



マニュアルに関するご意見は nexus9k-docfeedback@cisco.com まで電子メールでお知らせください。



Cisco Nexus 9000 シリーズ NX-OS インターフェイス コンフィギュレーション ガイド リリース 6.x

14/06/17

Cisco Systems, Inc.

www.cisco.com

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

**【注意】 シスコ製品をご使用になる前に、安全上の注意
(www.cisco.com/jp/go/safety_warning/) をご確認ください。**

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

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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

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

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

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

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

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.(<http://www.openssl.org/>)

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

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

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

Cisco Nexus 9000 シリーズ NX-OS インターフェイス コンフィギュレーション ガイド リリース 6.x
© 2014 Cisco Systems, Inc. All rights reserved.



新機能および変更された機能に関する情報 -xi

はじめに xiii

対象読者 xiii

表記法 xiii

関連資料 xiv

マニュアルに関するフィードバック xv

マニュアルの入手方法およびテクニカル サポート xv

第 1 章

概要 1-1

インターフェイスについて 1-1

イーサネット インターフェイス 1-2

管理インターフェイス 1-2

ポートチャネル インターフェイス 1-2

サブインターフェイス 1-3

ループバック インターフェイス 1-3

ブレイクアウト インターフェイス 1-3

仮想デバイス コンテキスト 1-3

インターフェイスのハイアベイラビリティ 1-3

第 2 章

基本インターフェイス パラメータの設定 2-1

基本インターフェイス パラメータについて 2-1

説明 2-2

ビーコン 2-2

Error Disabled 2-2

インターフェイス ステータス エラー ポリシー 2-2

ポート MTU サイズ 2-3

帯域幅 2-3

スループット遅延 2-4

管理ステータス 2-4

UDLD パラメータ 2-4

ポート チャネル パラメータ 2-6

ライセンス要件 2-7

注意事項と制約事項 2-7

Cisco QSFP+ to SFP+ アダプタ モジュールのサポート	2-8
デフォルト設定	2-8
基本インターフェイスパラメータの設定	2-9
設定するインターフェイスの指定	2-10
説明の設定	2-11
ビーコンモードの設定	2-13
Error-Disabled ステータスの設定	2-14
MTU サイズの設定	2-17
帯域幅の設定	2-20
スループット遅延の設定	2-21
インターフェイスのシャットダウンおよび再開	2-23
UDLD モードの設定	2-24
基本インターフェイスパラメータの確認	2-27
インターフェイスカウンタのモニタリング	2-27
インターフェイス統計情報の表示	2-27
インターフェイスカウンタのクリア	2-29

第 3 章

レイヤ2 インターフェイスの設定	3-1
アクセス インターフェイスとトランク インターフェイスについて	3-2
アクセス インターフェイスとトランク インターフェイスについて	3-2
IEEE 802.1Q カプセル化	3-4
アクセス VLAN	3-4
トランクポートのネイティブ VLAN ID	3-5
ネイティブ VLAN トラフィックのタグging	3-5
Allowed VLANs	3-5
デフォルト インターフェイス	3-6
スイッチ仮想インターフェイスおよび自動ステータス動作	3-6
ハイアベイラビリティ	3-7
仮想化のサポート	3-7
レイヤ2 ポート モードのライセンス要件	3-7
ライセンス2 インターフェイスの前提条件	3-7
レイヤ2 インターフェイスの注意事項および制約事項	3-8
レイヤ2 インターフェイスのデフォルト設定	3-9
アクセス インターフェイスとトランク インターフェイスの設定	3-9
アクセスおよびトランク インターフェイスの設定に関する注意事項	3-10
レイヤ2 アクセスポートとしての VLAN インターフェイスの設定	3-10
アクセス ホストポートの設定	3-12
トランクポートの設定	3-14

802.1Q トランク ポートのネイティブ VLAN の設定	3-15
トランキング ポートの許可 VLAN の設定	3-17
デフォルト インターフェイスの設定	3-19
SVI 自動ステート除外の設定	3-21
システムの SVI 自動ステートのディセーブル化の設定	3-23
SVI 単位の SVI 自動ステートのディセーブル化の設定	3-24
ネイティブ VLAN トラフィックにタグを付けるためのデバイス設定	3-26
システムのデフォルト ポート モードをレイヤ 2 に変更	3-28
インターフェイス コンフィギュレーションの確認	3-29
レイヤ 2 インターフェイスのモニタリング	3-30
アクセス ポートおよびトランク ポートの設定例	3-30
その他の参考資料	3-31
関連資料	3-31
標準	3-31
管理情報ベース (MIB)	3-31

第 4 章

レイヤ 3 インターフェイスの設定	4-1
レイヤ 3 インターフェイスについて	4-1
ルーテッド インターフェイス	4-2
サブインターフェイス	4-2
VLAN インターフェイス	4-3
ループバック インターフェイス	4-4
ハイ アベイラビリティ	4-4
仮想化のサポート	4-4
レイヤ 3 インターフェイスのライセンス要件	4-5
ライセンス 3 インターフェイスの前提条件	4-5
注意事項と制約事項	4-5
デフォルト設定値	4-5
レイヤ 3 インターフェイスの設定	4-6
ルーテッド インターフェイスの設定	4-6
サブインターフェイスの設定	4-8
インターフェイスでの帯域幅の設定	4-10
VLAN インターフェイスの設定	4-11
ループバック インターフェイスの設定	4-12
VRF へのインターフェイスの割り当て	4-13
レイヤ 3 インターフェイス設定の確認	4-15
レイヤ 3 インターフェイスのモニタリング	4-16
レイヤ 3 インターフェイスの設定例	4-17

関連項目	4-17
その他の参考資料	4-18
関連資料	4-18
管理情報ベース (MIB)	4-18
標準	4-18

双方向フォワーディング検出の設定 5-1

BFD について	5-1
非同期モード	5-2
BFD の障害検出	5-2
分散型動作	5-3
BFD エコー機能	5-3
セキュリティ	5-4
ハイアベイラビリティ	5-4
仮想化のサポート	5-4
BFD のライセンス要件	5-4
BFD の前提条件	5-4
注意事項と制約事項	5-5
デフォルト設定値	5-6
BFD の設定	5-6
設定階層	5-7
BFD 設定のタスクフロー	5-7
BFD 機能のイネーブル化	5-7
グローバルな BFD パラメータの設定	5-8
インターフェイスでの BFD の設定	5-9
ポートチャネルの BFD の設定	5-11
BFD エコー機能の設定	5-12
ルーティングプロトコルに対する BFD サポートの設定	5-14
BFD 相互運用性	5-27
BFD 設定の確認	5-31
BFD のモニタ	5-32
BFD の設定例	5-32
その他の関連資料	5-32
関連資料	5-33
RFC	5-33

第 6 章

ポート チャネルの設定	6-1
ポート チャネルについて	6-1
ポート チャネル	6-2
ポートチャネル インターフェイス	6-3
基本設定	6-4
互換性要件	6-4
ポート チャネルを使ったロード バランシング	6-6
LACP	6-7
仮想化のサポート	6-12
ハイアベイラビリティ	6-12
ポート チャネリングのライセンス要件	6-13
ポート チャネリングの前提条件	6-13
注意事項と制約事項	6-13
デフォルト設定	6-14
ポート チャネルの設定	6-14
ポート チャネルの作成	6-15
レイヤ 2 ポートをポート チャネルに追加	6-17
レイヤ 3 ポートをポート チャネルに追加	6-19
情報目的としての帯域幅および遅延の設定	6-21
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	6-22
ポート チャネルの説明の設定	6-24
ポート チャネル インターフェイスへの速度とデュプレックスの設定	6-25
ポート チャネルを使ったロード バランシングの設定	6-27
LACP のイネーブル化	6-28
LACP ポート チャネル ポート モードの設定	6-29
LACP ポート チャネルの最小リンクの設定	6-30
LACP ポートチャネル MaxBundle の設定	6-31
LACP 高速タイマーレートの設定	6-33
LACP システム プライオリティの設定	6-34
LACP ポート プライオリティの設定	6-35
LACP グレースフル コンバージェンス	6-36
LACP の個別一時停止のディセーブル化	6-38
LACP の個別一時停止の再イネーブル化	6-39
ポート チャネル ハッシュ分散の設定	6-40
ポートチャネル設定の確認	6-42
ポート チャネル インターフェイス コンフィギュレーションのモニタリング	6-43
ポート チャネルの設定例	6-44
その他の関連資料	6-44

関連資料	6-44
標準	6-45
管理情報ベース (MIB)	6-45

第 7 章

vPC の設定 7-1

vPC について	7-1
vPC の概要	7-2
vPC の用語	7-4
vPC ピア リンク	7-6
ピアキープアライブ リンクとメッセージ	7-9
vPC ピア ゲートウェイ	7-11
vPC ドメイン	7-11
vPC トポロジ	7-12
vPC インターフェイスの互換パラメータ	7-14
vPC 番号	7-16
他のポート チャネルの vPC への移行	7-17
単一モジュール上での vPC ピア リンクとコアへのリンクの設定	7-17
その他の機能との vPC の相互作用	7-19
仮想化のサポート	7-26
停電後の vPC リカバリ	7-26
ハイアベイラビリティ	7-27
vPC のライセンス要件	7-27
注意事項と制約事項	7-27
デフォルト設定値	7-29
vPC の設定	7-29
vPC のイネーブル化	7-30
vPC のディセーブル化	7-31
vPC ドメインの作成と vpc-domain モードの開始	7-32
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	7-33
vPC ピア リンクの作成	7-35
vPC ピアゲートウェイの設定	7-36
グレースフル整合性検査の設定	7-37
vPC ピア リンクの設定の互換性チェック	7-38
他のポート チャネルの vPC への移行	7-39
特定の vPC コマンドの自動イネーブル化	7-41
vPC ドメイン MAC アドレスの手動での設定	7-43
システムプライオリティの手動での設定	7-44
vPC ピア デバイス ロールの手動での設定	7-45
シングルモジュール vPC でのトラッキング機能の設定	7-46

停電後のリカバリの設定	7-48
孤立ポートの一時停止の設定	7-52
vPC ピア スイッチの設定	7-53
vPC 設定の確認	7-56
vPC のモニタリング	7-57
vPC の設定例	7-57
その他の参考資料	7-59
関連資料	7-59
標準	7-60
管理情報ベース (MIB)	7-60

付録 A

Cisco NX-OS インターフェイスがサポートする IETF RFC	A-1
IPv6 の RFC	A-1

付録 B

Cisco NX-OS インターフェイスの設定制限	B-1
----------------------------------	------------



新機能および変更された機能に関する情報

この章では、『Cisco Nexus 9000 シリーズNX-OS インターフェイス コンフィギュレーション ガイド』の新機能および変更された機能に関するリリース固有の情報を示します。

次の表では、『Cisco Nexus 9000 シリーズNX-OS インターフェイス コンフィギュレーション ガイド』における新機能および変更された機能を要約し、その参照先を示しています。

表 1 **新機能および変更された機能**

機能	説明	変更されたリリース	参照先
FEX サポート	Cisco Nexus 2000 Fabric Extender (FEX) サポートが追加されました。	6.1(2)I2(3)	第 7 章「vPC の設定」
Cisco QSFP+ to SFP+ Adapter (QSA) モジュール	40G から 10G への変換をサポートするために Cisco QSFP+ to SFP+ Adapter (QSA) モジュール機能が追加されました。	6.1(2)I2(2)	第 2 章「基本インターフェイスパラメータの設定」



はじめに

ここでは、『Cisco Nexus 9000 Series NX-OS インターフェイス コンフィギュレーション ガイド リリース 6.x』の対象読者、構成、および表記法について説明します。関連情報の取得方法も紹介します。

この前書きは、次の項で構成されています。

- 「対象読者」(P.xiii)
- 「表記法」(P.xiii)
- 「関連資料」(P.xiv)
- 「マニュアルに関するフィードバック」(P.xv)
- 「マニュアルの入手方法およびテクニカル サポート」(P.xv)

対象読者

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

表記法

コマンドの説明では、次の表記法を使用しています。

表記法	説明
太字フォント	コマンドおよびキーワードは太字で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で表記されています。
[]	角カッコの中の要素は、省略可能です。
[x y z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

出力例では、次の表記法を使用しています。

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

このマニュアルでは、次の表記法を使用しています。



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



注意

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

関連資料

完全な Cisco NX-OS 9000 シリーズ マニュアル セットは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.html

リリース ノート

リリース ノートは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps13386/prod_release_notes_list.html.

コンフィギュレーション ガイド

これらのマニュアルは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps13386/products_installation_and_configuration_guides_list.html

このカテゴリのマニュアルには、次が含まれます。

『Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide』

『Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide』

『Cisco Nexus 9000 シリーズ NX-OS インターフェイス コンフィギュレーション ガイド』

『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』

『Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide』

『Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide』
『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』
『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』
『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』
『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』
『Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide』

その他のソフトウェアのマニュアル

『Cisco Nexus 7000 Series and 9000 Series NX-OS MIB Quick Reference』
『Cisco Nexus 9000 Series NX-OS Programmability Guide』
『Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide』
『Cisco Nexus 9000 Series NX-OS System Messages Reference』
『Cisco Nexus 9000 Series NX-OS Troubleshooting Guide』
『Cisco NX-OS Licensing Guide』
『Cisco NX-OS XML Interface User Guide』

マニュアルに関するフィードバック

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

マニュアルの入手方法およびテクニカル サポート

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

『What's New in Cisco Product Documentation』では、シスコの新規および改訂版の技術マニュアルの一覧を RSS フィードとして購読できます。また、リーダー アプリケーションを使用して、コンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。





概要

この章では、Cisco NX-OS ソフトウェアでサポートするインターフェイス タイプの概要を説明します。

この章は、次の項で構成されています。

- 「インターフェイスについて」 (P.1-1)
- 「仮想デバイス コンテキスト」 (P.1-3)
- 「インターフェイスのハイ アベイラビリティ」 (P.1-3)

インターフェイスについて

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

表 1-1 に、インターフェイスに設定できるパラメータの情報の入手先を示します。

表 1-1 インターフェイスのパラメータ

機能	パラメータ	解説場所
基本パラメータ	説明、デュプレックス、エラー ディセーブル、フロー制御、MTU、ビーコン	第 2 章「基本インターフェイス パラメータの設定」
レイヤ 3	メディア、IPv4 および IPv6 アドレス	第 4 章「レイヤ 3 インターフェイスの設定」
	帯域幅、遅延、IP ルーティング、VRF	『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』 『Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide』
ポート チャネル	チャネル グループ、LACP	第 6 章「ポート チャネルの設定」
セキュリティ	EOU	『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』

この項では、次のトピックについて取り上げます。

- 「イーサネット インターフェイス」 (P.1-2)
- 「管理インターフェイス」 (P.1-2)
- 「ポートチャネル インターフェイス」 (P.1-2)
- 「サブインターフェイス」 (P.1-3)
- 「ループバック インターフェイス」 (P.1-3)
- 「ブレイクアウト インターフェイス」 (P.1-3)

イーサネット インターフェイス

イーサネット インターフェイスには、ルーテッド ポートが含まれます。

この項では、次のトピックについて取り上げます。

- 「ルーテッド ポート」 (P.1-2)
- 「アクセス ポート」 (P.1-2)

アクセス ポート

アクセス ポートは1つの VLAN のトラフィックを送受信します。このポートのタイプはレイヤ 2 インターフェイスだけです。アクセスポート インターフェイスの詳細については、「[アクセス インターフェイスとトランク インターフェイスについて](#)」 (P.3-2) を参照してください。

ルーテッド ポート

ルーテッド ポートは、IP トラフィックを他のデバイスにルーティングできる物理ポートです。ルーテッド ポートはレイヤ 3 インターフェイスだけです。ルーテッド ポートの詳細については、「[ルーテッド インターフェイス](#)」 (P.4-2) を参照してください。

管理インターフェイス

管理イーサネット インターフェイスを使用して、Telnet クライアント、簡易ネットワーク管理プロトコル (SNMP)、その他の管理エージェントを使用するリモート管理用ネットワークにデバイスを接続できます。管理ポート (mgmt0) は、自動検知であり、10/100/1000 Mb/s の速度の全二重モードで動作します。

管理インターフェイスの詳細については、『*Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide*』を参照してください。このマニュアルにも、管理インターフェイスの IP アドレスとデフォルト IP ルーティング設定に関する情報を記載しています。

ポートチャネル インターフェイス

ポート チャネルは、複数の物理インターフェイスを集約した論理インターフェイスです。最大 32 の物理ポートへの個別リンクを1つのポート チャネルにバンドルして、帯域幅と冗長性を向上させることができます。ポート チャネリングにより、これらの物理インターフェイスチャネルのトラフィックをロード バランスさせることもできます。ポート チャネル インターフェイスの詳細については、[第6章「ポート チャネルの設定」](#)を参照してください。

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かまいません。親インターフェイスはサブインターフェイスによって複数の仮想インターフェイスに分割されます。これらの仮想インターフェイスに IP アドレスやダイナミック ルーティング プロトコルなど固有のレイヤ3 パラメータを割り当てることができます。サブインターフェイスの設定の詳細については、「[サブインターフェイス](#)」(P.4-2) を参照してください。

ループバック インターフェイス

仮想ループバック インターフェイスは、常にアップ状態にあるシングル エンドポイントを持つ仮想インターフェイスです。パケットが仮想ループバック インターフェイスを通じて送信されると、仮想ループバック インターフェイスですぐに受信されます。ループバック インターフェイスは物理インターフェイスをエミュレートします。サブインターフェイスの設定の詳細については、「[ループバック インターフェイス](#)」(P.4-4) を参照してください。

ブレイクアウト インターフェイス

Cisco NX-OS はブレイクアウト インターフェイスをサポートします。ブレイクアウト コマンドは、モジュール レベルで動作し、モジュールの 40G インターフェイスをそれぞれ 4 つの 10G インターフェイスに分割します。コマンドが実行されると、モジュールがリロードされ、インターフェイスの設定は削除されます。

次に、コマンドの例を示します。

```
switch# configure terminal
switch(config)# interface breakout module 1
Module will be reloaded.Are you sure you want to continue(yes/no)?yes
```

no interface breakout module *module_number* コマンドはブレイクアウト設定を取り消します。モジュールのすべてのインターフェイスを 40G モードにし、前の 10G インターフェイスの設定を削除します。

仮想デバイス コンテキスト

Cisco NX-OS では、仮想デバイスをエミュレートするバーチャルデバイス コンテキスト (VDC) に、オペレーティング システムおよびハードウェア リソースを分割できます。Cisco Nexus 9000 シリーズ スイッチは、複数の VDC をサポートしていません。すべてのスイッチ リソースはデフォルト VDC で管理されます。

インターフェイスのハイアベイラビリティ

インターフェイスは、ステートフル再起動とステートレス再起動をサポートします。ステートフル再起動はスーパーバイザ切り替え時に発生します。切り替え後、Cisco NX-OS は実行時の設定を適用します。



基本インターフェイスパラメータの設定

この章では、で管理されるインターフェイスの基本インターフェイスパラメータを設定する方法について説明します。

この章は、次の項で構成されています。

- 「基本インターフェイスパラメータについて」 (P.2-1)
- 「ライセンス要件」 (P.2-7)
- 「注意事項と制約事項」 (P.2-7)
- 「デフォルト設定」 (P.2-8)
- 「基本インターフェイスパラメータの設定」 (P.2-9)
- 「基本インターフェイスパラメータの確認」 (P.2-27)
- 「インターフェイスカウンタのモニタリング」 (P.2-27)



(注)

レイヤ3 インターフェイス (ルーテッド インターフェイス、サブインターフェイス、および ループバック インターフェイス) で独自に使用するパラメータを設定するには、第 4 章「レイヤ 3 インターフェイスの設定」を参照してください。

基本インターフェイスパラメータについて

この項では、次のトピックについて取り上げます。

- 「説明」 (P.2-2)
- 「ビーコン」 (P.2-2)
- 「Error Disabled」 (P.2-2)
- 「インターフェイスステータスエラーポリシー」 (P.2-2)
- 「ポート MTU サイズ」 (P.2-3)
- 「帯域幅」 (P.2-3)
- 「スループット遅延」 (P.2-4)
- 「管理ステータス」 (P.2-4)
- 「UDLD パラメータ」 (P.2-4)
- 「ポートチャネルパラメータ」 (P.2-6)

説明

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

ポート チャネル インターフェイスに説明パラメータを設定する方法については、「[ポート チャネルの説明の設定](#)」(P.6-24)を参照してください。別のインターフェイスにこのパラメータを設定する方法については、「[説明の設定](#)」(P.2-11)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 ステータス LED が緑に点滅し、物理ポートを識別できます。デフォルトでは、このモードはディセーブルです。インターフェイスの物理ポートを識別するには、インターフェイスのビーコンパラメータを有効にします。

ビーコン パラメータの設定手順については、「[ビーコン モードの設定](#)」(P.2-13)を参照してください。

Error Disabled

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

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

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

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

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

原因に対する **error-disabled** 回復をイネーブルにしない場合、そのインターフェイスは **shutdown** コマンドおよび **no shutdown** コマンドが入力されるまで **error-disabled** ステータスのままです。原因に対して回復をイネーブルにすると、そのインターフェイスの **errdisable** ステータスは解消され、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。

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。

ポート MTU サイズ

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

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

レイヤ 3 インターフェイスでは、576 ~ 9216 バイトの MTU サイズを設定できます。



(注)

グローバル LAN ポート MTU サイズは、非デフォルト MTU サイズを設定したレイヤ 3 イーサネット LAN ポートを通じてのトラフィックに適用します。

レイヤ 2 ポートには、システム デフォルト (1500 バイト) またはシステム ジャンボ MTU サイズ (当初は 9216 バイト) のいずれかの MTU サイズを設定できます。



(注)

システム ジャンボ MTU サイズを変更すると、ポートの一部または全部に新しいシステム ジャンボ MTU サイズを指定しない限り、レイヤ 2 ポートは自動的にシステム デフォルト MTU サイズ (1500 バイト) を使用します。

MTU サイズの設定手順については、「[MTU サイズの設定](#)」(P.2-17) を参照してください。

帯域幅

イーサネット ポートには物理層で 1G、10G、または 40G 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 1G、10G、または 40G のまま変わりません。

ポート チャネル インターフェイスに帯域幅パラメータを設定する方法については、「[情報目的としての帯域幅および遅延の設定](#)」(P.6-21) を参照してください。他のインターフェイスに帯域幅パラメータを設定する方法については、「[帯域幅の設定](#)」(P.2-20) 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せんが、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に帯域幅パラメータを設定する方法については、「[情報目的としての帯域幅および遅延の設定](#)」(P.6-21)を参照してください。他のインターフェイスにスループット遅延パラメータを設定する方法については、「[スループット遅延の設定](#)」(P.2-21)を参照してください。

管理ステータス

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

ポートチャネルインターフェイスに管理ステータスパラメータを設定する方法については、「[ポートチャネルインターフェイスのシャットダウンと再起動](#)」(P.6-22)を参照してください。他のインターフェイスに管理ステータスパラメータを設定する方法については、「[インターフェイスのシャットダウンおよび再開](#)」(P.2-23)を参照してください。

UDLD パラメータ

この項では、次のトピックについて取り上げます。

- 「[UDLD の概要](#)」(P.2-4)
- 「[UDLD のデフォルト設定](#)」(P.2-5)
- 「[UDLD アグレッシブモードと非アグレッシブモード](#)」(P.2-6)

UDLD の概要

シスコ独自の単方向リンク検出 (UDLD) プロトコルにより、光ファイバまたは銅線 (カテゴリ5ケーブルなど) イーサネットケーブルを使用して接続されたデバイスで、ケーブルの物理構成をモニタし、単方向リンクの存在を検出することができます。デバイスで単方向リンクが検出されると、UDLD が関係のある LAN ポートをシャットダウンし、ユーザに通知します。単方向リンクは、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、物理的な単方向接続と論理的な単方向接続を防止し、その他のプロトコルの異常動作を防止できます。

リンク上でローカルデバイスから送信されたトラフィックはネイバーで受信されるのに対し、ネイバーから送信されたトラフィックはローカルデバイスで受信されない場合には常に、単方向リンクが発生します。対になったファイバケーブルのうち一方の接続が切断された場合、自動ネゴシエーションがアクティブである限り、そのリンクはアップ状態が維持されなくなります。この場合、論理リンクは不定であり、UDLD は何の処理も行いません。レイヤ1で両方のファイバが正常に動作していれば、UDLD はそれらのファイバが正しく接続しているかどうか

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。

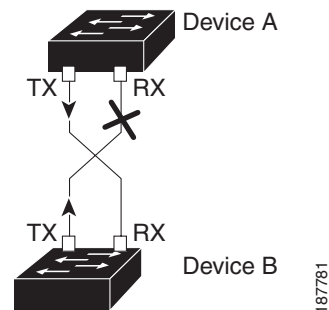
Cisco Nexus 9000 シリーズのデバイスは、UDLD をイネーブルにした LAN ポート上のネイバーデバイスに定期的に UDLD フレームを送信します。一定の時間内にフレームがエコーバックされてきて、特定の確認応答 (echo) が見つからなければ、そのリンクは単方向のフラグを立てられ、その LAN ポートはシャットダウンされます。UDLD プロトコルにより単方向リンクが正しく識別されその使用が禁止されるようにするためには、リンクの両端のデバイスで UDLD がサポートされている必要があります。UDLD フレームの送信間隔は、グローバル単位でも指定されたインターフェイスにも設定できます。



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

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

図 2-1 単方向リンク



UDLD のデフォルト設定

表 2-1 に、UDLD のデフォルト設定を示します。

表 2-1 UDLD のデフォルト設定

機能	デフォルト値
UDLD グローバル イネーブル ステート	グローバルにディセーブル
ポート別の UDLD イネーブル ステート (光ファイバメディア用)	すべてのイーサネット光ファイバ LAN ポートでイネーブル
ポート別の UDLD イネーブル ステート (ツイストペア (銅製) メディア用)	すべてのイーサネット 1G、10G、または 40G LAN ポートでディセーブル
UDLD アグレッシブ モード	ディセーブル
UDLD メッセージの間隔	15 秒

デバイスとそのポートの UDLD を設定する方法については、「UDLD モードの設定」(P.2-24)を参照してください。

UDLD アグレッシブ モードと非アグレッシブ モード

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

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

リンクの一方にポート スタックが生じる（送受信どちらも）

リンクの一方がダウンしているにもかかわらず、リンクのもう一方がアップしたままになる

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



(注)

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



ヒント

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 チャンネルのメンバーで 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 チャンネルパラメータ

ポート チャン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 チャンネルに最大 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 チャンネルの物理インターフェイスが少なくとも 1 つ動作していれば、そのポート チャンネルは動作しています。

レイヤ 3 ポート チャン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 チャンネルを作成できます。

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

ポート チャンネルおよびポート チャンネルの設定手順については、[第 6 章「ポート チャンネルの設定」](#)を参照してください。

ライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	基本インターフェイスパラメータにライセンスは必要ありません。ライセンスパッケージに含まれていない機能は nx-os イメージにバンドルされており、無料で提供されます。Cisco NX-OS のライセンススキームの詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

注意事項と制約事項

基本インターフェイスパラメータの設定には次の注意事項と制約事項があります。

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

デフォルトでは、どのポートもレイヤ3インターフェイスです。

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

- ポーズフレームを使用したフロー制御はサポートされていません。
- 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、表 2-2 (P.2-8) 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的に設定すると、デバイスは自動的にデュプレックスモードを自動的に設定します。
 - no speed** コマンドを開始すると、デバイスは速度およびデュプレックスパラメータの両方を自動的に自動的に設定します (**no speed** コマンドを入力すると、**speed auto** コマンドを入力した場合と同じ結果になります)。
 - イーサネットポート速度を自動以外の値 (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。



(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。

Cisco QSFP+ to SFP+ アダプタ モジュールのサポート

Cisco QSFP+ to SFP+ アダプタ (QSA) モジュールは、Cisco Nexus 9396PX (N9K-C9396PX) および Cisco Nexus 93128TX (N9K-C93128TX) デバイスの Cisco Nexus M12PQ アップリンク モジュールの一部である 40G アップリンク ポートに 10G サポートを提供します。

M12PQ アップリンク モジュールの 6 つの連続するポートは、QSA/QSFP モジュールを使用するために同じ速度 (40G または 10G) で稼動している必要があります。

- Cisco Nexus 9396PX デバイスでは、2/1-6 ポートは最初のポート速度グループを形成し、残りの 2/7-12 ポートが 2 番目のポート速度グループを形成します。
- Cisco Nexus 93128TX デバイスでは、2/1-6 ポートは最初のポート速度グループを形成し、残りの 2/7-8 ポートが 2 番目のポート速度グループを形成します。

speed-group 10000 コマンドを使用して QSA のポート速度グループの最初のポートを設定します。このコマンドは、ポートグループの管理者の速度のプリファレンスを指定します。(デフォルトのポート速度は 40G です)。

- **speed-group 10000** コマンドは 10G の速度を指定します。
- **no speed-group 10000** コマンドは 40G の速度を指定します。

速度を設定すると、互換性のあるトランシーバ モジュールがイネーブルになります。ポートグループ内の残りのトランシーバ モジュール (互換性のないトランシーバ モジュール) は「check speed-group config」として error disabled となります。

QSA の設定例

Cisco Nexus 9396PX :

- ポート 2/1 のデフォルト設定を使用して、ポートグループ 2/1-6 のすべての QSFP は速度 40G になります。ポートグループ 2/1-6 に QSA モジュールがある場合は、error disabled になります。
- **speed-group 10000** コマンドを使用してポート 2/7 を設定し、ポートグループ 2/7-12 内のすべての QSA を 10G の速度にします。ポートグループ 2/7-12 に QSFP モジュールがある場合は、error disabled になります。

デフォルト設定


表 2-2 に、基本インターフェイスパラメータのデフォルト設定を示します。

表 2-2 基本インターフェイスパラメータのデフォルト設定

パラメータ	デフォルト
説明	ブランク
ビーコン	ディセーブル
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

表 2-2 基本インターフェイスパラメータのデフォルト設定 (続き)

パラメータ	デフォルト
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
ポート プロファイル	ディセーブル
バッファ ブースト	イネーブル



(注) N9K-X9564TX および N9K-X9564PX ラインカードおよび Cisco Nexus 9300 シリーズ デバイスで使用可能な機能。

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。

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

- 「設定するインターフェイスの指定」 (P.2-10)
- 「説明の設定」 (P.2-11)
- 「ビーコン モードの設定」 (P.2-13)
- 「Error-Disabled ステートの設定」 (P.2-14)
- 「MTU サイズの設定」 (P.2-17)
- 「帯域幅の設定」 (P.2-20)
- 「スループット遅延の設定」 (P.2-21)
- 「インターフェイスのシャットダウンおよび再開」 (P.2-23)
- 「UDLD モードの設定」 (P.2-24)

設定するインターフェイスの指定

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

表 2-3 に、イーサネット インターフェイスおよび管理インターフェイスを指定するために使用するインターフェイスタイプとIDを示します。

表 2-3 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 の場合)

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

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

次に、連続しているインターフェイス範囲の設定例を示します。

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

次に、不連続なインターフェイス範囲の設定例を示します。

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

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、ブレイクアウト 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

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



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

インターフェイス コンフィギュレーション モードの場合、コマンドを入力するとこのモードに指定したインターフェイスが設定されます。

説明の設定

イーサネットおよび管理インターフェイスの説明を文字で設定します。

手順の概要

1. **configure terminal**
2. **interface interface**
3. **description text**
4. (任意) **show interface interface**
5. **exit**
6. (任意) **copy running-config startup-config**

手順の詳細

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

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

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

show interface eth 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. **{beacon | no beacon}**
4. (任意) **show interface ethernet slot/port**
5. **exit**
6. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface ethernet slot/port 例: switch(config)# interface ethernet 3/1 switch(config-if)#	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	{beacon no beacon} 例: switch(config-if)# beacon switch(config-if)#	ビーコン モードをイネーブルにします。またはビーコン モードをディセーブルにします。デフォルト モードはディセーブルです。
ステップ 4	show interface ethernet slot/port 例: switch(config)# show interface ethernet 2/1	(任意) ビーコン モード ステータスなど、インターフェイスのステータスを表示します。

	コマンド	目的
ステップ 5	exit 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 6	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

次に、イーサネット 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。この項では、次のトピックについて取り上げます。

- 「[Error-Disable 検出のイネーブル化](#)」 (P.2-14)
- 「[errdisable ステート回復のイネーブル化](#)」 (P.2-15)
- 「[errdisable ステート回復間隔の設定](#)」 (P.2-16)

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} shutdown**

3. **no shutdown**
4. (任意) **show interface status err-disabled**
5. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	errdisable detect cause {acl-exception all link-flap loopback} 例: switch(config)# errdisable detect cause all switch(config)#	インターフェイスを error-disabled ステートにする条件を指定します。デフォルトではイネーブルになっています。
ステップ 3	shutdown 例: switch(config)# shutdown switch(config)#	インターフェイスを管理的にダウンさせます。インターフェイスを error-disabled ステートから手動で回復させるには、最初にこのコマンドを入力します。
ステップ 4	no shutdown 例: switch(config)# no shutdown switch(config)#	インターフェイスを管理的にアップし、error-disabled ステートから手動で回復させるインターフェイスをイネーブルにします。
ステップ 5	show interface status err-disabled 例: switch(config)# show interface status err-disabled	(任意) error-disabled インターフェイスに関する情報を表示します。
ステップ 6	copy running-config startup-config 例: switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

errdisable ステート回復のイネーブル化

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

手順の概要

1. **configure terminal**
2. **errdisable recovery cause {all | bpduguard | failed-port-state | link-flap | loopback | miscabling | psecure-violation | security-violation | storm-control | udd | vpc-peerlink}**

■ 基本インターフェイスパラメータの設定

3. (任意) **show interface status err-disabled**
4. (任意) **copy running-config startup-config**

手順の詳細

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

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

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

errdisable ステート回復間隔の設定

error-disabled 回復タイマーの値を設定できます。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	errdisable recovery interval interval 例： switch(config)# errdisable recovery interval 32 switch(config-if)#	インターフェイスが error-disabled ステートから回復する間隔を指定します。有効範囲は 30 ~ 65535 秒で、デフォルトは 300 秒です。
ステップ 3	show interface status err-disabled 例： switch(config)# show interface status err-disabled	(任意) error-disabled インターフェイスに関する情報を表示します。
ステップ 4	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

MTU サイズの設定

レイヤ 2 およびレイヤ 3 イーサネット インターフェイスの最大伝送単位 (MTU) サイズを設定できます。レイヤ 3 インターフェイスでは、576 ~ 9216 バイトの MTU を設定できます (偶数値にする必要があります)。レイヤ 2 インターフェイスでは、システム デフォルト MTU (1500 バイト) またはシステム ジャンボ MTU サイズ (デフォルト サイズは 9216 バイト) の MTU を設定できます。



(注)

システム ジャンボ MTU のサイズを変更できますが、その値を変更すると、その値を使用するレイヤ 2 インターフェイスが新しいシステム ジャンボ MTU 値に自動的に変更します。

デフォルトでは、Cisco NX-OS はレイヤ 3 パラメータを設定します。レイヤ 2 パラメータを設定するには、ポート モードをレイヤ 2 に切り替える必要があります。

switchport コマンドを使用して、ポート モードを変更できます。

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

インターフェイス MTU サイズの設定

レイヤ 3 インターフェイスでは、576 ～ 9216 バイトの MTU サイズを設定できます。

レイヤ 2 インターフェイスでは、すべてのレイヤ 2 インターフェイスをデフォルト MTU サイズ (1500 バイト) またはシステム ジャンボ MTU サイズ (デフォルト サイズは 9216 バイト) を使用するように設定できます。

レイヤ 2 インターフェイスとは異なるシステム ジャンボ MTU サイズを使用する場合は、「[システム ジャンボ MTU サイズの設定](#)」(P.2-19) を参照してください。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface ethernet slot/port 例： switch(config)# interface ethernet 3/1 switch(config-if)#	設定するイーサネット インターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	{switchport no switchport} 例： switch(config-if)# no switchport switch(config-if)#	レイヤ 3 を使用するように指定します。
ステップ 4	mtu size 例： switch(config-if)# mtu 9216 switch(config-if)#	レイヤ 3 インターフェイスでは、576 ～ 9216 の任意の偶数を指定します。
ステップ 5	show interface ethernet slot/port 例： switch(config)# show interface ethernet 2/1	(任意) インターフェイス ステータスを表示します。MTU サイズもあわせて表示します。

	コマンド	目的
ステップ 6	exit 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 7	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、レイヤ 2 イーサネット ポート 3/1 にデフォルト MTU サイズ (1500) を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# switchport
switch(config-if)# mtu 1500
switch(config-if)#
```

システム ジャンボ MTU サイズの設定

システム ジャンボ MTU サイズを設定するとレイヤ 2 インターフェイスの MTU サイズを指定できます。1500 ~ 9216 の偶数を指定できます。システム ジャンボ MTU サイズを設定しない場合、デフォルトは 9216 バイトです。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	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。

■ 基本インターフェイスパラメータの設定

	コマンド	目的
ステップ 3	show running-config all 例： switch(config)# show running-config all include logfile	(任意) 現在の動作設定を表示します。システムジャンボ MTU サイズもあわせて表示します。
ステップ 4	interface type slot/port 例： switch(config)# interface ethernet 2/1 switch(config-if)#	設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	mtu size 例： switch(config-if)# mtu 1500 switch(config-if)#	レイヤ 2 インターフェイスでは、デフォルト MTU サイズ (1500) または以前指定したシステムジャンボ MTU サイズを指定します。 レイヤ 3 インターフェイスでは、576 ~ 9216 の任意の偶数サイズを指定します。
ステップ 6	exit 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 7	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

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

