



Cisco Nexus 5000 シリーズ NX-OS インターフェイス コンフィギュレーション ガイド リリース 5.2(1)N1(1)

初版：2012 年 07 月 02 日

最終更新：2012 年 07 月 02 日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

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

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

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

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

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を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://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。

© 2012 Cisco Systems, Inc. All rights reserved.



目次

はじめに ix

対象読者 ix

表記法 ix

関連資料 xi

マニュアルに関するフィードバック xiii

マニュアルの入手方法およびテクニカル サポート xiii

このリリースの新規および変更情報 1

このリリースの新規および変更情報 1

レイヤ2 インターフェイスの設定 3

イーサネット インターフェイスの概要 3

interface コマンドについて 3

ユニファイド ポートの概要 4

ユニファイド ポートに関する注意事項および制約事項 5

単一方向リンク検出パラメータについて 5

UDLD のデフォルト設定 6

UDLD アグレッシブ モードと非アグレッシブ モード 7

インターフェイス速度 7

Cisco Discovery Protocol について 7

CDP のデフォルト設定 8

error-disabled ステートについて 8

ポート プロファイルについて 9

ポート プロファイルに関する注意事項および制約事項 10

デバウンス タイマー パラメータについて 11

MTU 設定について 11

イーサネット インターフェイスの設定 11

Cisco Nexus 5500 プラットフォーム スイッチのレイヤ3 インターフェイスの設定 12

ユニファイド ポートの設定	12
UDLD モードの設定	14
インターフェイスの速度の設定	15
リンク ネゴシエーションのディセーブル化	17
CDP の特性の設定	18
CDP のイネーブル化/ディセーブル化	19
error-disabled 検出のイネーブル化	19
errdisable リカバリのイネーブル化	20
errdisable リカバリ間隔の設定	21
ポート プロファイル	22
ポート プロファイルの作成	22
ポート プロファイルの変更	23
特定のポート プロファイルのイネーブル化	24
ポート プロファイルの継承	25
継承されたポート プロファイルの削除	27
一定範囲のインターフェイスへのポート プロファイルの割り当て	28
一定範囲のインターフェイスからのポート プロファイルの削除	29
ポート プロファイルの設定例	30
デバウンス タイマーの設定	31
説明パラメータの設定	32
イーサネット インターフェイスのディセーブル化と再起動	32
インターフェイス情報の表示	33
物理イーサネットのデフォルト設定	36
レイヤ 3 インターフェイスの設定	37
レイヤ 3 インターフェイスについて	37
ルーテッド インターフェイス	37
サブインターフェイス	38
VLAN インターフェイス	39
ループバック インターフェイス	40
トンネル インターフェイス	40
レイヤ 3 インターフェイスのライセンス要件	40
レイヤ 3 インターフェイスの注意事項および制約事項	41

レイヤ 3 インターフェイスのデフォルト設定	41
レイヤ 3 インターフェイスの設定	41
ルーテッド インターフェイスの設定	41
サブインターフェイスの設定	42
インターフェイスでの帯域幅の設定	43
VLAN インターフェイスの設定	44
ループバック インターフェイスの設定	45
VRF へのインターフェイスの割り当て	46
レイヤ 3 インターフェイス設定の確認	47
レイヤ 3 インターフェイスのモニタリング	49
レイヤ 3 インターフェイスの設定例	50
レイヤ 3 インターフェイスの関連資料	51
レイヤ 3 インターフェイスの MIB	51
レイヤ 3 インターフェイスの標準	51
ポート チャネルの設定	53
ポート チャネルについて	53
ポート チャネルの概要	54
ポート チャネルの設定に関する注意事項および制約事項	54
互換性要件	55
ポート チャネルを使ったロード バランシング	57
LACP の概要	60
LACP の概要	60
LACP ID パラメータ	60
チャネル モード	61
LACP マーカー レスポンダ	63
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	63
ポート チャネルの設定	63
ポート チャネルの作成	63
ポート チャネルへのポートの追加	64
ポート チャネルを使ったロード バランシングの設定	65
マルチキャスト トラフィックのハードウェア ハッシュの設定	66

LACP のイネーブル化	67
ポートのチャンネル モードの設定	68
LACP 高速タイマー レートの設定	69
LACP のシステム プライオリティおよびシステム ID の設定	70
LACP ポート プライオリティの設定	71
LACP グレースフル コンバージェンス	72
LACP グレースフル コンバージェンスの再イネーブル化	73
ポート チャンネルの設定の確認	74
ロードバランシングの発信ポート ID の確認	75
仮想ポート チャンネルの設定	77
vPC について	77
vPC の概要	77
用語	79
vPC の用語	79
ファブリック エクステンダの用語	80
サポートされている vPC トポロジ	80
Cisco Nexus 5000 シリーズ スイッチ vPC トポロジ	80
シングルホーム接続ファブリック エクステンダ vPC トポロジ	81
デュアルホーム接続ファブリック エクステンダ vPC トポロジ	82
vPC ドメイン	83
ピアキープアライブ リンクとメッセージ	84
vPC ピア リンクの互換パラメータ	84
同じでなければならない設定パラメータ	85
同じにすべき設定パラメータ	86
グレースフル タイプ 1 チェック	87
VLAN ごとの整合性検査	87
vPC 自動リカバリ	87
vPC ピア リンク	87
vPC ピア リンクの概要	88
vPC 番号	89
その他の機能との vPC の相互作用	89
vPC と LACP	89

vPC ピア リンク と STP	90
vPC と ARP	90
CFS oE	91
vPC ピア スイッチ	91
vPC の注意事項および制約事項	92
vPC の設定	93
vPC のイネーブル化	93
vPC のディセーブル化	93
vPC ドメインの作成	94
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	95
vPC ピア リンクの作成	98
設定の互換性チェック	98
vPC 自動リカバリのイネーブル化	100
vPC トポロジのセカンダリ スイッチの孤立ポートの一時停止	101
EtherChannel ホスト インターフェイスの作成	102
他のポート チャネルの vPC への移行	103
vPC ドメイン MAC アドレスの手動での設定	104
システム プライオリティの手動での設定	105
vPC ピア スイッチ ロールの手動での設定	106
vPC ピア スイッチの設定	107
純粋な vPC ピア スイッチ トポロジの設定	107
ハイブリッド vPC ピア スイッチ トポロジの設定	109
vPC 設定の確認	110
グレースフル タイプ 1 チェック ステータスの表示	111
グローバル タイプ 1 不整合の表示	112
インターフェイス固有のタイプ 1 不整合の表示	113
VLAN ごとの整合ステータスの表示	114
vPC の設定例	116
デュアルホーム接続ファブリック エクステンダ vPC の設定例	116
シングルホーム接続ファブリック エクステンダ vPC の設定例	118
vPC のデフォルト設定	120



はじめに

ここでは、次の項目について説明します。

- [対象読者, ix ページ](#)
- [表記法, ix ページ](#)
- [関連資料, xi ページ](#)
- [マニュアルに関するフィードバック, xiii ページ](#)
- [マニュアルの入手方法およびテクニカル サポート, xiii ページ](#)

