータが、vPC ピア リンクによって接続されている各デバイスで同じでなければなりません (「vPC インターフェイスの互換パラメータ」(P.7-16) を参照)。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する必要があります。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 リンクを設定し終わったら、各 vPC ピア デバイスの設定を表示して、設定に互換性があることを確認してください。



(注) vPC ピア リンクによって接続されている 2 つのデバイスが、特定の同じ動作パラメータおよび設定パラメータを持っていることを確認する必要があります。一貫性が必要な設定の詳細については、「vPC インターフェイスの互換パラメータ」(P.7-16) を参照してください。

vPC ピア リンクを設定すると、vPC ピア デバイスは接続されたデバイスの一方がプライマリ デバイスで、もう一方の接続デバイスがセカンダリ デバイスであると交渉します (「vPC の設定」(P.7-33) を参照)。Cisco NX-OS ソフトウェアは、最小の MAC アドレスを使用してプライマリ デバイスを選択します。特定のフェールオーバー条件の下でだけ、ソフトウェアが各デバイス (つまり、プライマリ デバイスおよびセカンダリ デバイス) に対して異なるアクションを取ります。プライマリ デバイスに障害が発生すると、システムの回復時にセカンダリ デバイスが新しいプライマリ デバイスになり、以前のプライマリ デバイスがセカンダリ デバイスになります。

どちらの vPC デバイスをプライマリ デバイスにするか設定することもできます。vPC ピア デバイスのプライオリティを変更すると、ネットワークでインターフェイスがアップしたりダウンしたりする可能性があります。1 台の vPC デバイスをプライマリ デバイスにするよう再度ロールプライオリティを設定する場合は、プライオリティ値が低いプライマリ vPC デバイスと値が高いセカンダリ vPC デバイスの両方でロールプライオリティを設定します。次に、

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

shutdown コマンドを入力して、両方のデバイスで vPC ピア リンクであるポート チャネルをシャットダウンし、最後に **no shutdown** コマンドを入力して、両方のデバイスでポート チャネルを再度イネーブルにします。



(注)

各 vPC ピア 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推奨します。

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

両方の vPC ピア リンク デバイスおよびダウンストリーム デバイスで、任意の標準ロード バランシング スキームを設定できます (ロード バランシングの詳細については、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.7-28)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.7-28)を参照してください)。

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



(注)

独立した VRF を作成して設定し、その vPC ピアキープアライブリンクのための VRF 内の各 vPC ピア デバイス上でレイヤ3ポートを設定することを推奨します。ピアキープアライブのデフォルトポートとデフォルト VRF は、管理ポートと管理 VRF です。

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

vPC ピア デバイス間の設定可能なキープアライブメッセージの送信には、独立したリンク (vPC ピアキープアライブリンク) を使用します。vPC ピアキープアライブリンク上のキープアライブメッセージから、障害が vPC ピア リンク上でだけ発生したのか、vPC ピア デバイス上で発生したのかがわかります。キープアライブメッセージは、ピアリンク内のすべてのリンクで障害が発生した場合にだけ使用されます。キープアライブメッセージの詳細については、「[ピアキープアライブリンクとメッセージ](#)」(P.7-12)を参照してください。

プライマリおよびセカンダリ デバイス上で手動で設定する必要がある機能

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

- STP ルート : プライマリ vPC ピア デバイスを STP プライマリ ルート デバイスとして設定し、vPC セカンダリ デバイスを STP セカンダリ ルート デバイスとして設定します。vPC および STP の詳細については、「[vPC ピア リンクと STP](#)」(P.7-23)を参照してください。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- Bridge Assurance がすべての vPC ピア リンク上でイネーブルになるように、vPC ピア リンク インターフェイスを STP ネットワーク ポートとして設定することを推奨します。
- 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 を設定することを推奨します。
- レイヤ 3 VLAN ネットワーク インターフェイス: 両方のデバイスから同じ VLAN の VLAN ネットワーク インターフェイスを設定することにより、各 vPC ピア デバイスからのレイヤ 3 接続を設定します。
- HSRP アクティブ: vPC ピア デバイス上で 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.7-27) を参照してください)。

vPC ピア リンクの両側で単方向リンク検出 (UDLD) を設定することを推奨します。UDLD を設定する手順については「UDLD モードの設定」(P.2-40) を参照してください。

vPC ピア リンクのレイヤ 3 バックアップ ルートの設定

HSRP や PIM などのアプリケーション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推奨します。



(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 リリース 4.2(1) 以降では、指定した VLAN インターフェイスが vPC ピア リンクに障害が発生しても vPC セカンダリ デバイス上で停止しないようにすることができるようになりました。

この機能を設定するには、**dual-active exclude interface-vlan** コマンドを使用します。



(注)

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グはサポートされません。vPC ピア デバイスおよび汎用レイヤ 3 デバイスの間でルーティング プロトコルの隣接関係が必要な場合は、相互接続に物理的にルーティングされたインターフェイスを使用する必要があります。vPC ピアゲートウェイ機能の使用では、この要件は変わりません。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

ピアキーブアライブ リンクとメッセージ

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



(注)

vPC ピアキーブアライブ リンクを、各 vPC ピア デバイス内のレイヤ3 インターフェイスにマッピングされている独立した VRF に関連付けることを推奨します。独立した VRF を設定しなかった場合は、デフォルトで管理 VRF と管理ポートが使用されます。vPC ピアキーブアライブ 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、ピアキーブアライブ メッセージを受信しなくなることによってその障害を感知します。vPC ピアキーブアライブ メッセージのデフォルトの間隔は、1 秒です。この間隔は、400 ミリ秒～10 秒の範囲内で設定可能です。

ホールドタイムアウト値は、3～10 秒の範囲内で設定可能で、デフォルトのホールドタイムアウト値は3 秒です。このタイマーは、vPC ピア リンクが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 ピアキーブアライブ メッセージを無視します。ホールドタイムアウト期間の目的は、誤ったポジティブ ケースを防ぐことです。

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

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

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

キーブアライブ メッセージのタイマーの設定については、「[vPC の設定](#)」(P.7-33) を参照してください。



(注)

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

コマンドライン インターフェイス (CLI) を使用して、vPC ピアキーブアライブ 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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

```
(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 リリース 4.2(1) 以降では、vPC ピア デバイスを、vPC ピア デバイスの MAC アドレスを送信先とするパケットに対してもゲートウェイとして機能するように設定できるようになりました。

この機能を設定するには、**peer-gateway** コマンドを使用します。

一部の Network-Attached Storage (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 シリーズ デバイスの MAC アドレスを使用して、トラフィックに応答する場合があります。このような動作は、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、この機能によってピア リンクの使用が最適化され、トラフィック損失が回避されます。

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

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



(注)

Cisco NX-OS リリース 5.1(3) 以降では、VLAN インターフェイスが vPC ピア デバイスのレイヤ 3 バックアップ ルーティングに使用され、F1 ラインカードがピア リンクとして使用される場合は、**peer-gateway exclude-vlan vlan-number** コマンドを実行して VLAN をピアゲートウェイ機能から除外する必要があります (イネーブルの場合)。バックアップ ルートについての詳細については、「[vPC ピア リンクのレイヤ 3 バックアップ ルートの設定](#)」(P.7-11) を参照してください。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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 上で稼働している場合は、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.7-33) を参照してください。

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

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

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

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

vPC MAC の表示の詳細については、「[CFSおE](#)」(P.7-28) を参照してください。

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



(注)

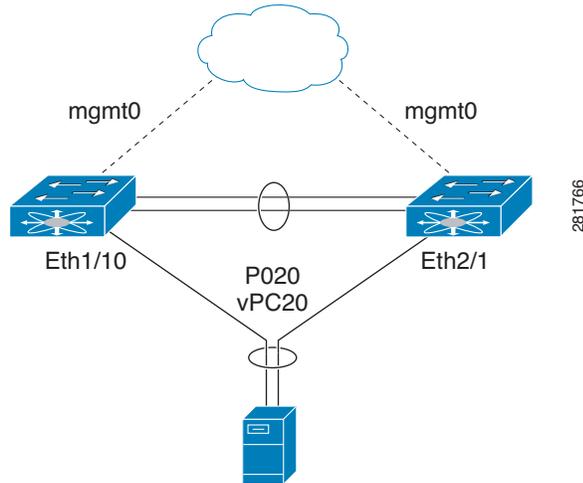
システムプライオリティを手動で設定する場合は、必ず両方の vPC ピア デバイス上で同じプライオリティ値を割り当てる必要があります。vPC ピア デバイス同士が異なるシステムプライオリティ値を持っていると、vPC は稼働しません。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

vPC トポロジ

図 7-3 では、Cisco Nexus 7000 シリーズ スイッチ ポートが別のスイッチまたはホストに直接接続され、vPC の一部となるポート チャンネルの一部として設定される基本設定を示します。

図 7-9 スイッチ vPC トポロジ

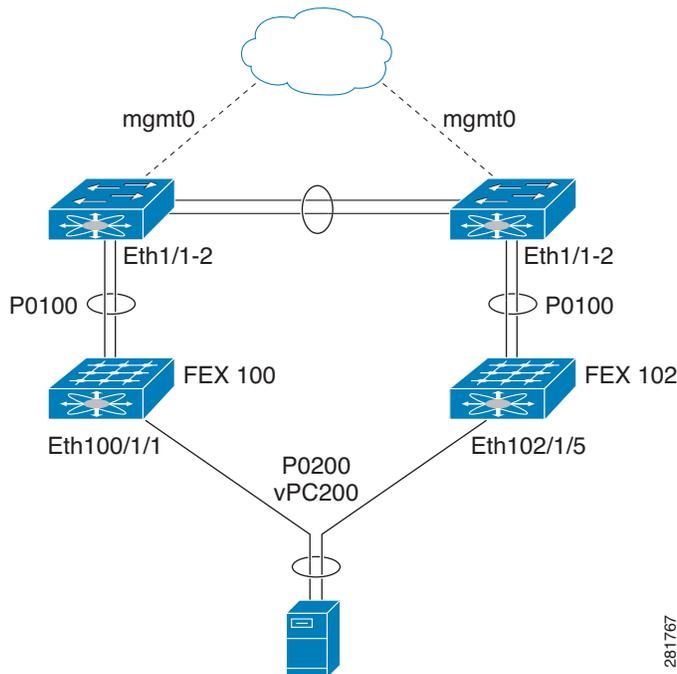


この図では、vPC 20 がポート チャンネル 20 で設定され、最初のスイッチには Eth1/10 が、2 番目のスイッチには Eth2/1 がメンバポートとしてあります。

Cisco NX-OS リリース 5.2(1) 以降では、図 7-10 に示すように、ファブリック エクステンダ (FEX) を通してピア デバイスから vPC を設定できます。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

図 7-10 FEX Straight-Through トポロジ (ホスト vPC)



この図では、各 FEX が Cisco Nexus 7000 シリーズ スイッチ でシングルホーム (Straight-Through FEX トポロジ) になっています。この FEX 上のホスト インターフェイスはポート チャネルとして設定され、それらのポート チャネルは vPC として設定されています。Eth100/1/1 および Eth102/1/5 は、PO200 のメンバーとして設定され、PO200 は vPC 200 に対し設定されます。

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

FEX ポート設定の詳細については、『*Configuring the Cisco Nexus 2000 Series Fabric Extender*』を参照してください。

vPC インターフェイスの互換パラメータ

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

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、「[CFSおE](#)」(P.7-28) 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 の稼働を制限する可能性のある設定だけです。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

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。

ここでは、次の内容について説明します。

- 「同じでなければならない設定パラメータ」 (P.7-17)
- 「同じにすべき設定パラメータ」 (P.7-18)
- 「パラメータの不一致の結果」 (P.7-19)

同じでなければならない設定パラメータ

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



注意

VPC VLAN かどうかにかかわらず、スパニング ツリーがいずれの VLAN に対してもディセーブルの場合、グローバル タイプ 1 の不整合が生じ、すべて VPC VLAN が一時停止します。この問題は、存在しない VLAN に対しスパニング ツリーをディセーブルにする場合にも発生します。



(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 の稼働を制限する可能性のある設定だけです。

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

- ポートチャネル モード : オン、オフ、またはアクティブ
- チャネル単位のリンク速度
- チャネル単位のデュプレックス モード
- チャネルごとのトランク モード :
 - ネイティブ VLAN
 - トランク上で許可される VLAN
 - ネイティブ VLAN トラフィックのタグging
- スパニング ツリー プロトコル (STP) モード
- Multiple Spanning Tree 用の STP リージョン コンフィギュレーション
- VLAN ごとのイネーブル/ディセーブル状態
- STP グローバル設定 :
 - ブリッジ保証設定
 - ポート タイプ設定
 - ループ ガード設定

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- STP インターフェイス設定 :
 - ポート タイプ設定
 - ループ ガード
 - ルート ガード
- 最大伝送単位 (MTU)

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



(注)

どの vPC インターフェイスもサスペンド モードになっていないことを確認するには、**show vpc brief** 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

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

- MAC エージング タイマー
- スタティック MAC エントリ
- VLAN インターフェイス : vPC ピア リンク エンドにある各デバイスの VLAN インターフェイスが両エンドで同じ VLAN 用に設定されていなければならない、さらに同じ管理モードで同じ動作モードになっていなければなりません。ピア リンクの片方のデバイスだけで設定されている VLAN は、vPC またはピア リンクを使用してトラフィックを通過させることはしません。すべての VLAN をプライマリ vPC デバイスとセカンダリ vPC デバイスの両方で作成する必要があります。そうならない VLAN は、停止します。
- ACL のすべての設定とパラメータ
- Quality of Service (QoS) の設定とパラメータ
- STP インターフェイス設定 :
 - BPDU Filter
 - BPDU ガード
 - コスト
 - リンク タイプ
 - プライオリティ
 - VLAN (Rapid PVST+)
- ポート セキュリティ
- Cisco Trusted Security (CTS)
- ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) スヌーピング
- ネットワーク アクセス コントロール (NAC)
- ダイナミック ARP インスペクション (DAI)
- IP ソース ガード (IPSG)
- インターネット グループ管理プロトコル (IGMP) スヌーピング
- ホット スタンバイルーティング プロトコル (HSRP)

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

- プロトコルに依存しないマルチキャスト (PIM)
- ゲートウェイロード バランシング プロトコル (GLBP)
- すべてのルーティング プロトコル設定

すべての設定パラメータで互換性が取れていることを確認するために、vPC の設定が終わったら、各 vPC ピア デバイスの設定を表示してみることを推奨します。

パラメータの不一致の結果

Cisco NX-OS リリース 5.2(1) より前のリリースでは、整合性検査により一致しなければならないパラメータのリストからパラメータの不一致が検出されると、vPC ピア リンクと vPC は稼働できません。vPC がすでに確立された後にパラメータの不一致が設定された場合は、vPC は一時停止モードに移動し、vPC にトラフィックは流れません。

Cisco NX-OS リリース 5.2(1) 以降では、グレースフルな整合性検査機能を設定でき、不一致が作動中の vPC で導入されたときに、セカンダリ ピア デバイス上のリンクのみを中断できます。この機能は CLI のみで設定可能で、デフォルトでイネーブルになっています。

この機能を設定するには、**graceful consistency-check** コマンドを使用します。

一致しなければならないパラメータのリストのすべてのパラメータに関する整合性検査の一部として、システムはすべての VLAN の一貫性をチェックします。NX-OS リリース 5.2(1) より前のリリースでは、有効な VLAN の設定がピア デバイス間で矛盾している場合は、vPC の確立や一時停止モードへの移動はできません。

Cisco NX-OS リリース 5.2(1) 以降では、vPC は動作可能なままで、矛盾した VLAN のみがダウンします。この VLAN 単位の整合性検査機能はディセーブルにできず、マルチ スパニングツリー (MST) VLAN には適用されません。

vPC 番号

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



(注)

スイッチとしてもブリッジとしても機能しないホストまたはネットワーク デバイスに接続されているダウンストリーム デバイス上のポートは、STP エッジポートとして設定することを推奨します。STP ポート タイプの詳細については、『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x』を参照してください。

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



(注)

vPC ピア デバイスからダウンストリーム デバイスに接続されているポート 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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。

他のポート チャネルの vPC への移行



(注)

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

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

単一モジュール上での vPC ピア リンクとコアへのリンクの設定



(注)

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

Cisco NX-OS 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、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れます。
- その vPC ピア デバイス上のすべてのダウンストリーム vPC を停止させます。これにより、すべてのトラフィックが強制的に他の vPC ピア デバイスに向けてそのアクセス スイッチでルーティングされます。

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

コアに対するすべてのリンクおよびすべての vPC ピア リンクを含むトラック リストを、そのオブジェクトとして作成します。このトラック リストの指定した vPC ドメインに対して、トラッキングをイネーブルにします。この同じ設定を他方の vPC ピア デバイスにも適用します。オブジェクトトラッキングとトラック リストについては、『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。

マニュアルに関するご意見は nexus7k-docfeedback@cisco.com まで電子メールでお知らせください。



(注)

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

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

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

## マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

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

この項では、次のトピックについて取り上げます。

- 「vPC と LACP」 (P.7-22)
- 「vPC ピア リンクと STP」 (P.7-23)
- 「vPC ピア スイッチ」 (P.7-25)
- 「vPC および ARP または ND」 (P.7-25)
- 「vPC マルチキャスト : PIM、IGMP、および IGMP スヌーピング」 (P.7-25)
- 「vPC ピア リンクとルーティング」 (P.7-27)
- 「CFSOE」 (P.7-28)
- 「vPC および孤立ポート」 (P.7-29)

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

M シリーズ モジュールおよび LACP では、vPC ピア リンクは、16 個の LACP インターフェイス (8 個のアクティブ リンクと 8 個のホット スタンバイ リンク) をサポートします。ダウンストリーム vPC チャネル上では、8 個のアクティブ リンクと 8 個のホット スタンバイ リンクとで、16 個の LACP リンクを設定できます。LACP を使用せずにポート チャネルを設定する場合は、各チャネルに 8 個のリンクしか持てません。F シリーズのラインカードでは、vPC ピア リンクとダウンストリーム vPC チャネルは最大 16 個のアクティブな LACP リンクをサポートします。ポート チャネルが LACP を使用して設定されていない場合でも、各チャネルに 16 個のリンクを設定できます。

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

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。



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

## vPC ピア リンクと STP

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

すべての vPC ピア リンク インターフェイスを STP ネットワーク ポート タイプに設定して、すべての vPC リンク上で Bridge Assurance が自動的にイネーブルになるようにすることを推奨します。また、vPC ピア リンク上ではどの STP 拡張機能もイネーブルにしないことも推奨します。STP 拡張がすでに設定されている場合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』



(注) パラメータのリストは、vPC ピア リンクの両サイドの vPC ピア デバイス上で同じになるように設定する必要があります。こ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 インターフェイスの互換パラメータ」(P.7-16) を参照してください。

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

プライマリ vPC デバイスは、Cisco Fabric Services over Ethernet (CFS over E) を使用して、vPC セカンダリ ピア デバイス上の STP の状態を同期させます。CFS over E については、「CFS over E」(P.7-28) 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.7-12) を参照してください。

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

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

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

## マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

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

- STP グローバル設定：
  - STP モード
  - MST のための STP リージョン設定
  - VLAN ごとのイネーブル/ディセーブル状態
  - ブリッジ保証設定
  - ポート タイプ設定
  - ループ ガード設定
- STP インターフェイス設定：
  - ポート タイプ設定
  - ループ ガード
  - ルート ガード



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

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

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



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

この機能がイネーブルになっている場合は、**show spanning-tree** コマンドで vPC に関する情報を表示できます。例については、『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, 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推奨します。スイッチに接続されているすべてのホストポートを STP エッジポートとして設定してください (STP ポートタイプの詳細については、『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x』を参照してください)。

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

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



(注)

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

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 および ARP または ND

Cisco Fabric Service over Ethernet (CFS over Ethernet) プロトコルの信頼性が高いトランスポート メカニズムを使用した、vPC ピア間のテーブル同期に対応する機能が Cisco NX-OS リリース 4.2(6) に追加されました。ip arp synchronize および ipv6 nd synchronize コマンドをイネーブルにし、vPC ピア間のアドレス テーブルのコンバージェンスの高速化をサポートする必要があります。このコンバージェンスは、ピア リンク ポート チャンネルがフラップしたり、vPC ピアがオンラインに戻るときに、IPv4 の場合は ARP テーブルの復元にまたは IPv6 の場合は ND テーブルの復元に関与する遅延を解消するように設計されています。

## 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。

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

- 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する必要があります。IGMP スヌーピングは、デフォルトで有効になっています。



(注) 次のコマンドは、vPC モードでサポートされていません。

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

マルチキャストの詳細については、『Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 5.x』を参照してください。

## マルチキャスト PIM デュアル DR (プロキシ DR)

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

Cisco NX-OS vPC 実装 (非 F2 モード) では、PIM はデュアル指定ルータ (DR) モードで動作します。つまり、vPC デバイスが vPC SVI OIF 上の DR である場合、そのピアは自動的にプロキシ DR ロールを引き継ぎます。IGMP は、OIF が DR である場合、OIF (レポートはその OIF で学習されます) をフォワーディングに追加します。デュアル DR では、両方の vPC デバイスには、次の例に示すように、vPC SVI OIF に対して同一のエントリ (\*,G) があります。