```
switch# configure terminal
switch(config)# system jumbomtu 8000
switch(config)# show running-config
switch(config)# interface ethernet 2/2
switch(config-if)# switchport
switch(config-if)# mtu 4608
switch(config-if)#
```

帯域幅の設定

イーサネット インターフェイスの帯域幅を設定できます。物理層は、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. (任意) **show interface ethernet slot/port**
5. **exit**
6. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface ethernet slot/port 例: switch(config)# interface ethernet 3/1 switch(config-if)#	設定するイーサネット インターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	bandwidth kbps 例: switch(config-if)# bandwidth 1000000 switch(config-if)#	情報用としてのみ 1 ~ 100,000,000 の値を帯域幅に指定します。
ステップ 4	show interface ethernet slot/port 例: switch(config)# show interface ethernet 2/1	(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。
ステップ 5	exit 例: switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 6	copy running-config startup-config 例: switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

スループット遅延の設定

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

手順の概要

1. **configure terminal**
2. **interface ethernet slot/port**
3. **delay value**
4. (任意) **show interface ethernet slot/port**

■ 基本インターフェイスパラメータの設定

5. **exit**
6. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバルコンフィギュレーションモードを開始します。
ステップ 2	interface ethernet slot/port 例: switch(config)# interface ethernet 3/1 switch(config-if)#	設定するインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 3	delay value 例: switch(config-if)# delay 10000 switch(config-if)#	遅延時間を 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。
ステップ 4	show interface ethernet slot/port 例: switch(config)# show interface ethernet 3/1 switch(config-if)#	(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。
ステップ 5	exit 例: switch(config-if)# exit switch(config)#	インターフェイスモードを終了します。
ステップ 6	copy running-config startup-config 例: switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

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

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



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

インターフェイスのシャットダウンおよび再開

イーサネットまたは管理インターフェイスはシャットダウンして再起動できます。インターフェイスはシャットダウンするとディセーブルになり、すべてのモニタ画面にはダウン状態で表示されます。この情報は、すべてのダイナミックルーティングプロトコルを通じて、他のネットワークサーバに伝達されます。シャットダウンしたインターフェイスはどのルーティングアップデートにも含まれません。インターフェイスを再開するには、インターフェ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. (任意) **show interface interface**
5. **no shutdown**
6. (任意) **show interface interface**
7. **exit**
8. (任意) **copy running-config startup-config**

手順の詳細

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

	コマンド	目的
ステップ 3	shutdown 例： switch(config-if)# shutdown switch(config-if)#	インターフェイスをディセーブルにします。
ステップ 4	show interface interface 例： switch(config-if)# show interface ethernet 2/1 switch(config-if)#	(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。
ステップ 5	no shutdown 例： switch(config-if)# no shutdown switch(config-if)#	インターフェイスを再びイネーブルにします。
ステップ 6	show interface interface 例： switch(config-if)# show interface ethernet 2/1 switch(config-if)#	(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。
ステップ 7	exit 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 8	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

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

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

UDLD モードの設定

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 UDLD モードをイネーブルにするには、そのインターフェイスを含むデバイス上で UDLD を事前にイネーブルにしておく必要があります。UDLD は他方のリンク先のインターフェイスおよびそのデバイスでもイネーブルになっている必要があります。

表 2-4 に、異なるインターフェイスで UDLD をイネーブルおよびディセーブルにする CLI 詳細を示します。

表 2-4 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	イネーブル	ディセーブル
enable UDLD コマンド	no udld disable	udld enable
disable UDLD コマンド	udld disable	no udld enable

はじめる前に

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

手順の概要

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

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	feature udld 例: switch(config)# feature udld switch(config)#	デバイスの UDLD をイネーブルにします。
	no feature udld 例: switch(config)# no feature udld switch(config)#	デバイスの UDLD をディセーブルにします。
ステップ 3	udld message-time seconds 例: switch(config)# udld message-time 30 switch(config)#	(任意) UDLD メッセージを送信する間隔を指定します。有効な範囲は 7 ~ 90 秒で、デフォルトは 15 秒です。

■ 基本インターフェイスパラメータの設定

	コマンド	目的
ステップ 4	udld aggressive 例： switch(config)# udld aggressive switch(config)#	(任意) UDLD モードをアグレッシブに指定します。 (注) 銅インターフェイスの場合、UDLD アグレッシブ モードに設定するインターフェイスのインターフェイス コマンド モードを入力し、インターフェイス コマンド モードでこのコマンドを発行します。
ステップ 5	interface ethernet slot/port 例： switch(config)# interface ethernet 3/1 switch(config-if)#	(任意) 設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	udld {enable disable} 例： switch(config-if)# udld enable switch(config-if)#	(任意) 指定した銅線ポートの UDLD をイネーブルにしたり、指定したファイバポートの UDLD をディセーブルにします。 銅線ポートで UDLD をイネーブルにするには、 udld enable コマンドを入力します。ファイバポートで UDLD をイネーブルにするには、 no udld disable コマンドを入力します。詳細については、表 2-4 を参照してください
ステップ 7	show udld [ethernet slot/port global neighbors] 例： switch(config)# show udld switch(config)#	(任意) UDLD のステータスを表示します。
ステップ 8	exit 例： switch(config-if-range)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 9	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、デバイスの UDLD をイネーブルにする例を示します。

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

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

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

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

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

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

次に、デバイスの UDLD をディセーブルにする例を示します。

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

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
<code>show cdp all</code>	CDP ステータスを表示します。
<code>show interface interface</code>	1 つまたはすべてのインターフェイスに設定されている状態を表示します。
<code>show interface brief</code>	インターフェイスの状態表を表示します。
<code>show interface status err-disabled</code>	error-disabled インターフェイスに関する情報を表示します。
<code>show udld interface</code>	現在のインターフェイスまたはすべてのインターフェイスの UDLD ステータスを表示します。
<code>show udld global</code>	現在のデバイスの UDLD ステータスを表示します。
<code>show port-profile</code>	ポート プロファイルに関する情報を表示します。
<code>show system internal pktmgr internal control</code>	pktmgr のコントロール メッセージを表示します。

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。ここでは、次の内容について説明します。

- 「[インターフェイス統計情報の表示](#)」 (P.2-27)
- 「[インターフェイスカウンタのクリア](#)」 (P.2-29)

インターフェイス統計情報の表示

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

手順の概要

1. `configure terminal`
2. `load-interval counters {{1 | 2 | 3} seconds}`

■ インターフェイスカウンタのモニタリング

3. (任意) `show interface interface`
4. `exit`
5. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例: switch# <code>configure terminal</code> switch#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface ether slot/port</code> 例: switch(config)# <code>interface ether 4/1</code> switch(config)#	インターフェイスを指定します。
ステップ 3	<code>load-interval counters {{1 2 3} seconds}</code> 例: switch(config)# <code>load-interval counters 1 100</code> switch(config)#	ビットレートおよびパケットレートの統計情報を収集する最大 3 つのサンプリング間隔を設定します。各カウンタのデフォルト値は、次のとおりです。 1 : 30 秒 (VLAN の場合は 60 秒) 2 : 300 秒 3 : 未設定
ステップ 4	<code>show interface interface</code> 例: switch(config)# <code>show interface ethernet 2/2</code> switch#	(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。
ステップ 5	<code>exit</code> 例: switch(config)# <code>exit</code> switch#	インターフェイス コンフィギュレーション モードを終了します。
ステップ 6	<code>copy running-config startup-config</code> 例: switch# <code>copy running-config startup-config</code>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

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

手順の詳細

	コマンド	目的
ステップ 1	clear counters interface {all ethernet slot/port loopback number mgmt number port channel channel-number} 例： switch# clear counters ethernet 2/1 switch#	インターフェイスカウンタをクリアします。
ステップ 2	show interface interface 例： switch# show interface ethernet 2/1 switch#	(任意) インターフェイスのステータスを表示します。
ステップ 3	show interface [ethernet slot/port port-channel channel-number] counters 例： switch# show interface ethernet 2/1 counters switch#	(任意) インターフェイスカウンタを表示します。

次に、イーサネットポート 5/5 のカウンタをクリアする例を示します。

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

■ インターフェイスカウンタのモニタリング



第 3 章

レイヤ 2 インターフェイスの設定

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



(注) レイヤ 2 ポートは、次のいずれかとして機能できます。

- トランク ポート
- アクセス ポート



(注) レイヤ 2 ポートは、トランク ポートまたはアクセス ポートとして機能することができます。

この章は、次の項で構成されています。

- 「アクセス インターフェイスとトランク インターフェイスについて」 (P.3-2)
- 「レイヤ 2 ポート モードのライセンス要件」 (P.3-7)
- 「ライセンス 2 インターフェイスの前提条件」 (P.3-7)
- 「レイヤ 2 インターフェイスの注意事項および制約事項」 (P.3-8)
- 「レイヤ 2 インターフェイスのデフォルト設定」 (P.3-9)
- 「アクセス インターフェイスとトランク インターフェイスの設定」 (P.3-9)
- 「インターフェイス コンフィギュレーションの確認」 (P.3-29)
- 「レイヤ 2 インターフェイスのモニタリング」 (P.3-30)
- 「アクセス ポートおよびトランク ポートの設定例」 (P.3-30)
- 「その他の参考資料」 (P.3-31)



(注) SPAN 宛先インターフェイスの設定の詳細については、『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』を参照してください。

レイヤ 2 スイッチング ポートをアクセス ポートまたはトランク ポートとして設定できます。トランクは 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張することができます。すべてのレイヤ 2 スイッチング ポートは、メディア アクセス コントロール (MAC) アドレス テーブルを維持します。



(注) VLAN、MAC アドレス テーブル、プライベート VLAN、およびスパンニング ツリー プロトコルの情報に関しては、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。



(注) レイヤ 2 ポートは、トランク ポートまたはアクセス ポートとして機能することができます。

アクセス インターフェイスとトランク インターフェイスについて



(注) ハイ アベイラビリティ機能の詳細については、『Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide』を参照してください。

この項では、次のトピックについて取り上げます。

- 「アクセス インターフェイスとトランク インターフェイスについて」 (P.3-2)
- 「IEEE 802.1Q カプセル化」 (P.3-4)
- 「アクセス VLAN」 (P.3-4)
- 「トランク ポートのネイティブ VLAN ID」 (P.3-5)
- 「ネイティブ VLAN トラフィックのタギング」 (P.3-5)
- 「Allowed VLANs」 (P.3-5)
- 「デフォルト インターフェイス」 (P.3-6)
- 「スイッチ仮想インターフェイスおよび自動ステート動作」 (P.3-6)
- 「レイヤ 2 ポート モードのライセンス要件」 (P.3-7)
- 「ハイ アベイラビリティ」 (P.3-7)
- 「仮想化のサポート」 (P.3-7)



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

アクセス インターフェイスとトランク インターフェイスについて

レイヤ 2 ポートは、アクセスまたはトランク ポートとして次のように設定できます。

- アクセス ポートには VLAN を 1 つだけ設定でき、1 つの VLAN のトラフィックだけを伝送できます。
- トランク ポートには複数の VLAN を設定でき、複数の VLAN のトラフィックを同時に伝送できます。

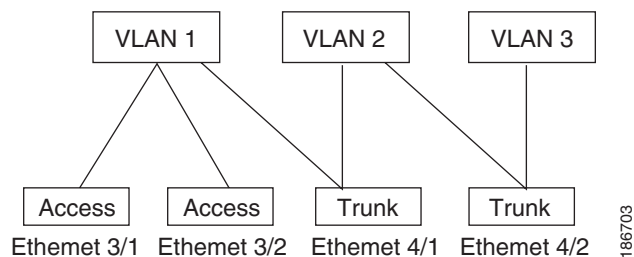
デフォルトでは、デバイスのポートはすべてレイヤ 3 ポートです。

セットアップ スクリプトを使用するか、**system default switchport** コマンドを入力して、すべてのポートをレイヤ 2 ポートにできます。セットアップ スクリプトを使用する詳細については、『Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide, Release 6.x』を参照してください。CLI を使用して、ポートをレイヤ 2 ポートとして設定するには、**switchport** コマンドを使用します。

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

図 3-1 に、ネットワークでトランク ポートを使用する手順を示します。トランク ポートは、2 つ以上の VLAN のトラフィックを伝送します。

図 3-1 トランクおよびアクセス ポートと VLAN トラフィック



(注) VLAN の作成の詳細については、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。

複数の VLAN に接続するトランク ポートのトラフィックを正しく伝送するために、デバイスは IEEE 802.1Q カプセル化 (タグging方式) を使用します (詳細については、「IEEE 802.1Q カプセル化」(P.3-4) を参照してください)。



(注) レイヤ 3 インターフェイス上のサブインターフェイスの詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

アクセス ポートのパフォーマンスを最適化するには、ポートをホスト ポートとして設定します。ホスト ポートとして設定されたポートは、自動的にアクセス ポートとして設定され、チャンネルグループ化はディセーブルになります。ホストを割り当てると、割り当てたポートがパケット転送を開始する時間が短縮されます。

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

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

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

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

IEEE 802.1Q カプセル化



(注) VLAN の詳細については、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。

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

複数の VLAN に接続するトランク ポートのトラフィックを正しく配信するために、デバイスは IEEE 802.1Q カプセル化 (タギング方式) を使用します。この方式では、フレーム ヘッダーに挿入したタグが使用されます (図 3-2 を参照)。このタグには、そのフレームおよびパケットが属する特定の VLAN に関する情報が含まれます。タグ方式を使用すると、複数の異なる VLAN 用にカプセル化されたパケットが、同じポートを通過しても、各 VLAN 間でトラフィック分離を維持できます。また、カプセル化された VLAN タグにより、トランクは同じ VLAN 上のネットワークの端から端までトラフィックを移動させます。

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

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

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

3 bits = User Priority field

1 bit = Canonical Format Identifier (CFI)

12 bits – VLAN Identifier (VLAN ID)

182779

アクセス VLAN

アクセス モードでポートを設定すると、そのインターフェイスのトラフィックを伝送する VLAN を指定できます。アクセス モードのポート (アクセス ポート) 用に VLAN を設定しないと、そのインターフェイスはデフォルトの VLAN (VLAN1) のトラフィックだけを伝送します。

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

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

トランク ポートのネイティブ VLAN ID

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



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

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



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

ネイティブ VLAN トラフィックのタグging

シスコのソフトウェアは、トランク ポートで IEEE 802.1Q 標準をサポートします。タグなしトラフィックがトランク ポートを通過するには、パケットにタグがない VLAN を作成する必要があります（またはデフォルト VLAN を使用することもできます）。タグなしパケットはトランク ポートとアクセス ポートを通過できます。

ただし、デバイスを通過するすべてのパケットに 802.1Q タグがあり、トランクのネイティブ VLAN の値と一致する場合はタグgingが取り除かれ、タグなしパケットとしてトランク ポートから出力されます。トランク ポートのネイティブ VLAN でパケットのタグgingを保持したい場合は、この点が問題になります。

トランク ポートのすべてのタグなしパケットをドロップし、ネイティブ VLAN ID と同じ 802.1Q の値付きでデバイスに届くパケットのタグを保持するようにデバイスを設定できます。この場合も、すべての制御トラフィックはネイティブ VLAN を通過します。この設定はグローバルです。デバイスのトランク ポートは、ネイティブ VLAN のタグgingを保持する場合と保持しない場合があります。

Allowed VLANs

デフォルトでは、トランク ポートはすべての VLAN に対してトラフィックを送受信します。各トランク上では、すべての VLAN ID が許可されます。ただし、この包括的なリストから VLAN を削除すれば、特定の VLAN からのトラフィックが、そのトランクを通過するのを禁止できます。後ほど、トラフィックを伝送するトランクの VLAN を指定してリストに追加し直すこともできます。

デフォルト VLAN のスパニングツリー プロトコル (STP) トポロジを区切るには、許容 VLAN のリストから VLAN1 を削除します。この分割を行わないと、VLAN1 (デフォルトでは、すべてのポートでイネーブル) が非常に大きな STP トポロジを形成し、STP の収束時に問題が発生する可能性があります。VLAN1 を削除すると、そのポート上で VLAN1 のデータトラフィックはすべてブロックされますが、制御トラフィックは通過し続けます。



(注) STP の詳細については、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。



(注) 内部使用に予約されている VLAN のブロックを変更できます。予約 VLAN 変更の詳細については、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。

デフォルト インターフェイス

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



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

スイッチ仮想インターフェイスおよび自動ステート動作

Cisco NX-OS では、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。

このインターフェイスの動作状態は、その対応する VLAN 内のさまざまなポートの状態によって決まります。VLAN の SVI インターフェイスは、その 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稼働します。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。

SVI 自動ステート除外

一般的に、VLAN インターフェイスに複数のポートがある場合、VLAN 内のすべてのポートがダウンすると、SVI はダウン状態になります。SVI 自動ステート除外機能を使用して、SVI が同じ VLAN に属する場合でも、SVI のステータス (アップまたはダウン) を定義すると同時に特定のポートおよびポートチャネルを除外することができます。たとえば、除外されたポートまたはポートチャネルがアップ状態であり、別のポートが VLAN 内でダウン状態である場合でも、SVI 状態はダウンに変更されます。



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

SVI 自動ステートのディセーブル化

デバイスのインバンド管理にも SVI を使用できます。具体的には、自動ステートのディセーブル化機能を設定して、対応する VLAN 内にアップ状態のインターフェイスがない場合でも SVI をアップ状態に保持することができます。この機能は、システム（すべての SVI 向け）または個々の SVI に対し設定できます。

ハイアベイラビリティ

ソフトウェアは、レイヤ2ポートのハイアベイラビリティをサポートします。



(注) ハイアベイラビリティ機能の詳細については、『Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide』を参照してください。

仮想化のサポート

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

レイヤ2ポート モードのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	レイヤ2ポート モードにライセンスは必要ありません。ライセンスパッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。

ライセンス2インターフェイスの前提条件

ライセンス2インターフェイスには次の前提条件があります。

- デバイスにログインしている。
- **switchport mode** コマンドを使用する前に、ポートをレイヤ2ポートとして設定する必要があります。デフォルトでは、Cisco Nexus 9396 および Cisco Nexus 93128 デバイスのすべてのポートはレイヤ3ポートです。デフォルトでは、Cisco Nexus 9504 および Cisco Nexus 9508 デバイスのすべてのポートはレイヤ2ポートです。

レイヤ2 インターフェイスの注意事項および制約事項

VLAN トランキングには次の設定上の注意事項と制限事項があります。

- ポートはレイヤ2 またはレイヤ3 インターフェイスのいずれかです。両方が同時に成立することはありません。
- レイヤ3 ポートをレイヤ2 ポートに変更する場合またはレイヤ2 ポートをレイヤ3 ポートに変更する場合は、レイヤに依存するすべての設定は失われます。アクセスまたはトランク ポートをレイヤ3 ポートに変更すると、アクセス VLAN、ネイティブ VLAN、許容 VLAN などの情報はすべて失われます。
- アクセス リンクを持つデバイスには接続しないでください。アクセス リンクにより VLAN が区分されることがあります。
- 802.1Q トランクを介してシスコ デバイスを接続するときは、802.1Q トランクのネイティブ VLAN がトランク リンクの両端で同じであることを確認してください。トランクの一端のネイティブ VLAN と反対側の端のネイティブ VLAN が異なると、スパニングツリー ループの原因になります。
- ネットワーク上のすべての VLAN についてスパニングツリーをディセーブルにせずに、802.1Q トランクのネイティブ VLAN 上のスパニングツリーをディセーブルにすると、スパニングツリーのループが発生する場合があります。802.1Q トランクのネイティブ VLAN のスパニングツリーはイネーブルのままにしておく必要があります。スパニングツリーをイネーブルにしておけない場合は、ネットワークの各 VLAN のスパニングツリーをディセーブルにする必要があります。スパニングツリーをディセーブルにする前に、ネットワークに物理ループがないことを確認してください。
- 802.1Q トランクを介して2 台のシスコ デバイスを接続すると、トランク上で許容される VLAN ごとにスパニングツリーブリッジプロトコルデータユニット (BPDU) が交換されます。トランクのネイティブ VLAN 上の BPDU は、タグなしの状態です。予約済み IEEE 802.1D スパニングツリー マルチキャスト MAC アドレス (01-80-C2-00-00-00) に送信されます。トランクの他のすべての VLAN 上の BPDU は、タグ付きの状態です。予約済み Cisco Shared Spanning Tree (SSTP) マルチキャスト MAC アドレス (01-00-0c-cc-cc-cd) に送信されます。
- 他社製の 802.1Q デバイスでは、すべての VLAN に対してスパニングツリー トポロジを定義するスパニングツリーのインスタンス (Mono Spanning Tree) が1 つしか維持されません。802.1Q トランクを介してシスコ製のスイッチを他社製のスイッチに接続すると、他社製のスイッチの Mono Spanning Tree とシスコ製のスイッチのネイティブ VLAN スパニングツリーが組み合わされて、Common Spanning Tree (CST) と呼ばれる単一のスパニングツリー トポロジが形成されます。
- シスコ デバイスは、トランクのネイティブ VLAN 以外の VLAN にある SSTP マルチキャスト MAC アドレスに BPDU を伝送します。したがって、他社製のデバイスではこれらのフレームが BPDU として認識されず、対応する VLAN のすべてのポート上でフラッドングされます。他社製の 802.1Q クラウドに接続された他のシスコ デバイスは、フラッドングされたこれらの BPDU を受信します。BPDU を受信すると、Cisco スイッチは、他社製の 802.1Q デバイス クラウドにわたって、VLAN 別のスパニングツリー トポロジを維持できません。シスコ デバイスを隔てている他社製の 802.1Q クラウドは、802.1Q トランクを介して他社製の 802.1Q クラウドに接続されたすべてのデバイス間の単一のブロードキャスト セグメントとして処理されます。
- シスコ デバイスを他社製の 802.1Q クラウドに接続するすべての 802.1Q トランク上で、ネイティブ VLAN が同じであることを確認します。

- 他社製の特定の 802.1Q クラウドに複数のシスコ デバイスを接続する場合は、すべての接続に 802.1Q トランクを使用する必要があります。シスコ デバイスを他社製の 802.1Q クラウドにアクセス ポート経由で接続することはできません。この場合、シスコ製のアクセス ポートはスパンニングツリー「ポート不一致」状態になり、トラフィックはポートを通過しません。
- トランク ポートをポート チャネル グループに含めることができますが、そのグループのトランクはすべて同じ設定にする必要があります。グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。パラメータの設定を変更すると、許容 VLAN やトランク ステータスなど、デバイスのグループのすべてのポートにその設定を伝えます。たとえば、ポート グループのあるポートがトランクになるのを中止すると、すべてのポートがトランクになるのを中止します。
- トランク ポートで 802.1X をイネーブルにしようとする、エラー メッセージが表示され、802.1X はイネーブルになりません。802.1X をイネーブルにしたポートをトランク モードに変更しようとしても、ポートのモードは変更されません。
- 入力ユニキャスト パケット カウンタだけが SVI カウンタでサポートされます。

レイヤ2 インターフェイスのデフォルト設定

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

表 3-1 デフォルトのアクセスおよびトランク ポート モード パラメータ

パラメータ	デフォルト
スイッチポート モード	アクセス
Allowed VLANs	1 ~ 3967, 4048 ~ 4094
アクセス VLAN ID	VLAN1
ネイティブ VLAN ID	VLAN1
ネイティブ VLAN ID タギング	ディセーブル
管理状態	閉じる
SVI 自動ステート	イネーブル

アクセス インターフェイスとトランク インターフェイスの設定

この項では、次のトピックについて取り上げます。

- 「アクセスおよびトランク インターフェイスの設定に関する注意事項」 (P.3-10)
- 「レイヤ2 アクセス ポートとしての VLAN インターフェイスの設定」 (P.3-10)
- 「アクセス ホスト ポートの設定」 (P.3-12)
- 「トランク ポートの設定」 (P.3-14)
- 「802.1Q トランク ポートのネイティブ VLAN の設定」 (P.3-15)
- 「トランッキング ポートの許可 VLAN の設定」 (P.3-17)

- 「デフォルト インターフェイスの設定」 (P.3-19)
- 「SVI 自動ステート除外の設定」 (P.3-21)
- 「システムの SVI 自動ステートのディセーブル化の設定」 (P.3-23)
- 「ネイティブ VLAN トラフィックにタグを付けるためのデバイス設定」 (P.3-26)
- 「システムのデフォルト ポート モードをレイヤ 2 に変更」 (P.3-28)
- 「インターフェイス コンフィギュレーションの確認」 (P.3-29)



(注)

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

アクセスおよびトランク インターフェイスの設定に関する注意事項

トランクのすべての VLAN は同じ VDC である必要があります。

レイヤ2 アクセスポートとしての VLAN インターフェイスの設定

レイヤ 2 ポートをアクセスポートとして設定できます。アクセスポートは、パケットを、1つのタグなし VLAN 上だけで送信します。インターフェイスが伝送する VLAN トラフィックを指定します。これがアクセス VLAN になります。アクセスポートの VLAN を指定しない場合、そのインターフェイスはデフォルト VLAN のトラフィックだけを伝送します。デフォルトの VLAN は VLAN 1 です。

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

はじめる前に

レイヤ 2 インターフェイスを設定することを確認します。

手順の概要

1. `configure terminal`
2. `interface {{type slot/port}} | {{port-channel number}}`
3. `switchport mode {access | trunk}`
4. `switchport access vlan vlan-id`
5. `exit`
6. (任意) `show interface`
7. (任意) `show interface status error policy [detail]`
8. (任意) `no shutdown`
9. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	interface {{type slot/port} {port-channel number}} 例： switch(config)# interface ethernet 3/1 switch(config-if)#	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switchport mode {access trunk} 例： switch(config-if)# switchport mode access	インターフェイスを、非トランキング、タグなし、シングル VLAN レイヤ 2 インターフェイスとして設定します。アクセス ポートは、1 つの VLAN のトラフィックだけを伝送できます。デフォルトでは、アクセス ポートは VLAN1 のトラフィックを伝送します。異なる VLAN のトラフィックを伝送するようにアクセス ポートを設定するには、 switchport access vlan コマンドを使用します。
ステップ 4	switchport access vlan vlan-id 例： switch(config-if)# switchport access vlan 5	このアクセス ポートでトラフィックを伝送する VLAN を指定します。このコマンドを入力しない場合、アクセス ポートは VLAN1 のトラフィックだけを伝送します。アクセス ポートがトラフィックを伝送する VLAN を変更する場合は、このコマンドを使用します。
ステップ 5	exit 例： switch(config-if)# exit switch(config)#	コンフィギュレーション モードを終了します。
ステップ 6	show interface 例： switch# show interface	(任意) インターフェイスのステータスと内容を表示します。
ステップ 7	show interface status error policy [detail] 例： switch# show interface status error policy detail	(任意) ポリシープログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、 detail コマンドを使用します。

	コマンド	目的
ステップ 8	<pre>no shutdown</pre> <p>例:</p> <pre>switch# conf t switch(config)#int e3/1 switch(config-if)# no shutdown</pre>	(任意) ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは <code>error-disabled</code> ポリシー状態になります。
ステップ 9	<pre>copy running-config startup-config</pre> <p>例:</p> <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、イーサネット 3/1 をレイヤ 2 アクセス ポートとして設定し、VLAN5 のトラフィックだけを伝送する例を示します。

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

アクセス ホスト ポートの設定



(注) `switchport host` コマンドは、端末に接続するインターフェイスだけに使用します。

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



(注) ポート チャネルインターフェイスの詳細は、[第 6 章「ポート チャネルの設定」](#) および『*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

はじめる前に

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

手順の概要

1. `configure terminal`
2. `interface type slot/port`
3. `switchport host`
4. `exit`
5. (任意) `show interface`
6. (任意) `show interface status error policy [detail]`

7. (任意) `no shutdown`
8. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例： switch# <code>configure terminal</code> switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface type slot/port</code> 例： switch(config)# <code>interface ethernet 3/1</code> switch(config-if)#	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport host</code> 例： switch(config-if)# <code>switchport host</code>	インターフェイスをアクセス ホスト ポートとして設定します。このポートはただちに、スパンニングツリー フォワーディング ステートに移行し、このインターフェイスのポート チャネル動作をディセーブルにします。 (注) このコマンドは端末だけに適用します。
ステップ 4	<code>exit</code> 例： switch(config-if)# <code>exit</code> switch(config)#	インターフェイス コンフィギュレーション モードを終了します。
ステップ 5	<code>show interface</code> 例： switch# <code>show interface</code>	(任意) インターフェイスのステータスと内容を表示します。
ステップ 6	<code>show interface status error policy [detail]</code> 例： switch# <code>show interface status error policy detail</code>	(任意) ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、 detail コマンドを使用します。
ステップ 7	<code>no shutdown</code> 例： switch# <code>configure terminal</code> switch(config)# <code>int e3/1</code> switch(config-if)# <code>no shutdown</code>	(任意) ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは <code>error-disabled</code> ポリシー状態になります。
ステップ 8	<code>copy running-config startup-config</code> 例： switch(config)# <code>copy running-config startup-config</code>	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、イーサネット 3/1 をレイヤ 2 アクセス ポートとして設定し、PortFast をイネーブルにしてポート チャネルをディセーブルにする例を示します。

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

トランク ポートの設定

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



(注) デバイスは 802.1Q カプセル化だけをサポートします。

はじめる前に

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

手順の概要

1. **configure terminal**
2. **interface** {type slot/port | port-channel number}
3. **switchport mode** {access | trunk}
4. **exit**
5. (任意) **show interface**
6. (任意) **show interface status error policy** [detail]
7. (任意) **no shutdown**
8. (任意) **copy running-config startup-config**

手順の詳細

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

	コマンド	目的
ステップ 3	<pre>switchport mode {access trunk}</pre> <p>例:</p> <pre>switch(config-if)# switchport mode trunk</pre>	<p>インターフェイスをレイヤ2 トランク ポートとして設定します。トランク ポートは、同じ物理リンクで1つ以上の VLAN 内のトラフィックを送送できます (各 VLAN はトランキングが許可された VLAN リストに基づいています)。デフォルトでは、トランク インターフェイスはすべての VLAN のトラフィックを送送できます。特定のトランク上で特定の VLAN だけを許可するように指定するには、switchport trunk allowed vlan コマンドを使用します。</p>
ステップ 4	<pre>exit</pre> <p>例:</p> <pre>switch(config-if)# exit switch(config)#</pre>	<p>インターフェイス コンフィギュレーション モードを終了します。</p>
ステップ 5	<pre>show interface</pre> <p>例:</p> <pre>switch# show interface</pre>	<p>(任意) インターフェイスのステータスと内容を表示します。</p>
ステップ 6	<pre>show interface status error policy [detail]</pre> <p>例:</p> <pre>switch# show interface status error policy detail</pre>	<p>(任意) ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。</p> <p>エラーを生成するインターフェイスの詳細を表示するには、detail コマンドを使用します。</p>
ステップ 7	<pre>no shutdown</pre> <p>例:</p> <pre>switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown</pre>	<p>(任意) ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続き、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。</p>
ステップ 8	<pre>copy running-config startup-config</pre> <p>例:</p> <pre>switch(config)# copy running-config startup-config</pre>	<p>(任意) 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。</p>

次に、イーサネット 3/1 をレイヤ2 トランク ポートとして設定する例を示します。

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

802.1Q トランク ポートのネイティブ VLAN の設定

ネイティブ VLAN を 802.1Q トランク ポートに設定できます。このパラメータを設定しない場合、トランク ポートはデフォルト VLAN をネイティブ VLAN ID として使用します。



(注)

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

手順の概要

1. **configure terminal**
2. **interface** {*type slot/port* | **port-channel number**}
3. **switchport trunk native vlan** *vlan-id*
4. **exit**
5. (任意) **show vlan**
6. (任意) **show interface status error policy** [detail]
7. (任意) **no shutdown**
8. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface { <i>type slot/port</i> port-channel number }	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switchport trunk native vlan <i>vlan-id</i> 例: switch(config-if)# switchport trunk native vlan 5	802.1Q トランクのネイティブ VLAN を設定します。指定できる範囲は 1 ~ 4094 です (ただし、内部使用に予約されている VLAN は除きます)。デフォルト値は VLAN 1 です。
ステップ 4	exit 例: switch(config-if)# exit switch(config)#	インターフェイス コンフィギュレーション モードを終了します。
ステップ 5	show vlan 例: switch# show vlan	(任意) VLAN のステータスと内容を表示します。
ステップ 6	show interface status error policy [detail] 例: switch# show interface status error policy detail	(任意) ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、 detail コマンドを使用します。

	コマンド	目的
ステップ 7	<pre>no shutdown</pre> <p>例:</p> <pre>switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown</pre>	(任意) ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは <code>error-disabled</code> ポリシー状態になります。
ステップ 8	<pre>copy running-config startup-config</pre> <p>例:</p> <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、ネイティブ VLAN をイーサネット 3/1 に設定し、レイヤ 2 トランク ポートを VLAN 5 に設定する例を示します。

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

トランキング ポートの許可 VLAN の設定

特定のトランク ポートで許可される VLAN の ID を指定できます。



(注)

`switchport trunk allowed vlan vlan-list` コマンドは、指定したポートの現在の VLAN リストを新しいリストと置き換えます。新しいリストが適用される前に確認を求められます。

大規模な設定のコピー アンド ペーストをしている場合は、CLI が他のコマンドを受け入れる前に確認のため待機しているため障害が発生する場合があります。この問題を回避するには、設定をペーストする前に `terminal dont-ask` コマンドを使用して、メッセージの表示をディセーブルにできます。

はじめる前に

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



(注)

内部使用に予約されている VLAN のブロックを変更できます。予約 VLAN 変更の詳細については、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。

手順の概要

1. `configure terminal`
2. `interface {ethernet slot/port | port-channel number}`
3. `switchport trunk allowed vlan {vlan-list | add vlan-list | all | except vlan-list | none | remove vlan-list}`
4. `exit`

■ アクセス インターフェイスとトランク インターフェイスの設定

5. (任意) **show vlan**
6. (任意) **show interface status error policy [detail]**
7. (任意) **no shutdown**
8. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface {ethernet slot/port port-channel number} 例: switch(config)# interface ethernet 3/1	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switchport trunk allowed vlan {vlan-list add vlan-list all except vlan-list none remove vlan-list} 例: switch(config-if)# switchport trunk allowed vlan add 15-20#	トランク インターフェイスの許可 VLAN を設定します。デフォルトでは、トランク インターフェイス上のすべての VLAN (1 ~ 3967 および 4048 ~ 4094) が許可されます。VLAN 3968 ~ 4047 は、内部で使用するデフォルトで予約されている VLAN です。デフォルトでは、すべてのトランク インターフェイスですべての VLAN が許可されます。デフォルトの予約済み VLAN は 3968 ~ 4094 で、予約 VLAN のブロックを変更できます。詳細については、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。 (注) 内部で割り当て済みの VLAN を、トランク ポート上の許可 VLAN として追加することはできません。内部で割り当て済みの VLAN を、トランク ポートの許可 VLAN として登録しようとする、メッセージが返されます。
ステップ 4	exit 例: switch(config-if)# exit switch(config)#	インターフェイス コンフィギュレーション モードを終了します。
ステップ 5	show vlan 例: switch# show vlan	(任意) VLAN のステータスと内容を表示します。
ステップ 6	show interface status error policy [detail] 例: switch# show interface status error policy detail	(任意) ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、 detail コマンドを使用します。

	コマンド	目的
ステップ 7	<pre>no shutdown</pre> <p>例:</p> <pre>switch# conf t switch(config)# int e3/1 switch(config-if)# no shutdown</pre>	(任意) ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは <code>error-disabled</code> ポリシー状態になります。
ステップ 8	<pre>copy running-config startup-config</pre> <p>例:</p> <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

デフォルト インターフェイスの設定

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



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

手順の概要

1. `configure terminal`
2. `default interface int-if [checkpoint name]`
3. `exit`
4. (任意) `show interface`
5. (任意) `show interface status error policy [detail]`
6. (任意) `no shutdown`

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	default interface int-if [checkpoint name] 例: switch(config)# default interface ethernet 3/1 checkpoint test8	インターフェイスの設定を削除し、デフォルトの設定を復元します。キーワードを使用して、サポートされているインターフェイスを表示します。 checkpoint キーワードを使用して、設定を消去する前にインターフェイスの実行コンフィギュレーションのコピーを保存します。
ステップ 3	exit 例: switch(config)# exit switch#	グローバル コンフィギュレーション モードを終了します。
ステップ 4	show interface 例: switch# show interface	(任意) インターフェイスのステータスと内容を表示します。
ステップ 5	show interface status error policy [detail] 例: switch# show interface status error policy detail	(任意) ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、 detail コマンドを使用します。
ステップ 6	no shutdown 例: switch# conf t switch(config)# int e3/1 switch(config-if)# no shutdown	(任意) ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。これにより、ポリシー プログラミングが続き、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

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

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

SVI 自動ステート除外の設定

イーサネット インターフェイスまたはポート チャネルに SVI 自動ステート除外機能を設定できます。自動ステート除外オプションを使用して、ポートが SVI 計算を稼働または停止したり、それを選択したポートでイネーブルのすべての VLAN に適用するのをイネーブルまたはディセーブルにすることができます。また、SVI 自動ステート除外 VLAN 機能を使用して、VLAN を自動ステート除外インターフェイスから除外することができます。

手順の概要

1. **configure terminal**
2. **interface** *{{type slot/port}}* | **{port-channel number}**
3. **switchport**
4. **[no] switchport autostate exclude**
5. (任意) **switchport autostate exclude vlan** *vlan id*
6. **exit**
7. (任意) **show running-config interface***{{type slot/port}}* | **{port-channel number}**
8. (任意) **show interface status error policy** [detail]
9. (任意) **no shutdown**
10. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface <i>{{type slot/port}}</i> {port-channel number} 例： switch(config)# interface ethernet 3/1 switch(config-if)#	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switchport 例： switch(config-if)# switchport	インターフェイスをレイヤ 2 インターフェイスとして設定します。
ステップ 4	[no]switchport autostate exclude 例： switch(config-if)# switchport autostate exclude	VLAN に複数のポートがあるときに、VLAN インターフェイスのリンクアップ計算からポートを除外します。 デフォルト設定に戻すには、このコマンドの no 形式を使用します。

	コマンド	目的
ステップ 5	<pre>[no]switchport autostate exclude vlan vlan id</pre> <p>例: switch(config-if)# switchport autostate exclude vlan 10</p>	<p>(任意) 自動ステート除外インターフェイスから vlan または vlan のセットを除外します。これにより、システムの中断を最小限に抑えることができます。</p> <p>デフォルト設定に戻すには、このコマンドの no 形式を使用します。</p>
ステップ 6	<pre>exit</pre> <p>例: switch(config-if)# exit switch(config)#</p>	<p>インターフェイス コンフィギュレーション モードを終了します。</p>
ステップ 7	<pre>show running-config interface {{type slot/port}} {{port-channel number}}</pre> <p>例: switch(config)# show running-config interface ethernet 3/1</p>	<p>(任意) 指定されたインターフェイスに関する設定情報を表示します。</p>
ステップ 8	<pre>show interface status error policy [detail]</pre> <p>例: switch# show interface status error policy detail</p>	<p>(任意) ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。</p> <p>エラーを生成するインターフェイスの詳細を表示するには、detail コマンドを使用します。</p>
ステップ 9	<pre>no shutdown</pre> <p>例: switch# conf t switch(config)# int e3/1 switch(config-if)# no shutdown</p>	<p>(任意) ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。</p>
ステップ 10	<pre>copy running-config startup-config</pre> <p>例: switch(config)# copy running-config startup-config</p>	<p>(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。</p>

次に、Cisco NX-OS デバイスで VLAN インターフェイスのリンクアップ計算からポートを除外する例を示します。

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

次に、自動除外インターフェイスから VLAN を除外する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# switchport
switch(config-if)# switchport autostate exclude
switch(config-if)# switchport autostate exclude vlan 10
```


システムの SVI 自動ステートのディセーブル化の設定

SVI 自動ステートのディセーブル化機能を設定して、対応する VLAN 内にアップ状態のインターフェイスがない場合でも SVI をアップ状態に保持することができます。システム全体にこの機能を設定するには、次の手順を使用します。

手順の概要

1. **configure terminal**
2. **system default interface-vlan no autostate**
3. (任意) **show running-config[all]**
4. (任意) **show interface status error policy [detail]**
5. (任意) **no shutdown**



(注) **system default interface vlan autostate** コマンドが SVI 自動ステート機能をイネーブルにします。

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	system default interface-vlan no autostate 例: switch(config)# system default interface-vlan no autostate	デバイスに対するデフォルトの自動ステート動作をディセーブルにします。
ステップ 3	show interface status error policy [detail] 例: switch# show interface status error policy detail	(任意) ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、 detail コマンドを使用します。
ステップ 4	no shutdown 例: switch# conf t switch(config)# int e3/1 switch(config-if)# no shutdown	(任意) ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 5	show running-config [all] 例: switch(config)# show running-config	(任意) 実行コンフィギュレーションを表示します。 デフォルト情報および設定情報を表示するには、 all キーワードを使用します。

次に、Cisco NX-OS デバイス上でデフォルトの自動ステート動作をディセーブルにする例を示します。

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

SVI 単位の SVI 自動ステートのディセーブル化の設定

個々の SVI 上で SVI 自動ステートのイネーブル化またはディセーブル化を設定できます。SVI レベルの設定は、その特定の SVI に対するシステムレベルの SVI 自動ステート設定より優先されます。

手順の概要

1. **configure terminal**
2. **feature interface-vlan**
3. **interface vlan *vlan-id***
4. **[no] autostate**
5. **exit**

6. (任意) **show running config-interface vlan *vlan-id***
7. (任意) **show interface status error policy [detail]**
8. (任意) **no shutdown**
9. (任意) **show startup-config *vlan id***

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	feature interface-vlan 例： switch(config)# feature interface-vlan	VLAN インターフェイス モードをイネーブルにします。
ステップ 3	interface vlan <i>vlan-id</i> 例： switch(config)#interface vlan10 switch(config-if)	VLAN インターフェイスを作成し、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 ~ 4094 です。
ステップ 4	[no] autostate 例： switch(config-if)# no autostate	デフォルトでは、指定されたインターフェイスの SVI 自動ステート機能をイネーブルにします。 デフォルト設定をディセーブルにするには、このコマンドの no 形式を使用します。
ステップ 5	exit 例： switch(config-if)# exit switch(config)#	インターフェイス コンフィギュレーション モードを終了します。
ステップ 6	show running-config interface vlan <i>vlan-id</i> 例： switch(config)# show running-config interface vlan10	(任意) 特定の VLAN インターフェイスの実行コンフィギュレーションを表示します。
ステップ 7	show interface status error policy [detail] 例： switch# show interface status error policy detail	(任意) ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、 detail コマンドを使用します。