対象読者

このマニュアルは、Cisco Nexus シリーズ デバイスと Cisco Nexus 2000 シリーズ ファブリック エクステンダの設定や保守を行う、経験のあるネットワーク管理者を対象にしています。

表記法

コマンドの説明には、次のような表記法が使用されます。

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

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

例では、次の表記法を使用しています。

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

このマニュアルでは、次の表記法を使用しています。



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

**注意**

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

関連資料

完全な Cisco NX-OS 5000 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/ps9670/tsd_products_support_series_home.html

リリース ノート

リリース ノートは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9670/prod_release_notes_list.html

コンフィギュレーション ガイド

これらのガイドは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html

このカテゴリのマニュアルは次のとおりです。

- 『*Adapter-FEX Configuration Guide*』
- 『*Cisco Fabric Manager Configuration Guide*』
- 『*Cisco Nexus 5000 Series NX-OS Software Configuration Guide*』
- 『*Configuration Limits for Cisco NX-OS*』
- 『*FabricPath Configuration Guide*』
- 『*Fibre Channel over Ethernet Configuration Guide*』
- 『*Layer 2 Switching Configuration Guide*』
- 『*Multicast Routing Configuration Guide*』
- 『*Operations Guide*』
- 『*SAN Switching Configuration Guide*』
- 『*Quality of Service Configuration Guide*』
- 『*Security Configuration Guide*』
- 『*System Management Configuration Guide*』
- 『*Unicast Routing Configuration Guide*』

メンテナンスおよび操作ガイド

さまざまな機能に対応する『Cisco Nexus 5000 Series NX-OS Operations Guide』は、http://www.cisco.com/en/US/products/ps9670/prod_maintenance_guides_list.html で入手できます。

インストールガイドおよびアップグレードガイド

これらのガイドは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9670/prod_installation_guides_list.html

このカテゴリのマニュアルは次のとおりです。

- 『*FabricPath Command Reference*』
- 『*Software Upgrade and Downgrade Guides*』
- 『*Regulatory Compliance and Safety Information*』

ライセンスガイド

『*License and Copyright Information for Cisco NX-OS Software*』は、http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/license_agreement/nx-oss_w_lisns.html で入手できます。

コマンドリファレンス

これらのガイドは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9670/prod_command_reference_list.html

このカテゴリのマニュアルは次のとおりです。

- 『*Command Reference Master Index*』
- 『*Fabric Extender Command Reference*』
- 『*FabricPath Command Reference*』
- 『*Fibre Channel Command Reference*』
- 『*Fundamentals Command Reference*』
- 『*Layer 2 Interfaces Command Reference*』
- 『*Multicast Routing Command Reference*』
- 『*QoS Command Reference*』
- 『*Security Command Reference*』
- 『*System Management Command Reference*』
- 『*TrustSec Command Reference*』
- 『*Unicast Routing Command Reference*』
- 『*vPC Command Reference*』

テクニカル リファレンス

『Cisco Nexus 5000 and Cisco Nexus 2000 MIBs Reference』は、http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/mib/reference/NX5000_MIBRef.html で入手できます。

エラー メッセージおよびシステム メッセージ

『Nexus 5000 Series NX-OS System Message Reference』は、http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/system_messages/reference/sl_nxos_book.html で入手できます。

トラブルシューティング ガイド

『Cisco Nexus 5000 Series Troubleshooting Guide』は、http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/troubleshooting/guide/N5K_Troubleshooting_Guide.html で入手できます。

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



第 1 章

このリリースの新規および変更情報

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

- [このリリースの新規および変更情報, 1 ページ](#)

このリリースの新規および変更情報

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

表 1：新機能

機能	説明	参照先
IPv6	IPv6 アドレッシングのサポートが追加されました。	<ul style="list-style-type: none">• ルーテッド インターフェイス, (37 ページ)• サブインターフェイスの設定, (42 ページ)• インターフェイスでの帯域幅の設定, (43 ページ)• VLAN インターフェイスの設定, (44 ページ)• ループバック インターフェイスの設定, (45 ページ)• VRF へのインターフェイスの割り当て, (46 ページ)



第 2 章

レイヤ 2 インターフェイスの設定

この章の内容は、次のとおりです。

- ・ [イーサネット インターフェイスの概要, 3 ページ](#)
- ・ [イーサネット インターフェイスの設定, 11 ページ](#)
- ・ [インターフェイス情報の表示, 33 ページ](#)
- ・ [物理イーサネットのデフォルト設定, 36 ページ](#)

イーサネット インターフェイスの概要

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

イーサネット インターフェイスでは、Fibre Channel over Ethernet (FCoE) もサポートされます。FCoE により、イーサネット トラフィックとファイバチャネル トラフィックの両方を物理イーサネット リンクで伝送できるようになります。

Cisco Nexus 5000 シリーズ スイッチでは、イーサネット インターフェイスがデフォルトでイネーブルになっています。

interface コマンドについて

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

- ・ インターフェイス タイプ：すべての物理イーサネット インターフェイスには、常にキーワード **ethernet** を使用します。
- ・ スロット番号
 - スロット 1 にはすべての固定ポートが含まれます。

- スロット 2 には上位拡張モジュールのポートが含まれます（実装されている場合）。
- スロット 3 には下位拡張モジュールのポートが含まれます（実装されている場合）。
- スロット 4 には下位拡張モジュールのポートが含まれます（実装されている場合）。



（注） スロット 4 は、Cisco Nexus 5596T スイッチでのみ使用できます。

- ポート番号
 - グループ内でのポート番号です。

Cisco Nexus 2000 シリーズ ファブリック エクステンダ との使用をサポートするために、インターフェイスのナンバリング規則は、次のように拡張されています。

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

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

ユニファイド ポートの概要

Cisco Nexus ユニファイド ポートでは、Cisco Nexus 5500 プラットフォーム スイッチの物理ポートを 1/10 ギガビット イーサネット、Fibre Channel over Ethernet (FCoE)、または 1、2、4、8 ギガビット ネイティブ ファイバ チャネル ポートとして設定することができます。

現在、ほとんどのネットワークには次の 2 つのタイプのスイッチが異なるタイプのネットワーク用に使用されています。たとえば、LAN スイッチは、Catalyst スイッチまでのイーサネットトラフィックを伝送し、SAN スイッチはサーバから MDS スイッチに FC トラフィックを伝送します。ユニファイド ポートテクノロジーを使用すれば、ユニファイドプラットフォーム、ユニファイドデバイス、ユニファイドワイヤアプローチを展開できます。ユニファイドポートを使用すると、LAN および SAN ポート オプションから選択する既存の分離されたプラットフォームアプローチから、トランスペアレントで、既存の方法と管理ソフトウェアと整合性のある単一のユニファイドファブリックに遷移できます。ユニファイドファブリックには、次が含まれます。

- ユニファイドプラットフォーム：同じハードウェアプラットフォームと同じソフトウェアコードレベルを使用し、ユーザの LAN および SAN 環境に対して 1 度認証します。
- ユニファイドデバイス：同じプラットフォーム スイッチで LAN および SAN サービスを実行します。ユニファイドデバイスを使用すると、同じデバイスにイーサネット ケーブルとファイバチャネル ケーブルを接続できます。
- ユニファイドワイヤ：単一の統合型ネットワーク アダプタ (CNA) 上に LAN および SAN ネットワークを収束し、サーバに接続します。

