



Cisco Nexus 3600 Switch NX-OS Interfaces Configuration Guide, Release 10.6(x)

First Published: 2025-08-13

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: <https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html>. Cisco product warranty information is available at <https://www.cisco.com/c/en/us/products/warranty-listing.html>. US Federal Communications Commission Notices are found here <https://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and-if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

はじめに xi

対象読者 xi

表記法 xi

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

マニュアルに関するフィードバック xiii

通信、サービス、およびその他の情報 xiii

CHAPTER 1

New and Changed Information 1

New and Changed Information 1

CHAPTER 2

概要 3

ライセンス要件 3

サポートされるプラットフォーム 3

CHAPTER 3

基本インターフェイス パラメータの設定 5

基本インターフェイス パラメータについて 5

説明 5

ビーコン 5

エラー ディセーブル化 6

MDIX 6

インターフェイス ステータス エラー ポリシー 6

インターフェイス MTU サイズの変更 7

帯域幅 7

スループット遅延 8

管理ステータス	8
UDLD パラメータ	8
UDLD の概要	8
UDLD のデフォルト設定	9
UDLD の通常モードとアグレッシブモード	10
ポートチャネルパラメータ	11
ポートプロファイル	11
注意事項と制約事項	13
デフォルト設定	15
基本インターフェイスパラメータの設定	15
設定するインターフェイスの指定	16
説明の設定	17
ビーコンモードの設定	19
Error-Disabledステートの設定	21
error-disableステート回復のイネーブル化	21
Error-Disable検出のイネーブル化	22
error-disableステート回復間隔の設定	23
MDIXパラメータの設定	24
MTU サイズの設定	26
MTU サイズの設定	26
システムジャンボ MTU サイズの設定	26
帯域幅の設定	28
スループット遅延の設定	29
インターフェイスのシャットダウンおよび再開	31
UDLD モードの設定	33
デバウンス タイマーの設定	36
ポートプロファイルの設定	38
ポートプロファイルの作成	38
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	39
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	40

特定のポートプロファイルのイネーブル化	41
ポートプロファイルの継承	43
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	44
継承されたポートプロファイルの削除	45
DWDMの設定	46
25G自動ネゴシエーションの設定	47
25G自動ネゴシエーションの注意事項と制限事項	47
インターフェイスでのFECの手動有効化	47
自動ネゴシエーションの有効化	48
自動ネゴシエーションのディセーブル化	49
基本インターフェイスパラメータの確認	50
インターフェイスカウンタのモニタリング	51
インターフェイス統計情報の表示	51
インターフェイスカウンタのクリア	52

CHAPTER 4

レイヤ2インターフェイスの設定	55
イーサネットインターフェイスの概要	55
インターフェイスコマンド	55
UDLDパラメータ	56
UDLDのデフォルト設定	57
UDLDアグレッシブモードと非アグレッシブモード	57
レイヤ2インターフェイスのガイドラインおよび制約事項	58
インターフェイス速度	58
40ギガビットイーサネットインターフェイスの速度	58
SVI自動ステート	59
Cisco Discovery Protocol	60
CDPのデフォルト設定	60
errordisableステート	60
デフォルトインターフェイス	62
デバウンスタイマーパラメータについて	62
MTU設定	62

カウンタ値	62
ダウンリンク遅延	64
物理イーサネットのデフォルト設定	64
インターフェイス情報の表示	65

CHAPTER 5

レイヤ3インターフェイスの設定	69
レイヤ3インターフェイスについて	69
ルーテッドインターフェイス	69
サブインターフェイス	70
VLANインターフェイス	71
インターフェイスのVRFメンバーシップの変更	72
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	72
ループバックインターフェイス	73
IPアンナンバード	73
トンネルインターフェイス	74
レイヤ3インターフェイスの注意事項および制約事項	74
レイヤ3インターフェイスのデフォルト設定	75
SVI自動ステートのディセーブル化	75
レイヤ3インターフェイスの設定	75
ルーテッドインターフェイスの設定	75
サブインターフェイスの設定	77
インターフェイスでの帯域幅の設定	78
VLANインターフェイスの設定	79
VRFメンバーシップ変更時のレイヤ3保持の有効化	80
ループバックインターフェイスの設定	81
イーサネットインターフェイスでのIPアンナンバードの設定	82
VRFへのインターフェイスの割り当て	83
インターフェイスMACアドレスの設定	84
MAC埋め込みIPv6アドレスの設定	85
SVI自動ステートの無効化の設定	88
インターフェイスでのDHCPクライアントの設定	89

レイヤ3インターフェイス設定の確認	90
レイヤ3インターフェイスのモニタリング	91
レイヤ3インターフェイスの設定例	93
レイヤ3インターフェイスの関連資料	94

CHAPTER 6**ポートチャネルの構成** 95

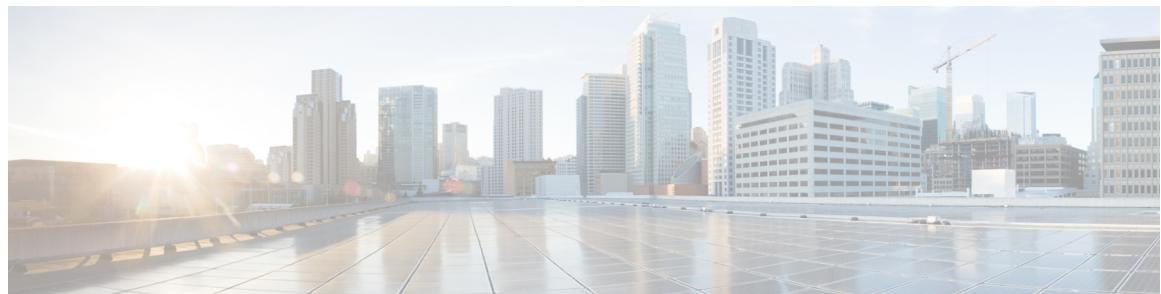
ポートチャネルについて	95
ポートチャネルの概要	96
互換性要件	97
ポートチャネルを使ったロードバランシング	99
シンメトリックハッギング	100
LACPについて	101
LACPの概要	101
LACP IDパラメータ	101
チャネルモード	102
LACPマーカーレスポンダ	104
LACPがイネーブルのポートチャネルとスタティックポートチャネルの相違点	104
LACPポートチャネルの最小リンクおよびMaxBundle	104
注意事項と制約事項	105
ポートチャネルの設定	106
ポートチャネルの作成	106
ポートチャネルへのポートの追加	107
ポートチャネルを使ったロードバランシングの設定	108
LACPのイネーブル化	109
ポートに対するチャネルモードの設定	110
LACPポートチャネルのMinLinkの設定	112
LACPポートチャネルMaxBundleの設定	113
LACP高速タイマー率の設定	114
LACPのシステムプライオリティおよびシステムIDの設定	115
LACPポートプライオリティの設定	116
LACPグレースフルコンバージェンスのディセーブル化	117

LACP グレースフル コンバージェンスの再イネーブル化	119
ポートチャネル構成の確認	120
ポートチャネルメンバーシップ整合性チェックのトリガー	121
ロードバランシング発信ポートIDの確認	122
ポートプロファイル	122
ポートプロファイルの設定	124
ポートプロファイルの作成	125
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	126
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	127
特定のポートプロファイルのイネーブル化	128
ポートプロファイルの継承	129
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	130
継承されたポートプロファイルの削除	131

CHAPTER 7**仮想ポートチャネルの設定** 133

vPCについて	134
vPCの概要	134
用語	135
vPCの用語	135
vPCドメイン	136
ピアキープアライブリンクとメッセージ	137
vPCピアリンクの互換パラメータ	137
同じでなければならない設定パラメータ	138
同じにすべき設定パラメータ	139
VLANごとの整合性検査	140
vPC自動リカバリ	140
vPCピアリンク	140
vPCピアリンクの概要	141
vPC番号	142
その他の機能とのvPCの相互作用	142

vPC と LACP	142
vPC ピア リンクと STP	143
CFSoE	144
vPC フォークリフト アップグレードシナリオ	144
VRF に関する注意事項と制約事項	147
vPC 設定の確認	149
グレースフル タイプ 1 検査ステータスの表示	149
グローバル タイプ 1 不整合の表示	150
インターフェイス別タイプ 1 不整合の表示	151
VLAN ごとの整合性ステータスの表示	152
vPC のデフォルト設定	155
vPC の設定	155
vPC のイネーブル化	155
vPC のディセーブル化	156
vPC ドメインの作成	157
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	158
vPC ピア リンクの作成	160
設定の互換性の検査	162
vPC 自動リカバリのイネーブル化	163
復元遅延時間の設定	164
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	165
VRF 名の設定	166
他のポート チャネルの vPC への移行	167
vPC ドメイン MAC アドレスの手動での設定	168
システム プライオリティの手動での設定	169
vPC ピア スイッチのロールの手動による設定	170
レイヤ 3 vPC 経由の設定	172



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 (xi ページ)
- 表記法 (xi ページ)
- Cisco Nexus 3600 プラットフォーム スイッチの関連資料 (xii ページ)
- マニュアルに関するフィードバック (xiii ページ)
- 通信、サービス、およびその他の情報 (xiii 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
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
<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。 <code>string</code> 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 <code>string</code> 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 <code>screen</code> 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 <code>screen</code> フォント	ユーザが値を指定する引数は、イタリック体の <code>screen</code> 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](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ひいたします。

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。
- ・重要な技術によって求めるビジネス成果を得るには、[Cisco Services \[英語\]](#) 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、[Cisco Support](#) 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 DevNet](#) にアクセスしてください。
- ・一般的なネットワーキング、トレーニング、認定関連の出版物入手するには、[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 Bug Search Tool](#) (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。



CHAPTER 1

New and Changed Information

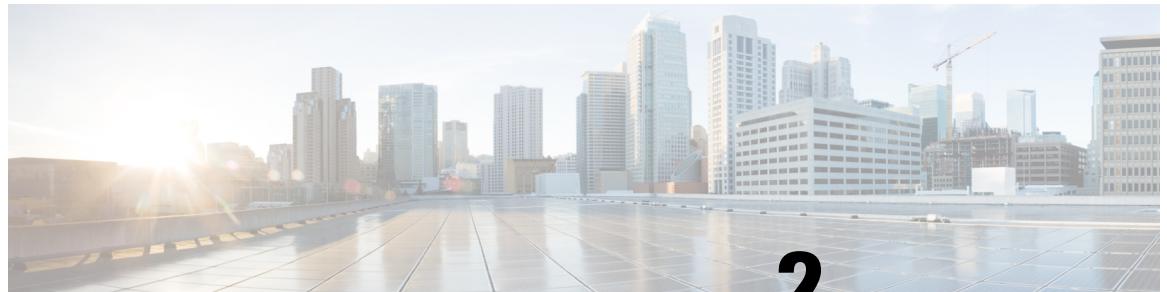
- [New and Changed Information, on page 1](#)

New and Changed Information

Table 1: New and Changed Features

Feature	Description	Changed in Release	Where Documented
NA	No feature updates for this release.	10.6(1)F	NA

New and Changed Information



第 2 章

概要

- ライセンス要件（3 ページ）
- サポートされるプラットフォーム（3 ページ）

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 ライセンス ガイド』および『Cisco NX-OS ライセンス オプション ガイド』を参照してください。

サポートされるプラットフォーム

Cisco NX-OS リリース 7.0(3)I7(1) 以降では、Nexus スイッチ プラットフォーム サポート マトリクスに基づいて、選択した機能をさまざまな Cisco Nexus 9000 および 3000 スイッチで使用するためには、どの Cisco NX-OS リリースが必要かを確認してください。

■ サポートされるプラットフォーム



第 3 章

基本インターフェイス パラメータの設定

この章では、Cisco NX-OS デバイス上で基本インターフェイス パラメータを構成する方法について説明します。

- [基本インターフェイス パラメータについて \(5 ページ\)](#)
- [注意事項と制約事項 \(13 ページ\)](#)
- [デフォルト設定 \(15 ページ\)](#)
- [基本インターフェイス パラメータの設定 \(15 ページ\)](#)
- [基本インターフェイス パラメータの確認 \(50 ページ\)](#)
- [インターフェイス カウンタのモニタリング \(51 ページ\)](#)

基本インターフェイス パラメータについて

Cisco Nexus 3548 スイッチでは、次のパラメータがサポートされています：

説明

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

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

ビーコン

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

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

■ エラー ディセーブル化

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

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

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

この項で説明している **errdisable recovery cause** コマンドを使用すると、300 秒後に自動的にリカバリします。

errdisable recovery interval コマンドを使用すれば コマンドを使用します。特定の err-disable 原因のリカバリ タイムアウトも設定できます。

原因に対する error-disabled 回復を有効にしない場合、そのインターフェイスは **shutdown** および **no shutdown** コマンドを開始するまでエラー無効状態です原因に対して回復をイネーブルにすると、そのインターフェイスの errdisabled ステートは解消され、すべての原因がタイムアウトになつた段階で動作を再試行できるようになります。**show interface status err-disabled** コマンドを使用し、コマンドを使用します。

MDIX

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

MDIX パラメータの設定については、「[MDIX パラメータの設定](#)」のセクションを参照してください。

インターフェイス ステータス エラー ポリシー

アクセス コントロール リスト (ACL) マネージャおよび Quality of Service (QoS) マネージャなどの Cisco NX-OS ポリシーサーバは、ポリシーデータベースを維持します。ポリシーは、コマンドラインインターフェイスを使用して定義します。

インターフェイス上でポリシーを設定するときにポリシーをプッシュして、プッシュされるポリシーがハードウェアのポリシーと一致するようにします。エラーをクリアし、ポリシープログラミングが実行コンフィギュレーションを続行できるようにするには、**no shutdown** コマンドを入力します。ポリシープログラミングが成功すると、ポートのアップが許可されます。ポリシープログラミングが失敗した場合、設定はハードウェアポリシーに矛盾し、ポートは error-disabled ポ

リシー状態になります。error-disabled ポリシー状態にとどまり、同じポートが今後アップされないように情報が保存されます。このプロセスにより、システムに不要な中断が生じるのを避けることができます。

インターフェイス MTU サイズの変更

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

Cisco NX-OS では、プロトコルスタックの異なるレベルで設定するオプションを使用して、インターフェイスに MTU を設定できます。デフォルトではそれぞれのインターフェイスの MTU は 1500 バイトです。これはイーサネットフレームに関する IEEE 802.3 標準です。MTU サイズを大きくすると、データの処理効率が向上し、さまざまなアプリケーション要件に対応できます。このようなフレームをジャンボフレームと呼び、最大 9216 バイトまで指定できます。

MTU はインターフェイスごとに設定されます。インターフェイスは、レイヤ2またはレイヤ3インターフェイスにすることができます。レイヤ2インターフェイスの場合、MTU サイズは、システムのデフォルト MTU 値またはシステム ジャンボ MTU 値の 2 つの値のいずれかで設定できます。システム デフォルトの MTU サイズは 1500 バイトです。すべてのレイヤ2インターフェイスは、デフォルトでこの値で設定されます。デフォルトのシステム ジャンボ MTU 値 (9216 バイト) を使用してインターフェイスを設定できます。1500 ~ 9216 の MTU 値を許可するには、インターフェイスが同じ値で設定できる適切な値にシステム ジャンボ MTU を調整する必要があります。