```
VPC Device1:

(*,G)
 oif1 (igmp)
```

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

```
VPC Device2:

(*,G)
 oif1 (igmp)
```

## IP PIM PRE-BUILD SPT

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

```
VPC Device1 (say this is Forwarder for Source 'S'):

(*,G)
 oif1 (igmp)

(S,G)
 oif1 (mrib)

VPC Device2:

(*,G)
 oif1 (igmp)

(S,G)
 NULL
```

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

この問題を排除し、より優れたコンバージェンスを取得するには、**ip pim pre-build-spt** コマンドを使用します。このコマンドにより、マルチキャスト ルートに 0 OIF があっても PIM はジョインを送信できます。vPC デバイスでは、非フォワーダは送信元へ PIM (S,G) ジョインをアップストリームに送信します。欠点は非フォワーダからのリンク帯域幅アップストリームがそれにより最終的に廃棄されるトラフィックに使用されることですが、利点はより優れたコンバージェンスによる結果がリンク使用帯域幅の結果よりはるかに勝るとい点です。したがって、すべての vPC カスタマーがこのコマンドを使用することを推奨します。

## vPC ピア リンクとルーティング

ファーストホップ冗長プロトコル (FHRP) は、vPC と相互運用できます。ホットスタンバイルーティングプロトコル (HSRP)、ゲートウェイロード バランシングプロトコル (GLBP)、および仮想ルータ冗長プロトコル (VRRP) のすべてが、vPC と相互運用できます。すべてのレイヤ 3 デバイスを両方の vPC ピア デバイスにデュアル接続することを推奨します。

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

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

## マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

さらに、if-hsrp コンフィギュレーション モードで **priority** コマンドを使用して、vPC ピア リンク上でイネーブルになっているグループの状態がスタンバイになっているか、またはリッスン状態になっている場合のフェールオーバーのしきい値を設定できます。インターフェイスがアップまたはダウンするのを防ぐために下限および上限しきい値を設定できます。

VRRP は、vPC ピア デバイス上で実行されている場合に HSRP とよく似た動作を示します。VRRP は、HSRP を設定したのと同じ方法で設定してください。GLBP については、両方の vPC ピア デバイス上のフォワーダがトラフィックを転送します。

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

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

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

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

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

Cisco NX-OS リリース 4.2(1) 以降では、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 の再稼働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バケットのドロップを回避できます。

この機能を設定するには、**delay restore** コマンドを使用します。

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

FHRP とルーティングの詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』を参照してください。

## CFSoS

Cisco Fabric Services over Ethernet (CFSoS) 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。CFSoS 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/CFSoS プロトコル データ ユニット (PDU) に入れて伝送されます。

CFSoS 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 CFSoS 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。CFSoS 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。

CFSoS 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、CFSoS 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。

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。



(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。CFS over vPC 機能のための CFS over E 機能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、CFS over E を使用しているアプリケーションを表します。

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。

## vPC および孤立ポート

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

ピア リンク障害またはリストアが発生すると、孤立ポートの接続は vPC 障害または復元プロセスにバインドされる可能性があります。たとえば、デバイスのアクティブな孤立ポートがセカンダリ vPC ピアに接続する場合、ピア リンク障害が発生し、vPC ポートがセカンダリピアによって一時停止されると、そのデバイスはプライマリピアを経由する接続を失います。セカンダリピアがアクティブな孤立ポートも一時停止する場合は、デバイスのスタンバイポートがアクティブになり、プライマリピアへの接続が提供され接続が復元されます。Cisco NX-OS リリース 5.2(1) 以降では、セカンダリピアが vPC ポートを一時停止するときに特定の孤立ポートがそのピアによって一時停止され、vPC が復元されるとそのポートが復元されるように CLI で設定できます。

## 仮想化のサポート



(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 リンクとピアキーブライブ 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 内になくてもなりません。このバージョンのソフトウェアは、VDC ごとに 1 つの vPC ドメインしかサポートしません。各 VDC で 1 ~ 4096 の番号を使用して、vPC に番号を付けることができます。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。

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## 停電後のvPCリカバリ

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。機能するピアキーブアライブまたはピアリンクがないと、vPCは正常に機能することができません。しかし、Cisco NX-OS リリースによっては、vPC サービスが機能するピアのローカルポートのみを使用するようにする方法が利用可能です。

### リロードでの復元



(注) Cisco NX-OS リリース 5.2(1) 以降では、**reload restore** コマンドおよびメソッドが非推奨となっています。**auto-recovery** コマンドおよびメソッドを使用することを推奨します。

Cisco NX-OS リリース 5.0(2) 以降では、ピアがオンラインになれなかった場合に、**reload restore** コマンドを使用してvPCサービスを復元するようにCisco Nexus 7000シリーズデバイスを設定できるようになりました。この設定は、スタートアップコンフィギュレーションに保存しなければなりません。リロード時に、Cisco NX-OS ソフトウェアは、ユーザによる設定可能なタイマーを開始します（デフォルトは240秒）。ピアリンクポートが物理的に稼働し始めるか、ピアキーブ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。

ピアキーブアライブパケットもピアリンクアップパケットも受信できないままタイマーが切れると、Cisco NX-OS ソフトウェアは、プライマリ STP ロールとプライマリ LACP ロールを引き継ぎます。ソフトウェアがvPCを初期化し、そのローカルポートを稼働させ始めます。ピアがないため、ローカルvPCポートの一貫性チェックはバイパスされます。デバイスは、自身をそのロールプライオリティに関係なくSTPプライマリに選出し、LACPポートロールのマスターとしても機能します。

### 自動リカバリ

Cisco NX-OS リリース 5.2(1) 以降では、ピアがオンラインになれなかった場合に、**auto-recovery** コマンドを使用してvPCサービスを復元するようにCisco Nexus 7000シリーズデバイスを設定できるようになりました。この設定は、スタートアップコンフィギュレーションに保存しなければなりません。リロード時に、ピアリンクがダウンし、3回連続してピアキーブアライブメッセージが失われた場合、セカンダリデバイスはプライマリ STP ロールとプライマリ LACP ロールを引き継ぎます。ソフトウェアがvPCを初期化し、そのローカルポートを稼働させ始めます。ピアがないため、ローカルvPCポートの一貫性チェックはバイパスされます。デバイスは、自身をそのロールプライオリティに関係なくSTPプライマリに選出し、LACPポートロールのマスターとしても機能します。

### リカバリ後のvPCピアロール

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

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

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## High Availability（高可用性）

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

## 注意事項と制約事項

vPC には、次の注意事項と制約事項があります。

- vPC ピアは、アップグレードまたはダウングレード プロセス中に、異なるバージョンの NX-OS ソフトウェアのみを稼働できます。
- アップグレード/ダウングレードの期間外に異なるバージョンを実行している VPC ピアはサポートされません。
- 1 つの vPC のすべてのポートが、同じ VDC 内になくてもなりません。
- vPC を設定するには、まず vPC をイネーブルにする必要があります。
- システムが vPC ピア リンクを形成するには、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 メッセージを設定する必要があります。
- vPC に入れられるのは、レイヤ 2 ポート チャンネルだけです。
- 両方の vPC ピア デバイスを設定しなければなりません。設定が片方のデバイスから他方へ送信されることはありません。
- マルチレイヤ（バックツーバック）vPC を設定するには、それぞれの vPC に一意の vPC ドメイン ID を割り当てる必要があります。
- 必要な設定パラメータが、vPC ピア リンクの両側で互換性を保っているかチェックしてください。互換性に関する推奨事項について、「[vPC インターフェイスの互換パラメータ](#)」(P.7-16) を参照してください。

## マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

- 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推奨します。
- この目的には VLAN ネットワーク インターフェイスを使用するよりも、vPC ピア デバイスからのルーティングのためのレイヤ 3 リンクを別途設定してください。
- バックツーバックのマルチレイヤ vPC トポロジでは、それぞれの vPC に一意のドメイン ID が必要です。
- vPC を使用する場合は、FHRP (HSRP、VRRP、GLBP) にデフォルトのタイマーを使用し、PIM 設定を行うことを推奨します。アグレッシブ タイマーを vPC 設定で使用すると、コンバージェンス時間のメリットがありません。
- vPC 環境で OSPF を設定する場合は、コア スイッチ上でルータ コンフィギュレーション モードで次のタイマー コマンドを使用することにより、vPC ピア リンクがシャットダウンしたときに OSPF の高速コンバージェンスを実現します。

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

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

- HSRP の BFD は、vPC 環境ではサポートされていません。
- STP ポート コストは、vPC 環境で 200 に固定されています。
- 同一の物理 Cisco Nexus 7000 デバイス上の 2 つの VDC 間の単一 vPC ドメインはサポートされません。
- ジャンボ フレームは、vPC ピア リンクではデフォルトでイネーブルです。

## デフォルト設定値

表 7-2 に、vPC パラメータのデフォルト設定を示します。

表 7-2 デフォルト vPC パラメータ

| パラメータ (Parameters)    | 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   |

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

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

- 「vPC のイネーブル化」 (P.7-33)
- 「vPC のディセーブル化」 (P.7-34)
- 「vPC ドメインの作成と vpc-domain モードの開始」 (P.7-35)
- 「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」 (P.7-36)
- 「vPC ピア リンクの作成」 (P.7-38)
- 「vPC ピア ゲートウェイの設定」 (P.7-40)
- 「グレースフル整合性検査の設定」 (P.7-41)
- 「vPC ピア リンクの設定の互換性チェック」 (P.7-42)
- 「他のポート チャネルの vPC への移行」 (P.7-43)
- 「vPC ドメイン MAC アドレスの手動での設定」 (P.7-45)
- 「システム プライオリティの手動での設定」 (P.7-46)
- 「vPC ピア デバイス ロールの手動での設定」 (P.7-47)
- 「シングルモジュール vPC でのトラッキング機能の設定」 (P.7-49)
- 「停電後のリカバリの設定」 (P.7-50)
- 「孤立ポートの一時停止の設定」 (P.7-54)
- 「vPC ピア スイッチの設定」 (P.7-55)



(注)

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

## vPC のイネーブル化

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

### はじめる前に

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

### 手順の概要

1. `configure terminal`
2. `feature vpc`
3. `exit`

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

4. (任意) `show feature`
5. (任意) `copy running-config startup-config`

## 手順の詳細

|        | コマンド                                                                                                                 | 目的                                             |
|--------|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| ステップ 1 | <code>configure terminal</code><br><br>例:<br><code>switch# configure terminal</code><br><code>switch(config)#</code> | グローバル コンフィギュレーション モードを開始します。                   |
| ステップ 2 | <code>feature vpc</code><br><br>例:<br><code>switch(config)# feature vpc</code>                                       | デバイス上で vPC をイネーブルにします。                         |
| ステップ 3 | <code>exit</code><br><br>例:<br><code>switch(config)# exit</code><br><code>switch#</code>                             | 設定モードを終了します。                                   |
| ステップ 4 | <code>show feature</code><br><br>例:<br><code>switch# show feature</code>                                             | (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 | <code>copy running-config startup-config</code><br><br>例:<br><code>switch# copy running-config startup-config</code> | (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。

### はじめる前に

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

### 手順の概要

1. `configure terminal`
2. `no feature vpc`
3. `exit`

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

4. (任意) `show feature`
5. (任意) `copy running-config startup-config`

### 手順の詳細

|        | コマンド                                                                                                                 | 目的                                             |
|--------|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| ステップ 1 | <code>configure terminal</code><br><br>例:<br><code>switch# configure terminal</code><br><code>switch(config)#</code> | グローバル コンフィギュレーション モードを開始します。                   |
| ステップ 2 | <code>no feature vpc</code><br><br>例:<br><code>switch(config)# no feature vpc</code>                                 | デバイスの vPC をディセーブルにします。                         |
| ステップ 3 | <code>exit</code><br><br>例:<br><code>switch(config)# exit</code><br><code>switch#</code>                             | 設定モードを終了します。                                   |
| ステップ 4 | <code>show feature</code><br><br>例:<br><code>switch# show feature</code>                                             | (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 | <code>copy running-config startup-config</code><br><br>例:<br><code>switch# copy running-config startup-config</code> | (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。

### はじめる前に

vPC 機能をイネーブルにしていることを確認します。

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

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## 手順の概要

1. `configure terminal`
2. `vpc domain domain-id`
3. `exit`
4. (任意) `show vpc brief`
5. (任意) `copy running-config startup-config`

## 手順の詳細

|        | コマンド                                                                                                                                | 目的                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <code>configure terminal</code><br><br>例:<br><code>switch# configure terminal</code><br><code>switch(config)#</code>                | グローバル コンフィギュレーション モードを開始します。                                                                               |
| ステップ 2 | <code>vpc domain domain-id</code><br><br>例:<br><code>switch(config)# vpc domain 5</code><br><code>switch(config-vpc-domain)#</code> | デバイス上に vPC ドメインを作成し、設定目的で <code>vpc-domain</code> 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 | <code>exit</code><br><br>例:<br><code>switch(config-vpc-domain)# exit</code><br><code>switch(config)#</code>                         | <code>vpc-domain</code> 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 | <code>show vpc brief</code><br><br>例:<br><code>switch# show vpc brief</code>                                                        | (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 | <code>copy running-config startup-config</code><br><br>例:<br><code>switch# copy running-config startup-config</code>                | (任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。                                                             |

次に、vPC ドメインを作成する例を示します。

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

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

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

## vPC キープアライブ リンクと vPC キープアライブ メッセージの設定



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

## マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

キープアライブ メッセージを送信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)

独立した仮想ルーティング/転送 (VRF) 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。ピアリンク自体を使用して vPC ピアキープアライブ メッセージを送信しないでください。VRF の作成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。ピアキープアライブ メッセージに使用される送信元と宛先の両方の IP アドレスがネットワーク内で一意であることを確認してください。

管理ポートと管理 VRF が、これらのキープアライブ メッセージのデフォルトです。

### はじめる前に

vPC 機能をイネーブルにしていることを確認します。

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

### 手順の概要

1. `configure terminal`
2. `vpc domain domain-id`
3. `peer-keepalive destination ip address [hold-timeout secs | interval msec {timeout secs} | precedence {prec-value | network | internet | critical | flash-override | flash | immediate | priority | routine}] | {tos {tos-value | max-reliability | max-throughput | min-delay | min-monetary-cost | normal}} | tos-byte tos-byte-value | source ipaddress | udp-port number | vrf {name | management | vpc-keepalive}]`
4. `exit`
5. (任意) `show vpc statistics`
6. (任意) `copy running-config startup-config`

### 手順の詳細

|        | コマンド                                                                                                                                | 目的                                                          |
|--------|-------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| ステップ 1 | <code>configure terminal</code><br><br>例:<br><code>switch# configure terminal</code><br><code>switch(config)#</code>                | グローバル コンフィギュレーション モードを開始します。                                |
| ステップ 2 | <code>vpc domain domain-id</code><br><br>例:<br><code>switch(config)# vpc domain 5</code><br><code>switch(config-vpc-domain)#</code> | 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。 |

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

|        | コマンド                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 目的                                                                                                                                                                                                                                                                                                                                                 |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 3 | <pre>peer-keepalive destination ipaddress [hold-timeout secs   interval msec {timeout secs}   {precedence {prec-value   network   internet   critical   flash-override   flash   immediate priority   routine}}   tos {tos-value   max-reliability   max-throughput   min-delay   min-monetary-cost   normal}}  tos-byte tos-byte-value}   source ipaddress   vrf {name   management vpc-keepalive}]</pre> <p>例:</p> <pre>switch(config-vpc-domain)# peer-keepalive destination 172.28.230.85 switch(config-vpc-domain)#</pre> | <p>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。</p> <p>(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。</p> <p>管理ポートと VRF がデフォルトです。</p> <p>(注) 独立した VRF を設定し、vPC ピアキープアライブ リンクのための VRF 内の各 vPC ピア デバイスからのレイヤ 3 ポートを使用することを推奨します。VRF の作成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。</p> |
| ステップ 4 | <pre>exit</pre> <p>例:</p> <pre>switch(config-vpc-domain)# exit switch(config)#</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                           | <p>vpc-domain コンフィギュレーション モードを終了します。</p>                                                                                                                                                                                                                                                                                                           |
| ステップ 5 | <pre>show vpc statistics</pre> <p>例:</p> <pre>switch# show vpc statistics</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                | <p>(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。</p>                                                                                                                                                                                                                                                                                                          |
| ステップ 6 | <pre>copy running-config startup-config</pre> <p>例:</p> <pre>switch# copy running-config startup-config</pre>                                                                                                                                                                                                                                                                                                                                                                                                                  | <p>(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。</p>                                                                                                                                                                                                                                                                                               |

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

### はじめる前に

vPC 機能をイネーブルにしていることを確認します。

レイヤ 2 ポート チャネルを使用していることを確認します。

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

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

## 手順の概要

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

## 手順の詳細

|        | コマンド                                                                                                                                 | 目的                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| ステップ 1 | <code>configure terminal</code><br><br>例:<br>switch# configure terminal<br>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 | <code>interface port-channel channel-number</code><br><br>例:<br>switch(config)# interface port-channel 20<br>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 | <code>switchport mode trunk</code><br><br>例:<br>switch(config-if)# switchport mode trunk                                             | (任意) このインターフェイスのトランキング モードで設定します。                                     |
| ステップ 4 | <code>switchport trunk allowed vlan vlan-list</code><br><br>例:<br>switch(config-if)# switchport trunk<br>allowed vlan 1-120,201-3967 | (任意) 許容 VLAN リストを設定します。                                               |
| ステップ 5 | <code>vpc peer-link</code><br><br>例:<br>switch(config-if)# vpc peer-link<br>switch(config-vpc-domain)#                               | 選択したポート チャネルを vPC ピア リンクとして設定し、vpc-domain コンフィギュレーション モードを開始します。      |
| ステップ 6 | <code>exit</code><br><br>例:<br>switch(config-vpc-domain)# exit<br>switch(config)#                                                    | vpc-domain コンフィギュレーション モードを終了します。                                     |

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

|        | コマンド                                                                                              | 目的                                                   |
|--------|---------------------------------------------------------------------------------------------------|------------------------------------------------------|
| ステップ 7 | <b>show vpc brief</b><br><br>例:<br>switch# show vpc brief                                         | (任意) 各 vPC に関する情報を表示します。<br>vPC ピア リンクに関する情報も表示されます。 |
| ステップ 8 | <b>copy running-config startup-config</b><br><br>例:<br>switch# copy running-config startup-config | (任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。        |

次の例は、vPC ピア リンクを設定する方法を示します。

```
switch# configure terminal
switch(config)# interface port-channel 20
switch(config-if)# switchport mode
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1-120,201-3967
switch(config-if)# vpc peer-link
switch(config-vpc-domain)#
```

## vPC ピアゲートウェイの設定

Cisco NX-OS リリース 4.2(1) とそれ以降のリリースでは、vPC ピア デバイスを、vPC ピア デバイスの MAC アドレスを送信先とするパケットに対してもゲートウェイとして機能するように設定できるようになりました。



(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する必要があります。vPC ピアゲートウェイ機能の使用では、この要件は変わりません。

### はじめる前に

vPC 機能をイネーブルにしていることを確認します。

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

### 手順の概要

1. **configure terminal**
2. **vpc domain *domain-id***
3. **peer-gateway**
4. **peer-gateway exclude-vlan *backup-vlan-id***
5. **exit**
6. (任意) **show vpc brief**
7. (任意) **copy running-config startup-config**

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## 手順の詳細

|        | コマンド                                                                                                                                                                                                    | 目的                                                                                                                                |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例：<br>switch# configure terminal<br>switch(config)#                                                                                                                    | グローバル コンフィギュレーション モードを開始します。                                                                                                      |
| ステップ 2 | <b>vpc domain domain-id</b><br><br>例：<br>switch(config-if)# vpc domain 5<br>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 3 | <b>peer-gateway</b><br><br>例：<br>switch(config-vpc-domain)# peer-gateway<br>(注)<br>-----:: 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 4 | <b>peer-gateway exclude-vlan backup-vlan-id</b><br><br>例：<br>switch(config-vpc-domain)# peer-gateway exclude-vlan 2                                                                                     | (任意) Cisco NX-OS リリース 5.1(3) 以降では、混在シャードモードの中継 VLAN トラフィックのソフトウェア スイッチングを回避します。<br>(注) 詳細については、「vPC ピア ゲートウェイ」(P.7-13) を参照してください。 |
| ステップ 5 | <b>exit</b><br><br>例：<br>switch(config-vpc-domain)# exit<br>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 6 | <b>show vpc brief</b><br><br>例：<br>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 7 | <b>copy running-config startup-config</b><br><br>例：<br>switch# copy running-config startup-config                                                                                                       | (任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。                                                                                    |

## グレースフル整合性検査の設定

Cisco NX-OS リリース 5.2(1) 以降では、グレースフル整合性検査機能を設定できます。それはデフォルトでイネーブルになっています。この機能がイネーブルでない場合、必須互換性パラメータの不一致が動作中の vPC で導入されると、vPC は完全に一時停止します。この機能がイネーブルの場合、セカンダリ ピア デバイスのリンクだけが一時停止します。vPC 上での一貫した設定については、「vPC インターフェイスの互換パラメータ」(P.7-16) を参照してください。

## 手順の概要

1. **configure terminal**
2. **vpc domain domain-id**

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

3. graceful consistency-check
4. exit
5. (任意) show vpc brief

## 手順の詳細

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

次に、グレースフル整合性検査機能をイネーブルにする例を示します。

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

## 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 インターフェイスの互換パラメータ](#)」(P.7-16) を参照してください。

## 手順の概要

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

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## 手順の詳細

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

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

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



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

## 他のポート チャネルの vPC への移行



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

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

### はじめる前に

vPC 機能をイネーブルにしていることを確認します。

レイヤ 2 ポート チャネルを使用していることを確認します。

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

### 手順の概要

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

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

4. `exit`
5. (任意) `show vpc brief`
6. (任意) `copy running-config startup-config`

## 手順の詳細

|        | コマンド                                                                                                                                                      | 目的                                                                                                                                                                                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <code>configure terminal</code><br><br>例:<br><code>switch# configure terminal</code><br><code>switch(config)#</code>                                      | グローバル コンフィギュレーション モードを開始します。                                                                                                                                                                             |
| ステップ 2 | <code>interface port-channel channel-number</code><br><br>例:<br><code>switch(config)# interface port-channel 20</code><br><code>switch(config-if)#</code> | 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 チャンネルを選択し、インターフェイス コンフィギュレーション モードを開始します。                                                                                                                              |
| ステップ 3 | <code>vpc number</code><br><br>例:<br><code>switch(config-if)# vpc 5</code><br><code>switch(config-vpc-domain)#</code>                                     | 選択したポート チャンネルを 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 チャンネルには、デバイス内の任意のモジュールを使用できます。範囲は、1 ~ 4096 です。<br><br>(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 チャンネルに割り当てる 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 | <code>exit</code><br><br>例:<br><code>switch(config-vpc-domain)# exit</code><br><code>switch(config)#</code>                                               | 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 | <code>show vpc brief</code><br><br>例:<br><code>switch# show vpc brief</code>                                                                              | (任意) vPC に関する情報を表示します。                                                                                                                                                                                   |
| ステップ 6 | <code>copy running-config startup-config</code><br><br>例:<br><code>switch# copy running-config startup-config</code>                                      | (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 チャン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)
```

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## vPC ドメイン MAC アドレスの手動での設定

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

### はじめる前に

vPC 機能をイネーブルにしていることを確認します。

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

### 手順の概要

1. `configure terminal`
2. `vpc domain domain-id`
3. `system-mac mac-address`
4. `exit`
5. (任意) `show vpc role`
6. (任意) `copy running-config startup-config`

### 手順の詳細

|        | コマンド                                                                                                                                | 目的                                                       |
|--------|-------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| ステップ 1 | <code>configure terminal</code><br><br>例：<br>switch# configure terminal<br>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 | <code>vpc domain domain-id</code><br><br>例：<br>switch(config)# vpc domain 5<br>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 | <code>system-mac mac-address</code><br><br>例：<br>switch(config-vpc-domain)# system-mac 23fb.4ab5.4c4e<br>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 | <code>exit</code><br><br>例：<br>switch(config-vpc-domain)# exit<br>switch(config)#                                                   | vpc-domain コンフィギュレーション モードを終了します。                        |

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

|        | コマンド                                                                                              | 目的                                            |
|--------|---------------------------------------------------------------------------------------------------|-----------------------------------------------|
| ステップ 5 | <b>show vpc role</b><br><br>例:<br>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 | <b>copy running-config startup-config</b><br><br>例:<br>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 の実行時には、vPC ピア デバイスが LACP のプライマリ デバイスになるように、vPC システムプライオリティを手動で設定することを推奨します。システムプライオリティを手動で設定する場合には、必ず同じプライオリティ値を両方の vPC ピア デバイスに設定します。これらの値が一致しないと、vPC は起動しません。