ユニファイドファブリックを使用すると、既存のシスコツールによってイーサネットおよびFCoE機能を個別に管理できます。

ユニファイドポートに関する注意事項および制約事項

- イーサネットポートとファイバチャネルポートは、次の順序で設定する必要があります。
- ファイバチャネルポートはモジュールの最後のポートから設定する必要があります。
- イーサネットポートはモジュールの最初のポートから設定する必要があります。

順序に従わない場合、次のエラーが表示されます。

```
ERROR: Ethernet range starts from first port of the module
ERROR: FC range should end on last port of the module
```

- Cisco Nexus 5548UP スイッチでは、メインスロット (slot1) の 32 個のポートがユニファイドポートです。イーサネットポートは、ポート 1/1 から開始し、ポート 1/32 に進みます。ファイバチャネルポートは、逆にポート 1/32 から開始し、ポート 1/1 に進みます。
- Cisco Nexus 5596T スイッチの場合、最後の 16 個のポート (ポート 33 ~ 48) はファイバチャネルであり、ユニファイドポートとして設定できます。最初の 32 個のポート (1 ~ 32) は 10GBase-T イーサネットポートのみであり、ユニファイドポートとしては設定できません。

単一方向リンク検出パラメータについて

シスコ独自の Unidirectional Link Detection (UDLD; 単一方向リンク検出) プロトコルでは、光ファイバまたは銅線 (たとえば、カテゴリ 5 のケーブル) のイーサネットケーブルで接続されているポートでケーブルの物理的な構成をモニタリングし、単一方向リンクの存在を検出できます。スイッチが単一方向リンクを検出すると、UDLD は関連する LAN ポートをシャットダウンし、ユーザに警告します。単一方向リンクは、スパンニングツリー トポロジープをはじめ、さまざまな問題を引き起こす可能性があります。

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

リンク上でローカルデバイスが送信したトラフィックはネイバーで受信されるが、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、単一方向リンクが発生します。対になっているファイバケーブルのいずれか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、そのリンクは存続できません。この場合、論理リンクは不定であり、UDLD は何の処理も行いません。レイヤ 1 で両方の光ファイバが正常に動作している場合は、レイヤ 2 で UDLD が、これらの光ファイバが正しく接続されているかどうか、および正しいネイバー間でトラフィックが双方向に流れているかを調べます。自動ネゴシエーションはレイヤ 1 で動作するため、このチェックは、自動ネゴシエーションでは実行できません。

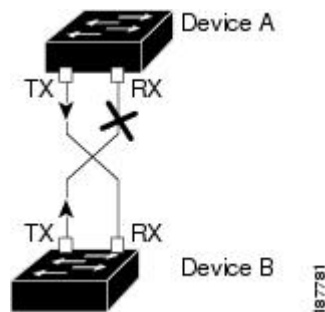
Cisco Nexus 5000 シリーズ スイッチは、UDLD をイネーブルにした LAN ポート上のネイバー デバイスに UDLD フレームを定期的に送信します。一定の時間内にフレームがエコーバックされてきて、特定の確認応答（echo）が見つからなければ、そのリンクは単方向のフラグを立てられ、その LAN ポートはシャットダウンされます。プロトコルが単方向リンクを正しく識別してディセーブルにするには、リンクの両端のデバイスで UDLD をサポートする必要があります。



(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。

次の図は、単方向リンク状態の例を示します。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されます。

図 1：単方向リンク



UDLD のデフォルト設定

次の表に、UDLD のデフォルト設定を示します。

表 2：UDLD のデフォルト設定

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

UDLD アグレッシブ モードと非アグレッシブ モード

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

スパニングツリー ループを防止するために、デフォルトの 15 秒間隔を使用する非アグレッシブ な UDLD により、（デフォルトのスパニングツリーパラメータを使用している場合）ブロッキングポートがフォワーディングステートに移行する前に、すみやかに単方向リンクをシャットダウンすることができます。

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

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

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

インターフェイス速度

Cisco Nexus 5000 シリーズ スイッチには、多数の固定 10 ギガビット ポートが装備されており、それぞれに SFP+ インターフェイス アダプタが搭載されています。

- Cisco Nexus 5010 スイッチには 20 個の固定ポートが装備されており、そのうち、最初の 8 個がスイッチ可能な 1 ギガビットおよび 10 ギガビットのポートです。
- Cisco Nexus 5020 スイッチには 40 個の固定ポートが装備されており、そのうち、最初の 16 個がスイッチ可能な 1 ギガビットおよび 10 ギガビットのポートです。

5596T スイッチには、48 個のベース ボード ポートと 3 つの GEM スロットが装備されています。最初の 32 個のポートは 10GBase-T ポートであり、最後の 16 個のポートは SFP+ ポートです。10GBase-T ポートは、1 ギガビット、10 ギガビット、または Auto の速度をサポートしています。Auto に設定すると、リンク パーサーと自動的にネゴシエートして 1 ギガビットまたは 10 ギガビットのどちらかの速度を選択します。

Cisco Discovery Protocol について

Cisco Discovery Protocol (CDP) はすべてのシスコ デバイス（ルータ、ブリッジ、アクセス サーバ、およびスイッチ）のレイヤ 2（データリンク層）で動作するデバイス検出プロトコルです。ネットワーク管理アプリケーションは CDP を使用することにより、既知のデバイスにネイバーシスコ デバイスを検出できます。また、下位レイヤのトランスペアレント プロトコルが稼働して

いるネイバー デバイスのデバイス タイプや、Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) エージェント アドレスを学習することもできます。この機能によって、アプリケーションからネイバー デバイスに SNMP クエリーを送信できます。

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

CDP が設定された各デバイスはマルチキャストアドレスに定期的にメッセージを送信して、SNMP メッセージを受信可能なアドレスを 1 つまたは複数アドバタイズします。このアドバタイズには、受信側デバイスで CDP 情報を廃棄せずに保持する時間を表す存続可能時間、つまりホールドタイム情報も含まれます。各デバイスは他のデバイスから送信されたメッセージも待ち受けて、ネイバー デバイスについて学習します。

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

CDP のデフォルト設定

次の表に、CDP のデフォルト設定を示します。

表 3: CDP のデフォルト設定

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

error-disabled ステートについて

インターフェイスが (**no shutdown** コマンドを使用して) 管理上イネーブルであるが、プロセスによってランタイム時にディセーブルになる場合、そのインターフェイスはerrdisable (err-disabled) ステートです。たとえば、UDLD が単一方向リンクを検出した場合、インターフェイスはランタイム時にシャットダウンされます。ただし、インターフェイスは管理上イネーブルなので、インターフェイス ステータスはerrdisabled として表示されます。インターフェイスがerrdisabled ステートになると、手動でそれを再びイネーブルにする必要があります。または、自動リカバリ タイムアウトの値を設定します。errdisabled 検出は、すべての原因に対してデフォルトでイネーブルになっています。自動リカバリはデフォルトでは設定されていません。

