



## **Cisco Nexus 3600 NX-OS インターフェイス設定ガイド、リリース 10.2(x)**

初版：2021年8月23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/>





## 目次

---

はじめに :

はじめに ix

対象読者 ix

表記法 ix

Cisco Nexus 3600 プラットフォーム スイッチの関連資料 x

マニュアルに関するフィードバック xi

通信、サービス、およびその他の情報 xi

---

第 1 章

新規および変更情報 1

新規および変更情報 1

---

第 2 章

レイヤ 2 インターフェイスの設定 3

ライセンス要件 3

イーサネット インターフェイスの概要 3

インターフェイス コマンド 4

UDLD パラメータ 4

UDLD のデフォルト設定 5

UDLD アグレッシブ モードと非アグレッシブ モード 5

レイヤ 2 インターフェイスの注意事項および制約事項 6

インターフェイス速度 6

40 ギガビット イーサネット インターフェイスの速度 7

SVI 自動ステート 7

Cisco Discovery Protocol 8

CDP のデフォルト設定 8

errordisable ステート 8

デフォルト インターフェイス	10
デバウンス タイマー パラメータについて	10
MTU 設定	10
カウンタ値	10
ダウンリンク遅延	12
物理イーサネットのデフォルト設定	12
インターフェイス情報の表示	13

## 第 3 章

レイヤ 3 インターフェイスの設定	17
レイヤ 3 インターフェイスについて	17
ルーテッド インターフェイス	17
サブインターフェイス	18
VLAN インターフェイス	19
インターフェイスの VRF メンバーシップの変更	20
インターフェイスの VRF メンバーシップの変更に関する注意事項	21
ループバック インターフェイス	21
IP アnnナンバード	22
トンネル インターフェイス	22
レイヤ 3 インターフェイスの注意事項および制約事項	22
レイヤ 3 インターフェイスのデフォルト設定	23
SVI 自動ステートのディセーブル化	23
レイヤ 3 インターフェイスの設定	23
ルーテッド インターフェイスの設定	23
サブインターフェイスの設定	25
インターフェイスでの帯域幅の設定	26
VLAN インターフェイスの設定	27
VRF メンバーシップ変更時のレイヤ 3 保持の有効化	28
ループバック インターフェイスの設定	28
イーサネット インターフェイスの IP アnnナンバードの設定	29
VRF へのインターフェイスの割り当て	30
インターフェイス MAC アドレスの設定	31

MAC 組み込み IPv6 アドレスの設定	33
SVI 自動ステートの無効化の設定	35
インターフェイスでの DHCP クライアントの設定	36
レイヤ 3 インターフェイス設定の確認	37
レイヤ 3 インターフェイスのモニタリング	39
レイヤ 3 インターフェイスの設定例	40
レイヤ 3 インターフェイスの関連資料	41

---

## 第 4 章

<b>ポートチャネルの設定</b>	<b>43</b>
ポートチャネルについて	43
ポートチャネルの概要	44
互換性要件	45
ポートチャネルを使用したロードバランシング	47
対称ハッシュ化	48
LACP について	49
LACP の概要	49
LACP ID パラメータ	50
チャンネルモード	50
LACP マーカー レスポンダ	52
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	52
LACP ポートチャネルの最小リンクおよび MaxBundle	52
注意事項と制約事項	53
ポートチャネルの設定	54
ポートチャネルの作成	54
ポートチャネルへのポートの追加	55
ポートチャネルを使ったロードバランシングの設定	56
LACP のイネーブル化	58
ポートに対するチャンネルモードの設定	58
LACP ポートチャネルの MinLink の設定	60
LACP ポートチャネル MaxBundle の設定	61
LACP 高速タイマー レートの設定	62

LACP のシステム プライオリティおよびシステム ID の設定	63
LACP ポート プライオリティの設定	64
LACP グレースフル コンバージェンス	65
LACP グレースフル コンバージェンスの再有効化	67
ポート チャネル設定の確認	68
ポート チャネル メンバーシップ整合性チェッカーのトリガー	69
ロードバランシング発信ポート ID の確認	70
ポート プロファイル	70
ポート プロファイルの設定	73
ポート プロファイルの作成	73
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	74
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	75
特定のポート プロファイルのイネーブル化	76
ポート プロファイルの継承	77
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	78
継承されたポート プロファイルの削除	79

## 第 5 章

## 仮想ポートチャネルの設定 81

vPC について	82
vPC の概要	82
用語	83
vPC の用語	83
vPC ドメイン	84
ピアキープアライブ リンクとメッセージ	85
vPC ピア リンクの互換パラメータ	85
同じでなければならない設定パラメータ	86
同じにすべき設定パラメータ	87
VLAN ごとの整合性検査	88
vPC 自動リカバリ	88
vPC ピア リンク	89

vPC ピア リンクの概要	89
vPC 番号	90
その他の機能との vPC の相互作用	91
vPC と LACP	91
vPC ピア リンクと STP	91
CFSoE	92
vPC フォークリフトアップグレード	92
VRF に関する注意事項と制約事項	96
vPC 設定の確認	97
グレースフル タイプ 1 検査ステータスの表示	98
グローバル タイプ 1 不整合の表示	99
インターフェイス別タイプ 1 不整合の表示	100
VLAN ごとの整合性ステータスの表示	101
vPC のデフォルト設定	104
vPC の設定	104
vPC のイネーブル化	104
vPC のディセーブル化	105
vPC ドメインの作成	106
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	107
vPC ピア リンクの作成	109
設定の互換性の検査	110
vPC 自動リカバリのイネーブル化	112
復元遅延時間の設定	113
vPC ピア リンク障害発生時における VLAN インターフェイスのシャットダウン回避	114
VRF 名の設定	115
他のポート チャネルの vPC への移行	115
vPC ドメイン MAC アドレスの手動での設定	117
システム プライオリティの手動での設定	118
vPC ピア スイッチのロールの手動による設定	119
Layer 3 over vPC の設定	120







## はじめに

この前書きは、次の項で構成されています。

- [対象読者](#) (ix ページ)
- [表記法](#) (ix ページ)
- [Cisco Nexus 3600 プラットフォーム スイッチの関連資料](#) (x ページ)
- [マニュアルに関するフィードバック](#) (xi ページ)
- [通信、サービス、およびその他の情報](#) (xi ページ)

## 対象読者

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

## 表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
<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]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x   y]	いずれか1つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x   y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。

表記法	説明
[x {y   z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
variable	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。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、スクリーンフォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字のスクリーンフォントで示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコ (<>) で囲んで示しています。
[]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。

## Cisco Nexus 3600 プラットフォーム スイッチの関連資料

Cisco Nexus 3600 プラットフォーム スイッチ全体のマニュアルセットは、次の URL にあります。

<http://www.cisco.com/c/en/us/support/switches/nexus-3000-series-switches/tsd-products-support-series-home.html>

## マニュアルに関するフィードバック

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

## 通信、サービス、およびその他の情報

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

### Cisco バグ検索ツール

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





# 第 1 章

## 新規および変更情報

- [新規および変更情報 \(1 ページ\)](#)

## 新規および変更情報

表 1: NX-OS リリース 10.2(x) の新機能および変更された機能

特長	説明	変更が行われたリリース	参照先
このリリースに新機能はありません。		10.2(1)F	





## 第 2 章

# レイヤ 2 インターフェイスの設定

- [ライセンス要件 \(3 ページ\)](#)
- [イーサネット インターフェイスの概要, on page 3](#)
- [レイヤ 2 インターフェイスの注意事項および制約事項 \(6 ページ\)](#)
- [インターフェイス速度 \(6 ページ\)](#)
- [40 ギガビットイーサネット インターフェイスの速度 \(7 ページ\)](#)
- [SVI 自動ステート \(7 ページ\)](#)
- [Cisco Discovery Protocol, on page 8](#)
- [errordisable ステート \(8 ページ\)](#)
- [デフォルト インターフェイス \(10 ページ\)](#)
- [デバウンス タイマー パラメータについて, on page 10](#)
- [MTU 設定, on page 10](#)
- [物理イーサネットのデフォルト設定, on page 12](#)
- [インターフェイス情報の表示, on page 13](#)

## ライセンス要件

Cisco NX-OS ライセンス方式の推奨の詳細と、ライセンスの取得および適用の方法については、『[Cisco NX-OS Licensing Guide](#)』を参照してください。

## イーサネット インターフェイスの概要

イーサネットポートは、サーバまたはLANに接続される標準のイーサネットインターフェイスとして機能します。

イーサネット インターフェイスはデフォルトでイネーブルです。

## インターフェイスコマンド

**interface** コマンドを使用すれば、イーサネットインターフェイスのさまざまな機能をインターフェイスごとにイネーブルにできます。**interface** コマンドを入力する際には、次の情報を指定します。

Cisco Nexus ファブリック エクステンダ との併用をサポートするために、インターフェイスのナンバリング規則は、次のように拡張されています。

```
switch(config)# interface ethernet [chassis/]slot/port
```

- シャーシ ID は、接続されている ファブリック エクステンダ のポートをアドレス指定するために使用できる任意のエントリです。インターフェイス経由で検出されたファブリック エクステンダ を識別するために、シャーシ ID はスイッチ上の物理イーサネットまたは EtherChannel インターフェイスに設定されます。シャーシ ID の範囲は、100 ~ 199 です。

## UDLD パラメータ

シスコ独自の単一方向リンク検出 (UDLD) プロトコルでは、光ファイバまたは銅線 (たとえば、カテゴリ 5 のケーブル) のイーサネットケーブルで接続されているポートでケーブルの物理的な構成をモニタリングし、単一方向リンクの存在を検出できます。スイッチが単一方向リンクを検出すると、UDLD は関連する LAN ポートをシャットダウンし、ユーザに警告します。単一方向リンクは、スパンニングツリートポロジグループをはじめ、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、オートネゴシエーションは物理シグナリングと障害検出を行います。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。

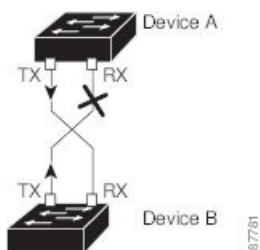
リンク上でローカルデバイスから送信されたトラフィックはネイバーで受信されるのに対し、ネイバーから送信されたトラフィックはローカルデバイスで受信されない場合には常に、単方向リンクが発生します。対になったファイバケーブルのうち一方の接続が切断された場合、自動ネゴシエーションがアクティブであると、そのリンクのアップ状態は維持されなくなります。この場合、論理リンクは不定であり、UDLD は何の処理も行いません。レイヤ 1 で両方の光ファイバが正常に動作している場合は、レイヤ 2 で UDLD が、これらの光ファイバが正しく接続されているかどうか、および正しいネイバー間でトラフィックが双方向に流れている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



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

Figure 1: 単方向リンク



## UDLD のデフォルト設定

次の表は、UDLD のデフォルト設定を示したものです。

Table 2: 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
UDLD アグレッシブ モード	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 モードがイネーブルになっている場合、UDLD ネイバー関係が確立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の再確立を試行します。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。

- リンク的一方にポート 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。

## レイヤ2インターフェイスの注意事項および制約事項

レイヤ2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。

- 自動ネゴシエーションはサポートされません。
- 1G 自動ネゴシエーションは N3K-C36180YC-R および N9K-X96136YC-R スイッチではサポートされません。この問題を回避するには、速度を手動で 1000 に設定する必要があります。ネイバーで自動ネゴシエーションが有効になっている場合は、それらのネイバーで自動ネゴシエーションを無効にする必要があります。
- Cisco Nexus N3K-C3636C-R および N3K-C36180YC-R スイッチでは、QSFP-100G-CR4 ケーブルを使用して 100G リンクを起動すると、ポート 49 ～ 64 で自動ネゴシエーションが機能しないことがあります。この問題を回避するには、ポート 49 ～ 64 の速度をハードコードし、自動ネゴシエーションを無効にする必要があります。

## インターフェイス速度

Cisco Nexus 36180YC-R スイッチには、デフォルト速度が 10 G の 48 個の Small Form-Factor Pluggable (SFP) ポートと、デフォルト速度が 100 G の 6 個の Quad Small Form-Factor Pluggable (QSFP) ポートがあります。48 個の SFP インターフェイス ポートは、25 G、10 G、1 G の速度をサポートできます。6 個の QSFP インターフェイスポートは、100 G および 40 G の速度をサポートできます。

最初の 48 ポートでは、ポート グループの各 4 ポートに同じ速度が設定されている必要があります。一度に 1 つのポートを設定することはできません。エラーが発生する可能性があります。詳細については、[CSCve80686](#) を参照してください。

表 3: ブレークアウト モードのサポート マトリックス

スイッチ	4x10G	4x25G	2x50G
N3K-C3636C-R	はい	はい	はい
N3K-C36180YC-R	はい	はい	はい

## 40 ギガビットイーサネットインターフェイスの速度



(注) 40G ポートを 4x10G モードにブレイクアウトするか、100G ポートを 4x25G モードにブレイクアウトすると、ブレイクアウトポートが管理上有効な状態になります。以前のリリースからのアップグレードでは、復元された設定によって、ポートの適切な管理状態が復元されます。



(注) 40 ギガビットイーサネットから 10 ギガビットイーサネットにブレイクアウトするか、10 ギガビットイーサネットから 40 ギガビットイーサネットにブレイクインすると、すべてのインターフェイス設定がリセットされ、影響を受けたポートは管理上使用できなくなります。これらのポートを使用可能にするには、**no shut** コマンドを使用します。



(注) 新しい QSFP+ 40 Gb トランシーバは、Cisco Nexus 3600 プラットフォーム スイッチでサポートされています。新しい QSFP+ (40-Gb) トランシーバには、4つの10Gb SFP-10G-LR トランシーバとして分割されるケーブルがあります。これを使用するには、ポートを 4x10G モードにする必要があります。ブレイクアウト ケーブルを使用している場合は、その 40G ポートを 4x10G モードで動作させる必要があります。

40 ギガビットイーサネット ポートを 4つの 10 ギガビットイーサネットポートにブレイクアウトし、4つの 10 ギガビットイーサネットポートを 40 ギガビットイーサネットポートに動的にブレイクインする機能により、永続的に定義せずに、任意のブレイクアウト対応ポートを 40 ギガビットイーサネットまたは 10 ギガビットイーサネットモードで動作させることができます。

## SVI 自動ステート

スイッチ仮想インターフェイス (SVI) は、デバイスの VLAN のブリッジ機能とルーティング機能間の論理インターフェイスを表します。デフォルトでは、VLAN インターフェイスが VLAN で複数のポートを有する場合、SVI は VLAN のすべてのポートがダウンするとダウン状態になります。

自動ステートの動作は、対応する VLAN のさまざまなポートの状態によって管理されるインターフェイスの動作状態です。VLAN の SVI インターフェイスは、VLAN に STP フォワーディングステートのポートが少なくとも 1 個ある場合にアップになります。同様に、このインターフェイスは最後の STP 転送ポートがダウンするか、別の STP 状態になったとき、ダウンします。

デフォルトでは、自動ステートの計算はイネーブルです。SVI インターフェイスの自動ステートの計算をディセーブルにし、デフォルト値を変更できます。

# Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) は、すべてのシスコ デバイス（ルータ、ブリッジ、アクセスサーバ、およびスイッチ）のレイヤ2（データリンク層）で動作するデバイス検出プロトコルです。ネットワーク管理アプリケーションは CDP を使用することにより、既知のデバイスのネイバーであるシスコ デバイスを検出することができます。CDP を使用すれば、下位レイヤのトランスペアレント プロトコルが稼働しているネイバー デバイスのデバイス タイプや、簡易ネットワーク管理プロトコル (SNMP) エージェントアドレスを学習することもできます。この機能によって、アプリケーションからネイバー デバイスに SNMP クエリーを送信できます。

CDPは、サブネットワークアクセスプロトコル (SNAP) をサポートしているすべてのメディアで動作します。CDPはデータリンク層でのみ動作するため、異なるネットワーク層プロトコルをサポートする2つのシステムで互いの情報を学習できます。

CDP が設定された各デバイスはマルチキャスト アドレスに定期的にメッセージを送信して、SNMP メッセージを受信可能なアドレスを1つまたは複数アドバタイズします。アドバタイズには、存続可能時間（保持時間）や情報も含まれています。これは、受信側のデバイスが CDP 情報を破棄せずに保持する時間の長さです。各デバイスは他のデバイスから送信されたメッセージも待ち受けて、ネイバー デバイスについて学習します。

このスイッチは、CDP バージョン1 とバージョン2 の両方をサポートします。

## CDP のデフォルト設定

次の表は、CDP のデフォルト設定を示したものです。

Table 4: CDP のデフォルト設定

機能	デフォルト設定
CDP インターフェイス ステート	有効
CDP タイマー（パケット更新頻度）	60 秒
CDP ホールドタイム（廃棄までの時間）	180 秒
CDP バージョン2 アドバタイズ	有効 (Enabled)

## errordisable ステート

あるインターフェイスが `errdisable` ステートであるというのは、そのインターフェイスが管理上は (`no shutdown` コマンドにより) イネーブルになっていながら、実行時に何らかのプロセスによってディセーブルになっていることを指します。たとえば、UDLDが単方向リンクを検

出した場合、そのインターフェイスは実行時にシャットダウンされます。ただし、そのインターフェイスは管理上イネーブルであるため、そのステータスは **errdisable** として表示されません。いったんインターフェイスが **errdisable** ステートになったら、手動で再イネーブル化する必要があります。あるいは、自動タイムアウト回復値を設定しておくこともできます。**errdisable** 検出はすべての原因に対してデフォルトでイネーブルです。自動回復はデフォルトでは設定されていません。

