



## **Cisco Nexus 3000 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 5.0(3)U3(1)**

初版：2012 年 02 月 29 日

最終更新：2012 年 02 月 29 日

### **シスコシステムズ合同会社**

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

**【注意】** シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。



## 目次

### はじめに vii

対象読者 vii

表記法 vii

Nexus 3000 シリーズ NX-OS ソフトウェアの関連資料 ix

マニュアルの入手方法およびテクニカル サポート x

### このリリースの新規および変更情報 1

このリリースの新規および変更情報 1

### レイヤ3 インターフェイスの設定 3

レイヤ3 インターフェイスについて 3

ルーテッド インターフェイス 4

サブインターフェイス 4

VLAN インターフェイス 5

ループバック インターフェイス 6

トンネル インターフェイス 6

レイヤ3 インターフェイスのライセンス要件 6

レイヤ3 インターフェイスの注意事項および制約事項 7

レイヤ3 インターフェイスのデフォルト設定 7

レイヤ3 インターフェイスの設定 7

ルーテッド インターフェイスの設定 7

サブインターフェイスの設定 8

インターフェイスでの帯域幅の設定 9

VLAN インターフェイスの設定 10

Nexus シャーシでのインバンド管理の設定 11

ループバック インターフェイスの設定 12

VRF へのインターフェイスの割り当て 13

レイヤ3 インターフェイス設定の確認 14

レイヤ 3 インターフェイスのモニタリング	15
レイヤ 3 インターフェイスの設定例	17
レイヤ 3 インターフェイスの関連資料	17
レイヤ 3 インターフェイスの MIB	18
レイヤ 3 インターフェイスの標準	18
レイヤ 3 インターフェイスの機能履歴	18
<b>ポート チャネルの設定</b>	<b>19</b>
ポート チャネルについて	19
ポート チャネルの概要	20
互換性要件	21
ポート チャネルを使ったロード バランシング	22
LACP の概要	24
LACP の概要	24
LACP ID パラメータ	25
チャンネル モード	26
LACP マーカー レスポンダ	27
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	27
LACP ポート チャネルの MinLink	28
ポート チャネルの設定	28
ポート チャネルの作成	28
ポート チャネルへのポートの追加	29
ポート チャネルを使ったロード バランシングの設定	30
マルチキャスト トラフィックのハードウェア ハッシュの設定	31
LACP のイネーブル化	31
ポートのチャンネル モードの設定	32
LACP ポート チャネルの MinLink の設定	34
LACP 高速タイマー レートの設定	35
LACP のシステム プライオリティおよびシステム ID の設定	35
LACP ポート プライオリティの設定	36
ポート チャネルの設定の確認	37
ロードバランシングの発信ポート ID の確認	38

ポートチャネルの機能履歴	39
仮想ポートチャネルの設定	41
vPCについて	41
vPCの概要	41
用語	42
vPCの用語	42
サポートされているvPCトポロジ	43
Cisco Nexus 3000 シリーズ スイッチ vPC トポロジ	43
vPC ドメイン	44
ピアキープアライブリンクとメッセージ	44
vPC ピアリンクの互換パラメータ	45
同じでなければならない設定パラメータ	45
同じにすべき設定パラメータ	47
グレースフルタイプ1チェック	47
VLAN ごとの整合性検査	48
vPC 自動リカバリ	48
vPC ピアリンク	48
vPC ピアリンクの概要	48
vPC 番号	50
その他の機能とのvPCの相互作用	50
vPC と LACP	50
vPC ピアリンクと STP	50
CFSOE	51
vPC の注意事項および制約事項	52
vPC の設定	52
vPC のイネーブル化	52
vPC のディセーブル化	53
vPC ドメインの作成	54
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	55
vPC ピアリンクの作成	57
設定の互換性チェック	58
vPC 自動リカバリのイネーブル化	59

復元遅延時間の設定	60
vPC ピア リンク障害時のシャットダウンからの VLAN インターフェイスの除外	61
VRF 名の設定	61
vPC への VRF インスタンスのバインド	62
他のポート チャネルの vPC への移行	63
vPC ドメイン MAC アドレスの手動での設定	64
システム プライオリティの手動での設定	64
vPC ピア スイッチ ロールの手動での設定	65
vPC 設定の確認	66
グレースフル タイプ 1 チェック ステータスの表示	67
グローバル タイプ 1 不整合の表示	68
インターフェイス固有のタイプ 1 不整合の表示	69
VLAN ごとの整合ステータスの表示	70
vPC のデフォルト設定	72



## はじめに

ここでは、次の項目について説明します。

- [対象読者](#), [vii ページ](#)
- [表記法](#), [vii ページ](#)
- [Nexus 3000 シリーズ NX-OS ソフトウェアの関連資料](#), [ix ページ](#)
- [マニュアルの入手方法およびテクニカル サポート](#), [x ページ](#)

## 対象読者

この出版物は Cisco Nexus シリーズ デバイスの設定と保守を行う経験豊富なネットワーク管理者を対象としています。

## 表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
<b>bold</b>	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
<i>Italic</i>	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	角カッコで囲まれているものは、省略可能な要素（キーワードまたは引数）です。
[x   y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。

表記法	説明
{x y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波カッコで囲み、縦棒で区切って示しています。
[x {y z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
variable	ユーザが値を入力する変数であることを表します。イタリック体を使用できない場合に使用されます。
string	引用符を付けない一組の文字。stringの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてstringとみなされます。

例では、次の表記法を使用しています。

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

このマニュアルでは、次の表記法を使用しています。



(注) 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

**注意**

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

## Nexus 3000 シリーズ NX-OS ソフトウェアの関連資料

完全な Cisco NX-OS 3000 シリーズ マニュアル セットは、次の URL で入手できます。

[http://www.cisco.com/en/US/products/ps11541/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html)

### リリースノート

リリース ノートは、次の URL で入手できます。

[http://www.cisco.com/en/US/products/ps11541/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps11541/prod_release_notes_list.html)

### インストールガイドおよびアップグレードガイド

インストールおよびアップグレード ガイドは次の URL で入手できます。

[http://www.cisco.com/en/US/products/ps11541/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps11541/prod_installation_guides_list.html)

このカテゴリのマニュアルは次のとおりです。

- 『Cisco Nexus 5000 Series, Cisco Nexus 3000 Series, and Cisco Nexus 2000 Series Safety Information and Documentation』
- 『Regulatory, Compliance, and Safety Information for the Cisco Nexus 5000 Series, Cisco Nexus 3000 Series, and Cisco Nexus 2000 Series』
- 『Cisco Nexus 3000 Series Hardware Installation Guide』

### コンフィギュレーションガイド

コンフィギュレーション ガイドは次の URL で入手できます。

[http://www.cisco.com/en/US/products/ps11541/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps11541/products_installation_and_configuration_guides_list.html)

このカテゴリのマニュアルは次のとおりです。

- 『Fundamentals Configuration Guide』
- 『Interfaces Configuration Guide』
- 『Layer 2 Switching Configuration Guide』
- 『Multicast Configuration Guide』
- 『Quality of Service Configuration Guide』
- 『Security Configuration Guide』
- 『System Management Configuration Guide』

- 『*Unicast Routing Configuration Guide*』
- 『*Verified Scalability Guide for Cisco NX-OS*』

#### テクニカル リファレンス

テクニカル リファレンスは、次の URL で入手できます。

[http://www.cisco.com/en/US/products/ps11541/prod\\_technical\\_reference\\_list.html](http://www.cisco.com/en/US/products/ps11541/prod_technical_reference_list.html)

#### エラー メッセージおよびシステム メッセージ

エラー メッセージとシステム メッセージのリファレンス ガイドは次の URL で入手できます。

[http://www.cisco.com/en/US/products/ps11541/products\\_system\\_message\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps11541/products_system_message_guides_list.html)

## マニュアルの入手方法およびテクニカル サポート

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

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

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



# 第 1 章

## このリリースの新規および変更情報

次の表に、最新リリースに関するこのガイドでの重要な変更点の概要を示します。この表は、実行コンフィギュレーションガイドへのすべての変更や、またはこのリリースの新機能の詳細なリストを提供しません。

- [このリリースの新規および変更情報, 1 ページ](#)

## このリリースの新規および変更情報

次の表に、最新リリースに関するこのガイドでの重要な変更点の概要を示します。この表は、実行コンフィギュレーションガイドへのすべての変更や、またはこのリリースの新機能の詳細なリストを提供しません。

機能	説明	追加または変更されたリリース	参照先
<b>show interface <i>vlan-id</i> counters</b>	<b>show interface vlan <i>vlan-id</i> counters</b> コマンドは、入力および出力パケットのカウンタを正しく表示するように拡張されました。	5.0(3)U3(1)	<a href="#">レイヤ3 インターフェイスの設定, (3 ページ)</a>
最小リンク	最小リンク機能の設定および使用に関する情報を追加しました。	5.0(3)U3(1)	<a href="#">ポートチャネルの設定, (19 ページ)</a>





## 第 2 章

# レイヤ 3 インターフェイスの設定

---

この章の内容は、次のとおりです。

- [レイヤ 3 インターフェイスについて, 3 ページ](#)
- [レイヤ 3 インターフェイスのライセンス要件, 6 ページ](#)
- [レイヤ 3 インターフェイスの注意事項および制約事項, 7 ページ](#)
- [レイヤ 3 インターフェイスのデフォルト設定, 7 ページ](#)
- [レイヤ 3 インターフェイスの設定, 7 ページ](#)
- [レイヤ 3 インターフェイス設定の確認, 14 ページ](#)
- [レイヤ 3 インターフェイスのモニタリング, 15 ページ](#)
- [レイヤ 3 インターフェイスの設定例, 17 ページ](#)
- [レイヤ 3 インターフェイスの関連資料, 17 ページ](#)
- [レイヤ 3 インターフェイスの MIB, 18 ページ](#)
- [レイヤ 3 インターフェイスの標準, 18 ページ](#)
- [レイヤ 3 インターフェイスの機能履歴, 18 ページ](#)

## レイヤ 3 インターフェイスについて

レイヤ 3 インターフェイスは、IPv4 および IPv6 パケットをスタティックまたはダイナミックルーティングプロトコルを使って別のデバイスに転送します。レイヤ 2 トラフィックの IP ルーティングおよび内部 Virtual Local Area Network (VLAN) ルーティングにはレイヤ 3 インターフェイスが使用できます。

## 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、デフォルトでスイッチ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、インターフェイスコンフィギュレーションモードで **no switchport** コマンドを使用します。複数のポートを一度に変更するには、インターフェイスの範囲を指定してから、**no switchport** コマンドを適用します。

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。

レイヤ3インターフェイスにスタティックMACアドレスを割り当てることができます。MACアドレスの設定については、『Cisco Nexus 3000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。

ルーテッドインターフェイスからレイヤ3ポートチャンネルも作成できます。

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

サブインターフェイスの名前は、親インターフェイスの名前（たとえば Ethernet 2/1）+ピリオド（.）+そのインターフェイス独自の番号です。たとえば、イーサネットインターフェイス 2/1 に Ethernet2/1.1 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。

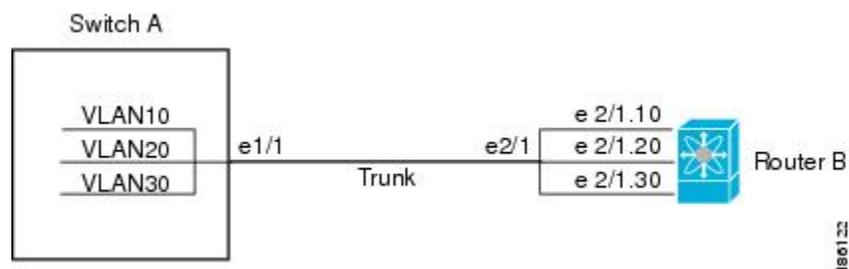
Cisco NX-OS では、親インターフェイスがイネーブルの場合にサブインターフェイスがイネーブルになります。サブインターフェイスは、親インターフェイスには関係なくシャットダウンでき

まず、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 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。

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

図 1: VLAN のサブインターフェイス



## 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、デバイスの VLAN を同じデバイスのレイヤ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。システムはこの機能をディセーブルにする前のチェックポイントを自動的に取得するため、このチェックポイントにロールバックできます。ロールバックとチェックポイントの詳細については、『Cisco Nexus 3000 NX-OS System Management Configuration Guide』を参照してください。

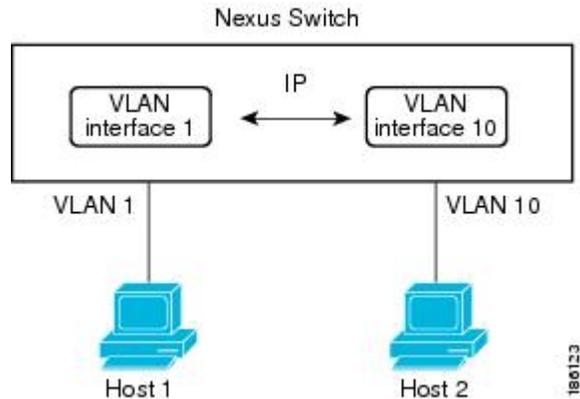


(注) VLAN 1 の VLAN インターフェイスは削除できません。

VLAN インターフェイスをルーティングするには、トラフィックをルーティングする VLAN ごとに VLAN インターフェイスを作成し、その VLAN インターフェイスに IP アドレスを割り当ててレイヤ3 内部 VLAN ルーティングを実現します。IP アドレスと IP ルーティングの詳細については、『Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