	コマンド	目的
ステップ 8	no shutdown 例: <pre>switch# conf terminal switch(config)# int e3/1 switch(config-if)# no shutdown</pre>	(任意) ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 9	show startup-config interface vlan vlan-id 例: <pre>switch(config)# show startup-config interface vlan10</pre>	(任意) スタートアップ コンフィギュレーションの VLAN 設定を表示します。

次に、個々の SVI 上でデフォルトの自動ステート動作をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature interface-vlan
switch(config)# interface vlan10
switch(config-if)# no autostate
```

ネイティブ VLAN トラフィックにタグを付けるためのデバイス設定

802.1Q トランク インターフェイスを使用する場合、ネイティブ VLAN ID の値と一致しすべてのタグなしトラフィックをドロップするタグで開始するすべてのパケットに対するタグgingを維持できます (この場合もインターフェイスの制御トラフィックは伝送されます)。この機能はデバイス全体に当てはまります。デバイスの VLAN を指定して当てはめることはできません。

vlan dot1q tag native グローバル コマンドを使用すると、デバイスのすべてのトランクですべてのネイティブ VLAN ID インターフェイスの動作を変更できます。



(注) あるデバイス上で 802.1Q タグgingをイネーブルにし、別のデバイスではディセーブルにすると、デバイス上のトラフィックはすべてドロップされ、この機能はディセーブルになります。この機能はデバイスごとに独自に設定する必要があります。

手順の概要

1. **configure terminal**
2. **vlan dot1q tag native**
3. **exit**
4. (任意) **show vlan**
5. (任意) **show interface status error policy [detail]**
6. (任意) **no shutdown**
7. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vlan dot1q tag native 例： switch(config)# vlan dot1q tag native	802.1Q トランキング ネイティブ VLAN ID インターフェイスの動作を変更します。このインターフェイスは、ネイティブ VLAN ID の値と一致してすべての非タグ付きトラフィックをドロップするタグを使って開始するすべてのパケットのタグgingを維持します。この場合も、制御トラフィックはネイティブ VLAN を通過します。デフォルトではディセーブルになっています。
ステップ 3	exit 例： switch(config)# exit switch#	グローバル コンフィギュレーション モードを終了します。
ステップ 4	show vlan 例： switch# show vlan	(任意) VLAN のステータスと内容を表示します。
ステップ 5	show interface status error policy [detail] 例： switch# show interface status error policy detail	(任意) ポリシープログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致を確認できます。 エラーを生成するインターフェイスの詳細を表示するには、 detail コマンドを使用します。
ステップ 6	no shutdown 例： switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown	(任意) ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが続き、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 7	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

次に、802.1Q トランク インターフェイスのネイティブ VLAN の動作を変更してタグ付きパケットを維持し、すべての非タグ付きトラフィックをドロップする例を示します（制御トラフィックは除く）。

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

システムのデフォルト ポート モードをレイヤ2に変更

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

手順の概要

1. **configure terminal**
2. **system default switchport [shutdown]**
3. **exit**
4. (任意) **show interface brief**
5. (任意) **show interface status error policy [detail]**
6. (任意) **no shutdown**
7. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	system default switchport [shutdown] 例: switch(config-if)# system default switchport	システムのすべてのインターフェイスに対するデフォルトのポート モードをレイヤ2 アクセス ポート モードに設定し、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。デフォルトでは、すべてのインターフェイスがレイヤ3 です。
ステップ 3	exit 例: switch(config-if)# exit switch(config)#	インターフェイス コンフィギュレーション モードを終了します。
ステップ 4	show interface brief 例: switch# show interface brief	(任意) インターフェイスのステータスと内容を表示します。
ステップ 5	show interface status error policy [detail] 例: switch# show interface status error policy detail	(任意) ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、 detail コマンドを使用します。

	コマンド	目的
ステップ 6	<pre>no shutdown</pre> <p>例:</p> <pre>switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown</pre>	(任意) ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 7	<pre>copy running-config startup-config</pre> <p>例:</p> <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

インターフェイス コンフィギュレーションの確認

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

コマンド	目的
show interface ethernet <i>slot/port</i> [brief counters debounce description flowcontrol mac-address status tranceiver]	インターフェイスの設定を表示します。
show interface brief	インターフェイス設定情報を、モードも含めて表示します。
show interface switchport	アクセスおよびトランク インターフェイスも含めて、すべてのレイヤ 2 インターフェイスの情報を表示します。
show interface trunk [module <i>module-number</i> vlan <i>vlan-id</i>]	トランク設定情報を表示します。
show interface capabilities	インターフェイスの機能に関する情報を表示します。
show interface status error policy [detail]	ハードウェア ポリシーと矛盾するインターフェイスおよび VLAN のエラーを表示します。 detail コマンドを使用すると、エラーを生成するインターフェイスの詳細が表示されます。
show running-config[all]	現在の設定に関する情報を表示します。 all コマンドを使用すると、デフォルトの設定と現在の設定が表示されます。
show running-config interface ethernet <i>slot/port</i>	指定されたインターフェイスに関する設定情報を表示します。

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

レイヤ2 インターフェイスのモニタリング

レイヤ2 インターフェイスを表示するには、次のコマンドを使用します。

コマンド	目的
<code>clear counters interface [interface]</code>	カウンタをクリアします。
<code>load- interval {interval seconds {1 2 3}}</code>	Cisco Nexus 9000 シリーズ デバイスは、ビットレートおよびパケットレートの統計情報に3種類のサンプリング インターバルを設定します。
<code>show interface counters [module module]</code>	入力および出力オクテット ユニキャスト パケット、マルチキャスト パケット、ブロードキャスト パケットを表示します。
<code>show interface counters detailed [all]</code>	入力パケット、バイト、マルチキャストを、出力パケットおよびバイトとともに表示します。
<code>show interface counters errors [module module]</code>	エラー パケットの数を表示します。

アクセス ポートおよびトランク ポートの設定例

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

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

次に、レイヤ2 トランク インターフェイスを設定してネイティブ VLAN および許容 VLAN を割り当て、デバイスにトランク インターフェイスのネイティブ VLAN トラフィックのタグを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/35
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk native vlan 10
switch(config-if)# switchport trunk allowed vlan 5, 10
switch(config-if)# exit
switch(config)# vlan dot1q tag native
switch(config)#
```


その他の参考資料

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

- 「関連資料」 (P.3-31)
- 「標準」 (P.3-31)
- 「管理情報ベース (MIB)」 (P.3-31)

関連資料

関連項目	マニュアル タイトル
レイヤ3 インターフェイスの設定	第4章、「レイヤ2 インターフェイスの設定」
ポート チャネル	第6章、「ポート チャネルの設定」
VLAN および STP	『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』
インターフェイス	『Interfaces Configuration Guide, Cisco DCNM for LAN』
システム管理	『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』
ハイアベイラビリティ	『Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide』
ライセンス	『Cisco NX-OS Licensing Guide』
リリース ノート	『Cisco Nexus 9000 Series NX-OS Release Notes』

標準

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

管理情報ベース (MIB)

MIB	MIB のリンク
<ul style="list-style-type: none"> • BRIDGE-MIB • IF-MIB • CISCO-IF-EXTENSION-MIB • ETHERLIKE-MIB 	<p>サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。</p> <p>ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html</p>



レイヤ 3 インターフェイスの設定

この章は、Cisco NX-OS デバイスに対するレイヤ 3 インターフェイスを設定する方法について説明し、次のセクションがあります。

- 「レイヤ 3 インターフェイスについて」 (P.4-1)
- 「レイヤ 3 インターフェイスのライセンス要件」 (P.4-5)
- 「ライセンス 3 インターフェイスの前提条件」 (P.4-5)
- 「注意事項と制約事項」 (P.4-5)
- 「デフォルト設定値」 (P.4-5)
- 「レイヤ 3 インターフェイスの設定」 (P.4-6)
- 「レイヤ 3 インターフェイス設定の確認」 (P.4-15)
- 「レイヤ 3 インターフェイスのモニタリング」 (P.4-16)
- 「レイヤ 3 インターフェイスの設定例」 (P.4-17)
- 「関連項目」 (P.4-17)
- 「その他の参考資料」 (P.4-18)

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

この項では、次のトピックについて取り上げます。

- 「ルーテッド インターフェイス」 (P.4-2)
- 「サブインターフェイス」 (P.4-2)
- 「ループバック インターフェイス」 (P.4-4)
- 「ハイ アベイラビリティ」 (P.4-4)
- 「仮想化のサポート」 (P.4-4)

ルーテッド インターフェイス

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

すべてのイーサネット ポートは、デフォルトでルーテッド インターフェイスです。CLI セットアップ スクリプトでこのデフォルトの動作を変更できます。

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。

ルーテッド インターフェイスからレイヤ3 ポート チャネルも作成できます。ポート チャネルの詳細については、第6章「ポート チャネルの設定」を参照してください。

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

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

サブインターフェイス

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

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

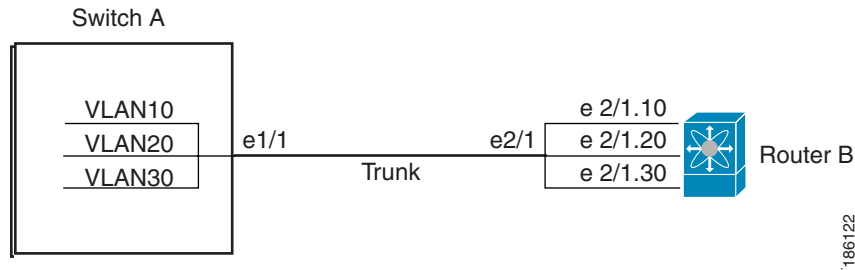
サブインターフェイスの名前は、親インターフェイスの名前（たとえば Ethernet 2/1）+ピリオド（.）+そのインターフェイス独自の番号です。たとえば、イーサネット インターフェイス 2/1 に Ethernet 2/1.1 というサブインターフェイスを作成できます。この場合、.1 はそのサブインターフェイスを表します。

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

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

図 4-1 に、インターフェイス E 2/1 のルータ B に接続するスイッチのトランッキングポートを示します。このインターフェイスには3つのサブインターフェイスがあり、トランッキングポートに接続する3つの VLAN にそれぞれ関連付けられています。

図 4-1 VLAN のサブインターフェイス



VLAN の詳細については、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。

VLAN インターフェイス

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

設定の前に VLAN ネットワーク インターフェイス機能をイネーブルにする必要があります。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については、『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』を参照してください。

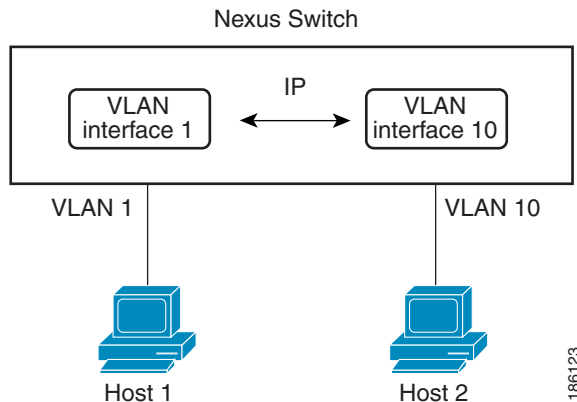


(注) VLAN 1 の VLAN インターフェイスは削除できません。

VLAN インターフェイスをルーティングするには、トラフィックをルーティングする VLAN ごとに VLAN インターフェイスを作成し、その VLAN インターフェイスに IP アドレスを割り当ててレイヤ3 内部 VLAN ルーティングを実現します。IP アドレスと IP ルーティングの詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

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

図 4-2 VLAN インターフェイスに接続した2つのVLAN



ループバック インターフェイス

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

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。

ハイアベイラビリティ

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

ハイアベイラビリティの詳細については、『Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide』を参照してください。

仮想化のサポート

レイヤ3 インターフェイスは、仮想ルーティング/転送 (VRF) インスタンスをサポートします。VRF は仮想化デバイス コンテキスト (VDC) 内にあります。デフォルトでは、Cisco NX-OS のデフォルトの VDC およびデフォルトの VRF が使用されます。

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

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

VRF でのインターフェイスの設定詳細を確認する場合には『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照します。



(注) そのインターフェイスに IP アドレスを設定する前に、インターフェイスを VRF に割り当てる必要があります。

レイヤ3 インターフェイスのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	レイヤ3 インターフェイスにライセンスは必要ありません。ライセンス パッケージに含まれていない機能は nx-os イメージにバンドルされており、無料で提供されます。

ライセンス3 インターフェイスの前提条件

ライセンス3 インターフェイスには次の前提条件があります。

- IP アドレッシングおよび基本設定を熟知している。IP アドレッシングの詳細については『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

注意事項と制約事項

レイヤ3 インターフェイスの設定には次の注意事項と制約事項があります。

- レイヤ3 インターフェイスをレイヤ2 インターフェイスに変更する場合、Cisco NX-OS はインターフェイスをシャットダウンしてインターフェイスを再度イネーブルにし、レイヤ3 固有の設定をすべて削除します。
- レイヤ2 インターフェイスをレイヤ3 インターフェイスに変更する場合、Cisco NX-OS はインターフェイスをシャットダウンしてインターフェイスを再度イネーブルにし、レイヤ2 固有の設定をすべて削除します。
- Cisco Nexus 9300 プラットフォームのサブインターフェイスはサポートされません。



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

デフォルト設定値

表 4-1 は、レイヤ3 インターフェイス パラメータのデフォルト設定です。

表 4-1 レイヤ3 インターフェイスのデフォルト パラメータ

パラメータ	デフォルト
管理ステート	閉じる

レイヤ3 インターフェイスの設定

この項では、次のトピックについて取り上げます。

- 「ルーテッド インターフェイスの設定」 (P.4-6)
- 「サブインターフェイスの設定」 (P.4-8)
- 「インターフェイスでの帯域幅の設定」 (P.4-10)
- 「ループバック インターフェイスの設定」 (P.4-12)
- 「VRF へのインターフェイスの割り当て」 (P.4-13)

ルーテッド インターフェイスの設定

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface ethernet slot/port 例: switch(config)# interface ethernet 2/1 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	no switchport 例: switch(config-if)# no switchport	その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ます。

	コマンド	目的
ステップ 4	ip address <i>ip-address/length</i> 例： switch(config-if)# ip address 192.0.2.1/8	このインターフェイスの IP アドレスを設定します。IP アドレッシングの詳細については、Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guideを参照してください。
	ipv6 address <i>ipv6-address/length</i> 例： switch(config-if)# ipv6 address 2001:0DB8::1/8	このインターフェイスの IPv6 アドレスを設定します。IPv6 アドレッシングの詳細については、Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guideを参照してください。
ステップ 5	show interfaces 例： switch(config-if)# show interfaces ethernet 2/1	(任意) レイヤ 3 インターフェイスの統計情報を表示します。
ステップ 6	no shutdown 例： switch# switch(config-if)# int e2/1 switch(config-if)# no shutdown	(任意) ポリシーがハードウェアポリシーに対応するインターフェイスのエラーをクリアします。このコマンドにより、ポリシープログラミングが続き、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 7	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) この設定の変更を保存します。

インターフェイス メディアをポイント ツー ポイントまたはブロードキャストのどちらかとして設定するには、**medium** コマンドを使用します。

コマンド	目的
medium { broadcast p2p } 例： switch(config-if)# medium p2p	インターフェイス メディアをポイント ツー ポイントまたはブロードキャストのどちらかとして設定します。



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

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

コマンド	目的
switchport 例： switch(config-if)# switchport	インターフェイスをレイヤ 2 インターフェイスとして設定し、このインターフェイス上のレイヤ 3 固有の設定を削除します。

次に、ルーテッド インターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# copy running-config startup-config
```

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

サブインターフェイスの設定

ルーテッド インターフェイスで構成されるルーテッド インターフェイスに1つまたは複数のサブインターフェイスを設定できます。

はじめる前に

親インターフェイスをルーテッド インターフェイスとして設定します。

「[ルーテッド インターフェイスの設定](#)」(P.4-6) を参照してください。

手順の概要

1. **configure terminal**
2. **interface ethernet slot/port.number**
3. **ip address ip-address/length**
または
ipv6 address ipv6-address/length
4. **encapsulation dot1Q vlan-id**
5. (任意) **show interfaces**
6. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface ethernet slot/port.number 例: switch(config)# interface ethernet 2/1.1 switch(config-subif)#	サブインターフェイスを作成し、サブインターフェイス コンフィギュレーション モードを開始します。 <i>number</i> の範囲は 1 ~ 4094 です。

	コマンド	目的
ステップ 3	ip address ip-address/length 例: switch(config-subif)# ip address 192.0.2.1/8	このサブインターフェイスの IP アドレスを設定します。IP アドレッシングの詳細については、Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guideを参照してください。
	ipv6 address ipv6-address/length 例: switch(config-subif)# ipv6 address 2001:0DB8::1/8	このサブインターフェイスの IPv6 アドレスを設定します。IPv6 アドレッシングの詳細については、Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guideを参照してください。
ステップ 4	encapsulation dot1Q vlan-id 例: switch(config-subif)# encapsulation dot1Q 33	サブインターフェイス上の IEEE 802.1Q VLAN カプセル化を設定します。範囲は 2 ~ 4093 です。
ステップ 5	show interfaces 例: switch(config-subif)# show interfaces ethernet 2/1.1	(任意) レイヤ 3 インターフェイスの統計情報を表示します。
ステップ 6	copy running-config startup-config 例: switch(config-subif)# copy running-config startup-config	(任意) この設定の変更を保存します。

次に、サブインターフェイスを作成する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1.1
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# encapsulation dot1Q 33
switch(config-if)# copy running-config startup-config
```

show interface eth コマンドの出力は、次の例に示すように、サブインターフェイス用に拡張されました。

```
switch# show interface ethernet 1/2.1
Ethernet1/2.1 is down (Parent Interface Admin down)
admin state is down, Dedicated Interface, [parent interface is Ethernet1/2]
Hardware: 40000 Ethernet, address: 0023.ac67.9bc1 (bia 4055.3926.61d4)
Internet Address is 10.10.10.1/24
MTU 1500 bytes, BW 40000000 Kbit, DLY 10 usec
reliability 255/255, txload 1/255, rxload 1/255
Auto-mdix is turned off
EtherType is 0x8100
L3 in Switched:
    ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
L3 out Switched:
    ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
```

インターフェイスでの帯域幅の設定

ルーテッド インターフェイス、ポート チャネル、またはサブインターフェイスに帯域幅を設定できます。上位層プロトコルは帯域幅パラメータを使用してパス コストを計算します。サブインターフェイスの帯域幅は、次のいずれかの方法で設定できます。

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

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

- 親インターフェイスがアップしている場合、サブインターフェイスの帯域幅は親インターフェイスの動作速度と同じです。ポートの場合、サブインターフェイスの帯域幅は設定されているリンク速度またはネゴシエート対象のリンク速度です。
- 親インターフェイスがダウンしている場合、サブインターフェイスの帯域幅は親インターフェイスのタイプによって異なります。
 - 1 Gb/s イーサネット ポートの場合、サブインターフェイスの帯域幅は 1 Gb/s です。
 - 10 Gb/s イーサネット ポートの場合、サブインターフェイスの帯域幅は 10 Gb/s です。
 - 100 Gb/s イーサネット ポートの場合、サブインターフェイスの帯域幅は 100 Gb/s です。

インターフェイスの帯域幅を設定するには、インターフェイス モードで次のコマンドを使用します。

コマンド	目的
bandwidth 例： switch(config-if)# bandwidth 100000	ルーテッド インターフェイス、ポート チャネル、またはサブインターフェイスに帯域幅パラメータを設定します。

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

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

VLAN インターフェイスの設定

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

手順の概要

1. **configure terminal**
2. **feature interface-vlan**
3. **interface vlan *number***
4. **ip address *ip-address/length***
または
ipv6 address *ipv6-address/length*
5. (任意) **show interface vlan *number***
6. (任意) **show interface status error policy [detail]**
7. (任意) **no shutdown**
8. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	feature interface-vlan 例： switch(config)# feature interface-vlan	VLAN インターフェイス モードをイネーブルにします。
ステップ 3	interface vlan <i>number</i> 例： Switch(config)# interface vlan 10 switch(config-if)#	VLAN インターフェイスを作成します。 <i>number</i> の範囲は 1 ~ 4094 です。
ステップ 4	ip address <i>ip-address/length</i> 例： switch(config-if)# ip address 192.0.2.1/8	この VLAN インターフェイスの IP アドレスを設定します。IP アドレッシングの詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。
	ipv6 address <i>ipv6-address/length</i> 例： switch(config-if)# ipv6 address 2001:0DB8::1/8	
ステップ 5	show interface vlan <i>number</i> 例： switch(config-if)# show interface vlan 10	(任意) レイヤ 3 インターフェイスの統計情報を表示します。

	コマンド	目的
ステップ 6	<pre>show interface status error policy [detail]</pre> <p>例:</p> <pre>switch(config-if)# show interface status error policy detail</pre>	<p>(任意) ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN を表示します。このコマンドより、ポリシーがハードウェアポリシーと一致を確認できます。</p> <p>エラーを生成するインターフェイスの詳細を表示するには、detail コマンドを使用します。</p>
ステップ 7	<pre>no shutdown</pre> <p>例:</p> <pre>switch# config-if) switch(config)# int e3/1 switch(config)# no shutdown</pre>	<p>(任意) ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。</p>
ステップ 8	<pre>copy running-config startup-config</pre> <p>例:</p> <pre>switch(config-if)# copy running-config startup-config</pre>	<p>(任意) この設定の変更を保存します。</p>

次に、VLAN インターフェイスを作成する例を示します。

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

ループバック インターフェイスの設定

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

はじめる前に

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface loopback instance 例: switch(config)# interface loopback 0 switch(config-if)#	ループバック インターフェイスを作成します。指定できる範囲は 0 ~ 1023 です。
ステップ 3	ip address ip-address/length 例: switch(config-if)# ip address 192.0.2.100/8 ipv6 address ipv6-address/length 例: switch(config-if)# ipv6 address 2001:0DB8::18/8	このインターフェイスの IP アドレスを設定します。IP アドレッシングの詳細については、Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guideを参照してください。 このインターフェイスの IPv6 アドレスを設定します。IPv6 アドレッシングの詳細については、Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guideを参照してください。
ステップ 4	show interfaces loopback instance 例: switch(config-if)# show interfaces loopback 0	(任意) ループバック インターフェイスの統計情報を表示します。
ステップ 5	copy running-config startup-config 例: switch(config-if)# copy running-config startup-config	(任意) この設定の変更を保存します。

次に、ループバック インターフェイスを作成する例を示します。

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

VRF へのインターフェイスの割り当て

VRF にレイヤ 3 インターフェイスを追加できます。

手順の概要

1. **configure terminal**
2. **interface interface-type number**
3. **vrf member vrf-name**
4. **ip-address ip-prefix/length**

■ レイヤ3 インターフェイスの設定

5. (任意) **show vrf [vrf-name] interface interface-type number**
6. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-type number 例: switch(config)# interface loopback 0 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	vrf member vrf-name 例: switch(config-if)# vrf member RemoteOfficeVRF	このインターフェイスを VRF に追加します。
ステップ 4	ip address ip-prefix/length 例: switch(config-if)# ip address 192.0.2.1/16	このインターフェイスの IP アドレスを設定します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。
ステップ 5	show vrf [vrf-name] interface interface-type number 例: switch(config-vrf)# show vrf Enterprise interface loopback 0	(任意) VRF 情報を表示します。
ステップ 6	copy running-config startup-config 例: switch(config)# copy running-config startup-config	(任意) この設定の変更を保存します。

次に、VRF にレイヤ 3 インターフェイスを追加する例を示します。

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


レイヤ3 インターフェイス設定の確認

レイヤ3 の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
<code>show interface ethernet slot/port</code>	レイヤ3 インターフェイスの設定情報、ステータス、カウンタ（インバウンドおよびアウトバウンド パケット レートおよびバイト レートが5分間に指数関数的に減少した平均値を含む）を表示します。
<code>show interface ethernet slot/port brief</code>	レイヤ3 インターフェイスの動作ステータスを表示します。
<code>show interface ethernet slot/port capabilities</code>	レイヤ3 インターフェイスの機能（ポート タイプ、速度、およびデュプレックスを含む）を表示します。
<code>show interface ethernet slot/port description</code>	レイヤ3 インターフェイスの説明を表示します。
<code>show interface ethernet slot/port status</code>	レイヤ3 インターフェイスの管理ステータス、ポート モード、速度、およびデュプレックスを表示します。
<code>show interface ethernet slot/port.number</code>	サブインターフェイスの設定情報、ステータス、カウンタ（インバウンドおよびアウトバウンド パケット レートおよびバイト レートが5分間に指数関数的に減少した平均値を含む）を表示します。
<code>show interface port-channel channel-id.number</code>	ポート チャネル サブインターフェイスの設定情報、ステータス、カウンタ（インバウンドおよびアウトバウンド パケット レートおよびバイト レートが5分間に指数関数的に減少した平均値を含む）を表示します。
<code>show interface loopback number</code>	ループバック インターフェイスの設定情報、ステータス、カウンタを表示します。
<code>show interface loopback number brief</code>	ループバック インターフェイスの動作ステータスを表示します。
<code>show interface loopback number description</code>	ループバック インターフェイスの説明を表示します。
<code>show interface loopback number status</code>	ループバック インターフェイスの管理ステータスおよびプロトコルステータスを表示します。
<code>show interface vlan number</code>	VLAN インターフェイスの設定情報、ステータス、カウンタを表示します。
<code>show interface vlan number brief</code>	VLAN インターフェイスの動作ステータスを表示します。
<code>show interface vlan number description</code>	VLAN インターフェイスの説明を表示します。

コマンド	目的
<code>show interface vlan number status</code>	VLAN インターフェイスの管理ステータスおよびプロトコル ステータスを表示します。
<code>show interface status error policy [detail]</code>	ハードウェア ポリシーと矛盾するインターフェイスおよび VLAN のエラーを表示します。 detail コマンドを使用すると、エラーを受信するインターフェイスおよび VLAN の詳細を表示できます。

レイヤ3 インターフェイスのモニタリング

レイヤ3 統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
<code>load- interval {interval seconds {1 2 3}}</code>	Cisco Nexus 9000 シリーズ デバイスは、ビットレートおよびパケットレートの統計情報に3種類のサンプリング インターバルを設定します。VLAN ネットワーク インターフェイスでの範囲は 60 ~ 300 秒であり、レイヤ インターフェイスでの範囲は 30 ~ 300 秒です。
<code>show interface ethernet slot/port counters</code>	レイヤ3 インターフェイスの統計情報を表示します (ユニキャスト、マルチキャスト、ブロードキャスト)。
<code>show interface ethernet slot/port counters brief</code>	レイヤ3 インターフェイスの入力および出力カウンタを表示します。
<code>show interface ethernet slot/port counters detailed [all]</code>	レイヤ3 インターフェイスの統計情報を表示します。オプションとして、32ビットと64ビットの packets およびバイト カウンタ (エラーを含む) をすべて含めることができます。
<code>show interface ethernet slot/port counters errors</code>	レイヤ3 インターフェイスの入力および出力エラーを表示します。
<code>show interface ethernet slot/port counters snmp</code>	SNMP MIB から報告されたレイヤ3 インターフェイス カウンタを表示します。
<code>show interface ethernet slot/port.number counters</code>	サブインターフェイスの統計情報 (ユニキャスト、マルチキャスト、およびブロードキャスト) を表示します。
<code>show interface port-channel channel-id.number counters</code>	ポート チャネル サブインターフェイスの統計情報 (ユニキャスト、マルチキャスト、およびブロードキャスト) を表示します。
<code>show interface loopback number counters</code>	ループバック インターフェイスの入力および出力カウンタ (ユニキャスト、マルチキャスト、およびブロードキャスト) を表示します。

コマンド	目的
<code>show interface loopback <i>number</i> counters detailed [all]</code>	ループバック インターフェイスの統計情報を表示します。オプションとして、32 ビットと 64 ビットのパケットおよびバイト カウンタ (エラーを含む) をすべて含めることができます。
<code>show interface loopback <i>number</i> counters errors</code>	ループバック インターフェイスの入力および出力エラーを表示します。
<code>show interface vlan <i>number</i> counters</code>	VLAN インターフェイスの入力および出力カウンタ (ユニキャスト、マルチキャスト、およびブロードキャスト) を表示します。
<code>show interface vlan <i>number</i> counters detailed [all]</code>	VLAN インターフェイスの統計情報を表示します。オプションとして、レイヤ3 パケットおよびバイト カウンタをすべて含めることができます (ユニキャストおよびマルチキャスト)。
<code>show interface vlan <i>number</i> counters snmp</code>	SNMP MIB から報告された VLAN インターフェイス カウンタを表示します。

レイヤ3 インターフェイスの設定例

次に、イーサネット サブインターフェイスを設定する例を示します。

```
interface ethernet 2/1.10
  description Layer 3
  ip address 192.0.2.1/8
```

次に、ループバック インターフェイスを設定する例を示します。

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

関連項目

レイヤ3 インターフェイスの詳細については、次の項目を参照してください。

- [第6章「ポートチャネルの設定」](#)
- 『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』

その他の参考資料

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

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

関連資料

関連項目	マニュアル タイトル
IP	『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』
VLAN	「Configuring VLANs」の章、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』

管理情報ベース (MIB)

MIB	MIB のリンク
レイヤ3 インターフェイスに関連する MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html

標準

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



双方向フォワーディング検出の設定

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

この章は、次の項で構成されています。

- 「BFD について」 (P.5-1)
- 「BFD のライセンス要件」 (P.5-4)
- 「BFD の前提条件」 (P.5-4)
- 「注意事項と制約事項」 (P.5-5)
- 「デフォルト設定値」 (P.5-6)
- 「BFD の設定」 (P.5-6)
- 「BFD 設定の確認」 (P.5-31)
- 「BFD のモニタ」 (P.5-32)
- 「BFD の設定例」 (P.5-32)
- 「その他の関連資料」 (P.5-32)

BFD について

BFD は、メディア タイプ、カプセル化、トポロジ、およびルーティング プロトコルの転送パス障害を高速で検出するように設計された検出プロトコルです。BFD を使用することで、さまざまなプロトコルの Hello メカニズムにより、変動速度ではなく一定速度で転送パス障害を検出できます。BFD はプロファイリングおよびプランニングを簡単にし、再コンバージェンス時間の一貫性を保ち、予測可能にします。

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

この項では、次のトピックについて取り上げます。

- 「非同期モード」 (P.5-2)
- 「BFD の障害検出」 (P.5-2)
- 「分散型動作」 (P.5-3)
- 「BFD エコー機能」 (P.5-3)
- 「セキュリティ」 (P.5-4)

- 「ハイアベイラビリティ」(P.5-4)
- 「仮想化のサポート」(P.5-4)

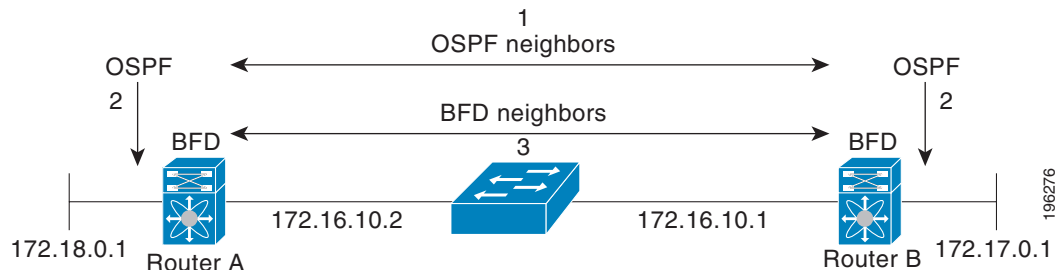
非同期モード

Cisco NX-OS は、BFD 非同期モードをサポートします。BFD 非同期モードでは、2 個の隣接するデバイス間で BFD 制御パケットが送信され、デバイス間の BFD ネイバーセッションがアクティベートされ、維持されます。両方のデバイス（または BFD ネイバー）で BFD を設定できます。インターフェイスおよび適切なプロトコルで一度 BFD がイネーブルになると、Cisco NX-OS は BFD セッションを作成し、BFD セッションパラメータをネゴシエートし、BFD 制御パケットをネゴシエートされた間隔で各 BFD ネイバーに送信し始めます。BFD セッションパラメータは、次のとおりです。

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

図 5-1 に BFD セッション確立方法を示します。この図は、Open Shortest Path First (OSPF) と BFD を実行する 2 台のルータがある単純なネットワークを示します。OSPF がネイバーを検出すると (1)、OSPF 隣接ルータで BFD ネイバーセッションを開始する要求が、ローカル BFD プロセスに送信されます (2)。OSPF ネイバールータとの BFD ネイバーセッションが確立されました (3)。

図 5-1 BFD ネイバー関係の確立



BFD の障害検出

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

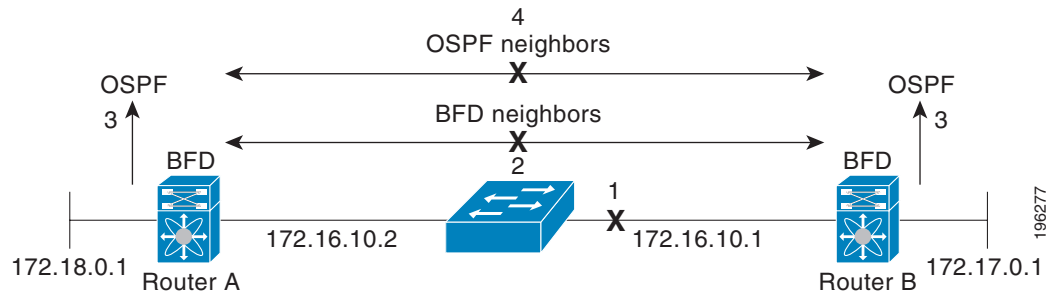
BFD は転送パスに障害を検出したとき、障害検出通知を BFD 対応プロトコルに送信します。ローカル デバイスは、プロトコル再計算プロセスを開始してネットワーク全体の収束時間を削減できます。

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



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

図 5-2 OSPF ネイバー関係の解除



分散型動作

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

BFD エコー機能

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

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

セキュリティ

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

BFD パケットの SHA-1 認証を設定できます。

ハイアベイラビリティ

BFD は、ステートレス リスタートをサポートします。リブートまたはスーパーバイザ スイッチオーバー後に、Cisco NX-OS が実行コンフィギュレーションを適用し、BFD がただちに制御パケットを BFD ピアに送信します。

仮想化のサポート

BFD は、仮想ルーティングおよび転送 (VRF) インスタンスをサポートしています。VRF は仮想化デバイス コンテキスト (VDC) 内にあります。デフォルトでは、Cisco NX-OS によりデフォルト VDC およびデフォルト VRF が使用されます。

BFD のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	BFD にはライセンスは不要です。ライセンス パッケージに含まれていない機能は nx-os イメージにバンドルされており、無料で提供されます。

BFD の前提条件

BFD には、次の前提条件があります。

- BFD 機能をイネーブルにする必要があります (「[BFD 機能のイネーブル化](#)」(P.5-7) を参照)。
- BFD 対応インターフェイスでインターネット制御メッセージプロトコル (ICMP) リダイレクト メッセージをディセーブルにします。
- 同一の IP 送信元アドレスおよび宛先アドレスを調べる IP パケット検証チェックをディセーブルにします。
- 設定作業とともに一覧表示されているその他の詳細な前提条件を参照してください。

注意事項と制約事項

BFD 設定時の注意事項と制約事項は次のとおりです。

- BFD は BFD バージョン 1 をサポートします。
- BFD は IPv4 をサポートします。
- BFD はアドレスファミリごとに 1 つのセッションのみをサポートします (インターフェイスごと)。
- BFD は、シングルホップ BFD をサポートします。
- ボーダー ゲートウェイ プロトコル (BGP) の BFD は、シングルホップ External BGP (EBGP) および Internal BGP (iBGP) ピアをサポートしています。
- BFD は、Cisco NX-OS リリース 5.2 以降ではキー付き SHA-1 認証をサポートします。
- BFD は、次のレイヤ 3 インターフェイスをサポートします。物理インターフェイス、ポート チャネル、サブインターフェイス、および VLAN インターフェイス。
- BFD はレイヤ 3 隣接情報に応じて、レイヤ 2 のトポロジ変更を含むトポロジ変更を検出します。レイヤ 3 隣接情報が使用できない場合、VLAN インターフェイス (SVI) の BFD セッションはレイヤ 2 トポロジのコンバージェンス後に稼働しない可能性があります。
- 2 台のデバイス間のスタティック ルート上の BFD については、両方のデバイスが BFD をサポートする必要があります。デバイスの一方または両方が BFD をサポートしていない場合、スタティック ルートはルーティング情報ベース (RIB) でプログラミングされません。
- ポート チャネル設定の制限事項
 - BFD で使用されるレイヤ 3 ポート チャネルでは、ポート チャネルの LACP をイネーブルにする必要があります。
 - SVI のセッションで使用されるレイヤ 2 ポート チャネルでは、ポート チャネルの LACP をイネーブルにする必要があります。
- SVI の制限事項
 - ASIC リセットにより他のポートのトラフィックが中断されます。このイベントは、その他のポートの SVI セッションがフラップする原因になることがあります。ASIC がリセットするトリガーには、VDC をリロードしているがあります。また、キャリア インターフェイスが仮想ポート チャネル (vPC) の場合、BFD は SVI インターフェイスではサポートされません。
 - トポロジを変更すると (たとえば、VLAN へのリンクの追加または削除、レイヤ 2 ポート チャネルからのメンバの削除など)、SVI セッションが影響を受ける場合があります。SVI セッションはダウンした後、トポロジ ディスカバリの終了後に起動する場合があります。



ヒント

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

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

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



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

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

デフォルト設定値

表 5-1 に、BFD パラメータのデフォルト設定を示します。

表 5-1 デフォルトの BFD パラメータ

パラメータ	デフォルト
BFD 機能	ディセーブル
必要最小受信間隔	50 ミリ秒
目的の最小送信間隔	50 ミリ秒
検出乗数	3
エコー機能	イネーブル
モード	非同期
Port-channel	論理モード (送信元/宛先ペアのアドレスごとに 1 セッション)
slow timer	2000 ミリ秒

BFD の設定

この項では、次のトピックについて取り上げます。

- 「設定階層」 (P.5-7)
- 「BFD 設定のタスク フロー」 (P.5-7)
- 「BFD 機能のイネーブル化」 (P.5-7)
- 「グローバルな BFD パラメータの設定」 (P.5-8)
- 「インターフェイスでの BFD の設定」 (P.5-9)
- 「ポート チャンネルの BFD の設定」 (P.5-11)
- 「BFD エコー機能の設定」 (P.5-12)
- 「ルーティング プロトコルに対する BFD サポートの設定」 (P.5-14)

設定階層

グローバル レベルおよびインターフェイス レベルで BFD を設定できます。インターフェイス コンフィギュレーションはグローバル コンフィギュレーションよりも優先されます。

ポート チャネルのメンバである物理ポートについては、メンバ ポートはマスター ポート チャネルの BFD 設定を継承します。

BFD 設定のタスク フロー

BFD の設定には、次の作業を行います。

-
- ステップ 1 **BFD 機能のイネーブル化。**
 - ステップ 2 **グローバルな BFD パラメータの設定またはインターフェイスでの BFD の設定。**
-

BFD 機能のイネーブル化

インターフェイスとプロトコルの BFD を設定する前に、BFD 機能をイネーブルにする必要があります。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	feature bfd 例： switch(config)# feature bfd	BFD 機能をイネーブルにします。
ステップ 3	show feature include bfd 例： switch(config)# show feature include bfd	(任意) イネーブルおよびディセーブルにされた機能を表示します。

	コマンド	目的
ステップ 4	copy running-config startup-config 例: <pre>switch(config)# copy running-config startup-config</pre>	(任意) この設定の変更を保存します。

no feature bfd コマンドを使用して、BFD 機能をディセーブルにし、関連するコンフィギュレーションをすべて削除します。

	コマンド	目的
	no feature bfd 例: <pre>switch(config)# no feature bfd</pre>	BFD 機能をディセーブルにして、関連するすべての設定を削除します。