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。

**errdisable** の特定の原因に対する **errdisable** 自動回復タイムアウトを設定する場合は、**time** 変数の値を変更します。

**errdisable recovery cause** コマンドを使用すると、300 秒後に自動回復します。回復までの時間を変更する場合は、**errdisable recovery interval** コマンドを使用して、タイムアウト時間を指定します。指定できる値は 30 ~ 65535 秒です。

インターフェイスが **errdisable** からリカバリしないようにするには、**no errdisable recovery cause** コマンドを使用します。

**errdisable recover cause** コマンドには、以下のさまざまなオプションがあります。

- **all** : すべての原因からの回復タイマーをイネーブル化します。
- **bpduguard** : ブリッジプロトコルデータユニット (BPDU) ガードの **errdisable** ステートからの回復タイマーをイネーブル化します。
- **failed-port-state** : スパニング ツリー プロトコル (STP) のポート設定状態障害からの回復タイマーをイネーブル化します。
- **link-flap** : リンクステート フラッピングからの回復タイマーをイネーブル化します。
- **pause-rate-limit** : ポーズレートリミットの **errdisable** ステートからの回復タイマーをイネーブル化します。
- **udld** : 単方向リンク検出 (UDLD) の **errdisable** ステートからの回復タイマーをイネーブル化します。
- **loopback** : ループバック **errdisable** ステートからの回復タイマーをイネーブル化します。

特定の原因に対し、**errdisable** からの回復をイネーブルにしなかった場合、**errdisable** ステートは、**shutdown** および **no shutdown** コマンドを入力するまで続きます。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。

## 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、管理、VLAN、およびポートチャン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。

## デバウンス タイマー パラメータについて

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。遅延時間の範囲は0~5000ミリ秒です。デフォルトでは、デバウンス タイマーは100 ms に設定されており、デバウンス タイマーは動作しません。このパラメータが0ミリ秒に設定されると、デバウンスタイマーはディセーブルになります。

**Caution**

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

## MTU 設定

スイッチは、フレームをフラグメント化しません。そのためスイッチでは、同じレイヤ2ドメイン内の2つのポートに別々の最大伝送単位 (MTU) を設定することはできません。物理イーサネット インターフェイス別 MTU はサポートされていません。代わりに、MTU は QoS クラスに従って設定されます。MTU を変更する場合は、クラスマップおよびポリシーマップを設定します。

**Note**

インターフェイス設定を表示すると、物理イーサネットインターフェイスに1500というデフォルトのMTUが表示されます。

## カウンタ値

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

設定 (Configuration)	パケットサイズ (Packet Size)	増分カウンタ (Incremented Counters)	トラフィック
L2 ポート : MTU 設定なし	6400 および 10000	ジャンボ、ジャイアント、および入力エラー	破棄
L2 ポート : ネットワーク QoS 設定のジャンボ MTU 9216	6400	ジャンボ	転送
L2 ポート : ネットワーク QoS 設定のジャンボ MTU 9216	10,000	ジャンボ、ジャイアント、および入力エラー	破棄
network-qos 設定のデフォルト レイヤ 3 MTU およびジャンボ MTU 9216 のレイヤ 3 ポート	6400	ジャンボ	パケットは CPU にパントされ (CoP P設定の対象)、フラグメント化されてから、ソフトウェアによって転送されます。
network-qos 設定のデフォルト レイヤ 3 MTU およびジャンボ MTU 9216 のレイヤ 3 ポート	6400	ジャンボ	パケットは CPU にパントされ (CoP P設定の対象)、フラグメント化されてから、ソフトウェアによって転送されます。
network-qos 設定のデフォルト レイヤ 3 MTU およびジャンボ MTU 9216 のレイヤ 3 ポート	10,000	ジャンボ、ジャイアント、および入力エラー	破棄
network-qos 設定のジャンボ レイヤ 3 MTU およびジャンボ MTU 9216 のレイヤ 3 ポート	6400	ジャンボ	フラグメンテーションなしで転送されます。
network-qos 設定のジャンボ レイヤ 3 MTU およびジャンボ MTU 9216 のレイヤ 3 ポート	10,000	ジャンボ、ジャイアント、および入力エラー	破棄

設定 (Configuration)	パケットサイズ (Packet Size)	増分カウンタ (Incremented Counters)	トラフィック
ジャンボ レイヤ 3 MTU およびデフォルト L2 MTU 設定の レイヤ 3 ポート	6400 および 10000	ジャンボ、ジャイアント、および入力エラー	破棄



- (注)
- CRC 正常の 64 バイト未満のパケット：ショート フレームカウンタが増加します。
  - CRC 不良の 64 バイト未満のパケット：runts カウンタが増加します。
  - CRC 不良の 64 バイトを超えるパケット：CRC カウンタが増加します。

## ダウンリンク遅延

Cisco Nexus 3048 スイッチのリロード後、ダウンリンク RJ-45 ポートの前に、アップリンク SFP+ポートを動作可能にできます。SFP+ポートが有効になるまで、ハードウェアで RJ-45 ポートの有効化を遅らせる必要があります。

リロード中に、指定したタイムアウト後にのみハードウェアでダウンリンク RJ-45 ポートを有効にするタイマーを設定できます。このプロセスにより、アップリンク SFP+ポートが最初に動作可能になります。タイマーは、admin-enable であるポートに対してのみハードウェアで有効になります。

デフォルトではダウンリンク遅延は無効になっているため、明示的に有効にする必要があります。有効にした場合、遅延タイマーが指定されていないと、デフォルトの遅延 20 秒に設定されます。

## 物理イーサネットのデフォルト設定

次の表に、すべての物理イーサネット インターフェイスのデフォルト設定を示します。

パラメータ	デフォルト設定
デュプレックス	オート (全二重)
カプセル化	ARPA
MTU <sup>1</sup>	1500 バイト
ポート モード	アクセス (Access)



パラメータ	デフォルト設定
スピード	オート (10000)

<sup>1</sup> MTU を物理イーサネット インターフェイスごとに変更することはできません。MTU の変更は、QoS クラスのマップを選択することにより行います

## インターフェイス情報の表示

定義済みインターフェイスに関する設定情報を表示するには、次のうちいずれかの手順を実行します。

コマンド	目的
switch# <b>show interface type slot/port</b>	指定したインターフェイスの詳細設定が表示されます。
switch# <b>show interface type slot/port capabilities</b>	指定したインターフェイスの機能に関する詳細情報が表示されます。このオプションは、物理インターフェイスにしか使用できません。
switch# <b>show interface type slot/port transceiver</b>	指定したインターフェイスに接続されているトランシーバに関する詳細情報が表示されます。このオプションは、物理インターフェイスにしか使用できません。
switch# <b>show interface brief</b>	すべてのインターフェイスのステータスが表示されます。
switch# <b>show interface flowcontrol</b>	すべてのインターフェイスでフロー制御設定の詳細なリストを表示します。

**show interface** コマンドは、EXEC モードから呼び出され、インターフェイスの設定を表示します。引数を入力せずにこのコマンドを実行すると、スイッチ内に設定されたすべてのインターフェイスの情報が表示されます。

次に、物理イーサネット インターフェイスを表示する例を示します。

```
switch# show interface ethernet 1/1
Ethernet1/1 is up
Hardware is 1000/10000 Ethernet, address is 000d.eca3.5f08 (bia 000d.eca3.5f08)
MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 190/255, rxload 192/255
Encapsulation ARPA
Port mode is trunk
full-duplex, 10 Gb/s, media type is 1/10g
Input flow-control is off, output flow-control is off
Auto-mdix is turned on
Rate mode is dedicated
Switchport monitor is off
Last clearing of "show interface" counters never
5 minute input rate 942201806 bytes/sec, 14721892 packets/sec
5 minute output rate 935840313 bytes/sec, 14622492 packets/sec
Rx
```

```

129141483840 input packets 0 unicast packets 129141483847 multicast packets
0 broadcast packets 0 jumbo packets 0 storm suppression packets
8265054965824 bytes
0 No buffer 0 runt 0 Overrun
0 crc 0 Ignored 0 Bad etype drop
0 Bad proto drop
Tx
119038487241 output packets 119038487245 multicast packets
0 broadcast packets 0 jumbo packets
7618463256471 bytes
0 output CRC 0 ecc
0 underrun 0 if down drop      0 output error 0 collision 0 deferred
0 late collision 0 lost carrier 0 no carrier
0 babble
0 Rx pause 8031547972 Tx pause 0 reset

```

次に、物理イーサネットの機能を表示する例を示します。

```

switch# show interface ethernet 1/1 capabilities
Ethernet1/1
  Model:                734510033
  Type:                 10Gbase-(unknown)
  Speed:                1000,10000
  Duplex:               full
  Trunk encap. type:    802.1Q
  Channel:              yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:          rx-(off/on),tx-(off/on)
  Rate mode:            none
  QOS scheduling:       rx-(6q1t),tx-(1p6q0t)
  CoS rewrite:          no
  ToS rewrite:          no
  SPAN:                 yes
  UDLD:                 yes
  MDIX:                 no
  FEX Fabric:           yes

```

次に、物理イーサネット トランシーバを表示する例を示します。

```

switch# show interface ethernet 1/1 transceiver
Ethernet1/1
  sfp is present
  name is CISCO-EXCELIGHT
  part number is SPP5101SR-C1
  revision is A
  serial number is ECL120901AV
  nominal bitrate is 10300 Mbits/sec
  Link length supported for 50/125mm fiber is 82 m(s)
  Link length supported for 62.5/125mm fiber is 26 m(s)
  cisco id is --
  cisco extended id number is 4

```

次に、インターフェイスステータスの要約を表示する例を示します（出力の一部を割愛してあります）。

```
switch# show interface brief
```

```

-----
Ethernet      VLAN   Type Mode   Status Reason           Speed   Port
Interface                                           Ch #
-----
Eth1/1        200   eth trunk up      none           10G(D) --

```

```

Eth1/2      1      eth trunk up      none      10G(D) --
Eth1/3      300    eth access down   SFP not inserted  10G(D) --
Eth1/4      300    eth access down   SFP not inserted  10G(D) --
Eth1/5      300    eth access down   Link not connected 1000(D) --
Eth1/6      20     eth access down   Link not connected 10G(D) --
Eth1/7      300    eth access down   SFP not inserted  10G(D) --
...

```

次に、CDP ネイバーを表示する例を示します。

```

switch# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device ID         Local Intrfce  Hldtme  Capability  Platform      Port ID
d13-dist-1       mgmt0         148     S I         WS-C2960-24TC Fas0/9
n5k(FLC12080012) Eth1/5        8       S I s      N5K-C5020P-BA Eth1/5

```





## 第 3 章

# レイヤ 3 インターフェイスの設定

- [レイヤ 3 インターフェイスについて \(17 ページ\)](#)
- [ルーテッドインターフェイス \(17 ページ\)](#)
- [サブインターフェイス \(18 ページ\)](#)
- [VLAN インターフェイス \(19 ページ\)](#)
- [インターフェイスの VRF メンバーシップの変更 \(20 ページ\)](#)
- [インターフェイスの VRF メンバーシップの変更に関する注意事項 \(21 ページ\)](#)
- [ループバック インターフェイス \(21 ページ\)](#)
- [IP アnnナナバード \(22 ページ\)](#)
- [トンネルインターフェイス \(22 ページ\)](#)
- [レイヤ 3 インターフェイスの注意事項および制約事項 \(22 ページ\)](#)
- [レイヤ 3 インターフェイスのデフォルト設定 \(23 ページ\)](#)
- [SVI 自動ステートのディセーブル化 \(23 ページ\)](#)
- [レイヤ 3 インターフェイスの設定 \(23 ページ\)](#)
- [レイヤ 3 インターフェイス設定の確認 \(37 ページ\)](#)
- [レイヤ 3 インターフェイスのモニタリング \(39 ページ\)](#)
- [レイヤ 3 インターフェイスの設定例 \(40 ページ\)](#)
- [レイヤ 3 インターフェイスの関連資料 \(41 ページ\)](#)

## 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、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。

イーサネットポートはすべて、デフォルトではレイヤ2 (スイッチポート) です。このデフォルト動作は、インターフェイス コンフィギュレーション モードから **no switchport** コマンドを使用して変更できます。複数のポートを一度に変更するために、インターフェイスの範囲を指定してから **no switchport** コマンドを適用することができます。

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。レイヤ3インターフェイスのデフォルト MAC アドレスは、割り当て先の仮想デバイス コンテキスト (VDC) の MAC アドレスです。インターフェイス コンフィギュレーション モードから **mac-address** コマンドを使用して、レイヤ3インターフェイスのデフォルト MAC アドレスを変更できます。スタティック MAC アドレスは、SVI、レイヤ3インターフェイス、ポートチャネル、レイヤ3サブインターフェイス、およびトンネルインターフェイスで設定できます。ポートおよびポートチャネルの範囲でスタティック MAC アドレスを設定することもできます。ただし、すべてのポートがレイヤ3にある必要があります。ポートの範囲内の1つのポートがレイヤ2にある場合でも、コマンドは拒否され、エラーメッセージが表示されます。MAC アドレスの設定については、デバイスの『Layer 2 Switching Configuration Guide』を参照してください。

ルーテッドインターフェイスからレイヤ3ポートチャネルも作成できます。

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

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

## サブインターフェイス

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

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

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

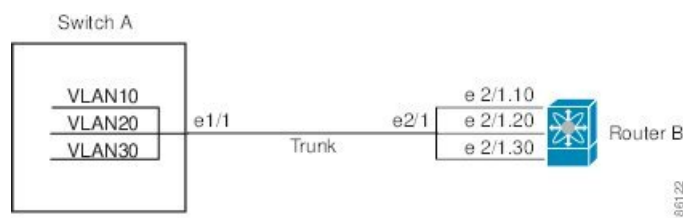
2/1 に Ethernet 2/1.1 というサブインターフェイスを作成できます。この場合、.1 はそのサブインターフェイスを表します。

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

サブインターフェイスを使用すると、親インターフェイスがサポートする各 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 トランッ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 トランッキングを使って VLAN ID に関連付けます。

次の図に、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ッ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、トランッ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 2: 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。1つの VLAN には1つの VLAN インターフェイスだけを関連付けできます。ただし、VLAN 同士をルーティングする場合や管理 Virtual Routing and Forwarding (VRF) 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は、VLAN に VLAN インターフェイスを設定する必要があります。VLAN インターフェイスの作成を有効にすると、Cisco NX-OS によってデフォルト VLAN (VLAN 1) に VLAN インターフェイスが作成され、リモートスイッチ管理が許可されます。

この設定では、事前に VLAN ネットワーク インターフェイス機能を有効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、デバイスの『System Management Configuration Guide』を参照してください。



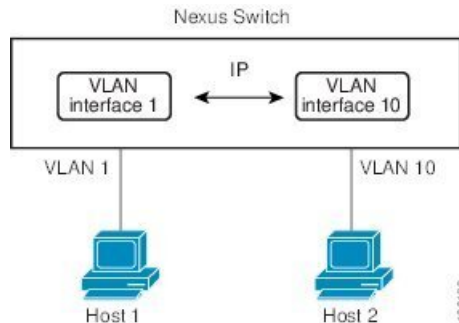
(注) VLAN 1 の VLAN インターフェイスは削除できません。

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、デバイスの『Unicast Routing Configuration Guide』を参照してください。

次の図に、デバイス上の2つのVLANに接続されている2つのホストを示します。VLANごとにVLANインターフェイスを設定し、VLAN間のIPルーティングを使ってホスト1とホスト2を通信させることができます。VLAN1はVLANインターフェイス1のレイヤ3で、VLAN10はVLANインターフェイス10のレイヤ3で通信します。

図3: VLANインターフェイスに接続した2つのVLAN



## インターフェイスのVRFメンバーシップの変更

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

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



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

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



# インターフェイスの VRF メンバーシップの変更に関する注意事項

- VRF 名を変更すると、瞬間的なトラフィック損失が発生することがあります。
- **system vrf-member-change retain-l3-config** コマンドを有効にすると、インターフェイスレベルでの設定だけが処理されます。VRF の変更後にルーティングプロトコルに対応するには、ルータレベルで設定を手動で処理する必要があります。
- **system vrf-member-change retain-l3-config** コマンドは、次によるインターフェイスレベルの設定をサポートしています。
  - CLI サーバによって保持されるレイヤ3設定 (**ip address** および **ipv6 address** (セカンダリ) やインターフェイス設定で使用可能なすべての OSPF/ISIS/EIGRP CLI など)
  - HSRP
  - DHCP リレー エージェント CLI (**ip dhcp relay address [use-vrf]** や **ipv6 dhcp relay address [use-vrf]** など)。
- DHCP の設定：
  - ベストプラクティスとして、クライアントとサーバのインターフェイス VRF は一度に1つずつ変更する必要があります。そうしないと、リレーエージェントで DHCP パケットを交換できません。
  - クライアントとサーバが異なる VRF にある場合は、**ip dhcp relay address [use-vrf]** コマンドを使用して、異なる VRF 経由でリレーエージェントの DHCP パケットを交換します。

## 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。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。

## IP アンナナンバード

IP アンナナンバード機能を使用すると、一意の IP アドレスを明示的に設定することなく、ポイントツーポイント (p2p) インターフェイスで IP パケットを処理できます。このアプローチでは、別のインターフェイスから IP アドレスを借りて、ポイントツーポイントリンクのアドレス空間を節約します。

ループバック インターフェイスは、常に機能的にアップしているという点で、ナンバード インターフェイスとして理想的です。ただし、ループバック インターフェイスはスイッチ/ルータに対してローカルであるため、アンナナンバード インターフェイスの到達可能性は、最初にスタティック ルートを通じて、または OSPF や ISIS などの内部ゲートウェイ プロトコルを使用して確立する必要があります。