### はじめる前に

vPC 機能をイネーブルにしていることを確認します。

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

### 手順の概要

1. `configure terminal`
2. `vpc domain domain-id`
3. `system-priority priority`
4. `exit`
5. (任意) `show vpc role`
6. (任意) `copy running-config startup-config`

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## 手順の詳細

|        | コマンド                                                                                                                       | 目的                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例：<br>switch# configure terminal<br>switch(config)#                                       | グローバル コンフィギュレーション モードを開始します。                                                  |
| ステップ 2 | <b>vpc domain domain-id</b><br><br>例：<br>switch(config)# vpc domain 5<br>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 | <b>system-priority priority</b><br><br>例：<br>switch(config-vpc-domain)# system-priority 4000<br>switch(config-vpc-domain)# | 指定した vPC ドメインに割り当てるシステム プライオリティを入力します。指定できる値の範囲は、1～65535 です。デフォルト値は 32667 です。 |
| ステップ 4 | <b>exit</b><br><br>例：<br>switch(config-vpc-domain)# exit<br>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 | <b>show vpc role</b><br><br>例：<br>switch# show vpc role                                                                    | (任意) vPC システム プライオリティを表示します。                                                  |
| ステップ 6 | <b>copy running-config startup-config</b><br><br>例：<br>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 リンクの両端を設定すると、Cisco NX-OS ソフトウェアはプライマリとセカンダリの vPC ピア デバイスを選択します。ただし、vPC のプライマリ デバイスとして、特定の vPC ピア デバイスを選択することもできます。選択したら、プライマリ デバイスにする vPC ピア デバイスに、他の vPC ピア デバイスより小さいロール値を手動で設定します。

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

### はじめる前に

vPC 機能をイネーブルにしていることを確認します。

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

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## 手順の概要

1. **configure terminal**
2. **vpc domain** *domain-id*
3. **role priority** *priority*
4. **exit**
5. (任意) **show vpc role**
6. (任意) **copy running-config startup-config**

## 手順の詳細

|        | コマンド                                                                                                                       | 目的                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例:<br>switch# configure terminal<br>switch(config)#                                       | グローバル コンフィギュレーション モードを開始します。                                                                                                            |
| ステップ 2 | <b>vpc domain</b> <i>domain-id</i><br><br>例:<br>switch(config)# vpc domain 5<br>switch(config-vpc-domain)#                 | 設定する vPC ドメインの番号を入力します。<br>vpc-domain コンフィギュレーション モードを開始します。                                                                            |
| ステップ 3 | <b>role priority</b> <i>priority</i><br><br>例:<br>switch(config-vpc-domain)# role priority 4<br>switch(config-vpc-domain)# | vPC システム プライオリティに与えるロール<br>プライオリティを入力します。指定できる値の<br>範囲は 1 ~ 65636 で、デフォルト値は 32667 で<br>す。低い値は、このスイッチがプライマリ vPC<br>になる可能性が高いということを意味します。 |
| ステップ 4 | <b>exit</b><br><br>例:<br>switch(config-vpc-domain)# exit<br>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 | <b>show vpc role</b><br><br>例:<br>switch# show vpc role                                                                    | (任意) vPC システム プライオリティを表示します。                                                                                                            |
| ステップ 6 | <b>copy running-config startup-config</b><br><br>例:<br>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<br>アップ コンフィギュレーションにコピーします。                                                                                      |

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

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

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## シングルモジュール vPC でのトラッキング機能の設定

Cisco NX-OS Release 4.2 以降では、すべての vPC ピア リンクとコアに面するインターフェイスを単一モジュール上で設定しなければならない場合は、両方のプライマリ vPC ピア デバイス上の vPC ピア リンクのすべてのリンク上の、およびコアへのレイヤ 3 リンクに関連付けられているトラック オブジェクトとトラック リストを設定しなければなりません。いったんこの機能を設定したら、プライマリ vPC ピア デバイスに障害が発生した場合には、プライマリ vPC ピア デバイス上のすべての vPC リンクを、システムが自動的に停止します。システムが安定するまでは、このアクションにより、すべての vPC トラフィックが強制的にセカンダリ vPC ピア デバイスに送られます。

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

### はじめる前に

vPC 機能をイネーブルにしていることを確認します。

正しい仮想デバイス コンテキスト (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)。

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. (任意) `show vpc`
6. (任意) `copy running-config startup-config`

### 手順の詳細

|        | コマンド                                                                                                                                | 目的                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| ステップ 1 | <code>configure terminal</code><br><br>例:<br><code>switch# configure terminal</code><br><code>switch(config)#</code>                | グローバル コンフィギュレーション モードを開始します。                                 |
| ステップ 2 | <code>vpc domain domain-id</code><br><br>例:<br><code>switch(config)# vpc domain 5</code><br><code>switch(config-vpc-domain)#</code> | 設定する vPC ドメインの番号を入力します。<br>vpc-domain コンフィギュレーション モードを開始します。 |

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

|        | コマンド                                                                                                                        | 目的                                                                                                                                                                              |
|--------|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 3 | <pre>track track-object-id</pre> <p>例:</p> <pre>switch(config-vpc-domain)# track object 23 switch(config-vpc-domain)#</pre> | 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 | <pre>exit</pre> <p>例:</p> <pre>switch(config-vpc-domain)# exit switch(config)#</pre>                                        | 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 | <pre>show vpc brief</pre> <p>例:</p> <pre>switch# show vpc brief</pre>                                                       | (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 | <pre>copy running-config startup-config</pre> <p>例:</p> <pre>switch# copy running-config startup-config</pre>               | (任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。                                                                                                                                  |

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

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

## 停電後のリカバリの設定

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。

### リロード復元の設定



(注) Cisco NX-OS リリース 5.2(1) 以降では、**reload restore** コマンドおよびこのセクションで説明されている手順が非推奨となっています。**auto-recovery** コマンドおよび「[自動リカバリの設定 \(P.7-52\)](#)」で説明されている手順を使用することを推奨します。

Cisco NX-OS リリース 5.0(2) 以降では、ピアがオンラインになれなかった場合に、**reload restore** コマンドを使用して vPC サービスを復元するように Cisco Nexus 7000 シリーズ デバイスを設定できるようになりました。

### はじめる前に

vPC 機能をイネーブルにしていることを確認します。

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

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## 手順の概要

1. `configure terminal`
2. `vpc domain domain-id`
3. `reload restore [delay time-out]`
4. `exit`
5. (任意) `show running-config vpc`
6. (任意) `show vpc consistency-parameters interface port-channel number`
7. (任意) `copy running-config startup-config`

## 手順の詳細

|        | コマンド                                                                                                                                                                  | 目的                                                                                                                                                |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <code>configure terminal</code><br><br>例:<br><code>switch# configure terminal</code><br><code>switch(config)#</code>                                                  | グローバル コンフィギュレーション モードを開始します。                                                                                                                      |
| ステップ 2 | <code>vpc domain domain-id</code><br><br>例:<br><code>switch(config)# vpc domain 5</code><br><code>switch(config-vpc-domain)#</code>                                   | 設定する vPC ドメインの番号を入力します。<br>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 | <code>reload restore [delay time-out]</code><br><br>例:<br><code>switch(config-vpc-domain)# reload restore</code>                                                      | vPC がそのピアが機能しないことを前提として vPC を稼働させ始めるように設定します。デフォルト遅延値は 240 秒です。タイムアウト遅延は 240 ~ 3600 秒の間で設定できます。<br>vPC を標準動作にリセットするには、このコマンドの <b>no</b> 形式を使用します。 |
| ステップ 4 | <code>exit</code><br><br>例:<br><code>switch(config-vpc-domain)# exit</code><br><code>switch(config)#</code>                                                           | 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 | <code>show running-config vpc</code><br><br>例:<br><code>switch# show running-config vpc</code>                                                                        | (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 | <code>show vpc consistency-parameters interface port-channel number</code><br><br>例:<br><code>switch# show vpc consistency-parameters interface port-channel 1</code> | (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 | <code>copy running-config startup-config</code><br><br>例:<br><code>switch# copy running-config startup-config</code>                                                  | (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。<br><b>(注)</b> 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。                                              |

## マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

次に、vPC リロード復元機能を設定し、それをスイッチのスタートアップ コンフィギュレーションに保存する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vpc domain 5
switch(config-vpc-domain)# reload restore
Warning:
 Enables restoring of vPCs in a peer-detached state after reload, will wait for 240
seconds (by default) to determine if peer is un-reachable
switch(config-vpc-domain)# exit
switch(config)# exit
switch# copy running-config startup-config
switch# show running-config vpc

!Command: show running-config vpc
!Time: Wed Mar 24 18:43:54 2010

version 5.0(2)
feature vpc

logging level vpc 6
vpc domain 5
 reload restore
```

次の例は、一貫性パラメータを確認する方法を示します。

```
switch# show vpc consistency-parameters interface port-channel 1
Legend:
 Type 1 : vPC will be suspended in case of mismatch
Name Type Local Value Peer Value

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

## 自動リカバリの設定

Cisco NX-OS リリース 5.2(1) 以降では、ピアがオンラインになれなかった場合に、**auto-recovery** コマンドを使用して vPC サービスを復元するように Cisco Nexus 7000 シリーズ デバイスを設定できるようになりました。

### はじめる前に

vPC 機能をイネーブルにしていることを確認します。

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

### 手順の概要

1. **configure terminal**
2. **vpc domain domain-id**

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

3. `auto-recovery [reload-delay time]`
4. `exit`
5. (任意) `show running-config vpc`
6. (任意) `show vpc consistency-parameters interface port-channel number`
7. (任意) `copy running-config startup-config`

## 手順の詳細

|        | コマンド                                                                                                                                                                  | 目的                                                                                                                                                                        |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <code>configure terminal</code><br><br>例:<br>switch# <code>configure terminal</code><br>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 | <code>vpc domain domain-id</code><br><br>例:<br>switch(config)# <code>vpc domain 5</code><br>switch(config-vpc-domain)#                                                | 設定する vPC ドメインの番号を入力します。<br>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 | <code>auto-recovery [reload-delay time]</code><br><br>例:<br>switch(config-vpc-domain)# <code>auto-recovery</code>                                                     | vPC がそのピアが機能しないことを前提として vPC を稼働させ始めるように設定し、vPC を復元するためのリロード後に待機する時間を指定します。デフォルト遅延値は 240 秒です。240 ~ 3600 秒の遅延を設定できます。<br><br>vPC を標準動作にリセットするには、このコマンドの <b>no</b> 形式を使用します。 |
| ステップ 4 | <code>exit</code><br><br>例:<br>switch(config-vpc-domain)# <code>exit</code><br>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 | <code>show running-config vpc</code><br><br>例:<br>switch# <code>show running-config vpc</code>                                                                        | (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 | <code>show vpc consistency-parameters interface port-channel number</code><br><br>例:<br>switch# <code>show vpc consistency-parameters interface port-channel 1</code> | (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 | <code>copy running-config startup-config</code><br><br>例:<br>switch# <code>copy running-config startup-config</code>                                                  | (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。<br><br>(注) 自動リカバリ機能がイネーブルになっていることを確認するには、この手順を実行します。                                                                        |

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

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

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vpc domain 5
switch(config-vpc-domain)# auto-recovery
Warning:
 Enables restoring of vPCs in a peer-detached state after reload, will wait for 240
seconds to determine if peer is un-reachable
switch(config-vpc-domain)# exit
switch(config)# exit
switch# copy running-config startup-config
```

## 孤立ポートの一時停止の設定

vPC 対応でないデバイスが各ピアに接続するとき、接続されたポートは vPC のメンバではないため、孤立ポートと称されます。Cisco NX-OS リリース 5.2(1) 以降では、ピア リンクまたはピア キープアライブ障害に応じてセカンダリ ピアが vPC ポートを一時停止するときに、セカンダリ ピアによって一時停止（シャットダウン）される孤立ポートとして物理インターフェイスを明示的に宣言できます。孤立ポートは vPC が復元されたときに復元されます。



(注)

vPC 孤立ポートの一時停止は、ポート チャネルのメンバ ポートではなく、物理ポートでのみ設定できます。

### はじめる前に

vPC 機能をイネーブルにしていることを確認します。

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

### 手順の概要

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

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## 手順の詳細

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

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

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

## vPC ピア スイッチの設定

Cisco Nexus 7000 シリーズ デバイスは、一対の vPC デバイスがレイヤ 2 トポロジ内で 1 つの STP ルートとして現れるように設定することができます。この項では、次のトピックについて取り上げます。

- 「[純粋な vPC ピア スイッチ トポロジの設定](#)」 (P.7-55)
- 「[ハイブリッド vPC ピア スイッチ トポロジの設定](#)」 (P.7-57)

### 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。

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## はじめる前に

vPC 機能をイネーブルにしていることを確認します。

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

## 手順の概要

1. `configure terminal`
2. `vpc domain domain-id`
3. `peer-switch`
4. `spanning-tree vlan vlan-range priority value`
5. `exit`
6. (任意) `show spanning-tree summary`
7. (任意) `copy running-config startup-config`

## 手順の詳細

|        | コマンド                                                                                                                         | 目的                                                                                                             |
|--------|------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <code>configure terminal</code><br><br>例：<br>switch# configure terminal<br>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 | <code>vpc domain domain-id</code><br><br>例：<br>switch(config)# vpc domain 5<br>switch(config-vpc-domain)#                    | 設定する vPC ドメインの番号を入力します。<br>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 | <code>peer-switch</code><br><br>例：<br>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。<br>ピア スイッチ vPC トポロジをディセーブルにするには、このコマンドの <b>no</b> 形式を使用します。 |
| ステップ 4 | <code>spanning-tree vlan vlan-range priority value</code><br><br>例：<br>switch(config)# spanning-tree vlan 1<br>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 | <code>exit</code><br><br>例：<br>switch(config-vpc-domain)# exit<br>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 6 | <code>show spanning-tree summary</code><br><br>例：<br>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 | <code>copy running-config startup-config</code><br><br>例：<br>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。                                                                 |

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

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 ID を変更した後、ルートブリッジ ID を最高のブリッジプライオリティよりもよい値に変更することにより、ハイブリッド vPC または非 vPC ピア スイッチ トポロジを設定することができます。次に、ピア スイッチをイネーブルにします。

### はじめる前に

vPC 機能をイネーブルにしていることを確認します。

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

### 手順の概要

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. (任意) **show spanning-tree summary**
9. (任意) **copy running-config startup-config**

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## 手順の詳細

|        | コマンド                                                                                                                               | 目的                                                                                                             |
|--------|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例:<br>switch# configure terminal<br>switch(config)#                                               | グローバル コンフィギュレーション モードを開始します。                                                                                   |
| ステップ 2 | <b>spanning-tree pseudo-information</b><br><br>例:<br>switch(config)# spanning-tree<br>pseudo-information<br>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 | <b>vlan vlan-id designated priority priority</b><br><br>例:<br>switch(config-pseudo)# vlan 1 designated<br>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 | <b>vlan vlan-id root priority priority</b><br><br>例:<br>switch(config-pseudo)# vlan 1 root<br>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 | <b>vpc domain domain-id</b><br><br>例:<br>switch(config)# vpc domain 5<br>switch(config-vpc-domain)#                                | 設定する vPC ドメインの番号を入力します。<br>vpc-domain コンフィギュレーション モードを開始します。                                                   |
| ステップ 6 | <b>peer-switch</b><br><br>例:<br>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。<br>ピア スイッチ vPC トポロジをディセーブルにするには、このコマンドの <b>no</b> 形式を使用します。 |
| ステップ 7 | <b>exit</b><br><br>例:<br>switch(config-vpc-domain)# exit<br>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 8 | <b>show spanning-tree summary</b><br><br>例:<br>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 | <b>copy running-config startup-config</b><br><br>例:<br>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
```