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

図 2: VLAN インターフェイスによる2つのVLANの接続



## 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。

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

## トンネル インターフェイス

Cisco NX-OS は、IP トンネルとしてトンネルインターフェイスをサポートします。IP トンネルを使うと、同じレイヤまたは上位レイヤの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。

## レイヤ3 インターフェイスのライセンス要件

この機能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。NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

# レイヤ3インターフェイスの注意事項および制約事項

レイヤ3インターフェイスの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。

## レイヤ3インターフェイスのデフォルト設定

レイヤ3の管理ステートのデフォルト設定は Shut です。

## レイヤ3インターフェイスの設定

### ルーテッドインターフェイスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>interface ethernet slot/port</b>	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# <b>no switchport</b>	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。  (注) 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再び変換するには、 <b>switchport</b> コマンドを使用します。
ステップ 4	switch(config-if)# [ <b>ip   ipv6</b> ] <i>ip-address/length</i>	このインターフェイスの IP アドレスを設定します。
ステップ 5	switch(config-if)# <b>medium {broadcast   p2p}</b>	(任意) ポイント ツー ポイントまたはブロードキャストとしてインターフェイスのメディアを設定します。

	コマンドまたはアクション	目的
		(注) デフォルト設定はbroadcastであり、この設定はいずれの <b>show</b> コマンドにも表示されません。ただし、 <b>p2p</b> に設定を変更した場合、 <b>show running-config</b> コマンドを入力すると、この設定が表示されます。
ステップ 6	switch(config-if)# <b>show interfaces</b>	(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 7	switch(config-if)# <b>copy running-config startup-config</b>	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

次に、IPv4 ルーテッドレイヤ3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
```

## サブインターフェイスの設定

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

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch(config-if)# <b>copy running-config startup-config</b>	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

	コマンドまたはアクション	目的
ステップ 2	<code>switch(config)# interface ethernet slot/port.number</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。 <i>slot</i> の範囲は 1 ~ 255 です。 <i>port</i> の範囲は 1 ~ 128 です。
ステップ 3	<code>switch(config-if)# [ip   ipv6] address ip-address/length</code>	このインターフェイスの IP アドレスを設定します。
ステップ 4	<code>switch(config-if)# encapsulation dot1Q vlan-id</code>	サブインターフェイスで IEEE 802.1Q VLAN カプセル化を設定します。 <i>vlan-id</i> の範囲は 2 ~ 4093 です。
ステップ 5	<code>switch(config-if)# show interfaces</code>	(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	<code>switch(config-if)# copy running-config startup-config</code>	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

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
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。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<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。

	コマンドまたはアクション	目的
ステップ 2	<code>switch(config)# interface ethernet slot/port</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。 <i>slot</i> の範囲は 1 ~ 255 です。 <i>port</i> の範囲は 1 ~ 128 です。
ステップ 3	<code>switch(config-if)# bandwidth [value   inherit [value]]</code>	次のように、ルーテッドインターフェイス、ポートチャネル、またはサブインターフェイスに帯域幅パラメータを設定します。 <ul style="list-style-type: none"> <li>• <b>value</b> : 帯域幅のサイズ (キロバイト)。 範囲は 1 ~ 10000000 です。</li> <li>• <b>inherit</b> : このインターフェイスのすべてのサブインターフェイスが、帯域幅の値 (値が指定されている場合) または親インターフェイスの帯域幅 (値が指定されていない場合) のどちらかを継承することを示します。</li> </ul>
ステップ 4	<code>switch(config-if)# copy running-config startup-config</code>	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

次に、イーサネットインターフェイス 2/1 に 80000 の帯域幅の値を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# bandwidth 80000
switch(config-if)# copy running-config startup-config
```

## VLAN インターフェイスの設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	<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>switch(config)# feature interface-vlan</code>	VLAN インターフェイス モードをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# <b>interface vlan number</b>	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	switch(config-if)# [ <b>ip   ipv6</b> ] <b>address ip-address/length</b>	このインターフェイスの IP アドレスを設定します。
ステップ 5	switch(config-if)# <b>show interface vlan number</b>	(任意) VLAN インターフェイスの統計情報を表示します。 <i>number</i> の範囲は 1 ~ 4094 です。
ステップ 6	switch(config-if)# <b>copy running-config startup-config</b>	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

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
```

## Nexus シャーシでのインバンド管理の設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# <b>feature interface-vlan</b>	VLAN インターフェイス モードをイネーブルにします。
ステップ 3	switch(config)# <b>interface vlan number</b>	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	switch(config-if)# <b>no shutdown</b>	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)。

	コマンドまたはアクション	目的
ステップ 5	switch(config-if)# <b>management</b>	VLAN インターフェイスの IP アドレスへのインバンド管理アクセスを許可します。
ステップ 6	switch(config-if)# [ <b>ip</b>   <b>ipv6</b> ] <b>address</b> <i>ip-address/length</i>	このインターフェイスの IPv4 アドレスまたは IPv6 アドレスを設定します。
ステップ 7	switch(config-if)# <b>show interface</b> <b>vlan</b> <i>number</i>	(任意) VLAN インターフェイスの統計情報を表示します。 <i>number</i> の範囲は 1 ~ 4094 です。
ステップ 8	switch(config-if)# <b>copy</b> <b>running-config startup-config</b>	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

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

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

## ループバック インターフェイスの設定

### 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。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>interface loopback</b> <i>instance</i>	ループバック インターフェイスを作成します。 <i>instance</i> の範囲は 0 ~ 1023 です。

	コマンドまたはアクション	目的
ステップ 3	switch(config-if)# [ip   ipv6 ] address ip-address/length	このインターフェイスの IPv4 アドレスまたは IPv6 アドレスを設定します。
ステップ 4	switch(config-if)# show interface loopback instance	(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。 instance の範囲は 0 ~ 1023 です。
ステップ 5	switch(config-if)# copy running-config startup-config	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

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

### 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。VDC の変更は **switchto vdc** コマンドを使用します。
- VRF 用のインターフェイスを設定した後で、トンネルインターフェイスに IP アドレスを割り当てます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# <b>interface</b> interface-typenumber	インターフェイス コンフィギュレーションモードを開始します。
ステップ 3	switch(config-if)# <b>vrf member</b> vrf-name	このインターフェイスを VRF に追加します。
ステップ 4	switch(config-if)# [ip   ipv6]ip-address/length	このインターフェイスの IP アドレスを設定します。このステップは、このインターフェイス

	コマンドまたはアクション	目的
		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	switch(config-if)# <b>show vrf</b> [vrf-name] <b>interface interface-type</b> <i>number</i>	(任意) VRF 情報を表示します。
ステップ6	switch(config-if)# <b>show interfaces</b>	(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7	switch(config-if)# <b>copy</b> <b>running-config startup-config</b>	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

## レイヤ3インターフェイス設定の確認

設定を確認するには、次のいずれかのコマンドを使用します。

コマンド	目的
<b>show interface ethernet slot/port</b>	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。
<b>show interface ethernet slot/port brief</b>	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。
<b>show interface ethernet slot/port capabilities</b>	ポートタイプ、速度、デュプレックスを含むレイヤ3インターフェイス機能を表示します。
<b>show interface ethernet slot/port description</b>	レイヤ3インターフェイスの説明を表示します。
<b>show interface ethernet slot/port status</b>	レイヤ3インターフェイスの管理ステータス、ポートモード、速度、およびデュプレックスを表示します。

コマンド	目的
<b>show interface ethernet</b> <i>slot/port.number</i>	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。
<b>show interface port-channel</b> <i>channel-id.number</i>	ポート チャンネル 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。
<b>show interface loopback</b> <i>number</i>	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。
<b>show interface loopback</b> <i>number brief</i>	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。
<b>show interface loopback</b> <i>number description</i>	ループバック インターフェイスの説明を表示します。
<b>show interface loopback</b> <i>number status</i>	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。
<b>show interface vlan</b> <i>number</i>	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。
<b>show interface vlan</b> <i>number brief</i>	VLAN インターフェイスの動作ステータスを表示します。
<b>show interface vlan</b> <i>number description</i>	VLAN インターフェイスの説明を表示します。
<b>show interface vlan</b> <i>number private-vlan mapping</i>	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。
<b>show interface vlan</b> <i>number status</i>	VLAN インターフェイスの管理ステータスおよびプロトコル ステータスを表示します。

## レイヤ3 インターフェイスのモニタリング

機能に関する統計情報を表示するには、次のいずれかのコマンドを使用します。

コマンド	目的
<b>load- interval {interval seconds {1   2   3}}</b>	3種類のサンプリング間隔をビットレートおよびパケット レートの統計情報に設定します。VLAN ネットワーク インターフェイスの範囲は 60 ~ 300 秒で、レイヤ インターフェイスの範囲は 30 ~ 300 秒です。
<b>show interface ethernet slot/port counters</b>	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)。
<b>show interface ethernet slot/port counters brief</b>	レイヤ3インターフェイスの入出力カウンタを表示します。
<b>show interface ethernet slot/port counters detailed [all]</b>	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、すべての 32 ビットおよび 64 ビット パケットおよびバイトカウンタ (エラーを含む) を含めることができます。
<b>show interface ethernet slot/port counters error</b>	レイヤ3インターフェイスの入出力エラーを表示します。
<b>show interface ethernet slot/port counters snmp</b>	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。
<b>show interface ethernet slot/port.number counters</b>	サブインターフェイスの統計情報を表示します (ユニキャスト、マルチキャスト、ブロードキャスト)。
<b>show interface port-channel channel-id.number counters</b>	ポート チャネル サブインターフェイスの統計情報を表示します (ユニキャスト、マルチキャスト、ブロードキャスト)。
<b>show interface loopback number counters</b>	ループバック インターフェイスの入出力カウンタを表示します (ユニキャスト、マルチキャスト、ブロードキャスト)。
<b>show interface loopback number counters detailed [all]</b>	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、すべての 32 ビットおよび 64 ビット パケットおよびバイトカウンタ (エラーを含む) を含めることができます。

コマンド	目的
<b>show interface loopback <i>number</i> counters errors</b>	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。
<b>show interface vlan <i>number</i> counters</b>	VLAN インターフェイスの入出力カウンタを表示します (ユニキャスト、マルチキャスト、ブロードキャスト)。
<b>show interface vlan <i>number</i> counters detailed [<i>all</i>]</b>	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)。
<b>show interface vlan <i>counters snmp</i></b>	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。

## 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。

```
switch# configuration terminal
switch(config)# interface ethernet 2/1.10
switch(config-if)# description Layer 3 for VLAN 10
switch(config-if)# encapsulation dot1q 10
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# copy running-config startup-config
```

次に、VLAN インターフェイスを設定する例を示します。

```
switch# configuration terminal
switch(config)# interface vlan 100
switch(config-if)# ipv6 address 33:0DB::2/8
switch(config-if)# copy running-config startup-config
```

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。