IP アンナナンバード機能はポート チャネル インターフェイスおよびサブインターフェイスでサポートされます。借りられるインターフェイスはループバック インターフェイスだけで、ナンバード インターフェイスと呼ばれます。

## 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。



(注) IP-in-IP トンネルのカプセル化とカプセル化解除は、Cisco Nexus N3K-C36180YC-R プラットフォーム スイッチではサポートされません。

## 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。

- 設定を削除しても、VLAN/SVI はレイヤ3 インターフェイス テーブルから削除されません。VLAN 自体は、レイヤ3 インターフェイス テーブルから削除する必要があります。
- 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管理状態のデフォルト設定は Shut です。

## SVI 自動ステートのディセーブル化

SVI自動ステートのディセーブル化機能は、対応するVLANで「アップ」状態のインターフェイスがない場合でも、スイッチ仮想インターフェイス (SVI) を「アップ」状態にすることができます。

SVIは、仮想ルーテッドインターフェイスでもあり、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。VLANのポートは、対応するSVIの動作状態を決定します。VLANのSVIインターフェイスは、対応するVLAN内の少なくとも1個のポートがスパニングツリープロトコル (STP) のフォワーディングステートにある場合に「アップ」状態になります。同様に、このSVIインターフェイスは最後のSTP転送ポートがダウンするか、別のSTP状態になったとき、ダウンします。SVIのこの特性は「自動ステート」と呼ばれます。

SVIを作成してVLANのレイヤ2またはレイヤ3の境界を定義したり、SVIインターフェイスを使用してデバイスを管理したりできます。2番目のシナリオでは、SVI自動ステートのディセーブル化機能により、対応するVLANで「アップ」状態のインターフェイスがない場合でも、SVIインターフェイスは「アップ」状態になります。

# 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

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet slot/port**
3. switch(config-if)# **no switchport**
4. switch(config-if)# **[ip|ipv6]ip-address/length**
5. (任意) switch(config-if)# **medium {broadcast | p2p}**
6. (任意) switch(config-if)# **show interfaces**
7. (任意) switch(config-if)# **copy running-config startup-config**

## 手順の詳細

	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固有の設定を削除します。  (注) レイヤ3インターフェイスを元のレイヤ2インターフェイスに変換するには、 <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	(任意) switch(config-if)# <b>medium {broadcast   p2p}</b>	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 <b>broadcast</b> であり、この設定はどの <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	(任意) switch(config-if)# <b>show interfaces</b>	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	(任意) switch(config-if)# <b>copy running-config startup-config</b>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

## 例

次の例は、IPv4 ルートが設定されたレイヤ3インターフェイスの設定方法を示したものです。

```
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

### 始める前に

- 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。

### 手順の概要

1. (任意) `switch(config-if)# copy running-config startup-config`
2. `switch(config)# interface ethernet slot/port.number`
3. `switch(config-if)# [ip | ipv6] address ip-address/length`
4. `switch(config-if)# encapsulation dot1Q vlan-id`
5. (任意) `switch(config-if)# show interfaces`
6. (任意) `switch(config-if)# copy running-config startup-config`

### 手順の詳細

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

### 例

次に、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。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet slot/port**
3. switch(config-if)# **bandwidth [value | inherit [value]]**
4. (任意) switch(config-if)# **copy running-config startup-config**

### 手順の詳細

	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。 <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	switch(config-if)# <b>bandwidth [value   inherit [value]]</b>	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、次のよう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 (KB 単位)。指定できる範囲は 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	(任意) switch(config-if)# <b>copy running-config startup-config</b>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

## 例

次に、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

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature interface-vlan**
3. switch(config)# **interface vlan number**
4. switch(config-if)# **[ip | ipv6 ] address ip-address/length**
5. switch(config-if)# **no shutdown**
6. (任意) switch(config-if)# **show interface vlan number**
7. (任意) switch(config-if)# **copy running-config startup-config**

### 手順の詳細

	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>[ip   ipv6 ] 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>no shutdown</b>	インターフェイスを管理上アップさせます。
ステップ 6	(任意) switch(config-if)# <b>show interface vlan number</b>	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 7	(任意) switch(config-if)# <b>copy running-config startup-config</b>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

## 例

次に、VLAN インターフェイスを作成する例を示します。

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

## VRF メンバーシップ変更時のレイヤ3 保持の有効化

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

### 手順の概要

1. **configure terminal**
2. **system vrf-member-change retain-l3-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	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>system vrf-member-change retain-l3-config</b> 例 : <pre>switch(config)# system vrf-member-change retain-l3-config</pre> <p>Warning: Will retain L3 configuration when vrf member change on interface.</p>	VRF メンバーシップ変更時のレイヤ3 保持を有効化します。 (注) レイヤ3 設定の保持を無効にするには、 <b>no system vrf-member-change retain-l3-config</b> コマンドを使用します。

## ループバック インターフェイスの設定

### 始める前に

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



## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface loopback instance**
3. switch(config-if)# **[ip | ipv6 ] address ip-address/length**
4. (任意) switch(config-if)# **show interface loopback instance**
5. (任意) switch(config-if)# **copy running-config startup-config**

## 手順の詳細

	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 instance</b>	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。
ステップ 3	switch(config-if)# <b>[ip   ipv6 ] 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 4	(任意) switch(config-if)# <b>show interface loopback instance</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。 <i>instance</i> の範囲は 0 ~ 1023 です。
ステップ 5	(任意) switch(config-if)# <b>copy running-config startup-config</b>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

## 例

次に、ループバック インターフェイスを作成する例を示します。

```
switch# configure terminal
switch(config)# interface loopback 0
switch(config-if)# ip address 192.0.2.100/8
switch(config-if)# copy running-config startup-config
```

## イーサネット インターフェイスの IP アンナンバードの設定

イーサネット インターフェイスで IP アンナンバード機能を設定できます。

## 手順の概要

1. **configure terminal**
2. **interface ethernet slot/port port-channel**
3. **medium p2p**
4. **ip unnumbered type number**

## VRFへのインターフェイスの割り当て

## 手順の詳細

	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# <b>configure terminal</b> 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 ethernet slot/port port-channel</b> 例： switch(config)# <b>interface ethernet 1/1</b> switch(config-if)# switch(config)# <b>interface port-channel 1/1</b> switch(config-if)#	インターフェイス設定モードを開始します。イーサネットおよびポートチャネルをサポート
ステップ 3	<b>medium p2p</b> 例： switch(config-if)# <b>medium p2p</b>	インターフェイス メディアをポイント ツー ポイントとして設定します。
ステップ 4	<b>ip unnumbered type number</b> 例： switch(config-if)# <b>ip unnumbered loopback 100</b>	明示的な IP アドレスをインターフェイスに割り当てずにインターフェイス上の IP 処理をイネーブルにします。  <i>type and number</i> IP アドレスが割り当てられているスイッチ上の別のインターフェイスを指定します。指定したインターフェイスを別のアンナンバードインターフェイスに設定することはできません。  (注) <i>type</i> は <b>loopback</b> に制限されます。 (7.0(3)I3(1)以降)

## VRF へのインターフェイスの割り当て

## 始める前に

VRF 用のインターフェイスを設定したあとで、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. switch# **configure terminal**
2. switch(config)# **interface interface-typenumber**
3. switch(config-if)#**vrf member vrf-name**
4. switch(config-if)# FID cleanup[**ip | ipv6**]ip-address/length
5. (任意) switch(config-if)# **show vrf [vrf-name] interface interface-type number**
6. (任意) switch(config-if)# **show interfaces**

## 7. (任意) switch(config-if)# copy running-config startup-config

## 手順の詳細

	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 interface-typenumber</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>vrf member vrf-name</b>	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)# <b>FID cleanup[ip   ipv6]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。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	(任意) switch(config-if)# <b>show vrf [vrf-name] interface interface-type number</b>	VRF 情報を表示します。
ステップ 6	(任意) switch(config-if)# <b>show interfaces</b>	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	(任意) switch(config-if)# <b>copy running-config startup-config</b>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

## 例

次に、VRF にレイヤ 3 インターフェイスを追加する例を示します。

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

## インターフェイス MAC アドレスの設定

SVI、レイヤ 3 インターフェイス、ポート チャネル、レイヤ 3 サブインターフェイス、およびトンネルインターフェイスにスタティック MAC アドレスを設定できます。ポートおよびポートチャネルの範囲でスタティック MAC アドレスを設定することもできます。ただし、すべてのポートがレイヤ 3 にある必要があります。ポートの範囲内の 1 つのポートがレイヤ 2 にある場合でも、コマンドは拒否され、エラーメッセージが表示されます。

## 手順の概要

## 1. switch# configure terminal

2. switch(config)# **interface ethernet slot/port**
3. switch(config-if)# [**no**] **mac-address static router MAC address**
4. switch(config-if)# **show interface ethernet slot/port**

## 手順の詳細

	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</b> ] <b>mac-address static router MAC address</b>	<p>インターフェイスの MAC アドレスを設定します。設定を削除するには、このコマンドの <b>no</b> 形式を使用します。MAC アドレスは、サポートされている次の 4 つの形式のいずれかで入力できます。</p> <ul style="list-style-type: none"> <li>• E.E.E</li> <li>• EE-EE-EE-EE-EE-EE</li> <li>• EE:EE:EE:EE:EE:EE</li> <li>• EEEE.EEEE.EEEE</li> </ul> <p>次の無効な MAC アドレスは入力しないでください。</p> <ul style="list-style-type: none"> <li>•ヌル MAC アドレス : 0000.0000.0000</li> <li>•ブロードキャスト MAC アドレス : FFFF.FFFF.FFFF</li> <li>•マルチキャスト MAC アドレス : 0100.DAAA.ADDD</li> </ul>
ステップ 4	switch(config-if)# <b>show interface ethernet slot/port</b>	(任意) インターフェイスのすべての情報を表示します。

## 例

次に、インターフェイスの MAC アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/3
switch(config-if)# mac-address aaaa.bbbb.dddd
switch(config-if)# show interface ethernet 3/3
switch(config-if)#
```

## MAC 組み込み IPv6 アドレスの設定

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot/port*
3. switch(config-if)# **no switchport**
4. switch(config-if)# **mac-address ipv6-extract**
5. switch(config-if)# **ipv6 address** *ip-address/length*
6. switch(config-if)# **ipv6 nd mac-extract [exclude nud-phase]**
7. (任意) switch(config)# **show ipv6 icmp interface** *type slot/port*

### 手順の詳細

	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> <i>type slot/port</i>	指定したインターフェイスのインターフェイス 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 固有の設定を削除します。  (注) レイヤ3 インターフェイスを元のレイヤ2 インターフェイスに変換するには、 <b>switchport</b> コマンドを使用します。
ステップ 4	switch(config-if)# <b>mac-address ipv6-extract</b>	インターフェイスに設定されている IPv6 アドレスに組み込まれている MAC アドレスを抽出します。  (注) 現在、MEv6 設定は、IPv6 アドレスの EUI-64 形式ではサポートされていません。
ステップ 5	switch(config-if)# <b>ipv6 address</b> <i>ip-address/length</i>	このインターフェイスの IPv6 アドレスを設定します。
ステップ 6	switch(config-if)# <b>ipv6 nd mac-extract [exclude nud-phase]</b>	ネクストホップ IPv6 アドレスに埋め込まれているネクストホップ MAC アドレスを抽出します。  <b>exclude nud-phase</b> オプションにより、ND フェーズでのみパケットがブロックされます。 <b>exclude nud-phase</b> (NUD) オプションが指定されていない場合は、ND フェーズと近隣到達不能検出 (NUD) フェーズの両方でパケットがブロックされます。

	コマンドまたはアクション	目的
ステップ7	(任意) switch(config)# show ipv6 icmp interface type slot/port	IPv6 インターネット制御メッセージプロトコルバージョン6 (ICMPv6) のインターフェイス情報を表示します。

### 例

次に、ND MAC 抽出をイネーブルにして、MAC 組み込み IPv6 アドレスを設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface ethernet 1/3
switch(config-if)# no switchport
switch(config-if)# mac-address ipv6-extract
switch(config-if)# ipv6 address 2002:1::10/64
switch(config-if)# ipv6 nd mac-extract
switch(config-if)# show ipv6 icmp interface ethernet 1/3
ICMPv6 Interfaces for VRF "default"
Ethernet1/3, Interface status: protocol-up/link-up/admin-up
  IPv6 address: 2002:1::10
  IPv6 subnet: 2002:1::/64
  IPv6 interface DAD state: VALID
  ND mac-extract : Enabled
  ICMPv6 active timers:
    Last Neighbor-Solicitation sent: 00:01:39
    Last Neighbor-Advertisement sent: 00:01:40
    Last Router-Advertisement sent: 00:01:41
    Next Router-Advertisement sent in: 00:03:34
  Router-Advertisement parameters:
    Periodic interval: 200 to 600 seconds
    Send "Managed Address Configuration" flag: false
    Send "Other Stateful Configuration" flag: false
    Send "Current Hop Limit" field: 64
    Send "MTU" option value: 1500
    Send "Router Lifetime" field: 1800 secs
    Send "Reachable Time" field: 0 ms
    Send "Retrans Timer" field: 0 ms
    Suppress RA: Disabled
    Suppress MTU in RA: Disabled
  Neighbor-Solicitation parameters:
    NS retransmit interval: 1000 ms
  ICMPv6 error message parameters:
    Send redirects: true
    Send unreachable: false
  ICMPv6-nd Statistics (sent/received):
    RAs: 3/0, RSs: 0/0, NAs: 2/0, NSs: 7/0, RDs: 0/0
    Interface statistics last reset: never
switch(config)#
```

次に、ND MAC 抽出をイネーブルにして、MAC 組み込み IPv6 アドレスを設定する例を示します (NUDフェーズを除く)。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface ethernet 1/5
```

```
switch(config-if)# no switchport
switch(config-if)# mac-address ipv6-extract
switch(config-if)# ipv6 address 2002:2::10/64
switch(config-if)# ipv6 nd mac-extract exclude nud-phase
switch(config-if)# show ipv6 icmp interface ethernet 1/5
ICMPv6 Interfaces for VRF "default"
Ethernet1/5, Interface status: protocol-up/link-up/admin-up
  IPv6 address: 2002:2::10
  IPv6 subnet: 2002:2::/64
  IPv6 interface DAD state: VALID
  ND mac-extract : Enabled (Excluding NUD Phase)
  ICMPv6 active timers:
    Last Neighbor-Solicitation sent: 00:06:45
    Last Neighbor-Advertisement sent: 00:06:46
    Last Router-Advertisement sent: 00:02:18
    Next Router-Advertisement sent in: 00:02:24
  Router-Advertisement parameters:
    Periodic interval: 200 to 600 seconds
    Send "Managed Address Configuration" flag: false
    Send "Other Stateful Configuration" flag: false
    Send "Current Hop Limit" field: 64
    Send "MTU" option value: 1500
    Send "Router Lifetime" field: 1800 secs
    Send "Reachable Time" field: 0 ms
    Send "Retrans Timer" field: 0 ms
    Suppress RA: Disabled
    Suppress MTU in RA: Disabled
  Neighbor-Solicitation parameters:
    NS retransmit interval: 1000 ms
  ICMPv6 error message parameters:
    Send redirects: true
    Send unreachable: false
  ICMPv6-nd Statistics (sent/received):
    RAs: 6/0, RSs: 0/0, NAs: 2/0, NSs: 7/0, RDs: 0/0
    Interface statistics last reset: never
switch(config-if)#
```

## SVI 自動ステートの無効化の設定

対応するVLANでインターフェイスが稼働していなくても、SVIがアクティブのままになるように設定できます。この機能拡張は自動ステートのディセーブル化と呼ばれます。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **[no] system default interface-vlan autostate**
3. switch(config)# **feature interface-vlan**
4. switch(config)# **interface vlan *vlan id***
5. (config-if)# **[no] autostate**
6. (config-if)# **end**
7. **show running-config interface vlan *vlan id***

## 手順の詳細

	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>[no] system default interface-vlan autostate</b>	VLAN のスイッチング仮想インターフェイス (SVI) のシステムデフォルトの自動ステート動作を再度有効にします。SVI の自動ステート動作を無効にするには、このコマンドの <b>no</b> 形式を使用します。
ステップ 3	switch(config)# <b>feature interface-vlan</b>	VLAN インターフェイス SVI の作成をイネーブルにします。
ステップ 4	switch(config)# <b>interface vlan vlan id</b>	VLAN インターフェイスをディスエーブルにし、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	(config-if)# <b>[no] autostate</b>	VLAN インターフェイスの SVI のデフォルトの自動ステート動作をディセーブルにします。
ステップ 6	(config-if)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>show running-config interface vlan vlan id</b>	(任意) 特定のポートチャネルの実行コンフィギュレーションを表示します。

## 例

次に、SVI 自動ステートのディセーブル機能を設定する例を示します。

```
switch# configure terminal
switch(config)# system default interface-vlan autostate
switch(config)# feature interface-vlan
switch(config)# interface vlan 2
switch(config-if)# no autostate
switch(config-if)# end
```

## インターフェイスでの DHCP クライアントの設定

DHCP クライアントの IP アドレスは SVI、管理インターフェイス、または物理イーサネットインターフェイスで設定できます。

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet type slot/port | mgmt mgmt-interface-number | vlan vlan id**
3. switch(config-if)# **[no] ip | ipv6 address dhcp**
4. (任意) switch(config)# **copy running-config startup-config**