グローバルな BFD パラメータの設定

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

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

はじめる前に

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	bfd interval mintx min_rx msec multiplier value 例： switch(config)# bfd interval 50 min_rx 50 multiplier 3	デバイスのすべての BFD セッションの BFD セッションパラメータを設定します。インターフェイスで BFD セッションパラメータを設定することにより、このコマンドでこれらの値を無効にすることができます。 <i>mintx</i> および <i>msec</i> の範囲は 50 ~ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ~ 50 です。乗数のデフォルトは 3 です。
ステップ 3	bfd slow-timer [interval] 例： switch(config)# bfd slow-timer 2000	エコー機能で使用される slow timer を設定します。この値は、エコー機能がイネーブルの場合、BFD が新しいセッションを開始する速度および非同期セッションが BFD 制御パケットに使用する速度を決定します。slow-timer 値は新しい制御パケット間隔として使用されますが、エコーパケットは設定された BFD 間隔を使用します。エコーパケットはリンク障害検出に使用されますが、低速の制御パケットは BFD セッションを維持します。指定できる範囲は 1000 ~ 30000 ミリ秒です。デフォルトは 2000 です。
ステップ 4	bfd echo-interface loopback interface number 例： switch(config-if)# bfd echo-interface loopback 1 3	双方向フォワーディング検出 (BFD) のエコーフレームに使用するインターフェイスを設定します。このコマンドは、指定されたループバックインターフェイスで設定されるアドレスに、エコーパケットの送信元アドレスを変更します。指定できるインターフェイス番号の範囲は 0 ~ 1023 です。
ステップ 5	show running-config bfd 例： switch(config)# show running-config bfd	(任意) BFD 実行コンフィギュレーションを表示します。
ステップ 6	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) この設定の変更を保存します。

インターフェイスでの BFD の設定

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

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

はじめる前に

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

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

手順の概要

1. **configure terminal**
2. **interface int-if**
3. **bfd interval mintx min_rx msec multiplier value**
4. (任意) **bfd authentication keyed-sha1 keyid id key ascii_key**
5. (任意) **show running-config bfd**
6. (任意) **copy running-config startup-config**

手順の詳細

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

	コマンド	目的
ステップ 5	show running-config bfd 例： switch(config-if)# show running-config bfd	(任意) BFD 実行コンフィギュレーションを表示します。
ステップ 6	copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	(任意) この設定の変更を保存します。

ポート チャネルの BFD の設定

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

この設定は、設定されたポート チャネルのグローバル セッション パラメータより優先されません。ポート チャネルのメンバポートは、ポート チャネルの BFD セッション パラメータを継承します。



(注)

ポート チャネル メンバがフラップすると、ポート チャネルの BFD セッションがフラップする場合があります。

はじめる前に

BFD をイネーブルにする前に、ポート チャネルの Link Aggregation Control Protocol (LACP) がイネーブルにされていることを確認します。

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

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

手順の概要

1. **configure terminal**
2. **interface port-channel *number***
3. **bfd per-link**
4. (任意) **bfd interval *mintx min_rx msec multiplier value***
5. (任意) **bfd authentication keyed-sha1 *keyid id key ascii_key***
6. (任意) **show running-config bfd**
7. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel number 例: switch(config)# interface port-channel 2 switch(config-if)#	ポート チャネル コンフィギュレーション モードを開始します。? キーワードを使用してサポートされている番号の範囲を表示します。
ステップ 3	bfd per-link 例: switch(config-if)# bfd per-link	ポート チャネルのリンクごとに BFD セッションを設定します。
ステップ 4	bfd interval mintx min_rx msec multiplier value 例: switch(config-if)# bfd interval 50 min_rx 50 multiplier 3	(任意) ポート チャネルのすべての BFD セッションの BFD セッション パラメータを設定します。このコマンドはグローバルな BFD セッション パラメータより優先されます。mintx および msec の範囲は 50 ~ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ~ 50 です。乗数のデフォルトは 3 です。
ステップ 5	bfd authentication keyed-sha1 keyid id key ascii_key 例: switch(config-if)# bfd authentication keyed-sha1 keyid 1 ascii_key cisco123	(任意) インターフェイス上のすべての BFD セッションの SHA-1 認証を設定します。ascii_key 文字列は BFD ピア間で共有される秘密キーです。0 ~ 255 の数値の id 値が、この特定の ascii_key に割り当てられます。BFD パケットは id でキーを指定し、複数のアクティブ キーが使用できます。 インターフェイスの SHA-1 認証をディセーブルにするには、コマンドの no 形式を使用します。
ステップ 6	show running-config bfd 例: switch(config-if)# show running-config bfd	(任意) BFD 実行コンフィギュレーションを表示します。
ステップ 7	copy running-config startup-config 例: switch(config-if)# copy running-config startup-config	(任意) この設定の変更を保存します。

BFD エコー機能の設定

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

はじめる前に

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

BFD セッションパラメータを設定します。「[グローバルな BFD パラメータの設定](#)」(P.5-8) または「[インターフェイスでの BFD の設定](#)」(P.5-9) を参照してください。

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

同一の送信元アドレスおよび宛先アドレスを調べる IP パケット検証チェックがディセーブルになっていることを確認します。 **no hardware ip verify address identical** コマンドを使用します。このコマンドの詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	bfd slow-timer echo-interval 例: switch(config)# bfd slow-timer 2000	エコー機能で使用される slow timer を設定します。この値は BFD が新しいセッションを開始する速度を決定し、BFD エコー機能がイネーブルの場合に非同期セッションの速度を低下させるために使用されます。この値は、エコー機能がイネーブルの場合、必要最小受信間隔より優先されます。指定できる範囲は 1000 ~ 30000 ミリ秒です。デフォルトは 2000 です。
ステップ 3	interface int-if 例: switch(config)# interface ethernet 2/1 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。キーワードを使用して、サポートされているインターフェイスを表示します。
ステップ 4	bfd echo 例: switch(config-if)# bfd echo	エコー機能をイネーブルにします。デフォルトではイネーブルになっています。

	コマンド	目的
ステップ 5	show running-config bfd 例: switch(config-if)# show running-config bfd	(任意) BFD 実行コンフィギュレーションを表示します。
ステップ 6	copy running-config startup-config 例: switch(config-if)# copy running-config startup-config	(任意) この設定の変更を保存します。

ルーティング プロトコルに対する BFD サポート の設定

この項では、次のトピックについて取り上げます。

- 「BGP での BFD の設定」 (P.5-14)
- 「EIGRP 上での BFD の設定」 (P.5-15)
- 「OSPF での BFD の設定」 (P.5-17)
- 「OSPFv3 での BFD の設定」 (P.5-18)
- 「IS-IS での BFD の設定」 (P.5-21)
- 「HSRP での BFD の設定」 (P.5-22)
- 「VRRP での BFD の設定」 (P.5-24)
- 「Protocol Independent Multicast (PIM) 上での BFD の設置」 (P.5-25)
- 「スタティック ルートでの BFD の設定」 (P.5-26)
- 「インターフェイスにおける BFD のディセーブル化」 (P.5-27)

BGP での BFD の設定

ボーダー ゲートウェイ プロトコル (BGP) の BFD を設定できます。

はじめる前に

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

BFD セッション パラメータを設定します。「グローバルな BFD パラメータの設定」 (P.5-8) または「インターフェイスでの BFD の設定」 (P.5-9) を参照してください。

BGP 機能をイネーブルにします。詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

手順の概要

1. **configure terminal**
2. **router bgp as-number**
3. **neighbor {ip-address | ipv6-address} remote-as as-number**
4. **bfd**

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

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例: <code>switch# configure terminal</code> <code>switch(config)#</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router bgp as-number</code> 例: <code>switch(config)# router bgp 64496</code> <code>switch(config-router)#</code>	BGP をイネーブルにして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による <code>xx.xx</code> という形式です。
ステップ 3	<code>neighbor {ip-address ipv6-address} remote-as as-number</code> 例: <code>switch(config-router)# neighbor 209.165.201.1 remote-as 64497</code> <code>switch(config-router-neighbor)#</code>	リモート BGP ピアの IPv4 アドレスまたは IPv6 アドレスおよび AS 番号を設定します。 <code>ip-address</code> の形式は <code>x.x.x.x</code> です。 <code>ipv6-address</code> の形式は <code>A:B::C:D</code> です。
ステップ 4	<code>bfd</code> 例: <code>switch(config-router-neighbor)# bfd</code>	この BGP ピアの BFD をイネーブルにします。
ステップ 5	<code>show running-config bgp</code> 例: <code>switch(config-router-neighbor)# show running-config bgp</code>	(任意) BGP 実行コンフィギュレーションを表示します。
ステップ 6	<code>copy running-config startup-config</code> 例: <code>switch(config-router-neighbor)# copy running-config startup-config</code>	(任意) この設定の変更を保存します。

EIGRP 上での BFD の設定

Enhanced Interior Gateway Routing Protocol (EIGRP) で BFD を設定できます。

はじめる前に

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

BFD セッションパラメータを設定します。「[グローバルな BFD パラメータの設定](#)」(P.5-8) または「[インターフェイスでの BFD の設定](#)」(P.5-9) を参照してください。

EIGRP 機能をイネーブルにします。詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

手順の概要

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

手順の詳細

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

	コマンド	目的
ステップ 1	copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	(任意) この設定の変更を保存します。

OSPF での BFD の設定

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

はじめる前に

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

BFD セッション パラメータを設定します。「[グローバルな BFD パラメータの設定](#)」(P.5-8) または「[インターフェイスでの BFD の設定](#)」(P.5-9) を参照してください。

OSPF 機能をイネーブルにします。詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	router ospf instance-tag 例： switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
ステップ 3	bfd 例： switch(config-router)# bfd	(任意) すべての OSPFv2 インターフェイスの BFD をイネーブルにします。

	コマンド	目的
ステップ 4	interface <i>int-if</i> 例: switch(config-router)# interface ethernet 2/1 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。キーワードを使用して、サポートされているインターフェイスを表示します。
ステップ 5	ip ospf bfd 例: switch(config-if)# ip ospf bfd	(任意) OSPFv2 インターフェイスの BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 6	show ip ospf [<i>vrf vrf-name</i>] [interface <i>if</i>] 例: switch(config-if)# show ip ospf	(任意) OSPF に関する情報を表示します。 <i>vrf-name</i> には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。
ステップ 7	copy running-config startup-config 例: switch(config-if)# copy running-config startup-config	(任意) この設定の変更を保存します。

OSPFv3 での BFD の設定

BFD は、IPv6 ネットワークのリンクステート ルーティング プロトコルである Open Shortest Path First バージョン 3 (OSPFv3) をサポートします。

OSPFv3 に対する BFD サポートをイネーブルにするには、2 つの方法があります。

- ルータ コンフィギュレーション モードで **bfd** コマンドを入力して、OSPFv3 がルーティングしているすべてのインターフェイスに対して BFD をイネーブルにできます。インターフェイス コンフィギュレーション モードで **ospfv3 bfd disable** コマンドを入力して、個々のインターフェイス上で BFD サポートをディセーブルにできます。
- インターフェイス コンフィギュレーション モードで **ospfv3 bfd** コマンドを入力して、OSPFv3 がルーティングしているインターフェイスのサブセットに対して BFD をイネーブルにできます。



(注) OSPF は、FULL ステートの OSPF ネイバーに対する BFD セッションを開始するだけです。

インターフェイスでの BFD セッションパラメータの設定

手順の概要

1. **configure terminal**
2. **interface type number**
3. **bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier**
4. **end**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface int-if 例： switch(config)# interface ethernet 2/1 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。キーワードを使用して、サポートされているインターフェイスを表示します。
ステップ 3	bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier 例： switch(config-if)# bfd interval 50 min_rx 50 multiplier 5	インターフェイスで BFD をイネーブルにします。
ステップ 4	end 例： switch(config-if)# end	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

すべてのインターフェイスでの OSPFv3 に対する BFD の設定

はじめる前に

OSPFv3 は、参加しているすべてのデバイスで実行されている必要があります。BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。

手順の概要

1. **configure terminal**
2. **router ospf process-id**
3. **bfd**
4. **exit**
5. **show bfd neighbors [details]**
6. **show ospfv3 [process-id]**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	router ospf process-id 例： switch(config)# router ospf 2	OSPFv3 ルーティング プロセスを設定します。
ステップ 3	bfd 例： switch(config-router)# bfd	ルーティング プロセスに参加するすべてのインターフェイスに対して BFD をイネーブルにします。
ステップ 4	exit 例： switch(config-router)# exit	EXEC モードに戻すには、このコマンドを 2 回入力します。
ステップ 5	show bfd neighbors [details] 例： switch# show bfd neighbors details	(任意) 既存の BFD 隣接関係の行単位のリストを表示します。
ステップ 6	show ospfv3 [process-id] 例： switch# show ospfv3	(任意) OSPFv3 ルーティング プロセスに関する一般情報を表示します。

1つ以上のインターフェイスでの OSPFv3 に対する BFD の設定

はじめる前に

OSPFv3 は、参加しているすべてのデバイスで実行されている必要があります。BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。

手順の概要

1. **configure terminal**
2. **interface type number**
3. **ospfv3 bfd [disable]**
4. **exit**
5. **show bfd neighbors [details]**
6. **show ospfv3 [process-id]**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface int-if 例： switch(config)# interface Ethernet 2/1	インターフェイスのタイプと番号を指定し、デバイスをインターフェイスコンフィギュレーションモードにします。
ステップ 3	ospfv3 bfd [disable] 例： switch(config-router)# ospfv3 bfd	OSPFv3 ルーティング プロセスに関連付けられた1つ以上のインターフェイスに対して、インターフェイスごとに BFD をイネーブルにします。
ステップ 4	exit 例： switch(config-if)# exit	EXEC モードに戻すには、このコマンドを2回入力します。
ステップ 5	show bfd neighbors [details] 例： switch# show bfd neighbors details	(任意) 既存の BFD 隣接関係の行単位のリストを表示します。
ステップ 6	show ospfv3 [process-id] 例： switch# show ospfv3	(任意) OSPFv3 ルーティング プロセスに関する一般情報を表示します。

IS-IS での BFD の設定

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

はじめる前に

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

BFD セッションパラメータを設定します。「[グローバルな BFD パラメータの設定](#)」(P.5-8) または「[インターフェイスでの BFD の設定](#)」(P.5-9) を参照してください。

IS-IS 機能をイネーブルにします。詳細については、『[Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide](#)』を参照してください。

手順の概要

1. **configure terminal**
2. **router isis instance-tag**
3. **bfd**
4. **interface int-if**
5. (任意) **isis bfd**

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

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例: <code>switch# configure terminal</code> <code>switch(config)#</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router isis instance-tag</code> 例: <code>switch(config)# router isis Enterprise</code> <code>switch(config-router)#</code>	<code>instance tag</code> を設定して、新しい IS-IS インスタンスを作成します。
ステップ 3	<code>bfd</code> 例: <code>switch(config-router)# bfd</code>	(任意) すべての OSPFv2 インターフェイスの BFD をイネーブルにします。
ステップ 4	<code>interface int-if</code> 例: <code>switch(config-router)# interface ethernet 2/1</code> <code>switch(config-if)#</code>	インターフェイス コンフィギュレーション モードを開始します。キーワードを使用して、サポートされているインターフェイスを表示します。
ステップ 5	<code>isis bfd</code> 例: <code>switch(config-if)# isis bfd</code>	(任意) IS-IS インターフェイスの BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 6	<code>show isis [vrf vrf-name] [interface if]</code> 例: <code>switch(config-if)# show isis</code>	(任意) IS-IS に関する情報を表示します。 <code>vrf-name</code> には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。
ステップ 7	<code>copy running-config startup-config</code> 例: <code>switch(config-if)# copy running-config startup-config</code>	(任意) この設定の変更を保存します。

HSRP での BFD の設定

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

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

はじめる前に

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

BFD セッション パラメータを設定します。「[グローバルな BFD パラメータの設定](#)」(P.5-8) または「[インターフェイスでの BFD の設定](#)」(P.5-9) を参照してください。

HSRP 機能をイネーブルにします。詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

手順の概要

1. **configure terminal**
2. **hsrp bfd all-interfaces**
3. **interface int-if**
4. (任意) **hsrp bfd**
5. (任意) **show running-config hsrp**
6. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 1	hsrp bfd all-interfaces 例: switch# hsrp bfd all-interfaces	(任意) すべての HSRP インターフェイスで BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 2	interface int-if 例: switch(config)# interface ethernet 2/1 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。キーワードを使用して、サポートされているインターフェイスを表示します。
ステップ 3	hsrp bfd 例: switch(config-if)# hsrp bfd	(任意) HSRP インターフェイスの BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 4	show running-config hsrp 例: switch(config-if)# show running-config hsrp	(任意) HSRP 実行コンフィギュレーションを表示します。
ステップ 5	copy running-config startup-config 例: switch(config-if)# copy running-config startup-config	(任意) この設定の変更を保存します。

VRRP での BFD の設定

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

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

はじめる前に

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

BFD セッション パラメータを設定します。「[グローバルな BFD パラメータの設定](#)」(P.5-8) または「[インターフェイスでの BFD の設定](#)」(P.5-9) を参照してください。

VRRP 機能をイネーブルにします。詳細については、『[Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide](#)』を参照してください。

手順の概要

1. **configure terminal**
2. **interface int-if**
3. **vrrp group-no**
4. **vrrp bfd address**
5. (任意) **show running-config vrrp**
6. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface int-if 例: switch(config)# interface ethernet 2/1 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。キーワードを使用して、サポートされているインターフェイスを表示します。
ステップ 3	vrrp group-no 例: switch(config-if)# vrrp group-no	VRRP グループ番号を指定します。
ステップ 4	vrrp bfd address 例: switch(config-if)# vrrp bfd	VRRP インターフェイスで BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。

	コマンド	目的
ステップ 5	show running-config vrrp 例： switch(config-if)# show running-config vrrp	(任意) VRRP 実行コンフィギュレーションを表示します。
ステップ 6	copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	(任意) この設定の変更を保存します。

Protocol Independent Multicast (PIM) 上での BFD の設置

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

はじめる前に

BFD 機能をイネーブルにします。「[BFD 機能のイネーブル化](#)」(P.5-7) を参照してください。
PIM 機能をイネーブルにします。詳細については、『*Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide*』を参照してください。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip pim bfd 例： switch(config)# ip pim bfd	PIM の BFD をイネーブルにします。
ステップ 3	interface int-if 例： switch(config)# interface ethernet 2/1 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。キーワードを使用して、サポートされているインターフェイスを表示します。

	コマンド	目的
ステップ 4	ip pim bfd-instance [<i>disable</i>] 例: switch(config-if)# ip pim bfd-instance	(任意) PIM インターフェイスの BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 5	show running-config pim 例: switch(config)# show running-config pim	(任意) PIM 実行コンフィギュレーションを表示します。
ステップ 6	copy running-config startup-config 例: switch(config)# copy running-config startup-config	(任意) この設定の変更を保存します。

スタティックルートでの BFD の設定

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

はじめる前に

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vrf context <i>vrf-name</i> 例: switch(config)# vrf context Red switch(config-vrf)#	(任意) VRF コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	<pre>ip route route interface {nh-address nh-prefix}</pre> <p>例: switch(config-vrf)# ip route 192.0.2.1 ethernet 2/1 192.0.2.4</p>	スタティック ルートを作成します。キーワードを使用して、サポートされているインターフェイスを表示します。
ステップ 4	<pre>ip route static bfd interface {nh-address nh-prefix}</pre> <p>例: switch(config-vrf)# ip route static bfd ethernet 2/1 192.0.2.4</p>	インターフェイスのすべてのスタティック ルートの BFD をイネーブルにします。キーワードを使用して、サポートされているインターフェイスを表示します。
ステップ 5	<pre>show ip route static [vrf vrf-name]</pre> <p>例: switch(config-vrf)# show ip route static vrf Red</p>	(任意) スタティック ルートを表示します。
ステップ 6	<pre>copy running-config startup-config</pre> <p>例: switch(config-vrf)# copy running-config startup-config</p>	(任意) この設定の変更を保存します。

インターフェイスにおける BFD のディセーブル化

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

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

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

BFD 相互運用性の設定

この項では、次のトピックについて取り上げます。

- 「ポイントツーポイント リンク内の Cisco NX-OS デバイスの BFD 相互運用性の設定」(P.5-28)

- 「スイッチ仮想インターフェイス内の Cisco NX-OS デバイスの BFD 相互運用性の設定」(P.5-29)
- 「BFD 設定の確認」(P.5-31)

ポイントツーポイント リンク内の Cisco NX-OS デバイスの BFD 相互運用性の設定

手順の概要

1. `configuration terminal`
2. `interface if-type`
3. `ip ospf bfd`
4. `no ip redirect`
5. `bfd interval mintx min_rx msec multiplier value`
6. `exit`

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface int-if</code> 例: switch(config)# interface ethernet 2/1 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。キーワードを使用して、サポートされているインターフェイスを表示します。
ステップ 3	<code>ip ospf bfd</code> 例: switch(config-if)# ip ospf bfd	OSPFv2 インターフェイスで BFD をイネーブルにします。デフォルトではディセーブルになっています。 OSPF は例として使用されています。サポートされている任意のプロトコルの BFD をイネーブルにできます。
ステップ 4	<code>no ip redirects</code> 例: switch(config-if)# no ip redirects	デバイスがリダイレクトを送信しないようにします。
ステップ 5	<code>bfd interval mintx min_rx msec multiplier value</code> 例: switch(config-if)# bfd interval 50 min_rx 50 multiplier 3	デバイスのすべての BFD セッションの BFD セッション パラメータを設定します。mintx および msec の範囲は 50 ~ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ~ 50 です。乗数のデフォルトは 3 です。
ステップ 6	<code>exit</code> 例: switch(config-if)# exit	インターフェイス コンフィギュレーション モードを終了し、EXEC モードに戻ります。

スイッチ仮想インターフェイス内の Cisco NX-OS デバイスの BFD 相互運用性の設定

手順の概要

1. `configuration terminal`
2. `interface vlan vlan-id`
3. `bfd interval mintx min_rx msec multiplier value`
4. `no ip redirect`
5. `ip address ip-address/length`
6. `ip ospf bfd`
7. `exit`

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface vlan vlan-id</code> 例： switch(config)# interface vlan 998 switch(config-if)#	ダイナミック スイッチ仮想インターフェイス (SVI) を作成します。
ステップ 3	<code>bfd interval mintx min_rx msec multiplier value</code> 例： switch(config-if)# bfd interval 50 min_rx 50 multiplier 3	デバイスのすべての BFD セッションの BFD セッション パラメータを設定します。mintx および msec の範囲は 50 ~ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ~ 50 です。乗数のデフォルトは 3 です。
ステップ 4	<code>no ip redirects</code> 例： switch(config-if)# no ip redirects	デバイスがリダイレクトを送信しないようにします。
ステップ 5	<code>ip address ip-address/length</code> 例： switch(config-if)# ip address 10.1.0.253/24	このインターフェイスの IP アドレスを設定します。
ステップ 6	<code>ip ospf bfd</code> 例： switch(config-if)# ip ospf bfd	OSPFv2 インターフェイスで BFD をイネーブ爾またはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 7	<code>exit</code> 例： switch(config-if)# exit	インターフェイス コンフィギュレーション モードを終了し、EXEC モードに戻ります。

論理モードの Cisco NX-OS デバイスの BFD 相互運用性の設定

手順の概要

1. **configuration terminal**
2. **interface type number.subinterface-id**
3. **bfd interval mintx min_rx msec multiplier value**
4. **no ip redirect**
5. **ip ospf bfd**
6. **exit**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface type number.subinterface-id 例: switch(config)# interface port-channel 50.2	ポート チャネル コンフィギュレーション モードを開始します。? キーワードを使用してサポートされている番号の範囲を表示します。
ステップ 3	bfd interval mintx min_rx msec multiplier value 例: switch(config-if)# bfd interval 50 min_rx 50 multiplier 3	デバイスのすべての BFD セッションの BFD セッション パラメータを設定します。mintx および msec の範囲は 50 ~ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ~ 50 です。乗数のデフォルトは 3 です。
ステップ 4	no ip redirects 例: switch(config-if)# no ip redirects	デバイスがリダイレクトを送信しないようにします。
ステップ 5	ip ospf bfd 例: switch(config-if)# ip ospf bfd	OSPFv2 インターフェイスで BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 6	exit 例: switch(config-if)# exit	インターフェイス コンフィギュレーション モードを終了し、EXEC モードに戻ります。

Cisco Nexus 9000 シリーズ デバイスでの BFD 相互運用性の確認

次に、Cisco Nexus 9000 シリーズ デバイス上で BFD 相互運用性を確認する例を示します。

```
switch# show bfd neighbors details
OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int
Vrf
10.1.1.1 10.1.1.2 1140850707/2147418093 Up 6393(4) Up Vlan2121
デフォルト
Session state is Up and using echo function with 50 ms interval
Local Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: None
```

```

MinTxInt: 50000 us, MinRxInt: 2000000 us, Multiplier: 3
Received MinRxInt: 2000000 us, Received Multiplier: 4
Holddown (hits): 8000 ms (0), Hello (hits): 2000 ms (108)
Rx Count: 92, Rx Interval (ms) min/max/avg: 347/1996/1776 last: 1606 ms ago
Tx Count: 108, Tx Interval (ms) min/max/avg: 1515/1515/1515 last: 1233 ms ago
Registered protocols: ospf
Uptime: 0 days 0 hrs 2 mins 44 secs
Last packet: Version: 1 - Diagnostic: 0
State bit: Up - Demand bit: 0
Poll bit: 0 - Final bit: 0
Multiplier: 4 - Length: 24
My Discr.: 2147418093 - Your Discr.: 1140850707
Min tx interval: 2000000 - Min rx interval: 2000000
Min Echo interval: 1000 - Authentication bit: 0
Hosting LC: 10, Down reason: None, Reason not-hosted: None

```

```

switch# show bfd neighbors details
OurAddr NeighAddr LD/RD RH/RS Holddown(mult) State Int
Vrf
10.0.2.1 10.0.2.2 1140850695/131083 Up 270(3) Up Po14.121
デフォルト
Session state is UP and not using echo function
Local Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: None
MinTxInt: 50000 us, MinRxInt: 50000 us, Multiplier: 3
Received MinRxInt: 100000 us, Received Multiplier: 3
Holddown (hits): 300 ms (0), Hello (hits): 100 ms (3136283)
Rx Count: 2669290, Rx Interval (ms) min/max/avg: 12/1999/93 last: 29 ms ago
Tx Count: 3136283, Tx Interval (ms) min/max/avg: 77/77/77 last: 76 ms ago
Registered protocols: ospf
Uptime: 2 days 21 hrs 41 mins 45 secs
Last packet: Version: 1 - Diagnostic: 0
State bit: Up - Demand bit: 0
Poll bit: 0 - Final bit: 0
Multiplier: 3 - Length: 24
My Discr.: 131083 - Your Discr.: 1140850695
Min tx interval: 100000 - Min rx interval: 100000
Min Echo interval: 0 - Authentication bit: 0
Hosting LC: 8, Down reason: None, Reason not-hosted: None

```

BFD 設定の確認

BFD 設定情報を表示するには、次の作業のいずれかを行います。

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

BFDのモニタ

BFDを表示するには、次のコマンドを使用します。

コマンド	目的
<code>show bfd neighbors [application name] [details]</code>	BGPやOSPFv2などのサポートされるアプリケーションのBFDに関する情報を表示します。
<code>show bfd neighbors [interface int-if] [details]</code>	インターフェイスのBGPセッションに関する情報を表示します。
<code>show bfd neighbors [dest-ip ip-address] [src-ip ip-address] [details]</code>	インターフェイス上の指定されたBGPセッションに関する情報を表示します。
<code>show bfd neighbors [vrf vrf-name] [details]</code>	VRFのBFDに関する情報を表示します。

BFDの設定例

次に、デフォルト BFD セッション パラメータを使用した、Ethernet 2/1 上の OSPFv2 の BFD 設定例を示します。

```
feature bfd
feature ospf
router ospf Test1
interface ethernet 2/1
  ip ospf bfd
  no shutdown
```

次に、デフォルト BFD セッション パラメータを使用した、EIGRP インターフェイスの BFD 設定例を示します。

```
feature bfd
feature eigrp
bfd interval 100 min_rx 100 multiplier 4
router eigrp Test2
  bfd
```

その他の関連資料

BFDの実装に関する詳細は、次の各項を参照してください。

- 「関連資料」(P.5-33)
- 「RFC」(P.5-33)

関連資料

関連項目	マニュアル タイトル
BFD コマンド	『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』

RFC

RFC	タイトル
RFC 5880	『Bidirectional Forwarding Detection (BFD)』
RFC 5881	『BFD for IPv4 and IPv6 (Single Hop)』



ポート チャンネルの設定

この章は、ポート チャンネルをより効率的に利用するために、ポート チャンネルを設定し、Link Aggregation Control Protocol (LACP) を適用および設定する方法について説明しています。

単一のスイッチでは、物理スイッチ上のすべてのポート チャンネル メンバー間で、ポート チャンネルの互換性パラメータが同一である必要があります。

この章は、次の項で構成されています。

- 「ポート チャンネルについて」 (P.6-1)
- 「ポート チャンネリングのライセンス要件」 (P.6-13)
- 「ポート チャンネリングの前提条件」 (P.6-13)
- 「注意事項と制約事項」 (P.6-13)
- 「デフォルト設定」 (P.6-14)
- 「ポート チャンネルの設定」 (P.6-14)
- 「ポートチャンネル設定の確認」 (P.6-42)
- 「ポート チャンネル インターフェイス コンフィギュレーションのモニタリング」 (P.6-43)
- 「その他の関連資料」 (P.6-44)

ポート チャンネルについて

ポート チャンネルは複数の物理インターフェイスの集合体で、論理インターフェイスを作成します。1つのポート チャンネルに最大 32 つの個別アクティブ リンクをバンドルして、帯域幅と冗長性を向上させることができます。ポート チャンネリングはまた、これらの物理インターフェイス全体でトラフィックのロード バランシングも行います。ポート チャンネルの物理インターフェイスが少なくとも 1 つ動作していれば、そのポート チャンネルは動作しています。

レイヤ 2 ポート チャンネルに適合するレイヤ 2 インターフェイスをバンドルすれば、レイヤ 2 ポート チャンネルを作成できます。レイヤ 3 ポート チャン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 チャンネルを作成できます。レイヤ 2 インターフェイスとレイヤ 3 インターフェイスを同一のポート チャンネルで組み合わせることはできません。

ポート セキュリティをポート チャンネルに適用できます。ポート セキュリティについては、『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』を参照してください。

ポート チャンネルをレイヤ 3 からレイヤ 2 に変更することもできます。レイヤ 2 インターフェイスの作成手順については、第 3 章「レイヤ 2 インターフェイスの設定」を参照してください。

変更した設定をポートチャネルに適用すると、そのポートチャネルのメンバーインターフェイスにもそれぞれ変更が適用されます。たとえば、スパンニングツリープロトコル (STP) パラメータをポートチャネルに設定すると、Cisco NX-OS ソフトウェアはこれらのパラメータをポートチャネルのそれぞれのインターフェイスに適用します。



(注)

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

集約プロトコルが関連付けられていない場合でもスタティックポートチャネルを使用して設定を簡略化できます。

柔軟性を高めたい場合は LACP を使用できます。Link Aggregation Control Protocol (LACP) は IEEE 802.3ad で定義されています。LACP を使用すると、リンクによってプロトコルパケットが渡されます。共有インターフェイスでは LACP を設定できません。

LACP については、「[LACP の概要](#)」(P.6-7) を参照してください。

この項では、次のトピックについて取り上げます。

- 「[ポートチャネル](#)」(P.6-2)
- 「[ポートチャネルインターフェイス](#)」(P.6-3)
- 「[基本設定](#)」(P.6-4)
- 「[互換性要件](#)」(P.6-4)
- 「[ポートチャネルを使ったロードバランシング](#)」(P.6-6)
- 「[LACP](#)」(P.6-7)
- 「[仮想化のサポート](#)」(P.6-12)
- 「[ハイアベイラビリティ](#)」(P.6-12)

ポートチャネル

ポートチャネルは、物理リンクをまとめて 1 つのチャネルグループに入れ、M シリーズ モジュール上の最大 32 の物理リンクの帯域幅を集約した単一の論理リンク。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。

ただし、LACP をイネーブルにすればポートチャネルをより柔軟に使用できます。LACP を使ってポートチャネルを設定する場合とスタティックポートチャネルを使って設定する場合は、手順が多少異なります（「[ポートチャネルの設定](#)」(P.6-14) を参照）。



(注)

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

各ポートにはポートチャネルが 1 つだけあります。ポートチャネルのすべてのポートには互換性があり、同じ速度とデュプレックスモードを使用します（「[互換性要件](#)」(P.6-4) を参照）。集約プロトコルを使わずにスタティックポートチャネルを実行する場合、物理リンクはすべて on チャネルモードです。このモードは、LACP をイネーブルにしない限り変更できません（「[ポートチャネルモード](#)」(P.6-8) を参照）。

ポートチャネル インターフェイスを作成すると、ポートチャネルを直接作成できます。またはチャンネルグループを作成して個別ポートをバンドルに集約させることができます。インターフェイスをチャンネルグループに関連付けると、ポートチャネルがない場合は対応するポートチャネルが自動的に作成されます。この場合、ポートチャネルは最初のインターフェイスのレイヤ2またはレイヤ3設定を行います。最初にポートチャネルを作成することもできます。この場合は、Cisco NX-OS ソフトウェアがポートチャネルと同じチャンネル番号の空のチャンネルグループを作成してデフォルトレイヤ2またはレイヤ3設定を行い、互換性も設定します（「互換性要件」(P.6-4)を参照）。



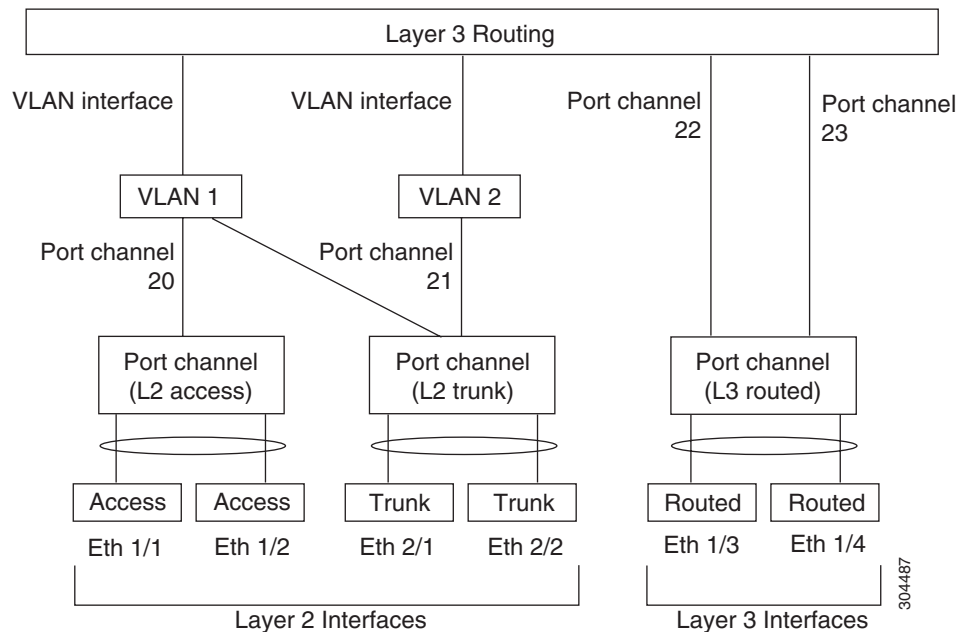
(注)

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

ポートチャネル インターフェイス

図 6-1 に、ポートチャネル インターフェイスを示します。

図 6-1 ポートチャネル インターフェイス



ポートチャネル インターフェイスは、レイヤ2またはレイヤ3 インターフェイスとして分類できます。さらに、レイヤ2ポートチャネルはアクセスモードまたはトランクモードに設定できます。レイヤ3ポートチャネル インターフェイスのチャンネルメンバにはルーテッドポートがあります。

レイヤ3ポートチャネルにスタティックMACアドレスを設定できます。この値を設定しない場合、レイヤ3ポートチャネルは、最初にアップになるチャンネルメンバのルータMACを使用します。レイヤ3ポートでスタティックMACアドレスを設定する情報については、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。

レイヤ2ポートにアクセスまたはトランクモードを設定する手順については、第3章「レイヤ2 インターフェイスの設定」を参照してください。レイヤ3 インターフェイスとサブインターフェイスを設定する手順については、第4章「レイヤ3 インターフェイスの設定」を参照してください。

基本設定

ポートチャネルインターフェイスには次の基本設定ができます。

- 帯域幅：この設定は情報目的で使用します。上位レベルプロトコルで使用されます。
- 遅延：この設定は情報目的で使用します。上位レベルプロトコルで使用されます。
- 説明
- デュプレックス
- IP アドレス
- 最大伝送単位 (MTU)
- シャットダウン
- 速度

互換性要件

チャネルグループにインターフェイスを追加する場合、ソフトウェアは特定のインターフェイス属性をチェックし、インターフェイスがチャネルグループと互換性があることを確認します。たとえば、レイヤ2チャネルグループにレイヤ3インターフェイスを追加できません。また、Cisco NX-OS ソフトウェアはインターフェイスの多数の動作属性をチェックしてから、そのインターフェイスがポートチャネル集約に参加することを許容します。

互換性チェックの対象となる動作属性は次のとおりです。

- ネットワーク層
- (リンク) 速度性能
- 速度設定
- デュプレックス性能
- デュプレックス設定
- ポートモード
- アクセス VLAN
- トランクネイティブ VLAN
- タグ付きまたは非タグ付き
- 許可 VLAN リスト
- MTU サイズ
- SPAN：SPANの始点または宛先ポートは不可
- レイヤ3ポート：サブインターフェイスは不可
- ストーム制御
- フロー制御性能

- フロー制御設定
- メディアタイプ、銅線またはファイバ

Cisco NX-OS で使用される完全な互換性チェックリストを確認するには、**show port-channel compatibility-parameters** コマンドを使用します。

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

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

- (リンク) 速度性能
- 速度設定
- デュプレックス性能
- デュプレックス設定
- フロー制御性能
- フロー制御設定

インターフェイスがポートチャネルに加入すると、個々のパラメータの一部が削除され、次のようなポートチャネルの値に置き換えられます。

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

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

- ビーコン
- 説明
- CDP
- LACP ポートプライオリティ
- デバウンス
- UDLD
- MDIX
- レートモード

- シャットダウン
- SNMPトラップ



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

ポートチャネルモードについては、「[LACP マーカーレスポング](#)」(P.6-10) を参照してください。

ポートチャネルを使ったロードバランシング

Cisco NX-OS ソフトウェアは、フレームのアドレスを数値にハッシュしてチャネルのリンクを1つ選択することで、ポートチャネルのすべての動作インターフェイス間のトラフィックをロードバランシングします。ポートチャネルはデフォルトでロードバランシングを備えています。ポートチャネルロードバランシングでは、MACアドレス、IPアドレス、またはレイヤ4ポート番号を使用してリンクを選択します。ポートチャネルロードバランシングは、送信元または宛先アドレスおよびポートの両方またはどちらか一方を使用します。

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

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

レイヤ3インターフェイスのデフォルトロードバランシングモードは、発信元および宛先IPアドレスです。非IPトラフィックのデフォルトロードバランシングモードは、送信元および宛先MACアドレスです。チャネルグループバンドルのインターフェイス間でロードバランシング方式を設定するには、**port-channel load-balance** コマンドを使用します。レイヤ2パケットのデフォルト方式は **src-dst-mac** です。レイヤ3パケットのデフォルト方式は **src-dst-ip** です。次のいずれかの方式を使用するデバイスを設定し、ポートチャネル全体をロードバランシングできます。

- 宛先 MAC アドレス
- 送信元 MAC アドレス
- 送信元および宛先 MAC アドレス
- 宛先 IP アドレス
- 送信元 IP アドレス
- 送信元および宛先 IP アドレス
- 送信元 TCP/UDP ポート番号
- 宛先 TCP/UDP ポート番号
- 送信元および宛先 TCP/UDP ポート番号

非IPおよびレイヤ3ポートチャネルはどちらも設定したロードバランシング方式に従い、発信元、宛先、または発信元および宛先パラメータを使用します。たとえば、発信元IPアドレスを使用するロードバランシングを設定すると、すべての非IPトラフィックは発信元MACアドレスを使用してトラフィックをロードバランシングしますが、レイヤ3トラフィックは発信元IPアドレスを使用してトラフィックをロードバランシングします。同様に、宛先MACアドレ