```
switch# configuration terminal
switch(config)# interface loopback 3
switch(config-if)# ip address 192.0.2.2/32
switch(config-if)# copy running-config startup-config
```

## レイヤ3 インターフェイスの関連資料

関連トピック	参照先
コマンド構文	『Cisco Nexus 3000 Series Command Reference』

関連トピック	参照先
IP	『Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide』の「Configuring IP」の章
VLAN	『Cisco Nexus 3000 Series NX-OS Layer 2 Switching Configuration Guide』の「Configuring VLANs」の章

## レイヤ3インターフェイスの MIB

MIB	MIB Link
IF-MIB	MIBを検索およびダウンロードするには、次のURLにアクセスしてください。 <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>
CISCO-IF-EXTENSION-MIB	
ETHERLIKE-MIB	

## レイヤ3インターフェイスの標準

この機能では、新規の標準がサポートされることも、一部変更された標準がサポートされることもありません。また、既存の標準に対するサポートが変更されることもありません。

## レイヤ3インターフェイスの機能履歴

機能名	リリース	機能情報
<b>show interface vlan <i>vlan-id</i> counters</b> command	5.0(3)U3(1)	<b>show interface vlan <i>vlan-id</i> counters</b> コマンドは、入力および出力パケットのカウンタを正しく表示するように拡張されました。



## 第 3 章

# ポート チャネルの設定

この章の内容は、次のとおりです。

- [ポート チャネルについて, 19 ページ](#)
- [ポート チャネルの設定, 28 ページ](#)
- [ポート チャネルの設定の確認, 37 ページ](#)
- [ロードバランシングの発信ポート ID の確認, 38 ページ](#)
- [ポート チャネルの機能履歴, 39 ページ](#)

## ポート チャネルについて

ポート チャネルは、最大 16 個のインターフェイスを 1 つのグループにバンドルしたもので、帯域幅を広げ冗長性を高めることができます。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。

互換性のあるインターフェイスをバンドルすることにより、ポートチャネルを作成します。スタティック ポートチャネル、またはリンク アグリゲーション制御プロトコル (LACP) を実行するポートチャネルを設定および実行できます。

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、スパン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 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。

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。より効率的にポートチャネルを使用するには、IEEE 802.3ad に規定されているリンクアグリゲーション制御プロトコル (LACP) を使用します。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。

## 関連トピック

[LACP の概要, \(24 ページ\)](#)

## ポートチャネルの概要

Cisco NX-OS は、ポートチャネルを使用して、広い帯域幅、冗長性、チャネル全体のロードバランシングを実現します。

ポートを1つのスタティックポートチャネルに集約するか、またはリンク集約制御プロトコル (LACP) をイネーブルにできます。LACPでポートチャネルを設定する場合、スタティックポートチャネルを設定する場合とは若干異なる手順が必要です。ポートチャネル設定の制約事項については、プラットフォームの『*Verified Scalability*』マニュアルを参照してください。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, \(22 ページ\)](#) を参照してください。



---

(注) Cisco NX-OS はポートチャネルのポート集約プロトコル (PAgP) をサポートしません。

---

ポートチャネルは、個々のリンクを1つのチャネルグループにバンドルしたもので、それによりいくつかの物理リンクの帯域幅を集約した単一の論理リンクが作成されます。ポートチャネル内のメンバ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ポートに切り替わります。

各ポートにはポートチャネルが1つだけあります。ポートチャネル内のすべてのポートは互換性がなければなりません。つまり、回線速度が同じで、全二重モードで動作する必要があります。スタティックポートチャネルをLACPなしで稼働すると、個々のリンクがすべて on チャネルモードで動作します。このモードを変更するには、LACP をイネーブルにする必要があります。



---

(注) チャネルモードを、on から active、または on から passive に変更することはできません。

---

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、ポートチャネルがまだ存在していない場合は、対応するポートチャネルが Cisco NX-OS によって自動的に作成されます。最初にポートチャネルを作成することもできます。このインスタンスで、Cisco NX-OS は、ポートチャネルと同じチャネル番号で空のチャネルグループを作成し、デフォルトの設定を採用します。



---

(注) 少なくともメンバポートの1つがアップしており、そのポートのステータスがチャネリングであれば、ポートチャネルはアップしています。メンバポートがすべてダウンしていれば、ポートチャネルはダウンしています。

---

## 互換性要件

ポートチャネルグループにインターフェイスを追加すると、Cisco NX-OS は、特定のインターフェイス属性をチェックし、その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。また Cisco NX-OS は、インターフェイスがポートチャネル集約に参加することを許可する前に、そのインターフェイスの多数の動作属性もチェックします。

互換性チェックの対象となる動作属性は次のとおりです。

- ポートモード
- アクセス VLAN
- トランク ネイティブ VLAN
- 許可 VLAN リスト
- 速度
- 802.3x フロー制御設定
- MTU
- ブロードキャスト/ユニキャスト/マルチキャスト ストーム制御設定
- プライオリティ フロー制御
- タグなし CoS

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

チャネルモードセットを **on** に設定したインターフェイスだけをスタティック ポートチャネルに追加できます。また、チャネルモードを **active** または **passive** に設定したインターフェイスだけを、LACP を実行するポートチャネルに追加できます。これらの属性は個別のメンバポートに設定できます。

インターフェイスがポートチャネルに参加すると、次の個々のパラメータは、ポートチャネルの値に置き換えられます。

- 帯域幅
- MAC アドレス
- スパニングツリー プロトコル (STP)

インターフェイスがポートチャネルに参加しても、次に示すインターフェイスパラメータは影響を受けません。

- 説明
- CDP
- LACP ポート プライオリティ

- デバウンス

**channel-group force** コマンドを入力して、ポートのチャネルグループへの強制追加をイネーブルにした後、次の2つの状態が発生します。

- インターフェイスがポートチャネルに参加すると、次のパラメータは削除され、動作上ポートチャネルの値と置き換えられます。ただし、この変更は、インターフェイスの実行コンフィギュレーションには反映されません

- QoS
- 帯域幅
- 遅延
- STP
- サービス ポリシー
- ACL

- インターフェイスがポートチャネルに参加するか脱退しても、次の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
- シャットダウン
- SNMP トラップ

## ポートチャネルを使ったロードバランシング

Cisco NX-OS は、ポートチャネルを構成するすべての動作中インターフェイス間でトラフィックのロードバランスを実現します。フレーム内のアドレスから生成されたバイナリパターンの一部を数値に圧縮変換し、それを使用してチャネル内の1つのリンクを選択することによってロードバランシングを行います。ポートチャネルはデフォルトでロードバランシングを行います。また、基本設定では、次の基準によってリンクを選択します。

- レイヤ2フレームの場合は、送信元および宛先のMACアドレスを使用します。
- レイヤ3フレームの場合は、送信元および宛先のMACアドレスと送信元および宛先のInternet Protocol (IP) アドレスを使用します。

- レイヤ4フレームの場合は、送信元および宛先のMACアドレスと送信元および宛先のIPアドレスを使用します。



(注) レイヤ4フレームには、送信元および宛先のポート番号を含めるオプションがあります。

次のいずれかに基づいてポートチャネル全体でのロードバランシングが行われるようにスイッチを設定することができます。

- 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
- 宛先TCP/UDPポート番号
- 送信元TCP/UDPポート番号
- 送信元および宛先TCP/UDPポート番号

表1: ポートチャネルにおけるロードバランシングの基準

設定	レイヤ2基準	レイヤ3基準	レイヤ4基準
宛先MAC	宛先MAC	宛先MAC	宛先MAC
送信元MAC	送信元MAC	送信元MAC	送信元MAC
送信元/宛先MAC	送信元/宛先MAC	送信元/宛先MAC	送信元/宛先MAC
宛先IP	宛先MAC	宛先MAC、宛先IP	宛先MAC、宛先IP
送信元IP	送信元MAC	送信元MAC、送信元IP	送信元MAC、送信元IP
送信元/宛先IP	送信元/宛先MAC	送信元/宛先MAC、送信元/宛先IP	送信元/宛先MAC、送信元/宛先IP
宛先TCP/UDPポート	宛先MAC	宛先MAC、宛先IP	宛先MAC、宛先IP、宛先ポート

設定	レイヤ 2 基準	レイヤ 3 基準	レイヤ 4 基準
送信元 TCP/UDP ポート	送信元 MAC	送信元 MAC、送信元 IP	送信元 MAC、送信元 IP、送信元ポート
送信元および宛先 TCP/UDP ポート	送信元/宛先 MAC	送信元/宛先 MAC、送信元/宛先 IP	送信元/宛先 MAC、送信元/宛先 IP、送信元/宛先ポート

使用する設定で最多の種類ロードバランス条件を提供するオプションを使用してください。たとえば、ポートチャネルのトラフィックが1つのMACアドレスにだけ送られ、ポートチャネルのロードバランシングの基準としてその宛先MACアドレスが使用されている場合、ポートチャネルでは常にそのポートチャネルの同じリンクが選択されます。したがって、送信元アドレスまたはIPアドレスを使用すると、結果的により優れたロードバランシングが得られることとなります。

## LACP の概要

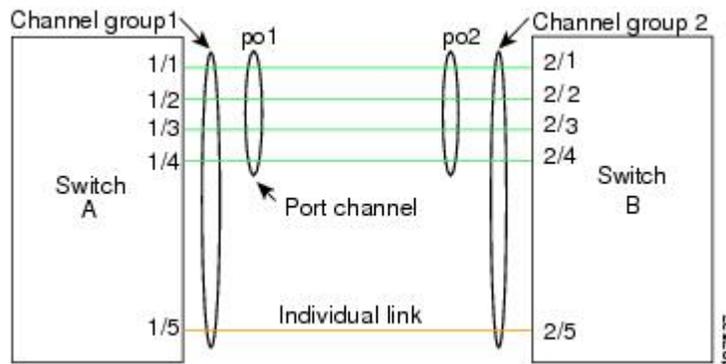
### LACP の概要



(注) LACP 機能を設定して使用する前に、LACP 機能をイネーブルにする必要があります。

次の図に、個別リンクを LACP ポートチャネルおよびチャネルグループに組み込み、個別リンクとして機能させる方法を示します。

図 3: 個別リンクをポートチャネルに組み込む



スタティックポートチャネルと同様に、LACP を使用すると、チャネルグループに最大 16 のインターフェイスをバンドルできます。



(注) ポートチャネルを削除すると、Cisco NX-OS は関連付けられたチャネルグループを自動的に削除します。すべてのメンバインターフェイスは以前の設定に戻ります。

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。

## LACP ID パラメータ

LACP では次のパラメータを使用します。

- **LACP システムプライオリティ** : LACP を稼働している各システムは、LACP システムプライオリティ値を持っています。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。



(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られたものです。

- **LACP ポートプライオリティ** : LACP を使用するように設定された各ポートには、LACP ポートプライオリティが割り当てられます。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 はポートプライオリティとポート番号を使用してポート ID を形成します。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各ポート上のチャネルグループ番号に等しい管理キー値を自動的に設定します。管理キーは、他のポートと集約されるポートの機能を定義します。他のポートと集約されるポート機能は、次の要因によって決まります。
  - ポートの物理特性 (データレート、デュプレックス機能、ポイントツーポイントまたは共有メディアステートなど)
  - ユーザが作成した設定に関する制限事項

## 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。プロトコルを使用せずにスタティックポートチャネルを実行すると、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。LACP チャネルグループを構成する個々のリンクについて、どちら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。

次の表に、各チャネルモードについて説明します。

表 2: 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	ポートをパッシブなネゴシエーション状態にする LACP モード。この状態では、ポートは受信した LACP パケットに応答はしますが、LACP ネゴシエーションを開始することはありません。
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、つまり LACP を稼働していないポートチャネルは、このモードのままになります。LACP をイネーブルにする前にチャネルモードを active または passive に変更しようとする、デバイスがエラーメッセージを返します。  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せん。つまり、LACP チャネルグループには参加しません。

passive および active の両モードでは、LACP は、ポート間でネゴシエートし、ポート速度やトラフィックステートなどの基準に基づいて、ポートチャネルを形成可能かどうかを決定できます。passive モードは、リモートシステム、つまり、パートナーが、LACP をサポートしているかどうか不明な場合に便利です。

ポートは、異なる LACP モードであっても、それらのモード間で互換性があれば、LACP ポートチャネルを形成できます。次に、LACP ポートチャネルのモードの組み合わせの例を示します。

- active モードのポートは、active モードの別のポートとともにポートチャネルを正しく形成できます。
- active モードのポートは、passive モードの別のポートとともにポートチャネルを形成できます。
- passive モードのポートは、どちらのポートもネゴシエーションを開始しないため、passive モードの別のポートとともにポートチャネルを形成できません。
- on モードのポートは LACP を実行していません。

## LACP マーカー レスポンダ

ポートチャネルを使用すると、リンク障害またはロードバランシング動作によって、データトラフィックが動的に再配信されます。LACP では、マーカープロトコルを使用して、こうした再配信によってフレームが重複したり順序が変わったりしないようにします。Cisco NX-OS は、マーカーレスポンスだけをサポートしています。

## 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

次の表に、LACP がイネーブルのポートチャネルとスタティックポートチャネルの主な相違点の簡単な概要を説明します。

表 3: 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 がイネーブルにされた EtherChannel	スタティック EtherChannel
適用されるプロトコル	グローバルにイネーブル化	該当なし
リンクのチャネルモード	次のいずれか。 <ul style="list-style-type: none"> <li>• Active</li> <li>• Passive</li> </ul>	on モードのみ
チャネルを構成する最大リンク数	16	16

## LACP ポートチャネルの MinLink

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。MinLink 機能を使用すると、ポートチャネルがダウンする前に停止する必要がある LACP バンドルからのインターフェイスの最小数を定義できます。

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し、バンドルする必要があるポートチャネルインターフェイス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。
- 少数のアクティブメンバポートだけが必要な最小帯域幅を提供する場合、LACP ポートチャネルが非アクティブになります。



(注) MinLink 機能は、LACP ポートチャネルだけで動作します。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。

# ポートチャネルの設定

## ポートチャネルの作成

チャネルグループを作成する前に、ポートチャネルを作成します。Cisco NX-OS は、対応するチャネルグループを自動的に作成します。



(注) LACP ベースのポートチャネルを使用する場合は、LACP をイネーブルにする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<code>switch# configure terminal</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>switch(config)# interface port-channel channel-number</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。指定できる範囲は 1～4096 です。チャネルグループがまだ存在していなければ、Cisco NX-OS によって自動的に作成されます。

	コマンドまたはアクション	目的
ステップ 3	<code>switch(config)# no interface port-channel channel-number</code>	ポートチャネルを削除し、関連するチャン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たものです。

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

## ポートチャネルへのポートの追加

新規のチャンネルグループ、または他のポートがすでに属しているチャンネルグループにポートを追加できます。Cisco NX-OS では、このチャンネルグループに関連付けられたポートチャネルがなければ作成されます。



(注) LACP ベースのポートチャネルが必要な場合は、LACP をイネーブ爾にする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<code>switch# configure terminal</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>switch(config)# interface type slot/port</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>switch(config-if)# switchport mode trunk</code>	(任意) トランクポートとしてインターフェイスを設定します。
ステップ 4	<code>switch(config-if)# switchport trunk {allowed vlan vlan-id   native vlan vlan-id}</code>	(任意) トランクポートに必要なパラメータを設定します。
ステップ 5	<code>switch(config-if)# channel-group channel-number</code>	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。Cisco NX-OS では、このチャンネルグループに関連付けられたポートチャネルがなければ作成されます。これはポートチャネルの暗黙的作成と呼ばれます。

	コマンドまたはアクション	目的
ステップ 6	switch(config-if)# <b>no channel-group</b>	(任意) チャネルグループからポートを削除します。チャネルグループから削除されたポートは元の設定に戻ります。

次に、イーサネットインターフェイス 1/4 をチャネルグループ 1 に追加する例を示します。

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

## ポートチャネルを使ったロードバランシングの設定

デバイス全体に適用される、ポートチャネル用のロードバランシングアルゴリズムを設定できます。



(注) LACP ベースのポートチャネルが必要な場合は、LACP をイネーブルにする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# <b>port-channel load-balance ethernet</b> {[ <b>destination-ip</b>   <b>destination-mac</b>   <b>destination-port</b>   <b>source-dest-ip</b>   <b>source-dest-mac</b>   <b>source-dest-port</b>   <b>source-ip</b>   <b>source-mac</b>   <b>source-port</b> ] <b>crc-poly</b> }	デバイス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。デフォルトは source-dest-mac です。
ステップ 3	switch(config)# <b>no port-channel load-balance ethernet</b>	(任意) source-dest-mac のデフォルトのロードバランシングアルゴリズムを復元します。
ステップ 4	switch# <b>show port-channel load-balance</b>	(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。

次に、ポートチャネルの送信元 IP ロードバランシングを設定する例を示します。