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## 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                                                                                             |
|----------------------------------------------|------------------------------------------------------------------------------------------------|
| <code>show feature</code>                    | vPC がイネーブルになっているかどうかを表示します。                                                                    |
| <code>show vpc brief</code>                  | vPC に関する簡単な情報を表示します。                                                                           |
| <code>show vpc consistency-parameters</code> | すべての vPC インターフェイス全体で一貫している必要があるパラメータのステータスを表示します。                                              |
| <code>show running-config vpc</code>         | vPC の実行コンフィギュレーションの情報を表示します。                                                                   |
| <code>show port-channel capacity</code>      | 設定されているポート チャンネルの数、およびデバイス上でまだ使用可能なポート チャンネル数を表示します。                                           |
| <code>show vpc statistics</code>             | vPC に関する統計情報を表示します。                                                                            |
| <code>show vpc peer-keepalive</code>         | ピアキープアライブ メッセージの情報を表示します。                                                                      |
| <code>show vpc role</code>                   | ピア ステータス、ローカル デバイスのロール、vPC システム MAC アドレスとシステムプライオリティ、およびローカル vPC デバイスの MAC アドレスとプライオリティを表示します。 |

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

## vPC のモニタリング

vPC 統計情報を表示するには、`show vpc statistics` コマンドを使用します。



(注)

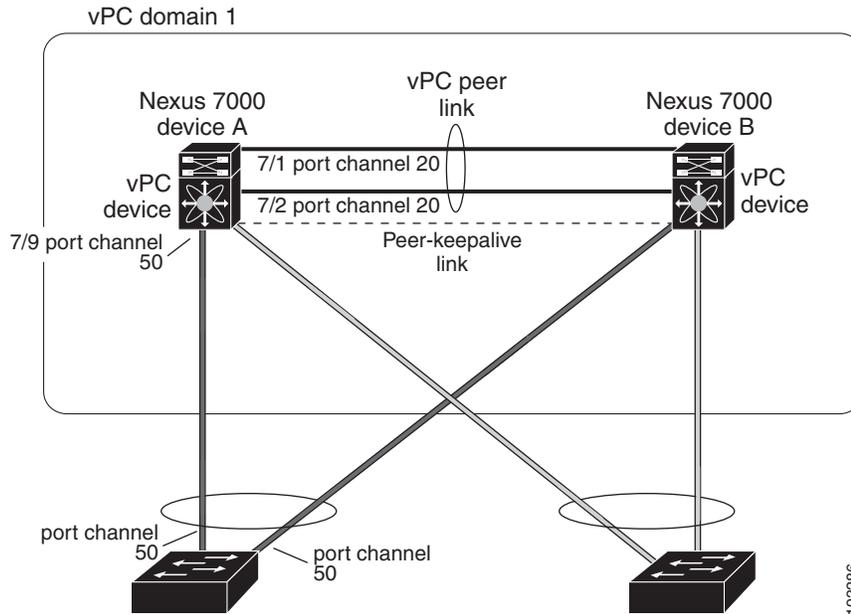
このコマンドは、現在作業している vPC ピア デバイスの vPC 統計情報しか表示しません。

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## vPC の設定例

次の例は、デバイス A 上で図 7-11 に示すとおり vPC を設定する方法を示します。

図 7-11 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)#
```

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

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

- ステップ 8** vPC ピア リンクを設定します。

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

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

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

- ステップ 10** 設定を保存します。

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

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。



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

## その他の参考資料

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.7-62)
- 「標準」 (P.7-62)
- 「管理情報ベース (MIB)」 (P.7-63)

## 関連資料

| 関連項目              | マニュアル タイトル                                                                              |
|-------------------|-----------------------------------------------------------------------------------------|
| ポート チャンネルの設定      | 第 6 章「ポート チャンネルの設定」                                                                     |
| 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

| 標準           | タイトル |
|--------------|------|
| IEEE 802.3ad | —    |

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## 管理情報ベース (MIB)

| MIB                                                                                              | MIB のリンク                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>IEEE8023-LAG-CAPABILITY</li> <li>CISCO-LAG-MIB</li> </ul> | <p>MIB を検索およびダウンロードするには、次の URL にアクセスしてください。</p> <p><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></p> |

## vPC の設定機能の履歴

表 7-3 に、この機能のリリース履歴を示します。

表 7-3 vPC の設定機能の履歴

| 機能名 | リリース   | 機能情報                                                                                                             |
|-----|--------|------------------------------------------------------------------------------------------------------------------|
| vPC | 5.2(1) | 矛盾した設定がピア間で検出されたときに、vPC プライマリ デバイスがトラフィックを転送することを可能にする <b>graceful consistency-check</b> コマンドが追加されました。           |
| vPC | 5.2(1) | 矛盾した設定の VLAN だけが一時停止されるように VLAN 単位整合性検査が追加されました。                                                                 |
| vPC | 5.2(1) | 停電後に vPC リカバリのスピードと信頼性を高めるための <b>auto-recovery</b> コマンドが追加されました。 <b>reload restore</b> コマンドが非推奨になりました。           |
| vPC | 5.2(1) | vPC で障害が発生したときに vPC セカンダリ デバイスの孤立ポートを一時停止するための <b>vpc orphan-ports suspend</b> コマンドが追加されました。                     |
| vPC | 5.2(1) | サポートが 528 vPC にまで増えました。                                                                                          |
| vPC | 5.0(2) | vPC スイッチがそのピアが機能しないことを前提として vPC を稼働させ始めるように設定する <b>reload restore</b> 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 <b>peer-switch</b> コマンドが追加されました。                            |
| vPC | 4.2(1) | サポートが 256 vPC にまで増えました。                                                                                          |
| vPC | 4.2(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、 <b>peer-gateway</b> コマンドが追加されました。                                 |
| vPC | 4.2(1) | vPC ピア リンクに障害が発生しても、確実に VLAN インターフェイスが稼働したままになるようにするために、 <b>dual-active exclude interface-vlan</b> コマンドが追加されました。 |
| vPC | 4.2(1) | リロード後にルーティング テーブルが収束できるまで vPC セカンダリ デバイスの稼働を遅延させるための <b>delay restore</b> コマンドが追加されました。                          |
| vPC | 4.1(4) | サポートが 192 vPC にまで増えました。                                                                                          |
| vPC | 4.1(2) | これらの機能が導入されました。                                                                                                  |

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## 第 8 章

# IP トンネルの設定

この章では、Cisco NX-OS デバイス上で Generic Routing Encapsulation (GRE) を使用して IP トンネルを設定する方法について説明します。

この章は、次の項で構成されています。

- 「IP トンネルについて」 (P.8-1)
- 「IP トンネルのライセンス要件」 (P.8-4)
- 「IP トンネルの前提条件」 (P.8-4)
- 「注意事項および制約事項」 (P.8-4)
- 「デフォルト設定」 (P.8-5)
- 「IP トンネルの設定」 (P.8-5)
- 「IP トンネル設定の確認」 (P.8-11)
- 「IP トンネリングの設定例」 (P.8-11)
- 「その他の関連資料」 (P.8-12)
- 「IP トンネル設定の機能履歴」 (P.8-12)

## IP トンネルについて

IP トンネルを使うと、同じレイヤまたは上位層プロトコルをカプセル化して、2 台のデバイス間で作成されたトンネルを通じて IP に結果を転送できます。

この項では、次のトピックについて取り上げます。

- 「IP トンネルの概要」 (P.8-2)
- 「GRE トンネル」 (P.8-2)
- 「パス MTU ディスカバリ」 (P.8-3)
- 「仮想化のサポート」 (P.8-3)
- 「High Availability (高可用性)」 (P.8-4)

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## 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.8-5) を参照してください。

設定の前にトンネル機能をイネーブルにする必要があります。Cisco NX-OS リリース 4.2 から、システムは機能のディセーブル化の前に自動的にチェックポイントを作成するため、このチェックポイントにロールバックできます。ロールバック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 以降では、ある VDC に設定されたトンネルは、同じ番号を持つ別の VDC に設定されたトンネルとは区別されます。たとえば、VDC 1 のトンネル 0 は VDC 2 のトンネル 0 とは異なります。

Cisco NX-OS Release 4.2 以降では、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。

## GRE トンネル



(注)

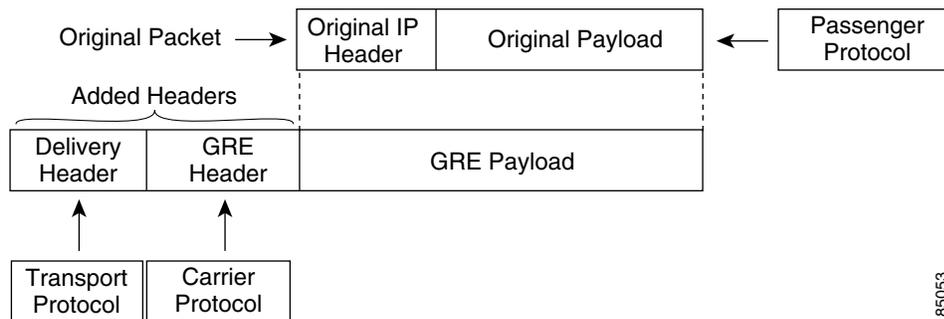
Cisco NX-OS リリース 5.1(1) 以降では、ソフトウェアは GRE トンネルを通じてマルチキャストをサポートします。

Generic Routing Encapsulation (GRE) をさまざまなパッセンジャ プロトコルのキャリア プロトコルとして使用できます。

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。

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

図 8-1 GRE Protocol Data Unit (PDU)



185053

## パス MTU ディスカバリ

パス最大伝送単位 (MTU) ディスカバリ (PMTUD) は、パケットの発信元から宛先へのパスに沿って最小 MTU を動的に決定することで、2つのエンドポイント間のパスのフラグメンテーションを防ぎます。PMTUD は、パケットにフラグメンテーションが必要であるという情報がインターフェイスに届くと、接続に対する送信 MTU 値を減らします。

PMTUD をイネーブルにすると、インターフェイスはトンネルを通過するすべてのパケットに Don't Fragment (DF) ビットを設定します。トンネルに入ったパケットがそのパケットの MTU 値よりも小さい MTU 値を持つリンクを検出すると、リモートリンクはそのパケットをドロップし、パケットの送信元にインターネット制御メッセージプロトコル (ICMP) メッセージを返します。このメッセージには、フラグメンテーションが要求されたこと (しかし許可されなかったこと) と、パケットをドロップしたリンクの MTU が含まれています。



(注)

トンネル インターフェイスの PMTUD は、トンネル エンドポイントがトンネルのパスでデバイスによって生成される ICMP メッセージを受信することを要求します。ファイアウォール接続を通じて PMTUD を使用する前に、ICMP メッセージが受信できることを確認してください。

## 仮想化のサポート

IP トンネルはデフォルトの仮想デバイス コンテキスト (VDC) およびデフォルトの仮想ルーティング/転送 (VRF) インスタンスにだけ設定できます。

Cisco NX-OS Release 4.2 以降では、トンネル インターフェイスを仮想ルーティングと転送 (VRF) インスタンスのメンバーおよび任意の VDC のメンバー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。また、トンネルの宛先を検索するために使用する VRF を設定できます。この VRF は、トンネル送信元 IP アドレスの VRF に一致させる必要があります。

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

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## High Availability（高可用性）

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の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。 |

## IPトンネルの前提条件

IPトンネルには次の前提条件があります。

- IPトンネルを設定するためのTCP/IPに関する基礎知識があること。
- スイッチにログインしている。
- Cisco NX-OS の Enterprise Services ライセンスをインストールしていること。
- IPトンネルを設定してイネーブルにする前にデバイスのトンネリング機能をイネーブルにしておくこと。

## 注意事項および制約事項

IPトンネルの設定に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS は、IETF RFC 2784 に定義されている GRE ヘッダーをサポートします。Cisco NX-OS は、トンネル キーと IETF RFC 1701 のその他のオプションをサポートしません。
- Cisco NX-OS Release 5.2(5) および 5.2(x) リリース以降、異なる仮想ルーティングと転送インスタンス（VRF）でトンネル インターフェイスおよびトンネル転送を設定できます。トンネルは、Cisco Nexus 7000 シリーズ プラットフォームの M1 シリーズのカードでのみサポートされます。
- Cisco NX-OS は、トンネル インターフェイスの WCCP をサポートしません。
- Cisco NX-OS は、GRE トンネル キープアライブをサポートしません。

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## 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 (Parameters)          | デフォルト  |
|-----------------------------|--------|
| Path MTU Discovery 経過時間タイマー | 10 分   |
| パス MTU ディスカバリの最小 MTU        | 64     |
| トンネル機能                      | ディセーブル |

## IP トンネルの設定

この項では、次のトピックについて取り上げます。

- 「トンネリングのイネーブル化」 (P.8-5)
- 「トンネル インターフェイスの作成」 (P.8-6)
- 「GRE トンネルの設定」 (P.8-8)
- 「Path MTU Discovery のイネーブル化」 (P.8-9)
- 「トンネル インターフェイスへの VRF メンバーシップの割り当て」 (P.8-10)



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

## 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`

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

### 手順の詳細

|        | コマンド                                                                                                         | 目的                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例:<br>switch# configure terminal<br>switch(config)#                         | グローバル コンフィギュレーション モードを開始します。                                                        |
| ステップ 2 | <b>feature tunnel</b><br><br>例:<br>switch(config)# feature tunnel<br>switch(config-if)#                      | 新しいトンネル インターフェイスを作成できます。<br>トンネル インターフェイス機能をディセーブルにするには、このコマンドの <b>no</b> 形式を使用します。 |
| ステップ 3 | <b>exit</b><br><br>例:<br>switch(config-if)# exit<br>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 4 | <b>show feature</b><br><br>例:<br>switch(config-if)# show feature                                             | (任意) デバイス上でイネーブルされている機能に関する情報を表示します。                                                |
| ステップ 5 | <b>copy running-config startup-config</b><br><br>例:<br>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 インターフェイスの作成

トンネル インターフェイスを作成して、この論理インターフェイスを IP トンネルに設定できます。

### はじめる前に

Cisco NX-OS Release 5.2(5) および 5.2(x) リリース以降、異なる VRF でトンネルの送信元とトンネルの宛先を設定できます。トンネリング機能がイネーブルになっていることを確認します。

### 手順の概要

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**

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## 手順の詳細

|        | コマンド                                                                                                            | 目的                                        |
|--------|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例:<br>switch# configure terminal<br>switch(config)#                            | コンフィギュレーション モードに入ります。                     |
| ステップ 2 | <b>interface tunnel number</b><br><br>例:<br>switch(config)# interface tunnel 1<br>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 | <b>tunnel source</b> {ip-address   interface-name}<br><br>例:<br>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 | <b>tunnel destination</b> {ip-address   host-name}<br><br>例:<br>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 | <b>tunnel use-vrf vrf-name</b><br><br>例:<br>switch(config-if)# tunnel use-vrf blue                              | (任意) 設定された VRF をトンネルの IP 宛先アドレスの検索に使用します。 |
| ステップ 6 | <b>show interfaces tunnel number</b><br><br>例:<br>switch(config-if)# show interfaces tunnel 1                   | (任意) トンネル インターフェイス統計情報を表示します。             |
| ステップ 7 | <b>copy running-config startup-config</b><br><br>例:<br>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関連するすべての設定を削除するには、**no interface tunnel** コマンドを使用します。

| コマンド                                                                                 | 目的                            |
|--------------------------------------------------------------------------------------|-------------------------------|
| <b>no interface tunnel number</b><br><br>例:<br>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。 |

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

次のオプションパラメータを設定して、インターフェイス コンフィギュレーション モードでトンネルを調整することができます。

| コマンド                                                                                        | 目的                                     |
|---------------------------------------------------------------------------------------------|----------------------------------------|
| <b>description</b> <i>string</i><br><br>例：<br><br>switch(config-if)# description GRE tunnel | トンネルの説明を設定します。                         |
| <b>mtu</b> <i>value</i><br><br>例：<br><br>switch(config-if)# mtu 1400                        | インターフェイスで送信される IP パケットの MTU を設定します。    |
| <b>tunnel ttl</b> <i>value</i><br><br>例：<br><br>switch(config-if)# tunnel ttl 100           | トンネルの存続可能時間を設定します。指定できる範囲は 1 ～ 255 です。 |

次に、トンネル インターフェイスを作成する例を示します。