## 手順の詳細

	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 type slot/port   mgmt mgmt-interface-number   vlan vlan id</b>	物理イーサネットインターフェイス、管理インターフェイス、またはVLANインターフェイスを作成します。  vlan id の範囲は 1 ~ 4094 です。
ステップ 3	switch(config-if)# <b>[no] ip   ipv6 address dhcp</b>	DHCP サーバに IPv4 または IPv6 アドレスを要求します。  取得されたいずれかのアドレスを削除するには、このコマンドの <b>no</b> 形式を使用します。
ステップ 4	(任意) switch(config)# <b>copy running-config startup-config</b>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

## 例

次に、SVI で DHCP クライアントの IP アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface vlan 15
switch(config-if)# ip address dhcp
```

次に、管理インターフェイスで DHCP クライアントの IPv6 アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface mgmt 0
switch(config-if)# ipv6 address dhcp
```

## レイヤ3インターフェイス設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
<b>show interface ethernet <i>slot/port</i></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の、5分間指数減少移動平均を含む）を表示します。
<b>show interface ethernet <i>slot/port</i> 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 <i>slot/port</i> capabilities</b>	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。
<b>show interface ethernet <i>slot/port</i> 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 <i>slot/port</i> 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。
<b>show interface ethernet <i>slot/port.number</i></b>	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 <i>channel-id.number</i></b>	ポートチャネル サブインターフェイスの設定情報、ステータス、カウンタ（インバウンドおよびアウトバウンドパケットレートおよびバイトレートの、5分間指数減少移動平均を含む）を表示します。
<b>show interface loopback <i>number</i></b>	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 <i>number</i> brief</b>	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 <i>number</i> description</b>	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 <i>number</i> status</b>	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。

コマンド	目的
<b>show interface vlan number</b>	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 number brief</b>	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 number description</b>	VLAN インターフェイスの説明を表示します。
<b>show interface vlan number status</b>	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

次のいずれかのコマンドを使用して、機能に関する統計情報を表示します。

コマンド	目的
<b>load-interval seconds   counter {1   2   3} seconds</b>	ビットレートとパケットレートの統計情報に対して3つの異なるサンプリング間隔を設定します。指定できる範囲は5～300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 load-interval-id</b>	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。  ロード間隔IDは、入力および出力レートを表示する単一のロード間隔IDを指定します。  ロード間隔IDの範囲は1～3です。
<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、32ビットと64ビットの packets 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。
<b>show interface ethernet slot/port counters error</b>	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。

コマンド	目的
<b>show interface ethernet <i>slot/port</i> 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 <i>slot/port.number</i> counters</b>	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。
<b>show interface port-channel <i>channel-id.number</i> counters</b>	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。
<b>show interface loopback <i>number</i> counters</b>	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。
<b>show interface loopback <i>number</i> 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、32ビットと64ビットの packets 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。
<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。
<b>show interface vlan <i>number</i> counters detailed [all]</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</i> snmp</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)# copy running-config startup-config
```

次に、スイッチング仮想インターフェイス (SVI) 自動ステートディセーブルを設定する例を示します。

```
switch# configure terminal
switch(config)# system default interface-vlan autostate
switch(config)# feature interface-vlan
switch(config)# interface vlan 2
switch(config-if)# no autostate
switch(config-if)# end
switch# show running-config interface vlan 2
```

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)# no switchport
switch(config-if)# ip address 192.0.2.2/32
switch(config-if)# copy running-config startup-config
```

次に、イーサネット ポートの 3 種類のサンプリング負荷間隔を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# load-interval counter 1 5
switch(config-if)# load-interval counter 2 135
switch(config-if)# load-interval counter 3 225
switch(config-if)#
```

## レイヤ3インターフェイスの関連資料

関連項目	マニュアルタイトル
コマンド構文	『Cisco Nexus 3600 NX-OS Command Reference』
IP	『Cisco Nexus 3600 NX-OS Unicast Routing Configuration Guide』の「Configuring IP」の章

関連項目	マニュアルタイトル
VLAN	『Cisco Nexus 3600 NX-OS Layer 2 Switching Configuration Guide』の「Configuring VLANs」の章



## 第 4 章

# ポート チャネルの設定

- [ポート チャネルについて, on page 43](#)
- [ポート チャネルの概要, on page 44](#)
- [互換性要件, on page 45](#)
- [ポート チャネルを使用したロード バランシング, on page 47](#)
- [対称ハッシュ化 \(48 ページ\)](#)
- [LACP について \(49 ページ\)](#)
- [注意事項と制約事項 \(53 ページ\)](#)
- [ポート チャネルの設定 \(54 ページ\)](#)
- [ポート チャネル設定の確認, on page 68](#)
- [ポート チャネルメンバーシップ整合性チェッカーのトリガー \(69 ページ\)](#)
- [ロードバランシング発信ポート ID の確認 \(70 ページ\)](#)
- [ポート プロファイル \(70 ページ\)](#)
- [ポート プロファイルの設定 \(73 ページ\)](#)
- [ポート プロファイルの作成 \(73 ページ\)](#)
- [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 \(74 ページ\)](#)
- [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 \(75 ページ\)](#)
- [特定のポート プロファイルのイネーブル化 \(76 ページ\)](#)
- [ポート プロファイルの継承 \(77 ページ\)](#)
- [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 \(78 ページ\)](#)
- [継承されたポート プロファイルの削除 \(79 ページ\)](#)

## ポート チャネルについて

ポートチャネルは、複数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。min-links 設定が1より大きく、min-links 条件が満たされない場合、ポートチャネルはダウンします。

ポートチャネルは、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って作成します。スタティックポートチャネルのほか、Link Aggregation Control Protocol (LACP) を実行するポートチャネルを設定して稼働させることができます。

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、スパニングツリープロトコル (STP) のパラメータをポートチャネルに設定すると、Cisco NX-OS ソフトウェアでは、これらのパラメータがポートチャネルの各インターフェイスに適用されます。

関連するプロトコルを使用せず、スタティックポートチャネルを使用すれば、設定を簡略化できます。IEEE 802.3ad に規定されている LACP を使用すると、ポートチャネルをより効率的に使用することができます。LACP を使用すると、リンクによってプロトコルパッケージが渡されます。

#### Related Topics

[LACP の概要](#) (49 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することにより、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ています。

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ことができるほか、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 によるポートチャネルを設定する手順は、スタティックポートチャネルの場合とは若干異なります。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用したロードバランシング, on page 47](#)を参照してください。



#### Note

Cisco NX-OS は、ポートチャネルに対するポート集約プロトコル (PAgP) をサポートしていません。

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。

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には互換性が必要です。つまり、回線速度が同じであり、かつ全二重方式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。



#### Note

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ことで、ポートチャネルを直接作成することができます。またチャンネルグループを作成して個々のポートを1つに集約することもできます。インターフェイスをチャンネルグループに関連付ける際、ポートチャネルがなければ、Cisco NX-OSでは対応するポートチャネルが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。その場合、Cisco NX-OSでは、ポートチャネルと同じチャンネル数で空のチャンネルグループが作成され、デフォルトの設定が適用されます。

**Note**

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ン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。

## 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では、そのインターフェイスとチャンネルグループとの互換性が確保されるように、特定のインターフェイス属性のチェックが行われます。またCisco NX-OSでは、インターフェイスがポートチャネル集約に加えられることを許可する場合にも、事前にそのインターフェイスに関するさまざまな動作属性のチェックが行われます。

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
- スピード
- 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

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場合は、**show port-channel compatibility-parameters** コマンドを使用します。

チャン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 LACP を実行するポートチャネルには、チャンネルモードが active または passive に設定されたインターフェイスだけを追加することもできます。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。

インターフェイスがポートチャネルに追加されると、次の各パラメータはそのポートチャネルに関する値に置き換えられます。

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

インターフェイスがポートチャネルに追加されても、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** コマンドを使用して、ポートをチャネルグループへ強制的に追加できるようにした場合、パラメータは次のように処理されます。

- インターフェイスがポートチャネルに追加されると、次のパラメータは削除され、代わってポートチャネルに関する値が指定されます。ただしこの変更は、インターフェイスに関する実行中の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追加またはポートチャネルから削除されても、次のパラメータはそのまま維持されます。
  - 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用したロードバランシング

Cisco NX-OS では、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、それを基にチャネル内のリンクを1つ選択することによって、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シングが行われます。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。

次のいずれかの方法（詳細については次の表を参照）を使用してポートチャネル全体をロードバランシングするようにスイッチを設定できます。

- 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

**Table 5:** 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 (Configuration)	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 (Destination IP)	Destination MAC	宛先 MAC、宛先 IP	宛先 MAC、宛先 IP
Source IP	Source 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 (Configuration)	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/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

使用している設定で最も多様なバランス基準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、ポートチャネルで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内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行われることとなります。

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：送信元 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：送信元 MAC アドレス、宛先 MAC アドレス



**Note** hardware multicast hw-hash コマンドは、Cisco Nexus 3000 シリーズスイッチではサポートされていません。これらのスイッチではこのコマンドを設定しないことを推奨します。デフォルトでは、Cisco Nexus 3000 シリーズスイッチは、マルチキャストトラフィックをハッシュします。

## 対称ハッシュ化

ポートチャネル上のトラフィックを効果的にモニタできるようにするには、ポートチャネルに接続された各インターフェイスが、順方向と逆方向の両方のトラフィックフローを受信できることが不可欠です。通常、順方向および逆方向のトラフィックフローが同じ物理インターフェイスを使用する保証はありません。ただし、ポートチャネルで対称ハッシュを有効にすると、双方向トラフィックは同じ物理インターフェイスを使用するように強制され、ポートチャネルの各物理インターフェイスは一連のフローに効果的にマッピングされます。

対称ハッシュを有効にすると、送信元および宛先 IP アドレスなどのハッシュに使用されるパラメータは、ハッシュアルゴリズムに入力される前に正規化されます。このプロセスにより、パラメータが逆になった場合（順方向トラフィックの送信元が逆方向トラフィックの宛先になる）、ハッシュ出力は同じになります。したがって、同じインターフェイスが選択されます。

対称ハッシュは、Cisco Nexus 3600 シリーズスイッチでのみサポートされます。  
次のロードバランシング アルゴリズムのみが対称ハッシュをサポートします。

- source-dest-ip-only
- source-dest-port-only
- source-dest-ip
- source-dest-port
- source-dest-ip-gre

## LACP について

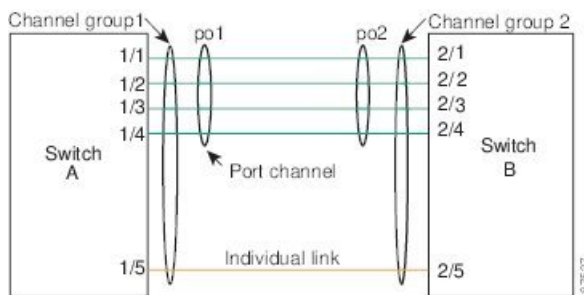
### LACP の概要



**Note** LACP 機能を設定して使用にする場合は、あらかじめ LACP 機能をイネーブルにしておく必要があります。

次の図は、個々のリンクを個別リンクとして機能させるだけでなく LACP ポートチャネルおよびチャネルグループに組み込む方法を示したものです。

**Figure 4:** 個別リンクをポートチャネルに組み込む



LACP を使用すると、スタティック ポートチャネルの場合と同じように、最大 32 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することができます。



**Note** ポートチャネルを削除すると、関連付けられたチャネルグループも Cisco NX-OS によって自動的に削除されます。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。この設定には、ポートチャネル上の LACP min-links などの LACP 設定が含まれていても、メンバーが含まれていないことがあります。その場合は、LACP を無効にできます。

## LACP ID パラメータ

LACP では次のパラメータが使用されます。

- **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。



**Note** 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 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、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約事項

## 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稼働すると、その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。



**Note** active または passive のチャンネルモードで、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化する必要があります。

次の図は、チャンネルモードをまとめたものです。

**Table 6:** ポートチャネルの個別リンクのチャンネルモード

チャンネルモード	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	ポートをアクティブ ネゴシエーション ステートにする LACP モード。この場合ポートでは LACP パケットを送信することにより、他のポートとのネゴシエーションが開始されます。
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ンネルモードを active または passive に変更しようとすると、デバイスがエラーメッセージを返します。  チャンネルで LACP をイネーブルにするには、そのチャンネルのインターフェイスでチャンネルモードを active または passive に設定します。LACP によって 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 チャンネルグループには参加しません。  デフォルトでは、LACP パケットが受信されなかった場合、LACP は中断状態になります。リンクを個別の状態にする場合は、 <b>no lacp suspend-individual</b> コマンドを入力します。

passive と active のどちらのモードでも、ポート速度やランキング ステートなどの基準に基づいてポートチャネルを構成可能かどうかを判定するため、LACP によるポート間のネゴシエーションが行われます。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。

次の例に示したとおり、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 ポートチャネルを構成することができます。

- active モードのポートは、active モードの別のポートと正常にポートチャネルを形成できます。
- active モードのポートは、passive モードの別のポートとともにポートチャネルを形成できます。

- passiveモードのポート同士ではポートチャネルを構成できません。これは、どちらのポートもネゴシエーションを開始しないためです。
- on モードのポートは LACP を実行していません。

## LACP マーカー レスポンダ

ポートチャネルを使用すると、リンク障害やロード バランシング動作に伴って、データトラフィックが動的に再配信される場合があります。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 レスポンダ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

次の表は、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との主な相違点をまとめたものです。設定の最大制限値の詳細については、デバイスの『*Verified Scalability*』マニュアルを参照してください。

Table 7. LACP がイネーブルのポートチャネルとスタティックポートチャネル

設定	LACP がイネーブルのポートチャネル	スタティックポートチャネル
適用されるプロトコル	グローバルにイネーブル化	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>• アクティブ</li> <li>• パッシブ</li> </ul>	on モードのみ

## LACP ポートチャネルの最小リンクおよび MaxBundle

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

LACP ポートチャネルの 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。



LACP MaxBundle は、LACP ポートチャネルで許可されるバンドルポートの最大数を定義します。LACP MaxBundle 機能では、次の処理が行われます。

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



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

## 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。

- Cisco Nexus 36180YC スイッチでは、最初の 24 個のポートは同じクワドラントの一部です。同じクワドラントのポートは、すべてのポートで同じ速度 (1/10G または 25G) である必要があります。クワドラント内のポートで異なる速度を使用することはサポートされていません。クワドラントのいずれかのポートに異なる速度を設定すると、ポートはエラーディセーブル状態になります。同じ象限のインターフェイスは次のとおりです。
  - 1 ~ 4
  - 5 ~ 8
  - 9 ~ 12
  - 13 ~ 16
  - 17 ~ 20
  - 21 ~ 24
  - 25 ~ 28
  - 29 ~ 32
  - 33 ~ 36
  - 37 ~ 40
  - 41 ~ 44
  - 45 ~ 48

# ポートチャネルの設定

## 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。Cisco NX-OSは自動的に、関連するチャンネルグループを作成します。



**Note** 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。



**Note** 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。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface port-channel channel-number**
3. switch(config)# **no interface port-channel channel-number**

### DETAILED STEPS

	Command or Action	Purpose
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 port-channel channel-number</b>	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は、チャンネルグループがない場合はそれを自動的に作成します。
ステップ 3	switch(config)# <b>no interface port-channel channel-number</b>	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。

### Example

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
```

## ポートチャネルへのポートの追加

新しいチャネルグループ、またはすでにポートが含まれているチャネルグループには、ポートを追加できます。ポートチャネルがまだ存在しない場合、Cisco NX-OS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を作成します。



**Note** 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。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot/port*
3. (Optional) switch(config-if)# **switchport mode trunk**
4. (Optional) switch(config-if)# **switchport trunk** {**allowed vlan** *vlan-id* | **native vlan** *vlan-id*}
5. switch(config-if)# **channel-group** *channel-number*
6. (Optional) switch(config-if)# **no channel-group**

### DETAILED STEPS

	Command or Action	Purpose
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> <i>type slot/port</i>	チャネルグループに追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	(Optional) switch(config-if)# <b>switchport mode trunk</b>	指定したインターフェイスをトランクポートとして設定します。
ステップ 4	(Optional) switch(config-if)# <b>switchport trunk</b> { <b>allowed vlan</b> <i>vlan-id</i>   <b>native vlan</b> <i>vlan-id</i> }	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	switch(config-if)# <b>channel-group</b> <i>channel-number</i>	チャネルグループ内にポートを設定し、モードを設定します。channel-number の範囲は 1 ~ 4096 です。ポートチャネルがない場合、Cisco NX-OSにより、このチャネルグループに関連付けられたポートチャネルが作成されます。これを、暗黙的なポートチャネル作成と言います。
ステップ 6	(Optional) switch(config-if)# <b>no channel-group</b>	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。

**Example**

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。



**Note** 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。

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config)# **port-channel load-balance ethernet** {[**destination-ip** | **destination-ip-gre** | **destination-mac** | **destination-port** | **source-dest-ip** | **source-dest-ip-gre** | **source-dest-mac** | **source-dest-port** | **source-ip** | **source-ip-gre** | **source-mac** | **source-port**] **symmetric** | **crc-poly**}
3. (Optional) switch(config)# **no port-channel load-balance ethernet**
4. (Optional) switch# **show port-channel load-balance**

**DETAILED STEPS**

	Command or Action	Purpose
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>port-channel load-balance ethernet</b> {[ <b>destination-ip</b>   <b>destination-ip-gre</b>   <b>destination-mac</b>   <b>destination-port</b>   <b>source-dest-ip</b>   <b>source-dest-ip-gre</b>   <b>source-dest-mac</b>   <b>source-dest-port</b>   <b>source-ip</b>   <b>source-ip-gre</b>   <b>source-mac</b>   <b>source-port</b> ] <b>symmetric</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およびハッシュを指定します。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 <b>source-dest-mac</b> です。