```
switch# configure terminal
switch (config)# port-channel load-balance ethernet source-ip
```

## マルチキャストトラフィックのハードウェアハッシュの設定

スイッチのいずれのポートにある入力マルチキャストトラフィックでも、デフォルトで、特定のポートチャネルメンバが選択され、トラフィックが出力されます。潜在的な帯域幅の問題を減らし、入力マルチキャストトラフィックの効率的なロードバランシングを提供するために、マルチキャストトラフィックにハードウェアハッシュを設定できます。ハードウェアハッシュをイネーブルにするには、**hardware multicast hw-hash** コマンドを使用します。デフォルトに戻すには、**no hardware multicast hw-hash** コマンドを使用します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# <b>interface port-channel channel-number</b>	ポートチャネルを選択し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 3	switch(config-if)# <b>hardware multicast hw-hash</b>	指定したポートチャネルにハードウェアハッシュを設定します。

次に、ポートチャネルでハードウェアハッシュを設定する例を示します。

```
switch# configure terminal
switch (config)# interface port-channel 21
switch(config-if)# hardware multicast hw-hash
```

次に、ポートチャネルからハードウェアハッシュを削除する例を示します。

```
switch# configure terminal
switch (config)# interface port-channel 21
switch(config-if)# no hardware multicast hw-hash
```

## 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、これらのリンクを 1 つのポートチャ

ネルとして容易にまとめます。次に、ポートチャネルは単一ブリッジポートとしてスパンニングツリーに追加されます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# <b>feature lacp</b>	スイッチ上で LACP をイネーブルにします。
ステップ 3	switch(config)# <b>show feature</b>	(任意) イネーブルにされた機能を表示します。

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
```

## ポートのチャネルモードの設定

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

LACP 機能がイネーブルになっていることを確認します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# <b>interface type slot/port</b>	設定するインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	switch(config-if)# <b>channel-group</b> <i>channel-number</i> [ <b>force</b> ] [ <b>mode</b> { <b>on</b>   <b>active</b>   <b>passive</b> }]	<p>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 <b>active</b> または <b>passive</b> に設定します。</p> <p><b>force</b> : LAN ポートをチャネルグループに強制的に追加することを指定します。このオプションは、Cisco NX-OS Release 5.0(2)N2(1) で使用できます。</p> <p><b>mode</b> : インターフェイスのポートチャネルモードを指定します。</p> <p><b>active</b> : LACPをイネーブルにすると、このコマンドは、指定されたインターフェイスでLACPをイネーブルにすることを指定します。インターフェイスはアクティブなネゴシエーション状態になります。この状態では、ポートはLACPパケットを送信して他のポートとネゴシエーションを開始します。</p> <p><b>on</b> : (デフォルトモード) LACPを実行していないすべてのポートチャネルがこのモードを維持することを指定します。</p> <p><b>passive</b> : LACPデバイスが検出された場合にだけ、LACPをイネーブルにします。インターフェイスはパッシブなネゴシエーション状態になります。この状態では、ポートは受信したLACPパケットに応答しますが、LACPネゴシエーションを開始しません。</p> <p>関連する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、チャネルモードは常に <b>on</b> です。</p>
ステップ 4	switch(config-if)# <b>no</b> <b>channel-group</b> <i>number</i> <b>mode</b>	指定インターフェイスのポートモードを <b>on</b> に戻します

次に、チャネルグループ 5 のイーサネット インターフェイス 1/4 で、LACP がイネーブルなインターフェイスを **active** 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
```

次に、強制的にチャネルグループ 5 にインターフェイスを追加する例を示します。

```
switch(config)# interface ethernet 1/1
switch(config-if)# channel-group 5 force
switch(config-if)#
```

## LACP ポートチャネルの MinLink の設定

MinLink 機能は、LACP ポートチャネルだけで動作します。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。



重要

シスコでは、ポートチャネルの一端にだけ MinLink 機能を設定することを推奨します。ポートチャネルの両側に `lacp min-links` コマンドを設定すると、リンクフラッピングが発生する可能性があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  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	<b>interface port-channel number</b>  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	<b>[no] lacp min-links number</b>  例： switch(config-if) # lacp min-links 3	ポートチャネルインターフェイスを指定して、最小リンクの数を設定し、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> のデフォルト値は、1 です。指定できる範囲は 1 ~ 16 です。  この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 4	<b>show running-config interface port-channel number</b>  例： switch(config) # show running-config interface port-channel 3 switch(config-if) #	(任意) ポートチャネルの MinLink 設定を表示します。

次に、モジュール 3 のポートチャネルインターフェイスの最小数を設定する例を示します。

```
switch# configure terminal
switch(config) # interface port-channel 3
```

```
switch(config-if) # lacp min-links 3
switch(config-if) #
```

## LACP 高速タイマー レートの設定

LACP タイムアウト期間を変更するには、LACP タイマー レートを変更します。LACP をサポートするインターフェイスに LACP 制御パケットが送信されるレートを設定するには、**lacp rate** コマンドを使用します。デフォルト レート (30 秒) から高速レート (1 秒) にタイムアウト レートを変更できます。このコマンドは、LACP 対応インターフェイスだけでサポートされます。

### 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。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# <b>interface type slot/port</b>	設定するインターフェイスを指定します。インターフェイスコンフィギュレーションモードを開始します。
ステップ 3	switch(config-if)# <b>lacp rate fast</b>	LACP をサポートするインターフェイスに LACP 制御パケットが送信される高速レート (1 秒) を設定します。

次に、イーサネットインターフェイス 1/4 の LACP 高速レートを設定する例を示します。

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

switch(config-if)# lacp rate fast
```

次に、イーサネットインターフェイス 1/4 の LACP のデフォルトレート (30 秒) を復元する例を示します。

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

## LACP のシステム プライオリティおよびシステム ID 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。

## 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。

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# <b>lACP system-priority priority</b>	LACP で使用するシステムプライオリティを設定します。指定できる範囲は 1～65535 で、値が大きいほどプライオリティは低くなります。デフォルト値は 32768 です。
ステップ 3	switch# <b>show lACP system-identifier</b>	(任意) LACP システム識別子を表示します。

次に、LACP システムプライオリティを 2500 に設定する例を示します。

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

## LACP ポートプライオリティの設定

ポートプライオリティに LACP ポートチャネルの各リンクを設定できます。

## 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。

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# <b>interface type slot/port</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 3	switch(config-if)# <b>lACP port-priority priority</b>	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。

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
```

## ポートチャネルの設定の確認

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
switch# <b>show interface port-channel</b> <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。
switch# <b>show feature</b>	イネーブルにされた機能を表示します。
switch# <b>show resource</b>	システムで現在使用可能なリソースの数を表示します。
switch# <b>show lacp</b> { <b>counters</b>   <b>interface type</b> <i>slot/port</i>   <b>neighbor</b>   <b>port-channel</b>   <b>system-identifier</b> }	LACP 情報を表示します。
switch# <b>show port-channel</b> <b>compatibility-parameters</b>	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。
switch# <b>show port-channel database</b> [ <b>interface</b> <b>port-channel</b> <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。
switch# <b>show port-channel summary</b>	ポートチャネルインターフェイスの概要を表示します。
switch# <b>show port-channel traffic</b>	ポートチャネルのトラフィック統計情報を表示します。
switch# <b>show port-channel usage</b>	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。
switch# <b>show port-channel database</b>	現在実行中のポートチャネル機能に関する情報を表示します。
switch# <b>show port-channel load-balance</b>	ポートチャネルを使用したロードバランシングに関する情報を表示します。

## ロードバランシングの発信ポートIDの確認

### コマンドのガイドライン

**show port-channel load-balance** コマンドでは、特定のフレームがハッシュされるポートチャネルのポートを確認することができます。正確な結果を得るためには、VLAN と宛先 MAC を指定する必要があります。



(注) ポートチャネルのポートが1つだけの場合など、特定のトラフィックフローはハッシュ対象ではありません。

ロードバランシングの発信ポートIDを表示するには、次の表に示すタスクの1つを実行します。

コマンド	目的
<pre>switch# show port-channel load-balance forwarding-path interface port-channel port-channel-id vlan vlan-id dst-ip src-ip dst-mac src-mac l4-src-port port-id l4-dst-port port-id</pre>	発信ポートIDを表示します。

### 例

次に、短い **port-channel load-balance** コマンドの出力例を示します。

```
switch#show port-channel load-balance forwarding-path interface port-channel 10 vlan 1 dst-ip
1.225.225.225 src-ip 1.1.10.10 src-mac aa:bb:cc:dd:ee:ff l4-src-port 0 l4-dst-port 1
```

```
Missing params will be substituted by 0's.Load-balance Algorithm on switch:
source-dest-portcrc8_hash: 204 Outgoing port id: Ethernet1/1 Param(s) used
to calculate load-balance:
```