インターフェイスがerrdisabled ステートにある場合は、エラーに関する情報を見つけるために、**errdisable detect cause** コマンドを使用します。

time 変数の変更によって起きる特定の errdisabled に対しては自動 errdisabled リカバリ タイムアウトを設定できます。

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。リカバリ期間を変更するには、**errdisable recovery interval** コマンドを使用してタイムアウト期間を指定します。30 ～ 65535 秒を指定できます。

原因に対する err-disabled リカバリをイネーブルにしない場合、インターフェイスは、**shutdown** および **no shutdown** コマンドが入力されるまで err-disabled ステートのままです。原因に対するリカバリをイネーブルにした場合、インターフェイスは errdisabled ステートから抜け出し、すべての原因がタイムアウトになったときに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には、**show interface status err-disabled** コマンドを使用します。

ポート プロファイルについて

多くのインターフェイス コマンドを含むポート プロファイルを作成でき、Cisco Nexus 5000 シリーズ スイッチのインターフェイス範囲にポート プロファイルを適用できます。ポート プロファイルは、次のインターフェイス タイプに適用できます。

- イーサネット
- VLAN ネットワーク インターフェイス
- ポート チャネル

ポート プロファイルに含まれるコマンドは、ポート プロファイル外に設定できます。ポート プロファイルの新規設定とポート プロファイル外にある設定が競合する場合、コンフィギュレーション ターミナル モードのインターフェイスに設定されているコマンドがポート プロファイルのコマンドよりもプライオリティが高くなります。ポート プロファイルがインターフェイスにアタッチされた後でインターフェイスの設定を変更したとき、ポート プロファイルの設定とインターフェイスの設定が競合する場合は、インターフェイスの設定が優先されます。

ポート プロファイルをインターフェイスまたはインターフェイスの範囲にアタッチするとポート プロファイルが継承されます。ポート プロファイルをインターフェイスまたはインターフェイスの範囲にアタッチするか継承すると、スイッチがそのポート プロファイルのすべてのコマンドをインターフェイスに適用します。

1 つのポート プロファイルで別のポート プロファイルから設定を継承できます。別のポート プロファイルを継承すると、最初のポート プロファイルは、2 番目の継承されたポート プロファイルのコマンドのすべてが最初のポート プロファイルと競合しないと想定できます。4 つのレベルの継承がサポートされています。任意の数のポート プロファイルで同じポート プロファイルを継承できます。

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

ポート プロファイルをインターフェイスの範囲から削除すると、まずスイッチはインターフェイスから設定を取り消して、ポート プロファイルリンク自体を削除します。また、ポート プロファ

イルを削除すると、スイッチによってインターフェイスの設定が確認され、直接入力されたインターフェイス コマンドで無効にされたポート プロファイル コマンドをスキップするか、それらのコマンドをデフォルト値に戻します。

他のポート プロファイルによって継承されたポート プロファイルを削除するには、ポート プロファイルを削除する前に継承を削除する必要があります。

最初にプロファイルを適用したインターフェイスのグループの中から、ポート プロファイルを削除するインターフェイスのサブセットを選択できます。たとえば、ポート プロファイルを設定し、そのポート プロファイルを継承するよう 10 個のインターフェイスを設定した場合、指定した 10 個のインターフェイスの一部だけからポート プロファイルを削除できます。ポート プロファイルは、適用されている残りのインターフェイスで引き続き動作します。

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

インターフェイスまたはインターフェイスの範囲のポート プロファイルを継承したあとに特定の設定値を削除すると、そのポート プロファイル設定は指定のインターフェイスで動作しなくなります。

ポート プロファイルを誤ったタイプのインターフェイスに適用しようとする、スイッチからエラーが返されます。

ポート プロファイルをイネーブル、継承、または変更しようとする、スイッチはチェックポイントを作成します。ポート プロファイルの設定が失敗すると、スイッチは前の設定にロールバックし、エラーが返されます。ポート プロファイルは部分的にだけ適用されることはありません。

ポート プロファイルに関する注意事項および制約事項

ポート プロファイル設定時の注意事項と制限事項は次のとおりです。

- 各ポート プロファイルは、インターフェイス タイプにかかわらず、ネットワーク全体で一意の名前を持つ必要があります。
- 競合が発生している場合、インターフェイス モードで入力するコマンドは、ポート プロファイルのコマンドに優先します。しかし、ポート プロファイルはそのコマンドをポート プロファイルに保持します。
- ポート プロファイルのコマンドは、デフォルト コマンドが明示的にポート プロファイルのコマンドを上書きしない限り、インターフェイスのデフォルト コマンドに優先します。
- ポート プロファイルをインターフェイスまたはインターフェイスの範囲に継承した後、インターフェイス コンフィギュレーション レベルで新しい値を入力して、個々の設定値を上書きできます。インターフェイス コンフィギュレーション レベルで個々の設定値を削除すると、インターフェイスによりその値がポート プロファイルで再度使用されます。
- ポート プロファイルに関連したデフォルト設定はありません。

- 指定するインターフェイス タイプにより、コマンドのサブセットがポート プロファイル コンフィギュレーション モードで使用できます。
- Session Manager にポート プロファイルは使用できません。

デバウンス タイマー パラメータについて

ポート デバウンス 時間は、リンクがダウンしたことをスーパーバイザに通知するためにインターフェイスが待機する時間です。この時間、インターフェイスはリンクがアップ状態に戻ったかどうかを確認するために待機します。待機時間は、トラフィックが停止している時間です。

デバウンス タイマーは各インターフェイスに対してイネーブルにでき、ミリ秒単位で遅延時間を指定できます。



注意

ポート デバウンス タイマーをイネーブルにすると、リンク アップ 検出とリンク ダウン 検出に遅延が発生するため、デバウンス 期間中にトラフィックが一部損失します。トラフィックが損失することにより、一部のプロトコルのコンバージェンスおよび再コンバージェンスに影響を及ぼす場合があります。

MTU 設定について

Cisco Nexus 5000 シリーズ スイッチは、フレームをフラグメントしません。その結果、スイッチは異なる最大伝送単位 (MTU) が設定された同じレイヤ 2 ドメイン内の 2 個のポートを持てません。物理イーサネット インターフェイスごとの MTU はサポートされません。代わりに、MTU は QoS クラスに応じて設定されます。クラス マップとポリシー マップを設定して、MTU を変更します。



(注)

インターフェイス設定を表示すると、物理イーサネット インターフェイスのデフォルト MTU である 1500 が表示され、ファイバ チャネル インターフェイスの受信データ フィールド サイズは 2112 と表示されます。

イーサネット インターフェイスの設定

ここでは、次の内容について説明します。

Cisco Nexus 5500 プラットフォーム スイッチのレイヤ3インターフェイスの設定

Cisco Nexus 5000 プラットフォーム スイッチ上の NX-OS Release 5.0(3)N1(1) 以降では、レイヤ3インターフェイスを設定できます。

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には、**no switchport** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ2	switch(config)# interface ethernet slot/port	指定されたインターフェイスのコンフィギュレーション モードを開始します。
ステップ3	switch(config-if)# no switchport	レイヤ3インターフェイスを選択します。
ステップ4	switch(config-if)# no shutdown	インターフェイスを再起動します。