(注) システム ジャンボ MTU サイズを変更できます。値が変更されると、システム ジャンボ MTU 値を使用するレイヤ2インターフェイスは新しいシステム ジャンボ MTU 値に自動的に変更します。

レイヤ3インターフェイスは、レイヤ3物理インターフェイス（スイッチポートなしで設定）、スイッチ仮想インターフェイス (SVI)、およびサブインターフェイスで、576~9216 バイトの MTU サイズを設定できます。

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

帯域幅

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

■ スループット遅延

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

スループット遅延

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

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

管理ステータス

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

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

UDLD パラメータ

UDLD の概要

シスコ独自の单方向リンク検出 (UDLD) プロトコルにより、光ファイバまたは銅線 (カテゴリ 5 ケーブルなど) イーサネットケーブルを使用して接続されたデバイスで、ケーブルの物理構成をモニタし、單一方向リンクの存在を検出することができます。デバイスで單一方向リンクが検出されると、UDLDが関係のある LAN ポートをシャットダウンし、ユーザに通知します。單一方向リンクは、さまざまな問題を引き起こす可能性があります。

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 の検出が動作して、物理的な單一方向接続と論理的な單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、单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

シェーディングがアクティブである限り、そのリンクはアップ状態が維持されなくなります。この場合、論理リンクは不定であり、UDLD は何の処理も行いません。レイヤ 1 で両方のファイバが正常に動作していれば、UDLD はこれらのファイバが正しく接続しているかどうか、また、トラフィックが適切なネイバー間で双方向に流れているかどうかを判別します。自動ネゴシエーションはレイヤ 1 で動作するため、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。

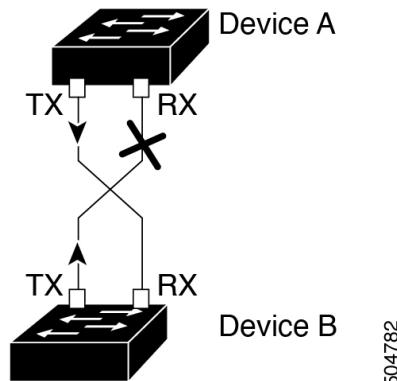
Cisco Nexus のデバイスは、UDLD をイネーブルにした LAN ポート上のネイバーデバイスに定期的に UDLD フレームを送信します。一定の時間内にフレームがエコーバックされてきて、特定の確認応答 (echo) が見つからなければ、そのリンクは單一方向のフラグが立てられ、その LAN ポートはシャットダウンされます。UDLD プロトコルにより单方向リンクが正しく識別されその使用が禁止されるようにするために、リンクの両端のデバイスで UDLD がサポートされている必要があります。UDLD フレームの送信間隔は、グローバル単位でも指定されたインターフェイスにも設定できます。



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

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

図 1: 单方向リンク



UDLD のデフォルト設定

次の表に、UDLD のデフォルト設定を示します。

表 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 の通常モードとアグレッシブ モード

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

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

UDLD の通常モードとアグレッシブ モード

UDLD は操作の通常およびアグレッシブ モードをサポートします。デフォルトでは、通常モードが有効です。

通常モードでは、UDLD はピア ポートからの着信 UDLD パケットを調べて、次のリンク エラーを検出します。

- 空のエコーパケット
- 単一方向
- TX/RX ループ
- ネイバーの不一致

デフォルトでは、UDLD アグレッシブ モードが無効になっています。UDLD アグレッシブ モードは、UDLD アグレッシブ モードをサポートするネットワーク デバイスの間のポイントツーポイントのリンク上に限って設定できます。

UDLD アグレッシブ モードを有効に設定した場合、UDLD 近接関係が設定されている双方向リンク上のポートが UDLD フレームを受信しなくなったとき、UDLD はネイバーとの接続を再確立しようとします。この再試行に 8 回失敗すると、ポートはディセーブルになります。

次のシナリオでは、UDLD アグレッシブ モードを有効にすると、トラフィックの廃棄を防ぐためにポートの 1 つが無効になります。

- リンクの一方でポート スタックが生じる（送受信どちらも）
- リンクの一方がダウンしているにもかかわらず、リンクのもう一方がアップしたままになる



(注)

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



ヒント

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

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

ポート チャネル パラメータ

ポート チャネルは物理インターフェイスの集合体で、論理インターフェイスを構成します。1つのポート チャネルに最大 32 の個別インターフェイスをバンドルして、帯域幅と冗長性を向上させることができます。これらの集約された各物理インターフェイス間でトラフィックのロードバランシングも行います。ポート チャネルの物理インターフェイスが少なくとも 1 つ動作していれば、そのポート チャネルは動作しています。

レイヤ 3 ポート チャネルに適合するレイヤ 3 インターフェイスをバンドルすれば、レイヤ 3 ポート チャネルを作成できます。

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

ポート チャネルおよびポート チャネルの設定については、第 6 章「ポート チャネルの設定」を参照してください。

ポート プロファイル

Cisco Nexus 3600 シリーズ スイッチの場合、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て、インターフェイスの範囲にそのポート プロファイルを適用できます。ポート プロファイルはそれぞれ特定のタイプのインターフェイスにだけ適用できます。次のインターフェイスから選択できます。

- イーサネット
- VLAN ネットワーク インターフェイス
- 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

■ ポートプロファイル

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つのレベルの継承に対応しています。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。



(注) Session Manager にポートプロファイルは使用できません。Session Manager の詳細については、『Cisco Nexus 3600 Series NX-OS System Management Configuration Guide』を参照してください。

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

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

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

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

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

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

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

ポートプロファイルをイネーブル化、継承、または変更しようとすると、システムによりチェックポイントが作成されます。ポートプロファイル設定が正常に実行されなかった場合は、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。

注意事項と制約事項

基本インターフェイスパラメータの設定には次の注意事項と制約事項があります。

- 銅線ポートでは、MDIXはデフォルトでイネーブルになっています。無効にすることはできません。
- **show** コマンド (**internal** キーワード付き) はサポートされていません。
- 光ファイバーサネットポートでは、シスコがサポートするトランシーバを使用する必要があります。シスコがサポートするトランシーバをポートに使用していることを確認するには、**show interface transceivers** コマンドを使用します。シスコがサポートするトランシーバを持つインターフェイスは、機能インターフェイスとして一覧表示されます。
- ポートはレイヤ2またはレイヤ3インターフェイスのいずれかです。両方が同時に成立することはありません。

■ 注意事項と制約事項

デフォルトでは、どのポートもレイヤ3インターフェイスです。

レイヤ3インターフェイスをレイヤ2インターフェイスに変更するには、**switchport** コマンドを使用します。 **no switchport** コマンドを使用すれば、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ことができます。

- 通常、イーサネット ポート速度およびデュプレックス モードパラメータは自動的に設定し、システムがポート間で速度およびデュプレックス モードをネゴシエートできるようにします。これらのポートのポート速度およびデュプレックス モードを手動で設定する場合は、次の点について考慮してください。
 - イーサネットまたは管理インターフェイスに速度およびデュプレックス モードを設定する前に、「デフォルト設定」の項を参照して同時に設定できる速度およびデュプレックス モードの組み合わせを確認します。
 - イーサネットポート速度を自動に設定すると、デバイスは自動的にデュプレックスモードを自動に設定します。
 - **no speed** コマンドを入力すると、デバイスは自動的に速度およびデュプレックスパラメータの両方を自動に設定します（**no speed** コマンドと **speed auto** コマンドは同じ結果になります）。
 - イーサネットポート速度を自動以外の値（1G、10G、または40Gなど）に設定する場合は、それに合わせて接続先ポートを設定してください。接続先ポートが速度をネゴシエーションするように設定しないでください。
 - イーサネットインターフェイスの速度、デュプレックス、および自動フロー制御を構成するには、**negotiate auto** コマンドを使用します。自動ネゴシエーションを無効化するには、**no negotiate auto** コマンドを使用します。



(注)

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



注意

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

- Base-T 銅線ポートの場合は、固定速度が設定されていても、自動ネゴシエーションがイネーブルになります。
- ケーブル長が5mを超える場合、自動ネゴシエーションはサポートされていません。このケーブル長の制限は、銅ケーブルにのみ適用されます。光ケーブルには適用されません。

デフォルト設定

次の表に、基本インターフェイス パラメータのデフォルト設定を示します。

パラメータ	デフォルト
説明	ブランク
ビーコン	ディセーブル
帯域幅	インターフェイスのデータ レート
スループット遅延	100 マイクロ秒
管理ステータス	シャットダウン
MTU	1500 バイト
UDLD グローバル	グローバルにディセーブル
ポート別の UDLD イネーブルステート（光ファイバ メディア用）	すべてのイーサネット光ファイバ LAN ポートでイネーブル
銅線メディア用のポート別 UDLD イネーブルステート	すべてのイーサネット 1G、10G、または 40G LAN ポートでディセーブル
UDLD メッセージの間隔	ディセーブル
UDLD アグレッシブ モード	ディセーブル
エラー ディセーブル	ディセーブル
エラー ディセーブル回復	ディセーブル
エラー ディセーブル回復間隔	300 秒

基本インターフェイス パラメータの設定

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

■ 設定するインターフェイスの指定

始める前に

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

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

表 3: 設定するインターフェイスの識別に必要な情報

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

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

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

次に、連続しているインターフェイス範囲の設定例を示します。

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

次に、不連続なインターフェイス範囲の設定例を示します。

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

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

次の例は、ブレークアウトケーブルを設定する方法を示しています。

```
switch(config)# interface ethernet 1/2/1
switch(config-if-range) #
```

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: <pre>switch# configure terminal switch(config)#</pre>	グローバルコンフィギュレーションモードを開始します
Step 2	interface interface 例: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre> 例: <pre>switch(config)# interface mgmt0 switch(config-if)#</pre>	設定するインターフェイスを指定します。インターフェイスタイプと ID を指定できます。イーサネットポートの場合は、 ethernet slot/port を使用します。管理インターフェイスの場合は、 mgmt0 を使用します。 例: <ul style="list-style-type: none"> • 1番目の例は、スロット 2、ポート 1 イーサネットインターフェイスを指定する方法を示します。 • 2番目の例は、管理インターフェイスを指定する方法を示しています。 (注) インターフェイスタイプと ID (ポートまたはスロット/ポート番号) の間にスペースを追加する必要はありません。たとえば、イーサネットスロット 4、ポート 5インターフェイスの場合は、「ethernet4/5」または「ethernet4/5」と指定できます。管理インターフェイスは「mgmt0」または「mgmt0」となります。 インターフェイスコンフィギュレーションモードの場合、コマンドを入力するとこのモードに指定したインターフェイスが設定されます。

説明の設定

イーサネットおよび管理インターフェイスの説明を文字で設定します。

手順の概要

1. **configure terminal**
2. **interface interface**
3. **description text**
4. **show interface interface**
5. **exit**

説明の設定

6. copy running-config startup-config

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: <pre>switch# configure terminal switch(config)#</pre>	グローバルコンフィギュレーションモードを開始します
Step 2	interface interface 例: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre> 例: <pre>switch(config)# interface mgmt0 switch(config-if)#</pre>	設定するインターフェイスを指定します。インターフェイスタイプと ID を指定できます。イーサネットポートの場合は、 ethernet slot/port を使用します。管理インターフェイスには、 mgmt0 を使用します。 例: <ul style="list-style-type: none">• 1番目の例は、スロット 2、ポート 1イーサネットインターフェイスを指定する方法を示します。• 2番目の例は、管理インターフェイスを指定する方法を示しています。
Step 3	description text 例: <pre>switch(config-if)# description Ethernet port 3 on module 1 switch(config-if)#</pre>	インターフェイスの説明を指定します。
Step 4	show interface interface 例: <pre>switch(config)# show interface ethernet 2/1</pre>	(任意) インターフェイスステータスを表示します。説明パラメータもあわせて表示します。
Step 5	exit 例: <pre>switch(config-if)# exit switch(config)#</pre>	インターフェイス モードを終了します。
Step 6	copy running-config startup-config 例: <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

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

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

show interface eth の出力 コマンドの出力は、次の例に示すように拡張されます。

```
Switch# show version
Software
BIOS: version 06.26
NXOS: version 6.1(2)I2(1) [build 6.1(2)I2.1]
BIOS compile time: 01/15/2014
NXOS image file is: bootflash:///n9000-dk9.6.1.2.I2.1.bin
NXOS compile time: 2/25/2014 2:00:00 [02/25/2014 10:39:03]

switch# show interface ethernet 6/36
Ethernet6/36 is up
admin state is up, Dedicated Interface
Hardware: 40000 Ethernet, address: 0022.bdf6.bf91 (bia 0022.bdf8.2bf3)
Internet Address is 192.168.100.1/24
MTU 9216 bytes, BW 40000000 Kbit, DLY 10 usec
```

ビーコン モードの設定

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: 	グローバル設定モードを開始します。

■ ビーコン モードの設定

	コマンドまたはアクション	目的
	switch# configure terminal switch(config)#	
Step 2	interface ethernet slot/port 例: switch(config)# interface ethernet 3/1 switch(config-if)#	設定するインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。
Step 3	[no] beacon 例: switch(config)# beacon switch(config-if)#	ビーコン モードをイネーブルにします。またはビーコン モードをディセーブルにします。デフォルト モードはディセーブルです。
Step 4	show interface ethernet slot/port 例: switch(config)# show interface ethernet 2/1 switch(config-if)#	(任意) ビーコン モードステートなど、インターフェイスのステータスを表示します。
Step 5	exit 例: switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
Step 6	copy running-config startup-config 例: switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

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

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

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

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

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

```
switch# configure terminal
switch(config)# interface ethernet 4/17, ethernet 4/19, ethernet 4/21, ethernet 4/23
switch(config-if)# shutdown
switch(config-if)# interface ethernet 4/17
```

```
switch(config-if)# no shutdown
switch(config-if)#

```

Error-Disabled ステートの設定

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

error-disable ステート回復のイネーブル化

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

手順の概要

1. **configure terminal**
2. **errdisable recovery cause {all | bpduguard | failed-port-state | link-flap | loopback | miscabling | psecure-violation | security-violation | storm-control | udld | vpc-peerlink}**
3. **show interface status err-disabled**
4. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: <pre>switch# configure terminal switch(config)# </pre>	グローバルコンフィギュレーションモードを開始します。
Step 2	errdisable recovery cause {all bpduguard failed-port-state link-flap loopback miscabling psecure-violation security-violation storm-control udld vpc-peerlink} 例: <pre>switch(config)# errdisable recovery cause all switch(config-if)# </pre>	インターフェイスが error-disabled ステートから自動的に回復する条件を指定すると、デバイスはインターフェイスを再びアップします。デバイスは 300 秒待機してからリトライします。デフォルトではディセブルになっています。
Step 3	show interface status err-disabled 例: <pre>switch(config)# show interface status err-disabled switch(config-if)# </pre>	(任意) error-disabled インターフェイスに関する情報を表示します。
Step 4	copy running-config startup-config 例: 	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