	Command or Action	Purpose
	<code>source-dest-mac   source-dest-port   source-ip   source-ip-gre   source-mac   source-port] symmetric   crc-poly}</code>	<p><b>Note</b> ハッシュ計算にNVGRE キーが含まれるようにするには、オプションの <b>destination-ip-gre</b>、<b>source-dest-ip-gre</b> および <b>source-ip-gre</b> キーワードを使用します。ポートチャネルの場合、NVGRE キーの包含はデフォルトで有効になっていません。これらのオプションのキーワードを使用して、明示的に設定する必要があります。</p> <p>対称ハッシュを有効または無効にするには、オプションの <b>symmetric</b> キーワードを使用します。対称ハッシュは、双方向のトラフィックが同じ物理インターフェイスを使用するように強制します。次のロードバランシングアルゴリズムのみが対称ハッシュをサポートします。</p> <ul style="list-style-type: none"> <li>• source-dest-ip-only</li> <li>• source-dest-port-only</li> <li>• source-dest-ip</li> <li>• source-dest-port</li> <li>• source-dest-ip-gre</li> </ul>
ステップ 3	(Optional) <code>switch(config)# no port-channel load-balance ethernet</code>	ロードバランシングアルゴリズムをデフォルトの <code>source-dest-mac</code> に戻します。
ステップ 4	(Optional) <code>switch# show port-channel load-balance</code>	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。

### Example

次の例は、ポートチャネルに対して送信元 IP によるロードバランシングを設定する方法を示したものです。

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

次の例は、ポートチャネルに対して対称ハッシュを設定する方法を示したものです。

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

## 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 ポートチャネルが設定されている場合、LACP はディセーブルにできません。

LACP は、LAN ポート グループの機能を動的に学習し、残りの LAN ポートに通知します。LACP では、適合する複数のイーサネット リンクが検出されると、これらのリンクが 1 つのポートチャネルにグループ化されます。そのあと、ポートチャネルは単一の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。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **feature lacp**
3. (Optional) switch(config)# **show feature**

### DETAILED STEPS

	Command or Action	Purpose
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 lacp</b>	スイッチ上で LACP をイネーブルにします。
ステップ 3	(Optional) switch(config)# <b>show feature</b>	イネーブルにされた機能を表示します。

### Example

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
```

## ポートに対する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では **on** チャネルモードが維持されます。

### Before you begin

LACP 機能がイネーブルになっていることを確認します。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **channel-group channel-number [force] [mode {on | active | passive}]**
4. switch(config-if)# **no channel-group number mode**

## DETAILED STEPS

	Command or Action	Purpose
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 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>channel-group channel-number [force] [mode {on   active   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 active または passive に設定します。</p> <p><b>force</b> : これを指定すると、チャネルグループに LAN ポートが強制的に追加されます。</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> : これを指定すると、LACP をイネーブルにした時点で、指定したインターフェイス上で LACP がイネーブルになります。インターフェイスはアクティブ ネゴシエーション ステートになります。この場合ポートでは、LACP パケットを送信することにより、他のポートとのネゴシエーションが開始されます。</p> <p><b>on</b> : (デフォルトモード) すべてのポートチャネル (LACP を稼働していないポートチャネル) に対して、このモードが維持されます。</p> <p><b>passive</b> : LACP デバイスが検出された場合にのみ、LACP をイネーブルにします。インターフェイスはパッシブ ネゴシエーション ステートになります。この場合ポートでは、受信した LACP パケットへの応答は行われますが、LACP ネゴシエーションは開始されません。</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 on です。</p>

	Command or Action	Purpose
ステップ 4	switch(config-if)# <b>no 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 on に戻します

### Example

次に、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 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
```

## LACP ポートチャネルの MinLink の設定

MinLink 機能は、LACP ポートチャネルでだけ動作します。デバイスでは非 LACP ポートチャネルでもこの機能を設定できますが、機能は動作しません。



**重要** LACP ポートチャネルの両端、つまり両方のスイッチで LACP MinLink 機能を設定することを推奨します。ポートチャネルの片側でだけ **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。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface port-channel** *number*
3. switch(config-if)# [**no**] **lACP min-links** *number*
4. (任意) switch(config)# **show running-config interface port-channel** *number*

### 手順の詳細

	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 port-channel</b> <i>number</i>	設定するインターフェイスを指定します。
ステップ 3	switch(config-if)# [ <b>no</b> ] <b>lACP min-links</b> <i>number</i>	最小リンク数を設定します。  <i>number</i> のデフォルト値は、1 です。指定できる範囲は 1 ~ 32 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。



	コマンドまたはアクション	目的
ステップ 4	(任意) <code>switch(config)# show running-config interface port-channel number</code>	インターフェイスのポートチャネル設定を表示します。

### 例

次に、バンドル全体として *up* とラベル付けされるリンクの最小数を設定する例を示します。

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

## LACP ポートチャネル MaxBundle の設定

LACP の `maxbundle` 機能を設定できます。最小リンクと `maxbundles` は LACP でのみ動作します。非 LACP ポートチャネルに対してこれらの機能の CLI コマンドを入力することはできませんが、これらのコマンドは動作しません。



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

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

### 始める前に

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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b> 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)# <b>interface port-channel 3</b> switch(config-if)#	設定するインターフェイスを選択します。
ステップ 3	<b>lacp max-bundle number</b> 例： switch(config-if)# <b>lacp max-bundle &lt;number&gt;</b>	ポートチャネルで許可される、アクティブなバンドルの LACP ポートの最大数を設定します。 ポートチャネルの max-bundle のデフォルト値は 32 です。指定できる範囲は 1 ~ 32 です。 (注) デフォルト値は 16 ですが、ポートチャネルのアクティブ メンバ数は、 <i>pc_max_links_config</i> およびポートチャネルで許可されている <i>pc_max_active_members</i> の最小数です。
ステップ 4	<b>show running-config interface port-channel &lt;number&gt;</b> 例： switch(config-if)# <b>show running-config interface port-channel 3</b>	(任意) インターフェイスのポートチャネル コンフィギュレーションを表示します。

## 例

次に、アクティブバンドル LACP ポートの最大数を設定する例を示します。

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

### 始める前に

LACP 機能がイネーブルになっていることを確認します。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **lacp rate fast**

### 手順の詳細

	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 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 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。

### 例

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

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

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

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

## LACP 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。

**Before you begin**

LACP 機能がイネーブルになっていることを確認します。

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config)# **lACP system-priority** *priority*
3. (Optional) switch# **show lACP system-identifier**

**DETAILED STEPS**

	Command or Action	Purpose
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>lACP system-priority</b> <i>priority</i>	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	(Optional) switch# <b>show lACP system-identifier</b>	LACP システム識別子を表示します。

**Example**

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 ポート チャネルの各リンクに対して、ポート プライオリティの設定を行うことができます。

**Before you begin**

LACP 機能がイネーブルになっていることを確認します。

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot/port*
3. switch(config-if)# **lACP port-priority** *priority*

## DETAILED STEPS

	Command or Action	Purpose
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 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。

## Example

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。ダウンストリーム アクセス スイッチが Cisco Nexus デバイスでない場合は、LACP グレースフル コンバージェンス オプションをディセーブルにします。



(注) コマンドが実行される前に、ポートチャネルが管理上のダウン状態である必要があります。

## 始める前に

LACP をイネーブルにします。

## 手順の概要

1. **configure terminal**
2. **interface port-channel number**
3. **shutdown**
4. **no lacp graceful-convergence**

5. **no shutdown**
6. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b> 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)# <b>interface port-channel 1</b> 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	<b>shutdown</b> 例： switch(config-if) <b>shutdown</b>	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	<b>no lacp graceful-convergence</b> 例： switch(config-if)# <b>no lacp graceful-convergence</b>	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	<b>no shutdown</b> 例： switch(config-if) <b>no shutdown</b>	ポート チャネルを管理的にアップします。
ステップ 6	<b>copy running-config startup-config</b> 例： switch(config)# <b>copy running-config startup-config</b>	(任意) 実行設定をスタートアップ設定にコピーします。

## 例

次に、ポートチャネルの LACP グレースフル コンバージェンスをディセーブルにする方法を示します。

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

## LACP グレースフル コンバージェンスの再有効化

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

### 手順の概要

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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b> 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 <i>number</i></b> 例： switch(config)# <b>interface port-channel 1</b> 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	<b>shutdown</b> 例： switch(config-if) <b>shutdown</b>	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	<b>lacp graceful-convergence</b> 例： switch(config-if) # <b>lacp graceful-convergence</b>	ポートチャネルの LACP グレースフル コンバージェンスを無効にします。
ステップ 5	<b>no shutdown</b> 例： switch(config-if) <b>no shutdown</b>	ポートチャネルを管理的にアップします。
ステップ 6	<b>copy running-config startup-config</b> 例： switch(config)# <b>copy running-config startup-config</b>	(任意) 実行設定をスタートアップ設定にコピーします。

## 例

次に、ポートチャネルの LACP グレースフルコンバージェンスをイネーブルにする方法を示します。

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

## ポートチャネル設定の確認

次のコマンドを使用すると、ポートチャネル設定情報を確認することができます。

コマンド	目的
<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。
<b>show feature</b>	イネーブルにされた機能を表示します。
<b>show resource</b>	システムで現在利用可能なリソースの数を表示します。
<b>show lacp</b> {counters   interface <i>type slot/port</i>   neighbor   port-channel   system-identifier}	LACP 情報を表示します。
<b>show port-channel 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と同じにするパラメータを表示します。
<b>show port-channel database</b> [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。
<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。
<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。
<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。
<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。
<b>show port-channel load-balance</b>	ポートチャネルによるロードバランシングについての情報を表示します。



# ポートチャネルメンバーシップ整合性チェッカーのトリガー

ポートチャネルメンバーシップ整合性チェッカーを手動でトリガーして、ポートチャネル上のすべてのポートのハードウェア設定とソフトウェア設定を比較し、結果を表示することができます。ポートチャネルメンバーシップ整合性チェッカーを手動でトリガーして結果を表示するには、次のコマンドを特定のモードで使用します。

## 手順の概要

1. switch# **show consistency-checker membership port-channels**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# <b>show consistency-checker membership port-channels</b>	ポートチャネルのメンバーポートでポートチャネルメンバーシップの整合性チェックを開始し、その結果を表示します。

## 例

次に、ポートチャネルメンバーシップ整合性検査をトリガーして結果を表示する例を示します。

```
switch# show consistency-checker membership port-channels
Checks: Trunk group and trunk membership table.
Consistency Check: PASSED
No Inconsistencies found for port-channel1111:
  Module:1, Unit:0
    ['Ethernet1/4', 'Ethernet1/5', 'Ethernet1/6']
No Inconsistencies found for port-channel2211:
  Module:1, Unit:0
    ['Ethernet1/7', 'Ethernet1/8', 'Ethernet1/9', 'Ethernet1/10']
No Inconsistencies found for port-channel3311:
  Module:1, Unit:0
    ['Ethernet1/11', 'Ethernet1/12', 'Ethernet1/13', 'Ethernet1/14']
No Inconsistencies found for port-channel4095:
  Module:1, Unit:0
    ['Ethernet1/33', 'Ethernet1/34', 'Ethernet1/35', 'Ethernet1/36', 'Ethernet1/37', 'Ethernet1/38', 'Ethernet1/39', 'Ethernet1/40', 'Ethernet1/41', 'Ethernet1/42', 'Ethernet1/43', 'Ethernet1/44', 'Ethernet1/45', 'Ethernet1/46', 'Ethernet1/47', 'Ethernet1/48', 'Ethernet1/29', 'Ethernet1/30', 'Ethernet1/31', 'Ethernet1/32']
```

## ロードバランシング発信ポート ID の確認

### コマンドに関する注意事項

**show port-channel load-balance** コマンドを使用すると、ポートチャネルにおいて特定のフレームがいずれのポートにハッシュされるかを確認することができます。正確な結果を取得するためには、VLAN および宛先 MAC を指定する必要があります。



(注) ポートチャネル内にポートが1つしかない場合などには、一部のトラフィックフローはハッシュの対象になりません。

**show port-channel load-balance** コマンドは、ユニキャストトラフィックハッシュのみをサポートします。マルチキャストトラフィックハッシュはサポートされていません。

ロードバランシング発信ポート ID を表示する場合は、次のいずれかの操作を実行します。

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

### 例

次に、ロードバランシングの発信ポート ID を表示する例を示します。

```
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-port crc8_hash:204 Outgoing port id: Ethernet 1/1 Param(s) used to calculate
load balance:
dst-port: 0
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 プロファイル

多くのインターフェイス コマンドを含むポート プロファイルを作成し、一定範囲のインターフェイスにそのポート プロファイルを適用することができます。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
- ポートチャネル

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した場合、ポートプロファイルはデフォルトモードになります。デフォルトモードはレイヤ3です。ポートプロファイルをレイヤ2モードに変更するには、**switchport** コマンドを入力します。

ポートプロファイルをインターフェイスまたはインターフェイスの範囲にアタッチするときにポートプロファイルを継承します。ポートプロファイルをインターフェイスまたはインターフェイスの範囲にアタッチ、または継承する場合、そのポートプロファイルのすべてのコマンドがインターフェイスに適用されます。また、ポートプロファイルには、別のポートプロファイルの設定を継承することができます。別のポートプロファイルを継承した場合、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。

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

- 競合が発生した場合は、インターフェイスモードで入力したコマンドがポートプロファイルのコマンドに優先します。しかし、ポートプロファイルはそのコマンドをポートプロファイルに保持します。
- ポートプロファイルのコマンドに対してデフォルトのコマンドを明示的に優先させない限り、ポートプロファイルのコマンドがインターフェイスのデフォルトの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。

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。

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

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

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

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

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

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

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

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対してポートプロファイルを継承した後、特定の設定値を削除すると、それらのインターフェイスではそのポートプロファイル設定が機能しなくなります。

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、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、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。

## ポートプロファイルの設定

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

## ポートプロファイルの作成

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



(注) ポートプロファイル名には、次の文字のみを含めることができます。

- a ~ z
- A ~ Z
- 0 ~ 9
- 次の場合を除き、特殊文字は使用できません。
  - .
  - -
  - \_

### 手順の概要

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

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<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。

	コマンドまたはアクション	目的
ステップ 2	<b>port-profile</b> [type { <b>ethernet</b>   <b>interface-vlan</b>   <b>port-channel</b> }] <i>name</i>	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	<b>exit</b>	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	(任意) <b>show port-profile</b>	ポートプロファイル設定を表示します。
ステップ 5	(任意) <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

### 例

次の例は、イーサネットインターフェイスに対して **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たものです。

```
switch# configure terminal
switch(config)# port-profile type ethernet 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変更するには、ポートプロファイルコンフィギュレーションモードにする必要があります。

### 手順の概要

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

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<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。

	コマンドまたはアクション	目的
ステップ 2	<b>port-profile</b> [type { <b>ethernet</b>   <b>interface-vlan</b>   <b>port-channel</b> }] <i>name</i>	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、ポート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	<b>exit</b>	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	(任意) <b>show port-profile</b>	ポートプロファイル設定を表示します。
ステップ 5	(任意) <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

### 例

次に、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 ethernet 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* | **port-channel** *number*]
3. **inherit port-profile** *name*
4. **exit**
5. (任意) **show port-profile**
6. (任意) **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<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	<b>interface</b> [ethernet <i>slot/port</i>   <b>interface-vlan</b> <i>vlan-id</i>   <b>port-channel</b> <i>number</i> ]	インターフェイスの範囲を選択します。
ステップ 3	<b>inherit port-profile</b> <i>name</i>	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	<b>exit</b>	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	(任意) <b>show port-profile</b>	ポートプロファイル設定を表示します。
ステップ 6	(任意) <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## 例

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

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

## 特定のポートプロファイルのイネーブル化

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

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

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

## 手順の概要

### 1. configure terminal



2. **port-profile** [**type** {**ethernet** | **interface-vlan** | **port-channel**}] *name*
3. **state enabled**
4. **exit**
5. (任意) **show port-profile**
6. (任意) **copy running-config startup-config**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<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	<b>port-profile</b> [ <b>type</b> { <b>ethernet</b>   <b>interface-vlan</b>   <b>port-channel</b> }] <i>name</i>	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	<b>state enabled</b>	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	<b>exit</b>	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	(任意) <b>show port-profile</b>	ポート プロファイル設定を表示します。
ステップ 6	(任意) <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

#### 例

次の例は、ポートプロファイル 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 ethernet test
switch(config-ppm)# state enabled
switch(config-ppm)#
```

## ポート プロファイルの継承

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

#### 手順の概要

1. **configure terminal**
2. **port-profile** *name*

3. **inherit port-profile name**
4. **exit**
5. (任意) **show port-profile**
6. (任意) **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<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	<b>port-profile name</b>	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	<b>inherit port-profile name</b>	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	<b>exit</b>	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	(任意) <b>show port-profile</b>	ポートプロファイル設定を表示します。
ステップ 6	(任意) <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## 例

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

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

## 一定範囲のインターフェイスからのポートプロファイルの削除

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

## 手順の概要

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

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<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	<b>interface</b> [ethernet <i>slot/port</i>   <b>interface-vlan</b> <i>vlan-id</i>   <b>port-channel</b> <i>number</i> ]	インターフェイスの範囲を選択します。
ステップ 3	<b>no inherit port-profile</b> <i>name</i>	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から割り当て解除します。
ステップ 4	<b>exit</b>	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	(任意) <b>show port-profile</b>	ポートプロファイル設定を表示します。
ステップ 6	(任意) <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## 例

次に、イーサネット インターフェイス 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割り当て解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。この設定は、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. (任意) **show port-profile**
6. (任意) **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<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	<b>port-profile name</b>	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	<b>no inherit port-profile name</b>	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	<b>exit</b>	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	(任意) <b>show port-profile</b>	ポートプロファイル設定を表示します。
ステップ 6	(任意) <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## 例

次の例では、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)#
```