スをロード バランシング方式として設定すると、すべてのレイヤ 3 トラフィックは宛先 IP アドレスを使用しますが、非 IP トラフィックは宛先 MAC アドレスを使用してロード バランシングします。

ロード バランシングは、システム全体または特定のモジュールによって設定できます。

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

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



(注)

Cisco IOS を実行するデバイスは、**port-channel hash-distribution** コマンドによって単一のメンバーに障害が発生した場合、メンバーポート ASIC の動作を最適化できます。Cisco Nexus 9000 シリーズのデバイスはこの最適化をデフォルトで実行し、このコマンドを必要とせず、またサポートしません。Cisco NX-OS は、デバイス全体に対してであり、モジュール単位であり、**port-channel load-balance** コマンドによるポートチャネル上のロードバランシング基準のカスタマイズをサポートします。

LACP

LACP では、最大 16 のインターフェイスを 1 つのポートチャネルに設定できます。

この項では、次のトピックについて取り上げます。

- 「[LACP の概要](#)」 (P.6-7)
- 「[ポートチャネルモード](#)」 (P.6-8)
- 「[LACP ID パラメータ](#)」 (P.6-9)
- 「[LACP マーカーレスポンド](#)」 (P.6-10)
- 「[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の相違点](#)」 (P.6-11)
- 「[LACP 互換性の拡張](#)」 (P.6-11)
- 「[LACP ポートチャネルの最小リンクおよび MaxBundle](#)」 (P.6-11)

LACP の概要



(注)

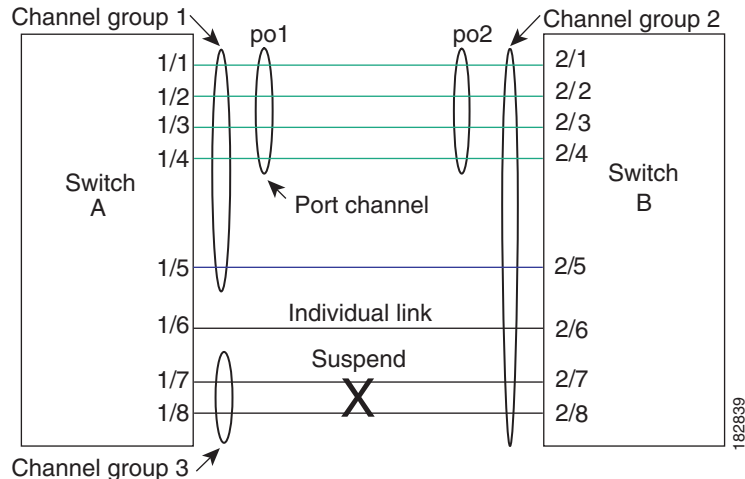
LCAP は、使用する前にイネーブルにする必要があります。デフォルトでは、LACP はディセーブルです。

LACP をイネーブルにする手順については、「[LACP のイネーブル化](#)」 (P.6-28) を参照してください。

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については、『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』を参照してください。

図 6-2 に、個別リンクを LACP ポートチャネルおよびチャネルグループに組み込み、個別リンクとして機能させる方法を示します。

図 6-2 個別リンクをポートチャネルに組み込む



LACP では、最大 16 のインターフェイスを 1 つのチャネルグループにバンドルできます。



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

LACP 設定が 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。

ポートチャネルモード

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

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



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

表 6-1 で、各チャネルモードについて説明します。

表 6-1 ポートチャネルの個別リンクのチャネルモード

チャネルモード	説明
passive	LACP モード。ポートをパッシブ ネゴシエーション ステートにします。ポートは受信した LACP パケットには応答しますが、LACP ネゴシエーションは開始しません。
active	LACP モード。ポートをアクティブ ネゴシエーション ステートにします。ポートは LACP パケットを送信して、他のポートとのネゴシエーションを開始します。
on	すべてのスタティック ポートチャネル (LACP を実行していない) がこのモードです。LACP をイネーブルにする前にチャネルモードをアクティブまたはパッシブにしようとする、デバイス表示はエラーメッセージを表示します。 チャネルで LACP をイネーブルにするには、そのチャネルのインターフェイスでチャネルモードを active または passive に設定します。LACP は、 on 状態のインターフェイスとネゴシエートする場合、LACP パケットを受信しないため、そのインターフェイスと個別のリンクを形成します。つまり、LACP チャネルグループには参加しません。 デフォルト ポートチャネルモードは on です。

LACP は、パッシブおよびアクティブモードの両方でポート間をネゴシエートして、ポート速度やトランキングステートなどを基準にしてポートチャネルを形成できるかどうかを決定します。パッシブモードは、リモートシステムやパートナーが LACP をサポートするかどうか不明の場合に役に立ちます。

次の例のようにモードに互換性がある場合、ポートの LACP モードが異なれば、ポートは LACP ポートチャネルを形成できません。

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

LACP ID パラメータ

ここでは、LACP パラメータについて次の内容を説明します。

- 「LACP システムプライオリティ」 (P.6-10)
- 「LACP ポートプライオリティ」 (P.6-10)
- 「LACP 管理キー」 (P.6-10)

LACP システムプライオリティ

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



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

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

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

LACP 管理キー

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

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

LACP マーカーレスポнда

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

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

LACP がイネーブルのポートチャネルとスタティックポートチャネルの相違点

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

表 6-2 LACP がイネーブルのポートチャネルとスタティックポートチャネル

構成	LACP がイネーブルのポートチャネル	スタティックポートチャネル
適用されるプロトコル	グローバルにイネーブル	N/A
リンクのチャネルモード	次のいずれか。 <ul style="list-style-type: none"> Active Passive 	On だけ
チャネルを構成する最大リンク数	32	32

LACP 互換性の拡張

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

Cisco Nexus 9000 シリーズのデバイスが非 Nexus ピアに接続されている場合、そのグレースフルフェールオーバーのデフォルトが、ディセーブルにされたポートがダウンになるための時間を遅らせる可能性があります。また、ピアからのトラフィックを喪失する原因にもなります。これらの状況を解決するために、**lacp graceful-convergence** コマンドが追加されました。

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

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 ポートチャネルの最小リンク機能は次の処理を実行します。

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

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

LACP MaxBundle 機能では、次の処理が行われます。

- LACP ポートチャネルのバンドルポート数の上限を定義します。

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



(注)

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

LACP 高速タイマー

LACP タイマーレートを変更することにより、LACP タイムアウトの時間を変更することができます。lACP rate コマンドを使用すれば、LACP がサポートされているインターフェイスに LACP 制御パケットを送信する際のレートを設定できます。タイムアウトレートは、デフォルトのレート（30 秒）から高速レート（1 秒）に変更することができます。このコマンドは、LACP がイネーブルになっているインターフェイスでのみサポートされます。LACP 高速時間レートを設定するには、「[LACP 高速タイマーレートの設定](#)」(P.6-33)を参照してください。

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

仮想化のサポート

メンバポートと他のポートチャネルに関連する設定は、ポートチャネルとメンバポートを持つ仮想デバイスコンテキスト（VDC）で設定します。各 VDC で 1 ~ 4096 の番号を使ってポートチャネルに番号を設定できます。

1つのポートチャネルのすべてのポートは同じ VDC に置く必要があります。LACP を使用する場合、8つすべてのアクティブポートと8つすべてのスタンバイポートは同じ VDC であることが必要です。



(注)

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

ハイアベイラビリティ

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

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

動作しているポート数が設定された最小リンク数を下回った場合、ポートチャネルはダウンします。



(注) ハイアベイラビリティ機能の詳細については、『Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide』を参照してください。

ポートチャネリングのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	ポートチャネリングにライセンスは必要ありません。ライセンスパッケージに含まれていない機能は Cisco NX-OS イメージにバンドルされており、無料で提供されます。

ポートチャネリングの前提条件

ポートチャネリングには次の前提条件があります。

- デバイスにログインしていること。
- シングルポートチャネルのすべてのポートは、レイヤ2またはレイヤ3ポートであること。
- シングルポートチャネルのすべてのポートが、互換性の要件を満たしていること。互換性の要件の詳細については、「[互換性要件](#)」(P.6-4)を参照してください。
- デフォルトVDCのロードバランシングを設定すること。

注意事項と制約事項

ポートチャネリング設定時の注意事項および制約事項は、次のとおりです。

- LACPポートチャネルの最小リンクおよびmaxbundle機能は、ホストインターフェイスポートチャネルではサポートされていません。
- この機能を使用する前にLACPをイネーブルにする必要があります。
- デバイスに複数のポートチャネルを設定できます。
- 共有および専用ポートは同じポートチャネルに設定できません（共有および専用ポートについては、[第2章「基本インターフェイスパラメータの設定」](#)を参照してください）。
- レイヤ2ポートチャネルでは、ポートに互換性が設定されていれば、STPポートパスコストが異なる場合でもポートチャネルを形成できます。互換性の要件の詳細については、「[互換性要件](#)」(P.6-4)を参照してください。
- STPでは、ポートチャネルのコストはポートメンバーの集約帯域幅に基づきます。
- ポートチャネルを設定した場合、ポートチャネルインターフェイスに適用した設定はポートチャネルメンバポートに影響を与えます。メンバポートに適用した設定は、設定を適用したメンバポートにだけ影響します。
- LACPは半二重モードをサポートしません。LACPポートチャネルの半二重ポートは中断ステートになります。

- ポートチャネルにポートを追加する前に、ポートセキュリティ情報をそのポートから削除しておく必要があります。同様に、チャンネルグループのメンバであるポートにポートセキュリティ情報を追加できません。
- ポートチャネルグループに属するポートはプライベート VLAN ポートとして設定しないでください。ポートがプライベート VLAN の設定に含まれている間は、そのポートチャネルの設定は非アクティブになります。
- チャンネルメンバポートを発信元または宛先 SPAN ポートにできません。

デフォルト設定

表 6-3 に、ポートチャネルパラメータのデフォルト設定を示します。

表 6-3 デフォルトポートチャネルパラメータ

パラメータ	デフォルト
ポートチャネル	管理アップ
レイヤ3 インターフェイスのロードバランシング方式	送信元および宛先 IP アドレス
レイヤ2 インターフェイスのロードバランシング方式	送信元および宛先 MAC アドレス
モジュールごとのロードバランシング	ディセーブル
LACP	ディセーブル
チャンネルモード	on
LACP システムプライオリティ	32768
LACP ポートプライオリティ	32768
LACP の最小リンク	1
Maxbundle	32
FEX ファブリックポートチャネル用最少リンク数	1

ポートチャネルの設定

この項では、次のトピックについて取り上げます。

- 「ポートチャネルの作成」 (P.6-15)
- 「レイヤ3 ポートをポートチャネルに追加」 (P.6-19)
- 「情報目的としての帯域幅および遅延の設定」 (P.6-21)
- 「ポートチャネルインターフェイスのシャットダウンと再起動」 (P.6-22)
- 「ポートチャネルの説明の設定」 (P.6-24)
- 「ポートチャネルを使ったロードバランシングの設定」 (P.6-27)
- 「LACP のイネーブル化」 (P.6-28)
- 「LACP ポートチャネルポートモードの設定」 (P.6-29)

- 「LACP ポートチャネルの最小リンクの設定」 (P.6-30)
- 「LACP ポートチャネル MaxBundle の設定」 (P.6-31)
- 「LACP システムプライオリティの設定」 (P.6-34)
- 「LACP ポートプライオリティの設定」 (P.6-35)
- 「LACP グレースフルコンバージェンス」 (P.6-36)
- 「LACP の個別一時停止のディセーブル化」 (P.6-38)
- 「LACP の個別一時停止の再イネーブル化」 (P.6-39)
- 「ポートチャネルハッシュ分散の設定」 (P.6-40)



(注) ポートチャネルインターフェイスに最大伝送単位 (MTU) を設定する手順については、第2章「基本インターフェイスパラメータの設定」を参照してください。ポートチャネルインターフェイスに IPv4 および IPv6 アドレスを設定する手順については、第4章「レイヤ3インターフェイスの設定」を参照してください。



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

ポートチャネルの作成

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



(注) ポートチャネルがチャンネルグループの前に作成されると、ポートチャネルは、メンバーインターフェイスが設定されるインターフェイス属性のすべてを使用して設定される必要があります。**switchport mode trunk {allowed vlan vlan-id | native vlan-id}** コマンドを使用してメンバーを設定します。これは、チャンネルグループのメンバがレイヤ2ポート (switchport) およびトランク (switchport mode trunk) の場合にのみ必要です。

はじめる前に

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

手順の概要

1. **configure terminal**
2. **interface port-channel channel-number**
3. (任意) **show port-channel summary**
4. (任意) **show interface status error policy [detail]**
5. (任意) **no shutdown**
6. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel <i>channel-number</i> 例: switch(config)# interface port-channel 1 switch(config-if)	設定するポートチャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。範囲は 1 ~ 4096 です。Cisco NX-OS ソフトウェアは、チャネルグループがない場合はそれを自動的に作成します。
ステップ 3	show port-channel summary 例: switch(config-router)# show port-channel summary	(任意) ポートチャネルに関する情報を表示します。
ステップ 4	show interface status error policy [detail] 例: switch# show interface status error policy detail	(任意) ポリシープログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェアポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、 detail コマンドを使用します。
ステップ 5	no shutdown 例: switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown	(任意) ポリシーがハードウェアポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 6	copy running-config startup-config 例: switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

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

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

次の例は、ポートチャネルの作成方法を示しています。

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

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

レイヤ2ポートをポートチャネルに追加

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

はじめる前に

LACPベースのポートチャネルにする場合はLACPをイネーブルにします。

すべてのレイヤ2メンバポートは、全二重モードで同じ速度で実行されている必要があります。

手順の概要

1. **configure terminal**
2. **interface type slot/port**
3. **switchport**
4. (任意) **switchport mode trunk**
5. (任意) **switchport trunk {allowed vlan vlan-id | native vlan-id}**
6. **channel-group channel-number [force] [mode {on | active | passive}]**
7. (任意) **show interface type slot/port**
8. (任意) **show interface status error policy [detail]**
9. (任意) **no shutdown**
10. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバルコンフィギュレーションモードを開始します。
ステップ 2	interface type slot/port 例: switch(config)# interface ethernet 1/4 switch(config-if)	チャンネルグループに追加するインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 3	switchport 例: switch(config-if)# switchport	インターフェイスをレイヤ2アクセスポートとして設定します。
ステップ 4	switchport mode trunk 例: switch(config-if)# switchport mode trunk	(任意) インターフェイスをレイヤ2トランクポートとして設定します。

	コマンド	目的
ステップ 5	<pre>switchport trunk {allowed vlan vlan-id native vlan-id}</pre> <p>例: switch(config-if)# switchport trunk native 3</p>	(任意) レイヤ2 トランク ポートに必要なパラメータを設定します。
ステップ 6	<pre>channel-group channel-number [force] [mode {on active passive}]</pre> <p>例: switch(config-if)# channel-group 5</p> <p>例: switch(config-if)# channel-group 5 force</p>	<p>チャンネルグループ内にポートを設定し、モードを設定します。channel-number の指定できる範囲は 1 ~ 4096 です。ポートチャネルがない場合は、このチャンネルグループに関連付けられたポートチャネルが作成されます。すべてのスタティックポートチャネルインターフェイスは、on モードに設定されます。すべての LACP 対応ポートチャネルインターフェイスを active または passive に設定する必要があります。デフォルトモードは on です。</p> <p>(任意) 一部の設定に互換性がないインターフェイスをチャンネルに追加します。強制されるインターフェイスは、チャンネルグループと同じ速度、デュプレックス、およびフロー制御設定を持っている必要があります。</p> <p>(注) force オプションは、ポートにポートチャネルの他のメンバーとの QoS ポリシーの不一致がある場合に失敗します。</p>
ステップ 7	<pre>show interface type slot/port</pre> <p>例: switch(config-router)# show interface port channel 5</p>	(任意) インターフェイスの内容を表示します。
ステップ 8	<pre>show interface status error policy [detail]</pre> <p>例: switch# show interface status error policy detail</p>	<p>(任意) ポリシープログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェアポリシーと一致することを確認できます。</p> <p>エラーを生成するインターフェイスの詳細を表示するには、detail コマンドを使用します。</p>
ステップ 9	<pre>no shutdown</pre> <p>例: switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown</p>	(任意) ポリシーがハードウェアポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 10	<pre>copy running-config startup-config</pre> <p>例: switch(config)# copy running-config startup-config</p>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

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

コマンド	目的
<pre>no channel-group</pre> <p>例:</p> <pre>switch(config)# no channel-group</pre>	チャンネルグループからポートを削除します。

次に、レイヤ2イーサネットインターフェイス1/4をチャンネルグループ5に追加する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# switchport
switch(config-if)# channel-group 5
```

レイヤ3ポートをポートチャネルに追加

新しいチャンネルグループまたはすでにレイヤ3ポートが設定されているチャンネルグループにレイヤ3ポートを追加できます。ポートチャネルがない場合は、このチャンネルグループに関連付けられたポートチャネルが作成されます。

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

はじめる前に

LACPベースのポートチャネルにする場合はLACPをイネーブルにします。

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

手順の概要

1. **configure terminal**
2. **interface type slot/port**
3. **no switchport**
4. **channel-group channel-number [force] [mode {on | active | passive}]**
5. (任意) **show interface type slot/port**
6. (任意) **show interface status error policy [detail]**
7. (任意) **no shutdown**
8. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface type slot/port 例: switch(config)# interface ethernet 1/4 switch(config-if)	チャネルグループに追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	no switchport 例: switch(config-if)# no switchport	インターフェイスをレイヤ 3 ポートとして設定します。
ステップ 4	channel-group channel-number [force] [mode {on active passive}] 例: switch(config-if)# channel-group 5 例: switch(config-if)# channel-group 5 force	チャネルグループ内にポートを設定し、モードを設定します。channel-number の指定できる範囲は 1 ~ 4096 です。ポートチャネルがない場合は、Cisco NX-OS ソフトウェアによってこのチャネルグループに関連付けられたポートチャネルが作成されます。 (任意) 一部の設定に互換性がないインターフェイスをチャネルに追加します。強制されるインターフェイスは、チャネルグループと同じ速度、デュプレックス、およびフロー制御設定を持っている必要があります。
ステップ 5	show interface type slot/port 例: switch(config-router)# show interface ethernet 1/4	(任意) インターフェイスの内容を表示します。
ステップ 6	show interface status error policy [detail] 例: switch# show interface status error policy detail	(任意) ポリシープログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェアポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、 detail コマンドを使用します。
ステップ 7	no shutdown 例: switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown	(任意) ポリシーがハードウェアポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 8	copy running-config startup-config 例: switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

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

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

次に、レイヤ 3 イーサネット インターフェイス 1/5 を on モードのチャンネルグループ 6 に追加する例を示します。

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

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

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

情報目的としての帯域幅および遅延の設定

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel channel-number 例: switch(config)# interface port-channel 2 switch(config-if)	設定するポートチャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	bandwidth value 例: switch(config-if)# bandwidth 60000000 switch(config-if)#	情報目的で使用される帯域幅を指定します。有効な範囲は 1 ~ 80,000,000 kbs です。デフォルト値はチャネルグループのアクティブ インターフェイスの合計によって異なります。
ステップ 4	delay value 例: switch(config-if)# delay 10000 switch(config-if)#	情報目的で使用されるスループット遅延を指定します。範囲は、1 ~ 16,777,215 (10 マイクロ秒単位) です。デフォルト値は 10 マイクロ秒です。 (注) Cisco リリース 4.2(1) より前は、デフォルトの遅延値が 100 マイクロ秒でした。
ステップ 5	exit 例: switch(config-if)# exit switch(config)#	インターフェイス モードを終了し、コンフィギュレーション モードに戻ります。
ステップ 6	show interface port-channel channel-number 例: switch(config-router)# show interface port-channel 2	(任意) 指定したポートチャネルのインターフェイス情報を表示します。
ステップ 7	copy running-config startup-config 例: switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、ポートチャネル 5 の帯域幅および遅延の情報パラメータを設定する例を示します。

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

ポートチャネル インターフェイスのシャットダウンと再起動

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

手順の概要

1. **configure terminal**
2. **interface port-channel** *channel-number*
3. **shutdown** | **no shutdown**
4. **exit**
5. (任意) **show interface port-channel** *channel-number*
6. (任意) **show interface status error policy** [**detail**]
7. (任意) **no shutdown**
8. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel <i>channel-number</i> 例： switch(config)# interface port-channel 2 switch(config-if)#	設定するポートチャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	shutdown 例： switch(config-if)# shutdown switch(config-if)#	インターフェイスをシャットダウンします。トラフィックは通過せず、インターフェイスは管理ダウン状態になります。デフォルトは no shutdown です。
	no shutdown 例： switch(config-if)# no shutdown switch(config-if)#	インターフェイスを開きます。インターフェイスは管理的にアップとなります。操作上の問題がなければ、トラフィックが通過します。デフォルトは no shutdown です。
ステップ 4	exit 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了し、コンフィギュレーション モードに戻ります。
ステップ 5	show interface port-channel <i>channel-number</i> 例： switch(config-router)# show interface port-channel 2	(任意) 指定したポートチャネルのインターフェイス情報を表示します。
ステップ 6	show interface status error policy [detail] 例： switch# show interface status error policy detail	(任意) ポリシー プログラミング中にエラーを生成するインターフェイスおよび VLAN が表示され、ポリシーがハードウェア ポリシーと一致することを確認できます。 エラーを生成するインターフェイスの詳細を表示するには、 detail コマンドを使用します。

	コマンド	目的
ステップ 7	no shutdown 例: <pre>switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown</pre>	(任意) ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは <code>error-disabled</code> ポリシー状態になります。
ステップ 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。

次に、ポートチャネル 2 のインターフェイスをアップする例を示します。

```
switch# configure terminal
switch (config)# interface port-channel 2
switch(config-if)# no shutdown
```

ポートチャネルの説明の設定

ポートチャネルの説明を設定できます。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel <i>channel-number</i> 例: <pre>switch(config)# interface port-channel 2 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。

	コマンド	目的
ステップ 3	description 例: <pre>switch(config-if)# description engineering switch(config-if)#</pre>	ポートチャネルインターフェイスに説明を追加できます。説明に 80 文字まで使用できます。デフォルトでは、説明は表示されません。このパラメータを設定してから、出力に説明を表示する必要があります。
ステップ 4	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、コンフィギュレーションモードに戻ります。
ステップ 5	show interface port-channel <i>channel-number</i> 例: <pre>switch(config-router)# show interface port-channel 2</pre>	(任意) 指定したポートチャネルのインターフェイス情報を表示します。
ステップ 6	copy running-config startup-config 例: <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

次に、ポートチャネル 2 に説明を追加する例を示します。

```
switch# configure terminal
switch (config)# interface port-channel 2
switch(config-if)# description engineering
```

ポートチャネルインターフェイスへの速度とデュプレックスの設定

ポートチャネルインターフェイスに速度とデュプレックスを設定できます。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel channel-number 例: switch(config)# interface port-channel 2 switch(config-if)	設定するポートチャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	speed {10 100 1000 auto} 例: switch(config-if)# speed auto switch(config-if)#	ポートチャネル インターフェイスの速度を設定します。デフォルトの自動ネゴシエーションは auto です。
ステップ 4	duplex {auto full half} 例: switch(config-if)# speed auto switch(config-if)#	ポートチャネル インターフェイスのデュプレックスを設定します。デフォルトの自動ネゴシエーションは auto です。
ステップ 5	exit 例: switch(config-if)# exit switch(config)#	インターフェイス モードを終了し、コンフィギュレーション モードに戻ります。
ステップ 6	show interface port-channel channel-number 例: switch(config-router)# show interface port-channel 2	(任意) 指定したポートチャネルのインターフェイス情報を表示します。
ステップ 7	copy running-config startup-config 例: switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、ポートチャネル 2 に 100 Mb/s を設定する例を示します。

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


ポートチャネルを使ったロードバランシングの設定

VDC アソシエーションにかかわらず、ポートチャネルのロードバランシングアルゴリズムを設定し、デバイス全体または1のモジュールだけに適用できます。モジュールベースのロードバランシングは、デバイスベースのロードバランシングに優先します。

はじめる前に

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

手順の概要

1. `configure terminal`
2. `[no] port-channel load-balance method {dst ip | dst ip-port-vlan | dst ip-vlan | dst mac | dst port | src-dst ip | src-dst ip-l4port | source-dst mac | source-dst port | src-ip port | src-ip-port-vlan | src ip-vlan | src mac | src-port | hash-modulo [force]} [module module-number | fex {fex-range | all}] [asymmetric] [rotate rotate]`
3. (任意) `show port-channel load-balance`
4. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<pre>configure terminal</pre> <p>例:</p> <pre>switch# configure terminal switch(config)#</pre>	<p>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。</p>
ステップ 2	<pre>port-channel load-balance method {dst ip dst ip-port-vlan dst ip-vlan dst mac dst port src-dst ip source-dst mac source-dst port src-ip port src-dst ip-l4port src-ip-port-vlan src ip-vlan src mac src-port hash-modulo [force]} [module module-number fex {fex-range all}] [asymmetric] [rotate rotate]</pre> <p>例:</p> <pre>switch(config)# port-channel load-balance src-dst mac asymmetric switch(config)#</pre> <p>例:</p> <pre>switch(config)# no port-channel load-balance src-dst mac asymmetric switch(config)#</pre> <p>例:</p> <pre>switch(config)# no port-channel load-balance src-dst mac asymmetric module 1 switch(config)#</pre>	<p>デバイスまたはモジュールのロードバランシングアルゴリズムを指定します。指定可能なアルゴリズムはデバイスによって異なります。レイヤ3のデフォルトはIPv4とIPv6の両方で src-dst-ip で、非IPのデフォルトは src-dst-mac です。</p> <p>デフォルトのシステム設定（対称）に戻るには、no port-channel load-balance src-dst mac asymmetric コマンドを使用します。</p> <p>(注) モジュールベースの設定がすでに存在する場合は、それがデフォルトのシステム設定よりも優先されます。</p> <p>システムレベルの設定（対称）に戻るには、モジュールレベルで no port-channel load-balance src-dst mac asymmetric module コマンドを使用します。</p>

	コマンド	目的
ステップ 3	<code>show port-channel load-balance</code> 例: switch(config-router)# show port-channel load-balance	(任意) ポートチャネルロードバランシングアルゴリズムを表示します。
ステップ 4	<code>copy running-config startup-config</code> 例: switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

デフォルトのロードバランシングアルゴリズムである、非 IP トラフィック用の `source-dest-mac`、および IP トラフィック用の `source-dest-ip` を復元するには、**no port-channel load-balance** コマンドを使用します。

コマンド	目的
<code>no port-channel load-balance</code> 例: switch(config)# no port-channel load-balance	デフォルトのロードバランシングアルゴリズムを復元します。

次に、モジュール 5 のポートチャネルに発信元 IP ロードバランシングを設定する例を示します。

```
switch# configure terminal
switch (config)# port-channel load-balance src-ip-port module 5
```

LACP のイネーブル化

LACP はデフォルトではディセーブルです。LACP の設定を開始するには、LACP をイネーブルにする必要があります。LACP 設定が 1 つでも存在する限り、LACP をディセーブルにはできません。

LACP は、LAN ポートグループの機能を動的に学習し、残りの LAN ポートに通知します。LACP は、正確に一致しているイーサネットリンクを識別すると、リンクを 1 つのポートチャネルとしてまとめます。次に、ポートチャネルは単ブリッジポートとしてスパンニングツリーに追加されます。

LACP を設定する手順は次のとおりです。

- LACP をグローバルにイネーブルにするには、**feature lacp** コマンドを使用します。
- LACP をイネーブルにした同一ポートチャネルでは、異なるインターフェイスに異なるモードを使用できます。指定したチャネルグループに割り当てられた唯一のインターフェイスである場合に限り、モードを **active** と **passive** で切り替えることができます。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	feature lacp 例： switch(config)# feature lacp	デバイスの LACP をイネーブルにします。
ステップ 3	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、LACP をイネーブルにする例を示します。

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

LACP ポート チャネルポート モードの設定

LACP をイネーブルにしたら、LACP ポート チャネルのそれぞれのリンクのチャネル モードを **active** または **passive** に設定できます。このチャネル コンフィギュレーション モードを使用すると、リンクは LACP で動作可能になります。

関連する集約プロトコルを使用せずにポート チャネルを設定すると、リンク両端のすべてのインターフェイスは **on** チャネル モードを維持します。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface type slot/port 例: switch(config)# interface ethernet 1/4 switch(config-if)	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	channel-group number mode {active on / passive} 例: switch(config-if)# channel-group 5 mode active	ポートチャネルのリンクのポートモードを指定します。LACP をイネーブルにしたら、各リンクまたはチャネル全体を active または passive に設定します。 関連する集約プロトコルを使用せずにポートチャネルを実行する場合、ポートチャネルモードは常に on です。 デフォルト ポートチャネルモードは on です。
ステップ 4	show port-channel summary 例: switch(config-if)# show port-channel summary	(任意) ポートチャネルの概要を表示します。
ステップ 5	copy running-config startup-config 例: switch(config-if)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

次に、LACP をイネーブルにしたインターフェイスを、チャネルグループ 5 のイーサネット インターフェイス 1/4 のアクティブ ポートチャネルモードに設定する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# channel-group 5 mode active
```

LACP ポートチャネルの最小リンクの設定

LACP の最小リンク機能を設定できます。最小リンクと maxbundles は LACP でのみ動作しますが、ただし、非 LACP ポートチャネルに対してこれらの機能の CLI コマンドを入力できますが、これらのコマンドは動作不能です。

はじめる前に

適切なポートチャネル インターフェイスであることを確認します。

手順の概要

1. `configure terminal`
2. `interface port-channel number`
3. `lACP min-links number`
4. (任意) `show running-config interface port-channel number`

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例: <code>switch# configure terminal</code> <code>switch(config)#</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface port-channel number</code> 例: <code>switch(config)# interface port-channel 3</code> <code>switch(config-if)</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>lACP min-links number</code> 例: <code>switch(config-if)# lACP min-links 3</code>	ポート チャネル インターフェイスを指定して、最小リンクの数を設定し、インターフェイス コンフィギュレーション モードを開始します。指定できる範囲は 1 ~ 16 です。
ステップ 4	<code>show running-config interface port-channel number</code> 例: <code>switch(config-if)# show running-config interface port-channel 3</code>	(任意) ポート チャネル最小リンク設定を表示します。

デフォルトのポートチャネル最小リンク設定を復元するには、`no lACP min-links` コマンドを使用します。

コマンド	目的
<code>no lACP min-links</code> 例: <code>switch(config)# no lACP min-links</code>	デフォルトのポートチャネル最小リンク設定を復元します。

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

```
switch# configure terminal
switch (config)# lACP min-links 3
```

LACP ポートチャネル MaxBundle の設定

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。

はじめる前に

適切なポートチャネル インターフェイスであることを確認します。

手順の概要

1. **configure terminal**
2. **interface port-channel number**
3. **lACP max-bundle number**
4. (任意) **show running-config interface port-channel number**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel number 例: switch(config)# interface port-channel 3 switch(config-if)	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	lACP max-bundle number 例: switch(config-if)# lACP max-bundle	ポートチャネル インターフェイスを指定して、 max-bundle を設定し、インターフェイス コンフィギュレーション モードを開始します。 ポートチャネルの max-bundle のデフォルト値は 16 です。指定できる範囲は 1 ~ 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。
ステップ 4	show running-config interface port-channel number 例: switch(config-if)# show running-config interface port-channel 3	(任意) ポートチャネル max-bundle 設定を表示します。

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

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

```
switch# configure terminal
switch (config)# lacp max-bundle 3
```

LACP 高速タイマーレートの設定

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



(注) LACP タイマーレートの変更は推奨しません。HA および SSO は、LACP 高速レートのタイマーが設定されている場合はサポートされません。

はじめる前に

LACP 機能がイネーブルになっていることを確認します。

手順の概要

1. `configure terminal`
2. `interface type slot/port`
3. `lacp rate fast`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>configure terminal</code> 例： switch# <code>configure terminal</code> switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface type slot/port</code> 例： switch(config)# <code>interface ethernet 1/4</code>	設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>lacp rate fast</code> 例： switch(config-if)# <code>lacp rate fast</code>	LACP がサポートされているインターフェイスに LACP 制御パケットを送信する際のレートとして高速レート（1秒）を設定します。 タイムアウト レートをデフォルトにリセットするには、コマンドの <code>no</code> 形式を使用します。

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

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

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

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

LACP システム プライオリティの設定

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

はじめる前に

LACP をイネーブルにします。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	lacp system-priority <i>priority</i> 例: switch(config)# lacp system-priority 40000	LACP で使用するシステム プライオリティを設定します。指定できる範囲は 1 ~ 65535 で、値が大きいほどプライオリティは低くなります。デフォルト値は 32768 です。 (注) VDC ごとに LACP システム ID が異なります。これは、この設定値に MAC アドレスが追加されるためです。
ステップ 3	show lacp system-identifier 例: switch(config-if)# show lacp system-identifier	(任意) LACP システム識別子を表示します。
ステップ 4	copy running-config startup-config 例: switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

LACP ポート プライオリティの設定

LACP をイネーブルにしたら、ポート プライオリティの LACP ポート チャネルにそれぞれのリンクを設定できます。

はじめる前に

LACP をイネーブルにします。

手順の概要

1. `configure terminal`
2. `interface type slot/port`
3. `lacp port-priority priority`
4. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface type slot/port</code> 例: switch(config)# interface ethernet 1/4 switch(config-if)	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>lacp port-priority priority</code> 例: switch(config-if)# lacp port-priority 40000	LACP で使用するポート プライオリティを設定します。指定できる範囲は 1 ~ 65535 で、値が大きいほどプライオリティは低くなります。デフォルト値は 32768 です。
ステップ 4	<code>copy running-config startup-config</code> 例: switch(config-if)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、イーサネット インターフェイス 1/4 の LACP ポート プライオリティを 40000 に設定する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# lacp port-priority 40000
```

LACP グレースフル コンバージェンス

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



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

はじめる前に

LACP をイネーブルにします。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel <i>number</i> 例: switch(config)# interface port-channel 1 switch(config-if)	設定するポートチャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	shutdown 例: switch(config-if) shutdown	ポートチャネルを管理シャットダウンします。
ステップ 4	no lacp 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。

	コマンド	目的
ステップ 5	no shutdown 例： switch(config-if) no shutdown	ポートチャネルを管理的にアップします。
ステップ 6	copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

次に、ポートチャネルの 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. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバルコンフィギュレーションモードを開始します。
ステップ 2	interface port-channel <i>number</i> 例： switch(config)# interface port-channel 1 switch(config-if)	設定するポートチャネルインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 3	shutdown 例： switch(config-if) shutdown	ポートチャネルを管理シャットダウンします。

	コマンド	目的
ステップ 4	lACP graceful-convergence 例: switch(config-if)# lACP graceful-convergence	ポートチャネルの LACP グレースフル コンバージェンスをイネーブルにします。
ステップ 5	no shutdown 例: switch(config-if) no shutdown	ポートチャネルを管理的にアップします。
ステップ 6	copy running-config startup-config 例: switch(config-if)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

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

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

LACP の個別一時停止のディセーブル化

ポートがピアから LACP PDU を受信しない場合、LACP はポートを中断ステートに設定します。このプロセスによって、サーバの中には起動に失敗するものがあります。そのようなサーバは、LACP が論理的にポートを稼働状態にしていることを必要とするからです。



(注)

エッジポートで **lACP suspend-individual** コマンドを入力するだけです。このコマンドを使用する前に、ポートチャネルが管理上のダウン状態である必要があります。

はじめる前に

LACP をイネーブルにします。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel <i>number</i> 例： switch(config)# interface port-channel 1 switch(config-if)	設定するポートチャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	shutdown 例： switch(config-if) shutdown	ポートチャネルを管理シャットダウンします。
ステップ 4	no lacp suspend-individual 例： switch(config-if)# no lacp suspend-individual	ポートチャネルで LACP 個別ポートの一時停止動作をディセーブルにします。
ステップ 5	no shutdown 例： switch(config-if) no shutdown	ポートチャネルを管理的にアップします。
ステップ 6	copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

次に、ポートチャネルで LACP 個別ポートの一時停止をディセーブルにする方法を示します。

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

LACP の個別一時停止の再イネーブル化

デフォルトの LACP 個別ポートの一時停止を再度イネーブルにできます。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel number 例: switch(config)# interface port-channel 1 switch(config-if)	設定するポートチャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	shutdown 例: switch(config-if) shutdown	ポートチャネルを管理シャットダウンします。
ステップ 4	lacp suspend-individual 例: switch(config-if)# lacp suspend-individual	ポートチャネルで LACP 個別ポートの一時停止動作をイネーブルにします。
ステップ 5	no shutdown 例: switch(config-if) no shutdown	ポートチャネルを管理的にアップします。
ステップ 6	copy running-config startup-config 例: switch(config-if)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

次に、ポートチャネルで LACP 個別ポートの一時停止を再度イネーブルにする方法を示します。

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

ポートチャネルハッシュ分散の設定

Cisco NX-OS リリース 6.1(1) 以降、ハッシュ分散のアダプティブおよび固定設定は、グローバルレベルおよびポートチャネルレベルの両方でサポートされます。このオプションは、メンバがアップまたはダウンしたときに Result Bundle Hash (RBH) 分散の変化を最小限に抑えることにより、トラフィックの中断を最小限に抑えます。このため、変化のない RBH 値にマッピングされているフローが同じリンクを流れ続けるようになります。ポートチャネルレベルの設定はグローバル設定よりも優先されます。デフォルト設定はグローバルに適用し、各ポートチャネルの設定がないので、ISSU 中に変更はありません。コマンドが適用されたときにポートはフラップされず、設定は次のメンバーリンクの変更イベントで有効になります。どちらのモードも RBH モジュールまたは非モジュールスキームで動作します。

この機能がサポートされない下位バージョンへの ISSU 時には、固定モードコマンドがグローバルに使用されている場合や、ポートチャネルレベルの設定がある場合は、この機能を無効にする必要があります。

グローバルレベルでのポートチャネルハッシュ分散の設定

手順の概要

1. **configure terminal**
2. **no port-channel hash-distribution {adaptive | fixed}**
3. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no port-channel hash-distribution {adaptive fixed} 例: switch(config)# port-channel hash-distribution adaptive switch(config)	グローバル レベルでポートチャネルハッシュ分散を指定します。 デフォルトはアダプティブ モードです。 コマンドは、次のメンバーリンク イベント (link down/up/no shutdown/shutdown) まで有効になりません。Do you want to continue (y/n) ?[yes]
ステップ 3	copy running-config startup-config 例: switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

次に、グローバルレベルでハッシュ分散を設定する例を示します。

```
switch# configure terminal
switch(config)# no port-channel hash-distribution fixed
```

ポートチャネルレベルでのポートチャネルハッシュ分散の設定

手順の概要

1. **configure terminal**
2. **interface port-channel {channel-number | range}**
3. **no port-channel port hash-distribution [{adaptive | fixed}]**
4. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 1	interface port-channel {channel-number range} 例： switch# interface port-channel 4 switch(config-if)#	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	no port-channel port hash-distribution {adaptive fixed} 例： switch(config-if)# port-channel port hash-distribution adaptive switch(config-if)	ポート チャネル レベルでポート チャネル ハッシュ分散を指定します。 デフォルトはありません。 コマンドは、次のメンバー リンク イベント (link down/up/no shutdown/shutdown) まで有効になりません。Do you want to continue (y/n) ?[yes]
ステップ 3	copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、グローバル レベル コマンドとしてハッシュ分散を設定する例を示します。