Error-Disable 検出のイネーブル化

コマンドまたはアクション	目的
switch(config)# copy running-config startup-config	

例

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

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

Error-Disable 検出のイネーブル化

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: <pre>switch# configure terminal switch(config)#{</pre>	グローバルコンフィギュレーションモードを開始します。
Step 2	errdisable detect cause {acl-exception all link-flap loopback} 例: <pre>switch(config)# errdisable detect cause all switch(config-if)#{</pre>	インターフェイスを error-disabled ステートにする条件を指定します。デフォルトではイネーブルになっています。
Step 3	shutdown 例: <pre>switch(config-if)#{ shutdown switch(config)#{</pre>	インターフェイスを管理ダウンさせます。インターフェイスを error-disabled ステートから手動で回復させるには、最初にこのコマンドを入力します。

	コマンドまたはアクション	目的
Step 4	no shutdown 例: <pre>switch(config-if)# no shutdown switch(config)#</pre>	インターフェイスを管理アップし、error-disabled ステートから手動で回復させるインターフェイスをイネーブルにします。
Step 5	show interface status err-disabled 例: <pre>switch(config)# show interface status err-disabled</pre>	(任意) error-disabled インターフェイスに関する情報を表示します。
Step 6	copy running-config startup-config 例: <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

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

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

error-disable ステート回復間隔の設定

error-disabled 回復タイマーの値を設定できます。

手順の概要

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

手順の詳細**手順**

	コマンドまたはアクション	目的
Step 1	configure terminal 例: <pre>switch# configure terminal switch(config)#</pre>	グローバルコンフィギュレーションモードを開始します。

MDIX パラメータの設定

	コマンドまたはアクション	目的
Step 2	errdisable recovery interval <i>interval</i> 例: <pre>switch(config)# errdisable recovery interval 32 switch(config-if) #</pre>	インターフェイスが error-disabled ステートから回復する間隔を指定します。有効範囲は 30 ~ 65535 秒で、デフォルトは 300 秒です。
Step 3	show interface status err-disabled 例: <pre>switch(config)# show interface status err-disabled switch(config-if) #</pre>	(任意) error-disabled インターフェイスに関する情報を表示します。
Step 4	copy running-config startup-config 例: <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

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

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

MDIX パラメータの設定

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

始める前に

リモートポートの MDIX を有効にします。

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: <pre>switch# configure terminal switch(config)#</pre>	グローバルコンフィギュレーションモードを開始します。
Step 2	interface ethernet slot / port 例: <pre>switch(config)# interface ethernet 3/1 switch(config-if)#</pre>	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。
Step 3	mdix auto 例: <pre>switch(config)# mdix auto switch(config-if)#</pre>	ポートの MDIX 検出をイネーブルまたはディセーブルにするかどうかを指定します。
Step 4	show interface ethernet slot / port 例: <pre>switch(config)# show interface ethernet 3/1 switch(config-if)#</pre>	インターフェイス ステータスを表示します。MDIX ステータスもあわせて表示します。
Step 5	exit 例: <pre>switch(config)# exit</pre>	インターフェイス モードを終了します。
Step 6	copy running-config startup-config 例: <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

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

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

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

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

■ MTU サイズの設定

MTU はインターフェイスごとに設定されます。インターフェイスはレイヤ2またはレイヤ3インターフェイスにすることができます。すべてのインターフェイスのデフォルト MTU は 1500 バイトです。この値は、システムデフォルト MTU と呼ばれます。レイヤ2インターフェイスは、システム ジャンボ MTU のデフォルト値である 9216 バイトの値で設定できます。1500 ～ 9216 の MTU 値を許可するには、インターフェイスを同じ値に設定できる適切な値にシステム ジャンボ MTU を調整する必要があります。



(注) システム ジャンボ MTU サイズを変更できます。値が変更されると、システム ジャンボ MTU 値を使用するレイヤ2インターフェイスは新しいシステム ジャンボ MTU 値に自動的に変更します。

レイヤ3インターフェイスは、レイヤ3物理インターフェイススイッチ仮想インターフェイス(SVI)にすることでき、サブインターフェイスでは、MTU サイズを 576 ～ 9216 バイトに設定できます。

MTU サイズの設定

MTU はインターフェイスごとに設定されます。インターフェイスはレイヤ2またはレイヤ3インターフェイスにすることができます。すべてのインターフェイスのデフォルト MTU は 1500 バイトです。この値は、システムデフォルト MTU と呼ばれます。レイヤ2インターフェイスは、システム ジャンボ MTU のデフォルト値である 9216 バイトの値で設定できます。1500 ～ 9216 の MTU 値を許可するには、インターフェイスを同じ値に設定できる適切な値にシステム ジャンボ MTU を調整する必要があります。



(注) システム ジャンボ MTU サイズを変更できます。値が変更されると、システム ジャンボ MTU 値を使用するレイヤ2インターフェイスは新しいシステム ジャンボ MTU 値に自動的に変更します。

レイヤ3インターフェイスは、レイヤ3物理インターフェイススイッチ仮想インターフェイス(SVI)にすることでき、サブインターフェイスでは、MTU サイズを 576 ～ 9216 バイトに設定できます。

システム ジャンボ MTU サイズの設定

レイヤ2インターフェイス MTU 値のシステム ジャンボ MTU を設定して使用できます。システム ジャンボ MTU は、1500 ～ 9216 の偶数で指定する必要があります。システム ジャンボ MTU のデフォルト値は 9216 バイトです。

手順の概要

1. **configure terminal**
2. **system jumbomtu size**
3. **interface type slot/port**

4. **mtu size**
5. **exit**
6. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: switch# configure terminal switch(config)#	グローバルコンフィギュレーションモードを開始します。
Step 2	system jumbomtu size 例: switch(config)# system jumbomtu 8000 switch(config)#	システム ジャンボ MTU サイズを指定します。1500 ~ 9216 の偶数を使用します。
Step 3	interface type slot/port 例: switch(config)# interface ethernet 2/1 switch(config-if)#	設定するインターフェイスを指定し、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。
Step 4	mtu size 例: switch(config-if)# mtu 8000 switch(config-if)#	システム ジャンボ MTU がレイヤ2インターフェイスに追加されます。
Step 5	exit 例: switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
Step 6	copy running-config startup-config 例: switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

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

```
switch# configure terminal
switch(config)# system jumbomtu 8000
```

帯域幅の設定

```
switch(config)# interface ethernet 2/2
switch(config-if)# mtu 8000
```

帯域幅の設定

イーサネットインターフェイスの帯域幅を設定できます。物理層は、1G、10G、または40Gの変更されない帯域幅を使用しますが、レベル3プロトコルに対して1から100,000,000 KBの値を設定できます。

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: <pre>switch# configure terminal switch(config) #</pre>	グローバル設定モードを開始します。
Step 2	interface ethernet slot/port 例: <pre>switch(config)# interface ethernet 3/1 switch(config-if) #</pre>	設定するイーサネットインターフェイスを指定します。インターフェイスコンフィギュレーションモードを開始します。
Step 3	bandwidth kbps 例: <pre>switch(config-if) # bandwidth 1000000 switch(config-if) #</pre>	情報用としてのみ1～100,000,000の値を帯域幅に指定します。
Step 4	show interface ethernet slot/port 例: <pre>switch(config)# show interface ethernet 2/1</pre>	(任意)インターフェイスステータスを表示します。帯域幅の値もあわせて表示します。
Step 5	exit 例:	インターフェイスモードを終了します。

	コマンドまたはアクション	目的
	switch(config-if) # exit switch(config) #	
Step 6	copy running-config startup-config 例: switch(config) # copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

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

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

スループット遅延の設定

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: switch# configure terminal switch(config) #	グローバル設定モードを開始します。

スループット遅延の設定

	コマンドまたはアクション	目的
Step 2	interface ethernet slot/port 例: <pre>switch(config)# interface ethernet 3/1 switch(config-if) #</pre>	設定するイーサネットインターフェイスを指定します。インターフェイスコンフィギュレーションモードを開始します。
Step 3	delay value 例: <pre>switch(config-if)# delay 10000 switch(config-if) #</pre>	遅延時間を 10 マイクロ秒単位で指定します。1 ~ 16777215 の範囲の情報値を 10 マイクロ秒単位で設定できます。
Step 4	show interface ethernet slot/port 例: <pre>switch(config)# show interface ethernet 3/1 switch(config-if) #</pre>	(任意) インターフェイスステータスを表示します。スループット遅延時間もあわせて表示します。
Step 5	exit 例: <pre>switch(config-if)# exit switch(config) #</pre>	インターフェイス モードを終了します。
Step 6	copy running-config startup-config 例: <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

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

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



(注)

feature eigrp コマンドを実行して、最初に EIGRP 機能がイネーブルであることを確認するコマンドを使用します。

インターフェイスのシャットダウンおよび再開

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

手順の概要

1. **configure terminal**
2. **interface interface**
3. **shutdown**
4. **show interface interface**
5. **no shutdown**
6. **show interface interface**
7. **exit**
8. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: <pre>switch# configure terminal switch(config) #</pre>	グローバルコンフィギュレーションモードを開始します
Step 2	interface interface 例: <pre>switch(config)# interface ethernet 2/1 switch(config-if) # switch(config)# interface mgmt0 switch(config-if) #</pre>	設定するインターフェイスを指定します。インターフェイスタイプと ID を指定できます。イーサネットポートの場合は、 <i>ethernet slot/port</i> を使用します。管理インターフェイスの場合は、 <i>mgmt0</i> を使用します。 例: <ul style="list-style-type: none"> 1番目の例は、スロット2、ポート1イーサネットインターフェイスを指定する方法を示します。

■ インターフェイスのシャットダウンおよび再開

	コマンドまたはアクション	目的
		• 2番目の例は、管理インターフェイスを指定する方法を示しています。
Step 3	shutdown 例: <pre>switch(config-if) # shutdown switch(config-if) #</pre>	インターフェイスをディセーブルにします。
Step 4	show interface interface 例: <pre>switch(config-if) # show interface ethernet 2/1 switch(config-if) #</pre>	(任意) インターフェイスステータスを表示します。管理ステータスもあわせて表示します。
Step 5	no shutdown 例: <pre>switch(config-if) # no shutdown switch(config-if) #</pre>	インターフェイスを再びイネーブルにします。
Step 6	show interface interface 例: <pre>switch(config-if) # show interface ethernet 2/1 switch(config-if) #</pre>	(任意) インターフェイスステータスを表示します。管理ステータスもあわせて表示します。
Step 7	exit 例: <pre>switch(config-if) # exit switch(config) #</pre>	インターフェイス モードを終了します。
Step 8	copy running-config startup-config 例: <pre>switch(config) # copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

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

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

```

UDLD モードの設定

単一方向リンク検出（UDLD）を実行するように設定されているデバイス上のイーサネットインターフェイスには、ノーマルモードの UDLD を設定できます。

インターフェイスのアグレッシブ UDLD モードをイネーブルにするには前もって、そのデバイス上でグローバルに、および指定したインターフェイスで、UDLD をイネーブルにしておく必要があります。



(注) インターフェイスが銅線ポートの場合は、enable UDLD コマンドを使用して UDLD をイネーブルにする必要があります。インターフェイスがファイバポートの場合、インターフェイスで UDLD を明示的にイネーブルにする必要はありません。ただし、enable UDLD コマンドを使用してファイバポートで UDLD をイネーブルにしようとすると、それが有効なコマンドではないことを示すエラー メッセージが表示されることがあります。

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

表 4: 異なるインターフェイスで **UDLD** をイネーブルおよびディセーブルにする CLI 詳細

説明	ファイバポート	銅線またはファイバ以外のポート
デフォルト設定	有効	無効
enable UDLD コマンド	no udld disable	udld enable
disable UDLD コマンド	udld disable	no udld enable

始める前に

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

手順の概要

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

UDLD モードの設定

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: <pre>switch# configure terminal switch(config) #</pre>	グローバル構成モードを開始します。
Step 2	[no] feature udld 例: <pre>switch(config)# feature udld switch(config)# switch(config)# no feature udld switch(config) #</pre>	デバイスのUDLDをイネーブル/ディセーブルにします。
Step 3	udld message-time seconds 例: <pre>switch(config)# udld message-time 30 switch(config) #</pre>	(任意) UDLD メッセージを送信する間隔を指定します。有効な範囲は 7 ~ 90 秒で、デフォルトは 15 秒です。
Step 4	udld aggressive 例: <pre>switch(config)# udld aggressive switch(config) #</pre>	すべての光ファイバインターフェイス上で、アグレッシブモードUDLDをデフォルトで有効にします。すべてのファイバポートでアグレッシブモードのUDLDをデフォルトでディセーブルにするには、 no 形式を使用します。 (注) UDLD モードを使用するようにポートを構成するには、 udld aggressive コマンドを使用します。 <ul style="list-style-type: none"> アグレッシブモードの光ファイバインターフェイスをイネーブルにするには、グローバルコマンドモードで udld aggressive コマンドを入力します。これにより、すべての光ファイバインターフェイスがアグレッシブUDLDモードになります。 銅線インターフェイスでアグレッシブモードをイネーブルにするには、インターフェイスモードで udld aggressive コマンドを入力し、アグレッシブUDLDモードに設定したい各インターフェイスを指定します。

	コマンドまたはアクション	目的
		アグレッシブ UDLD モードを使用するには、リンクの両端のインターフェイスをアグレッシブ UDLD モードに構成する必要があります。
Step 5	interface ethernet slot/port 例: <pre>switch(config)# interface ethernet 3/1 switch(config-if)# </pre>	(任意) 設定するインターフェイスを指定します。インターフェイスコンフィギュレーションモードを開始します。
Step 6	udld [enable disable] 例: <pre>switch(config-if)# udld enable switch(config-if)# </pre>	すべての光ファイバインターフェイス上で、標準モードの UDLD をデフォルトでイネーブルにします。すべてのファイバポートで通常モードの UDLD をデフォルトでディセーブルにするには、 no 形式を使用します。
Step 7	show udld [ethernet slot/port global neighbors] 例: <pre>switch(config)# show udld switch(config)# </pre>	(任意) UDLD のステータスを表示します。
Step 8	exit 例: <pre>switch(config-if-range)# exit switch(config)# </pre>	インターフェイス モードを終了します。
Step 9	copy running-config startup-config 例: <pre>switch(config)# copy running-config startup-config </pre>	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、デバイスの UDLD をイネーブルにする例を示します。

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

```

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

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

```

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

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

```

■ デバウンス タイマーの設定

```
switch(config-if-range)# no udld enable
switch(config-if-range)# exit
```