## 第 5 章

# 仮想ポートチャネルの設定

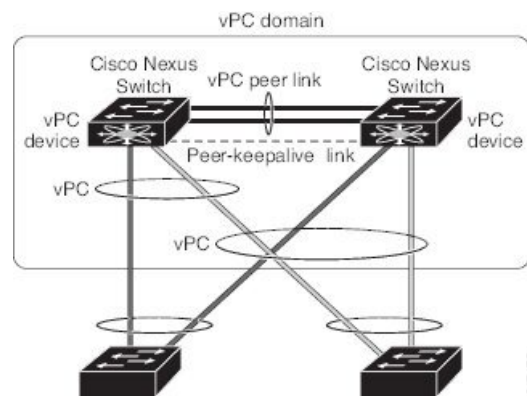
- vPC について (82 ページ)
- VLAN ごとの整合性検査 (88 ページ)
- vPC 自動リカバリ (88 ページ)
- vPC ピア リンク, on page 89
- vPC 番号, on page 90
- その他の機能との vPC の相互作用 (91 ページ)
- vPC フォークリフト アップグレード (92 ページ)
- VRF に関する注意事項と制約事項 (96 ページ)
- vPC 設定の確認, on page 97
- グレースフル タイプ 1 検査ステータスの表示 (98 ページ)
- グローバル タイプ 1 不整合の表示 (99 ページ)
- インターフェイス別タイプ 1 不整合の表示 (100 ページ)
- VLAN ごとの整合性ステータスの表示 (101 ページ)
- vPC のデフォルト設定, on page 104
- vPC の設定 (104 ページ)
- 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, on page 107
- vPC ピア リンクの作成, on page 109
- 設定の互換性の検査 (110 ページ)
- vPC 自動リカバリのイネーブル化 (112 ページ)
- 復元遅延時間の設定 (113 ページ)
- vPC ピア リンク障害発生時における VLAN インターフェイスのシャットダウン回避 (114 ページ)
- VRF 名の設定 (115 ページ)
- 他のポートチャネルの vPC への移行, on page 115
- vPC ドメイン MAC アドレスの手動での設定, on page 117
- システム プライオリティの手動での設定, on page 118
- vPC ピア スイッチのロールの手動による設定, on page 119
- Layer 3 over vPC の設定 (120 ページ)

## vPC について

### vPC の概要

仮想ポートチャネル (vPC) を使用すると、物理的には2台の異なる Cisco Nexus デバイスに接続されている複数のリンクを、第3のデバイスからは単一のポートチャネルとして認識されるようにすることができます (次の図を参照)。第3のデバイスには、スイッチやサーバなどあらゆる networking デバイスが該当します。vPC では、マルチパス機能を使用することができます。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、さらには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り、冗長性が確保されます。

Figure 5: vPC のアーキテクチャ



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
- リンク集約制御プロトコル (LACP)

vPC ピア リンク チャネルなど、vPC で EtherChannel を設定した場合、それぞれのスイッチでは1つの EtherChannel に最大 32 個のアクティブ リンクをまとめることができます。



**Note** 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ためには、vPC 機能を実現する2つの vPC ピア スイッチの vPC ドメインにピアキープアライブ リンクおよびピアリンクを作成する必要があります。

vPC ピア リンクを作成する場合は、まず一方の Cisco Nexus デバイス上で、2つ以上の Ethernet ポートを使用して EtherChannel を設定します。さらに他方のスイッチ上で、2つ以上の Ethernet ポートを使用して別の EtherChannel を設定します。これら2つの EtherChannel を接続することにより、vPC ピア リンクが作成されます。



**Note** vPC ピアリンク EtherChannel はトランクとして設定することが推奨されます。

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 チャンネルが含まれます。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。



**Note** EtherChannel を使用する vPC デバイスはすべて、両方の vPC ピア デバイスに接続する必要があります。

vPC には次のような利点があります。

- 単独のデバイスが、2つのアップストリーム デバイスを介して EtherChannel を使用できるようになります。
- 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。
- リンクまたはスイッチに障害が発生した場合、高速コンバージェンスが実行されます。
- 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。

## 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 により接続されることで対をなす個々のデバイス。
- 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 : 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ポート チャネルが含まれるドメイン。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、両スイッチで同じであることが必要です。

- vPC ピアキープアライブ リンク：ピアキープアライブ リンクでは、さまざまな vPC ピア Cisco Nexus デバイスの稼働力のモニタリングが行われます。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。

vPCs ピアキープアライブ リンク上を移動するデータまたは同期トラフィックはありません。このリンクを流れるトラフィックは、送信元スイッチが稼働しており、vPC を実行していることを知らせるメッセージだけです。

## vPC ドメイン

vPC ドメインを作成するには、まず各 vPC ピア スイッチに対し、1 ~ 1000 の範囲にある値を使用して vPC ドメイン ID を作成する必要があります。この ID は、対象となるすべての vPC ピア デバイス上で同じであることが必要です。

EtherChannel および vPC ピア リンクは、LACP を使用するかまたはプロトコルなしのいずれかで設定できます。可能な場合、ピアリンクで LACP を使用することを推奨します。これは、LACP が EtherChannel の設定の不一致に対する設定チェックを提供するためです。

vPC ピア スイッチでは、設定した vPC ドメイン ID に基づいて、一意の vPC システム MAC アドレスが自動的に割り当てられます。各 vPC ドメインには一意の MAC アドレスがあり、vPC に関連する特定の処理の際に固有識別子として使用されます。ただしスイッチで vPC システム MAC アドレスが使用されるのは、LACP などリンク関連の処理に限ります。連続したネットワーク内の vPC ドメインはそれぞれ、一意のドメイン ID を使用して作成することが推奨されます。ただし、Cisco NX-OS ソフトウェアでアドレスを割り当てる代わりに、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 スイッチでは、設定した vPC ドメイン ID に基づいて、一意の vPC システム MAC アドレスが自動的に割り当てられます。スイッチで vPC システム MAC アドレスが使用されるのは、LACP や BPDU などリンク関連の処理に限ります。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。

どちらのピアにも同じ vPC ドメイン ID を設定することが推奨されます。またドメイン ID はネットワーク内で一意であることが必要です。たとえば、2つの異なる vPC（一方がアクセススイッチ、もう一方が集約スイッチ）がある場合は、それぞれの vPC に固有のドメイン ID を割り当ててください。

vPC ドメインを作成すると、その vPC ドメインのシステムプライオリティが Cisco NX-OS ソフトウェアによって自動的に作成されます。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。



**Note** 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 スイッチ上に同じプライオリティ値を割り当てるようにしてください。両側の vPC ピア スイッチに異なるシステムプライオリティ値が割り当てられている場合、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 ソフトウェアでは、vPC ピア間のピアキープアライブリンクを使用して、設定可能なキープアライブメッセージが定期的送信されます。これらのメッセージを送信するためには、ピアスイッチ間にレイヤ3 接続が必要です。ピアキープアライブリンクがアップ状態で稼働していなければ、システムでは vPC ピアリンクをアップすることができません。

一方の vPC ピアスイッチに障害が発生すると、vPC ピアリンクのもう一方の側にある vPC ピアスイッチでは、ピアキープアライブメッセージを受信しなくなることによってその障害を検知します。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。この時間間隔は、400 ミリ秒～10 秒の範囲で設定することができます。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の確認は、ピアリンクがダウンした場合にのみ行われます。

vPC ピアキープアライブは、Cisco Nexus デバイス上の管理 VRF でもデフォルトの VRF でも伝送できます。管理 VRF を使用するようスイッチを設定した場合は、`mgmt 0` インターフェイスの IP アドレスがキープアライブメッセージの送信元および宛先となります。デフォルトの VRF を使用するようスイッチを設定した場合は、vPC 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の役割を果たす 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 アドレスがどちらもネットワーク上で一意であり、かつそれらの IP アドレスがその vPC ピアキープアライブリンクに関連付けられている VRF から到達可能であることを確認してください。



**Note** Cisco Nexus デバイスの vPC ピアキープアライブリンクは、管理 VRF で `mgmt 0` インターフェイスを使用して実行されるように設定することが推奨されます。デフォルトの VRF を設定する場合は、vPC ピアキープアライブメッセージの伝送に vPC ピアリンクが使用されないようにしてください。

## 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、さらに両方の vPC ピアスイッチ上でピアリンクを設定すると、シスコファブリックサービス (CFS) メッセージにより、ローカル vPC ピアスイッチに関する設定のコピーがリモート vPC ピアスイッチへ送信されます。これによりシステムでは、2つのスイッチ間で重要な設定パラメータに違いがないかどうか判定が行われます。

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 に関する互換性チェックのプロセスは、正規の EtherChannel に関する互換性チェックとは異なります。

### vPC ポートチャネルでの新しいタイプ2 整合性チェック

vPC ポートチャネルのスイッチポート MAC 学習設定を検証するために、新しいタイプ2 整合性チェックが追加されました。 **show vpc consistency-check vPC <vpc no.>** の CLI は、MAC 学習設定のローカル値とピア値を表示するように拡張されました。これはタイプ2チェックであるため、ローカル値とピア値の間に不一致がある場合でも vPC は動作しますが、CLI 出力から不一致が表示されることがあります。

```
switch# sh vpc consistency-parameters vpc 1112
```

Legend:

Type 1 : vPC will be suspended in case of mismatch

Name Value	Type	Local Value	Peer
Shut Lan	1	No	No
STP Port Type	1	Default	Default
STP Port Guard	1	None	None
STP MST Simulate PVST	1	Default	Default
nve configuration lag-id	1	nve	nve
	1	[(fa0, 0-23-4-ee-be-64, 8458, (8000, f4-4e-5-84-5e-3c, 457, 0, 0)], (8000, f4-4e-5-84-5e-3c, 457, 0, 0)]	[(fa0, 0, 0), (8000, 0, 0)]
mode	1	active	active
Speed	1	10 Gb/s	10 Gb/s
Duplex	1	full	full
Port Mode	1	trunk	trunk
Native Vlan	1	1	1
MTU	1	1500	1500
Admin port mode	1		
Switchport MAC Learn	2	Enable	Disable>
Newly added consistency parameter			
vPC card type	1	Empty	Empty
Allowed VLANs	-	311-400	311-400
Local suspended VLANs	-	-	-

## 同じでなければならない設定パラメータ

ここで説明する設定パラメータは、vPC ピアリンクの両側のスイッチ上で設定が同じであることが必要です。



### Note

ここで説明する動作パラメータおよび設定パラメータは、vPC 内のすべてのインターフェイスで一致している必要があります。

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。

スイッチでは、vPC インターフェイス上でこれらのパラメータに関する互換性チェックが自動的に行われます。インターフェイス別のパラメータはインターフェイスごとに整合性を保っていることが必要であり、グローバルパラメータはグローバルに整合性を保っていることが必要です。

- 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
- マルチ スパニングツリーの STP 領域コンフィギュレーション (MST)
- 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：vPC インターフェイスはすべて標準ポートとして設定することが推奨されます
  - 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

これらのうち、イネーブルでないパラメータや一方のスイッチでしか定義されていないパラメータは、vPC の整合性検査では無視されます。

**Note**

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で、両側の vPC ピア スイッチ上の設定が一致しないと、誤設定に伴ってトラフィック 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 ピアリンクの両端にある各スイッチの VLAN インターフェイスは同じ VLAN 用に設定されている必要があり、さらにそれらの管理モードおよび動作モードも同じであることが必要です。ピアリンクの一方のスイッチでのみ設定されている VLAN では、vPC またはピアリンクを使用したトラフィックの転送は行われません。VLAN はすべて、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。両方で作成されていない場合、VLAN は停止することになります。
- ACL のすべての設定とパラメータ
- Quality of Service (QoS) の設定およびパラメータ：ローカルパラメータです。グローバルパラメータは同じであることが必要です
- 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
  - 優先度
  - VLAN (Rapid PVST+)

すべての設定パラメータについて互換性があることを確認するためにも、vPC の設定後は各 vPC ピアスイッチの設定を表示することが推奨されます。

## VLAN ごとの整合性検査

VLAN 上でスパンニングツリーのイネーブル/ディセーブルが切り替わるたびに、いくつかのタイプ 1 整合性検査が VLAN 単位で実行されます。この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でダウン状態になりますが、その他の VLAN は影響を受けません。

## vPC 自動リカバリ

両側の vPC ピアスイッチでリロードが実行され、かつ一方のスイッチのみリブートした場合、自動リカバリによってそのスイッチがプライマリスイッチとして機能し、一定時間が経過した後に vPC リンクがアップ状態になります。このシナリオにおけるリロード遅延時間は、240～3600 秒の範囲で設定できます。

ピアリンクの障害に伴ってセカンダリ vPC スイッチ上の vPC がディセーブルになり、さらにプライマリ vPC スイッチで障害が発生するか、またはトラフィックが転送できなくなると、セカンダリスイッチでは vPC が再イネーブル化されます。このシナリオの場合、vPC ではキープアラームが 3 回連続して検出されないのを待ってから vPC リンクが回復します。

vPC 自動リカバリ機能は、デフォルトでイネーブルです。

## 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。



**Note** 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 ピア リンクの概要

vPC ピアとして設定できるのは、対をなす2台のスイッチです。それぞれのスイッチは互いに、他方のvPC ピアに対してのみvPC ピアとして機能します。vPC ピア スイッチには、他のスイッチへの非vPC リンクを設定することもできます。

適正な設定を行うため、各スイッチにEtherChannelを設定し、さらにvPC ドメインを設定します。各スイッチのEtherChannelをピアリンクとして割り当てます。冗長性を確保できるよう、EtherChannelには少なくとも2つの専用ポートを設定することが推奨されます。これにより、vPC ピアリンクのインターフェイスの1つに障害が発生すると、スイッチは自動的にフォールバックし、そのピアリンクの別のインターフェイスが使用されます。



**Note** EtherChannel はトランク モードで設定することが推奨されます。

多くの動作パラメータおよび設定パラメータは、vPC ピア リンクにより接続されている各スイッチ上で同じ値であることが必要です。各スイッチは管理プレーンから完全に独立しているため、重要なパラメータについてスイッチ同士に互換性があることを確認する必要があります。vPC ピア リンクの設定が完了したら、各vPC ピア スイッチの設定を表示し、それらの設定に互換性があることを確認してください。



**Note** vPC ピア リンクによって接続されている2つのスイッチでは必ず、同一の動作パラメータおよび設定パラメータが設定されている必要があります。

vPC ピア リンクを設定する際、vPC ピア スイッチでは、接続されたスイッチの一方がプライマリスイッチ、もう一方がセカンダリスイッチとなるようにネゴシエーションが行われます。デフォルトの場合、Cisco NX-OS ソフトウェアでは、最小のMACアドレスを基にプライマリスイッチが選択されます。特定のフェールオーバー条件の下でのみ、このソフトウェアは各スイッチ（つまり、プライマリ スイッチとセカンダリ スイッチ）に対して別々の処理を行います。プライマリ スイッチに障害が発生した場合、システムが回復した時点でセカンダリ スイッチがプライマリ スイッチとして動作し、元々のプライマリ スイッチがセカンダリ スイッチとなります。

ただし、どちらの vPC スイッチをプライマリ スイッチにするか設定することもできます。一方の vPC スイッチをプライマリ スイッチにするためロール プライオリティを再設定する場合は、まずプライマリ vPC スイッチとセカンダリ vPC スイッチのそれぞれに対してロール プライオリティを適切な値に設定し、**shutdown** コマンドを入力して両スイッチの vPC ピア リンクである EtherChannel をシャットダウンした後、**no shutdown** コマンドを入力して両スイッチの EtherChannel を再度イネーブルにします。

ピア間では、vPC リンクを介して認識された MAC アドレスの同期も行われます。

設定情報は、Cisco Fabric Service over Ethernet (CFSoS) プロトコルを使用して vPC ピア リンクを転送されます。両方のスイッチ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、CFSoS が使用されます。

vPC ピア リンクに障害が発生すると、ソフトウェアでは、両方のスイッチが稼働していることを確認するため、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確認が行われます。vPC ピア スイッチが稼働している場合は、セカンダリ vPC スイッチにあるすべて vPC ポートがディセーブルになります。さらにデータは、EtherChannel において依然アクティブ状態にある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 リンクを介してキープアライブ メッセージが返されない場合、vPC ピア スイッチに障害が発生したと認識します。

vPC ピア スイッチ間では、別途用意されたリンク (vPC 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 メッセージが送信されます。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により、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判断されます。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 リンクを作成すると、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 を作成することができます。ダウンストリーム スイッチ上で EtherChannel を 1 つだけ作成し、そのポートの半分をプライマリ vPC ピア スイッチ用、残りの半分をセカンダリ vPC ピア スイッチ用として使用します。

各 vPC ピア スイッチ上では、ダウンストリーム スイッチに接続された 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、各 EtherChannel に対してその EtherChannel と同じ番号の vPC ID 番号を割り当てることもできます (EtherChannel 10 に対しては vPC ID 10 を割り当てるなど)。



**Note** 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 チャネルに割り当てる 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