次に、レイヤ3インターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# no shutdown
```

ユニファイド ポートの設定

はじめる前に

サポートされる Cisco Nexus スイッチが存在することを確認します。ユニファイドポートは、次の Cisco Nexus スイッチで使用できます。

- Cisco Nexus 5596T
- Cisco Nexus 5548UP
- Cisco Nexus 5596UP
- Cisco N55-M16UP 拡張モジュールが搭載されている Cisco Nexus 5548P スイッチ

ユニファイドポートをファイバチャネルまたはFCoEとして設定している場合は、**feature fcoe** コマンドをイネーブルにしていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # slot slot number	スイッチのスロットを識別します。
ステップ 3	switch(config-slot) # port port number type {ethernet fc}	<p>ネイティブ ファイバチャネル ポートとイーサネット ポートとしてユニファイドポートを設定します。</p> <ul style="list-style-type: none"> • type : ポートのタイプをシャーシのスロットに設定するように指定します。 • ethernet : イーサネット ポートを指定します。 • fc : ファイバチャネル (FC) ポートを指定します。 <p>(注) 拡張モジュール (GEM) 上のユニファイドポートを変更するには、GEM カードの電源を再投入する必要があります。変更を有効にするためにスイッチ全体をリブートする必要はありません。</p>
ステップ 4	switch(config-slot) # copy running-config startup-config	実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。
ステップ 5	switch(config-slot) # reload	スイッチをリブートします。
ステップ 6	switch(config) # no port port number type fc	ユニファイドポートを削除します。

次に、Cisco Nexus 5548UP スイッチまたは Cisco Nexus 5596UP スイッチでユニファイドポートを設定する例を示します。

```
switch# configure terminal
switch(config)# slot 1
switch(config-slot)# port 32 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
```

次に、20 個のポートをイーサネットポートとして、12 個のポートを FC ポートとして設定する例を示します。

```
switch# configure terminal
switch(config)# slot 1
switch(config-slot)# port 21-32 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
```

次に、Cisco N55-M16UP 拡張モジュールでユニファイドポートを設定する例を示します。

```
switch# configure terminal
switch(config)# slot 2
switch(config-slot)# port 16 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# poweroff module 2
switch(config-slot)# no poweroff module 2
```

UDLD モードの設定

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

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



(注) 設定前に、リンクされている他方のポートとそのデバイスのUDLDをイネーブルにしておかなければなりません。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# feature udld	デバイスのUDLDをイネーブルにします。
ステップ 3	switch(config)# no feature udld	デバイスのUDLDをディセーブルにします。
ステップ 4	switch(config)# show udld global	デバイスのUDLDステータスを表示します。
ステップ 5	switch(config)# interface type slot/port	設定するインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 6	switch(config-if)# udld {enable disable aggressive}	ノーマルUDLDモードをイネーブルにするか、UDLDをディセーブルにするか、またはアグレッシブUDLDモードをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 7	switch(config-if)# show udld interface	インターフェイスの UDLD ステータスを表示します。

次の例は、スイッチの UDLD をイネーブルにする方法を示しています。

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

次の例は、イーサネット ポートのノーマル UDLD モードをイネーブルにする方法を示しています。

```
switch# configure terminal  
switch(config)# interface ethernet 1/4  
switch(config-if)# udld enable
```

次の例は、イーサネット ポートのアグレッシブ UDLD モードをイネーブルにする方法を示しています。

```
switch# configure terminal  
switch(config)# interface ethernet 1/4  
switch(config-if)# udld aggressive
```

次の例は、イーサネット ポートの UDLD をディセーブルにする例を示しています。

```
switch# configure terminal  
switch(config)# interface ethernet 1/4  
switch(config-if)# udld disable
```

次の例は、スイッチの UDLD をディセーブルにする方法を示しています。

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

インターフェイスの速度の設定

Cisco Nexus 5010 スイッチの最初の 8 個のポートと、Cisco Nexus 5020 スイッチの最初の 16 個のポートはスイッチ可能な 1 ギガビット ポートと 10 ギガビット ポートです。デフォルトのインターフェイス速度は 10 ギガビットです。これらのポートを 1 ギガビットイーサネットに設定するには、1 ギガビットイーサネット SFP トランシーバを該当するポートに挿入してから、その速度を **speed** コマンドで設定します。

Cisco Nexus 5596T スイッチの最初の 32 個のポートは、スイッチ可能な 1 ギガビット ポートと 10 ギガビット ポートです。これらのポートはまた、1 ギガビットまたは 10 ギガビットに自動ネゴシエーションするようにも設定できます。最後のポート 33 ~ 48 は SFP+ ポートであり、自動ネゴシエーションをサポートしていません。



(注) インターフェイスとトランシーバの速度が一致しない場合、**show interface ethernet slot/port** コマンドを入力すると、SFP 検証失敗メッセージが表示されます。たとえば、**speed 1000** コマンドを設定しないで1ギガビット SFP トランシーバをポートに挿入すると、このエラーが発生します。デフォルトでは、すべてのポートが 10 ギガビットです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface type slot/port	特定のインターフェイスのインターフェイス コンフィギュレーションモードを開始します。このインターフェイスに、1 ギガビット イーサネット SFP トランシーバが挿入されている必要があります。
ステップ 3	switch(config-if)# speed speed	<p>物理イーサネット インターフェイスの速度を設定します。</p> <p>Cisco Nexus 5000 シリーズ スイッチの場合は、<i>speed</i> 引数を次のいずれかに設定できます。</p> <ul style="list-style-type: none"> • 10 : 10 Mbps • 100 : 100 Mbps • 1000 : 1 Gbps • 10000 : 10Gbps • auto <p>Cisco Nexus 5500 シリーズ スイッチの場合は、<i>speed</i> 引数を次のいずれかに設定できます。</p> <ul style="list-style-type: none"> • 1000 : 1 Gbps • 10000 : 10Gbps • auto <p>(注) 100 Mbps は、Cisco Nexus 5596 スイッチまたは CU-96 GEM カードでサポートされる速度ではありません。</p> <p>Cisco Nexus 5596T スイッチの場合、ベース ボードポートは 1 Gbps と 10 Gbps をサポートしています。10GBase-T ポートでは、auto も選択できます。</p>

次に、1 ギガビット イーサネット ポートを設定する例を示します。

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

リンク ネゴシエーションのディセーブル化

リンク ネゴシエーションをディセーブルにするには、**no negotiate auto** コマンドを使用します。デフォルトでは、自動ネゴシエーションは1 ギガビット ポートでイネーブルであり、10 ギガビット ポートでディセーブルです。

このコマンドは、Cisco IOS の **speed non-negotiate** コマンドに相当します。



(注) 10 ギガビット ポートで自動ネゴシエーションをイネーブルにすることは推奨しません。10 ギガビット ポートで自動ネゴシエーションをイネーブルにすると、リンクがダウンします。デフォルトでは、リンク ネゴシエーションは10 ギガビット ポートでディセーブルです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface ethernet slot/port	インターフェイスを選択し、インターフェイス モードを開始します。
ステップ 3	switch(config-if)# no negotiate auto	選択したイーサネットインターフェイス (1 ギガビット ポート) のリンク ネゴシエーションをディセーブルにします。
ステップ 4	switch(config-if)# negotiate auto	<p>(任意)</p> <p>選択したイーサネットインターフェイスのリンク ネゴシエーションをイネーブルにします。1 ギガビット ポートに対するデフォルトはイネーブルです。</p> <p>(注) このコマンドは、10GBase-T ポートには適用できません。このコマンドを 10GBase-T ポートでは使用しないでください。</p>

次に、指定したイーサネット インターフェイス (1 ギガビット ポート) で自動ネゴシエーションをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no negotiate auto
switch(config-if)#
```