次に、デバイスの UDLD をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature udld
switch(config)# exit
```

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

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

次の例は、銅線イーサネットインターフェイス 3/1 のアグレッシブ UDLD モードをイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 3
switch(config-if)# udld aggressive
```

次の例は、アグレッシブ モードがイネーブルになっているかどうかを確認する方法を示しています。

```
switch# sh udld global

UDLD global configuration mode: enabled-aggressive
UDLD global message interval: 15
switch#
```

次に、udld アグレッシブ モードが特定のインターフェイスで動作可能かどうかを確認する例を示します。

```
switch# sh udld ethernet 8/2

Interface Ethernet8/2
-----
Port enable administrative configuration setting: device-default
Port enable operational state: enabled-aggressive
Current bidirectional state: bidirectional
Current operational state: advertisement - Single neighbor detected
Message interval: 15
Timeout interval: 5
<>
```

デバウンス タイマーの設定

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



(注)

サービス プロバイダー ネットワークに接続すると、10G および 100G ポートのリンク状態が繰り返し変化することがあります。リンクリセットまたはブレークリンク機能の一部として、リンク状態が変更された場合に、SFP の Tx 電源ライトが N/A 状態に変更されることが予想されます。

ただし、リンク状態の変更中にこの動作を防ぐには、リンクデバウンス タイマーを 500 ミリ秒から開始し、リンクが安定するまで 500 ミリ秒間隔で増加します。DWDM、UVN、および WAN ネットワークでは、可能な限り自動リンク一時停止 (ALS) を無効にすることをお勧めします。Nexus がリンクをオフにすると、ALS は WAN 上のリンクを一時停止します。



(注)

link debounce time および **link debounce link-up time** コマンドは、物理的なイーサネットインターフェイスにしか適用できません。

すべてのイーサーネット ポートのデバウンス時間を表示するには、**show interface debounce** コマンドを使用します。

この **link debounce time** コマンドは、Cisco Nexus 3600 シリーズスイッチの 1G、10G、40G、25G、および 100G SFP / QSFP ポートでサポートされます。

手順の概要

1. **configure terminal**
2. **interface ethernet slot/port**
3. **link debounce time time**

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
Step 2	interface ethernet slot/port 例: <pre>switch(config)# interface ethernet 3/1 switch(config-if)#</pre>	設定するイーサネットインターフェイスを指定します。インターフェイスコンフィギュレーションモードを開始します。
Step 3	link debounce time time 例:	指定した時間 (1 ~ 5,000 ミリ秒) でデバウンス タイマーをイネーブルにします。

■ ポートプロファイルの設定

コマンドまたはアクション	目的
switch(config-if)# link debounce time 1000 switch(config-if)#	0ミリ秒を指定すると、デバウンス タイマーがディセーブルになります。

例

- 次に、イーサネットインターフェイスのデバウンス タイマーをイネーブルにし、デバウンス時間を1000ミリ秒に設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# link debounce time 1000
```

- 次に、イーサネットインターフェイスのデバウンス タイマーをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# link debounce time 0
```

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

手順

	コマンドまたはアクション	目的
Step 1	configure terminal	グローバルコンフィギュレーション モードを開始します。
Step 2	port-profile [type {ethernet interface-vlan port-channel}] name	指定されたタイプのインターフェイスのポート プロファイルを作成して命名し、ポート プロファイル コンフィギュレーション モードを開始します。
Step 3	exit	ポート プロファイル コンフィギュレーション モードを終了します。
Step 4	(任意) show port-profile	ポート プロファイル 設定を表示します。
Step 5	(任意) copy running-config startup-config	実行 コンフィギュレーション を、スタートアップ コンフィギュレーション にコピーします。

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。

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

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

手順

	コマンドまたはアクション	目的
Step 1	configure terminal	グローバルコンフィギュレーションモードを開始します。
Step 2	port-profile [type {ethernet interface-vlan port-channel}] name	指定されたポートプロファイルのポートプロファイルコンフィギュレーションモードを開始し、プロファイルの設定を追加または削除します。
Step 3	exit	ポートプロファイルコンフィギュレーションモードを終了します。
Step 4	(任意) show port-profile	ポートプロファイル設定を表示します。
Step 5	(任意) copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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

手順

	コマンドまたはアクション	目的
Step 1	configure terminal	グローバルコンフィギュレーションモードを開始します。
Step 2	interface [ethernet slot/port interface-vlan vlan-id port-channel number]	インターフェイスの範囲を選択します。
Step 3	inherit port-profile name	指定したポート プロファイルを、選択したインターフェイスに割り当てます。
Step 4	exit	ポート プロファイルコンフィギュレーションモードを終了します。
Step 5	(任意) show port-profile	ポート プロファイル設定を表示します。
Step 6	(任意) copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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。

■ 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

手順

	コマンドまたはアクション	目的
Step 1	configure terminal	グローバルコンフィギュレーション モードを開始します。
Step 2	port-profile [type {ethernet interface-vlan port-channel}] name	指定されたタイプのインターフェイスのポートプロファイルを作成して命名し、ポートプロファイルコンフィギュレーション モードを開始します。
Step 3	state enabled	そのポートプロファイルをイネーブルにします。
Step 4	exit	ポートプロファイルコンフィギュレーション モードを終了します。
Step 5	(任意) show port-profile	ポートプロファイル設定を表示します。
Step 6	(任意) copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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

手順

	コマンドまたはアクション	目的
Step 1	configure terminal	グローバルコンフィギュレーションモードを開始します。
Step 2	port-profile <i>name</i>	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。
Step 3	inherit port-profile <i>name</i>	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。
Step 4	exit	ポート プロファイルコンフィギュレーションモードを終了します。
Step 5	(任意) show port-profile	ポート プロファイル設定を表示します。
Step 6	(任意) copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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
```

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

```
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

手順

	コマンドまたはアクション	目的
Step 1	configure terminal	グローバルコンフィギュレーションモードを開始します。
Step 2	interface [ethernet slot/port interface-vlan vlan-id port-channel number]	インターフェイスの範囲を選択します。
Step 3	no inherit port-profile name	指定したポートプロファイルを、選択したインターフェイスから割り当て解除します。
Step 4	exit	ポートプロファイルコンフィギュレーションモードを終了します。
Step 5	(任意) show port-profile	ポートプロファイル設定を表示します。
Step 6	(任意) copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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

手順

	コマンドまたはアクション	目的
Step 1	configure terminal	グローバルコンフィギュレーションモードを開始します。
Step 2	port-profile <i>name</i>	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。
Step 3	no inherit port-profile <i>name</i>	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。
Step 4	exit	ポートプロファイルコンフィギュレーションモードを終了します。
Step 5	(任意) show port-profile	ポートプロファイル設定を表示します。
Step 6	(任意) copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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
```

DWDMの設定

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

DWDMの設定

使用可能な96の波長のいずれかで動作するようにDWDMを設定できます。

手順の概要

1. **configure terminal**
2. **interface interface**
3. **itu channel 1-96**
4. **exit**
5. **show run interface**
6. **show itu channel all**

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: <pre>switch# configure terminal switch(config) #</pre>	グローバルコンフィギュレーションモードを開始します
Step 2	interface interface 例: <pre>config) # interface <type slot/port> switch(config-if) #</pre>	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。
Step 3	itu channel 1-96 例: <pre>config) # interface <type slot/port> switch(config-if) # itu channel ?</pre>	ituチャネル値を指定し、設定を入力します。
Step 4	exit 例: <pre>switch(config-if) # exit switch(config) #</pre>	インターフェイスモードを終了します。
Step 5	show run interface 例: <pre>switch(config) # show run interface <type slot/port> switch(config) #</pre>	ituチャネルの値を表示します。

	コマンドまたはアクション	目的
Step 6	show itu channel all 例: <pre>switch(config)# show itu channel [<> all] switch# sh itu channel ?</pre>	すべてのITUチャネル、波長、および周波数のマッピングを表示します。

25G 自動ネゴシエーションの設定

自動ネゴシエーションを使用すると、デバイスはリンク セグメントを介して所有する拡張動作モードをアドバタイズし、他のデバイスがアドバタイズする可能性がある対応する拡張動作モードを検出できます。自動ネゴシエーションは、リンク セグメントを共有する 2 つのデバイス間で情報を交換し、両方のデバイスの機能を最大限に活用するように自動的に設定する方法を提供します。

25G 自動ネゴシエーションの注意事項と制限事項

- Cisco NX-OS Release 9.2 (1) 以降では、Cisco Nexus 3600 シリーズ プラットフォーム スイッチで、銅ケーブルを使用したネイティブ 25G ポートでの自動ネゴシエーションがサポートされています。
- 自動ネゴシエーションは、25G ブレークアウトポートではサポートされていません。
- Cisco Nexus 3600 スイッチが 9K-C93108TC-FX3P スイッチに接続されている場合、自動ネゴシエーションはサポートされません。
- SFP-H25GB-CU4M または SFP -H25GB-CU5M ケーブルを使用して Cisco Nexus 3600 を 9300-FX/FX2 スイッチに接続する場合は、両方のデバイスで FEC モードを **rs-ieee** に手動で構成する必要があります。この手動構成を行わないと、FEC の不一致により、接続の自動ネゴシエーションとリンクの確立が失敗する可能性があります。

インターフェイスでの FEC の手動有効化

インターフェイス 上で FEC を手動で有効にするには、次の手順を実行します:

手順の概要

1. **configure terminal**
2. **interface ethernet port number**
3. **fec { auto | rs-fec | rs-ieee | fc-fec }**

■ 自動ネゴシエーションの有効化

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: <pre>switch# configure terminal switch(config)#</pre>	グローバルコンフィギュレーションモードを開始します。
Step 2	interface ethernet port number 例: <pre>switch# int e1/7 switch(config-if)#</pre>	インターフェイスを選択し、インターフェイス モードを開始します。
Step 3	fec { auto rs-fec rs-ieee fc-fec } 例: <pre>switch(config-if)# fec auto switch(config-if)#</pre>	選択したインターフェイスで指定した FEC タイプを有効にします。

自動ネゴシエーションの有効化

negotiate auto を使用して自動ネゴシエーションを有効にできます コマンドを使用する必要があります。自動ネゴシエーションを有効にするには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface ethernet port number**
3. **negotiate auto port speed**

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: <pre>switch# configure terminal switch(config)#</pre>	グローバルコンフィギュレーションモードを開始します。
Step 2	interface ethernet port number 例: <pre>switch# int e1/7 switch(config-if)#</pre>	インターフェイスを選択し、インターフェイス モードを開始します。

	コマンドまたはアクション	目的
	switch# int e1/7 switch(config-if)#	
Step 3	negotiate auto port speed 例: switch(config-if)# negotiate auto 25000 switch(config-if)#	選択したインターフェイスの自動ネゴシエーションを有効にします。 (注) このコマンドは、25G ネイティブリンクの両側のインターフェイスに適用する必要があります。

次に、指定したイーサネットインターフェイスで自動ネゴシエーションを有効にする例を示します。

例

```
switch# sh int e1/7 st
-----
Port          Name           Status      Vlan     Duplex    Speed     Type
-----
Eth1/7        --            connected   routed   full      25G      SFP-H25GB-CU1M
switch# conf
switch(config)# int e1/7
switch(config-if)# negotiate auto 25000
```

自動ネゴシエーションのディセーブル化

no negotiate auto コマンドを使用することにより、自動ネゴシエーションをディセーブルすることができます。自動ネゴシエーションを設定するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface ethernet port number**
3. **no negotiate auto port speed**

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: switch# configure terminal switch(config)#	グローバルコンフィギュレーションモードを開始します。

■ 基本インターフェイス パラメータの確認

	コマンドまたはアクション	目的
Step 2	interface ethernet port number 例: <pre>switch# int e1/7 switch(config-if) #</pre>	インターフェイスを選択し、インターフェイス モードを開始します。
Step 3	no negotiate auto port speed 例: <pre>switch(config-if) # no negotiate auto 25000 switch(config-if) #</pre>	選択したインターフェイスの自動ネゴシエーションをディセーブルにします。 (注) このコマンドは、リンクの両側のインターフェイスに適用する必要があります。

次に、指定したイーサネットインターフェイスで自動ネゴシエーションをディセーブルにする例を示します。

例

```
switch# sh int e1/7 st
-----
Port      Name       Status   Vlan    Duplex  Speed   Type
-----
Eth1/7    --        connected routed   full    25G    SFP-H25GB-CU1M
switch# conf
switch(config)# int e1/7
switch(config-if)# no negotiate auto 25000
```

基本インターフェイス パラメータの確認

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

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

コマンド	目的
show cdp all	CDP ステータスを表示します。
show interface interface	1つまたはすべてのインターフェイスに設定されている状態を表示します。
show interface brief	インターフェイスの状態表を表示します。
show interface status err-disabled	error-disabledインターフェイスに関する情報を表示します。

コマンド	目的
show udld interface	現在のインターフェイスまたはすべてのインターフェイスの UDLD ステータスを表示します。
show udld global	現在のデバイスの UDLD ステータスを表示します。
show interface fec	すべてのインターフェイスの FEC ステータスが表示されます。

インターフェイス カウンタのモニタリング

Cisco NX-OS を使用して、インターフェイス カウンタを表示し、クリアできます。

インターフェイス統計情報の表示

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

手順の概要

1. **configure terminal**
2. **interface ether slot/port**
3. **load-interval counters [1 | 2 | 3] seconds**
4. **show interface interface**
5. **exit**
6. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: <pre>switch# configure terminal switch(config) #</pre>	グローバル設定モードを開始します。
Step 2	interface ether slot/port 例: <pre>switch(config)# interface ether 4/1 switch(config) #</pre>	インターフェイスを指定します。

■ インターフェイス カウンタのクリア

	コマンドまたはアクション	目的
Step 3	load-interval counters [1 2 3] seconds 例: <pre>switch(config)# load-interval counters 1 100 switch(config)# </pre>	ビットレートおよびパケットレートの統計情報を収集する最大3つのサンプリング間隔を設定します。各カウンタのデフォルト値は、次のとおりです。 1: 30秒 (VLANの場合 60秒) 2: 300秒 3: 未設定
Step 4	show interface interface 例: <pre>switch(config)# show interface ethernet 2/2 switch# </pre>	(任意) インターフェイスステータスを表示します。カウンタもあわせて表示します。
Step 5	exit 例: <pre>switch(config-if-range)# exit switch(config)# </pre>	インターフェイス モードを終了します。
Step 6	copy running-config startup-config 例: <pre>switch(config)# copy running-config startup-config </pre>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

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

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

```

インターフェイス カウンタのクリア

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

手順の概要

1. **clear counters interface [all | ethernet slot/port | loopback number | mgmt number | port channel channel-number]**

2. **show interface *interface***
3. **show interface [ethernet *slot/port* | port channel *channel-number*] counters**