```
switch# configure terminal
switch(config)# no port-channel hash-distribution fixed
```

ポートチャネル設定の確認

ポート チャネルの設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show interface port-channel channel-number	ポート チャネル インターフェイスのステータスを表示します。
show feature	イネーブルにされた機能を表示します。
load- interval {interval seconds {1 2 3}}	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。
show port-channel compatibility-parameters	ポート チャネルに追加するためにメンバポート間で同じにするパラメータを表示します。
show port-channel database [interface port-channel channel-number]	1 つ以上のポート チャネル インターフェイスの集約状態を表示します。

コマンド	目的
show port-channel load-balance	ポートチャネルで使用するロードバランシングのタイプを表示します。
show port-channel summary	ポートチャネルインターフェイスのサマリーを表示します。
show port-channel traffic	ポートチャネルのトラフィック統計情報を表示します。
show port-channel usage	使用済みおよび未使用のチャネル番号の範囲を表示します。
show lacp {counters [interface port-channel channel-number] [interface type/slot] neighbor [interface port-channel channel-number] port-channel [interface port-channel channel-number] system-identifier]}}	LACPに関する情報を表示します。
show running-config interface port-channel channel-number	ポートチャネルの実行コンフィギュレーションに関する情報を表示します。

ポートチャネルインターフェイスコンフィギュレーションのモニタリング

次のコマンドを使用すると、ポートチャネルインターフェイス構成情報を表示することができます。

コマンド	目的
clear counters interface port-channel channel-number	カウンタをクリアします。
clear lacp counters [interface port-channel channel-number]	LACPカウンタをクリアします。
load- interval {interval seconds {1 2 3}}	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。
show interface counters [module module]	入力および出力オクテット、ユニキャストパケット、マルチキャストパケット、ブロードキャストパケットを表示します。
show interface counters detailed [all]	入力パケット、バイト、マルチキャストおよび出力パケット、バイトを表示します。
show interface counters errors [module module]	エラーパケットの数を表示します。
show lacp counters	LACPの統計情報を表示します。

ポートチャネルの設定例

次に、LACP ポートチャネルを作成し、そのポートチャネルに2つのレイヤ2 インターフェイスを追加する例を示します。

```
switch# configure terminal
switch (config)# feature lacp
switch (config)# interface port-channel 5
switch (config-if)# interface ethernet 1/4
switch(config-if)# switchport
switch(config-if)# channel-group 5 mode active
switch(config-if)# lacp port priority 40000
switch(config-if)# interface ethernet 1/7
switch(config-if)# switchport
switch(config-if)# channel-group 5 mode
```

次に、チャンネルグループに2つのレイヤ3 インターフェイスを追加する例を示します。Cisco NX-OS ソフトウェアは自動的にポートチャネルを作成します。

```
switch# configure terminal
switch (config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# no ip address
switch (config-if)# channel-group 6 mode active
switch (config)# interface ethernet 2/5
switch(config-if)# no switchport
switch(config-if)# no ip address
switch(config-if)# channel-group 6 mode active
switch (config)# interface port-channel 6
switch(config-if)# ip address 192.0.2.1/8
```

その他の関連資料

ポートチャネルの実装に関する追加情報については、次の項を参照してください。

- 「関連資料」 (P.6-44)
- 「標準」 (P.6-45)
- 「管理情報ベース (MIB)」 (P.6-45)

関連資料

関連項目	マニュアルタイトル
システム管理	『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』
ハイアベイラビリティ	『Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide』
ライセンス	『Cisco NX-OS Licensing Guide』

標準

標準	タイトル
IEEE 802.3ad	—

管理情報ベース (MIB)

MIB	MIB のリンク
ポートチャネルに関連する MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html



第 7 章

vPC の設定

この章では、Cisco NX-OS デバイス上で仮想ポート チャンネル (vPC) を設定する方法について説明しています。



(注) vPC は FabricPath と相互運用するように拡張されました。

vPC ピア リンクに Nexus 9000 デバイスの任意のインターフェイスを使用できます。

ポート チャンネルの互換性パラメータは、物理スイッチのすべてのポート チャンネル メンバーで同じである必要があります。

vPC の一部になるように共有インターフェイスを設定することはできません。



(注) ポート チャンネルの互換性パラメータは、両方のピアのすべての vPC メンバポートでも同じでなければならないので、シャーシごとに同じタイプのモジュールを使用する必要があります。

この章は、次の項で構成されています。

- [「vPC について」 \(P.7-1\)](#)
- [「vPC のライセンス要件」 \(P.7-27\)](#)
- [「注意事項と制約事項」 \(P.7-27\)](#)
- [「デフォルト設定値」 \(P.7-29\)](#)
- [「vPC の設定」 \(P.7-29\)](#)
- [「vPC 設定の確認」 \(P.7-56\)](#)
- [「vPC のモニタリング」 \(P.7-57\)](#)
- [「vPC の設定例」 \(P.7-57\)](#)
- [「その他の参考資料」 \(P.7-59\)](#)

vPC について

この項では、次のトピックについて取り上げます。

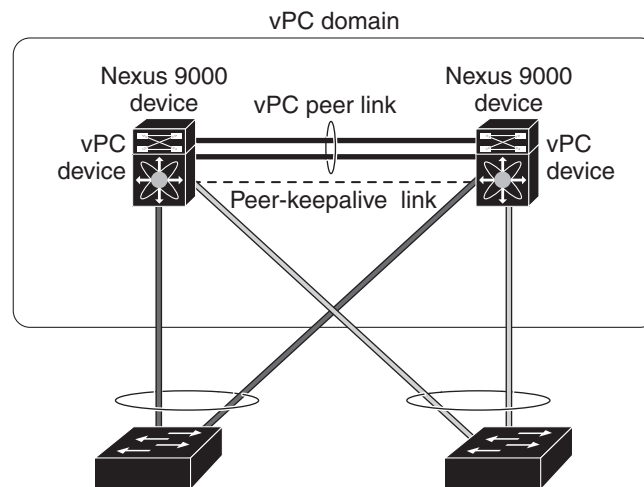
- [「vPC の概要」 \(P.7-2\)](#)
- [「vPC の用語」 \(P.7-4\)](#)
- [「vPC ピア リンク」 \(P.7-6\)](#)

- 「ピアキープアライブ リンクとメッセージ」 (P.7-9)
- 「vPC ピア ゲートウェイ」 (P.7-11)
- 「vPC ドメイン」 (P.7-11)
- 「vPC トポロジ」 (P.7-12)
- 「vPC インターフェイスの互換パラメータ」 (P.7-14)
- 「vPC 番号」 (P.7-16)
- 「他のポート チャネルの vPC への移行」 (P.7-17)
- 「単一モジュール上での vPC ピア リンクとコアへのリンクの設定」 (P.7-17)
- 「その他の機能との vPC の相互作用」 (P.7-19)
- 「仮想化のサポート」 (P.7-26)
- 「停電後の vPC リカバリ」 (P.7-26)
- 「ハイアベイラビリティ」 (P.7-27)

vPC の概要

仮想ポートチャネル (vPC) は、物理的には 2 台の異なる Cisco Nexus 9000 シリーズ デバイスに接続されているリンクを、第 3 のデバイスには単一のポートに見えるようにします (図 7-1 を参照)。第 3 のデバイスは、スイッチ、サーバ、ポートチャネルをサポートするその他の任意のネットワーキング デバイスのいずれでもかまいません。vPC は、ノード間の複数の並列パスを可能にし、トラフィックのロード バランシングを可能にすることによって、冗長性を作り、バイセクショナルな帯域幅を増やすレイヤ 2 マルチパスを提供できます。

図 7-1 vPC のアーキテクチャ



vPC で使用できるのは、レイヤ 2 ポートチャネルだけです。vPC ドメインは単一の仮想デバイス コンテキスト (VDC) に関連付けられるため、同じ 1 つの vPC ドメインに所属するすべての vPC インターフェイスが同一 VDC 内で定義されていなければなりません。

ポートチャネルの設定は、次のいずれかを使用して行います。

- プロトコルなし
- リンク集約制御プロトコル (LACP)

LACP を使用せずに vPC (vPC ピア リンク チャンネルも含めて) のポート チャンネルを設定する場合は、各デバイスが、単一のポート チャンネル内に最大 8 つのアクティブ リンクを持てます。LACP を使用して vPC (vPC ピア リンク チャンネルも含めて) のポート チャンネルを設定する場合は、各デバイスが、単一のポート チャンネル内に 8 つのアクティブ リンクと 8 つのスタンバイ リンクを持つことができます (LACP と vPC の使用方法の詳細については、「[その他の機能との vPC の相互作用](#)」(P.7-19) を参照してください)。



(注)

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

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。

vPC 機能をイネーブルにしたら、ピアキープアライブ リンクを作成します。このリンクは、2 つの vPC ピア デバイス間でのハートビート メッセージの送信を行います。

2 つ以上の 10 ギガビット イーサネット ポートを使用することにより、1 台の Cisco Nexus 9000 シリーズ シャーシでポート チャンネルを設定して vPC ピア リンクを作成できます。vPC をイネーブルにして実行するための正しいハードウェアが揃っていることを確認するには **show hardware feature-capability** コマンドを入力します。コマンド出力で vPC の向かいに X が表示されている場合、そのハードウェアでは vPC 機能をイネーブルにできません。

vPC ピア リンク レイヤ 2 ポート チャンネルは、トランクとして設定することを推奨します。もう 1 つの Cisco Nexus 9000 シリーズ シャーシで、再度 2 つ以上の 10 ギガビット イーサネット ポートを専用モードで使用して、もう 1 つのポート チャンネルを設定します。これらの 2 つのポート チャンネルを接続すると、リンクされた 2 つの Cisco Nexus デバイスが第 3 のデバイスには 1 つのデバイスとして見える vPC ピア リンクが作成されます。第 3 のデバイス、またはダウンストリーム デバイスは、スイッチ、サーバ、vPC に接続された正規のポート チャンネルを使用するその他の任意のネットワーク デバイスのいずれでもかまいません。正しいモジュールを使用していないと、システムからエラー メッセージが表示されます。



(注)

異なるモジュールの専用ポート上で vPC ピア リンクを設定して、障害発生の可能性を下げることをお勧めします。復元力を最適にしたい環境では、少なくとも 2 つのモジュールを使用してください。

すべての vPC ピア リンクおよびコアに面したインターフェイスを 1 つのモジュール上で設定しなければならない場合、コアへのレイヤ 3 リンクに関連付けられているトラック オブジェクトおよび両方の vPC ピア デバイス上の vPC ピア リンク上のすべてのリンクを設定してください。いったんこの機能を設定したら、プライマリ vPC ピア デバイスに障害が発生した場合には、プライマリ vPC ピア デバイス上のすべての vPC リンクを、システムが自動的に停止します。システムが安定するまでは、このアクションにより、すべての vPC トラフィックが強制的にセカンドリ vPC ピア デバイスに送られます。

トラック オブジェクトを作成し、コアおよび vPC ピア リンクに接続されているプライマリ vPC ピア デバイス上のすべてのリンクにそのオブジェクトを適用できます。 **track interface** コマンドに関する詳細情報については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

vPC ドメインには、両方の vPC ピア デバイス、vPC ピアキープアライブ リンク、vPC ピア リンク、および vPC ドメイン内にあってダウンストリーム デバイスに接続されているすべてのポート チャンネルが含まれます。各デバイスに設定できる vPC ドメイン ID は、1 つだけです。このバージョンでは、各ダウンストリーム デバイスを、単一のポート チャンネルを使用して単一の vPC ドメイン ID に接続できます。



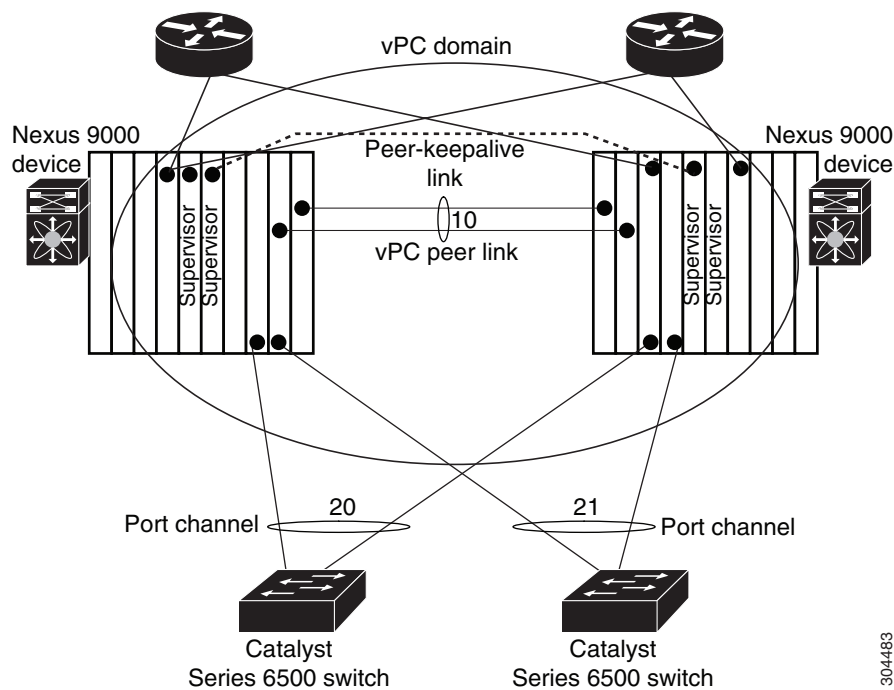
(注)

常にすべての vPC デバイスを両方の vPC ピア デバイスに、ポート チャネルを使用して接続してください。

vPC (図 7-2 を参照) には、次の利点があります。

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

図 7-2 1 つの VDC 内の vPC インターフェイス



304483

vPC の用語

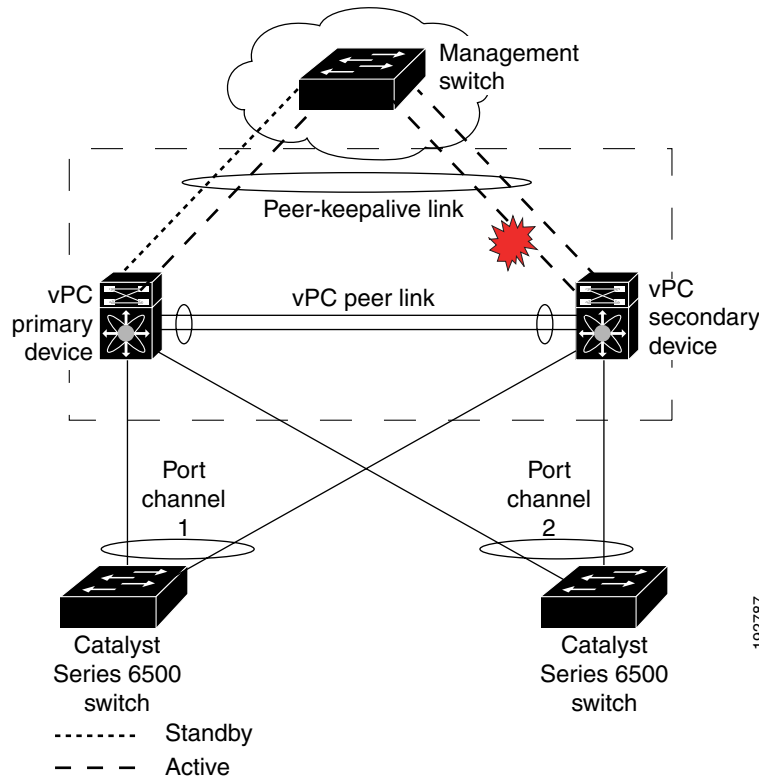
vPC で使用される用語は、次のとおりです。

- vPC : vPC ピア デバイスとダウンストリーム デバイスの間の結合されたポート チャネル。
- vPC ピア デバイス : vPC ピア リンクと呼ばれる特殊なポート チャネルで接続されている一対のデバイスの 1 つ。

- vPC ピア リンク : vPC ピア デバイス間の状態を同期するために使用されるリンク。両エンドが 10 ギガバイト イーサネット インターフェイス上にはなりません。
- vPC メンバ ポート : vPC に属するインターフェイス。
- ホスト vPC ポート : vPC に属するファブリック エクステンダのホスト インターフェイス。
- vPC ドメイン : このドメインには、両方の vPC ピア デバイス、vPC ピアキープアライブ リンク、vPC 内においてダウンストリーム デバイスに接続されているすべてのポート チャンネルが含まれます。また、このドメインは、vPC グローバル パラメータを割り当てるために使用する必要があるコンフィギュレーション モードに関連付けられています。
- vPC ピアキープアライブ リンク : ピアキープアライブ リンクは、さまざまな vPC ピア Cisco Nexus 9000 シリーズのデバイスをモニタします。ピアキープアライブ リンクは、vPC ピア デバイス間での設定可能なキープアライブ メッセージの定期的な送信を行います。

ピアキープアライブ リンクを、各 vPC ピア デバイス内のレイヤ 3 インターフェイスにマッピングされている独立した仮想ルーティングおよび転送 (VRF) インスタンスに関連付けることを推奨します。独立した VRF を設定しなかった場合は、デフォルトで管理 VRF が使用されます。ただし、ピアキープアライブ リンクに管理インターフェイスを使用する場合は、各 vPC ピア デバイスのアクティブ管理ポートとスタンバイ管理ポートの両方に接続した管理スイッチを置く必要があります (図 7-3 を参照)。

図 7-3 vPC ピアキープアライブ リンクの管理ポートを接続するための独立したスイッチが必要



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

- vPC メンバ ポート : vPC に属するインターフェイス。

- デュアル アクティブ：プライマリとして動作する両方の vPC ピア。この状況は、両方のピアがまだアクティブなときにピアキープアライブとピア リンクがダウンした場合に発生します。この場合、セカンダリ vPC はプライマリ vPC が動作しないと想定し、プライマリ vPC として機能します。
- リカバリ：ピアキープアライブとピア リンクが起動すると、1 台のスイッチがセカンダリ vPC になります。セカンダリ vPC になるスイッチで、vPC リンクが停止してから復帰します。

vPC ピア リンク

vPC ピア リンクは、vPC ピア デバイス間の状態を同期するために使用されるリンクです。リンクの両エンドが、10 ギガビット イーサネット インターフェイス上になくてもなりません。

vPC に 2 台のスイッチで作動するスプリット コントロール プレーンが含まれるので、vPC は次のようにピア リンクを使用します。

- 両方の vPC ピア スイッチにコントロール プレーン情報を同期します (vPC 状態、一貫性パラメータ、MAC アドレスなど)。
- ローカル vPC がダウンしたとき、vPC ピア スイッチにデータ パケットを転送します。

ここでは、vPC ピア リンクについて説明します。内容は次のとおりです。

- 「vPC ピア リンクの概要」 (P.7-6)
- 「プライマリおよびセカンダリ デバイス上で手動で設定する必要がある機能」 (P.7-8)
- 「vPC ピア リンクのレイヤ 3 バックアップ ルートの設定」 (P.7-9)



(注)

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 のピアキープアライブ リンクとメッセージの詳細については、「ピアキープアライブ リンクとメッセージ」 (P.7-9) を参照してください)。

vPC ピア リンクは、2 つのデバイスを vPC ピアとして設定するように設定できます。vPC ピア リンクを設定するためには、モジュールを使用する必要があります。



(注)

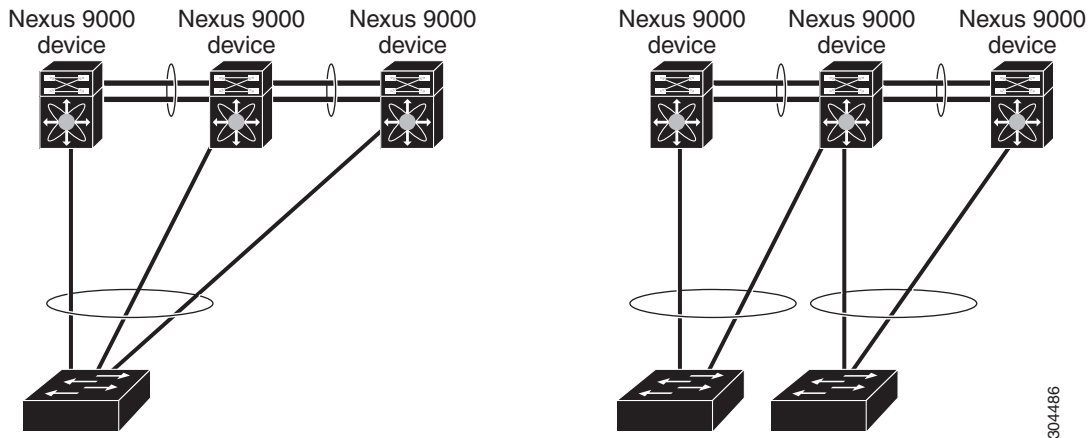
vPC ピア リンクを設定する場合は、専用ポート モードを使用することを推奨します。専用ポート モードの詳細については、第 2 章「基本インターフェイス パラメータの設定」を参照してください。

vPC ピア リンクの概要

vPC ピアとして持てるのは 2 台のデバイスだけです。各デバイスが、他方の 1 つの vPC ピアに対してだけ vPC ピアとして機能します。vPC ピア デバイスは、他のデバイスに対する非 vPC リンクも持つことができます。

無効な vPC ピア設定については、図 7-4 を参照してください。

図 7-4 許可されていない vPC ピア設定



有効な設定を作成するには、まず各デバイス上でポート チャンネルを設定してから、vPC ドメインを設定します。ポート チャンネルを各デバイスに、同じ vPC ドメイン ID を使用してピア リンクとして割り当てます。vPC ピア リンクのインターフェイスの片方に障害が発生した場合に、デバイスが自動的にピア リンク内の他方のインターフェイスを使用するようにフォールバックするため、冗長性のために少なくとも 2 つの専用ポートをポート チャンネルに設定することを推奨します。



(注)

レイヤ 2 ポート チャンネルをトランク モードで設定することを推奨します。

多くの動作パラメータおよび設定パラメータが、vPC ピア リンクによって接続されている各デバイスで同じでなければなりません（「[vPC インターフェイスの互換パラメータ](#)」(P.7-14) を参照)。各デバイスが管理プレーンから完全に独立しているため、デバイスが重要なパラメータについて互換性があることを管理者が確認する必要があります。vPC ピア デバイスは、独立したコントロールプレーンを持っています。vPC ピア リンクを設定し終わったら、各 vPC ピア デバイスの設定を表示して、設定に互換性があることを確認してください。



(注)

vPC ピア リンクによって接続されている 2 つのデバイスが、特定の同じ動作パラメータおよび設定パラメータを持っていることを確認する必要があります。一貫性が必要な設定の詳細については、「[vPC インターフェイスの互換パラメータ](#)」(P.7-14) を参照してください。

vPC ピア リンクを設定すると、vPC ピア デバイスは接続されたデバイスの一方がプライマリ デバイスで、もう一方の接続デバイスがセカンダリ デバイスであると交渉します（「[vPC の設定](#)」(P.7-29) を参照)。Cisco NX-OS ソフトウェアは、最小の MAC アドレスを使用してプライマリ デバイスを選択します。特定のフェールオーバー条件の下でだけ、ソフトウェアが各デバイス（つまり、プライマリ デバイスおよびセカンダリ デバイス）に対して異なるアクションを取ります。プライマリ デバイスに障害が発生すると、システムの回復時にセカンダリ デバイスが新しいプライマリ デバイスになり、以前のプライマリ デバイスがセカンダリ デバイスになります。

どちらの vPC デバイスをプライマリ デバイスにするか設定することもできます。vPC ピア デバイスのプライオリティを変更すると、ネットワークでインターフェイスがアップしたりダウンしたりする可能性があります。1 台の vPC デバイスをプライマリ デバイスにするよう再度ロールプライオリティを設定する場合は、プライオリティ値が低いプライマリ vPC デバイスと値が高いセカンダリ vPC デバイスの両方でロールプライオリティを設定します。次に、**shutdown** コマンドを入力して、両方のデバイスで vPC ピア リンクであるポート チャンネルをシャットダウンし、最後に **no shutdown** コマンドを入力して、両方のデバイスでポート チャンネルを再度イネーブルにします。



(注)

各 vPC ピア リンクの各 vPC ピア デバイスの冗長性のために、2 つの異なるモジュールを使用することを推奨します。

ソフトウェアは、vPC ピアを介して転送されたすべてのトラフィックをローカルトラフィックとしてキープします。ポート チャンネルから入ってきたパケットは、vPC ピア リンクを介して移動するのではなく、ローカルリンクの1つを使用します。不明なユニキャスト、マルチキャスト、およびブロードキャストトラフィック (STP BPDU を含む) は、vPC ピア リンクでフラッディングされます。ソフトウェアが、マルチキャスト フォワーディングを両方の vPC ピア デバイス上で同期された状態に保ちます。

両方の vPC ピア リンク デバイスおよびダウンストリーム デバイスで、任意の標準ロードバランシング スキームを設定できます (ロード バランシングの詳細については、第6章「ポート チャンネルの設定」を参照してください)。

設定情報は、Cisco Fabric Service over Ethernet (CFSoE) プロトコルを使用して vPC ピア リンクを転送されます。(CFSoE の詳細については、「vPC および孤立ポート」(P.7-26) を参照してください)。

両方のデバイス上で設定されているこれらの VLAN の MAC アドレスはすべて、vPC ピア デバイス間で同期されています。この同期に、CFSoE が使用されます (CFSoE については、「vPC および孤立ポート」(P.7-26) を参照してください)。

vPC ピア リンクに障害が発生した場合は、ソフトウェアが、両方のデバイスが稼働していることを確認するための vPC ピア デバイス間のリンクであるピアキープアライブ リンクを使用して、リモート vPC ピア デバイスのステータスをチェックします。vPC ピア デバイスが稼働している場合は、セカンダリ vPC デバイスは、ループやトラフィックの消失あるいはフラッディングを防ぐために、そのデバイス上のすべての vPC ポートをディセーブルにします。したがって、データは、ポート チャンネルの残っているアクティブなリンクに転送されます。



(注)

独立した VRF を作成して設定し、その vPC ピアキープアライブ リンクのための VRF 内の各 vPC ピア デバイス上でレイヤ3 ポートを設定することを推奨します。ピアキープアライブのデフォルト ポートとデフォルト VRF は、管理ポートと管理 VRF です。

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

vPC ピア デバイス間の設定可能なキープアライブ メッセージの送信には、独立したリンク (vPC ピアキープアライブ リンク) を使用します。vPC ピアキープアライブ リンク上のキープアライブ メッセージから、障害が vPC ピア リンク上でだけ発生したのか、vPC ピア デバイス上で発生したのかがわかります。キープアライブ メッセージは、ピア リンク内のすべてのリンクで障害が発生した場合にだけ使用されます。キープアライブ メッセージの詳細については、「ピアキープアライブ リンクとメッセージ」(P.7-9) を参照してください。

プライマリおよびセカンダリ デバイス上で手動で設定する必要がある機能

各 vPC ピア デバイスのプライマリ/セカンダリ マッピングに従うために、次の機能を手動で設定する必要があります。

- STP ルート : プライマリ vPC ピア デバイスを STP プライマリ ルート デバイスとして設定し、vPC セカンダリ デバイスを STP セカンダリ ルート デバイスとして設定します。vPC および STP の詳細情報については、「vPC ピア リンクと STP」(P.7-20) を参照してください。
 - Bridge Assurance がすべての vPC ピア リンク上でイネーブルになるように、vPC ピア リンク インターフェイスを STP ネットワーク ポートとして設定することを推奨します。

- VLAN 単位の高速スパンニングツリー (PVST+) を設定してプライマリ デバイスがすべての VLAN のルートになるようにし、マルチ スパンニングツリー (MST) を設定してプライマリ デバイスがすべてのインスタンスのルートになるようにすることを推奨します。
- レイヤ 3 VLAN ネットワーク インターフェイス: 両方のデバイスから同じ VLAN の VLAN ネットワーク インターフェイスを設定することにより、各 vPC ピア デバイスからのレイヤ 3 接続を設定します。
- HSRP アクティブ: vPC ピア デバイス上でホットスタンバイルータ プロトコル (HSRP) と VLAN インターフェイスを使用する場合は、プライマリ vPC ピア デバイスを HSRP アクティブの最も高いプライオリティで設定します。セカンダリ デバイスを HSRP スタンバイになるように設定し、各 vPC デバイスの VLAN インターフェイスが同じ管理/動作モードにあることを確認します (vPC および HSRP の詳細については、「vPC ピア リンクとルーティング」(P.7-24) を参照してください)。

vPC ピア リンクの両側で単方向リンク検出 (UDLD) を設定することを推奨します。UDLD の設定については、「UDLD モードの設定」(P.2-24) を参照してください。

vPC ピア リンクのレイヤ 3 バックアップ ルートの設定

HSRP や PIM などのアプリケーションを使用するネットワークのレイヤ 3 にリンクするために、vPC ピア デバイス上の VLAN ネットワーク インターフェイスを使用できます。ただし、この目的には VLAN ネットワーク インターフェイスを使用するよりも、vPC ピア デバイスからのルーティングのためのレイヤ 3 リンクを別途設定することを推奨します。



(注)

各ピア デバイス上で VLAN ネットワーク インターフェイスが設定されており、そのインターフェイスが各デバイス上で同じ VLAN に接続されていることを確認してください。また、各 VLAN インターフェイスが、同じ管理/動作モードになっていなければなりません。VLAN ネットワーク インターフェイスの設定の詳細については、第 4 章「レイヤ 3 インターフェイスの設定」を参照してください。

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

vPC ピア リンクに障害が発生したときに特定の VLAN インターフェイスが vPC セカンダリ デバイス上で停止しないようにできます。

この機能を設定するには、**dual-active exclude interface-vlan** コマンドを使用します。



(注)

vPC ドメインにレイヤ 3 デバイスを接続した場合、vPC ピア リンク上でも送信される VLAN を使用したルーティング プロトコルのピアリングはサポートされません。vPC ピア デバイスおよび汎用レイヤ 3 デバイスの間でルーティング プロトコルの隣接関係が必要な場合は、相互接続に物理的にルーティングされたインターフェイスを使用する必要があります。vPC ピアゲートウェイ機能の使用では、この要件は変わりません。

ピアキープアライブ リンクとメッセージ

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



(注)

vPC ピアキープアライブ リンクを、各 vPC ピア デバイス内のレイヤ 3 インターフェイスにマッピングされている独立した VRF に関連付けることを推奨します。独立した VRF を設定しなかった場合は、デフォルトで管理 VRF と管理ポートが使用されます。vPC ピアキープアライブ メッセージの送受信にピア リンク自体を使用することはしないでください。

片方の vPC ピア デバイスに障害が発生したら、vPC ピア リンクの他方の側にある vPC ピア デバイスは、ピアキープアライブ メッセージを受信しなくなることによってその障害を感知します。vPC ピアキープアライブ メッセージのデフォルトの間隔は、1 秒です。この間隔は、400 ミリ秒～10 秒の範囲内で設定可能です。

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

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

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

- ホールドタイムアウトの間は、vPC セカンダリ デバイスは、受信したキープアライブ メッセージに基づいてアクションを起こしません。それにより、たとえばスーパーバイザがピア リンクがダウンした数秒後に失敗した場合などに、キープアライブが一時的に受信される可能性がある場合に、システムがアクションを起こすのを回避できます。
- タイムアウト中は、vPC セカンダリ デバイスは、設定された間隔が終了するまでにキープアライブ メッセージを受信できないと、vPC プライマリ デバイスになるというアクションを取ります。

キープアライブ メッセージのタイマーの設定については、「[vPC の設定](#)」(P.7-29) を参照してください。



(注)

ピアキープアライブ メッセージに使用される送信元 IP アドレスと宛先 IP アドレス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。

コマンドライン インターフェイス (CLI) を使用して、vPC ピアキープアライブ メッセージを使用するインターフェイスを信頼できるポートとして設定してください。優先順位をデフォルト (6) のままにしておくか、またはもっと高い値に設定します。次に、インターフェイスを信頼できるポートとして設定する例を示します。

```
(config)# class-map type qos match-all trust-map
(config-cmap-qos)# match cos 4-7