```
switch# configure terminal
switch(config)# interface tunnel 1
switch(config-if)# tunnel source ethernet 1/2
switch(config-if)# tunnel destination 192.0.2.1
switch(config-if)# copy running-config startup-config
```

## GRE トンネルの設定

トンネル インターフェイスを GRE トンネル モードに設定できます。

### はじめる前に

トンネリング機能がイネーブルになっていることを確認します。

### 手順の概要

1. **configure terminal**
2. **interface tunnel** *number*
3. **tunnel mode gre ip**
4. **show interfaces tunnel** *number*
5. **copy running-config startup-config**

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

### 手順の詳細

|        | コマンド                                                                                                         | 目的                                   |
|--------|--------------------------------------------------------------------------------------------------------------|--------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例：<br>switch# configure terminal<br>switch(config)#                         | コンフィギュレーション モードに入ります。                |
| ステップ 2 | <b>interface tunnel number</b><br><br>例：<br>switch(config)# interface tunnel 1<br>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 | <b>tunnel mode gre ip</b><br><br>例：<br>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 | <b>show interfaces tunnel number</b><br><br>例：<br>switch(config-if)# show interfaces tunnel 1                | (任意) トンネル インターフェイス統計情報を表示します。        |
| ステップ 5 | <b>copy running-config startup-config</b><br><br>例：<br>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 インターフェイスを GRE に設定して、GRE トンネル キープアライブを設定する例を示します。

```
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

トンネルでパス MTU ディスカバリをイネーブルにするには、**tunnel path-mtu discovery** コマンドを使用します。

| コマンド                                                                                                                               | 目的                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>tunnel path-mtu-discovery [age-timer min] [min-mtu bytes]</b><br><br>例：<br>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。パラメータは次のとおりです。 <ul style="list-style-type: none"> <li><i>mins</i> : 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。</li> <li><i>mtu-bytes</i> : 認識された最小 MTU。範囲は 92 ~ 65535 です。デフォルト値は 92 です。</li> </ul> |

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## トンネル インターフェイスへの VRF メンバーシップの割り当て

VRF にトンネル インターフェイスを追加できます。

### はじめる前に

トンネリング機能がイネーブルになっていることを確認します。

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

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

### 手順の概要

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 | <code>configure terminal</code><br><br>例:<br>switch# configure terminal<br>switch(config)#                                                  | コンフィギュレーション モードに入ります。                                                 |
| ステップ 2 | <code>interface tunnel number</code><br><br>例:<br>switch(config)# interface tunnel 0<br>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 | <code>vrf member vrf-name</code><br><br>例:<br>switch(config-if)# vrf member<br>RemoteOfficeVRF                                              | このインターフェイスを VRF に追加します。                                               |
| ステップ 4 | <code>ip address ip-prefix/length</code><br><br>例:<br>switch(config-if)# ip address<br>192.0.2.1/16                                         | このインターフェイスの IP アドレスを設定します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。 |
| ステップ 5 | <code>show vrf [vrf-name] interface interface-type number</code><br><br>例:<br>switch(config-vrf)# show vrf Enterprise<br>interface tunnel 0 | (任意) VRF 情報を表示します。                                                    |

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

|        | コマンド                                                                                                                       | 目的                  |
|--------|----------------------------------------------------------------------------------------------------------------------------|---------------------|
| ステップ 6 | <pre>copy running-config startup-config</pre> <p>例：<br/> <pre>switch(config)# copy running-config startup-config</pre></p> | (任意) この設定の変更を保存します。 |

次に、VRF にトンネル インターフェイスを追加する例を示します。

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

## IP トンネル設定の確認

IP トンネルの設定情報を確認するには、次のいずれかの作業を行います。

| コマンド                                                          | 目的                                                                               |
|---------------------------------------------------------------|----------------------------------------------------------------------------------|
| <code>show interface tunnel number</code>                     | トンネル インターフェイスの設定を表示します (MTU、プロトコル、転送、および VRF)。入力および出力パケット、バイト、およびパケット レートを表示します。 |
| <code>show interface tunnel number brief</code>               | 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。                                 |
| <code>show interface tunnel number description</code>         | トンネル インターフェイスに設定された説明を表示します。                                                     |
| <code>show interface tunnel number status</code>              | トンネル インターフェイスの動作ステータスを表示します。                                                     |
| <code>show interface tunnel number status err-disabled</code> | トンネル インターフェイスの errdisable 状態を表示します。                                              |

## IP トンネリングの設定例

次の例では、簡易 GRE トンネルを示します。イーサネット 1/2 は、ルータ A のトンネル送信元であり、ルータ B のトンネル宛先です。イーサネット インターフェイス 2/1 は、ルータ B のトンネル送信元であり、ルータ A のトンネル宛先です。

ルータ A :

```
feature tunnel
interface tunnel 0
 ip address 209.165.20.2/8
 tunnel source ethernet 1/2
 tunnel destination 192.0.2.2
 tunnel mode gre ip
 tunnel path-mtu-discovery 25 1500
interface Ethernet1/2
 ip address 192.0.2.55/8
```