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	clear counters interface [all ethernet <i>slot/port</i> loopback <i>number</i> mgmt <i>number</i> port channel <i>channel-number</i>] 例: <pre>switch# clear counters ethernet 2/1 switch#</pre>	インターフェイス カウンタをクリアします。
Step 2	show interface <i>interface</i> 例: <pre>switch# show interface ethernet 2/1 switch#</pre>	(任意) インターフェイスのステータスを表示します。
Step 3	show interface [ethernet <i>slot/port</i> port channel <i>channel-number</i>] counters 例: <pre>switch# show interface ethernet 2/1 counters switch#</pre>	(任意) インターフェイス カウンタを表示します。

例

次に、イーサネット ポート 5/5 のカウンタをクリアする例を示します。

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

■ インターフェイス カウンタのクリア



第 4 章

レイヤ2インターフェイスの設定

- イーサネットインターフェイスの概要, [on page 55](#)
- レイヤ2インターフェイスのガイドラインおよび制約事項 ([58 ページ](#))
- インターフェイス速度 ([58 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 ([58 ページ](#))
- SVI 自動ステート ([59 ページ](#))
- Cisco Discovery Protocol, [on page 60](#)
- errordisable ステート ([60 ページ](#))
- デフォルトインターフェイス ([62 ページ](#))
- デバウンス タイマー パラメータについて, [on page 62](#)
- MTU 設定, [on page 62](#)
- 物理イーサネットのデフォルト設定, [on page 64](#)
- インターフェイス情報の表示, [on page 65](#)

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

UDLD パラメータ

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

シスコ独自の單一方向リンク検出（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、單一方向リンクの存在を検出できます。スイッチが单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。单方向リンクは、スパニングツリートポロジループをはじめ、さまざまな問題を引き起こす可能性があります。

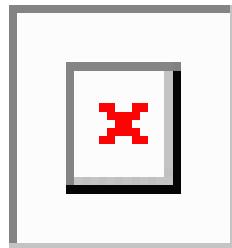
UDLDは、レイヤ1プロトコルと協調してリンクの物理ステータスを検出するレイヤ2プロトコルです。レイヤ1では、オートネゴシエーションは物理シグナリングと障害検出を行います。

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、物理的な單一方向接続と論理的な單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、单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、これらの光ファイルが正しく接続されているかどうか、および正しいネイバー間でトラフィックが双方向に流れているかを調べます。自動ネゴシエーションはレイヤ1で動作するため、このチェックは、自動ネゴシエーションでは実行できません。

Cisco Nexus 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、そのリンクは單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プロトコルにより单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、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、单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 2: 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 5: 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。

- リンクの一方にポート スタックが生じる (送受信どちらも)
- リンクの一方がダウンしているにもかかわらず、リンクのもう一方がアップしたままになる

このような場合、UDLD アグレッシブ モードでは、リンクのポートの 1 つがディセーブルになり、トラフィックが廃棄されるのを防止します。

レイヤ2インターフェイスのガイドラインおよび制約事項

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 6: 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

Cisco Nexus 3600 プラットフォーム ポートでは、QSFP ポートを 40 ギガビットイーサネット モードまたは 4x10 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。デフォルトでは、49 ～ 54 の番号が付けられた 6 つの QSFP インターフェイス ポートがあり、40 ギガビットイーサネット モードで動作できます。これらの 40 ギガビットイーサネット ポートには、2 タップの命

名規則で番号が割り当てられます。たとえば、2番目の40ギガビットイーサネットポートには1/50という番号が割り当てられます。設定を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変更するプロセスをブレークアウトと呼び、10ギガビットイーサネットからギガビットイーサネットに設定を変更するプロセスをブレークインと呼びます。40Gポートを10Gポートにブレークアウトする場合、得られたポートには3タプルの命名規則を使って番号が割り当てられます。たとえば、2番目の40ギガビットイーサネットポートのブレークアウトポートには1/49/1、1/49/2、1/49/3、1/49/4という番号が割り当てられます。



(注) 40Gポートを4x10Gモードにブレークアウトするか、100Gポートを4x25Gモードにブレークアウトすると、ブレー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ークアウトするか、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ークインすると、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+40Gb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10GbSFP-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。ブレー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ークアウトし、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ークインする機能により、永続的に定義せずに、任意のブレー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のブリッジング機能とルーティング機能間の論理インターフェイスを表します。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、アクセサー、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、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 7: 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)

errdisable 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として表示されます。いったんインターフェイスがerrdisabl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

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	パケットサイズ	増分カウンタ	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	Dropped

設定	パケットサイズ	増分カウンタ	トラフィック
L2ポート: ネットワーク QoS 設定のジャンボ MTU 9216	6400	Jumbo	Forwarded
L2ポート: ネットワーク QoS 設定のジャンボ MTU 9216	10000	ジャンボ、ジャイアント、および入力エラー	Dropped
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	Jumbo	パケットはCPUにパントされ(CoPP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	Jumbo	パケットはCPUにパントされ(CoPP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	10000	ジャンボ、ジャイアント、および入力エラー	Dropped
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	Jumbo	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	10000	ジャンボ、ジャイアント、および入力エラー	Dropped
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	Dropped

■ ダウンリンク遅延



- (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 ¹ 。	1500 バイト
ポートモード	アクセス（Access）
スピード	オート（10000）

¹ 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# show interface type slot/port	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# show interface type slot/port capabilities	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# show interface type slot/port transceiver	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# show interface brief	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# show interface flowcontrol	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
```

■ インターフェイス情報の表示

```
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 Interface	VLAN	Type	Mode	Status	Reason	Speed	Port 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   Holdtme  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
```

■ インターフェイス情報の表示



第 5 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 (69 ページ)
- ルーテッドインターフェイス (69 ページ)
- サブインターフェイス (70 ページ)
- VLANインターフェイス (71 ページ)
- インターフェイスの VRF メンバーシップの変更 (72 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 (72 ページ)
- ループバックインターフェイス (73 ページ)
- IP アンナンバード (73 ページ)
- トンネルインターフェイス (74 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 (74 ページ)
- レイヤ3インターフェイスのデフォルト設定 (75 ページ)
- SVI 自動ステートのディセーブル化 (75 ページ)
- レイヤ3インターフェイスの設定 (75 ページ)
- レイヤ3インターフェイス設定の確認 (90 ページ)
- レイヤ3インターフェイスのモニタリング (91 ページ)
- レイヤ3インターフェイスの設定例 (93 ページ)
- レイヤ3インターフェイスの関連資料 (94 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、パケットを静态的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

■ サブインターフェイス

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

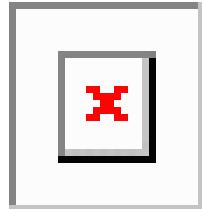
Ethernet2/1.1というサブインターフェイスを作成できます。この場合、.1はそのサブインターフェイスを表します。

Cisco NX-OSでは、親インターフェイスがイネーブルの場合にサブインターフェイスがイネーブルになります。サブインターフェイスは、親インターフェイスには関係なくシャットダウンできます。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ки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ки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E2/1のルータBに接続するスイッチのトランки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ки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3: 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ィングインターフェイスです。

VLANには1つのVLANインターフェイスだけを関連付けることができますが、VLANにVLANインターフェイスを設定する必要があるのは、VLAN間でルーティングする場合か、または管理VRF(仮想ルーティング/転送)以外のVRFインスタンスを経由してデバイスをIPホスト接続する場合だけです。VLANインターフェイスの作成を有効にすると、Cisco NX-OSによってデフォルトVLAN(VLAN1)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) VLAN1のVLANインターフェイスは削除できません。

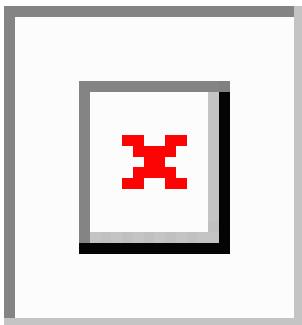
VLANインターフェイスをルーティングするには、トラフィックをルーティングするVLANごとにVLANインターフェイスを作成し、そのVLANインターフェイスにIPアドレスを割り当てて

■ インターフェイスのVRFメンバーシップの変更

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4: 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**vrfmember**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/リストナー（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（バックア）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/リスト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（バックア）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は一度につ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 アンナンバード

IP アン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。

■ トンネルインターフェイス

ポイントツーポイントモードに準拠するインターフェイスは、IPアンナンバードインターフェイスとして使用できます。IPアンナンバード機能はイーサネットインターフェイスとサブインターフェイスでのみサポートされています。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。

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。

- EPBR は、次のCisco Nexus 3600 プラットフォームではサポートされていません：
 - N3K-C36180YC-R
 - N3K-C3636C-R
- 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。

- Cisco Nexus 3000 シリーズ スイッチは、レイヤ3 MTUがすべてのレイヤ3インターフェイスで同じではない場合、そして MTU QoS がジャンボに変更されていた場合、マルチキャスト レイヤ2 トライフィックを CPU にパンクトします。この問題を回避するには、すべてのレイヤ3インターフェイスに同じレイヤ3 MTUが必要です。

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

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

ルーテッドインターフェイスの設定

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface ethernet slot/port	インターフェイスコンフィギュレーションモードを開始します。
Step 3	switch(config-if)# no switchport	インターフェイスをレイヤ3インターフェイスとして設定し、このインターフェイス上のレイヤ2固有の設定を削除します。 (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、 switchport コマンドを使用します。
Step 4	switch(config-if)# [ip ipv6]ip-address/length	このインターフェイスのIPアドレスを設定します。
Step 5	(任意) switch(config-if)# medium {broadcast p2p}	インターフェイスメディアをポイントツーポイントまたはブロードキャストのどちらかとして設定します。 (注) デフォルト設定は broadcast であり、この設定はどの show コマンドにも表示されません。ただし、 p2p に設定を変更した場合、 show running-config コマンドを入力すると、この設定が表示されます。
Step 6	(任意) switch(config-if)# show interfaces	レイヤ3インターフェイスの統計情報を表示します。
Step 7	(任意) switch(config-if)# copy running-config startup-config	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

手順

	コマンドまたはアクション	目的
Step 1	(任意) switch(config-if)# copy running-config startup-config	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。
Step 2	switch(config)# interface ethernet slot/port.number	インターフェイスコンフィギュレーションモードを開始します。slot の範囲は 1 ~ 255 です。port の範囲は 1 ~ 128 です。
Step 3	switch(config-if)# [ip ipv6] address ip-address/length	このインターフェイスの IP アドレスを設定します。
Step 4	switch(config-if)# encapsulation dot1Q vlan-id	サブインターフェイス上の IEEE 802.1Q VLAN カプセル化を設定します。vlan-id の範囲は 2 ~ 4093 です。
Step 5	(任意) switch(config-if)# show interfaces	レイヤ3インターフェイスの統計情報を表示します。
Step 6	(任意) switch(config-if)# copy running-config startup-config	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。

■ インターフェイスでの帯域幅の設定

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

手順

	コマンドまたはアクション	目的
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface ethernet slot/port	インターフェイスコンフィギュレーションモードを開始します。slotの範囲は1～255です。portの範囲は1～128です。
Step 3	switch(config-if)# bandwidth [value inherit [value]]	<p>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。</p> <ul style="list-style-type: none"> • value: 帯域幅のサイズ（KB 単位）。指定できる範囲は1～10000000です。 • inherit: 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。

	コマンドまたはアクション	目的
Step 4	(任意) switch(config-if)# copy running-config startup-config	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

手順

	コマンドまたはアクション	目的
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# feature interface-vlan	VLANインターフェイスモードをイネーブルにします。
Step 3	switch(config)# interface vlan number	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。
Step 4	switch(config-if)# [ip ipv6] address ip-address/length	このインターフェイスのIPアドレスを設定します。
Step 5	switch(config-if)# no shutdown	インターフェイスを管理上アップさせます。

■ VRF メンバーシップ変更時のレイヤ3保持の有効化

	コマンドまたはアクション	目的
Step 6	(任意) switch(config-if)# show interface vlan number	VLANインターフェイスの統計情報を表示します。 number の範囲は 1 ~ 4094 です。
Step 7	(任意) switch(config-if)# copy running-config startup-config	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

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: switch# configure terminal switch(config) #	コンフィギュレーションモードに入ります。
Step 2	system vrf-member-change retain-l3-config 例: switch(config) # system vrf-member-change	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)

コマンドまたはアクション	目的
retain-l3-config Warning: Will retain L3 configuration when vrf member change on interface.	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。

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

手順

	コマンドまたはアクション	目的
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface loopback instance	ループバックインターフェイスを作成します。 <i>instance</i> の範囲は 0 ~ 1023 です。
Step 3	switch(config-if)# [ip ipv6] address ip-address/length	このインターフェイスのIPアドレスを設定します。
Step 4	(任意) switch(config-if)# show interface loopback instance	ループバックインターフェイスの統計情報を表示します。 <i>instance</i> の範囲は 0 ~ 1023 です。
Step 5	(任意) switch(config-if)# copy running-config startup-config	リブートおよびリスト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
```

■ イーサネットインターフェイスでのIPアンナンバードの設定

```
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での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**

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: <pre>switch# configure terminal switch(config) #</pre>	グローバル設定モードを開始します。
Step 2	interface ethernet slot/port port-channel 例: <pre>switch(config)# interface ethernet 1/1 switch(config-if) # switch(config)# interface port-channel 1/1 switch(config-if) #</pre>	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
Step 3	medium p2p 例: <pre>switch(config-if) # medium p2p</pre>	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。
Step 4	ip unnumbered type number 例: <pre>switch(config-if) # ip unnumbered loopback 100</pre>	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</i> および <i>number</i> は、IPアドレスが割り当てられているルータ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)

コマンドまたはアクション	目的
	<i>type</i> は loopback 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

手順

	コマンドまたはアクション	目的
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface interface-typenumber	インターフェイスコンフィギュレーションモードを開始します。
Step 3	switch(config-if)# vrf member vrf-name	このインターフェイスをVRFに追加します。
Step 4	switch(config-if)# FID cleanup[ip ipv6]ip-address/length	このインターフェイスのIPアドレスを設定します。 このステップは、このインターフェイスをVRFに割り当てたあとに行う必要があります。
Step 5	(任意) switch(config-if)# show vrf [vrf-name] interface interface-type number	VRF情報を表示します。
Step 6	(任意) switch(config-if)# show interfaces	レイヤ3インターフェイスの統計情報を表示します。
Step 7	(任意) switch(config-if)# copy running-config startup-config	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。

■ インターフェイス MAC アドレスの設定

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

手順

	コマンドまたはアクション	目的
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface ethernet slot/port	インターフェイスコンフィギュレーションモードを開始します。
Step 3	switch(config-if)# [no] mac-address static router MAC address	<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 no 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"> • E.E.E • EE-EE-EE-EE-EE-EE • EE:EE:EE:EE:EE:EE • EEEE.EEEE.EEEE <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"> • ヌルMACアドレ: 0000.0000.0000

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> ・ブロードキャストMACアドレス: FFFF.FFFF.FFFF ・マルチキャストMACアドレス: 0100.DAAA.ADDD
Step 4	switch(config-if)# show interface ethernet slot/port	(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埋め込み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

手順

	コマンドまたはアクション	目的
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface type slot/port	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。
Step 3	switch(config-if)# no switchport	インターフェイスをレイヤ3インターフェイスとして設定し、このインターフェイス上のレイヤ2固有の設定を削除します。 (注)

■ MAC埋め込みIPv6アドレスの設定

	コマンドまたはアクション	目的
		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、 switchport コマンドを使用します。
Step 4	switch(config-if)# mac-address ipv6-extract	インターフェイスに設定されているIPv6アドレスに埋め込まれている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。
Step 5	switch(config-if)# ipv6 address ip-address/length	このインターフェイスのIPv6アドレスを設定します。
Step 6	switch(config-if)# ipv6 nd mac-extract [exclude nud-phase]	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。 exclude nud-phase 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。 exclude nud-phase (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。
Step 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 unreachables: false
ICMPv6-nd Statistic (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（NUDフェーズを除く）を有効にして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 1/5
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 unreachables: false
  ICMPv6-nd Statistic (sent/received):
    RAs: 6/0, RSs: 0/0, NAs: 2/0, NSs: 7/0, RDs: 0/0
    Interface statistics last reset: never