```
dst-port: 1
```

```
src-port: 0
```

```
dst-ip: 1.225.225.225
```

```
src-ip: 1.1.10.10
```

```
dst-mac: 0000.0000.0000
```

```
src-mac: aabb.ccdd.eeff
```

## ポートチャネルの機能履歴

機能名	リリース	機能情報
最小リンク	5.0(3)U3(1)	最小リンク機能の設定および使用に関する情報を追加しました。





## 第 4 章

# 仮想ポート チャネルの設定

この章の内容は、次のとおりです。

- [vPC について, 41 ページ](#)
- [vPC の注意事項および制約事項, 52 ページ](#)
- [vPC の設定, 52 ページ](#)
- [vPC 設定の確認, 66 ページ](#)
- [vPC のデフォルト設定, 72 ページ](#)

## vPC について

### vPC の概要

仮想ポート チャネル (vPC) は、物理的には 2 台の異なる Cisco Nexus 3000 シリーズ スイッチ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 チャネルに見えるようにします (次の図を参照)。第 3 のデバイスは、スイッチ、サーバ、またはその他の任意のネットワーキング デバイスです。vPC では、マルチパスを提供できます。この機能では、ノード間の複数のパラレルパスをイネーブルにし、存在する代替パスでトラフィックのロードバランシングを行うことによって、冗長化することができます。

EtherChannel 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 アグリゲーション制御プロトコル (LACP)

vPC に EtherChannel を設定する場合 (vPC ピア リンク チャネルも含める)、各スイッチは、単一の EtherChannel 内に最大 16 個のアクティブ リンクを設定できます。



(注) vPC の機能を設定したり実行したりするには、まず vPC 機能をイネーブルにする必要があります。

vPC 機能をイネーブルにするには、vPC 機能を提供するように 2 台の vPC ピア スイッチに対して vPC ドメインでピアキープアライブ リンクとピア リンクを作成する必要があります。

vPC ピア リンクを作成するには、2 つ以上のイーサネット ポートを使用して、1 台の Cisco Nexus 3000 シリーズ スイッチ上で EtherChannel を設定します。もう 1 台のスイッチには、2 つ以上のイーサネット ポートをまた使用して別の EtherChannel を設定します。これら 2 つの EtherChannel を同時に接続すると、vPC ピア リンクが作成されます。



(注) トランクとして vPC ピア リンク EtherChannel を設定することを推奨します。

vPC ドメインには、両方の vPC ピア デバイス、vPC ピアキープアライブ リンク、vPC ピア リンク、および vPC ドメイン内にあるダウンストリーム デバイスに接続されているすべての EtherChannel が含まれます。各 vPC ピア デバイスに設定できる vPC ドメイン ID は、1 つだけです。



(注) 常にすべての vPC デバイスを両方の vPC ピア デバイスに、EtherChannel を使用して接続します。

vPC 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 EtherChannel を使用することを可能にします。
- スパニングツリー プロトコル (STP) のブロック ポートをなくします。
- ループフリーなトポロジを提供します。
- 利用可能なすべてのアップリンク帯域幅を使用します。
- リンクまたはスイッチに障害が発生した場合に高速なコンバージェンスを提供します。
- リンクレベルの復元力を提供します。
- ハイ アベイラビリティを保証します。

## 用語

### 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 EtherChannel。

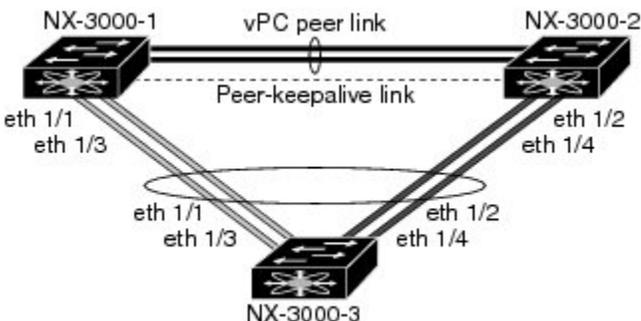
- vPC ピア デバイス : vPC ピア リンクと呼ばれる特殊な EtherChannel で接続されている一対のデバイスの 1 つ。
  - vPC ピア リンク : vPC ピア デバイス間の状態を同期するために使用されるリンク。
  - vPC メンバ ポート : vPC に属するインターフェイス。
  - vPC ドメイン : このドメインには、両方の vPC ピア デバイス、vPC ピア キープアライブ リンク、vPC 内にあってダウンストリームデバイスに接続されているすべてのポートチャネルが含まれます。また、このドメインは、vPC グローバルパラメータを割り当てるために使用する必要があるコンフィギュレーションモードに関連付けられています。vPC ドメイン ID は両方のスイッチで同じである必要があります。
  - 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 3000 シリーズ 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。
- vPC ピア キープアライブ リンク上を移動するデータまたは同期トラフィックはありません。このリンクを流れるトラフィックは、送信元スイッチが稼働しており、vPC を実行していることを知らせるメッセージだけです。

## サポートされている vPC トポロジ

### Cisco Nexus 3000 シリーズ スイッチ vPC トポロジ

vPC の Cisco Nexus 3000 シリーズ スイッチを別のスイッチまたはサーバに直接接続できます。最大 8 台のインターフェイスを各 Cisco Nexus 3000 シリーズ スイッチに接続でき、vPC のペアにバンドルされる 16 台のインターフェイスを提供できます。次の図に示すトポロジでは、デュアル接続されたスイッチまたはサーバに 10 ギガビットまたは 1 ギガビット イーサネットアップリンク インターフェイスの vPC 機能を提供します。

図 4 : スイッチ間 vPC トポロジ



Cisco Nexus 3000 シリーズ スイッチのペアに接続されたスイッチは、任意の標準ベースのイーサネットスイッチです。この設定を使用する共通環境には、Cisco Nexus 3000 シリーズ スイッチのペアに接続されているデュアルスイッチを使用するブレード シャーシが含まれます。これは、

vPC または Unified Computing System を介して Cisco Nexus 3000 シリーズ スイッチのペアに接続されます。

## vPC ドメイン

vPC ドメインを作成するには、まず各 vPC ピア スイッチ上で、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。この ID は、一連の vPC ピア デバイス上で同じである必要があります。

EtherChannel および vPC ピア リンクは、LACP を使用するかプロトコルなしで設定できます。LACP では EtherChannel における設定不一致の検査を実行できるため、ピアリンク上では可能な限り、LACP を使用することが推奨されます。

vPC ピア スイッチは、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、特定の vPC 関連操作に一意の 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、スイッチは 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だけ使用します。連続した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 ピア スイッチは、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。スイッチは LACP または BPDU など、リンクスコープ操作のためだけに vPC システム MAC アドレスを使用します。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。

シスコでは、両方のピアに同じ vPC ドメイン ID を設定し、ドメイン ID をネットワークで一意にすることを推奨します。たとえば、2 つの異なる vPC (1 つがアクセスで 1 つが集約) がある場合は、各 vPC には、一意のドメイン ID がある必要があります。

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手動で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 スイッチ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 スイッチ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。

## ピアキープアライブリンクとメッセージ

Cisco NX-OS ソフトウェアは、vPC ピア間でピアキープアライブリンクを使用して、設定可能なキープアライブメッセージを定期的送信します。これらのメッセージを送信するには、ピアスイッチ間にレイヤ 3 接続がなくてはなりません。ピアキープアライブリンクが有効になって稼働していないと、システムは vPC ピアリンクを稼働させることができません。

片方の vPC ピアスイッチに障害が発生したら、vPC ピアリンクの他方の側にある vPC ピアスイッチは、ピアキープアライブメッセージを受信しないことによってその障害を感知します。vPC ピアキープアライブメッセージのデフォルトの時間間隔は 1 秒です。間隔には 400 ミリ秒～10 秒を設定できます。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。ピアキープアライブのステータスは、ピアリンクがダウンした場合にだけチェックされます。

vPC ピアキープアライブは、Cisco Nexus 3000 シリーズスイッチ上で管理 VRF またはデフォルト VRF で伝送できます。管理 VRF を使用するようにスイッチを設定するとき、キープアライブメッセージの送信元および宛先は、mgmt 0 インターフェイス IP アドレスです。デフォルト VRF を使用するようにスイッチを設定するとき、vPC ピアキープアライブメッセージの送信元アドレスおよび宛先アドレスとして機能するように SVI を作成する必要があります。ピアキープアライブメッセージに使用される送信元 IP アドレスと宛先 IP アドレスの両方が、ネットワーク上で一意であり、それらの IP アドレスがその vPC ピアキープアライブリンクに関連付けられている VRF から到達できることを確認します。



(注) mgmt 0 インターフェイスを使用して管理 VRF で動作するように、Cisco Nexus 3000 シリーズスイッチで vPC ピアキープアライブリンクを設定することを推奨します。デフォルト VRF を設定するときは、vPC ピアキープアライブメッセージを伝送するために vPC ピアリンクが使用されていないことを確認してください。

## vPC ピアリンクの互換パラメータ

多くの設定パラメータおよび動作パラメータが、vPC 内のすべてのインターフェイスで同じでなければなりません。vPC 機能をイネーブルにし、両方の vPC ピアスイッチでピアリンクを設定した後で、Cisco Fabric Services (CFS) メッセージは、ローカル vPC ピアスイッチ設定の設定のコピーをリモート vPC ピアスイッチに提供します。これにより、システムが 2 つのスイッチ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。

vPC 内のすべてのインターフェイスで設定されている値を表示するには、**show vpc consistency-parameters** コマンドを入力します。表示される設定は、vPC ピアリンクおよび vPC の稼働を制限する可能性のある設定だけです。

vPC の互換性チェックプロセスは、正規の EtherChannel の互換性チェックとは異なります。

## 同じでなければならない設定パラメータ

ここで示す設定パラメータは、vPC ピアリンクの両端にある両方のスイッチで同一に設定する必要があります。



(注) vPC内のすべてのインターフェイスで、ここ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ることを確認してください。

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 インターフェイスのこれらのパラメータは、スイッチ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りません。

- ポートチャネルモード : on、off、active
- チャネルごとのリンク速度
- チャネルごとのデュプレックスモード
- チャネルごとのトランクモード :
  - ネイティブ VLAN
  - トランク上の許可 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
- マルチスパニングツリー (MST) の STP リージョン コンフィギュレーション
- VLAN ごとのイネーブルまたはディセーブルステート
- STP グローバル設定 :
  - Bridge Assurance 設定
  - ポートタイプの設定 : 標準ポートとしてすべての vPC インターフェイスを設定することを推奨します
  - ループガード設定
- STP インターフェイス設定 :
  - ポートタイプ設定
  - ループガード
  - ルートガード

これらのパラメータのいずれかがイネーブルになっていなかったり、片方のスイッチでしか定義されていないと、vPCの整合性検査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すべてが両方のvPCピアスイッチ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 エンドにある各スイッチの 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スイッチ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スイッチとセカンダリvPCスイッチの両方で作成する必要があります。そうしないと、VLANは停止します。
- プライベート VLAN 設定
- 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：ローカルパラメータ、グローバルパラメータは同じでなければなりません
- STP インターフェイス設定：
  - BPDU フィルタ
  - BPDU ガード
  - コスト
  - リンク タイプ
  - プライオリティ
  - VLAN (Rapid PVST+)

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ピアスイッチの設定を表示してみることを推奨します。

## グレースフルタイプ1チェック

整合性検査に失敗すると、セカンダリvPCスイッチでだけvPCはダウンします。VLANはプライマリスイッチでアップのまま、タイプ1の設定は、トラフィックの中断なしで実行できま

す。この機能は、グローバルな、またインターフェイス固有のタイプ 1 不整合の場合の両方で使用されます。

## VLAN ごとの整合性検査

一部のタイプ 1 整合性検査は、スパンニングツリーが VLAN でイネーブルまたはディセーブルにされるときに VLAN ごとに行われます。整合性検査に合格しない VLAN は、プライマリ スイッチおよびセカンダリ スイッチの両方でダウンにされますが、その他の VLAN は影響を受けません。

## vPC 自動リカバリ

vPC 自動リカバリ機能は、次のシナリオの vPC リンクを再びイネーブルにします。

両方の vPC ピア スイッチをリロードし、1 つだけのスイッチをリブートすると、自動リカバリによってスイッチがプライマリ スイッチのロールを負い、vPC リンクが所定の期間後に稼働できるようになります。このシナリオのリロード遅延時間は 240 ~ 3600 秒の範囲で指定します。

次に、ピアリンク障害によってセカンダリ vPC スイッチで vPC がディセーブルになり、その後プライマリ vPC スイッチに障害が発生するかトラフィックを転送できない場合、セカンダリ スイッチが vPC を再度イネーブルにします。このシナリオでは、vPC は 3 回連続してキープアライブに失敗するまで待機してから、vPC リンクを回復します。

vPC 自動リカバリ機能は、デフォルトでディセーブルです。

## 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。



(注) vPC ピア リンクを設定するよりも前にピアキープアライブリンクを設定する必要があります。そうしないと、ピア リンクは稼働しません。

## vPC ピア リンクの概要

vPC ピアとして持てるのは 2 台のスイッチだけです。各スイッチが、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 スイッチは、他のスイッチに対する非 vPC リンクも持つことができます。

有効な設定を作成するには、各スイッチで EtherChannel を設定してから、vPC ドメインを設定します。ピアリンクとして、各スイッチの EtherChannel を割り当てます。vPC ピアリンクのインターフェイスのいずれかに障害が発生した場合に、スイッチ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 EtherChannel に設定することを推奨します。



(注) トランク モードの EtherChannel を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スイッチで同じでなければなりません。各スイッチが管理プレーンから完全に独立しているため、スイッチ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 ピアスイッチは、独立したコントロールプレーンを持っています。vPC ピアリンクを設定し終えたら、各 vPC ピアスイッチの設定を表示して、設定に互換性があることを確認します。



(注) vPC ピアリンクによって接続されている 2 つのスイッチが、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。

vPC ピアリンクを設定する場合、vPC ピアスイッチは接続されたスイッチの 1 つがプライマリスイッチであり、もう 1 つの接続されたスイッチがセカンダリスイッチであることをネゴシエートします。デフォルトでは、Cisco NX-OS ソフトウェアが最小の MAC アドレスを使用してプライマリスイッチを選択します。特定のフェールオーバー条件の下でだけ、ソフトウェアが各スイッチ（つまり、プライマリスイッチおよびセカンダリスイッチ）に対して異なるアクションを実行します。プライマリスイッチに障害が発生した場合は、このセカンダリスイッチがシステム回復時に動作可能なプライマリスイッチになり、元のプライマリスイッチがセカンダリスイッチになります。

どの vPC スイッチがプライマリスイッチになるのかも設定できます。1 つの vPC スイッチをプライマリスイッチにするために再度ロールプライオリティを設定するには、プライマリとセカンダリの両方の vPC スイッチに適切な値でロールプライオリティを設定し、両方のスイッチの vPC ピアリンクである EtherChannel を **shutdown** コマンドを入力してシャットダウンします。次に、**no shutdown** コマンドを入力して両方のスイッチの EtherChannel を再度イネーブルにします。

vPC リンクに学習された MAC アドレスは、ピア間でも同期されます。

設定情報は、Cisco Fabric Services over Ethernet (CFS over Ethernet) プロトコルを使用して vPC ピアリンク間を流れます。両方のスイッチ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 ピアスイッチ間で同期されています。この同期に、CFS over Ethernet が使用されます。

vPC ピアリンクに障害が発生した場合は、ソフトウェアが、両方のスイッチが稼働していることを確認するための vPC ピアスイッチ間のリンクであるピアキープアライブリンクを使用して、リモート vPC ピアスイッチのステータスをチェックします。vPC ピアスイッチが稼働している場合は、セカンダリ vPC スイッチはスイッチのすべての vPC ポートをディセーブルにします。その後、データは、EtherChannel の残っているアクティブなリンクに転送されます。

ソフトウェアは、ピアキープアライブリンクを介したキープアライブメッセージが返されない場合に、vPC ピアスイッチに障害が発生したことを学習します。

vPC ピアスイッチ間の設定可能なキープアライブメッセージの送信には、別のリンク（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 ピアスイッチ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。

## vPC 番号

vPC ドメイン ID と vPC ピア リンクを作成し終えたら、ダウンストリームスイッチを各 vPC ピアスイッチに接続するための EtherChannel を作成します。つまり、ダウンストリームスイッチ上に単一の EtherChannel を作成し、プライマリ vPC ピアスイッチにポートの半分を、セカンダリピアスイッチにポートの残り半分を使用します。

各 vPC ピアスイッチでは、ダウンストリームスイッチに接続する EtherChannel に同じ 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。設定を簡素化するために、各 EtherChannel に対して EtherChannel 自体と同じである vPC ID 番号を割り当てられます（つまり、EtherChannel 10 に対して vPC ID 10）。



(注) vPC ピアスイッチからダウンストリームスイッチに接続されている EtherChannel に割り当てる vPC 番号は、両方の vPC スイッチで同じでなければなりません。

## その他の機能との vPC の相互作用

### vPC と LACP

リンクアグリゲーション制御プロトコル (LACP) は、vPC の LACP アグリゲーショングループ (LAG) ID を形成するために、vPC ドメインのシステム MAC アドレスを使用します。

ダウンストリームスイッチからのチャンネルも含めて、すべての vPC EtherChannel 上の LACP を使用できます。LACP は、vPC ピアスイッチの各 EtherChannel 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、スイッチ、単一方向リンク、およびマルチホップ接続の間の互換性をより簡単に検出できるようになり、実行時の変更およびリンク障害に対してダイナミックな応答が可能になります。

vPC ピアリンクは、16 の EtherChannel インターフェイスをサポートします。



(注) システムプライオリティを手動で設定する場合は、必ず両方の vPC ピアスイッチ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 ピアスイッチ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

最初に vPC 機能を起動したときに、STP が再収束します。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 STP 拡張機能を一切イネーブルにしないことも推奨します。

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 スイッチ 上で同じになるように設定する必要があります。

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 スイッチ 上で実行され続けます。ただし、プライマリ スイッチ として選択されている vPC ピア スイッチ 上での設定が、セカンダリ vPC ピア スイッチ 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 スイッチは、Cisco Fabric Services over Ethernet (CFS over E) を使用して、vPC セカンダリ ピア スイッチ 上の STP の状態を同期させます。

vPC マネージャが、vPC ピア スイッチ 間で、プライマリ スイッチ とセカンダリ スイッチ を設定して 2 つのスイッチを STP 用に調整する提案/ハンドシェイク合意を実行します。次に、プライマリ vPC ピア スイッチ が、プライマリ スイッチ とセカンダリ スイッチ の両方の vPC インターフェイスの STP プロトコルの制御を行います。

ブリッジプロトコルデータユニット (BPDU) は、指定ブリッジ 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 スイッチ が、vPC インターフェイス 上でこれらの BPDU を送信します。



---

(注) vPC ピア リンクの両側での設定を表示して、設定が同じであることを確認してください。vPC に関する情報を表示するには、**show spanning-tree** コマンドを使用します。

---

## CFS over E

Cisco Fabric Services over Ethernet (CFS over E) 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する信頼性の高い状態転送メカニズムです。CFS over E 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/CFS over E プロトコルデータユニット (PDU) に入れて伝送されます。

CFS over E 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 CFS over E 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。CFS over E 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。

**show mac address-table** コマンドを使用すれば、CFS over E が vPC ピア リンクのために同期する MAC アドレスを表示できます。



---

(注) **no cfs eth distribute** コマンドまたは **no cfs distribute** コマンドを入力しないでください。CFS over E は、vPC 機能に対してイネーブルにする必要があります。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システムによって表示されます。

---

**show cfs application** コマンドを入力すると、出力に「Physical-eth」と表示されます。これは、CFSoE を使用しているアプリケーションを示します。

## vPC の注意事項および制約事項

vPC には、次の注意事項と制約事項があります。

- vPC ピアリンクおよび vPC インターフェイスを設定する前に、vPC 機能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、その前にピアキーブアライブリンクを設定する必要があります。
- vPC ピアリンクは、少なくとも 2 台の 10 ギガビットイーサネットインターフェイスを使用して形成する必要があります。
- シスコでは、両方のピアに同じ vPC ドメイン ID を設定し、ドメイン ID をネットワークで一意にすることを推奨します。たとえば、2 つの異なる vPC (1 つがアクセスで 1 つが集約) がある場合は、各 vPC には、一意のドメイン ID がある必要があります。
- vPC に入れられるのは、ポートチャネルだけです。vPC は標準ポートチャネル (スイッチ間の vPC トポロジ) およびポートチャネルホストインターフェイス (ホストインターフェイスの vPC トポロジ) で設定できます。
- 両方の vPC ピアスイッチを設定する必要があります。設定は、vPC ピアデバイス間で自動的に同期されません。
- 必要な設定パラメータが、vPC ピアリンクの両側で互換性を保っているかチェックしてください。
- 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。
- アクティブモードのインターフェイスで LACP を使用して vPC のすべてのポートチャネルを設定する必要があります。

## vPC の設定

### vPC のイネーブル化

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

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>feature vpc</b>	スイッチで vPC をイネーブルにします。
ステップ 3	switch# <b>show feature</b>	(任意) スイッチ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 4	switch# <b>copy running-config startup-config</b>	(任意) 実行コンフィギュレーションを、ス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
```