次に、指定したイーサネット インターフェイス（1 ギガビット ポート）で自動ネゴシエーションをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# negotiate auto
switch(config-if)#
```

CDP の特性の設定

Cisco Discovery Protocol（CDP）更新の頻度、廃棄するまで情報を保持する期間、およびバージョン 2 アドバタイズメントを送信するかどうかを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [no] cdp advertise {v1 v2}	（任意） 使用するバージョンを設定して、CDP アドバタイズメントを送信します。バージョン 2 がデフォルトステートです。 デフォルト設定に戻すには、このコマンドの no 形式を使用します。
ステップ 3	switch(config)# [no] cdp format device-id {mac-address serial-number system-name}	（任意） CDP デバイス ID の形式を設定します。デフォルトはシステム名です。完全修飾ドメイン名で表すことができます。 デフォルト設定に戻すには、このコマンドの no 形式を使用します。
ステップ 4	switch(config)# [no] cdp holdtime seconds	（任意） 受信デバイスがユーザのデバイスから送信された情報を破棄せずに保持する時間を指定します。指定できる範囲は 10 ～ 255 秒です。デフォルトは 180 秒です。 デフォルト設定に戻すには、このコマンドの no 形式を使用します。
ステップ 5	switch(config)# [no] cdp timer seconds	（任意） CDP アップデートの送信頻度を秒単位で設定します。指定できる範囲は 5 ～ 254 です。デフォルトは 60 秒です。 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。

次の例は、CDP 特性を設定する方法を示しています。

```
switch# configure terminal
switch(config)# cdp timer 50
switch(config)# cdp holdtime 120
switch(config)# cdp advertise v2
```

CDP のイネーブル化/ディセーブル化

CDP をイーサネットインターフェイスに対してイネーブルにしたり、ディセーブルにしたりできます。このプロトコルは、同一リンクの両方のインターフェイスでイネーブルになっている場合にだけ機能します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface type slot/port	特定のインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# cdp enable	インターフェイスに対して CDP をイネーブルにします。 正常に機能するには、このパラメータが同一リンク上の両方のインターフェイスでイネーブルになっている必要があります。
ステップ 4	switch(config-if)# no cdp enable	インターフェイスに対して CDP をディセーブルにします。

次に、イーサネット ポートに対して CDP をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# cdp enable
```

このコマンドは、物理的なイーサネット インターフェイスにしか適用できません。

error-disabled 検出のイネーブル化

アプリケーションでの error-disable (err-disabled) 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 err-disabled ステート（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

	コマンドまたはアクション	目的
ステップ 1	config t 例： switch# config t switch(config)#	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 {all link-flap loopback} 例： switch(config)# errdisable detect cause all switch(config)#	インターフェイスを err-disabled ステートにする条件を指定します。デフォルトはイネーブルです。
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 err-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、err-disabled ステートからインターフェイスを手動で回復できるようにします。
ステップ 5	show interface status err-disabled 例： switch(config)# show interface status err-disabled	err-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 err-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 リカバリのイネーブル化

アプリケーションを指定してインターフェイスを errdisable (err-disabled) ステートから抜け出させ、稼働を再試行できます。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

	コマンドまたはアクション	目的
ステップ 1	config t 例 : <pre>switch#config t switch(config)#</pre>	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 udld bpduguard link-flap failed-port-state pause-rate-limit} 例 : <pre>switch(config)#errdisable recovery cause all switch(config-if)#</pre>	インターフェイスが err-disabled ステートから自動的に回復する条件を指定し、デバイスはインターフェイスのアップを再試行します。デバイスは 300 秒待機してからリトライします。デフォルトはディセーブルです。
ステップ 3	show interface status err-disabled 例 : <pre>switch(config)#show interface status err-disabled</pre>	err-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 : <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、すべての条件下で err-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 リカバリ間隔の設定

errdisabled リカバリ時間値を設定するには、この手順を使用します。有効な範囲は 30 ～ 65535 秒です。デフォルト値は 300 秒です。

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例 : <pre>switch#config t switch(config)#</pre>	コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 2	errdisable recovery interval <i>interval</i> 例 : <pre>switch(config)#errdisable recovery interval 32 switch(config-if)#</pre>	インターフェイスが errdisabled ステートから回復する間隔を指定します。有効な範囲は 30 ～ 65535 秒です。デフォルト値は 300 秒です。
ステップ 3	show interface status err-disabled 例 : <pre>switch(config)#show interface status err-disabled</pre>	errdisabled 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 : <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、すべての条件下で errdisabled リカバリをイネーブ爾にする例を示します。

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

ポート プロファイル

ポート プロファイルの作成

スイッチにポート プロファイルを作成できます。各ポート プロファイルは、インターフェイスタイプにかかわらず、ネットワーク全体で一意的な名前を持つ必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	port-profile [type {ethernet interface-vlan port channel}] <i>name</i> 例 : <pre>switch(config)# port-profile type ethernet test switch(config-port-prof)#</pre>	指定されたタイプのインターフェイスのポート プロファイルを作成して命名し、ポートプロファイルコンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	exit 例 : <pre>switch(config-port-prof)# exit switch(config)#</pre>	ポートプロファイルコンフィギュレーションモードを終了します。
ステップ 4	show port-profile 例 : <pre>switch(config)# show port-profile name</pre>	(任意) ポートプロファイルの設定を表示します。
ステップ 5	copy running-config startup-config 例 : <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、イーサネットインターフェイスの **test** という名前のポート プロファイルを作成する例を示します。

```
switch# configure terminal
switch(config)# port-profile type ethernet test
switch(config-port-prof)#
```

次に、イーサネットインターフェイスに設定された **ppEth** という名前のポート プロファイルにインターフェイス コマンドを追加する例を示します。

```
switch# configure terminal
switch(config)# port-profile ppEth
switch(config-port-prof)# switchport mode trunk
switch(config-port-prof)# switchport trunk allowed vlan 300-400
switch(config-port-prof)# flowcontrol receive on
switch(config-port-prof)# speed 10000
switch(config-port-prof)#
```

ポート プロファイルの変更

ポート プロファイル コンフィギュレーション モードでポート プロファイルを変更できます。

このコマンドの **no** 形式を使用して、ポート プロファイルからコマンドを削除できます。ポート プロファイルからコマンドを削除すると、対応するコマンドは、ポート プロファイルにアタッチされているインターフェイスから削除されます。