```

SVI 自動ステートの無効化の設定

```
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

手順

	コマンドまたはアクション	目的
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# [no] system default interface-vlan autostate	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 no 形式を使用します。
Step 3	switch(config)# feature interface-vlan	VLAN インターフェイス SVI の作成をイネーブルにします。
Step 4	switch(config)# interface vlan <i>vlan id</i>	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。
Step 5	(config-if)# [no] autostate	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。
Step 6	(config-if)# end	特権 EXEC モードに戻ります。
Step 7	show running-config interface vlan <i>vlan id</i>	(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を設定できます。

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

手順

	コマンドまたはアクション	目的
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface ethernet type slot/port mgmt mgmt-interface-number vlan vlan id	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。 <i>vlan id</i> の範囲は 1 ~ 4094 です。
Step 3	switch(config-if)# [no] ip ipv6 address dhcp	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 no 形式を使用します。
Step 4	(任意) switch(config)# copy running-config startup-config	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。

■ レイヤ3インターフェイス設定の確認

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
show interface ethernet slot/port	レイヤ3インターフェイスの設定情報、ステータス、カウンタ（インバウンドおよびアウトバウンドパケットレートおよびバイトレートの、5分間指数減少移動平均を含む）を表示します。
show interface ethernet slot/port brief	レイヤ3インターフェイスの動作ステータスを表示します。
show interface ethernet slot/port capabilities	レイヤ3インターフェイスの機能（ポートタイプ、速度、およびデュプレックスを含む）を表示します。
show interface ethernet slot/port description	レイヤ3インターフェイスの説明を表示します。
show interface ethernet slot/port status	レイヤ3インターフェイスの管理ステータス、ポートモード、速度、およびデュプレックスを表示します。
show interface ethernet slot/port.number	サブインターフェイスの設定情報、ステータス、カウンタ（インバウンドおよびアウトバウンドパケットレートおよびバイトレートが5分間に指数関数的に減少した平均値を含む）を表示します。

コマンド	目的
show interface port-channel channel-id,number	ポートチャネルサブインターフェイスの設定情報、ステータス、カウンタ（インバウンドおよびアウトバウンドパケットレートおよびバイオレートの、5分間指數減少移動平均を含む）を表示します。
show interface loopback number	ループバックインターフェイスの設定情報、ステータス、カウンタを表示します。
show interface loopback number brief	ループバックインターフェイスの動作ステータスを表示します。
show interface loopback number description	ループバックインターフェイスの説明を表示します。
show interface loopback number status	ループバックインターフェイスの管理ステータスおよびプロトコルステータスを表示します。
show interface vlan number	VLANインターフェイスの設定情報、ステータス、カウンタを表示します。
show interface vlan number brief	VLANインターフェイスの動作ステータスを表示します。
show interface vlan number description	VLANインターフェイスの説明を表示します。
show interface vlan number status	VLANインターフェイスの管理ステータスおよびプロトコルステータスを表示します。

レイヤ3インターフェイスのモニタリング

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
load-interval seconds counter {1 2 3} seconds	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。
show interface ethernet slot/port counters	レイヤ3インターフェイスの統計情報を表示します（ユニキャスト、マルチキャスト、ブロードキャスト）。

■ レイヤ3インターフェイスのモニタリング

コマンド	目的
show interface ethernet slot/port counters brief load-interval-id	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。
show interface ethernet slot/port counters detailed [all]	レイヤ3インターフェイスの統計情報を表示します。オプションとして、32ビットと64ビットのパケットおよびバイトカウンタ（エラーを含む）をすべて含めることができます。
show interface ethernet slot/port counters error	レイヤ3インターフェイスの入力および出力エラーを表示します。
show interface ethernet slot/port counters snmp	SNMP MIBから報告されたレイヤ3インターフェイスカウンタを表示します。これらのカウンタはクリアできません。
show interface ethernet slot/port.number counters	サブインターフェイスの統計情報（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。
show interface port-channel channel-id.number counters	ポートチャネルサブインターフェイスの統計情報（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。
show interface loopback number counters	ループバックインターフェイスの入力および出力カウンタ（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。
show interface loopback number counters detailed [all]	ループバックインターフェイスの統計情報を表示します。オプションとして、32ビットと64ビットのパケットおよびバイトカウンタ（エラーを含む）をすべて含めることができます。
show interface loopback number counters errors	ループバックインターフェイスの入力および出力エラーを表示します。
show interface vlan number counters	VLANインターフェイスの入力および出力カウンタ（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。

コマンド	目的
show interface vlan <i>number</i> counters detailed [all]	VLANインターフェイスの統計情報を表示します。オプションとして、レイヤ3パケットおよびバイトカウンタをすべて含めることができます（ユニキャストおよびマルチキャスト）。
show interface vlan <i>counters</i> snmp	SNMP MIB から報告された VLANインターフェイスカウンタを表示します。これらの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。

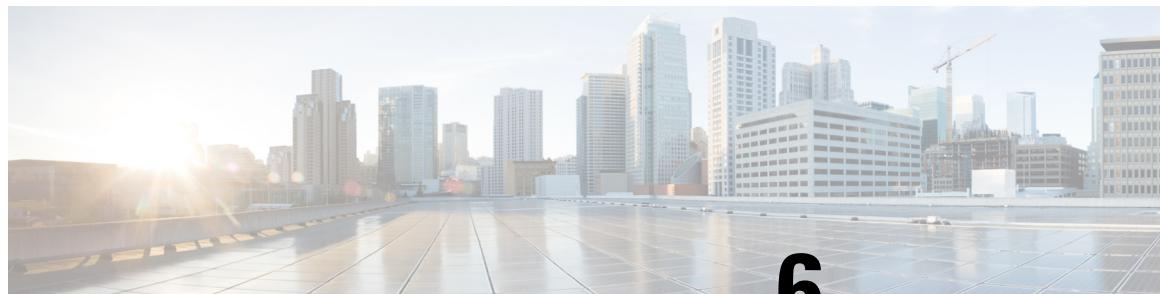
```

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
VLAN	『Cisco Nexus 3600 NX-OS Layer 2 Switching Configuration Guide』の「Configuring VLANs」の章



第 6 章

ポートチャネルの構成

- ポートチャネルについて, on page 95
- ポートチャネルの概要, on page 96
- 互換性要件, on page 97
- ポートチャネルを使ったロードバランシング, on page 99
- シンメトリック ハッシング (100 ページ)
- LACP について (101 ページ)
- 注意事項と制約事項 (105 ページ)
- ポートチャネルの設定 (106 ページ)
- ポートチャネル構成の確認, on page 120
- 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 (121 ページ)
- ロードバランシング発信ポート ID の確認 (122 ページ)
- ポートプロファイル (122 ページ)
- ポートプロファイルの設定 (124 ページ)
- ポートプロファイルの作成 (125 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 (126 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 (127 ページ)
- 特定のポートプロファイルのイネーブル化 (128 ページ)
- ポートプロファイルの継承 (129 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 (130 ページ)
- 継承されたポートプロファイルの削除 (131 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。

ポートチャネルの概要

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ケットが渡されます。

Related Topics

[LACP の概要](#), on page 101

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ったロードバランシング](#), on page 99 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ネル数で空のチャネル 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。メンバー 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。

互換性要件

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
- 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
- Debounce

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
 - Debounce
 - UDLD
 - シャットダウン
 - SNMP トラップ

ポートチャネルを使ったロードバランシング

Cisco NX-OS 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 8: 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)	宛先 MAC	宛先 MAC、宛先 IP	宛先 MAC、宛先 IP
Source IP	送信元 MAC	送信元 MAC、送信元 IP	送信元 MAC、送信元 IP
送信元/宛先 IP	送信元/宛先 MAC	送信元/宛先 MAC、送信元/宛先 IP	送信元/宛先 MAC、送信元/宛先 IP
宛先 TCP/UDP ポート	宛先 MAC	宛先 MAC、宛先 IP	宛先 MAC、宛先 IP、宛先 ポート
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

シンメトリック ハッシング

設定 (Configuration)	レイヤ 2 基準	レイヤ 3 基準	レイヤ 4 基準
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イフィックが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になります。

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イ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イフィック：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イフィック：発信元IPアドレス、宛先IPアドレス
- 非IPマルチキャストトライフィック：発信元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イフィックをハッシュします。

シンメトリック ハッシング

ポートチャネル上のトライ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イフィックフローを受信することが不可欠です。通常、順方向および逆方向のトライ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、双方向トライ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（順方向トライフィックの送信元が逆方向トライ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

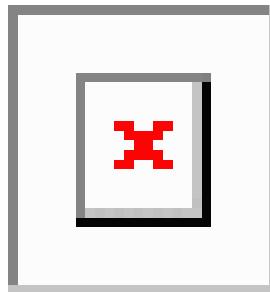
LACP の概要



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 5: 個々のリンクをポート 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。

■ チャネルモード

- **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てシステムIDを生成します。また、システムプライオリティを他のデバイスとのネゴシエーションにも使用します。システムプライオリティ値が大きいほど、プライオリティは低くなります。



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、チャネル モードをまとめたものです。

Table 9: ポート チャネルの個別リンクのチャネル モード

チャネル モード	説明
passive	ポートをパッシブなネゴシエーション状態にする LACP モード。この状態では、ポートは受信した LACP パケットに応答はしますが、LACP ネゴシエーションを開始することはありません。
active	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。 チャネルで LACP をイネーブルにするには、そのチャネルのインターフェイスでチャネル モードを active または passive に設定します。LACP 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 チャネル グループには参加しません。 no lACP suspend-individual 構成は、Cisco Nexus 3600 スイッチではデフォルトでサポートされます。

passive と active のどちらのモードでも、ポート速度やトランки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が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 10: LACP がイネーブルのポート チャネルとスタティック ポート チャネル

構成	LACP がイネーブルのポート チャネル	スタティック ポート チャネル
適用されるプロトコル	グローバルにイネーブル化	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"> • Active • Passive 	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

ポートチャネル設定時のガイドラインおよび制約事項は、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

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


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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface port-channel channel-number	設定するポートチャネルインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。範囲は 1 ~ 4096 です。チャネルグループがまだ存在していないければ、Cisco NX-OS によって自動的に作成されます。
Step 3	switch(config)# no interface port-channel channel-number	ポートチャネルを削除し、関連するチャネルグループを削除します。

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

新規のチャネルグループ、または他のポートがすでに属しているチャネルグループにポートを追加できます。ポート チャネルがない場合は、Cisco NX-OS によってこのチャネル 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。



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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface type slot/port	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。
Step 3	(Optional) switch(config-if)# switchport mode trunk	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。
Step 4	(Optional) switch(config-if)# switchport trunk {allowed vlan vlan-id native vlan vlan-id}	トランク ポートに必要なパラメータを設定します。
Step 5	switch(config-if)# channel-group channel-number	チャネル グループ内にポートを設定し、モードを設定します。channel-number の指定できる範囲は 1 ~ 4096 です。ポート チャネルがない場合は、Cisco NX-OS によってこのチャネル 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。
Step 6	(Optional) switch(config-if)# no channel-group	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。

ポートチャネルを使ったロードバランシングの設定

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-pol}**
3. (Optional) switch(config)# **no port-channel load-balance ethernet**
4. (Optional) switch# **show port-channel load-balance**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 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-pol}	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source-dest-macです。

Note

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 **destination-ip-gre**、**source-dest-ip-gre** および **source-ip-gre** 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

	Command or Action	Purpose
		<p>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 symmetric キーワードを使用します。対称ハッシュは、双方向のトライ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"> • source-dest-ip-only • source-dest-port-only • source-dest-ip • source-dest-port • source-dest-ip-gre
Step 3	(Optional) switch(config)# no port-channel load-balance ethernet	ロードバランシングアルゴリズムをデフォルトの source-dest-mac に戻します。
Step 4	(Optional) switch# show port-channel load-balance	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

■ ポートに対するチャネルモードの設定

ネルにグループ化されます。その後、ポートチャネルは单一のブリッジポートとしてスパニングツリーに追加されます。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# feature lacp	スイッチ上で LACP をイネーブルにします。
Step 3	(Optional) switch(config)# show feature	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**Procedure**

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface type slot/port	設定するインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。
Step 3	switch(config-if)# channel-group channel-number [force] [mode {on active passive}]	<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>force: 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>mode: 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>active: 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>on: (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>passive: 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>
Step 4	switch(config-if)# no channel-group number mode	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。