(config)# policy-map type qos ingresspolicy
(config-pmap-qos)# class trust-map

(config)# interface Ethernet8/11
(config-if)# service-policy type qos input ingresspolicy
```

vPC ピア ゲートウェイ

vPC ピア デバイスを、vPC ピア デバイスの MAC アドレスに送信されるパケットに対してもゲートウェイとして機能するように設定できます。

この機能を設定するには、**peer-gateway** コマンドを使用します。



(注) **mode auto** コマンドを使用してこの機能を自動的に有効化できます。このコマンドの使用に関する詳細情報については、「特定の vPC コマンドの自動イネーブル化」(P.7-41) を参照してください。

一部のネットワーク接続ストレージ (NAS) デバイスまたはロードバランサは、特定のアプリケーションのパフォーマンスを最適化するのに役立つ機能を備えている場合があります。これらの機能により、同じサブネットにローカルに接続されていないホストから送信された要求に応答するときに、デバイスはルーティング テーブルのルックアップを回避できます。このようなデバイスは、一般的な HSRP ゲートウェイではなく、送信元 Cisco Nexus 9000 シリーズ デバイスの MAC アドレスを使用して、トラフィックに応答する場合があります。この動作は、一部の基本的なイーサネット RFC 基準に準拠していません。ローカルではないルータ MAC アドレスの vPC デバイスに到達するパケットは、ピア リンクを介して送信され、最終的な宛先が他の vPC の背後にある場合には、組み込みの vPC ループ回避メカニズムによってドロップされる場合があります。

vPC ピアゲートウェイ機能は、vPC スイッチが、vPC ピアのルータ MAC アドレスを宛先とするパケットに対して、アクティブなゲートウェイとして機能することを可能にします。この機能は、このようなパケットが vPC ピア リンクを通過する必要なしにローカルに転送されることを可能にします。このシナリオでは、この機能によってピア リンクの使用が最適化され、トラフィック損失が回避されます。

ピアゲートウェイ機能の設定は、プライマリ vPC ピアとセカンダリ vPC ピアの両方で行う必要がありますが、デバイスの稼働も vPC トラフィックも中断しません。vPC ピアゲートウェイ機能は、vPC ドメイン サブモードの下でグローバルに設定できます。

この機能をイネーブルにすると、ピアゲートウェイルータを介してスイッチングされたパケットの IP リダイレクト メッセージの発生を避けるために、Cisco NX-OS は vPC VLAN を介してマッピングされるすべてのインターフェイス VLAN 上で IP リダイレクトを自動的にディセーブルにします。

TTL が 1 のパケットが TTL の有効期限が原因で伝送中にドロップされるように、ピアゲートウェイ vPC デバイスに到達するパケットは、デクリメントされたパケット存続時間 (TTL) を有しています。ピアゲートウェイ機能がイネーブルで、TTL が 1 のパケットを送信する特定のネットワーク プロトコルが vPC VLAN で動作する場合は、この状況を考慮する必要があります。

vPC ドメイン

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

vPC ドメインは、キープアライブ メッセージや他の vPC ピア リンク パラメータを、デフォルト値をそのまま使用するのではなく値を設定する場合に使用するコンフィギュレーション モードでもあります。これらのパラメータの設定方法については、「vPC の設定」(P.7-29) を参照してください。

vPC ドメインを作成するには、まず各 vPC ピア デバイス上で、1 ~ 1000 の値を使用して vPC ドメイン ID を作成しなければなりません。VDC につき設定できる vPC ドメインは、1 つだけです。

各デバイス上で、ピア リンクとして機能させるポート チャネルを明示的に設定する必要があります。各デバイス上でピア リンクにしたポート チャネルを、1 つの vPC ドメインからの同じ vPC ドメイン ID に関連付けます。このドメイン内で、システムはループフリー トポロジとレイヤ 2 マルチパスを提供します。

これらのポート チャネルと vPC ピア リンクは、静的にしか設定できません。各 vPC ピア デバイス上の vPC 内のすべてのポートが、同じ VDC 内になくはなりません。ポート チャネルおよび vPC ピア リンクは、LACP を使用するかまたはプロトコルなしのいずれかで設定できます。各 vPC でポート チャネルを設定するにはアクティブ モードのインターフェイスで LACP を使用することを推奨します。それにより、ポート チャネルのフェールオーバー シナリオの最適でグレースフルなリカバリが保証され、ポート チャネル間の設定不一致に対する設定検査が行われます。

vPC ピア デバイスは、設定された vPC ドメイン ID を使用して、一意の vPC システム MAC アドレスを自動的に割り当てます。各 vPC ドメインが、具体的な vPC 関連操作に ID として使用される一意の MAC アドレスを持ちます。ただし、デバイスは vPC システム MAC アドレスを LACP などのリンクスコープでの操作にしか使用しません。連続したレイヤ 2 ネットワーク内の各 vPC ドメインを、一意のドメイン ID で作成することを推奨します。Cisco NX-OS ソフトウェアにアドレスを割り当てさせるのではなく、vPC ドメインに特定の MAC アドレスを設定することもできます。

vPC MAC テーブルの表示の詳細については、「[vPC および孤立ポート](#)」(P.7-26) を参照してください。

vPC ドメインを作成した後は、Cisco NX-OS ソフトウェアによって vPC ドメインのシステムプライオリティが作成されます。vPC ドメインに特定のシステムプライオリティを設定することもできます。



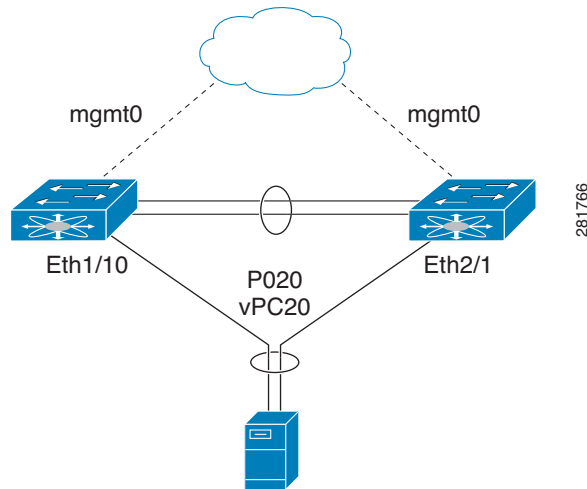
(注)

システムプライオリティを手動で設定する場合は、必ず両方の vPC ピア デバイス上で同じプライオリティ値を割り当てる必要があります。vPC ピア デバイス同士が異なるシステムプライオリティ値を持っていると、vPC は稼働しません。

vPC トポロジ

次の図は、Cisco Nexus 9000 シリーズ デバイス ポートが別のスイッチまたはホストに直接接続され、vPC の一部となるポート チャネルの一部として設定される基本設定を示しています。

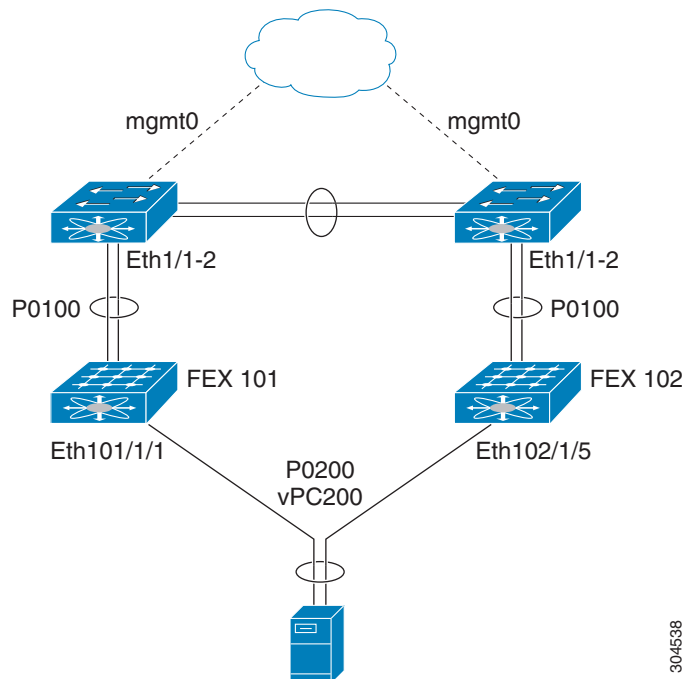
図 7-5 スイッチ vPC トポロジ



この図では、vPC 20 がポート チャネル 20 で設定され、最初のデバイスには Eth1/10 が、2 番目のデバイスには Eth2/1 がメンバポートとしてあります。

図 7-6 で示されるように、ファブリック エクステンダ (FEX) を通してピア デバイスから vPC を設定できます。

図 7-6 FEX Straight-Through トポロジ (ホスト vPC)



図では、各 FEX は Cisco Nexus 9000 シリーズ デバイスがあるシングル ホーム接続 (Straight-Through FEX トポロジ) です。この FEX 上のホスト インターフェイスはポート チャネルとして設定され、それらのポート チャネルは vPC として設定されています。Eth101/1/1 および Eth102/1/5 は、P0200 のメンバとして設定され、P0200 は vPC 200 に対し設定されます。

どちらのトポロジでも、ポート チャンネル P020 および P0200 をピア スイッチ上でまったく同じように設定する必要があります。その後、設定の同期を使用して vPC スイッチの設定を同期します。

FEX ポートの設定に関する詳細は、『Cisco Nexus 2000 Series NX-OS Fabric Extender Configuration Guide for Cisco Nexus 9000 Series Switches』を参照してください。

vPC インターフェイスの互換パラメータ

多くの設定パラメータおよび動作パラメータが、vPC 内のすべてのインターフェイスで同じでなければなりません。vPC ピア リンクに使用するレイヤ 2 ポート チャンネルはトランク モードに設定することを推奨します。

vPC 機能をイネーブルにし、さらに両方の vPC ピア デバイス上でピア 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 デバイスに関する設定のコピーがリモート vPC ピア デバイスへ送信されます。これにより、システムが 2 つのデバイス上で異なっている重要な設定パラメータがないか調べます (CFS の詳細については、「vPC および孤立ポート」(P.7-26) を参照してください)。



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

vPC の互換性チェックプロセスは、正規のポート チャンネルの互換性チェックとは異なります。正規のポート チャンネルについては、第 6 章「ポート チャンネルの設定」を参照してください。

ここでは、次の内容について説明します。

- 「同じでなければならない設定パラメータ」(P.7-14)
- 「同じにすべき設定パラメータ」(P.7-15)
- 「パラメータの不一致によってもたらされる結果」(P.7-16)

同じでなければならない設定パラメータ

このセクションの設定パラメータは、vPC ピア リンクの両方のデバイスで同じに設定する必要があります。そうしないと、vPC は一時停止モードに完全にまたは部分的に移動します。



(注) 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。



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

vPC インターフェイスでのこれらのパラメータの一部は、デバイスによって自動的に互換性がチェックされます。インターフェイスごとのパラメータは、インターフェイスごとに一貫性を保っていなければならない、グローバル パラメータはグローバルに一貫性を保っていなければならない。

- ポートチャンネル モード：オン、オフ、またはアクティブ (ただし、ポートチャンネル モードは vPC ピアの各サイドでアクティブ/パッシブにできます)

- チャンネル単位のリンク速度
- チャンネル単位のデュプレックス モード
- チャンネルごとのトランク モード :
 - ネイティブ VLAN
 - トランク上で許可される VLAN
 - ネイティブ VLAN トラフィックのタグging
- スパニング ツリー プロトコル (STP) モード
- Multiple Spanning Tree 用の STP リージョン コンフィギュレーション
- VLAN ごとのイネーブル/ディセーブル状態
- STP グローバル設定 :
 - ブリッジ保証設定
 - ポート タイプ設定
 - ループ ガード設定
- STP インターフェイス設定 :
 - ポート タイプ設定
 - ループ ガード
 - ルート ガード
- 最大伝送単位 (MTU)

これらのパラメータのいずれかがイネーブルになっていなかったり、片方のデバイスでしか定義されていないと、vPC の一貫性チェックではそのパラメータは無視されます。



(注)

どの vPC インターフェイスもサスペンド モードになっていないことを確認するには、**show vpc brief** コマンドおよび **show vpc consistency-parameters** コマンドを入力して、syslog メッセージをチェックします。

同じにすべき設定パラメータ

次の挙げるパラメータのいずれかが両方の vPC ピア デバイス上で同じように設定されていないと、誤設定が原因でトラフィック フローに望ましくない動作が発生する可能性があります。

- MAC エージング タイマー
- スタティック MAC エントリ
- VLAN インターフェイス: vPC ピア リンク エンドにある各デバイスの VLAN インターフェイスが両エンドで同じ VLAN 用に設定されていなければならない、さらに同じ管理モードで同じ動作モードになっていなければなりません。ピア リンクの片方のデバイスだけで設定されている VLAN は、vPC またはピア リンクを使用してトラフィックを通過させることはしません。すべての VLAN をプライマリ vPC デバイスとセカンダリ vPC デバイスの両方で作成する必要があります。そうならない VLAN は、停止します。
- ACL のすべての設定とパラメータ
- Quality of Service (QoS) の設定とパラメータ
- STP インターフェイス設定 :
 - BPDU Filter

- BPDU ガード
- コスト
- リンク タイプ
- プライオリティ
- VLAN (Rapid PVST+)
- ポート セキュリティ
- Cisco Trusted Security (CTS)
- ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) スヌーピング
- ネットワーク アクセス コントロール (NAC)
- ダイナミック ARP インスペクション (DAI)
- IP ソース ガード (IPSG)
- インターネット グループ管理プロトコル (IGMP) スヌーピング
- ホット スタンバイ ルーティング プロトコル (HSRP)
- プロトコルに依存しないマルチキャスト (PIM)
- ゲートウェイ ロード バランシング プロトコル (GLBP)
- すべてのルーティング プロトコル設定

すべての設定パラメータで互換性が取れていることを確認するために、vPC の設定が終わったら、各 vPC ピア デバイスの設定を表示してみることを推奨します。

パラメータの不一致によってもたらされる結果

稼働中の vPC で不一致が発生した場合にセカンダリ ピア デバイス上のリンクのみを一時停止する、グレースフル整合性確認機能を設定できます。この機能は CLI のみで設定可能で、デフォルトでイネーブルになっています。

この機能を設定するには、**graceful consistency-check** コマンドを使用します。

一致しなければならないパラメータのリストのすべてのパラメータに関する整合性検査の一部として、システムはすべての VLAN の一貫性をチェックします。

vPC は稼働を継続し、矛盾した VLAN のみがダウンします。この VLAN 単位の整合性検査機能はディセーブルにできず、マルチ スパニングツリー (MST) VLAN には適用されません。

vPC 番号

vPC ドメイン ID と vPC ピア リンクを作成し終わったら、ダウンストリーム デバイスを各 vPC ピア デバイスに接続するためのポート チャネルを作成します。つまり、プライマリ vPC ピア デバイスからダウンストリーム デバイスへのポート チャネルを 1 つ作成し、もう 1 つ、セカンダリ ピア デバイスからダウンストリーム デバイスへのポート チャネルも作成します。



(注)

スイッチとしてもブリッジとしても機能しないホストまたはネットワーク デバイスに接続されているダウンストリーム デバイス上のポートは、STP エッジ ポートとして設定することを推奨します。

各 vPC ピア デバイス上で、ダウンストリーム デバイスに接続するポート チャンネルに vPC 番号を割り当てます。vPC の作成時にトラフィックが中断されることはほとんどありません。すべてのポート番号に、ポート チャンネル自体と同じ vPC ID 番号を割り当てると（つまり、ポート チャンネル 10 には vPC ID 10）、設定が簡単になります。



(注) vPC ピア デバイスからダウンストリーム デバイスに接続するためにポート チャンネルに割り当てる vPC 番号は、**両方の vPC ピア デバイスで同じである必要があります。**

他のポート チャンネルの vPC への移行



(注) ダウンストリーム デバイスは、ポート チャンネルを使用して両方の vPC ピア デバイスに接続する必要があります。

ダウンストリーム デバイスを接続するために、プライマリ vPC ピア デバイスからダウンストリーム デバイスへのポート チャンネルを作成し、セカンダリ ピア デバイスからダウンストリーム デバイスへのもう 1 つのポート チャンネルを作成します。各 vPC ピア デバイス上で、ダウンストリーム デバイスに接続するポート チャンネルに vPC 番号を割り当てます。vPC の作成時にトラフィックが中断されることはほとんどありません。

単一モジュール上での vPC ピア リンクとコアへのリンクの設定



(注) 異なるモジュールの専用ポート上で vPC ピア リンクを設定して、障害発生の可能性を下げることをお勧めします。復元力を最適にしたい環境では、少なくとも 2 つのモジュールを使用してください。

すべての vPC ピア リンクとコアに面するインターフェイスを単一モジュール上で設定しなければならない場合は、両方の vPC ピア デバイス上のすべての vPC ピア リンク上にあり、コアへのレイヤ 3 リンクに関連付けられているトラックオブジェクトとトラックリストをコマンドライン インターフェイスを使用して設定してください。トラックリスト上のすべてのトラッキング対象オブジェクトが停止した場合、システムは次のように動作するため、この設定を使用すれば、その特定のモジュールが停止した場合のトラフィックのドロップを避けることができます。

- vPC プライマリ ピア デバイスによるピアキープアライブ メッセージの送信を停止します。これにより、vPC セカンダリ ピア デバイスが強制的に引き継がれます。
- その vPC ピア デバイス上のすべてのダウンストリーム vPC を停止させます。これにより、すべてのトラフィックが強制的に他の vPC ピア デバイスに向けてそのアクセス スイッチでルーティングされます。

いったんこの機能を設定したら、モジュールに障害が発生した場合には、システムが自動的にプライマリ vPC ピア デバイス上のすべての vPC リンクを停止させ、ピアキープアライブ メッセージを停止します。このアクションにより、vPC セカンダリ デバイスが強制的にプライマリ ロールを引き継がされ、システムが安定するまで、すべての vPC トラフィックがこの新しい vPC プライマリ デバイスに送られます。

コアに対するすべてのリンクおよびすべての vPC ピア リンクを含むトラック リストを、そのオブジェクトとして作成する必要があります。このトラック リストの指定した vPC ドメインに

対して、トラッキングをイネーブルにします。この同じ設定を他方の vPC ピア デバイスにも適用します。オブジェクト トラッキングおよびトラック リストの詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。



(注)

次の例では、Boolean OR を追跡リストで使用し、完全なモジュール障害の場合にのみすべてのトラフィックが vPC ピア デバイスへ流れるよう強制します。コア インターフェイスまたはピア リンクがダウンしたときにスイッチオーバーをトリガーする場合は、次の追跡リストでブール AND を使用します。

単一モジュール上の関連するすべてのインターフェイスが故障したときに vPC をリモートピアに切替えるように追跡リストを設定するには、次の手順に従います。

- ステップ 1** インターフェイス上（コアへのレイヤ 3）およびポート チャネル上（vPC ピア リンク）でトラック オブジェクトを設定します。

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

- ステップ 2** ブール OR を使って追跡リスト内のすべてのインターフェイスを含むトラック リストを作成して、すべてのオブジェクトに障害が発生したときにトリガーします。

```
switch(config)# track 44 list boolean OR
switch(config-track)# object 23
switch(config-track)# object 35
switch(config-track)# object 55
switch(config-track)# end
```

- ステップ 3** このトラック オブジェクトを vPC ドメインに追加します。

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

- ステップ 4** トラック オブジェクトを表示します。

```
switch# show vpc brief
Legend:
          (*) - local vPC is down, forwarding via vPC peer-link
vPC domain id           : 1
Peer status              : peer adjacency formed ok
vPC keep-alive status   : peer is alive
Configuration consistency status: success
vPC role                 : secondary
Number of vPCs configured : 52
Track object             : 44

vPC Peer-link status
-----
id   Port   Status Active vlans
--   ---   -
1    Po100  up     1-5,140

vPC status
-----
id   Port   Status Consistency Reason          Active vlans
--   ---   -
1    Po1    up     success  success          1-5,140
```

次に、オブジェクト トラッキングに関する情報を表示する例を示します。

```
switch# show track brief
Track Type           Instance           Parameter          State  Last
Change
23  Interface          Ethernet8/33      Line Protocol     UP     00:03:05
35  Interface          Ethernet8/35      Line Protocol     UP     00:03:15
44  List               -----          Boolean
or   UP               00:01:19
55  Interface          port-channel100   Line Protocol     UP     00:00:34
```

その他の機能との vPC の相互作用

この項では、次のトピックについて取り上げます。

- 「vPC と LACP」 (P.7-19)
- 「vPC ピア リンクと STP」 (P.7-20)
- 「vPC ピア スイッチ」 (P.7-21)
- 「vPC および ARP または ND」 (P.7-22)
- 「vPC マルチキャスト : PIM、IGMP、および IGMP スヌーピング」 (P.7-22)
- 「vPC ピア リンクとルーティング」 (P.7-24)
- 「vPC および孤立ポート」 (P.7-26)
- 「vPC および孤立ポート」 (P.7-26)

vPC と LACP

LACP は、vPC ドメインのシステム MAC アドレスを使用して、vPC の LACP Aggregation Group (LAG) ID を形成します (LAG-ID と LACP については、第 6 章「ポート チャンネルの設定」を参照してください)。

ダウンストリーム デバイスからのチャンネルも含めて、すべての vPC ポート チャンネル上の LACP を使用できます。LACP は、vPC ピア デバイスの各ポート チャンネル上のインターフェイスのアクティブ モードで設定することを推奨します。この設定により、デバイス、単方向リンク、およびマルチホップ接続の間の互換性をより簡単に検出できるようになり、実行時の変更およびリンク障害に対してダイナミックな応答が可能になります。

vPC ピア リンク デバイスのシステム プライオリティを手動で設定して、vPC ピア リンク デバイスが、接続されているダウンストリーム デバイスより確実に高い LACP プライオリティを持つようにすることを推奨します。システム プライオリティの値が低いほど、高い LACP プライオリティを意味します。



(注)

システム プライオリティを手動で設定する場合は、必ず両方の vPC ピア デバイス上で同じプライオリティ値を割り当てる必要があります。vPC ピア デバイス同士が異なるシステム プライオリティ値を持っていると、vPC は稼働しません。

vPC ピア リンクと STP

vPC はループフリーなレイヤ 2 トポロジを提供しますが、それでもやはり、誤った配線やケーブルの欠陥、誤設定などから保護するためのフェールセーフ メカニズムを STP が提供する必要があります。vPC を初めて稼働させたときに、STP による再コンバージェンスが発生します。STP は、vPC ピア リンクを特殊なリンクとして扱い、常に vPC ピア リンクを STP のアクティブ トポロジに含めます。

すべての vPC ピア リンク インターフェイスを STP ネットワーク ポート タイプに設定して、すべての vPC リンク上で Bridge Assurance が自動的にイネーブルになるようにすることを推奨します。また、vPC ピア リンク上ではどの STP 拡張機能もイネーブルにしないことも推奨します。STP 拡張がすでに設定されている場合、その拡張が vPC ピア リンクの問題の原因となることはありません。

MST と Rapid PVST+ の両方を実行している場合は、必ず PVST シミュレーション機能を正しく設定してください。

STP 拡張機能および PVST シミュレーションについては、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。



(注)

パラメータのリストは、vPC ピア リンクの両サイドの vPC ピア デバイス上で同じになるように設定する必要があります。これらの一致していなければならない必須設定については、「[vPC インターフェイスの互換パラメータ](#)」(P.7-14)を参照してください。

STP は分散しています。つまり、このプロトコルは、両方の vPC ピア デバイス上で実行され続けます。ただし、プライマリ デバイスとして選択されている vPC ピア デバイス上での設定が、セカンダリ vPC ピア デバイス上の vPC インターフェイスの STP プロセスを制御します。

プライマリ vPC デバイスは、Cisco Fabric Services over Ethernet (CFSOE) を使用して、vPC セカンダリ ピア デバイス上の STP の状態を同期させます。CFSOE については、「[vPC および孤立ポート](#)」(P.7-26)を参照してください。

vPC の STP プロセスも、ピア リンク上で接続されているデバイスの 1 つに障害が発生したときにそれを検出するために、定期的なキープアライブ メッセージに依存しています。これらのメッセージについては、「[ピアキープアライブ リンクとメッセージ](#)」(P.7-9)を参照してください。

vPC マネージャが、vPC ピア デバイス間で、プライマリ デバイスとセカンダリ デバイスを設定して 2 つのデバイスを STP 用に調整する提案/ハンドシェイク合意を実行します。その後、プライマリ vPC ピア デバイスが、プライマリ デバイスとセカンダリ デバイス両方での STP プロトコルの制御を行います。プライマリ vPC ピア デバイスを STP プライマリ ルート デバイスとして設定し、セカンダリ vPC デバイスを STP セカンダリ ルート デバイスになるように設定することを推奨します。

プライマリ vPC ピア デバイスがセカンダリ vPC ピア デバイスにフェールオーバーした場合、STP トポロジには何の変化も発生しません。

BPDU は、代表ブリッジ ID フィールドで、STP ブリッジ ID の vPC に設定されている MAC アドレスを使用します。vPC プライマリ デバイスが、vPC インターフェイス上でこれらの BPDU を送信します。

次のパラメータについて同じ STP 設定を使用して、vPC ピア リンクの両エンドを設定する必要があります。

- STP グローバル設定：
 - STP モード
 - MST のための STP リージョン設定

- VLAN ごとのイネーブル/ディセーブル状態
- ブリッジ保証設定
- ポート タイプ設定
- ループ ガード設定
- STP インターフェイス設定：
 - ポート タイプ設定
 - ループ ガード
 - ルート ガード



(注)

これらのパラメータのいずれかに誤設定があった場合、Cisco NX-OS ソフトウェアが vPC 内のすべてのインターフェイスを停止します。syslog をチェックし、**show vpc brief** コマンドを入力して、vPC インターフェイスが停止していないか確認してください。

次の STP インターフェイス設定が、vPC ピア リンクの両側で同じになっていることを確認します。そうならないと、トラフィック フローに予測不能な動作が発生する可能性があります。

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



(注)

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

この機能がイネーブルになっている場合は、**show spanning-tree** コマンドで vPC に関する情報を表示できます。例については、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。



(注)

ダウンストリーム デバイスのポートは、STP エッジ ポートとして設定することを推奨します。スイッチに接続されているすべてのホスト ポートを STP エッジ ポートとして設定してください。STP ポート タイプの詳細については、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。

vPC ピア スイッチ

vPC ピア スイッチ機能は、STP コンバージェンスに関連するパフォーマンス上の問題を解決するために、Cisco NX-OS Release 5.0(2) に追加されました。この機能により、一対の Cisco Nexus 9000 シリーズ デバイスをレイヤ 2 トポロジ内に 1 つの STP ルートとして表示できます。この機能は、STP ルートを vPC プライマリ スイッチに固定する必要性をなくし、vPC プライマリ スイッチに障害が発生した場合の vPC コンバージェンスを向上させます。

ループを回避するために、vPC ピア リンクは STP 計算からは除外されます。vPC ピア スイッチモードでは、ダウンストリーム スイッチでの STP BPDU タイムアウトに関連した問題（この問題は、トラフィックの中断につながります）を避けるために、STP BPDU が両方の vPC ピア デバイスから送信されます。

この機能は、すべてのデバイス vPC に属する純粋なピア スイッチ トポロジで使用できます。



(注) ピア スイッチ機能は、vPC を使用するネットワークでサポートされ、STP ベースの冗長性はサポートされません。ハイブリッド ピア スイッチ設定で vPC ピア リンクに障害が発生すると、トラフィックが失われる場合があります。このシナリオでは、vPC ピアは同じ STP ルート ID や同じブリッジ ID を使用します。アクセス スイッチのトラフィックは 2 つに別れ、その半分が最初の vPC ピアに、残りの半分が 2 番目の vPC ピアに転送されます。ピア リンク障害は、南北のトラフィックには影響がありませんが、東西のトラフィックが失われます。

STP 拡張機能および Rapid PVST+ については、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。

vPC および ARP または ND

Cisco Fabric Service over Ethernet (CFSoE) プロトコルの信頼性が高いトランスポート メカニズムを使用した、vPC ピア間のテーブル同期に対応する機能が Cisco NX-OS リリース 4.2(6) に追加されました。ip arp synchronize および ipv6 nd synchronize コマンドをイネーブルにし、vPC ピア間のアドレス テーブルのコンバージェンスの高速化をサポートする必要があります。このコンバージェンスにより、ピア リンク ポート チャネルがフラップしたり、vPC ピアがオンラインに戻るときに、IPv4 の場合は ARP テーブルの復元でまたは IPv6 の場合は ND テーブルの復元で発生する遅延を解消できます。



(注) mode auto コマンドを使用してこの機能を自動的に有効化できます。このコマンドの使用については、「特定の vPC コマンドの自動イネーブル化」(P.7-41) を参照してください。

vPC マルチキャスト : PIM、IGMP、および IGMP スヌーピング



(注) Nexus 9000 シリーズ デバイスの Cisco NX-OS ソフトウェアは、vPC での Product Independent Multicast (PIM)、Source-Specific Multicast (SSM) または双方向 (PIM) をサポートしません。Cisco NX-OS ソフトウェアは、vPC での PIM Any Source Multicast (ASM) を完全にサポートします。

ソフトウェアが、マルチキャスト フォワーディングを両方の vPC ピア デバイス上で同期された状態に保ちます。vPC ピア デバイス上の IGMP スヌーピング プロセスは、学習したグループ情報を vPC ピア リンクを通じて他の vPC ピア デバイスと共有します。マルチキャスト状態は、常に両方の vPC ピア デバイス上で同期されます。vPC モードでの PIM プロセスは、1 つの vPC ピア デバイスだけが受信者に向けてマルチキャスト トラフィックを転送する状態を確保します。

各 vPC ピアは、レイヤ 2 またはレイヤ 3 デバイスです。マルチキャスト トラフィックは 1 つの vPC ピア デバイスだけから伝送されます。次のシナリオで、重複したパケットが観察される場合があります。

- 孤立ホスト
- 送信元と受信者が、マルチキャスト ルーティングのイネーブルになった異なる VLAN 内のレイヤ 2 vPC クラウド内にあり、vPC メンバ リンクが停止している場合。

次のシナリオで、ごくわずかなトラフィック損失が観察される場合があります。

- トラフィックを転送している vPC ピア デバイスをリロードした場合。
- トラフィックを転送している vPC ピア デバイスの PIM を再起動した場合。

必ずすべてのレイヤ 3 デバイスを両方の vPC ピア デバイスにデュアル接続してください。片方の vPC ピア デバイスが停止した場合、他方の vPC ピア デバイスが、通常どおりにすべてのマルチキャストトラフィックを転送し続けます。

次に、vPC PIM および vPC IGMP/IGMP スヌーピングについて説明します。

- **vPC PIM** : vPC モードの PIM プロセスは、1 台の vPC ピア デバイスのみがマルチキャストトラフィックを転送する状態を確保します。vPC モードの PIM プロセスは、送信元の状態を両方の vPC ピア デバイスと同期させ、トラフィックを転送する vPC ピア デバイスを選出します。
- **vPC IGMP/IGMP スヌーピング** : vPC モードの IGMP プロセスは、両方の vPC ピア デバイスで指定ルータ (DR) 情報を同期させます。デュアル DR は、vPC モードのときに IGMP で利用可能です。デュアル DR は、vPC モードでない場合は利用できません。これは、両方の vPC ピア デバイスがピア間のマルチキャスト グループ情報を保持するためです。



(注)

vPC VLAN (vPC ピア リンクで伝送される VLAN) とダウンストリーム vPC が接続されたレイヤ 3 デバイス間の PIM ネイバー関係はサポートされません。それによりマルチキャストパケットのドロップが生じる場合があります。PIM ネイバー関係がダウンストリームレイヤ 3 デバイスが必要な場合、物理レイヤ 3 インターフェイスを vPC インターフェイスの代わりに使用する必要があります。

IGMP スヌーピングは、両方の vPC ピア デバイス上で同じようにイネーブルにしたりディセーブルにしたりする必要があり、すべての機能設定を同じにする必要があります。IGMP スヌーピングは、デフォルトで有効になっています。



(注)

次のコマンドは、vPC モードでサポートされていません。

- **ip pim spt-threshold infinity**
- **ip pim use-shared-tree-only**

マルチキャストに関する詳細情報については、『Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide』を参照してください。

マルチキャスト PIM デュアル DR (プロキシ DR)

デフォルトでは、マルチキャスト ルータは該当する受信先が存在する場合のみ PIM ジョインをアップストリームに送信します。これらの該当する受信先は、IGMP ホスト (IGMP レポートを通じて通信します) または他のマルチキャスト ルータ (PIM ジョインを通じて通信します) のどちらかの場合があります。

Cisco NX-OS vPC 実装では、PIM はデュアル指定ルータ (DR) モードで動作します。つまり、vPC デバイスが vPC SVI の発信インターフェイス (OIF) 上の DR である場合、そのピアは自動的にプロキシ DR ロールを引き継ぎます。IGMP は、OIF が DR である場合、OIF (レポートはその OIF で学習されます) をフォワーディングに追加します。デュアル DR では、両方の vPC デバイスには、次の例に示すように、vPC SVI OIF に対して同一のエントリ (*,G) があります。

```
VPC Device1:
-----
```

```
(*,G)
  oif1 (igmp)

VPC Device2:
-----
(*,G)
  oif1 (igmp)
```

IP PIM PRE-BUILD SPT

マルチキャスト ソースがレイヤ 3 クラウド (vPC ドメイン外) にある場合、1 つの vPC ピアが送信元のフォワーダとして選定されます。このフォワーダの選択は、送信元に到達するためのメトリックに基づきます。関係がある場合、vPC プライマリはフォワーダとして選択されます。フォワーダのみがその関連する (S,G) 内に vPC OIF を持っており、非フォワーダ (S,G) は 0 OIF を持っています。したがって、フォワーダのみがこの例に示すように、送信元へ PIM (S,G) ジョインを送信します。

```
VPC Device1 (say this is Forwarder for Source 'S'):
-----
(*,G)
  oif1 (igmp)

(S,G)
  oif1 (mrrib)

VPC Device2:
-----
(*,G)
  oif1 (igmp)

(S,G)
  NULL
```

障害が発生した場合 (たとえば、フォワーダのレイヤ 3 リバースパス転送 (RPF) リンクが動作しない、またはフォワーダがリロードされるなど)、現在の非フォワーダが最終的にフォワーダになる場合は、トラフィック取得するために送信元への (S,G) に対する PIM ジョインの送信を開始をする必要があります。送信元に到達するホップ数によって、この操作には時間がかかる場合があります (PIM はホップバイホッププロトコルです)。

この問題を排除し、より優れたコンバージェンスを取得するには、**ip pim pre-build-spt** コマンドを使用します。このコマンドにより、マルチキャスト ルートに 0 OIF があっても PIM はジョインを送信できます。vPC デバイスでは、非フォワーダは送信元へ PIM (S,G) ジョインをアップストリームに送信します。欠点は、非フォワーダからのリンク帯域幅のアップストリームが最終的にそれによってドロップされるトラフィックに使用されることです。コンバージェンスの向上によるメリットは、リンク使用帯域幅をはるかに上回っていることです。したがって、vPC を使用する場合は、このコマンドを使用することを推奨します。

vPC ピア リンクとルーティング

ファースト ホップ ルーティング プロトコル (FHRP) は、vPC と相互運用します。ホットスタンバイルーティングプロトコル (HSRP)、ゲートウェイロード バランシングプロトコル (GLBP)、および仮想ルータ冗長プロトコル (VRRP) のすべてが、vPC と相互運用できます。すべてのレイヤ 3 デバイスを両方の vPC ピア デバイスにデュアル接続することを推奨します。

プライマリ FHRP デバイスは、たとえセカンダリ vPC デバイスがデータトラフィックを転送したとしても、ARP 要求に応答します。

プライマリ vPC ピア デバイスを FHRP アクティブ ルータの最も高いプライオリティで設定しておく、初期の設定確認と vPC/HSRP のトラブルシューティングを簡単にできます。

さらに、`if-hsrp` コンフィギュレーション モードで `priority` コマンドを使用して、vPC ピア リンク上でイネーブルになっているグループの状態がスタンバイになっているか、またはリッスン状態になっている場合のフェールオーバーのしきい値を設定できます。インターフェイスがアップまたはダウンするのを防ぐために下限および上限しきい値を設定できます。

VRRP は、vPC ピア デバイス上で実行されている場合に HSRP とよく似た動作を示します。VRRP は、HSRP を設定したのと同じ方法で設定してください。GLBP については、両方の vPC ピア デバイス上のフォワーダがトラフィックを転送します。

プライマリ vPC ピア デバイスに障害が発生した場合は、セカンダリ vPC ピア デバイスにフェールオーバーされ、FHRP トラフィックはシームレスに流れ続けます。

バックアップ ルーティング パスとして機能するように 2 台の vPC ピア デバイス間にルーティング隣接を設定することを推奨します。1 台の vPC ピア デバイスがレイヤ 3 アップリンクを失うと、その vPC はルーテッド トラフィックを他の vPC ピア デバイスにリダイレクトでき、そのアクティブ レイヤ 3 アップリンクを活用できます。

次の方法で、バックアップのルーティング パス用のスイッチ間リンクを設定できます。

- 2 台の vPC ピア デバイス間でレイヤ 3 リンクを作成します。
- 専用の VLAN インターフェイスを持つ非 VPC VLAN トランクを使用します。
- 専用の VLAN インターフェイスを持つ vPC ピア リンクを使用します。

vPC 環境での HSRP の焼き付け MAC アドレス オプション (`use-bia`) の設定、および任意の FHRP プロトコルのための仮想 MAC アドレスの手動での設定は、推奨できません。これらの設定は、vPC ロード バランシングに不利な影響を与えるためです。HSRP `use-bia` オプションは、vPC ではサポートされていません。カスタム MAC アドレスを設定するには、両方の vPC ピア デバイスに同じ MAC アドレスを設定する必要があります。

`delay restore` コマンドを使用して、ピアの隣接関係が確立され VLAN インターフェイスが再びアップ状態になるまで vPC の再稼働を遅延させるための復元タイマーを設定することができます。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。この機能を設定するには、`delay restore` コマンドを使用します。

復元した vPC ピア デバイス上の VLAN インターフェイスが稼働するのを遅延するには、`interfaces-vlan` オプションを `delay restore` コマンドに使用します。

FHRP およびルーティングに関する詳細情報については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

CFSoS

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

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

CFSoS 転送は、各 VDC にローカルです。

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



(注) **no cfs eth distribute** コマンドと **no cfs distribute** コマンドは入力しないでください。CFSoE for vPC 機能のための CFSoE をイネーブルにしなければなりません。vPC をイネーブルにしてこれらのコマンドのいずれかを入力すると、エラー メッセージが表示されます。

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

CFS は、TCP/IP を介したデータも転送します。IP 経由の CFS の詳細については、『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』を参照してください。



(注) CFS リージョンはサポートされていません。

vPC および孤立ポート

vPC 対応でないデバイスが各ピアに接続するとき、接続されたポートは vPC のメンバではないため、孤立ポートと称されます。一方のピアへのデバイスのリンクがアクティブ（フォワーディング）になり、他方のリンクは STP のためスタンバイ（ブロッキング）になります。

ピアリンク障害またはリストアが発生すると、孤立ポートの接続は vPC 障害または復元プロセスにバインドされる可能性があります。たとえば、デバイスのアクティブな孤立ポートがセカンダリ vPC ピアに接続する場合、ピアリンク障害が発生し、vPC ポートがセカンダリピアによって一時停止されると、そのデバイスはプライマリピアを経由する接続を失います。セカンダリピアがアクティブな孤立ポートも一時停止した場合は、デバイスのスタンバイポートがアクティブになり、プライマリピアへの接続が提供され、接続が復元されます。セカンダリピアが vPC ポートを一時停止するとき特定の孤立ポートがそのピアによって一時停止され、vPC が復元されるとそのポートが復元されるように CLI で設定できます。

仮想化のサポート

1 つの vPC 内のすべてのポートが、同じ VDC 内になくてもなりません。このバージョンのソフトウェアは、VDC ごとに 1 つの vPC ドメインしかサポートしません。各 VDC で 1 ~ 4096 の番号を使用して、vPC に番号を付けることができます。

停電後の vPC リカバリ

データセンターの停電時には、vPC を含む両方の Cisco Nexus 9000 シリーズ デバイスがリロードされます。場合によっては、1 つのピアのみが復元される場合があります。機能するピア キープアライブまたはピアリンクがないと、vPC は正常に機能することができません。しかし、Cisco NX-OS リリースによっては、vPC サービスが機能するピアのローカルポートのみを使用するようにする方法が利用可能です。

自動リカバリ

Cisco Nexus 9000 シリーズ デバイスは、**auto-recovery** コマンドを使用して、そのピアがオンラインになるのに失敗した場合に vPC サービスを復元するように設定できます。この設定は、スタートアップ コンフィギュレーションに保存しなければなりません。リロード時に、ピアリンクがダウンし、3 回連続してピアキープアライブ メッセージが失われた場合、セカンダリ デバイスはプライマリ STP ロールとプライマリ LACP ロールを引き継ぎます。ソフトウェアが

vPC を初期化し、そのローカル ポートを稼働させ始めます。ピアがないため、ローカル vPC ポートの一貫性チェックはバイパスされます。デバイスは、自身をそのロール プライオリティに関係なく STP プライマリに選出し、LACP ポート ロールのマスターとしても機能します。



(注) **mode auto** コマンドを使用してこの機能を自動的に有効化できます。このコマンドの使用については、「特定の vPC コマンドの自動イネーブル化」(P.7-41) を参照してください。

リカバリ後の vPC ピア ロール

ピア デバイスのリロードが完了し、隣接が形成されたら、次のプロセスが発生します。

1. 最初の vPC ピアがその現在のロールを維持して、その他のプロトコルへの任意の移行リセットを回避します。ピアが、他の可能なロールを受け入れます。
2. 隣接が形成されたら、整合性検査が実行され、適切なアクションが取られます。

ハイアベイラビリティ

In-Service Software Upgrade (ISSU) では、最初の vPC デバイス上のソフトウェア リロード プロセスが、vPC 通信チャネルを介した CFS メッセージングを使用して、その vPC ピア デバイスをロックします。一度に 1 つのデバイスだけアップグレードできます。最初のデバイスは、そのアップグレードが完了したら、そのピア デバイスのロックを解除します。次に、2 つ目のデバイスが、最初のデバイスが行ったのと同じように最初のデバイスをロックして、アップグレード プロセスを実行します。アップグレード中は、2 つの vPC デバイスが一時的に異なるリリースの Cisco NX-OS を実行することになりますが、その下位互換性サポートにより、システムは正常に機能します。



(注) ハイアベイラビリティ機能の詳細については、『Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide』を参照してください。

vPC のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	vPC にライセンスは必要ではありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。

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 ピアは、アップグレードまたはダウングレード プロセス中に、異なるバージョンの NX-OS ソフトウェアのみを稼働できます。
- アップグレード/ダウングレード期間外に異なるバージョンを実行する vPC ピアはサポートされません。

- 1 つの vPC のすべてのポートが、同じ VDC 内になくはなりません。
- vPC を設定するには、まず vPC をイネーブルにする必要があります。
- システムが vPC ピア リンクを形成するには、その前にピアキープアライブ リンクとピアキープアライブ メッセージを設定する必要があります。
- vPC に入れられるのは、レイヤ 2 ポート チャンネルだけです。
- 両方の vPC ピア デバイスを設定しなければなりません。設定が片方のデバイスから他方へ送信されることはありません。
- マルチレイヤ (バックツーバック) vPC を設定するには、それぞれの vPC に一意の vPC ドメイン ID を割り当てる必要があります。
- 必要な設定パラメータが、vPC ピア リンクの両側で互換性を保っているかチェックしてください。互換性に関する推奨事項については、「[vPC インターフェイスの互換パラメータ \(P.7-14\)](#)」を参照してください。
- vPC の設定中に、最小限のトラフィックの中断が発生する可能性があります。
- vPC 上での BIDR PIM および SSM はサポートされていません。
- vPC 環境での DHCP スヌーピング、DAI、IPSG はサポートされていません。DHCP リレーはサポートされています。
- CFS リージョンはサポートされていません。
- ポート チャンネル上でのポート セキュリティは、サポートされていません。
- vPC 内の LACP を使用するすべてのポート チャンネルを、アクティブ モードのインターフェイスで設定することを推奨します。
- この目的には VLAN ネットワーク インターフェイスを使用するよりも、vPC ピア デバイスからのルーティングのためのレイヤ 3 リンクを別途設定してください。
- バックツーバックのマルチレイヤ vPC トポロジでは、それぞれの vPC に一意のドメイン ID が必要です。
- vPC を使用する場合は、FHRP (HSRP、VRRP、GLBP) にデフォルトのタイマーを使用し、PIM 設定を行うことを推奨します。アグレッシブ タイマーを vPC 設定で使用すると、コンバージェンス時間のメリットがありません。
- vPC 環境で open shortest path first (OSPF) を設定する場合は、コア スイッチ上でルータ コンフィギュレーション モードで次のタイマー コマンドを使用することにより、vPC ピア リンクがシャットダウンしたときに OSPF の高速コンバージェンスを実現します。

```
switch (config-router)# timers throttle spf 1 50 50
switch (config-router)# timers lsa-arrival 10
```

OSPF に関する詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

- HSRP の BFD は、vPC 環境ではサポートされていません。
- STP ポート コストは、vPC 環境で 200 に固定されています。
- ジャンボ フレームは、vPC ピア リンクではデフォルトでイネーブルです。

デフォルト設定値

表 7-1 に、vPC パラメータのデフォルト設定を示します。

表 7-1 デフォルト vPC パラメータ

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

vPC の設定



(注)

vPC ピア リンクの両側のデバイス両方でこれらの手順を使用する必要があります。両方の vPC ピア デバイスをこの手順で設定します。

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

- 「vPC のイネーブル化」 (P.7-30)
- 「vPC のディセーブル化」 (P.7-31)
- 「vPC ドメインの作成と vpc-domain モードの開始」 (P.7-32)
- 「vPC キーブアライブ リンクと vPC キーブアライブ メッセージの設定」 (P.7-33)
- 「vPC ピア リンクの作成」 (P.7-35)
- 「vPC ピアゲートウェイの設定」 (P.7-36)
- 「グレースフル整合性検査の設定」 (P.7-37)
- 「vPC ピア リンクの設定の互換性チェック」 (P.7-38)
- 「他のポート チャネルの vPC への移行」 (P.7-39)
- 「特定の vPC コマンドの自動イネーブル化」 (P.7-41)
- 「vPC ドメイン MAC アドレスの手動での設定」 (P.7-43)
- 「システム プライオリティの手動での設定」 (P.7-44)
- 「vPC ピア デバイス ロールの手動での設定」 (P.7-45)
- 「シングルモジュール vPC でのトラッキング機能の設定」 (P.7-46)
- 「停電後のリカバリの設定」 (P.7-48)
- 「孤立ポートの一時停止の設定」 (P.7-52)
- 「vPC ピア スイッチの設定」 (P.7-53)



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

vPC のイネーブル化

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	feature vpc 例: switch(config)# feature vpc	デバイス上で vPC をイネーブルにします。
ステップ 3	exit 例: switch(config)# exit switch#	グローバル コンフィギュレーション モードを終了します。
ステップ 4	show feature 例: switch# show feature	(任意) デバイス上でイネーブルになっている機能を表示します。
ステップ 5	copy running-config startup-config 例: switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例は、vPC 機能をイネーブルにする方法を示します。

```
switch# configure terminal
switch(config)# feature vpc
switch(config)# exit
switch(config)#
```

vPC のディセーブル化



(注) vPC 機能をディセーブルにすると、デバイス上のすべての vPC 設定がクリアされます。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no feature vpc 例: switch(config)# no feature vpc	デバイスの vPC をディセーブルにします。
ステップ 3	exit 例: switch(config)# exit switch#	グローバル コンフィギュレーション モードを終了します。
ステップ 4	show feature 例: switch# show feature	(任意) デバイス上でイネーブルになっている機能を表示します。
ステップ 5	copy running-config startup-config 例: switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例は、vPC 機能をディセーブルにする方法を示します。

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

vPC ドメインの作成と vpc-domain モードの開始

vPC ドメインを作成し、両方の vPC ピア デバイス上で vPC ピア リンク ポート チャンネルを同じ vPC ドメイン内に置くことができます。1 つの VDC 全体を通じて一意の vPC ドメイン番号を使用してください。このドメイン ID は、vPC システム MAC アドレスを自動的に形成するのに使用されます。

このコマンドを使用して、vpc-domain コマンド モードを開始することもできます。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vpc domain domain-id 例: switch(config)# vpc domain 5 switch(config-vpc-domain)#	デバイス上に vPC ドメインを作成し、設定目的で vpc-domain コンフィギュレーション モードを開始します。デフォルトはありません。指定できる範囲は 1 ~ 1000 です。
ステップ 3	exit 例: switch(config-vpc-domain)# exit switch(config)#	vpc-domain コンフィギュレーション モードを終了します。
ステップ 4	show vpc brief 例: switch# show vpc brief	(任意) 各 vPC ドメインに関する簡単な情報を表示します。
ステップ 5	copy running-config startup-config 例: switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、vPC ドメインを作成する例を示します。

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