手順

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

	コマンドまたはアクション	目的
ステップ 2	port-profile [type {ethernet interface-vlan port channel}] name 例 : <pre>switch(config)# port-profile type ethernet test switch(config-port-prof)#</pre>	指定されたポート プロファイルのポート プロファイルコンフィギュレーションモードを開始し、ポートファイルの設定を追加または削除します。
ステップ 3	exit 例 : <pre>switch(config-port-prof)# exit switch(config)#</pre>	ポートプロファイルコンフィギュレーションモードを終了します。
ステップ 4	show port-profile 例 : <pre>switch(config)# show port-profile name</pre>	(任意) ポートプロファイルの設定を表示します。
ステップ 5	copy running-config startup-config 例 : <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 インターフェイスに設定された ppEth という名前のポート プロファイルからコマンドを削除する例を示します。

```
switch# configure terminal
switch(config)# port-profile ppEth
switch(config-port-prof)# switchport mode trunk
switch(config-port-prof)# switchport trunk allowed vlan 300-400
switch(config-port-prof)# flowcontrol receive on
switch(config-port-prof)# no speed 10000
switch(config-port-prof)#
```

特定のポート プロファイルのイネーブル化

手順

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

	コマンドまたはアクション	目的
ステップ 2	port-profile [type {ethernet interface-vlan port channel}] name 例 : <pre>switch(config)# port-profile type ethernet test switch(config-port-prof)# no shutdown switch(config-port-prof)#</pre>	指定されたポート プロファイルに対して、ポート プロファイル コンフィギュレーション モードを開始します。
ステップ 3	state enabled name 例 : <pre>switch(config-port-prof)# state enabled switch(config-port-prof)#</pre>	ポート プロファイルをイネーブルにします。
ステップ 4	exit 例 : <pre>switch(config-port-prof)# exit switch(config)#</pre>	ポート プロファイル コンフィギュレーション モードを終了します。
ステップ 5	show port-profile 例 : <pre>switch(config)# show port-profile name</pre>	(任意) ポート プロファイルの設定を表示します。
ステップ 6	copy running-config startup-config 例 : <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 プロファイル コンフィギュレーション モードを開始し、ポート プロファイルをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# port-profile type ethernet test
switch(config-port-prof)# state enabled
switch(config-port-prof)#
```

ポート プロファイルの継承

ポート プロファイルを既存のポート プロファイルに継承できます。スイッチは 4 つのレベルの継承をサポートしています。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	port-profile name 例 : switch(config)# port-profile test switch(config-port-prof)#	指定したポートプロファイルのポートプロファイルコンフィギュレーションモードを開始します。
ステップ 3	inherit port-profile name 例 : switch(config-port-prof)# inherit port-profile adam switch(config-port-prof)#	別のポートプロファイルを既存のポートプロファイルに継承します。元のポートプロファイルは、継承されたポートプロファイルのすべての設定を想定します。
ステップ 4	exit 例 : switch(config-port-prof)# exit switch(config)#	ポートプロファイルコンフィギュレーション モードを終了します。
ステップ 5	show port-profile 例 : switch(config)# show port-profile name	(任意) ポート プロファイルの設定を表示します。
ステップ 6	copy running-config startup-config 例 : switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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

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

次に、イーサネット インターフェイスに設定された ppEth という名前のポート プロファイルにインターフェイス コマンドを追加する例を示します。

```
switch# configure terminal
switch(config)# port-profile ppEth
switch(config-port-prof)# switchport mode trunk
switch(config-port-prof)# switchport trunk allowed vlan 300-400
switch(config-port-prof)# flowcontrol receive on
```



```
switch(config-port-prof)# speed 10000
switch(config-port-prof)#
```

次に、**test** という名前の既存のポート プロファイルにイーサネット インターフェイスに設定された **ppEth** という名前のポート プロファイルを継承する例を示します。

```
switch# configure terminal
switch(config)# port-profile test
switch(config-port-prof)# inherit port-profile ppEth
switch(config-port-prof)#
```

次に、**ppEth** という名前のイーサネット インターフェイスに設定されたポート プロファイルをイーサネット インターフェイスの範囲に割り当てる例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2-5
switch(config-if)# inherit port-profile ppEth
switch(config-if)#
```

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

```
switch# configure terminal
switch(config)# port-profile test
switch(config-port-prof)# no inherit port-profile ppEth
switch(config-port-prof)#
```

継承されたポート プロファイルの削除

継承されたポート プロファイルを削除できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	port-profile name 例 : switch(config)# port-profile test switch(config-port-prof)#	指定したポート プロファイルのポート プロファイル コンフィギュレーション モードを開始します。
ステップ 3	no inherit port-profile name 例 : switch(config-port-prof)# no inherit port-profile adam switch(config-port-prof)#	このポート プロファイルから継承されたポート プロファイルを削除します。
ステップ 4	exit 例 : switch(config-port-prof)# exit switch(config)#	ポート プロファイル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 5	show port-profile 例 : <pre>switch(config)# show port-profile name</pre>	(任意) ポート プロファイルの設定を表示します。
ステップ 6	copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

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

一定範囲のインターフェイスへのポート プロファイルの割り当て

インターフェイスまたはインターフェイスの範囲にポート プロファイルを割り当てることができます。すべてのインターフェイスが同じタイプである必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 interface-vlan vlan-id port-channel number] 例 : <pre>switch(config)# interface ethernet 7/3-5, 10/2, 11/20-25 switch(config-if)#</pre>	インターフェイスの範囲を選択します。
ステップ 3	inherit port-profile name 例 : <pre>switch(config-if)# inherit port-profile adam switch(config-if)#</pre>	選択したインターフェイスに指定されたポート プロファイルを割り当てます。

	コマンドまたはアクション	目的
ステップ 4	exit 例 : <pre>switch(config-port-prof)# exit switch(config)#</pre>	ポートプロファイルコンフィギュレーションモードを終了します。
ステップ 5	show port-profile 例 : <pre>switch(config)# show port-profile name</pre>	(任意) ポートプロファイルの設定を表示します。
ステップ 6	copy running-config startup-config 例 : <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、イーサネットインターフェイス 2/3 ~ 2/5、3/2、および 1/20 ~ 1/25 に **adam** という名前のポートプロファイルを割り当てる例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3 to 2/5, 3/2, and 1/20 to 1/25
switch(config-if)# inherit port-profile adam
switch(config-if)#
```

一定範囲のインターフェイスからのポート プロファイルの削除

プロファイルを適用した一部またはすべてのインターフェイスから、ポートプロファイルを削除できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 interface-vlan vlan-id port-channel number] 例 : <pre>switch(config)# interface ethernet 7/3-5, 10/2, 11/20-25 switch(config-if)#</pre>	インターフェイスの範囲を選択します。

	コマンドまたはアクション	目的
ステップ 3	no inherit port-profile <i>name</i> 例 : <pre>switch(config-if)# no inherit port-profile adam switch(config-if)#</pre>	選択されたインターフェイスから指定されたポート プロファイルを削除します。
ステップ 4	exit 例 : <pre>switch(config-port-prof)# exit switch(config)#</pre>	ポート プロファイル コンフィギュレーション モードを終了します。
ステップ 5	show port-profile 例 : <pre>switch(config)# show port-profile name</pre>	(任意) ポート プロファイルの設定を表示します。
ステップ 6	copy running-config startup-config 例 : <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。

tos がイーサネット インターフェイス 1/3-5 から adam という名前のポート プロファイルを削除する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/3-5
switch(config-if)# no inherit port-profile adam
switch(config-if)#
```