## vPC のディセーブル化

vPC 機能をディセーブルにできます。



(注) vPC 機能をディセーブルにすると、Cisco Nexus 3000 シリーズ スイッチがすべての vPC 設定をクリアします。

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>no feature vpc</b>	スイッチの vPC をディセーブルにします。
ステップ 3	switch# <b>show feature</b>	(任意) スイッチ上でイネーブルになっている機能を表示します。

	コマンドまたはアクション	目的
ステップ 4	switch# <b>copy running-config startup-config</b>	(任意) 実行コンフィギュレーションを、ス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
```

## vPC ドメインの作成

両方の vPC ピア デバイスで、同じ vPC ドメイン ID を作成する必要があります。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ために使用されます。

### 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。

次の手順に従って、vPC ピア リンクの両側に両方のスイッチを設定する必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>vpc domain domain-id</b>	スイッチで vPC ドメインを作成し、 <b>vpc-domain</b> 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 <i>domain-id</i> はありません。範囲は 1 ~ 1000 です。  (注) 既存の vPC ドメインの <b>vpc-domain</b> コンフィギュレーションモードを開始するには、 <b>vpc domain</b> コマンドも使用できます。
ステップ 3	switch# <b>show vpc brief</b>	(任意) 各 vPC ドメインに関する要約情報を表示します。
ステップ 4	switch# <b>copy running-config startup-config</b>	(任意) 実行コンフィギュレーションを、ス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
```

## vPC キープアライブリンクと vPC キープアライブメッセージの設定

キープアライブメッセージを伝送するピアキープアライブリンクの宛先 IP を設定できます。必要に応じて、キープアライブメッセージのその他のパラメータも設定できます。

Cisco NX-OS ソフトウェアは、vPC ピア間でピアキープアライブリンクを使用して、設定可能なキープアライブメッセージを定期的送信します。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接続が必要です。ピアキープアライブリンクが起動および動作していないと、システムは vPC ピアリンクを開始できません。

ピアキープアライブメッセージに使用される送信元 IP アドレスと宛先の IP アドレスの両方が、ネットワーク内で一意であることを確認してください。また、vPC ピアキープアライブリンクに関連付けられている Virtual Routing and Forwarding (VRF; 仮想ルーティングおよび転送) から、これらの IP アドレスが到達可能であることを確認してください。



(注) vPC ピアキープアライブリンクを使用する際は、個別の VRF インスタンスを設定して、各 vPC ピアスイッチからその VRF にレイヤ3ポートを接続することを推奨します。ピアリンク自体を使用して vPC ピアキープアライブメッセージを送信しないでください。

### 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。

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。

次の手順に従って、vPC ピアリンクの両側に両方のスイッチを設定する必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# <b>vpc domain domain-id</b>	スイッチの vPC ドメインがまだない場合は作成し、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	switch(config-vpc-domain)# <b>peer-keepalive destination ipaddress</b> [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	vPC ピアキープアライブリンクのリモートエンドの IPv4 アドレスを設定します。  (注) vPC ピアキープアライブリンクを設定するまでは、vPC ピアリンクはシステムによって形成されません。 管理ポートと VRF がデフォルトです。

	コマンドまたはアクション	目的
	<code>ipaddress   vrf {name   management vpc-keepalive}]</code>	
ステップ 4	<code>switch(config-vpc-domain)# vpc peer-keepalive destination ipaddress source ipaddress</code>	(任意) vPC ピアキープアライブリンクを使用する際は、個別のVRFインスタンスを設定して、各vPCピアデバイスからそのVRFにレイヤ3ポートを接続します。
ステップ 5	<code>switch# show vpc peer-keepalive</code>	(任意) キープアライブメッセージのコンフィギュレーションに関する情報を表示します。
ステップ 6	<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 ピアキープアライブリンクの宛先 IP アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# peer-keepalive destination 10.10.10.42
```

次に、プライマリとセカンダリのvPCデバイス間でピアキープアライブリンク接続を設定する例を示します。

```
switch(config)# vpc domain 100
switch(config-vpc-domain)# peer-keepalive destination 192.168.2.2 source 192.168.2.1
Note:-----:: Management VRF will be used as the default VRF ::-----
switch(config-vpc-domain)#
```

次に、vPC キープアライブリンクに vpc\_keepalive という名前の別のVRFを作成し、新規VRFを確認する例を示します。

次に、vPC キープアライブリンクに vpc\_keepalive という名前の別のVRFを作成し、新規VRFを確認する例を示します。

```
vrf context vpc_keepalive
interface Ethernet1/31
  switchport access vlan 123
interface Vlan123
  vrf member vpc_keepalive
  ip address 123.1.1.2/30
  no shutdown
vpc domain 1
  peer-keepalive destination 123.1.1.1 source 123.1.1.2 vrf
  vpc_keepalive
```

```
L3-NEXUS-2# sh vpc peer-keepalive
```

```
vPC keep-alive status           : peer is alive
--Peer is alive for             : (154477) seconds, (908) msec
--Send status                   : Success
--Last send at                  : 2011.01.14 19:02:50 100 ms
--Sent on interface             : Vlan123
```

```

--Receive status          : Success
--Last receive at        : 2011.01.14 19:02:50 103 ms
--Received on interface  : Vlan123
--Last update from peer  : (0) seconds, (524) msec

vPC Keep-alive parameters
--Destination            : 123.1.1.1
--Keepalive interval     : 1000 msec
--Keepalive timeout      : 5 seconds
--Keepalive hold timeout : 3 seconds
--Keepalive vrf          : vpc_keepalive
--Keepalive udp port     : 3200
--Keepalive tos          : 192

The services provided by the switch , such as ping, ssh, telnet,
radius, are VRF aware. The VRF name need to be configured or
specified in order for the correct routing table to be used.
L3-NEXUS-2# ping 123.1.1.1 vrf vpc_keepalive
PING 123.1.1.1 (123.1.1.1): 56 data bytes
64 bytes from 123.1.1.1: icmp_seq=0 ttl=254 time=3.234 ms
64 bytes from 123.1.1.1: icmp_seq=1 ttl=254 time=4.931 ms
64 bytes from 123.1.1.1: icmp_seq=2 ttl=254 time=4.965 ms
64 bytes from 123.1.1.1: icmp_seq=3 ttl=254 time=4.971 ms
64 bytes from 123.1.1.1: icmp_seq=4 ttl=254 time=4.915 ms

--- 123.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 3.234/4.603/4.971 ms

```

## 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 EtherChannel を各スイッチ上で指定します。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する EtherChannel を設定し、各 vPC ピアスイッチで個別のモジュールの 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。

次の手順に従って、vPC ピアリンクの両側に両方のスイッチを設定する必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# <b>interface port-channel channel-number</b>	このスイッチの vPC ピアリンクとして使用する EtherChannel を選択し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 3	switch(config-if)# <b>vpc peer-link</b>	選択した EtherChannel 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。

	コマンドまたはアクション	目的
ステップ 4	switch# <b>show vpc brief</b>	(任意) vPC ピアリンクに関する情報など、各 vPC の情報を表示します。
ステップ 5	switch# <b>copy running-config startup-config</b>	(任意) 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

次の例は、vPC ピアリンクを設定する方法を示します。

```
switch# configure terminal
switch(config)# interface port-channel 20
switch(config-if)# vpc peer-link
```

## 設定の互換性チェック

両方の vPC ピアスイッチ上の 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。



(注) 次の QoS パラメータはタイプ 2 整合性検査をサポートします。

- ネットワーク QoS : [MTU] および [Pause]
- 入力キューイング : [Bandwidth] および [Absolute Priority]
- 出力キューイング : [Bandwidth] および [Absolute Priority]

タイプ 2 の不一致の場合、vPC は一時停止されません。タイプ 1 の不一致は、vPC を一時停止します。

パラメータ	デフォルト設定
switch# <b>show vpc consistency-parameters {global   interface port-channel channel-number}</b>	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# show vpc consistency-parameters global
Legend:
      Type 1 : vPC will be suspended in case of mismatch
Name      Type  Local Value      Peer Value
-----
QoS              2      ([], [], [], [], [], ([], [], [], [], [],
                [])
```

```

Network QoS (MTU)                2      (1538, 0, 0, 0, 0, 0)  (1538, 0, 0, 0, 0, 0)
Network QoS (Pause)              2      (F, F, F, F, F, F)    (1538, 0, 0, 0, 0, 0)
Input Queuing (Bandwidth)        2      (100, 0, 0, 0, 0, 0)  (100, 0, 0, 0, 0, 0)
Input Queuing (Absolute Priority) 2      (F, F, F, F, F, F)    (100, 0, 0, 0, 0, 0)
Output Queuing (Bandwidth)       2      (100, 0, 0, 0, 0, 0)  (100, 0, 0, 0, 0, 0)
Output Queuing (Absolute Priority) 2      (F, F, F, F, F, F)    (100, 0, 0, 0, 0, 0)
STP Mode                          1      Rapid-PVST             Rapid-PVST
STP Disabled                       1      None                   None
STP MST Region Name                1      ""                      ""
STP MST Region Revision            1      0                       0
STP MST Region Instance to VLAN Mapping 1
STP Loopguard                      1      Disabled               Disabled
STP Bridge Assurance               1      Enabled                 Enabled
STP Port Type, Edge                1      Normal, Disabled,     Normal, Disabled,
BPDUFilter, Edge BPDUGuard         Disabled                Disabled
STP MST Simulate PVST              1      Enabled                 Enabled
Allowed VLANs                      -      1,624                  1
Local suspended VLANs              -      624                     -
switch#
    
```