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

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
```

## 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.8-12)
- 「標準」(P.8-12)

## 関連資料

| 関連項目                                | マニュアル タイトル                                                                |
|-------------------------------------|---------------------------------------------------------------------------|
| 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

| 標準                                                         | タイトル |
|------------------------------------------------------------|------|
| この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。 | —    |

## IP トンネル設定の機能履歴

表 8-2 に、この機能のリリース履歴を示します。

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                                                    |
|-----------------------------------------------|--------|---------------------------------------------------------|
| M1 シリーズ I/O モジュールのみに関する異なる VRF 内のトンネルと転送のサポート | 5.2(5) | この機能拡張は、NX-OS Release 5.2(5) と 5.2(x) リリース以降でサポートされました。 |
| デフォルト以外の VDC および VRF 内の IP トンネル               | 4.2(1) | この機能が導入されました。                                           |
| IP トンネル                                       | 4.0(1) | この機能が導入されました。                                           |

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

# 第 9 章

## Q-in-Q VLAN トンネルの設定

この章では、Cisco NX-OS デバイス上で IEEE 802.1Q-in-Q (Q-in-Q) VLAN トンネルおよびレイヤ 2 プロトコルのトンネリングを設定する方法について説明します。

この章は、次の項で構成されています。

- 「Q-in-Q トンネルについて」 (P.9-1)
- 「レイヤ 2 プロトコルのトンネリングについて」 (P.9-5)
- 「Q-in-Q トンネルのライセンス要件」 (P.9-7)
- 「注意事項と制約事項」 (P.9-7)
- 「Q-in-Q トンネルおよびレイヤ 2 プロトコルのトンネリングの設定」 (P.9-8)
- 「Q-in-Q 設定の確認」 (P.9-16)
- 「Q-in-Q およびレイヤ 2 プロトコルのトンネリングの設定例」 (P.9-16)
- 「Q-in-Q トンネルおよびレイヤ 2 プロトコルのトンネリングの機能履歴」 (P.9-17)

### Q-in-Q トンネルについて

Q-in-Q VLAN トンネルを使用することで、サービスプロバイダーは第 2 の 802.1Q タグをすでにタグ付けされたフレームに追加して、カスタマーに内部使用の VLAN をすべて提供しながら、インフラストラクチャ内で異なるカスタマーのトラフィックを分離することができます。

この項では、次のトピックについて取り上げます。

- 「Q-in-Q トンネリング」 (P.9-1)
- 「ネイティブ VLAN のリスク」 (P.9-3)

### Q-in-Q トンネリング

サービスプロバイダーのビジネス カスタマーには、多くの場合、サポートする VLAN ID および VLAN の数に固有の要件があります。同一サービスプロバイダー ネットワークのさまざまなカスタマーが必要とする VLAN 範囲は重複し、インフラストラクチャを通るカスタマーのトラフィックは混合してしまうことがあります。カスタマーごとに一意の VLAN ID 範囲を割り当てると、カスタマーの設定が制限され、802.1Q 仕様の 4096 の VLAN に関する上限を容易に超えてしまいます。

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。



(注) Q-in-Q は、ポート チャンネルと vPC でサポートされています。非対称リンクとしてポート チャンネルを設定するには、ポート チャンネル内のすべてのポートが同じトンネリング設定でなければなりません。

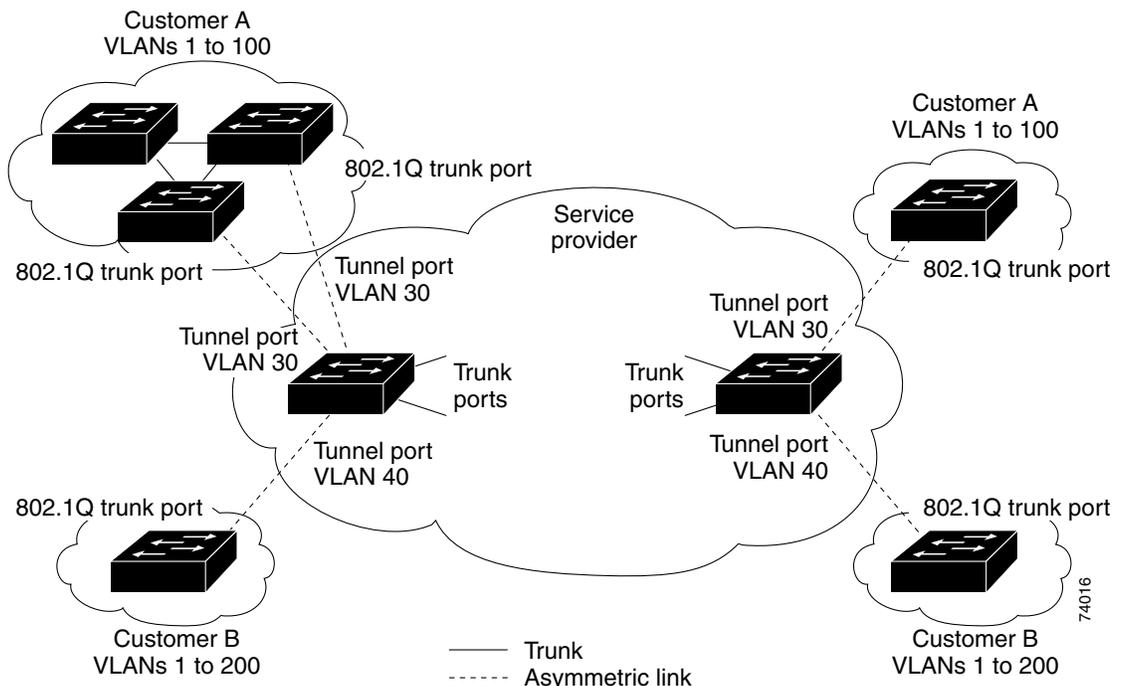
サービスプロバイダーは、802.1Q トンネリング機能を使用すると、単一の VLAN を使用して、複数の VLAN を含む顧客をサポートできます。同一の VLAN 上にあるように見えるときでも、サービスプロバイダー インフラストラクチャ内の顧客の VLAN ID を保護したり、異なる顧客の VLAN トラフィックを分離しておくことができます。IEEE 802.1Q トンネリングは、VLAN-in-VLAN 階層構造およびタグ付きパケットへのタグgingによって、VLAN スペースを拡張します。802.1Q トンネリングをサポートするように設定したポートは、トンネルポートと呼ばれます。トンネリングを設定する場合、トンネリング専用の VLAN にトンネルポートを割り当てます。顧客ごとに個別の VLAN が必要ですが、その VLAN は顧客の VLAN をすべてサポートします。

適切な VLAN ID で通常どおりにタグ付けされた顧客のトラフィックは、顧客デバイス の 802.1Q トランクポートからサービスプロバイダー側のエッジスイッチのトンネルポートに発信されます。顧客デバイスとエッジスイッチの間のリンクは、一方の端が 802.1Q トランクポート、反対側がトンネルポートとして設定されているので、非対称リンクです。顧客ごとに一意のアクセス 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。トンネルポートに着信するすべてのフレームは、Q-in-Q タグging の対象となります。

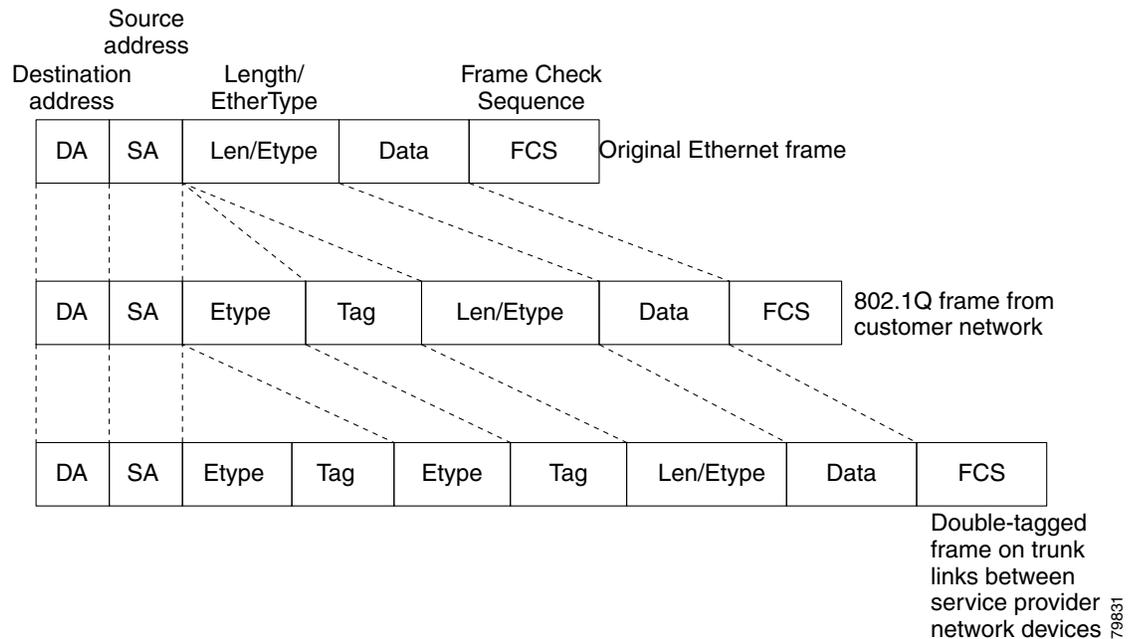
図 9-1 802.1Q-in-Q トンネルポート



マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

サービスプロバイダー エッジ スイッチのトンネル ポートに着信するパケット（適切な VLAN ID すでに 802.1Q タグ付けされている）は、カスタマーに一意である VLAN ID を含む 802.1Q タグの別のレイヤでカプセル化されます。元々のカスタマーの 802.1Q タグは、カプセル化されたパケットの中に維持されます。したがって、サービスプロバイダー インフラストラクチャに着信するパケットは二重にタグ付けされます。外部タグには、カスタマーの（サービスプロバイダーによって割り当てられた）アクセス VLAN ID が含まれます。内部 VLAN ID は、（カスタマーによって割り当てられた）受信トラフィックの VLAN です。この二重タギングは、図 9-2 に示すようにタグ スタック構成 Double-Q または Q-in-Q と呼ばれます。

図 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



この方法で、外部タグの VLAN ID スペースは内部タグの VLAN ID スペースに依存しません。単一の外部 VLAN ID は、個々のカスタマーの全体の VLAN ID スペースを表すことができます。この方法により、カスタマーのレイヤ 2 ネットワークをサービスプロバイダー ネットワーク全体に拡張して、複数のサイトに仮想 LAN インフラストラクチャを作成することも可能になります。



(注) 階層型タギング、すなわちマルチレベルの dot1q タギング Q-in-Q はサポートされていません。

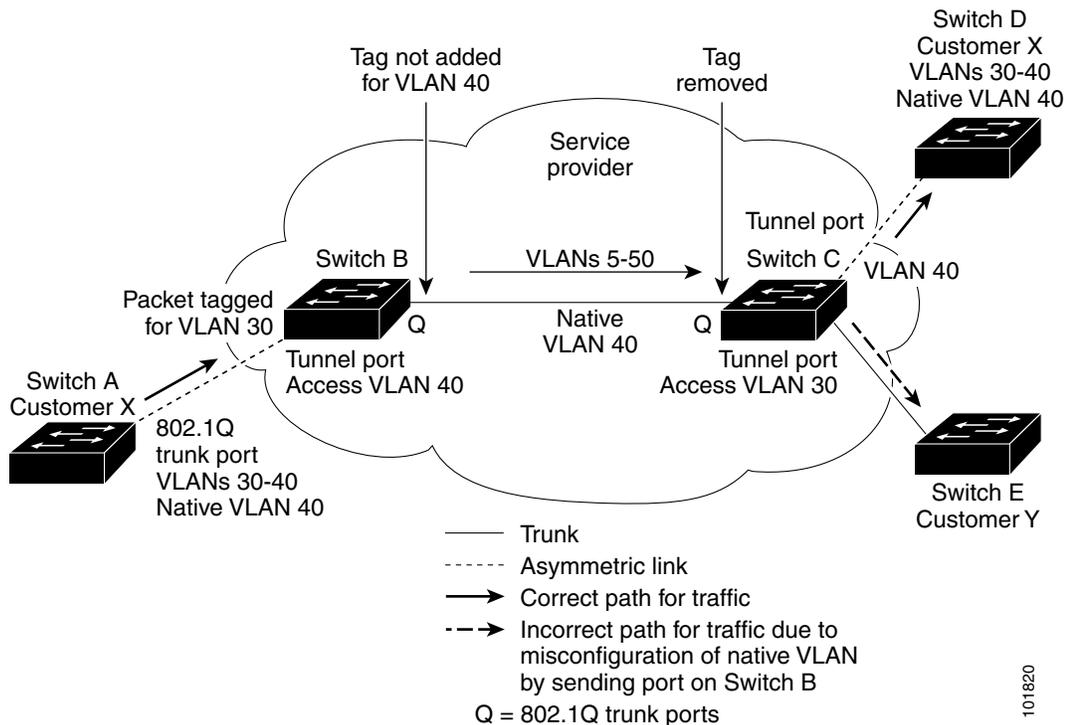
## ネイティブ VLAN のリスク

エッジ スイッチで 802.1Q トンネリングを設定する場合は、サービスプロバイダー ネットワークにパケットを送信するために、802.1Q トランク ポートを使用する必要があります。ただし、サービスプロバイダー ネットワークのコアを通過するパケットは、802.1Q トランク、ISL トランク、または非ランキング リンクで伝送される場合があります。802.1Q トランクをこれらのコア スイッチで使用する場合には、802.1Q トランクのネイティブ VLAN を、同じスイッチ上の dot1q トンネル ポートのどのネイティブ VLAN にも一致させないでください。ネイティブ VLAN 上のトラフィックが 802.1Q 送信トランク ポートでタグ付けされなくなるためです。

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

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）において、カスタマー X からの 802.1Q トランク ポートのネイティブ VLAN として設定されています。カスタマー X のスイッチ A は、VLAN 30 のタグ付きパケットを、アクセス VLAN 40 に属する、サービスプロバイダー ネットワークのスイッチ B の入力トンネルポートに送信します。トンネルポートのアクセス VLAN（VLAN 40）は、エッジスイッチのトランクポートのネイティブ VLAN（VLAN 40）と同じなので、トンネルポートから受信したタグ付きパケットに 802.1Q タグは追加されません。パケットには VLAN 30 タグだけが付いて、サービスプロバイダー ネットワークで出力エッジ スイッチ（スイッチ C）のトランクポートに送信され、出力スイッチ トンネルによってカスタマー Y に間違えて送信されます。

図 9-3 ネイティブ VLAN のリスク



ネイティブ VLAN の問題を解決する方法は 2 つあります。

- 802.1Q トランクから出るすべてのパケット（ネイティブ VLAN を含む）が、**vlan dot1q tag native** コマンドを使用してタグ付けされるように、エッジ スイッチを設定します。すべての 802.1Q トランクでネイティブ VLAN パケットにタグを付けるようにスイッチを設定した場合、スイッチはタグなしパケットを受信しますが、タグ付きパケットだけを送信します。



(注) **vlan dot1q tag native** コマンドは、すべてのトランク ポート上のタギング動作に影響を与えるグローバル コマンドです。

- エッジ スイッチのトランク ポートのネイティブ VLAN ID が、カスタマー VLAN 範囲に属さないようにします。たとえばトランク ポートが VLAN100 ~ 200 のトラフィックを運ぶ場合は、この範囲以外の番号をネイティブ VLAN に割り当てます。

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## レイヤ2プロトコルのトンネリングについて