LACP ポートチャネルの MinLink の設定

```
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

手順

	コマンドまたはアクション	目的
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface port-channel <i>number</i>	設定するインターフェイスを指定します。
Step 3	switch(config-if)# [no] lacp min-links <i>number</i>	<p>最小リンク数を設定します。</p> <p><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。</p> <p>この機能をディセーブルにするには、このコマンドの no 形式を使用します。</p>
Step 4	(任意) switch(config)# show running-config interface port-channel <i>number</i>	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。ただし、非 LACP ポートチャネルに対してこれらの機能の CLI コマンドを入力できますが、これらのコマンドは動作不能です。



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

始める前に

正しいポートチャネルインターフェイスを使用してい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 <i>number</i>**

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例:	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。

■ LACP 高速タイマー レートの設定

	コマンドまたはアクション	目的
	switch# configure terminal switch(config)#	
Step 2	interface port-channel number 例: switch(config)# interface port-channel 3 switch(config-if)#	設定するインターフェイスを選択します。
Step 3	lacp max-bundle number 例: switch(config-if)# lacp max-bundle <number>	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、pc_max_links_config およびポートチャネルで許可されている pc_max_active_members の最小数です。
Step 4	show running-config interface port-channel <number> 例: switch(config-if)# show running-config interface port-channel 3	(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

手順

	コマンドまたはアクション	目的
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface type slot/port	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。
Step 3	switch(config-if)# lacp rate fast	LACP がサポートされているインターフェイスに LACP 制御パケットを送信する際のレートとして高速レート（1 秒）を設定します。

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。

LACP ポート プライオリティの設定

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# lacp system-priority priority	LACP で使用するシステム プライオリティを設定します。指定できる範囲は 1 ~ 65535 で、値が大きいほどプライオリティは低くなります。デフォルト値は 32768 です。
Step 3	(Optional) switch# show lacp system-identifier	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**Procedure**

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface type slot/port	設定するインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。
Step 3	switch(config-if)# lacp port-priority priority	LACP で使用するポートプライオリティを設定します。指定できる範囲は 1 ~ 65535 で、値が大きいほどプライオリティは低くなります。デフォルト値は 32768 です。

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 コンバージェンスのディセーブル化

デフォルトで、LACP グレースフル コンバージェンスはイネーブルになっています。あるデバイスとの LACP 相互運用性をサポートする必要がある場合、コンバージェンスをディセーブルにできます。そのデバイスとは、グレースフルフェールオーバーのデフォルトが、ディセーブルにされたポートがダウンになるための時間を遅らせる可能性がある、または、ピアからのトラフィックを喪失する原因にもなるデバイスです。ダウンストリーム アクセス スイッチが Cisco Nexus デバイスでない場合は、LACP グレースフル コンバージェンス オプションをディセーブルにします。



(注) このコマンドを使用する前に、ポートチャネルが管理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**

LACP グレースフルコンバージェンスのディセーブル化

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

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: switch# configure terminal switch(config)#	グローバルコンフィギュレーションモードを開始します。
Step 2	interface port-channel number 例: switch(config)# interface port-channel 1 switch(config-if)#	設定するポートチャネルインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。
Step 3	shutdown 例: switch(config-if) shutdown	ポートチャネルを管理シャットダウンします。
Step 4	no lacp graceful-convergence 例: switch(config-if) # no lacp graceful-convergence	ポートチャネルの LACP グレースフルコンバージェンスをディセーブルにします。
Step 5	no shutdown 例: switch(config-if) no shutdown	ポートチャネルを管理的にアップします。
Step 6	copy running-config startup-config 例: switch(config) # copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

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イネーブル化

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

手順の概要

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

手順

	コマンドまたはアクション	目的
Step 1	configure terminal 例: <pre>switch# configure terminal switch(config)#</pre>	グローバルコンフィギュレーションモードを開始します。
Step 2	interface port-channel <i>number</i> 例: <pre>switch(config)# interface port-channel 1 switch(config-if)#</pre>	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。
Step 3	shutdown 例: <pre>switch(config-if) shutdown</pre>	ポートチャネルを管理シャットダウンします。
Step 4	lacp graceful-convergence 例: <pre>switch(config-if) lacp graceful-convergence</pre>	ポートチャネルの LACP グレースフルコンバージェンスをイネーブルにします。
Step 5	no shutdown 例: <pre>switch(config-if) no shutdown</pre>	ポートチャネルを管理アップします。
Step 6	copy running-config startup-config 例: <pre>switch(config) copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

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
```

ポートチャネル構成の確認

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
show interface port channel<channel-number>	ポートチャネルインターフェイスのステータスを表示します。
show feature	イネーブルにされた機能を表示します。
show resource	システムで現在利用可能なリソースの数を表示します。
show lacp {counters interface type slot/port neighbor port-channel system-identifier}	LACP 情報を表示します。
show port-channel compatibility-parameters	ポートチャネルに追加するためにメンバーポート間で同じにするパラメータを表示します。
show port-channel database [interface port-channel <channel-number>]	1つ以上のポートチャネルインターフェイスの集約状態を表示します。
show port-channel summary	ポートチャネルインターフェイスの概要を表示します。
show port-channel traffic	ポートチャネルのトラフィック統計情報を表示します。
show port-channel usage	使用済みおよび未使用的チャネル番号の範囲を表示します。
show port-channel database	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。
show port-channel load-balance	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クのトリガー

ポートチャネルメンバーシップ整合性チェック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ク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

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

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	switch# show consistency-checker membership port-channels	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

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
<code>switch# show port-channel load-balance forwarding-path interface port-channel port-channel-id vlan vlan-id dst-ip src-ip dst-mac src-mac l4-src-port port-id l4-dst-port port-id ether-type ether-type ip-proto ip-proto</code>	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
14-src-port 0 14-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つのレベルの継承に対応しています。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の設定

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

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

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

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

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

ポートプロファイルをイネーブル化、継承、または変更しようとすると、システムによりチェックポイントが作成されます。ポートプロファイル設定が正常に実行されなかった場合は、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

手順

	コマンドまたはアクション	目的
Step 1	configure terminal	グローバルコンフィギュレーションモードを開始します。
Step 2	port-profile [type {ethernet interface-vlan port-channel}] name	指定されたタイプのインターフェイスのポート プロファイルを作成して命名し、ポート プロファイル コンフィギュレーションモードを開始します。
Step 3	exit	ポート プロファイル コンフィギュレーションモードを終了します。
Step 4	(任意) show port-profile	ポート プロファイル 設定を表示します。

■ 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

	コマンドまたはアクション	目的
Step 5	(任意) copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

手順

	コマンドまたはアクション	目的
Step 1	configure terminal	グローバルコンフィギュレーションモードを開始します。
Step 2	port-profile [type {ethernet interface-vlan port-channel}] name	指定されたポートプロファイルのポートプロファイルコンフィギュレーションモードを開始し、プロファイルの設定を追加または削除します。
Step 3	exit	ポートプロファイルコンフィギュレーションモードを終了します。

	コマンドまたはアクション	目的
Step 4	(任意) show port-profile	ポート プロファイル設定を表示します。
Step 5	(任意) copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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することができます。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**手順**

	コマンドまたはアクション	目的
Step 1	configure terminal	グローバルコンフィギュレーションモードを開始します。
Step 2	interface [ethernet slot/port interface-vlan vlan-id port-channel number]	インターフェイスの範囲を選択します。

■ 特定のポート プロファイルのイネーブル化

	コマンドまたはアクション	目的
Step 3	inherit port-profile name	指定したポート プロファイルを、選択したインターフェイスに割り当てます。
Step 4	exit	ポート プロファイルコンフィギュレーションモードを終了します。
Step 5	(任意) show port-profile	ポート プロファイル設定を表示します。
Step 6	(任意) copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

手順

	コマンドまたはアクション	目的
Step 1	configure terminal	グローバルコンフィギュレーションモードを開始します。
Step 2	port-profile [type {ethernet interface-vlan port-channel}] name	指定されたタイプのインターフェイスのポートプロファイルを作成して命名し、ポートプロファイルコンフィギュレーションモードを開始します。
Step 3	state enabled	そのポートプロファイルをイネーブルにします。
Step 4	exit	ポートプロファイルコンフィギュレーションモードを終了します。
Step 5	(任意) show port-profile	ポートプロファイル設定を表示します。
Step 6	(任意) copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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**

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

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	configure terminal	グローバルコンフィギュレーションモードを開始します。
Step 2	port-profile <i>name</i>	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。
Step 3	inherit port-profile <i>name</i>	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。
Step 4	exit	ポートプロファイルコンフィギュレーションモードを終了します。
Step 5	(任意) show port-profile	ポートプロファイル設定を表示します。
Step 6	(任意) copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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

手順

	コマンドまたはアクション	目的
Step 1	configure terminal	グローバルコンフィギュレーションモードを開始します。
Step 2	interface [ethernet slot/port interface-vlan vlan-id port-channel number]	インターフェイスの範囲を選択します。
Step 3	no inherit port-profile name	指定したポート プロファイルを、選択したインターフェイスから割り当て解除します。
Step 4	exit	ポート プロファイルコンフィギュレーションモードを終了します。
Step 5	(任意) show port-profile	ポート プロファイル設定を表示します。
Step 6	(任意) copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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。

継承されたポートプロファイルの削除

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

手順

	コマンドまたはアクション	目的
Step 1	configure terminal	グローバルコンフィギュレーションモードを開始します。
Step 2	port-profile <i>name</i>	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。
Step 3	no inherit port-profile <i>name</i>	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。
Step 4	exit	ポートプロファイルコンフィギュレーションモードを終了します。
Step 5	(任意) show port-profile	ポートプロファイル設定を表示します。
Step 6	(任意) copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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 7 章

仮想ポート チャネルの設定

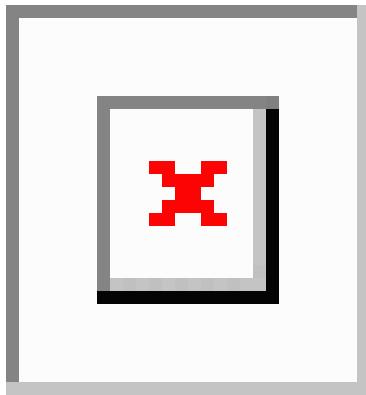
- vPCについて (134 ページ)
- VLANごとの整合性検査 (140 ページ)
- vPC自動リカバリ (140 ページ)
- vPCピアリンク, on page 140
- vPC番号, on page 142
- その他の機能とのvPCの相互作用 (142 ページ)
- vPCフォークリフトアップグレードシナリオ (144 ページ)
- VRFに関する注意事項と制約事項 (147 ページ)
- vPC設定の確認, on page 149
- グレースフルタイプ1検査ステータスの表示 (149 ページ)
- グローバルタイプ1不整合の表示 (150 ページ)
- インターフェイス別タイプ1不整合の表示 (151 ページ)
- VLANごとの整合性ステータスの表示 (152 ページ)
- vPCのデフォルト設定, on page 155
- vPCの設定 (155 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 158
- vPCピアリンクの作成, on page 160
- 設定の互換性の検査 (162 ページ)
- vPC自動リカバリのイネーブル化 (163 ページ)
- 復元遅延時間の設定 (164 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 (165 ページ)
- VRF名の設定 (166 ページ)
- 他のポートチャネルのvPCへの移行, on page 167
- vPCドメインMACアドレスの手動での設定, on page 168
- システムプライオリティの手動での設定, on page 169
- vPCピアスイッチのロールの手動による設定, on page 170
- レイヤ3vPC経由の設定 (172 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のデバイスからは单一のポートチャネルとして認識されるようになります（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ネットワーキング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 6: 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ル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 ドメイン内にあってダウンストリームデバイスに接続されているすべての EtherChannel チャネルが含まれます。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 内にあってダウンストリームデバイスに接続されているすべてのポートチャネルが含まれるドメイン。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。

vPC ドメイン

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に送信されます。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。

同じでなければならない設定パラメータ

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
```

Name	Type	Local Value	Peer Value
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	1	nve	nve
lag-id	1	[(fa0, 0-23-4-ee-be-64, 8458, 0, 0), (8000, (8000, f4-4e-5-84-5e-3c, 457, f4-4e-5-84-5e-3c, 457, 0, 0)]	[(fa0, 0-23-4-ee-be-64, 8458, 0, 0), (8000, f4-4e-5-84-5e-3c, 457, 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つことが必要です。

- 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 トラフィックのタギング
- 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ます、さらにそれらの管理モードおよび動作モード

VLANごとの整合性検査

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イ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
 - プライオリティ
 - 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、またはトライ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 ではキープアライブが 3 回連続して検出されないを待ってから 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プアライブ リンクを設定しておく必要があります。設定しておかないと、ピア リンクは機能しません

vPC ピア 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。

vPC 番号

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 (CFSoE) 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、CFSoE 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。ダウント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 と同じ 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 番号を割り当てる也可以です (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 (CFSoE) 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シナリオ

次に、vPC トポジ内 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（現在動作可能なプライマリ）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、稼働中のデバイスがリロードされたデバイスに勝ちます。したがって、vPCプライマリはvPCの動作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

遅延復元タイマーは、ピア隣接が既に確立されている場合、リロードの後で復元済みの vPC ピア デバイスで起動する vPC の遅延のために使用されます。

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 コマンドを使用します。

- **vPC 自動リカバリ**

両方のvPCピアスイッチがダウンしたデータセンターの停電中に、1つ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。

	移行ステップ	予想される動作	Node1 Configured role (Ex: role priority 100)	Node1 動作のロール	Node2 Configured role (Ex: role priority 200)	Node2 動作のロール
1	初期状態です。	トラフィックは vPC ピア (Node1 と Node2) の両方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 ステイツ キービット: False	セカンダリ	セカンダリ ステイツ キービット: False
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 ステイツ キービット: False	セカンダリ	セカンダリ ステイツ 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 ステイツ キービット: False	適用対象外	適用対象外

■ vPC フォークリフト アップグレードシナリオ

	移行ステップ	予想される動作	Node1 Configured role (Ex: role priority 100)	Node1 動作 のロール	Node2 Configured role (Ex: role priority 200)	Node2 動作 のロール
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。管理アップ状態のvPCピアリンクおよびピアキープアライブ。 New_Node2の電源をオフにします。 すべての接続を確立します。 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。 トライフィックはNode01で引き続き転送されます。	プライマリ	プライマリ スティックービット: False	セカンダリ	セカンダリ スティックービット: False
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。	トライフィックは、ノード1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 スティックービット: False	セカンダリ	セカンダリ スティックービット: 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。	トライフィックはNew_Node2に収束します。	プライマリ	プライマリ スティックービット: False	セカンダリ	セカンダリ スティックービット: False
7	Node1を削除します。	New_Node2がセカンダリになり、プライマリが動作し、スティックービットがTrueに設定されます。	適用対象外	適用対象外	セカンダリ	プライマリ スティックービット: True

	移行ステップ	予想される動作	Node1 Configured role (Ex: role priority 100)	Node1 動作のロール	Node2 Configured role (Ex: role priority 200)	Node2 動作のロール
8	New_Node1を設定します。スタートアップ実行をコピーします。 新しいNode1の電源をオフにします。 すべての接続を確立します。 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 ステイックービット: False	セカンダリ	プライマリ ステイックービット: True
9	New_Node1のすべてのvPCとリンクポートを起動します。	トライフィックは、新しいノード1と新しいノード2の両方によって転送されます。	プライマリ	セカンダリ ステイックービット: False	セカンダリ	プライマリ ステイックービット: True



(注) 設定済みのセカンダリノードを動作可能なセカンダリとして設定し、設定済みのプライマリを動作可能な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。これオプションであり、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。

VRFに関する注意事項と制約事項

- システムにおいて vPC ピアリンクを構成するためには、その前にピアキープ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リンクがピアキープ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 ピアキープ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 ミスペケットが含まれます。ピアキープ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 ピアキープ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 ピアキープアライブに使用される場合は、次の ACL を設定して vPC ピアキープ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 がキープ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# show feature	vPC がイネーブルかどうかを表示します。
switch# show port-channel capacity	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# show running-config vpc	vPC の実行コンフィギュレーションの情報を表示します。
switch# show vpc brief	vPC に関する簡単な情報を表示します。
switch# show vpc consistency-parameters	すべての vPC インターフェイス全体で一貫している必要があるパラメータのステータスを表示します。
switch# show vpc peer-keepalive	ピアキープアライブ メッセージの情報を表示します。
switch# show vpc role	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 スイッチの MAC アドレスとプライオリティを表示します。
switch# show vpc statistics	vPC に関する統計情報を表示します。 Note 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
```