## vPC 自動リカバリのイネーブル化

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# <b>vpc domain domain-id</b>	既存の vPC ドメインの 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	switch(config-vpc-domain)# <b>auto-recovery reload-delay delay</b>	自動リカバリ機能をイネーブルにし、リロード遅延期間を設定します。デフォルトはディセーブルです。

次の例は、vPC ドメイン 10 で自動リカバリ機能をイネーブルにし、遅延時間を 240 秒に設定する方法を示したものです。

```

switch(config)# vpc domain 10
switch(config-vpc-domain)# auto-recovery reload-delay 240
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
    
```

次の例は、vPC ドメイン 10 における自動リカバリ機能のステータスを表示する方法を示したものです。

```

switch(config-vpc-domain)# show running-config vpc
!Command: show running-config vpc
!Time: Tue Dec 7 02:38:44 2010
    
```

```

version 5.0(3)U2(1)
feature vpc
vpc domain 10
  peer-keepalive destination 10.193.51.170
  auto-recovery

```

## 復元遅延時間の設定

ピアの隣接が形成され、VLAN インターフェイスがバックアップされるまで、vPC の再稼働を遅らせるように復元タイマーをユーザは設定できます。この機能により、vPC が再びトラフィックの受け渡しをしはじめる前にルーティングテーブルが収束できなかった場合のパケットのドロップを回避できます。

### 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。

次の手順に従って、vPC ピア リンクの両側に両方のスイッチを設定する必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# <b>vpc domain domain-id</b>	スイッチの vPC ドメインがまだない場合は作成し、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	switch(config-vpc-domain)# <b>delay restore time</b>	vPC が復元されるまでの遅延時間を設定します。復元時間は、復元された vPC ピア デバイスの起動を遅らせる秒数です。有効な範囲は 1 ~ 3600 です。デフォルトは 30 秒です。
ステップ 4	switch# <b>copy running-config startup-config</b>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

次に、vPC リンクにリロードの遅延時間を設定する例を示します。

```

switch(config)# vpc domain 1
switch(config-vpc-domain)# delay restore 10
switch(config-vpc-domain)#

```

## vPC ピア リンク障害時のシャットダウンからの VLAN インターフェイスの除外

vPC ピア リンクが失われた場合、vPC セカンダリ スイッチがその vPC メンバ ポートとその SVI インターフェイスを一時停止します。すべてのレイヤ 3 転送は、vPC セカンダリ スイッチ上のすべての VLAN でディセーブルになります。特定の SVI インターフェイスを除外して、一時停止されないようにできます。

### はじめる前に

VLAN インターフェイスが設定されていることを確認します。

- 

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>vpc domain domain-id</b>	スイッチの vPC ドメインがまだない場合は作成し、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	switch(config-vpc-domain)# <b>dual-active exclude interface-vlan range</b>	vPC ピア リンクが失われた場合に、アップのままにする必要がある VLAN インターフェイスを指定します。  range : シャットダウンから除外する VLAN インターフェイスの範囲。範囲は 1 ~ 4094 です。

次に、ピア リンクに障害が発生した場合に、vPC ピア スイッチの VLAN 10 インターフェイスをアップのままにする例を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# dual-active exclude interface-vlan 10
switch(config-vpc-domain)#
```

## VRF 名の設定

ping、ssh、telnet、radius などのスイッチ サービスは、VRF を認識します。正しいルーティング テーブルが使用されるようにするために、VRF 名を設定する必要があります。

VRF 名を指定できます。

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>ping ipaddress vrf vrf-name</b>	使用する仮想ルーティングおよび転送 (VRF) を指定します。VRF 名は最大 32 文字で、大文字と小文字が区別されます。

次の例は、vpc\_keepalive という名前の VRF を指定する方法を示したものです。

```
switch# ping 123.1.1.1 vrf vpc_keepalive
PING 123.1.1.1 (123.1.1.1): 56 data bytes
64 bytes from 123.1.1.1: icmp_seq=0 ttl=254 time=3.234 ms
64 bytes from 123.1.1.1: icmp_seq=1 ttl=254 time=4.931 ms
64 bytes from 123.1.1.1: icmp_seq=2 ttl=254 time=4.965 ms
64 bytes from 123.1.1.1: icmp_seq=3 ttl=254 time=4.971 ms
64 bytes from 123.1.1.1: icmp_seq=4 ttl=254 time=4.915 ms

--- 123.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 3.234/4.603/4.971 ms
```

## vPC への VRF インスタンスのバインド

vPC に VRF インスタンスをバインドできます。VRF ごとに 1 つの予約済み VLAN が必要です。このコマンドを使用しないと、非 vPC VLAN のレシーバおよびレイヤ 3 インターフェイスに接続されているレシーバがマルチキャストトラフィックを受信しない可能性があります。非 vPC VLAN は、ピアリンクにトランクされない VLAN です。

### はじめる前に

スイッチで使用されているインターフェイスを表示するには、**show interfaces brief** コマンドを使用します。vPC に VRF をバインドするには、使用されていない VLAN を使用する必要があります。

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# <b>vpc bind-vrf vrf-name vlan vlan-id</b>	VRF インスタンスを vPC にバインドし、vPC にバインドする VLAN を指定します。VLAN ID の範囲は 1 ~ 3967 および 4049 ~ 4093 です。

次に、VLAN 2 を使用してデフォルトの VRF に vPC をバインドする例を示します。

```
switch(config)# vpc bind-vrf default vlan vlan2
```

## 他のポートチャネルのvPCへの移行

### 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。

次の手順に従って、vPCピアリンクの両側に両方のスイッチを設定する必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# <b>interface port-channel channel-number</b>	ダウンストリームスイッチに接続するためにvPCに入れるポートチャネルを選択し、インターフェイスコンフィギュレーションモードを開始します。  (注) vPCは、標準ポートチャネル(物理的なvPCトポロジ)およびポートチャネルのホストインターフェイス(ホストインターフェイスのvPCトポロジ)で設定できます。
ステップ 3	switch(config-if)# <b>vpc number</b>	選択したポートチャネルをvPCに入れてダウンストリームスイッチに接続するように設定します。指定できる範囲は1～4096です。  vPCピアスイッチからダウンストリームスイッチに接続しているポートチャネルに割り当てるvPC numberは、両方のvPCピアスイッチで同じでなければなりません。
ステップ 4	switch# <b>show vpc brief</b>	(任意) 各vPCに関する情報を表示します。
ステップ 5	switch# <b>copy running-config startup-config</b>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

次の例は、ダウンストリームデバイスに接続されるポートチャネルを設定する方法を示します。

```
switch# configure terminal
switch(config)# interface port-channel 20
switch(config-if)# vpc 5
```

## vPC ドメイン MAC アドレスの手動での設定



(注) `system-mac` の設定は、オプションの設定手順です。ここでは、必要な場合にそれを設定する方法について説明します。

### 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。

次の手順に従って、vPC ピア リンクの両側に両方のスイッチを設定する必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>vpc domain</b> <i>domain-id</i>	スイッチの既存の vPC ドメインを選択するか、新しい vPC ドメインを作成し、 <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 <i>domain-id</i> はありません。範囲は 1 ~ 1000 です。
ステップ 3	switch(config-vpc-domain)# <b>system-mac mac-address</b>	指定した vPC ドメインに割り当てる MAC アドレスを <code>aaaa.bbbb.cccc</code> の形式で入力します。
ステップ 4	switch# <b>show vpc role</b>	(任意) vPC システム MAC アドレスを表示します。
ステップ 5	switch# <b>copy running-config</b> <b>startup-config</b>	(任意) 実行コンフィギュレーションを、ス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 MAC アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-if)# system-mac 23fb.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。

## 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。

次の手順に従って、vPC ピア リンクの両側に両方のスイッチを設定する必要があります。

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>vpc domain domain-id</b>	スイッチの既存の vPC ドメインを選択するか、新しい vPC ドメインを作成し、vpc-domain コンフィギュレーション モードを開始します。デフォルト domain-id はありません。範囲は 1 ~ 1000 です。
ステップ 3	switch(config-vpc-domain)# <b>system-priority priority</b>	指定した vPC ドメインに割り当てるシステム プライオリティを入力します。指定できる値の範囲は、1 ~ 65535 です。デフォルト値は 32667 です。
ステップ 4	switch# <b>show vpc brief</b>	(任意) vPC ピア リンクに関する情報など、各 vPC の情報を表示します。
ステップ 5	switch# <b>copy running-config startup-config</b>	(任意) 実行コンフィギュレーションを、スタートアップ 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)# vpc domain 5
switch(config-if)# system-priority 4000
```

## vPC ピア スイッチ ロールの手動での設定

デフォルトでは、vPC ドメインおよび vPC ピア リンクの両側を設定した後、Cisco NX-OS ソフトウェアによってプライマリおよびセカンダリ vPC ピア スイッチが選択されます。ただし、vPC のプライマリ スイッチとして、特定の vPC ピア スイッチを選択することもできます。その場合、プライマリ スイッチにする vPC ピア スイッチに、他の vPC ピア スイッチより小さいロール値を手動で設定します。

vPC はロールのプリエンプションをサポートしていません。プライマリ vPC ピア スイッチに障害が発生すると、セカンダリ vPC ピア スイッチが、vPC プライマリ スイッチの機能を引き継ぎます。ただし、以前のプライマリ vPC が再稼働しても、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。

次の手順に従って、vPC ピア リンクの両側に両方のスイッチを設定する必要があります。

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>vpc domain domain-id</b>	スイッチの既存の vPC ドメインを選択するか、新しい vPC ドメインを作成し、vpc-domain コンフィギュレーション モードを開始します。デフォルト domain-id はありません。範囲は 1 ~ 1000 です。
ステップ 3	switch(config-vpc-domain)# <b>role priority priority</b>	vPC システム プライオリティに割り当てるロール プライオリティを入力します。指定できる値の範囲は、1 ~ 65535 です。デフォルト値は 32667 です。
ステップ 4	switch# <b>show vpc brief</b>	(任意) vPC ピア リンクに関する情報など、各 vPC の情報を表示します。
ステップ 5	switch# <b>copy running-config startup-config</b>	(任意) 実行コンフィギュレーションを、スタートアップ 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)# vpc domain 5
switch(config-if)# role priority 4000
```

## vPC 設定の確認

vPC の設定情報を表示するには、次のコマンドを使用します。

コマンド	目的
switch# <b>show feature</b>	vPC がイネーブルになっているかどうかを表示します。

コマンド	目的
switch# <b>show port-channel capacity</b>	スイッチで設定されている EtherChannel の数、およびまだ使用可能なポートチャネル数を表示します。
switch# <b>show running-config vpc</b>	vPC の実行コンフィギュレーションの情報を表示します。
switch# <b>show vpc brief</b>	vPC に関する簡単な情報を表示します。
switch# <b>show vpc consistency-parameters</b>	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。
switch# <b>show vpc peer-keepalive</b>	ピアキープアライブメッセージの情報を表示します。
switch# <b>show vpc role</b>	ピアステータス、ローカルスイッチのロール、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 スwitch の MAC アドレスとプライオリティを表示します。
switch# <b>show vpc statistics</b>	vPC に関する統計情報を表示します。  (注) このコマンドは、現在作業している vPC ピア デバイスの vPC 統計情報しか表示しません。

スイッチの出力の詳細については、使用する Cisco Nexus シリーズ スwitch のコマンドリファレンスを参照してください。

## グレースフルタイプ1チェックステータスの表示

グレースフルタイプ1整合性検査の現在のステータスを表示する場合は、**show vpc brief** コマンドを入力します。

```
switch# show vpc brief
Legend:
      (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id           : 10
Peer status              : peer adjacency formed ok
vPC keep-alive status   : peer is alive
Configuration consistency status: success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role                 : secondary
Number of vPCs configured : 34
Peer Gateway             : Disabled
Dual-active excluded VLANs : -
```

```
Graceful Consistency Check      : Enabled
```

```
vPC Peer-link status
```

```
-----
id   Port   Status Active vlans
-----
1    Po1    up      1
-----
```

## グローバルタイプ1不整合の表示

グローバルタイプ1の不整合が発生すると、セカンダリスイッチでvPCがダウンします。次の例に、スパンニングツリーモードの不一致がある場合のこのタイプの不整合を示します。

一時停止したvPC VLANのステータスを表示する場合は、セカンダリスイッチに対して **show vpc** コマンドを入力します。