サービスプロバイダー ネットワーク経由で接続される複数のサイトの顧客は、さまざまなレイヤ2プロトコルを実行して、すべてのリモート サイトおよびローカル サイトを含むようにトポロジを拡大する必要があります。スパンニングツリープロトコル (STP) が適切に稼働している必要があります。すべての VLAN で、ローカル サイトおよびサービスプロバイダー インフラストラクチャ経由のすべてのリモート サイトを含む、適切なスパンニング ツリーを構築する必要があります。Cisco Discovery Protocol (CDP) は、ローカルおよびリモート サイトから隣接するシスコ デバイスを検出することができる必要があります。VLAN トランッキングプロトコル (VTP) は、顧客 ネットワークのすべてのサイトを通して一貫した VLAN 設定を提供する必要があります。

プロトコル トンネリングがイネーブルになると、サービスプロバイダー インフラストラクチャの受信側にあるエッジスイッチが、レイヤ2プロトコルを特別な MAC アドレスでカプセル化し、サービスプロバイダー ネットワークの端まで送信します。ネットワークのコアスイッチでは、このパケットが処理されずに通常のパケットとして転送されます。CDP、STP、または VTP のブリッジプロトコルデータユニット (BPDU) は、サービスプロバイダー インフラストラクチャを通過し、サービスプロバイダー ネットワークの発信側にある顧客スイッチまで配信されます。同一パケットは同じ VLAN のすべての顧客 ポートで受信されます。

802.1Q トンネリング ポートでプロトコルのトンネリングをイネーブルにしていない場合、サービスプロバイダー ネットワークの受信側のリモート スイッチでは BPDU を受信せず、STP、CDP、802.1X、および VTP を適切に実行できません。プロトコルのトンネリングがイネーブルである場合、それぞれの顧客 ネットワークのレイヤ2プロトコルは、サービスプロバイダー ネットワーク内で動作しているものから完全に区別されます。802.1Q トンネリングでサービスプロバイダー ネットワークを通してトラフィックを送信する、さまざまなサイトの顧客 スイッチでは、顧客 VLAN が完全に認識されます。



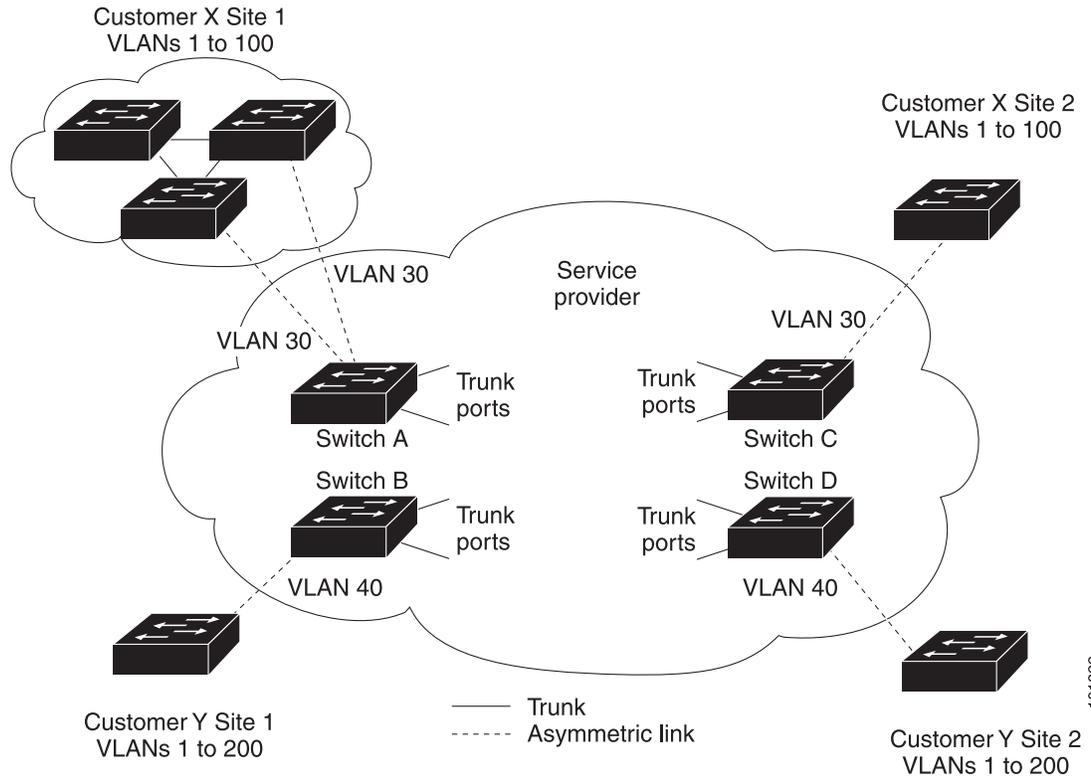
(注)

レイヤ2プロトコルのトンネリングは、ソフトウェアで BPDU をトンネリングすることで動作します。SUP が受信する多数の BPDU により CPU の負荷が大きくなります。SUP CPU の負荷を軽減するために、ハードウェア レート リミッタを使用する必要がある場合があります。「[レイヤ2プロトコルトンネルポートのレート制限の設定](#)」(P.9-13) を参照してください。

たとえば図 9-4 の場合、顧客 X には、サービスプロバイダー ネットワーク経由で接続された同じ VLAN 上のスイッチが 4 つあります。ネットワークが BPDU をトンネリングしないと、ネットワークの遠端のスイッチは STP、CDP、802.1X、および VTP プロトコルを正しく実行できません。

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

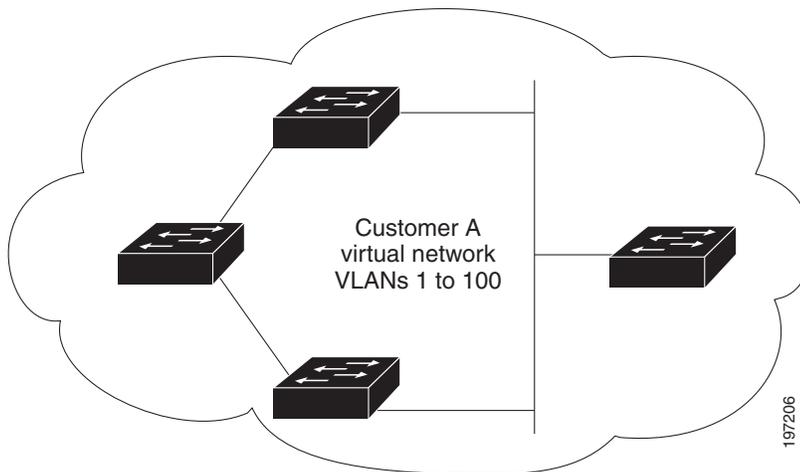
図 9-4 レイヤ2 プロトコル トンネリング



前の例では、カスタマー X、サイト 1 のスイッチ上の VLAN で動作する STP は、カスタマー X、サイト 2 のスイッチに基づくコンバージェンス パラメータを考慮せずに、このサイトのスイッチのスパニング ツリーを構築します。

図 9-5 では、BPDU トンネリングがイネーブルになっていない場合にカスタマーのネットワークで生じるトポロジを示します。

図 9-5 BPDU トンネリングを使用しない仮想ネットワーク トポロジ



マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## 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 プロトコルの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 スキームの詳細は、『Cisco NX-OS Licensing Guide』を参照してください。 |

## 注意事項と制約事項

Q-in-Q トンネリングおよびレイヤ 2 トンネリングには、次の設定に関する注意事項と制約事項があります。

- サービスプロバイダー ネットワーク内のスイッチは、Q-in-Q タギングによる MTU サイズの増加に対応するように設定する必要があります。
- Q-in-Q タグ付きパケットの MAC アドレス ラーニングは、外部 VLAN (サービスプロバイダー VLAN) タグに基づいています。単一の MAC アドレスが複数の内部 (カスタマー) VLAN で使用される配置においては、パケット転送の問題が発生する場合があります。
- レイヤ 3 以上のパラメータは、トンネルトラフィックでは識別できません (レイヤ 3 宛先や送信元アドレスなど)。トンネル型トラフィックはルーティングできません。
- Cisco Nexus 7000 シリーズのデバイスは、トンネルトラフィックに対する MAC レイヤ ACL/QoS (VLAN ID および送信元/宛先 MAC アドレス) のみを提供できます。
- MAC アドレスに基づくフレーム配布を使用する必要があります。
- 非対称リンクでは 1 つのポートだけがトラッキングするため、Dynamic Trunking Protocol (DTP) をサポートしません。無条件でトランクになるように、非対称リンクの 802.1Q トランク ポートを設定する必要があります。
- プライベート VLAN をサポートするように設定されたポートに 802.1Q トンネリング機能を設定することはできません。プライベート VLAN は、これらの導入には必要ではありません。
- トンネル VLAN の IGMP スヌーピングをディセーブルにする必要があります。
- コントロールプレーン ポリシング (CoPP) はサポートされません。
- ネイティブ VLAN でのタギングを維持し、タグなしトラフィックを廃棄するには、**vlan dot1Q tag native** コマンドを実行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。
- 802.1Q インターフェイスをエッジ ポートにするように手動で設定する必要があります。
- Dot1x トンネリングはサポートされていません。
- EtherType 設定が複数の Cisco Nexus デバイスで有効になるように、EPLD を新しいバージョンにアップグレードする必要があります。

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## Q-in-Q トンネルおよびレイヤ2プロトコルのトンネリングの設定

このセクションでは、Cisco Nexus 7000 シリーズ デバイスで Q-in-Q トンネルとレイヤ 2 プロトコルのトンネリングを設定する方法について説明します。

この項では、次のトピックについて取り上げます。

- 「802.1Q トンネル ポートの作成」 (P.9-8)
- 「Q-in-Q 用の EtherType の変更」 (P.9-10)
- 「レイヤ 2 プロトコル トンネルのイネーブル化」 (P.9-11)
- 「L2 プロトコル トンネル ポートに対するグローバル CoS の設定」 (P.9-12)
- 「レイヤ 2 プロトコル トンネル ポートのレート制限の設定」 (P.9-13)
- 「レイヤ 2 プロトコル トンネル ポートのしきい値の設定」 (P.9-14)



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

### 802.1Q トンネル ポートの作成

`switchport mode` コマンドを使用して `dot1q-tunnel` ポートを作成します。



(注) `spanning-tree port type edge` コマンドを使用して、エッジポートに 802.1Q トンネル ポートを設定する必要があります。ポートの VLAN メンバーシップは、`switchport access vlan vlan-id` コマンドを使用して変更されます。

`dot1q-tunnel` ポートに割り当てられたアクセス VLAN の IGMP スヌーピングをディセーブルにして、マルチキャスト パケットが Q-in-Q トンネルを通過できるようにする必要があります。

#### はじめる前に

はじめに、スイッチポートとしてインターフェイスを設定する必要があります。

#### 手順の概要

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`

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

### 手順の詳細

|        | コマンド                                                                                              | 目的                                                                                                                            |
|--------|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例：<br>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 | <b>interface ethernet slot/port</b><br><br>例：<br>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 | <b>switchport</b><br><br>例：<br>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 | <b>switchport mode dot1q-tunnel</b><br><br>例：<br>switch(config-if)# switchport mode dot1q-tunnel  | ポートに 802.1Q トンネルを作成します。インターフェイス モードを変更すると、ポートはダウンし、再初期化（ポート フラップ）されます。トンネル インターフェイスでは BPDU フィルタリングがイネーブルになり、CDP がディセーブルになります。 |
| ステップ 5 | <b>no switchport mode</b><br><br>例：<br>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 | <b>exit</b><br><br>例：<br>switch(config-if)# exit<br>switch(config)# exit                          | 設定モードを終了します。                                                                                                                  |
| ステップ 7 | <b>show dot1q-tunnel [interface if-range]</b><br><br>例：<br>switch# show dot1q-tunnel              | (任意) dot1q-tunnel モードにあるすべてのポートを表示します。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 | <b>copy running-config startup-config</b><br><br>例：<br>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
```