Link Aggregation Control Protocol (LACP) では、vPC ドメインのシステム MAC アドレスに基づいて、その vPC に対する LACP Aggregation Group (LAG) ID が構成されます。

LACP は、ダウンストリームスイッチからのチャンネルも含め、すべての vPC EtherChannel 上で使用できます。vPC ピアスイッチの各 EtherChannel のインターフェイスに対しては、LACP をアクティブモードで設定することが推奨されます。この設定により、スイッチ、単方向リンク、およびマルチホップ接続の間の互換性をより簡単に検出できるようになり、実行時の変更およびリンク障害に対してダイナミックな応答が可能になります。

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



**Note** 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 ピアスイッチ上に同じプライオリティ値を割り当てるようにしてください。両側の vPC ピアスイッチに異なるシステムプライオリティ値が割り当てられている場合、vPC は稼働しません。

### vPC ピアリンクと STP

vPC 機能の初回起動時には、STP は再コンバージェンスします。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が推奨されます。

一連のパラメータは、vPC ピアリンクの両端の vPC ピアスイッチ上で設定を同じにする必要があります。

STP は分散型です。つまり、このプロトコルは、両端の vPC ピアスイッチ上で継続的に実行されます。ただし、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 プロセスは、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により制御されます。

プライマリ vPC スイッチでは、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 状態の同期化が行われます。

vPC ピアスイッチ間では、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が vPC マネージャによって実行されます。さらにプライマリ vPC ピアスイッチにより、プライマリスイッチおよびセカンダリスイッチの vPC インターフェイスに対する STP プロトコルの制御が行われます。

ブリッジプロトコルデータユニット (BPDU) では、代表ブリッジ ID フィールドの STP ブリッジ ID として、vPC に対して設定された MAC アドレスが使用されます。これら vPC インターフェイスの BPDU は vPC プライマリ スイッチにより送信されます。



**Note** 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場合は、**show spanning-tree** コマンドを使用します。

## CFSOE

Cisco Fabric Services over Ethernet (CFSOE) は、vPC ピア デバイスの動作を同期化するために使用される信頼性の高い状態転送メカニズムです。CFSOE は、vPC にリンクされている、STP、IGMP などの多くの機能のメッセージとパケットを伝送します。情報は、CFS/CFSOE プロトコルデータユニット (PDU) に入れて伝送されます。

CFSOE は、vPC 機能をイネーブルにすると、デバイスによって自動的にイネーブルになります。何も設定する必要はありません。vPC の CFSOE 分散には、IP を介してまたは CFS リージョンに分散する機能は必要ありません。CFSOE 機能が vPC 上で正常に機能するために必要な設定は一切ありません。

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



**Note** **no cfs eth distribute** または **no cfs distribute** コマンドは入力しないでください。vPC 機能に対しては CFSOE をイネーブルにする必要があります。vPC がイネーブルの場合にこれらのコマンドのいずれかを入力すると、エラー メッセージが表示されます。

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

## vPC フォークリフト アップグレード

次に、vPC トポロジ内の Cisco Nexus 3600 プラットフォーム スイッチのペアから異なる Cisco Nexus 3600 プラットフォーム スイッチのペアへの移行のシナリオについて説明します。

vPC フォークリフト アップグレードの考慮事項：

- vPC ロール選択とスティッキビット

2つの vPC システムを結合して vPC ドメインを形成する場合、優先順位によって、どのデバイスが vPC プライマリで、どのデバイスが vPC セカンダリであるかが決まります。プライマリデバイスがリロードされると、システムがオンラインに戻り、vPC セカンダリデバイス（現在動作中のプライマリ）への接続が復元されます。セカンダリデバイス（動作上のプライマリ）の動作ロールは変更されません（不要な中断を回避するため）。この



動作は、スティッキ情報がスタートアップコンフィギュレーションに保存されないスティッキビットで実現されます。この方法では、動作中のデバイスがリロードされたデバイスよりも優先されます。したがって、vPC プライマリは vPC の動作中のセカンダリになります。スティッキビットは、vPC ノードがピアリンクおよびピアキープアライブダウンで起動し、自動回復期間後にプライマリになるときにも設定されます。

• vPC の遅延復元

リロード後、そしてピア隣接が確立されたとき、復元された vPC ピア デバイス上で vPC が起動するのを遅延するには、delay restore タイマーを使用します。

復元した vPC ピア デバイス上の VLAN インターフェイスが起動するのを遅延するには、**interfaces-vlan** オプションを **delay restore** のオプション コマンドを使用して、ACI イメージがスタンドアロン スイッチに正常に転送されたことを確認します。

• vPC 自動リカバリ

データセンターの停電中、両方のvPCピアスイッチがダウンした場合、一方のスイッチのみが復元された場合、自動回復機能により、そのスイッチがプライマリスイッチの役割を引き継ぎ、自動回復期間後にvPCリンクが起動します。デフォルトの自動回復期間は240秒です。

次の例は、vPC ピア ノード Node1 と Node2 を New\_Node1 と New\_Node2 に置き換える移行シナリオです。

	移行手順	予期される動作	Node1 で設定されるロール (たとえばロールプライオリティ 100)	Node1 の動作ロール。	Node1 で設定されるロール (たとえばロールプライオリティ 200)	Node2 の動作ロール。
1	初期状態	トラフィックは vPC ピアの両方 (Node1 と Node2) によって転送されます。  Node1 はプライマリで、Node2 はセカンダリです。	プライマリ	プライマリ  スティッキビット : False	secondary	セカンダリ  スティッキビット : False

	移行手順	予期される動作	Node1で設定されるロール (たとえばロールプライオリティ 100)	Node1の動作ロール。	Node1で設定されるロール (たとえばロールプライオリティ 200)	Node2の動作ロール。
2	Node2の交換： Node2のすべてのvPCとアップリンクをシャットダウンします。ピアリンクおよびvPCピアキープアライブは管理アップ状態です。	プライマリ vPCピア Node1でトラフィックが収束しました。	プライマリ	プライマリ スティッキービット：False	secondary	セカンダリ スティッキービット：False
3	Node2を削除します。	Node1は引き続きトラフィックを転送します。	プライマリ	プライマリ スティッキービット：False	適用対象外	適用対象外
4	New_Node2を設定します。設定をスタートアップコンフィギュレーションにコピーします。vPCピアリンクおよびピアキープアライブは管理上アップ状態です。 New_Node2の電源をオフにします。 すべての接続部を接続します。 New_Node2の電源をオンにします。	New_Node2がセカンダリとして起動します。 Node1は引き続きプライマリです。 トラフィックは引き続きNode1で転送されます。	プライマリ	プライマリ スティッキービット：False	secondary	セカンダリ スティッキービット：False

	移行手順	予期される動作	Node1で設定されるルール (たとえばルールプライオリティ100)	Node1の動作ルール。	Node1で設定されるルール (たとえばルールプライオリティ200)	Node2の動作ルール。
5	New_Node2のすべてのvPCとアップリンクポートを起動します。	トラフィックは、Node1とNew_Node2の両方によって転送されます。	プライマリ	プライマリ スティッキービット: False	secondary	セカンダリ スティッキービット: False
6	Node1の交換: Node1でvPCとアップリンクをシャットダウンします。	トラフィックはNew_Node2に収束します。	プライマリ	プライマリ スティッキービット: False	secondary	セカンダリ スティッキービット: False
7	Node1を削除します。	New_Node2がセカンダリ、運用上のプライマリになり、スティッキービットはTrueに設定されます。	適用対象外	適用対象外	secondary	プライマリ スティッキービット: True
8	New_Node1を設定します。実行コンフィギュレーションをスタートアップにコピーします。  新しいNode1の電源をオフにします。すべての接続部を接続します。New_Node1の電源をオンにします。	New_Node1がプライマリ、運用上のセカンダリとして起動します。	プライマリ	セカンダリ スティッキービット: False	secondary	プライマリ スティッキービット: True

	移行手順	予期される動作	Node1で設定されるロール (たとえばロールプライオリティ 100)	Node1の動作ロール。	Node1で設定されるロール (たとえばロールプライオリティ 200)	Node2の動作ロール。
9	New_Node1のすべてのvPCとアップリンクポートを起動します。	トラフィックは、New_Node1とNew_Node2の両方によって転送されます。	プライマリ	セカンダリ ステイックビット : False	secondary	プライマリ ステイックビット : True



(注) 設定済みのセカンダリノードを運用上のセカンダリとして設定し、設定済みのプライマリを運用上のプライマリとして使用する場合は、移行の最後にNode2をリロードできます。これは任意で、クラスタに対する機能上の影響はありません。

## VRFに関する注意事項と制約事項

vPC設定時の注意事項と制限事項は次のとおりです。

- vPCは、異なるタイプのCisco Nexus 3000シリーズスイッチ間ではサポートされません。
- VPCピアには、VXLAN用に同じ予約済みVLANが必要です。ピアの予約済みVLANが異なると、VXLANで望ましくない動作が発生する可能性があります。
- CLIコマンドの **sh vpc brief** の出力に、Delay-restore status と Delay-restore SVI status の2つの追加のフィールドが表示されます。
- vPCピアリンクおよびvPCインターフェイスを設定する場合は、あらかじめvPC機能をイネーブルにしておく必要があります。
- システムにおいてvPCピアリンクを構成するためには、その前に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。
- vPCピアリンクは、少なくとも2つの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構成する必要があります。
- どちらのピアにも同じvPCドメインIDを設定することが推奨されます。またドメインIDはネットワーク内で一意であることが必要です。たとえば、2つの異なるvPC（一方がアクセススイッチ、もう一方が集約スイッチ）がある場合は、それぞれのvPCに固有のドメインIDを割り当ててください。

- vPC に使用できるのは、ポートチャネルのみです。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。
- 両側の vPC ピアスイッチを設定する必要があります。ただし vPC ピアデバイス間で設定が自動的に同期化されることはありません。
- 必要な設定パラメータが、vPC ピアリンクの両側で互換性を保っているかチェックしてください。
- 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 内の LACP を使用するポートチャネルはすべて、アクティブモードのインターフェイスで設定することが推奨されます。
- vPC の最初のメンバが起動すると、トラフィックが中断する可能性があります。
- OSPF over vPC および BFD with OSPF は、Cisco Nexus 3000 シリーズスイッチでサポートされます。

SVI の制限：BFD セッションが仮想ポートチャネル（vPC）ピアリンクを使用して SVI 経由で行われる場合、BFD エコー機能はサポートされません。SVI 設定レベルで **no bfd echo** を使用して、vPC ピアノード間で行われる SVI 経由のすべてのセッションに関して BFD エコー機能を無効にする必要があります。

- mgmt インターフェイスの代わりにレイヤ 3 リンクがピアキーブアライブに使用され、CPU キューがコントロールプレーントラフィックで輻輳している場合、vPC ピアキーブアライブパケットがドロップされる可能性があります。CPU トラフィックには、ルーティングプロトコル、ARP、Glean、および IPMC ミスパケットが含まれます。ピアキーブアライブインターフェイスが管理インターフェイスではなくレイヤ 3 リンクの場合、vPC ピアキーブアライブパケットは低優先度キューで CPU に送信されます。

レイヤ 3 リンクが vPC ピアキーブアライブに使用される場合は、次の ACL を設定して vPC ピアキーブアライブを優先します。

```
ip access-list copp-system-acl-routingproto2
30 permit udp any any eq 3200
```

ここでは、3200 がキーブアライブパケットのデフォルト UDP ポートです。この ACL は、デフォルトポートが変更された場合に、設定された UDP ポートと一致する必要があります。

## vPC 設定の確認

vPC の設定情報を表示する場合は、次のコマンドを使用します。

コマンド	目的
switch# <b>show feature</b>	vPC がイネーブルかどうかを表示します。

コマンド	目的
switch# <b>show port-channel capacity</b>	設定されている EtherChannel の数、およびスイッチ上でまだ使用可能な EtherChannel の数を表示します。
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 システムの 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。  <b>Note</b> 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。

スイッチの出力に関する詳細については、ご使用の Cisco Nexus シリーズ スイッチに関する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検査ステータスの表示

次に、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例を示します。

```
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
Auto-recovery status         : Disabled
Delay-restore status         : Timer is off.(timeout = 30s)
Delay-restore SVI status     : Timer is off.(timeout = 10s)

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不整合が発生すると、セカンダリスイッチのvPCはダウンします。次の例は、スパンニングツリーモードでの不一致に伴って生じたこのタイプの不整合を示したものです。

次に、セカンダリスイッチ上の一時停止されたvPC VLANのステータスを表示する例を示します。

```

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 -

```

次に、プライマリスイッチ上の不整合ステータス（プライマリvPC上のVLANは一時停止されていない）を表示する例を示します。

```

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 Mo
de 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

```

## インターフェイス別タイプ1不整合の表示

インターフェイス別タイプ1不整合が発生すると、セカンダリスイッチのvPCポートはダウンしますが、プライマリスイッチのvPCポートはアップ状態が維持されます。次の例は、スイッチポートモードでの不一致に伴って生じたこのタイプの不整合を示したものです。

次に、セカンダリスイッチ上の一時停止されたvPC VLANのステータスを表示する例を示します。

```

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
Auto-recovery status           : Disabled
Delay-restore status           : Timer is off.(timeout = 30s)
Delay-restore SVI status       : Timer is off.(timeout = 10s)

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

```



次に、プライマリスイッチ上の不整合ステータス（プライマリ vPC 上の VLAN は一時停止されていない）を表示する例を示します。

```
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               : primary
Number of vPCs configured : 2
Peer Gateway          : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status   : Disabled
Delay-restore status   : Timer is off.(timeout = 30s)
Delay-restore SVI status : Timer is off.(timeout = 10s)

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 ごとの整合性ステータスの表示

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

### 例

次に、プライマリおよびセカンダリスイッチ上の VLAN の整合ステータスを表示する例を示します。

```
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
```

## VLAN ごとの整合性ステータスの表示

```
Type-2 consistency status      : success
vPC role                       : secondary
Number of vPCs configured     : 2
Peer Gateway                   : Disabled
Dual-active excluded VLANs    : -
Graceful Consistency Check    : Enabled
Auto-recovery status          : Disabled
Delay-restore status           : Timer is off.(timeout = 30s)
Delay-restore SVI status      : Timer is off.(timeout = 10s)
```

```
vPC Peer-link status
```

```
-----
id  Port  Status Active vlans
--  ---  -----
1   Pol   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
```

次に、セカンダリスイッチ上の VLAN ごとの整合ステータスを **Failed** として表示する例を示します。

```
switch(config)# 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
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 and BDs : -
Graceful Consistency Check    : Enabled
Auto-recovery status          : Enabled, timer is off.(timeout = 240s)
Delay-restore status           : Timer is off.(timeout = 30s)
Delay-restore SVI status      : Timer is off.(timeout = 10s)
```

```
vPC Peer-link status
```

```
-----
id  Port      Status Active vlans
--  ---  -----
1   Po1000    up    1-5,8,11-19
-----
```

```
vPC status
```

```
-----
id  Port      Status Consistency Active VLANs
-----
101 Po101      up    success    1-5,8,11-19
-----
```

```
102 Po102 up success 1-5,8,11-19
```

次に、プライマリスイッチ上の VLAN ごとの整合ステータスを Failed として表示する例を示します。

```
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
Auto-recovery status   : Disabled
Delay-restore status   : Timer is off.(timeout = 30s)
Delay-restore SVI status : Timer is off.(timeout = 10s)

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
STP Disabled                               1 vPC type-1 configuration incompatible - STP is enabled or disabled on some or all vlans 0-4,6-4095
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
BPDUFilter, 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

次の表は、vPC パラメータのデフォルト設定をまとめたものです。

Table 8: デフォルト vPC パラメータ

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

## vPC の設定

### vPC のイネーブル化

vPC を設定して使用する場合は、事前に vPC 機能をイネーブルにしておく必要があります。

#### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **feature vpc**
3. (Optional) switch# **show feature**
4. (Optional) switch# **copy running-config startup-config**

#### DETAILED STEPS

	Command or Action	Purpose
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 vpc</b>	スイッチで vPC をイネーブルにします。
ステップ 3	(Optional) switch# <b>show feature</b>	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	(Optional) switch# <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

**Example**

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。

**Note**

vPC 機能をディセーブルにすると、Cisco Nexus デバイスはすべての vPC 設定をクリアします。

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config)# **no feature vpc**
3. (Optional) switch# **show feature**
4. (Optional) switch# **copy running-config startup-config**

**DETAILED STEPS**

	Command or Action	Purpose
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>no feature vpc</b>	スイッチで vPC をディセーブルにします。
ステップ 3	(Optional) switch# <b>show feature</b>	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	(Optional) switch# <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

**Example**

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

両側の vPC ピア スイッチに対して、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 を基に、vPC システムの MAC アドレスが自動的に構成されます。

### Before you begin

vPC 機能をイネーブルにしていることを確認します。

vPC ピア リンクの両端にあるそれぞれのスイッチで設定を行う必要があります。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vpc domain domain-id**
3. (Optional) switch# **show vpc brief**
4. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
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>vpc domain domain-id</b>	スイッチに対して 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。 <i>domain-id</i> のデフォルト値はありません。指定できる値の範囲は 1 ~ 1000 です。 <b>Note</b> 既存の vPC ドメインに対して vpc-domain コンフィギュレーション モードを開始する場合は、 <b>vpc domain</b> コマンドを使用することもできます。
ステップ 3	(Optional) switch# <b>show vpc brief</b>	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	(Optional) switch# <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

### Example

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仮想ルーティングおよび転送 (VRF) インスタンスから、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。



## Note

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 インスタンスにレイヤ 3 ポートを接続することが推奨されます。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。

## Before you begin

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。

vPC ピアリンクの両端にあるそれぞれのスイッチで設定を行う必要があります。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vpc domain** *domain-id*
3. switch(config-vpc-domain)# **peer-keepalive destination** *ipaddress* [**hold-timeout** *secs* | **interval** *msecs* {**timeout** *secs*} | **precedence** {*prec-value* | **network** | **internet** | **critical** | **flash-override** | **flash** | **immediate priority** | **routine**} | **tos** {*tos-value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal**} | **tos-byte** *tos-byte-value*} | **source** *ipaddress* | **vrf** {*name* | **management vpc-keepalive**}]
4. (Optional) switch(config-vpc-domain)# **vpc peer-keepalive destination** *ipaddress* **source** *ipaddress*
5. (Optional) switch# **show vpc peer-keepalive**
6. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
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>vpc domain domain-id</b>	スイッチ上に vPC ドメインが存在し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	switch(config-vpc-domain)# <b>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}]</b>	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。  <b>Note</b> vPC ピアキープアライブリンクを設定するまで、vPC ピアリンクは構成されません。  管理ポートと VRF がデフォルトです。
ステップ 4	(Optional) switch(config-vpc-domain)# <b>vpc peer-keepalive destination ipaddress source ipaddress</b>	vPC ピアキープアライブリンクに対し、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	(Optional) switch# <b>show vpc peer-keepalive</b>	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	(Optional) switch# <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## Example

次の例は、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方法を示したものです。