```
switch(config)# show vpc
```

```
Legend:
```

```
(*) - local vPC is down, forwarding via vPC peer-link
```

```
vPC domain id           : 10
Peer status             : peer adjacency formed ok
vPC keep-alive status   : peer is alive
Configuration consistency status: failed
Per-vlan consistency status : success
Configuration consistency reason: vPC type-1 configuration incompatible - STP
                               Mode inconsistent
Type-2 consistency status : success
vPC role                 : secondary
Number of vPCs configured : 2
Peer Gateway             : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
```

```
vPC Peer-link status
```

```
-----
id   Port   Status Active vlans
-----
1    Po1    up      1-10
-----
```

```
vPC status
```

```
-----
id   Port   Status Consistency Reason Active vlans
-----
20   Po20   down*  failed   Global compat check failed -
30   Po30   down*  failed   Global compat check failed -
-----
```

不整合のステータスを表示する場合は、プライマリスイッチに対して **show vpc** コマンドを入力します（プライマリvPCのVLANは一時停止しません）。

```
switch(config)# show vpc
```

```
Legend:
```

```
(*) - local vPC is down, forwarding via vPC peer-link
```

```
vPC domain id           : 10
Peer status             : peer adjacency formed ok
vPC keep-alive status   : peer is alive
Configuration consistency status: failed
Per-vlan consistency status : success
Configuration consistency reason: vPC type-1 configuration incompatible - STP Mode inconsistent
Type-2 consistency status : success
vPC role                 : primary
Number of vPCs configured : 2
Peer Gateway             : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
```

```
vPC Peer-link status
-----
id   Port   Status Active vlans
--   -
1    Po1    up    1-10

vPC status
-----
id   Port   Status Consistency Reason                Active vlans
--   -
20   Po20   up    failed    Global compat check failed 1-10
30   Po30   up    failed    Global compat check failed 1-10
```

## インターフェイス固有のタイプ1不整合の表示

インターフェイス固有のタイプ1不整合が発生すると、プライマリスイッチのvPCポートはアップ状態のままセカンダリスイッチのvPCポートはダウンします。次の例では、スイッチポートモードの不一致がある場合のこのタイプの不整合を示します。

一時停止したvPC VLANのステータスを表示する場合は、セカンダリスイッチに対して **show vpc brief** コマンドを入力します。

```
switch(config-if)# show vpc brief
Legend:
      (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id           : 10
Peer status             : peer adjacency formed ok
vPC keep-alive status   : peer is alive
Configuration consistency status: success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role                 : secondary
Number of vPCs configured : 2
Peer Gateway            : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled

vPC Peer-link status
-----
id   Port   Status Active vlans
--   -
1    Po1    up    1

vPC status
-----
id   Port   Status Consistency Reason                Active vlans
--   -
20   Po20   up    success    success                1
30   Po30   down* failed    Compatibility check failed -
                               for port mode
```

不整合のステータスを表示する場合は、プライマリスイッチに対して **show vpc brief** コマンドを入力します（プライマリvPCのVLANは一時停止しません）。

```
switch(config-if)# show vpc brief
Legend:
      (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id           : 10
Peer status             : peer adjacency formed ok
vPC keep-alive status   : peer is alive
Configuration consistency status: success
Per-vlan consistency status : success
```

```

Type-2 consistency status      : success
vPC role                       : primary
Number of vPCs configured     : 2
Peer Gateway                   : Disabled
Dual-active excluded VLANs    : -
Graceful Consistency Check    : Enabled

vPC Peer-link status
-----
id   Port   Status Active vlans
--   -
1    Po1    up     1

vPC status
-----
id   Port   Status Consistency Reason              Active vlans
--   -
20   Po20   up     success      success                          1
30   Po30   up     failed       Compatibility check failed 1
                                         for port mode

```

## VLAN ごとの整合ステータスの表示

VLAN ごとの整合または不整合のステータスを表示するには、**show vpc consistency-parameters vlans** コマンドを入力します。

次の例では最初に、不整合が発生する前の（整合性がある状態での）VLAN のステータスが表示されています。その後で **no spanning-tree vlan 5** コマンドを入力することにより、プライマリスイッチとセカンダリスイッチとの間に不整合が生じます。

**show vpc brief** コマンドを実行して、プライマリスイッチおよびセカンダリスイッチのVLANの整合性ステータスを表示します。

```

switch(config-if)# show vpc brief
Legend:
          (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                  : 10
Peer status                    : peer adjacency formed ok
vPC keep-alive status          : peer is alive
Configuration consistency status: success
Per-vlan consistency status    : success
Type-2 consistency status     : success
vPC role                       : secondary
Number of vPCs configured     : 2
Peer Gateway                   : Disabled
Dual-active excluded VLANs    : -
Graceful Consistency Check    : Enabled

vPC Peer-link status
-----
id   Port   Status Active vlans
--   -
1    Po1    up     1-10

vPC status
-----
id   Port   Status Consistency Reason              Active vlans
--   -
20   Po20   up     success      success                          1-10
30   Po30   up     success      success                          1-10

```

**no spanning-tree vlan 5** コマンドを実行することにより、プライマリ VLAN とセカンダリ VLAN との間に不整合が生じます。

```
switch(config)# no spanning-tree vlan 5
```

セカンダリ スイッチに対して **show vpc brief** コマンドを実行すると、VLAN ごとの整合性ステータスが **Failed** と表示されます。

```
switch(config)# show vpc brief
Legend:
          (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id          : 10
Peer status            : peer adjacency formed ok
vPC keep-alive status  : peer is alive
Configuration consistency status: success
Per-vlan consistency status : failed
Type-2 consistency status : success
vPC role               : secondary
Number of vPCs configured : 2
Peer Gateway          : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled

vPC Peer-link status
-----
id   Port   Status Active vlans
--   -
1    Po1    up    1-4,6-10

vPC status
-----
id   Port   Status Consistency Reason          Active vlans
-----
20   Po20   up    success    success    1-4,6-10
30   Po30   up    success    success    1-4,6-10
```

プライマリ スイッチに対して **show vpc brief** コマンドを実行しても、VLAN ごとの整合性ステータスが **Failed** と表示されます。

```
switch(config)# show vpc brief
Legend:
          (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id          : 10
Peer status            : peer adjacency formed ok
vPC keep-alive status  : peer is alive
Configuration consistency status: success
Per-vlan consistency status : failed
Type-2 consistency status : success
vPC role               : primary
Number of vPCs configured : 2
Peer Gateway          : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled

vPC Peer-link status
-----
id   Port   Status Active vlans
--   -
1    Po1    up    1-4,6-10

vPC status
-----
id   Port   Status Consistency Reason          Active vlans
-----
20   Po20   up    success    success    1-4,6-10
30   Po30   up    success    success    1-4,6-10
```

次の例では、STP Disabled という不整合が表示されています。

```
switch(config)# show vpc consistency-parameters vlans
```

Name	Type	Reason Code	Pass Vlans
-----	----	-----	-----
STP Mode	1	success	0-4095
<b>STP Disabled</b>	<b>1</b>	<b>vPC type-1 configuration incompatible - STP is enabled or disabled on some or all vlans</b>	<b>0-4,6-4095</b>
STP MST Region Name	1	success	0-4095
STP MST Region Revision	1	success	0-4095
STP MST Region Instance to VLAN Mapping	1	success	0-4095
STP Loopguard	1	success	0-4095
STP Bridge Assurance	1	success	0-4095
STP Port Type, Edge	1	success	0-4095
BPDUGuard, Edge BPDUGuard	1	success	0-4095
STP MST Simulate PVST	1	success	0-4095
Pass Vlans	-		0-4,6-4095

## vPC のデフォルト設定

次の表に、vPC パラメータのデフォルト設定を示します。

表 4: デフォルト vPC パラメータ

パラメータ	デフォルト
vPC システム プライオリティ	32667
vPC ピアキープアライブ メッセージ	ディセーブル
vPC ピアキープアライブ間隔	1 秒
vPC ピアキープアライブ タイムアウト	5 秒
vPC ピアキープアライブ UDP ポート	3200



## 索引

### L

- LACP [20, 24, 25, 27, 28, 31, 34, 36](#)
  - システム ID [25](#)
  - 設定 [31](#)
  - ポート チャンネル [24](#)
  - ポート チャンネル、MinLink [28, 34](#)
  - ポート プライオリティ [36](#)
  - マーカー レスポンダ [27](#)
- LACP がイネーブル対スタティック [27](#)
  - ポート チャンネル [27](#)
- LACP の設定 [31](#)

### M

- MIB [18](#)
  - レイヤ 3 インターフェイス [18](#)

### S

- STP [19](#)
  - ポート チャンネル [19](#)

### V

- VLAN [5](#)
  - インターフェイス [5](#)
- VLAN インターフェイス [10](#)
  - 設定 [10](#)
- vPC [52, 63](#)
  - 注意事項および制約事項 [52](#)
  - ポート チャンネルの移行 [63](#)
- VRF [13](#)
  - インターフェイスの割り当て [13](#)

### い

- インターフェイス [3, 4, 5, 6, 9, 10, 12, 13, 15, 17](#)
  - VLAN [5, 10](#)
    - 設定 [10](#)
  - VRF への割り当て [13](#)
  - 帯域幅の設定 [9](#)
  - トンネル [6](#)
  - ルーテッド [4](#)
  - ループバック [6, 12](#)
  - レイヤ 3 [3, 15, 17](#)
    - 設定例 [17](#)
    - モニタリング [15](#)
- インバンド管理 [11](#)
  - 設定 [11](#)

### か

- 確認 [14](#)
  - レイヤ 3 インターフェイス設定 [14](#)
- 管理 [11](#)
  - インバンド [11](#)
    - 設定 [11](#)
- 関連資料 [17](#)
  - レイヤ 3 インターフェイス [17](#)

### き

- 機能の履歴 [18, 39](#)
  - ポート チャンネル [39](#)
  - レイヤ 3 インターフェイス [18](#)

## さ

サブインターフェイス [4, 8, 9](#)  
 設定 [8](#)  
 帯域幅の設定 [9](#)

## し

新機能に関する情報 [1](#)  
 説明 [1](#)

## せ

設定 [7, 8, 9, 10, 11, 12, 14](#)  
 VLAN インターフェイス [10](#)  
 インターフェイス帯域幅 [9](#)  
 インバンド管理 [11](#)  
 サブインターフェイス [8](#)  
 ルーテッド インターフェイス [7](#)  
 ループバック インターフェイス [12](#)  
 レイヤ 3 インターフェイス [14](#)  
 確認 [14](#)  
 設定例 [17](#)  
 レイヤ 3 インターフェイス [17](#)

## た

帯域幅 [9](#)  
 設定 [9](#)

## ち

チャンネルモード [26, 32](#)  
 ポートチャンネル [26, 32](#)  
 注意事項および制約事項 [7, 52](#)  
 vPC [52](#)  
 レイヤ 3 インターフェイス [7](#)

## て

デフォルト設定 [7](#)  
 レイヤ 3 インターフェイス [7](#)

## と

トンネル インターフェイス [6](#)

## は

ハードウェア ハッシュ [31](#)  
 マルチキャスト トラフィック [31](#)

## ひ

標準 [18](#)  
 レイヤ 3 インターフェイス [18](#)

## へ

変更された機能に関する情報 [1](#)  
 説明 [1](#)

## ほ

ポート チャネリング [20](#)  
 ポート チャネル [9, 19, 21, 22, 24, 27, 28, 29, 30, 31, 32, 37, 39, 63](#)  
 LACP [24](#)  
 LACP がイネーブル対スタティック [27](#)  
 STP [19](#)  
 vPC への移行 [63](#)  
 機能の履歴 [39](#)  
 互換性要件 [21](#)  
 作成 [28](#)  
 設定の確認 [37](#)  
 帯域幅の設定 [9](#)  
 チャンネルモード [32](#)  
 ハードウェア ハッシュ [31](#)  
 ポートの追加 [29](#)  
 ロード バランシング [22, 30](#)  
 ポート チャネル [22](#)  
 ポート チャネル、MinLink [28, 34](#)  
 LACP [28, 34](#)  
 ポートの追加 [29](#)  
 ポート チャネル [29](#)

## ま

- マルチキャスト トラフィック [31](#)
  - ハードウェア ハッシュ [31](#)
  - ポート チャネル [31](#)

## も

- モニタリング [15](#)
  - レイヤ 3 インターフェイス [15](#)

## ら

- ライセンス要件 [6](#)
  - レイヤ 3 インターフェイス [6](#)

## る

- ルーテッド インターフェイス [4,7,9](#)
  - 設定 [7](#)
  - 帯域幅の設定 [9](#)
- ループバック インターフェイス [6,12](#)
  - 設定 [12](#)

## れ

- レイヤ 3 インターフェイス [3,6,7,14,15,17,18](#)
  - MIB [18](#)
  - インターフェイス [17,18](#)
    - レイヤ 3 [17,18](#)
    - MIB [18](#)
    - 関連資料 [17](#)
    - 機能の履歴 [18](#)
    - 標準 [18](#)
  - 確認 [14](#)
  - 関連資料 [17](#)
  - 機能の履歴 [18](#)
  - 設定例 [17](#)
  - 注意事項および制約事項 [7](#)
  - デフォルト設定 [7](#)
  - 標準 [18](#)
  - モニタリング [15](#)
  - ライセンス要件 [6](#)
  - ルーテッド インターフェイスの設定 [7](#)

## ろ

- ロード バランシング [30](#)
  - ポート チャネル [30](#)
    - 設定 [30](#)