■ グローバルタイプ1不整合の表示

```

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

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

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

```

インターフェイス別タイプ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
-- -- --

```

VLANごとの整合性ステータスの表示

```

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
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 1-10

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

```

VLANごとの整合性ステータスの表示

```
--  -----
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 ごとの整合性ステータスを 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			
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 11: デフォルト vPC パラメータ

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

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。

vPC のディセーブル化

	Command or Action	Purpose
Step 2	switch(config)# feature vpc	スイッチで vPC をイネーブルにします。
Step 3	(Optional) switch# show feature	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。
Step 4	(Optional) switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# no feature vpc	スイッチで vPC をディセーブルにします。
Step 3	(Optional) switch# show feature	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。
Step 4	(Optional) switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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 機能が有効なことを確認します。

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# vpc domain domain-id	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。 Note 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、 vpc domain コマンドを使用することもできます。
Step 3	(Optional) switch# show vpc brief	各 vPC ドメインに関する要約情報を表示します。
Step 4	(Optional) switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

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に送信します。これらのメッセージを送信するには、ピアデバイス間にレイヤ 3 接続が必要です。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 機能が有効なことを確認します。

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# vpc domain domain-id	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。
Step 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}]	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。 Note 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。
Step 4	(Optional) switch(config-vpc-domain)# vpc peer-keepalive destination ipaddress source ipaddress	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。
Step 5	(Optional) switch# show vpc peer-keepalive	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。
Step 6	(Optional) switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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
```

vPC ピアリンクの作成

```
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

```
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 for          : peer is alive
  --Send status                : (154477) seconds, (908) msec
  --Last send at              : Success
  --Sent on interface         : 2011.01.14 19:02:50 100 ms
  --Receive status            : Vlan123
  --Last receive at          : 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 機能が有効なことを確認します。

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface port-channel <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。
Step 3	switch(config-if)# vpc peer-link	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。
Step 4	(Optional) switch# show vpc brief	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。
Step 5	(Optional) switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

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-channelchannel-number}**

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	switch# show vpc consistency-parameters{global interface port-channelchannel-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
      Type 2 : vPC will be continued even if mismatch occurs
      Name      Type  Local Value      Peer Value
      -----
      QoS          2      ([], [], [], [], [],      ([], [], [], [], [],
                           [])                                     [])
      Network QoS (MTU)    2      (1538, 0, 0, 0, 0, 0)  (1538, 0, 0, 0, 0, 0)
      Network Qos (Pause)  2      (F, F, F, F, F, F)   (1538, 0, 0, 0, 0, 0)
      Input Queuing (Bandwidth) 2      (100, 0, 0, 0, 0, 0)  (100, 0, 0, 0, 0, 0)
      Input Queuing (Absolute Priority) 2      (F, F, F, F, F, F)  (100, 0, 0, 0, 0, 0)
      Output Queuing (Bandwidth) 2      (100, 0, 0, 0, 0, 0)  (100, 0, 0, 0, 0, 0)
      Output Queuing (Absolute Priority) 2      (F, F, F, F, F, F)  (100, 0, 0, 0, 0, 0)
```

```

STP Mode           1   Rapid-PVST          Rapid-PVST
STP Disabled       1   None                None
STP MST Region Name 1   ""                 ""
STP MST Region Revision 1   0                  0
STP MST Region Instance to 1
    VLAN Mapping

STP Loopguard      1   Disabled            Disabled
STP Bridge Assurance 1   Enabled             Enabled
STP Port Type, Edge 1   Normal, Disabled, Normal, Disabled,
BPDUFilter, Edge BPDUGuard 1   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

手順

	コマンドまたはアクション	目的
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# vpc domain domain-id	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。
Step 3	switch(config-vpc-domain)# auto-recovery reload-delay delay	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

```

復元遅延時間の設定

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 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

手順

	コマンドまたはアクション	目的
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# vpc domain domain-id	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。
Step 3	switch(config-vpc-domain)# delay restore time	vPC が復元されるまでの遅延時間を設定します。

	コマンドまたはアクション	目的
		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。
Step 4	(任意) switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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**手順**

	コマンドまたはアクション	目的
Step 1	switch# configure terminal	グローバル構成モードを開始します。

■ VRF名の設定

	コマンドまたはアクション	目的
Step 2	switch(config)# vpc domain domain-id	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。
Step 3	switch(config-vpc-domain))# dual-active exclude interface-vlan range	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

手順

	コマンドまたはアクション	目的
Step 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**Procedure**

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface port-channel <i>channel-number</i>	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。 Note 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

vPC ドメイン MAC アドレスの手動での設定

	Command or Action	Purpose
		イースト（ホストインターフェイスのvPCトポロジ）で設定できます。
Step 3	switch(config-if)# vpc <i>number</i>	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。
Step 4	(Optional) switch# show vpc brief	各vPCに関する情報を表示します。
Step 5	(Optional) switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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機能が有効なことを確認します。

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# vpc domain domain-id	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。
Step 3	switch(config-vpc-domain)# system-mac mac-address	指定したvPC ドメインに割り当てるMAC アドレスをaaaa.bbbb.cccc の形式で入力します。
Step 4	(Optional) switch# show vpc role	vPC システムの MAC アドレスを表示します。
Step 5	(Optional) switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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 機能が有効なことを確認します。

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。

vPC ピアスイッチのロールの手動による設定

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# vpc domain domain-id	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。
Step 3	switch(config-vpc-domain)# system-priority priority	指定した vPC ドメインに割り当てるシステムプライオリティを入力します。指定できる値の範囲は、1 ~ 65535 です。デフォルト値は 32667 です。
Step 4	(Optional) switch# show vpc brief	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。
Step 5	(Optional) switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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プションをサポートしていません。プライマリ vPC ピアスイッチに障害が発生すると、セカンダリ vPC ピアスイッチが、vPC プライマリ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 機能が有効なことを確認します。

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# vpc domain domain-id	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。
Step 3	switch(config-vpc-domain)# role priority priority	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。
Step 4	(Optional) switch# show vpc brief	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。
Step 5	(Optional) switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

Example

次の例は、vPC ピアリンクを設定する方法を示します。

■ レイヤ3vPC 経由の設定

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-if)# role priority 4000
```

レイヤ3vPC 経由の設定

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

手順

	コマンドまたはアクション	目的
Step 1	switch# configure terminal 例: switch# configure terminal switch(config) #	グローバル構成モードを開始します。
Step 2	switch(config)# vpc domain domain-id 例: switch(config) # vpc domain 5 switch(config-vpc-domain) #	vPCドメインがまだ存在しなかった場合はそれを作成し、vpc-domainコンフィギュレーションモードを開始します。デフォルトはありません。指定できる範囲は<1～1000>です。
Step 3	switch(config-vpc-domain)# layer3 peer-router	両方のピアとのピアリング隣接関係を形成するためレイヤ3デバイスを有効にします。 (注)

	コマンドまたはアクション	目的
		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。
Step 4	switch(config-vpc-domain)# exit	vpc-domain コンフィギュレーションモードを終了します。
Step 5	(任意) switch# show vpc brief	各 vPC ドメインに関する要約情報を表示します。
Step 6	(任意) switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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)#

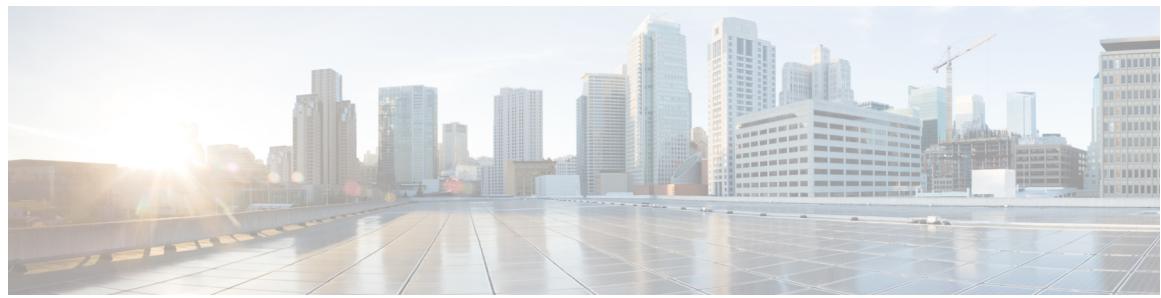
```

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
```

■ レイヤ3vPC 経由の設定



INDEX

イーサネットインターフェイス **58**
 インターフェイスの速度 **58**
インターフェイス **26–27, 55–56, 69, 73–74, 78–79, 81, 83, 91, 93**
 loopback **73, 81**
 tunnel **74**
 UDLD **56**
 VLAN **79**
 構成 **79**
 VRFへの割り当て **83**
 オプション **55**
 シャーシID **55**
 ルーティング **69**
 レイヤ3 **69, 91, 93**
 monitoring **91**
 設定例 **93**
 帯域幅の設定 **78**
 インターフェイスMACアドレス、設定 **84**
 インターフェイスでのDHCPクライアントの設定 **89**
 インターフェイスの速度 **58**
 イーサネットインターフェイス **58**
 インターフェイス情報、表示 **65**
 レイヤ2 **65**
サブインターフェイス **70, 77–78**
 帯域幅の設定 **78**
 構成 **77**
シャットダウン **6, 22, 31–32, 118–119**
ダウンリンク遅延 **64**
チャネルモード **102, 110**
 ポートチャネル **102, 110**
デバウンスタイマー **62**
 parameters **62**
デフォルトインターフェイス **62**
デフォルト設定 **75**
 レイヤ3インターフェイス **75**
トンネルインターフェイス **74**
パラメータ、概要 **62**
 デバウンスタイマー **62**
ポートチャネリング **96**
ポートチャネル **78, 95, 97, 99, 101, 104, 106–108, 110, 120, 167**
 LACP **101**
 LACPがイネーブルとスタティック **104**

ポートチャネル(*continued*)
 STP **95**
 vPCへの移行 **167**
 チャネルモード **110**
 ポートの追加 **107**
 ロードバランシング **99, 108**
 ポートチャネル **99**
 互換性要件 **97**
 作成 **106**
 帯域幅の設定 **78**
 設定の確認 **120**
 ポートチャネル、MinLink **104, 112**
 LACP **104, 112**
 ポートの追加 **107**
 ポートチャネル **107**
 ルーティングインターフェイス **69, 75, 78**
 帯域幅の設定 **78**
 構成 **75**
 ループバックインターフェイス **73, 81**
 構成 **81**
 レイヤ2 **59, 65**
 SVI自動ステート **59**
 インターフェイス情報、表示 **65**
 レイヤ3インターフェイス **69, 75, 90–91, 93–94**
 インターフェイス **94**
 レイヤ3 **94**
 関連資料 **94**
 デフォルト設定 **75**
 モニタリング **91**
 ルーティングインターフェイスの設定 **75**
 確認 **90**
 設定例 **93**
 関連資料 **94**
 ロードバランシング **108**
 ポートチャネル **108**
 構成 **108**
 単方向リンク検出 **56**
 対称ハッシュ化 **100**
 構成 **75, 77–79, 81, 114, 116**
 LACPポートプライオリティ **116**
 LACP高速タイマーレート **114**

構成 (*continued*)

VLAN インターフェイス **79**
 インターフェイス帯域幅 **78**
 サブインターフェイス **77**
 ルーティングインターフェイス **75**
 ループバックインターフェイス **81**

無効化 **156**vPC **156**物理イーサネットの設定 **64**確認 **90**レイヤ3インターフェイス設定 **90**設定: **90**レイヤ3インターフェイス **90**確認 **90**設定例 **93**レイヤ3インターフェイス **93**関連資料 **94**レイヤ3インターフェイス **94****B**

bandwidth **28, 78**
 設定 **78**

C

clear counters interface **52–53**
 copy **16–17**

D

delay **29–30**
 delay restore **145**
 description **17–18**

E

errdisable detect cause **6, 22**
 errdisable detect cause acl-exception **22**
 errdisable detect cause link-flap **22**
 errdisable detect cause loopback **22**
 errdisable detect cause all **22**
 errdisable recovery cause **6, 21**
 errdisable recovery cause all **21**
 errdisable recovery cause bpduguard **21**
 errdisable recovery cause failed-port-state **21**
 errdisable recovery cause link-flap **21**
 errdisable recovery cause loopback **21**
 errdisable recovery cause miscabling **21**
 errdisable recovery cause psecure-violation **21**
 errdisable recovery cause security-violation **21**
 errdisable recovery cause storm-control **21**
 errdisable recovery cause udld **21**

errdisable recovery cause vpc-peerlink **21**
 errdisable recovery interval **6, 23–24**
 ethernet **18**

Ffeature eigrp **31****I**

interface **17–18, 31**
 interface ether **51**
 interface ethernet **19–20, 28–30, 33, 35, 37**
 interface port-channel **113–114, 117–119**
 interfaces **71**
 VLAN **71**
 interfaces-vlan **145**

L

LACP **96, 101, 104, 109, 112**
 システム ID **101**
 ポートチャネル **101**
 ポートチャネル、MinLink **104, 112**
 マーカー レスポンダ **104**
 設定 **109**
 lacp graceful-convergence **119**
 lacp max-bundle **113–114**
 LACP がイネーブルとスタティック **104**
 ポートチャネル **104**
 LACP の設定 **109**
 LACP ポートプライオリティ **116**
 設定 **116**
 LACP 高速タイマー レート **114**
 設定 **114**
 Link Aggregation Control Protocol **96**
 link debounce time **37**
 load-interval counters **51–52**

M

mgmt0 **18**
 monitoring **91**
 レイヤ3インターフェイス **91**
 mtu **27**

N

negotiate auto **14, 48–50**
 negotiate auto 25000 **48**

S

SFP+ トランシーバ **58**
show cdp all **50**
show interface **17–18, 31–32, 46–47, 50–53**
show interface brief **50**
show interface eth **19**
show interface ethernet **19–20, 28–30**
show interface status err-disabled **6, 21–24, 50**
show interface transceivers **13**
show running-config interface port-channel **113–114**
show udld **33, 35, 51**
show udld global **51**
Small Form-Factor Pluggable（プラス）トランシーバ **58**
speed auto **14**
STP **95**
 ポート チャネル **95**
SVI 自動ステート **59**
 レイヤ2 **59**
SVI 自動ステートのディセーブル化 **75**
SVI 自動ステートの無効化の設定 **88**
switchport **14**
system jumbomtu **26–27**

U

udld **33, 35**
UDLD **56–57**
 アグレッシブモード **57**
 定義 **56**
 非アグレッシブ モード **57**
udld aggressive **33–34**
udld message-time **33–34**

V

VLAN **71**
 interfaces **71**
VLAN インターフェイス **79**
 構成 **79**
vPC **167**
 ポート チャネルの移行 **167**
vPC の用語 **135**
VRF **83**
 インターフェイスの割り当て **83**

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。