```
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)#
```

次の例は、vPC ピアキープアライブリンクに対して、vpc\_keepalive という名前の VRF インスタンスを別途設定する方法、およびその新しい VRF を検査する方法を示したものです。



```
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# show 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 リンクを作成する場合は、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。

### Before you begin

vPC 機能をイネーブルにしていることを確認します。

vPC ピア リンクの両端にあるそれぞれのスイッチで設定を行う必要があります。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface port-channel** *channel-number*
3. switch(config-if)# **vpc peer-link**
4. (Optional) switch# **show vpc brief**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
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 port-channel</b> <i>channel-number</i>	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。
ステップ 4	(Optional) switch# <b>show vpc brief</b>	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	(Optional) switch# <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

### Example

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
```

## 設定の互換性の検査

両側の vPC ピア スイッチに 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に整合性があるかどうかの検査を行います。

次の QoS パラメータでタイプ 2 整合性検査がサポートされています。

- Network QoS : MTU および Pause
- Input Queuing : Bandwidth および Absolute Priority

- Output Queuing : Bandwidth および Absolute Priority

タイプ2の不一致の場合、vPCは停止しません。タイプ1の不一致が検出されるとvPCは停止します。

手順の概要

1. switch# show vpc consistency-parameters {global|interface port-channel channel-number}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# show vpc consistency-parameters {global interface port-channel channel-number}	すべてのvPCインターフェイス全体で一貫している必要があるパラメータのステータスを表示します。

例

次の例は、すべてのvPCインターフェイスの間で必須設定の互換性が保たれているかチェックする方法を示します。

```
switch# 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, 0)                    (1538, 0, 0, 0, 0, 0, 0)
Network Qos (Pause)                 2      (F, F, F, F, F, F)                          (1538, 0, 0, 0, 0, 0, 0)
Input Queuing (Bandwidth)           2      (100, 0, 0, 0, 0, 0, 0)                     (100, 0, 0, 0, 0, 0, 0)
Input Queuing (Absolute Priority)    2      (F, F, F, F, F, F)                          (100, 0, 0, 0, 0, 0, 0)
Output Queuing (Bandwidth)          2      (100, 0, 0, 0, 0, 0, 0)                     (100, 0, 0, 0, 0, 0, 0)
Output Queuing (Absolute Priority)  2      (F, F, F, F, F, F)                          (100, 0, 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
STP Loopguard                       1      Disabled                                    Disabled
STP Bridge Assurance                1      Enabled                                     Enabled
STP Port Type, Edge BPDUGuard       1      Normal, Disabled, Disabled                 Normal, 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

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **vpc domain domain-id**
3. switch(config-vpc-domain)# **auto-recovery reload-delay delay**

## 手順の詳細

	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>vpc domain domain-id</b>	既存の vPC ドメインに対して 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、リロード遅延時間を設定します。デフォルトではディセーブルになっています。

## 例

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

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、バックアップからの vPC の回復を遅らせるようにリストア タイマーを設定できます。この機能により、vPC が再びトラフィックの受け渡しをし始める前にルーティングテーブルが収束できなかった場合のパケットのドロップを回避できます。

### 始める前に

vPC 機能をイネーブルにしていることを確認します。

vPC ピアリンクの両端にあるそれぞれのスイッチで設定を行う必要があります。手順は次のとおりです。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **vpc domain domain-id**
3. switch(config-vpc-domain)# **delay restore time**
4. (任意) switch# **copy running-config startup-config**

### 手順の詳細

	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>vpc domain domain-id</b>	スイッチ上に vPC ドメインが存在し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	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 デバイスが稼働するまで遅延時間（単位は秒）です。値の範囲は 1 ～ 3600 です。デフォルトは 30 秒です。
ステップ 4	(任意) switch# <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

### 例

次の例は、vPC リンクに対する復元遅延時間の設定方法を示したものです。

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

# vPC ピアリンク障害発生時における VLAN インターフェイスのシャットダウン回避

vPC ピアリンクが失われると、vPC セカンダリ スイッチによりその vPC メンバ ポートおよびスイッチ仮想インターフェイス (SVI) が一時停止されます。また、vPC セカンダリ スイッチのすべての VLAN に対して、レイヤ 3 転送はすべてディセーブルになります。ただし、特定の SVI インターフェイスを一時停止の対象から除外することができます。

## 始める前に

VLAN インターフェイスが設定済みであることを確認します。

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **vpc domain domain-id**
3. switch(config-vpc-domain)# **dual-active exclude interface-vlan range**

## 手順の詳細

	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>vpc domain domain-id</b>	スイッチ上に vPC ドメインが存在し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	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でもアップ状態を維持する必要がある VLAN インターフェイスを指定します。  range : シャットダウンしないようにする VLAN インターフェイスの範囲を指定します。値の範囲は 1 ~ 4094 です。

## 例

次の例は、vPC ピアリンクに障害が発生した場合でも vPC ピア スイッチの VLAN 10 に対してインターフェイスのアップ状態を維持する方法を示したものです。

```
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 対応です。適切なルーティングテーブルを使用するためには、VRF 名を設定する必要があります。

VRF 名を指定することができます。

### 手順の概要

1. switch# ping ipaddress vrf vrf-name

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# ping ipaddress vrf vrf-name	Virtual Routing and Forwarding (VRF) 名を指定します。VRF 名は、長さが最大 32 文字で、大文字と小文字は区別されます。

### 例

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
```

## 他のポートチャネルの vPC への移行

### Before you begin

vPC 機能をイネーブルにしていることを確認します。

vPC ピアリンクの両端にあるそれぞれのスイッチで設定を行う必要があります。手順は次のとおりです。

### SUMMARY STEPS

1. switch# configure terminal
2. switch(config)# interface port-channel channel-number

3. switch(config-if)# vpc number
4. (Optional) switch# show vpc brief
5. (Optional) switch# copy running-config startup-config

## DETAILED STEPS

	Command or Action	Purpose
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 port-channel</b> channel-number	vPCに配置してダウンストリームスイッチに接続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。  <b>Note</b> vPC は、通常のポートチャネル上（物理 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上（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)# vpc number	選択したポートチャネルをvPCに配置し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。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スイッチで同じでなければなりません。
ステップ 4	(Optional) switch# <b>show vpc brief</b>	各vPCに関する情報を表示します。
ステップ 5	(Optional) switch# <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## Example

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



**Note** システムアドレスの設定を行うかどうかは任意です。

## Before you begin

vPC 機能をイネーブルにしていることを確認します。

vPC ピア リンクの両端にあるそれぞれのスイッチで設定を行う必要があります。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vpc domain domain-id**
3. switch(config-vpc-domain)# **system-mac mac-address**
4. (Optional) switch# **show vpc role**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
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>vpc domain domain-id</b>	スイッチ上にある既存の vPC ドメインを選択するか、または新規の vPC ドメインを作成して、vpc-domain コンフィギュレーションモードを開始します。 <i>domain-id</i> のデフォルト値はありません。指定できる値の範囲は 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 <i>aaaa.bbbb.cccc</i> の形式で入力します。
ステップ 4	(Optional) switch# <b>show vpc role</b>	vPC システムの MAC アドレスを表示します。
ステップ 5	(Optional) switch# <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## Example

次の例は、vPC ドメインの MAC アドレスを設定する方法を示したものです。

```
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。

### Before you begin

vPC機能をイネーブルにしていることを確認します。

vPCピアリンクの両端にあるそれぞれのスイッチで設定を行う必要があります。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vpc domain domain-id**
3. switch(config-vpc-domain)# **system-priority priority**
4. (Optional) switch# **show vpc brief**
5. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
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>vpc domain domain-id</b>	スイッチ上にある既存の vPC ドメインを選択するか、または新規の vPC ドメインを作成して、vpc-domain コンフィギュレーションモードを開始します。domain-id のデフォルト値はありません。指定できる値の範囲は 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	(Optional) switch# <b>show vpc brief</b>	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	(Optional) switch# <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

**Example**

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 スイッチのロールの手動による設定

デフォルトの場合、Cisco NX-OS 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、プライマリおよびセカンダリの 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。選択したら、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ブ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 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 が再び稼働しても、機能のロールは元に戻りません。

**Before you begin**

vPC 機能をイネーブルにしていることを確認します。

vPC ピア リンクの両端にあるそれぞれのスイッチで設定を行う必要があります。

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config)# **vpc domain** *domain-id*
3. switch(config-vpc-domain)# **role priority** *priority*
4. (Optional) switch# **show vpc brief**
5. (Optional) switch# **copy running-config startup-config**

**DETAILED STEPS**

	Command or Action	Purpose
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>vpc domain</b> <i>domain-id</i>	スイッチ上にある既存の vPC ドメインを選択するか、または新規の vPC ドメインを作成して、vpc-domain コンフィギュレーション モードを開始し

	Command or Action	Purpose
		ます。 <i>domain-id</i> のデフォルト値はありません。指定できる値の範囲は 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として使用するロールプライオリティを指定します。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	(Optional) switch# <b>show vpc brief</b>	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	(Optional) switch# <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

### Example

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
```

## Layer 3 over vPC の設定

### 始める前に

ピア ゲートウェイ機能が両方のピアで有効かつ設定済みで、両方のピアが vPC 経由のレイヤ 3 に対応したイメージを実行していることを確認します。ピアゲートウェイ機能を有効にせずに **layer3 peer-router** コマンドを入力した場合は、ピアゲートウェイ機能を有効にするように勧める syslog メッセージが表示されます。

ピアリンクがアップしていることを確認します

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **vpc domain domain-id**
3. switch(config-vpc-domain)#**layer3 peer-router**
4. switch(config-vpc-domain)# **exit**
5. (任意) switch# **show vpc brief**
6. (任意) switch# **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b> 例： switch# <b>configure terminal</b> 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	switch(config)# <b>vpc domain domain-id</b> 例： switch(config)# <b>vpc domain 5</b> 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。デフォルトはありません。指定できる範囲は <1 ~ 1000> です。
ステップ 3	switch(config-vpc-domain)# <b>layer3 peer-router</b>	両方のピアとのピアリング隣接関係を形成するためにレイヤ 3 デバイスを有効にします。  (注) 両方のピアでこのコマンドを設定します。このコマンドをピアのうち1つでのみ設定するか、1つのピアで無効にすると、レイヤ 3 ピアルータの動作状態が無効になります。動作状態に変更があると、通知が表示されます。
ステップ 4	switch(config-vpc-domain)# <b>exit</b>	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	(任意) switch# <b>show vpc brief</b>	各 vPC ドメインに関する要約情報を表示します。
ステップ 6	(任意) switch# <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## 例

次に、vPC 機能経由でレイヤ 3 を設定する例を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# layer3 peer-router

switch(config-vpc-domain)# exit

switch(config)#
```

次に、vPC 経由でレイヤ 3 機能が設定されているかどうかを確認する例を示します。**動作レイヤ 3 ピア**は、vPC 経由のレイヤ 3 の動作状態の設定に応じて有効または無効になります。

```
switch# show vpc brief

vPC domain id : 5
```

```
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
Configuration consistency status : success
Per-vlan consistency status : failed
Type-2 consistency status : success
vPC role : secondary
Number of vPCs configured : 2
Peer Gateway : Enabled
Peer gateway excluded VLANs : -
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Enabled (timeout = 240 seconds)
Operational Layer3 Peer : Enabled
```



## 索引

### D

delay restore 93

### I

interface port-channel 61–62, 65–67

interfaces-vlan 93

### L

LACP 44, 49–50, 52, 58, 60

システム ID 50

設定 58

ポートチャネル 49

ポートチャネル、MinLink 52, 60

マーカレスポンド 52

lacp graceful-convergence 67

lacp max-bundle 61–62

LACP がイネーブルとスタティック 52

ポートチャネル 52

LACP 高速タイマーレート 62

設定 62

LACP の設定 58

LACP ポートプライオリティ 64

設定 64

Link Aggregation Control Protocol 44

### S

SFP+ トランシーバ 6

show running-config interface port-channel 61–62

shutdown 65–67

Small Form-Factor Pluggable (プラス) トランシーバ 6

STP 43

ポートチャネル 43

SVI 自動ステート 7

レイヤ 2 7

SVI 自動ステートのディセーブル化 23

SVI 自動ステートの無効化の設定 35

### U

UDLD 4–5

アグレッシブモード 5

定義 4

非アグレッシブモード 5

### V

VLAN 19

インターフェイス 19

VLAN インターフェイス 27

設定 27

vPC 115

ポートチャネルの移行 115

vPC の用語 83

VRF 30

インターフェイスの割り当て 30

### い

イーサネット インターフェイス 6

インターフェイスの速度 6

インターフェイス 4, 17, 19, 21–22, 26–28, 30, 39–40

UDLD 4

VLAN 19, 27

設定 27

VRF への割り当て 30

オプション 4

シャーシ ID 4

帯域幅の設定 26

tunnel 22

ルーテッド 17

loopback 21, 28

レイヤ 3 17, 39–40

設定例 40

モニタリング 39

インターフェイス MAC アドレス、設定 31

インターフェイス情報、表示 13

レイヤ 2 13

インターフェイスでの DHCP クライアントの設定 36

インターフェイスの速度 **6**  
 イーサネット インターフェイス **6**

## か

確認 **37**  
 レイヤ 3 インターフェイス設定 **37**  
 関連資料 **41**  
 レイヤ 3 インターフェイス **41**

## さ

サブインターフェイス **18, 25–26**  
 設定 **25**  
 帯域幅の設定 **26**

## せ

設定 **23, 25–28, 37, 62, 64**  
 LACP 高速タイマー レート **62**  
 LACP ポートプライオリティ **64**  
 VLAN インターフェイス **27**  
 インターフェイス帯域幅 **26**  
 サブインターフェイス **25**  
 ルーテッドインターフェイス **23**  
 ループバック インターフェイス **28**  
 レイヤ 3 インターフェイス **37**  
 確認 **37**  
 設定例 **40**  
 レイヤ 3 インターフェイス **40**

## た

bandwidth **26**  
 設定 **26**  
 対称ハッシュ化 **48**  
 ダウンリンク遅延 **12**  
 単方向リンク検出 **4**

## ち

チャンネルモード **50, 58**  
 ポート チャンネル **50, 58**

## て

ディセーブル化 **105**  
 vPC **105**  
 デバウンスタイマー **10**  
 パラメータ **10**

デフォルト インターフェイス **10**  
 デフォルト設定 **23**  
 レイヤ 3 インターフェイス **23**

## と

トンネル インターフェイス **22**

## は

パラメータ、概要 **10**  
 デバウンスタイマー **10**

## ふ

物理イーサネットの設定 **12**

## ほ

ポート チャネリング **44**  
 ポート チャンネル **26, 43, 45, 47, 49, 52, 54–56, 58, 68, 115**  
 LACP **49**  
 LACP がイネーブルとスタティック **52**  
 STP **43**  
 vPC への移行 **115**  
 互換性要件 **45**  
 作成 **54**  
 設定の確認 **68**  
 帯域幅の設定 **26**  
 チャンネル モード **58**  
 ポートの追加 **55**  
 ロード バランシング **47, 56**  
 ポート チャンネル **47**  
 ポート チャンネル、MinLink **52, 60**  
 LACP **52, 60**  
 ポートの追加 **55**  
 ポート チャンネル **55**

## も

モニタリング **39**  
 レイヤ 3 インターフェイス **39**

## る

ルーテッドインターフェイス **17, 23, 26**  
 設定 **23**  
 帯域幅の設定 **26**  
 ループバック インターフェイス **21, 28**  
 設定 **28**



## れ

レイヤ 2 [7, 13](#)

SVI 自動ステート [7](#)

インターフェイス情報、表示 [13](#)

レイヤ 3 インターフェイス [17, 23, 37, 39–41](#)

インターフェイス [41](#)

レイヤ 3 [41](#)

関連資料 [41](#)

確認 [37](#)

関連資料 [41](#)

レイヤ 3 インターフェイス (続き)

設定例 [40](#)

デフォルト設定 [23](#)

モニタリング [39](#)

ルーテッドインターフェイスの設定 [23](#)

## ろ

ロード バランシング [56](#)

ポート チャネル [56](#)

設定 [56](#)