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## Q-in-Q 用の EtherType の変更

Q-in-Q カプセル化に使用するように 802.1Q EtherType 値を変更できます。



(注)

二重タグ フレームを伝送する出力トランク インターフェイス（サービス プロバイダーに接続するトランク インターフェイス）だけに EtherType を設定する必要があります。トランクの一方で EtherType を変更した場合、トランクのもう一方でも同じ値を設定する必要があります（対称構成）。



注意

設定した EtherType 値は、(Q-in-Q パケットだけではなく) インターフェイスから出るすべてのタグ付きパケットに影響します。

### 手順の概要

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 | <code>configure terminal</code><br><br>例:<br><code>switch# configure terminal</code>                                         | グローバル コンフィギュレーション モードを開始します。                     |
| ステップ 2 | <code>interface ethernet slot/port</code><br><br>例:<br><code>switch(config)# interface ethernet 7/1</code>                   | 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 | <code>switchport</code><br><br>例:<br><code>switch(config-if)# switchport</code>                                              | 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 | <code>switchport dot1q ethertype value</code><br><br>例:<br><code>switch(config-if)# switchport dot1q ethertype 0x9100</code> | ポート上の Q-in-Q トンネル用に EtherType を設定します。            |
| ステップ 5 | <code>no switchport dot1q ethertype</code><br><br>例:<br><code>switch(config-if)# no switchport dot1q ethertype</code>        | (任意) ポートの EtherType を 0x8100 のデフォルト値にリセットします。    |

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

|        | コマンド                                                                                              | 目的                                             |
|--------|---------------------------------------------------------------------------------------------------|------------------------------------------------|
| ステップ 6 | <b>exit</b><br><br>例：<br>switch(config-if)# exit<br>switch(config)# exit                          | 設定モードを終了します。                                   |
| ステップ 7 | <b>copy running-config startup-config</b><br><br>例：<br>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の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 | <b>configure terminal</b><br><br>例：<br>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 | <b>interface ethernet slot/port</b><br><br>例：<br>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。 |

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

|        | コマンド                                                                                               | 目的                                                                     |
|--------|----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| ステップ 3 | <b>switchport</b><br><br>例:<br>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 | <b>switchport mode dot1q-tunnel</b><br><br>例:<br>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 | <b>l2protocol tunnel [cdp   stp   vtp]</b><br><br>例:<br>switch(config-if)# l2protocol tunnel stp   | レイヤ 2 プロトコルのトンネリングをイネーブルにします。必要に応じて、CDP、STP、または VTP トンネリングをイネーブルにできます。 |
| ステップ 6 | <b>no l2protocol tunnel [cdp   stp   vtp]</b><br><br>例:<br>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 | <b>exit</b><br><br>例:<br>switch(config-if)# exit<br>switch(config)# exit                           | 設定モードを終了します。                                                           |
| ステップ 8 | <b>copy running-config startup-config</b><br><br>例:<br>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のトンネリングをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 7/1
switch(config-if)# switchport
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# l2protocol tunnel stp
switch(config-if)# exit
switch(config)# exit
```

## L2 プロトコルトンネルポートに対するグローバル CoS の設定

トンネルポートの入力 BPDU が指定されたクラスでカプセル化されるように、サービス クラス (CoS) の値をグローバルに指定できます。

### 手順の概要

1. **configure terminal**
2. **l2protocol tunnel cos value**
3. **no l2protocol tunnel cos**
4. **exit**
5. **copy running-config startup-config**

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

### 手順の詳細

|        | コマンド                                                                                              | 目的                                                             |
|--------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例:<br>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 | <b>l2protocol tunnel cos cos-value</b><br><br>例:<br>switch(config)# l2protocol tunnel cos 6       | すべてのレイヤ 2 プロトコルのトンネリングポートでグローバル CoS 値を指定します。デフォルト CoS 値は 5 です。 |
| ステップ 3 | <b>no l2protocol tunnel cos</b><br><br>例:<br>switch(config)# no l2protocol tunnel cos             | (任意) グローバル CoS 値をデフォルト値に設定します。                                 |
| ステップ 4 | <b>exit</b><br><br>例:<br>switch(config)# exit                                                     | 設定モードを終了します。                                                   |
| ステップ 5 | <b>copy running-config startup-config</b><br><br>例:<br>switch# copy running-config startup-config | (任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。                 |

次に、レイヤ 2 プロトコルのトンネリングのためのグローバル CoS 値を指定する例を示します。

```
switch# configure terminal
switch(config)# l2protocol tunnel cos 6
switch(config)# exit
```

## レイヤ 2 プロトコル トンネル ポートのレート制限の設定

レイヤ 2 プロトコルのトンネリング用にハードウェア レート リミッタの設定を指定できます。デフォルトは 500 パケット/秒に設定されます。ロードまたはカスタマーにトンネリングされる VLAN 数によって、カスタマーのネットワーク上の STP のエラーを回避するためにこの値を調整する必要がある場合があります。

### 手順の概要

1. **configure terminal**
2. **hardware rate-limiter layer-2 l2pt packets-per-sec**
3. **no hardware rate-limiter layer-2 l2pt**

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

### 手順の詳細

|        | コマンド                                                                                                                                     | 目的                                                                                           |
|--------|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例:<br>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 | <b>hardware rate-limiter layer-2 l2pt<br/>packets-per-second</b><br><br>例:<br>switch(config)# hardware rate-limiter<br>layer-2 l2pt 4096 | dot1q-tunnel ポートからの着信プロトコルパケットがハードウェアにドロップされる 1 秒あたりのパケット数のしきい値を設定します。有効な値の範囲は 0 ~ 30000 です。 |
| ステップ 3 | <b>no hardware rate-limiter layer-2 l2pt</b><br><br>例:<br>switch(config)# no hardware rate-limiter<br>layer-2 l2pt                       | (任意) しきい値をデフォルトの毎秒 500 パケットにリセットします。                                                         |

## レイヤ2プロトコルトンネルポートのしきい値の設定

レイヤ2プロトコルのトンネリング ポートに対するポートドロップおよびシャットダウン値を指定できます。

### 手順の概要

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**

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

### 手順の詳細

|         | コマンド                                                                                                                                                 | 目的                                                                                                                           |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1  | <b>configure terminal</b><br><br>例：<br>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  | <b>interface ethernet slot/port</b><br><br>例：<br>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  | <b>switchport</b><br><br>例：<br>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  | <b>switchport mode dot1q-tunnel</b><br><br>例：<br>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  | <b>l2protocol tunnel drop-threshold [cdp   stp   vtp] packets-per-sec</b><br><br>例：<br>switch(config)# l2protocol tunnel drop-threshold 3000         | 廃棄される前にインターフェイスで処理できる最大パケット数を指定します。必要に応じて、CDP、STP、または VTP を指定できます。パケットの有効な値は 1 ~ 4096 です。                                    |
| ステップ 6  | <b>no l2protocol tunnel drop-threshold [cdp   stp   vtp]</b><br><br>例：<br>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  | <b>l2protocol tunnel shutdown-threshold [cdp   stp   vtp] packets-per-sec</b><br><br>例：<br>switch(config)# l2protocol tunnel shutdown-threshold 3000 | インターフェイスで処理できる最大パケット数を指定します。パケット数が超過すると、ポートは error-disabled ステートになります。必要に応じて、CDP、STP、または VTP を指定できます。パケットの有効な値は 1 ~ 4096 です。 |
| ステップ 8  | <b>no l2protocol tunnel shutdown-threshold [cdp   stp   vtp]</b><br><br>例：<br>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  | <b>exit</b><br><br>例：<br>switch(config)# exit                                                                                                        | 設定モードを終了します。                                                                                                                 |
| ステップ 10 | <b>copy running-config startup-config</b><br><br>例：<br>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。                                                                                |

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## Q-in-Q 設定の確認

Q-in-Q トンネルおよびレイヤ 2 プロトコルのトンネリング設定情報を表示するには、次のタスクのいずれかを実行します。

| コマンド                                                                    | 目的                                                                                                |
|-------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| <code>clear l2protocol tunnel counters [interface if-range]</code>      | すべての統計情報カウンタをクリアします。インターフェイスが指定されていない場合、すべてのインターフェイスのレイヤ 2 プロトコル トンネル統計情報がクリアされます。                |
| <code>show dot1q-tunnel [interface if-range]</code>                     | 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。                                                  |
| <code>show l2protocol tunnel [interface if-range   vlan vlan-id]</code> | 一定範囲のインターフェイス（特定の VLAN の一部であるすべての dot1q-tunnel インターフェイスまたはすべてのインターフェイス）のレイヤ 2 プロトコル トンネル情報を表示します。 |
| <code>show l2protocol tunnel summary</code>                             | レイヤ 2 プロトコル トンネルが設定されているすべてのポートのサマリーを表示します。                                                       |
| <code>show running-config l2pt</code>                                   | 現在のレイヤ 2 プロトコル トンネルの実行コンフィギュレーションを表示します。                                                          |

## Q-in-Q およびレイヤ 2 プロトコルのトンネリングの設定例

次に、イーサネット 7/1 に着信するトラフィックに対し Q-in-Q を処理するよう設定されたサービスプロバイダーのスイッチを示します。レイヤ 2 プロトコル トンネルが STP BPDU に対してイネーブルにされます。このカスタマーは VLAN 10（外部 VLAN タグ）に割り当てられます。

```
switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
switch(config)# vlan 10
switch(config-vlan)# no shutdown
switch(config-vlan)# no ip igmp snooping
switch(config-vlan)# exit
switch(config)# interface ethernet 7/1
switch(config-if)# switchport
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# switchport access vlan 10
switch(config-if)# spanning-tree port type edge
switch(config-if)# l2protocol tunnel stp
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# exit
switch#
```

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

## Q-in-Q トンネルおよびレイヤ2プロトコルのトンネリングの機能履歴

表 9-1 に、この機能のリリース履歴を示します。

表 9-1 Q-in-Q トンネルおよびレイヤ2 プロトコルのトンネリングの機能履歴

| 機能名              | リリース   | 機能情報          |
|------------------|--------|---------------|
| Q-in-Q VLAN トンネル | 5.0(2) | この機能が導入されました。 |
| L2 プロトコルのトンネリング  | 5.0(2) | この機能が導入されました。 |

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

付録

**A**

## Cisco NX-OS インターフェイスがサポートする IETF RFC

この付録では、Cisco NX-OS インターフェイス Nexus 7000 シリーズ NX-OS リリース5.xでサポートされているインターフェイスの IETF RFC をリスト表示します。

### IPv6 の RFC

| RFC      | タイトル                                                                                                  |
|----------|-------------------------------------------------------------------------------------------------------|
| RFC 1981 | 『Path MTU Discovery for IP version 6』                                                                 |
| RFC 2373 | 『IP Version 6 Addressing Architecture』                                                                |
| RFC 2374 | 『An Aggregatable Global Unicast Address Format』                                                       |
| RFC 2460 | 『Internet Protocol, Version 6 (IPv6) Specification』                                                   |
| RFC 2461 | 『Neighbor Discovery for IP Version 6 (IPv6)』                                                          |
| RFC 2462 | 『IPv6 Stateless Address Autoconfiguration』                                                            |
| RFC 2463 | 『Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification』 |
| RFC 2464 | 『Transmission of IPv6 Packets over Ethernet Networks』                                                 |
| RFC 2467 | 『Transmission of IPv6 Packets over FDDI Networks』                                                     |
| RFC 2472 | 『IP Version 6 over PPP』                                                                               |
| RFC 2492 | 『IPv6 over ATM Networks』                                                                              |
| RFC 2590 | 『Transmission of IPv6 Packets over Frame Relay Networks Specification』                                |
| FCS 3021 | 『Using 31-Bit Prefixes on IPv4 Point-to-Point Links』                                                  |
| RFC 3152 | 『Delegation of IP6.ARPA』                                                                              |
| RFC 3162 | 『RADIUS and IPv6』                                                                                     |
| RFC 3513 | 『Internet Protocol Version 6 (IPv6) Addressing Architecture』                                          |
| RFC 3596 | 『DNS Extensions to Support IP version 6』                                                              |
| RFC 4193 | 『Unique Local IPv6 Unicast Addresses』                                                                 |

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。

付録

**B**

## Cisco NX-OS インターフェイスの設定制限

---

設定の制限は、『Cisco Nexus 7000 Series NX-OS Verified Scalability Guide』に記載されています。

マニュアルに関するご意見は [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com) まで電子メールでお知らせください。