```
switch(config)#
```

次に、vpc-domain コマンド モードを開始して、既存の vPC ドメインを設定する例を示します。

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

vPC キープアライブ リンクと vPC キープアライブ メッセージの設定



(注) システムで vPC ピア リンクを形成できるようにするには、まず vPC ピアキープアライブ リンクを設定する必要があります。

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



(注) vPC ピアキープアライブ リンクを使用する際は、個別の VRF インスタンスを設定して、各 vPC ピア デバイスからその VRF にレイヤ 3 ポートを接続することを推奨します。ピア リンク自体を使用して vPC ピアキープアライブ メッセージを送信しないでください。VRF の作成および設定方法については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

ピアキープアライブ メッセージに使用される送信元と宛先の両方の IP アドレスがネットワーク内で一意であることを確認してください。

管理ポートと管理 VRF が、これらのキープアライブ メッセージのデフォルトです。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain domain-id**
3. **peer-keepalive destination ip address [hold-timeout secs | interval msec {timeout secs} | precedence {prec-value | network | internet | critical | flash-override | flash | immediate | priority | routine}] | {tos {tos-value | max-reliability | max-throughput | min-delay | min-monetary-cost | normal}} | tos-byte tos-byte-value | source i,paddress | udp-port number | vrf {name | management | vpc-keepalive}]**
4. **exit**
5. (任意) **show vpc statistics**
6. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vpc domain domain-id 例: switch(config)# vpc domain 5 switch(config-vpc-domain)#	デバイスで 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。
ステップ 3	peer-keepalive destination ipaddress [hold-timeout secs interval msec {timeout secs} {precedence {prec-value network internet critical flash-override flash immediate priority routine}} tos {tos-value max-reliability max-throughput min-delay min-monetary-cost normal}} tos-byte tos-byte-value} source ipaddress vrf {name management vpc-keepalive}] 例: switch(config-vpc-domain)# peer-keepalive destination 172.28.230.85 switch(config-vpc-domain)#	vPC ピアキープアライブ リンクのリモート エンドの IPv4 アドレスを設定します。 (注) vPC ピアキープアライブ リンクを設定するまで、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。 (注) 独立した VRF を設定し、vPC ピアキープアライブ リンクのための VRF 内の各 vPC ピア デバイスからのレイヤ 3 ポートを使用することを推奨します。VRF の作成および設定の詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。
ステップ 4	exit 例: switch(config-vpc-domain)# exit switch(config)#	vpc-domain コンフィギュレーション モードを終了します。
ステップ 5	show vpc statistics 例: switch# show vpc statistics	(任意) キープアライブ メッセージの設定に関する情報を表示します。
ステップ 6	copy running-config startup-config 例: switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

VRF の設定方法については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

次の例は、vPC ピアキープアライブ リンクの宛先と送信元の IP アドレスおよび VRF を設定する方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 100
switch(config-vpc-domain)# peer-keepalive destination 172.168.1.2 source 172.168.1.1 vrf
vpc-keepalive
switch(config-vpc-domain)# exit
switch#
```

vPC ピア リンクの作成

vPC ピア リンクを作成するには、指定した vPC ドメインのピア リンクとするポート チャネルを各デバイス上で指定します。冗長性を確保するため、トランク モードで vPC ピア リンクとして指定したレイヤ 2 ポート チャネルを設定し、各 vPC ピア デバイス上の個別のモジュールで 2 つのポートを使用することを推奨します。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

レイヤ 2 ポート チャネルを使用していることを確認します。

手順の概要

1. **configure terminal**
2. **interface port-channel *channel-number***
3. (任意) **switchport mode trunk**
4. (任意) **switchport trunk allowed vlan *vlan-list***
5. **vpc peer-link**
6. **exit**
7. (任意) **show vpc brief**
8. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel <i>channel-number</i> 例: switch(config)# interface port-channel 20 switch(config-if)#	このデバイスの vPC ピア リンクとして使用するポート チャネルを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switchport mode trunk 例: switch(config-if)# switchport mode trunk	(任意) このインターフェイスをトランク モードで設定します。
ステップ 4	switchport trunk allowed vlan <i>vlan-list</i> 例: switch(config-if)# switchport trunk allowed vlan 1-120,201-3967	(任意) 許容 VLAN リストを設定します。
ステップ 5	vpc peer-link 例: switch(config-if)# vpc peer-link switch(config-vpc-domain)#	選択したポート チャネルを vPC ピア リンクとして設定し、vpc-domain コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 6	exit 例： switch(config-vpc-domain)# exit switch(config)#	vpc-domain コンフィギュレーション モードを終了します。
ステップ 7	show vpc brief 例： switch# show vpc brief	(任意) 各 vPC に関する情報を表示します。 vPC ピア リンクに関する情報も表示されます。
ステップ 8	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例は、vPC ピア リンクを設定する方法を示します。

```
switch# configure terminal
switch(config)# interface port-channel 20
switch(config-if)# switchport mode
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1-120,201-3967
switch(config-if)# vpc peer-link
switch(config-vpc-domain)# exit
switch(config)#
```

vPC ピアゲートウェイの設定

vPC ピア デバイスを、vPC ピア デバイスの MAC アドレスに送信されるパケットに対してゲートウェイとして機能するように設定できます。



(注)

vPC ドメインにレイヤ 3 デバイスを接続した場合、vPC ピアリンク上でも送信される VLAN を使用したルーティング プロトコルのピアリンクはサポートされません。vPC ピア デバイスおよび汎用レイヤ 3 デバイスの間でルーティング プロトコルの隣接関係が必要な場合は、相互接続に物理的にルーティングされたインターフェイスを使用する必要があります。vPC ピアゲートウェイ機能の使用では、この要件は変わりません。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vpc domain domain-id 例： switch(config-if)# vpc domain 5 switch(config-vpc-domain)#	vPC ドメインがまだ存在していない場合はそれを作成し、vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	peer-gateway 例： switch(config-vpc-domain)# peer-gateway (注) -----:: Disable IP redirects on all interface-vlans of this vPC domain for correct operation of this feature ::-----	ピアのゲートウェイ MAC アドレスを宛先とするパケットのレイヤ 3 フォワーディングをイネーブルにします。
ステップ 4	exit 例： switch(config-vpc-domain)# exit switch(config)#	vpc-domain コンフィギュレーション モードを終了します。
ステップ 5	show vpc brief 例： switch# show vpc brief	(任意) 各 vPC に関する情報を表示します。vPC ピア リンクに関する情報も表示されます。
ステップ 6	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

グレースフル整合性検査の設定

デフォルトでイネーブルになるグレースフル整合性検査機能を設定できます。この機能がイネーブルでない場合、必須互換性パラメータの不一致が動作中の vPC で導入されると、vPC は完全に一時停止します。この機能がイネーブルの場合、セカンダリ ピア デバイスのリンクだけが一時停止します。vPC の一貫した設定については、「[vPC インターフェイスの互換パラメータ](#)」(P.7-14) を参照してください。

手順の概要

1. **configure terminal**
2. **vpc domain domain-id**
3. **graceful consistency-check**
4. **exit**
5. (任意) **show vpc brief**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vpc domain domain-id 例: switch(config-if)# vpc domain 5 switch(config-vpc-domain)#	vPC ドメインがまだ存在していない場合はそれを作成し、vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	graceful consistency-check 例: switch(config-vpc-domain)# graceful consistency-check	必須互換性パラメータで不一致が検出された場合に、セカンダリ ピア デバイスのリンクのみが一時停止するということを指定します。 この機能をディセーブルにする場合は、このコマンドの no 形式を使用します。
ステップ 4	exit 例: switch(config-vpc-domain)# exit switch(config)#	vpc-domain コンフィギュレーション モードを終了します。
ステップ 5	show vpc brief 例: switch# show vpc brief	(任意) vPC に関する情報を表示します。

次に、グレースフル整合性検査機能をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# graceful consistency-check
switch(config-vpc-domain)# exit
switch(config)#
```

vPC ピア リンクの設定の互換性チェック

両方の vPC ピア デバイス上の vPC ピア リンクを設定した後に、すべての vPC インターフェイスで設定が一貫していることをチェックします。vPC の一貫した設定については、「[vPC インターフェイスの互換パラメータ](#)」(P.7-14) を参照してください。

手順の概要

1. **configure terminal**
2. (任意) **show vpc consistency-parameters {global | interface port-channel channel-number}**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	show vpc consistency-parameters {global interface port-channel channel-number} 例： switch(config)# show vpc consistency-parameters global switch(config)#	(任意) すべての vPC インターフェイス全体で一貫している必要があるパラメータのステータスを表示します。

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

```
switch# configure terminal
switch(config)# show vpc consistency-parameters global
switch(config)#
```



(注) vPC インターフェイス設定の互換性に関するメッセージが syslog にも記録されます。

他のポート チャネルの vPC への移行



(注) 冗長性を確保するために、vPC ドメイン ダウンストリーム ポート チャネルを 2 つのデバイスに接続することを推奨します。

ダウンストリーム デバイスに接続するには、ダウンストリーム デバイスからプライマリ vPC ピア デバイスへのポート チャネルを作成し、ダウンストリーム デバイスからセカンダリ ピア デバイスへのもう 1 つのポート チャネルを作成します。各 vPC ピア デバイス上で、ダウンストリーム デバイスに接続するポート チャネルに vPC 番号を割り当てます。vPC の作成時にトラフィックが中断されることはほとんどありません。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。
レイヤ 2 ポート チャネルを使用していることを確認します。

手順の概要

1. **configure terminal**
2. **interface port-channel channel-number**
3. **vpc number**
4. **exit**

5. (任意) **show vpc brief**
6. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel channel-number 例: switch(config)# interface port-channel 20 switch(config-if)#	ダウンストリーム デバイスに接続するために vPC に入れるポート チャンネルを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	vpc number 例: switch(config-if)# vpc 5 switch(config-vpc-domain)#	選択したポート チャンネルを vPC に入れてダウンストリーム デバイスに接続するように設定します。これらのポート チャンネルには、デバイス内の任意のモジュールを使用できます。範囲は、1 ~ 4096 です。 (注) vPC ピア デバイスからダウンストリーム デバイスに接続されているポート チャンネルに割り当てる vPC 番号は、 <i>両方の vPC デバイスで同じでなければなりません。</i>
ステップ 4	exit 例: switch(config-vpc-domain)# exit switch(config)#	vpc-domain コンフィギュレーション モードを終了します。
ステップ 5	show vpc brief 例: switch# show vpc brief	(任意) vPC に関する情報を表示します。
ステップ 6	copy running-config startup-config 例: switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、ダウンストリーム デバイスに接続するポート チャンネルを設定する例を示します。

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

特定の vPC コマンドの自動イネーブル化

mode auto コマンドを使用して、次のコマンドを自動的および同時にイネーブルにできます。
peer-gateway、**auto-recovery**、**ip arp synchronize**、および **ipv6 nd synchronize**。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

手順の概要

1. **configure terminal**
2. **feature vpc**
3. **vpc domain domain-id**
4. **[no] mode auto**
5. **exit**
6. (任意) **show running-config vpc**
7. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	feature vpc 例： switch(config)# feature vpc	デバイス上で vPC をイネーブルにします。
ステップ 3	vpc domain domain-id 例： switch(config)# vpc domain 1 switch(config-vpc-domain)#	デバイスで 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。指定できる範囲は 1 ~ 1000 です。
ステップ 4	[no] mode auto 例： switch(config-vpc-domain)# mode auto	次のコマンドを同時にイネーブルにします。 peer-gateway 、 auto-recovery 、 ip arp synchronize 、および ipv6 nd synchronize 。 この機能をディセーブルにする場合は、このコマンドの no 形式を使用します。
ステップ 5	exit 例： switch(config-vpc-domain)# exit switch(config)#	vpc ドメイン コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 6	exit 例: switch(config)# exit switch#	グローバル コンフィギュレーション モードを終了します。
ステップ 7	show running-config vpc 例: switch# show running-config vpc	(任意) イネーブルにするコマンドを含む vPC に関する情報を表示します。
ステップ 8	copy running-config startup-config 例: switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次のコマンドを同時にイネーブルにする例を次に示します。 **peer-gateway**、**auto-recovery**、**ip arp synchronize**、および **ipv6 nd synchronize**。

```
switch# configure terminal
switch# feature vpc
switch(config)# vpc domain 1
switch(config-vpc-domain)# mode auto
The following commands are executed:
peer-gateway ;
auto-recovery ;
ip arp synchronize ;
ipv6 nd synchronize ;
```

Warning:

Enables restoring of vPCs in a peer-detached state after reload, will wait for 240 seconds to determine if peer is un-reachable

```
switch(config-vpc-domain)# exit
switch(config)# exit
switch# show running-config vpc
```

```
!Command: show running-config vpc
!Time: Thu Feb 18 12:31:42 2013
```

```
version 6.2(2)
feature vpc

vpc domain 1
peer-gateway
auto-recovery
ip arp synchronize
ipv6 nd synchronize
```

vPC ドメイン MAC アドレスの手動での設定

vPC ドメインを作成すると、Cisco NX-OS ソフトウェアが自動的に vPC システム MAC アドレスを作成します。このアドレスは、LACP など、リンク スコープに制限される操作に使用されます。ただし、vPC ドメインの MAC アドレスを手動で設定するように選択することもできます。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vpc domain <i>domain-id</i> 例： switch(config)# vpc domain 5 switch(config-vpc-domain)#	設定する vPC ドメインの番号を入力します。システムは、vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	system-mac <i>mac-address</i> 例： switch(config-vpc-domain)# system-mac 23fb.4ab5.4c4e switch(config-vpc-domain)#	指定した vPC ドメインに割り当てる MAC アドレスを <code>aaaa.bbbb.cccc</code> の形式で入力します。
ステップ 4	exit 例： switch(config-vpc-domain)# exit switch(config)#	vpc-domain コンフィギュレーション モードを終了します。
ステップ 5	show vpc role 例： switch# show vpc brief	(任意) vPC システム MAC アドレスを表示します。
ステップ 6	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例は、vPC ドメイン MAC アドレスを手動で設定する方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# system-mac 13gb.4ab5.4c4e
switch(config-vpc-domain)# exit
switch(config)#
```

システムプライオリティの手動での設定

vPC ドメインを作成すると、vPC システムプライオリティが自動的に作成されます。ただし、vPC ドメインのシステムプライオリティは手動で設定することもできます。



(注) LACP の実行時には、vPC ピア デバイスが LACP のプライマリ デバイスになるように、vPC システムプライオリティを手動で設定することを推奨します。システムプライオリティを手動で設定する場合には、必ず同じプライオリティ値を両方の vPC ピア デバイスに設定します。これらの値が一致しないと、vPC は起動しません。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain domain-id**
3. **system-priority priority**
4. **exit**
5. (任意) **show vpc role**
6. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vpc domain domain-id 例: switch(config)# vpc domain 5 switch(config-vpc-domain)#	設定する vPC ドメインの番号を入力します。システムは、vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	system-priority priority 例: switch(config-vpc-domain)# system-priority 4000 switch(config-vpc-domain)#	指定した vPC ドメインに割り当てるシステムプライオリティを入力します。指定できる値の範囲は、1 ~ 65535 です。デフォルト値は 32667 です。

	コマンド	目的
ステップ 4	exit 例： switch(config-vpc-domain)# exit switch(config)#	vpc-domain コンフィギュレーション モードを終了します。
ステップ 5	show vpc role 例： switch# show vpc role	(任意) vPC システム プライオリティを表示します。
ステップ 6	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例は、vPC ドメインのシステム プライオリティを手動で設定する方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# system-priority 4000
switch(config-vpc-domain)# exit
switch(config)#
```

vPC ピア デバイス ロールの手動での設定

デフォルトでは、vPC ドメインと、vPC ピア リンクの両端を設定すると、Cisco NX-OS ソフトウェアはプライマリとセカンダリの vPC ピア デバイスを選択します。ただし、vPC のプライマリ デバイスとして、特定の vPC ピア デバイスを選択することもできます。選択したら、プライマリ デバイスにする vPC ピア デバイスに、他の vPC ピア デバイスより小さいロール値を手動で設定します。

vPC はロールのプリエンブションをサポートしません。プライマリ vPC ピア デバイスに障害が発生すると、セカンダリ vPC ピア デバイスが、vPC プライマリ デバイスの機能を引き継ぎます。ただし、以前のプライマリ vPC が再起動しても、機能のロールは元に戻りません。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain *domain-id***
3. **role priority *priority***
4. **exit**
5. (任意) **show vpc role**
6. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vpc domain domain-id 例: switch(config)# vpc domain 5 switch(config-vpc-domain)#	設定する vPC ドメインの番号を入力します。システムは、vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	role priority priority 例: switch(config-vpc-domain)# role priority 4 switch(config-vpc-domain)#	vPC システム プライオリティに与えるロール プライオリティを入力します。指定できる値の範囲は 1 ~ 65636 で、デフォルト値は 32667 です。低い値は、このスイッチがプライマリ vPC になる可能性が高いということを意味します。
ステップ 4	exit 例: switch(config-vpc-domain)# exit switch(config)#	vpc-domain コンフィギュレーション モードを終了します。
ステップ 5	show vpc role 例: switch# show vpc role	(任意) vPC システム プライオリティを表示します。
ステップ 6	copy running-config startup-config 例: switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例は、vPC ピア デバイスのロール プライオリティを手動で設定する方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# role priority 4
switch(config-vpc-domain)# exit
switch(config)#
```

シングルモジュール vPC でのトラッキング機能の設定

すべての vPC ピア リンクとコアに面するインターフェイスを単一モジュール上で設定しなければならない場合は、両方のプライマリ vPC ピア デバイス上の vPC ピア リンクのすべてのリンク上にあり、コアへのレイヤ 3 リンクに関連付けられているトラック オブジェクトとトラック リストを設定しなければなりません。いったんこの機能を設定したら、プライマリ vPC ピア デバイ스에 障害が発生した場合には、プライマリ vPC ピア デバイス上のすべての vPC リンクを、システムが自動的に停止します。システムが安定するまでは、このアクションにより、すべての vPC トラフィックが強制的にセカンダリ vPC ピア デバイスに送られます。

この設定は、両方の vPC ピア デバイスに置かなければなりません。さらに、いずれの vPC ピア デバイスも機能上のプライマリ vPC ピア デバイスになる場合があるため、両方の vPC ピア デバイスに同じ設定を置いておく必要があります。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

トラック オブジェクトとトラック リストが設定済みであることを確認します。コアおよび vPC ピア リンクに接続されているすべてのインターフェイスが両方の vPC ピア デバイス上のトラックリスト オブジェクトに割り当てられていることを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain *domain-id***
3. **track *track-object-id***
4. **exit**
5. (任意) **show vpc**
6. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vpc domain <i>domain-id</i> 例: switch(config)# vpc domain 5 switch(config-vpc-domain)#	設定する vPC ドメインの番号を入力し、vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	track <i>track-object-id</i> 例: switch(config-vpc-domain)# track object 23 switch(config-vpc-domain)#	以前に関連するインターフェイスで設定されたトラックリスト オブジェクトを vPC ドメインに追加します。オブジェクト トラッキングおよびトラック リストの詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。
ステップ 4	exit 例: switch(config-vpc-domain)# exit switch(config)#	vpc-domain コンフィギュレーション モードを終了します。
ステップ 5	show vpc brief 例: switch# show vpc brief	(任意) 追跡対象オブジェクトに関する情報を表示します。
ステップ 6	copy running-config startup-config 例: switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、以前に設定されたトラック リスト オブジェクトを、vPC ピア デバイス上の vPC ドメインに配置する例を示します。

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

停電後のリカバリの設定

停電が発生すると、vPC はピア隣接がスイッチ リロード時に形成するのを待ちます。この状況は、許容範囲内に収まらないほど長いサービスの中断に至る場合があります。Cisco Nexus 9000 シリーズ デバイスは、そのピアがオンラインになるのに失敗した場合に vPC サービスを復元するように設定できます。

リロード復元の設定



(注)

このセクションで説明されている **reload restore** コマンドおよび手順は廃止されます。**auto-recovery** コマンドおよび「[自動リカバリの設定](#)」(P.7-50) で説明されている手順を使用することを推奨します。

Cisco Nexus 9000 シリーズ デバイスは、**reload restore** コマンドを使用して、そのピアがオンラインになるのに失敗した場合に vPC サービスを復元するように設定できます。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain *domain-id***
3. **reload restore [*delay time-out*]**
4. **exit**
5. (任意) **show running-config vpc**
6. (任意) **show vpc consistency-parameters interface port-channel *number***
7. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vpc domain domain-id 例： switch(config)# vpc domain 5 switch(config-vpc-domain)#	設定する vPC ドメインの番号を入力し、vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	reload restore [delay time-out] 例： switch(config-vpc-domain)# reload restore	vPC がそのピアが機能しないことを前提として vPC を稼働させ始めるように設定します。デフォルト遅延値は 240 秒です。タイムアウト遅延は 240 ~ 3600 秒の間で設定できます。 vPC をデフォルト設定にリセットするには、このコマンドの no 形式を使用します。
ステップ 4	exit 例： switch(config-vpc-domain)# exit switch(config)#	vpc-domain コンフィギュレーション モードを終了します。
ステップ 5	show running-config vpc 例： switch# show running-config vpc	(任意) vPC に関する情報、特にリロード ステータスを表示します。
ステップ 6	show vpc consistency-parameters interface port-channel number 例： switch# show vpc consistency-parameters interface port-channel 1	(任意) 指定したインターフェイスの vPC の一貫性パラメータに関する情報を表示します。
ステップ 7	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。 (注) リロード機能がイネーブルになっていることを確認するには、この手順を実行します。

次に、vPC リロード復元機能を設定し、それをスイッチのスタートアップ コンフィギュレーションに保存する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vpc domain 5
switch(config-vpc-domain)# reload restore
Warning:
  Enables restoring of vPCs in a peer-detached state after reload, will wait for 240
seconds (by default) to determine if peer is un-reachable
switch(config-vpc-domain)# exit
switch(config)# exit
switch# copy running-config startup-config
switch# show running-config vpc
```

```
!Command: show running-config vpc
!Time: Wed Mar 24 18:43:54 2010
```

```
version 5.0(2)
feature vpc

logging level vpc 6
vpc domain 5
  リロード復元
```

次の例は、一貫性パラメータを確認する方法を示します。

```
switch# show vpc consistency-parameters interface port-channel 1
Legend:
  Type 1 : vPC will be suspended in case of mismatch
Name          Type Local Value Peer Value
-----
STP Port Type      1   Default      -
STP Port Guard     1   None          -
STP MST Simulate PVST mode 1   Default      -
Speed             1   1000 Mb/s     -
Duplex            1   full          -
Port Mode         1   trunk         -
Native Vlan       1   1             -
MTU               1   1500          -
Allowed VLANs     -   1-3967,4048-4093 -
Local suspended VLANs -   -             -
```

自動リカバリの設定

Cisco Nexus 9000 シリーズ デバイスは、**auto-recovery** コマンドを使用して、そのピアがオンラインになるのに失敗した場合に vPC サービスを復元するように設定できます。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain *domain-id***
3. **auto-recovery [reload-delay *time*]**
4. **exit**
5. (任意) **show running-config vpc**
6. (任意) **show vpc consistency-parameters interface port-channel *number***
7. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vpc domain domain-id 例： switch(config)# vpc domain 5 switch(config-vpc-domain)#	設定する vPC ドメインの番号を入力し、vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	auto-recovery [reload-delay time] 例： switch(config-vpc-domain)# auto-recovery	vPC がそのピアが機能しないことを前提として vPC を稼働させ始めるように設定し、vPC を復元するためのリロード後に待機する時間を指定します。デフォルト遅延値は 240 秒です。240 ~ 3600 秒の遅延を設定できます。 vPC をデフォルト設定にリセットするには、このコマンドの no 形式を使用します。
ステップ 4	exit 例： switch(config-vpc-domain)# exit switch(config)#	vpc-domain コンフィギュレーション モードを終了します。
ステップ 5	show running-config vpc 例： switch# show running-config vpc	(任意) vPC に関する情報、特にリロード ステータスを表示します。
ステップ 6	show vpc consistency-parameters interface port-channel number 例： switch# show vpc consistency-parameters interface port-channel 1	(任意) 指定したインターフェイスの vPC の一貫性パラメータに関する情報を表示します。
ステップ 7	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。 (注) 自動リカバリ機能がイネーブルになっていることを確認するには、この手順を実行します。

次に、vPC 自動リカバリ機能を設定し、それをスイッチのスタートアップ コンフィギュレーションに保存する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vpc domain 5
switch(config-vpc-domain)# auto-recovery
Warning:
  Enables restoring of vPCs in a peer-detached state after reload, will wait for 240
seconds to determine if peer is un-reachable
switch(config-vpc-domain)# exit
switch(config)# exit
switch# copy running-config startup-config
```

孤立ポートの一時停止の設定

vPC 対応でないデバイスが各ピアに接続するとき、接続されたポートは vPC のメンバではないため、孤立ポートと称されます。ピア リンクまたはピア キープアライブ障害に応じてセカンダリ ピアが vPC ポートを一時停止するときに、セカンダリ ピアによって一時停止（シャットダウン）される孤立ポートとして物理インターフェイスを明示的に宣言できます。孤立ポートは vPC が復元されたときに復元されます。



(注) vPC 孤立ポートの一時停止は、ポート チャンネルのメンバ ポートではなく、物理ポートでのみ設定できます。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

手順の概要

1. **configure terminal**
2. (任意) **show vpc orphan-ports**
3. **interface type slot/port**
4. **vpc orphan-ports suspend**
5. **exit**
6. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	show vpc orphan-ports 例： switch# show vpc orphan-ports	(任意) 孤立ポートのリストを表示します。
ステップ 3	interface type slot/port 例： switch(config)# interface ethernet 3/1 switch(config-if)#	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	vpc orphan-ports suspend 例： switch(config-if)# vpc orphan-ports suspend	選択したインターフェイスを vPC 障害時にセカンダリ ピアにより一時停止される vPC 孤立ポートとして設定します。

	コマンド	目的
ステップ 5	exit 例： switch(config-if)# exit switch(config)#	インターフェイス コンフィギュレーション モードを終了します。
ステップ 6	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、インターフェイスを vPC 障害時にセカンダリ ピアにより一時停止される vPC 孤立ポートとして設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# vpc orphan-ports suspend
switch(config-if)# exit
switch(config)#
```

vPC ピア スイッチの設定

Cisco Nexus 9000 シリーズ デバイスは、一対の vPC デバイスがレイヤ 2 トポロジ内で 1 つの STP ルートとして現れるように設定することができます。この項では、次のトピックについて取り上げます。

- 「[純粋な vPC ピア スイッチ トポロジの設定](#)」 (P.7-53)
- 「[ハイブリッド vPC ピア スイッチ トポロジの設定](#)」 (P.7-55)

純粋な vPC ピア スイッチ トポロジの設定

純粋な vPC ピア スイッチ トポロジを設定するには、**peer-switch** コマンドを使用し、次に可能な範囲内で最高の（最も小さい）スパンニングツリーブリッジプライオリティ値を設定します。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。



(注)

VPC ピア間の非 VPC 専用トランク リンクを使用する場合は、STP が VLAN をブロックするのを防ぐために、非 VPC VLAN はピアによって異なるグローバルプライオリティが必要です。

手順の概要

1. **configure terminal**
2. **vpc domain domain-id**
3. **peer-switch**
4. **spanning-tree vlan vlan-range priority value**
5. **exit**
6. (任意) **show spanning-tree summary**
7. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vpc domain domain-id 例: switch(config)# vpc domain 5 switch(config-vpc-domain)#	設定する vPC ドメインの番号を入力し、 vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	peer-switch 例: switch(config-vpc-domain)# peer-switch	vPC スイッチ ペアがレイヤ 2 トポロジ内で 1 つの STP ルートとして現れるようにします。 ピア スイッチ vPC トポロジをディセーブルにするには、このコマンドの no 形式を使用します。
ステップ 4	spanning-tree vlan vlan-range priority value 例: switch(config)# spanning-tree vlan 1 priority 8192	VLAN のブリッジ プライオリティを設定します。有効な値は、4096 の倍数です。デフォルト値は 32768 です。
ステップ 5	exit 例: switch(config-vpc-domain)# exit switch(config)#	vpc-domain コンフィギュレーション モードを終了します。
ステップ 6	show spanning-tree summary 例: switch# show spanning-tree summary	(任意) スパニングツリー ポートの状態の概要を表示します。これに、vPC ピア スイッチも含まれます。
ステップ 7	copy running-config startup-config 例: switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例は、純粋な vPC ピア スイッチ トポロジを設定する方法を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vpc domain 5
switch(config-vpc-domain)# peer-switch
2010 Apr 28 14:44:44 switch %STP-2-VPC_PEERSWITCH_CONFIG_ENABLED: vPC peer-switch
configuration is enabled.Please make sure to configure spanning tree "bridge" priority as
per recommended guidelines to make vPC peer-switch operational.
switch(config-vpc-domain)# spanning-tree vlan 1 priority 8192
switch(config-vpc-domain)# exit
switch(config)#
```

ハイブリッド vPC ピア スイッチ トポロジの設定

spanning-tree pseudo-information コマンドを使用して STP VLAN ベースのロード バランシング 条件を満たすように代表ブリッジ ID を変更した後、ルート ブリッジ ID を最高のブリッジ プライオリティよりも高い値に変更することにより、ハイブリッド vPC または非 vPC ピア スイッチ トポロジを設定することができます。次に、ピア スイッチをイネーブルにします。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。



(注)

VPC ピア間の非 VPC 専用トランク リンクを使用する場合は、STP が VLAN をブロックするのを防ぐために、非 VPC VLAN はピアによって異なる疑似ルート プライオリティが必要です。

手順の概要

1. **configure terminal**
2. **spanning-tree pseudo-information**
3. **vlan *vlan-range* designated priority *value***
4. **vlan *vlan-range* root priority *value***
5. **vpc domain *domain-id***
6. **peer-switch**
7. **exit**
8. (任意) **show spanning-tree summary**
9. (任意) **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree pseudo-information 例： switch(config)# spanning-tree pseudo-information switch(config-pseudo)#	スパンニングツリー疑似情報を設定します。
ステップ 3	vlan <i>vlan-id</i> designated priority <i>priority</i> 例： switch(config-pseudo)# vlan 1 designated priority 8192	VLAN の指定ブリッジ プライオリティを設定します。有効な値は、0 ~ 61440 の範囲内の 4096 の倍数です。

	コマンド	目的
ステップ 4	vlan <i>vlan-id</i> root priority <i>priority</i> 例: switch(config-pseudo)# vlan 1 root priority 4096	VLAN のルート ブリッジプライオリティを設定します。有効な値は、0 ~ 61440 の範囲内の 4096 の倍数です。
ステップ 5	vpc domain <i>domain-id</i> 例: switch(config)# vpc domain 5 switch(config-vpc-domain)#	設定する vPC ドメインの番号を入力し、vpc-domain コンフィギュレーション モードを開始します。
ステップ 6	peer-switch 例: switch(config-vpc-domain)# peer-switch	vPC スイッチ ペアがレイヤ 2 トポロジ内で 1 つの STP ルートとして現れるようにします。 ピア スイッチ vPC トポロジをディセーブルにするには、このコマンドの no 形式を使用します。
ステップ 7	exit 例: switch(config-vpc-domain)# exit switch(config)#	vpc-domain コンフィギュレーション モードを終了します。
ステップ 8	show spanning-tree summary 例: switch# show spanning-tree summary	(任意) スパニングツリー ポートの状態の概要を表示します。これに、vPC ピア スイッチも含まれます。
ステップ 9	copy running-config startup-config 例: switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例は、ハイブリッド vPC ピア スイッチ トポロジを設定する方法を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# spanning-tree pseudo-information
switch(config-pseudo)# vlan 1 designated priority 8192
switch(config-pseudo)# vlan 1 root priority 4096
switch(config-pseudo)# vpc domain 5
switch(config-vpc-domain)# peer-switch
switch(config-vpc-domain)# exit
switch(config)#
```

vPC 設定の確認

vPC 設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show feature	vPC がイネーブルになっているかどうかを表示します。
show vpc brief	vPC に関する要約情報を表示します。
show vpc consistency-parameters	すべての vPC インターフェイス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。
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。

コマンド	目的
<code>show port-channel capacity</code>	設定されているポート チャンネルの数、およびデバイス上でまだ使用可能なポート チャンネル数を表示します。
<code>show vpc statistics</code>	vPC に関する統計情報を表示します。
<code>show vpc peer-keepalive</code>	ピアキープアライブ メッセージに関する情報を表示します。
<code>show vpc role</code>	ピア ステータス、ローカル デバイスのロール、vPC システム MAC アドレスとシステム プライオリティ、およびローカル vPC デバイスの MAC アドレスとプライオリティを表示します。

vPC のモニタリング

vPC 統計情報を表示するには、`show vpc statistics` コマンドを使用します。

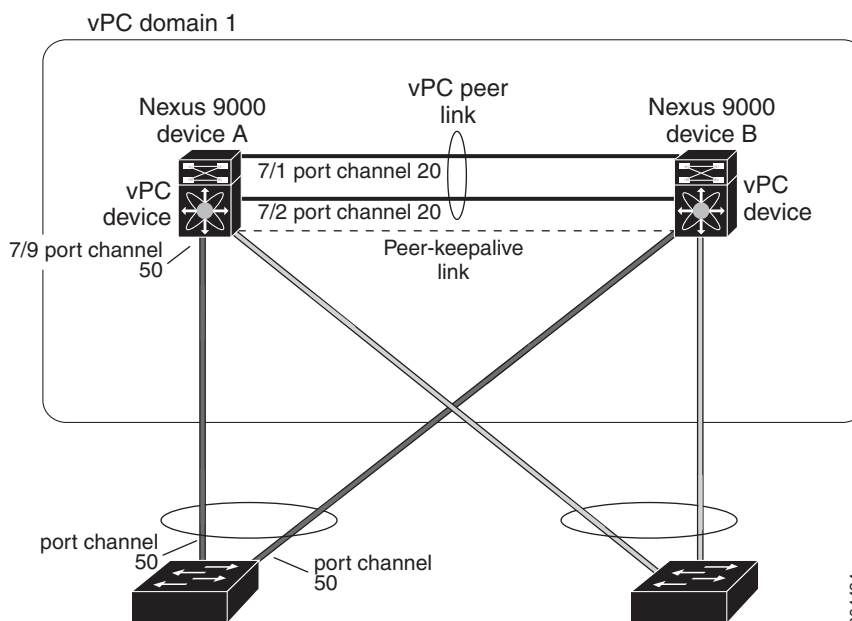


(注) このコマンドは、現在作業している vPC ピア デバイスの vPC 統計情報しか表示しません。

vPC の設定例

次の例は、デバイス A 上で図 7-7 に示すとおり vPC を設定する方法を示します。

図 7-7 vPC の設定例



ステップ 1 vPC および LACP をイネーブルにします。

```
switch# configure terminal
switch(config)# feature vpc
switch(config)# feature lacp
```

ステップ 2 (任意) ピア リンクにするインターフェイスの 1 つを専用モードに設定します。

```
switch(config)# interface ethernet 7/1, ethernet 7/3, ethernet 7/5.ethernet 7/7
switch(config-if)# shutdown
switch(config-if)# exit
switch(config)# interface ethernet 7/1
switch(config-if)# rate-mode dedicated
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)#
```

ステップ 3 (任意) ピア リンクにする 2 つ目の冗長インターフェイスを専用ポート モードに設定します。

```
switch(config)# interface ethernet 7/2, ethernet 7/4, ethernet 7/6.ethernet 7/8
switch(config-if)# shutdown
switch(config-if)# exit
switch(config)# interface ethernet 7/2
switch(config-if)# rate-mode dedicated
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)#
```

ステップ 4 ピア リンクに入れる 2 つのインターフェイス (冗長性のために) をアクティブ レイヤ 2 LACP ポート チャンネルに設定します。

```
switch(config)# interface ethernet 7/1-2
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1-50
switch(config-if)# switchport trunk native vlan 20
switch(config-if)# channel-group 20 mode active
switch(config-if)# exit
```

ステップ 5 VLAN を作成し、イネーブルにします。

```
switch(config)# vlan 1-50
switch(config-vlan)# no shutdown
switch(config-vlan)# exit
```

ステップ 6 vPC ピアキープアライブ リンク用の独立した VEF を作成し、レイヤ 3 インターフェイスをその VRF に追加します。

```
switch(config)# vrf context pkal
switch(config-vrf)# exit
switch(config)# interface ethernet 8/1
switch(config-if)# vrf member pkal
switch(config-if)# ip address 172.23.145.218/24
switch(config-if)# no shutdown
switch(config-if)# exit
```

ステップ 7 vPC ドメインを作成し、vPC ピアキープアライブ リンクを追加します。

```
switch(config)# vpc domain 1
switch(config-vpc-domain)# peer-keepalive destination 172.23.145.217 source 172.23.145.218
vrf pkal
switch(config-vpc-domain)# exit
```

ステップ 8 vPC ピア リンクを設定します。

```
switch(config)# interface port-channel 20
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1-50
switch(config-if)# vpc peer-link
switch(config-if)# exit
switch(config)#
```

ステップ 9 vPC のダウンストリーム デバイスへのポート チャンネルのインターフェイスを設定します。

```
switch(config)# interface ethernet 7/9
switch(config-if)# switchport mode trunk
switch(config-if)# allowed vlan 1-50
switch(config-if)# native vlan 20
switch(config-if)# channel-group 50 mode active
switch(config-if)# exit
switch(config)# interface port-channel 50
switch(config-if)# vpc 50
switch(config-if)# exit
switch(config)#
```

ステップ 10 設定を保存します。

```
switch(config)# copy running-config startup-config
```



(注)

まずポート チャンネルを設定する場合は、それがレイヤ 2 ポート チャンネルであることを確認してください。

その他の参考資料

vPC を実装する方法の詳細については、次の項目を参照してください。

- 「関連資料」 (P.7-59)
- 「標準」 (P.7-60)
- 「管理情報ベース (MIB)」 (P.7-60)

関連資料

関連項目	マニュアル タイトル
システム管理	『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』
ハイ アベイラビリティ	『Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide』
リリース ノート	『Cisco Nexus 9000 Series NX-OS Release Notes』

標準

標準	タイトル
IEEE 802.3ad	—

管理情報ベース (MIB)

MIB	MIB のリンク
<ul style="list-style-type: none">• IEEE8023-LAG-CAPABILITY• CISCO-LAG-MIB	<p>サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。</p> <p>ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html</p>

A

Cisco NX-OS インターフェイスがサポートする IETF RFC

ここでは、Cisco NX-OS でサポートされているインターフェイスの IETF RFC を示します。

IPv6 の RFC

RFC	タイトル
RFC 1981	『Path MTU Discovery for IP version 6』
RFC 2373	『IP Version 6 Addressing Architecture』
RFC 2374	『An Aggregatable Global Unicast Address Format』
RFC 2460	『Internet Protocol, Version 6 (IPv6) Specification』
RFC 2462	『IPv6 Stateless Address Autoconfiguration』
RFC 2464	『Transmission of IPv6 Packets over Ethernet Networks』
RFC 2467	『Transmission of IPv6 Packets over FDDI Networks』
RFC 2472	『IP Version 6 over PPP』
RFC 2492	『IPv6 over ATM Networks』
RFC 2590	『Transmission of IPv6 Packets over Frame Relay Networks Specification』
RFC 3021	『Using 31-Bit Prefixes on IPv4 Point-to-Point Links』
RFC 3152	『Delegation of IP6.ARPA』
RFC 3162	『RADIUS and IPv6』
RFC 3513	『Internet Protocol Version 6 (IPv6) Addressing Architecture』
RFC 3596	『DNS Extensions to Support IP version 6』
RFC 4193	『Unique Local IPv6 Unicast Addresses』

B

Cisco NX-OS インターフェイスの設定制限

設定の制限は、『*Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*』に記載されています。