ポート プロファイルの設定例

次に、ポート プロファイルを設定し、イーサネット インターフェイスのポート プロファイルを継承して、ポート プロファイルをイネーブルにする例を示します。

```
switch(config)#
switch(config)# show running-config interface Ethernet1/14

!Command: show running-config interface Ethernet1/14
!Time: Thu Aug 26 07:01:32 2010

version 5.0(2)N1(1)

interface Ethernet1/14

switch(config)# port-profile type ethernet alpha
switch(config-port-prof)# switchport mode trunk
switch(config-port-prof)# switchport trunk allowed vlan 10-15
switch(config-port-prof)#
switch(config-port-prof)# show running-config port-profile alpha

!Command: show running-config port-profile alpha
!Time: Thu Aug 26 07:02:29 2010

version 5.0(2)N1(1)
```

```

port-profile type ethernet alpha
  switchport mode trunk
  switchport trunk allowed vlan 10-15

switch(config-port-prof)# int eth 1/14
switch(config-if)# inherit port-profile alpha
switch(config-if)#
switch(config-if)# port-profile type ethernet alpha
switch(config-port-prof)# state enabled
switch(config-port-prof)#
switch(config-port-prof)# sh running-config interface ethernet 1/14

!Command: show running-config interface Ethernet1/14
!Time: Thu Aug 26 07:03:17 2010

version 5.0(2)N1(1)

interface Ethernet1/14
  inherit port-profile alpha

switch(config-port-prof)# sh running-config interface ethernet 1/14 expand-port-profile

!Command: show running-config interface Ethernet1/14 expand-port-profile
!Time: Thu Aug 26 07:03:21 2010

version 5.0(2)N1(1)

interface Ethernet1/14
  switchport mode trunk
  switchport trunk allowed vlan 10-15

switch(config-port-prof)#

```

デバウンス タイマーの設定

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

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

デバウンス タイマーをイネーブル/ディセーブルにする手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface type slot/port	特定のインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# link debounce time milliseconds	指定した時間（1 ～ 5,000 ミリ秒）でデバウンス タイマーをイネーブルにします。 0 ミリ秒を指定すると、デバウンス タイマーはディセーブルになります。

次の例は、イーサネットインターフェイスでデバウンスタイマーをイネーブルにして、デバウンス時間を 1000 ミリ秒に設定する方法を示しています。

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

次の例は、イーサネットインターフェイスでデバウンスタイマーをディセーブルにする方法を示しています。

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

説明パラメータの設定

イーサネット ポートのインターフェイスに関する説明を入力することができます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# interface type slot/port	特定のインターフェイスのインターフェイス コンフィギュレーションモードを開始します。
ステップ 3	switch(config-if)# description test	インターフェイスの説明を指定します。

次に、インターフェイスの説明を Server 3 Interface に設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# description Server 3 Interface
```

イーサネット インターフェイスのディセーブル化と再起動

イーサネットインターフェイスは、シャットダウンして再起動することができます。この操作により、すべてのインターフェイス機能がディセーブル化され、すべてのモニタリング画面でインターフェイスがダウンしているものとしてマークされます。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。シャットダウンされ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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# interface type slot/port	特定のインターフェイスのインターフェイス コンフィギュレーションモードを開始します。
ステップ 3	switch(config-if)# shutdown	インターフェイスをディセーブルにします。
ステップ 4	switch(config-if)# no shutdown	インターフェイスを再起動します。

次に、イーサネット ポートをディセーブルにする例を示します。

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

次に、イーサネット インターフェイスを再起動する例を示します。

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

インターフェイス情報の表示

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

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

コマンド	目的
switch# show interface debounce	すべてのインターフェイスのデバウンスステータスが表示されます。
switch# show interface flowcontrol	すべてのインターフェイスでフロー制御設定の詳細なリストを表示します。
show port--profile	ポート プロファイルに関する情報を表示します。

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

次に、物理イーサネット インターフェイスを表示する例を示します。

```
switch# show interface ethernet 1/1
Ethernet1/1 is up
Hardware is 1000/10000 Ethernet, address is 000d.eca3.5f08 (bia 000d.eca3.5f08)
MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 190/255, rxload 192/255
Encapsulation ARPA
Port mode is trunk
full-duplex, 10 Gb/s, media type is 1/10g
Input flow-control is off, output flow-control is off
Auto-mdix is turned on
Rate mode is dedicated
Switchport monitor is off
Last clearing of "show interface" counters never
5 minute input rate 942201806 bytes/sec, 14721892 packets/sec
5 minute output rate 935840313 bytes/sec, 14622492 packets/sec
Rx
  129141483840 input packets 0 unicast packets 129141483847 multicast packets
  0 broadcast packets 0 jumbo packets 0 storm suppression packets
  8265054965824 bytes
  0 No buffer 0 runt 0 Overrun
  0 crc 0 Ignored 0 Bad etype drop
  0 Bad proto drop
Tx
  119038487241 output packets 119038487245 multicast packets
  0 broadcast packets 0 jumbo packets
  7618463256471 bytes
  0 output CRC 0 ecc
  0 underrun 0 if down drop 0 output error 0 collision 0 deferred
  0 late collision 0 lost carrier 0 no carrier
  0 babble
  0 Rx pause 8031547972 Tx pause 0 reset
```

次に、物理イーサネットの機能を表示する例を示します。

```
switch# show interface ethernet 1/1 capabilities
Ethernet1/1
  Model: 734510033
  Type: 10Gbase-(unknown)
  Speed: 1000,10000
  Duplex: full
  Trunk encaps. type: 802.1Q
  Channel: yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol: rx-(off/on),tx-(off/on)
  Rate mode: none
  QOS scheduling: rx-(6q1t),tx-(1p6q0t)
```



```

CoS rewrite:          no
ToS rewrite:          no
SPAN:                 yes
UDLD:                 yes
Link Debounce:        yes
Link Debounce Time:   yes
MDIX:                 no
FEX Fabric:           yes

```

次に、物理イーサネット トランシーバを表示する例を示します。

```

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

```

次に、インターフェイス ステータスの要約を表示する例を示します（簡潔にするため、一部の出力が削除されています）。

```
switch# show interface brief
```

Ethernet Interface	VLAN	Type	Mode	Status	Reason	Speed	Port Ch #
Eth1/1	200	eth	trunk	up	none	10G(D)	--
Eth1/2	1	eth	trunk	up	none	10G(D)	--
Eth1/3	300	eth	access	down	SFP not inserted	10G(D)	--
Eth1/4	300	eth	access	down	SFP not inserted	10G(D)	--
Eth1/5	300	eth	access	down	Link not connected	1000(D)	--
Eth1/6	20	eth	access	down	Link not connected	10G(D)	--
Eth1/7	300	eth	access	down	SFP not inserted	10G(D)	--

次に、リンクのデバウンス ステータスを表示する例を示します（簡潔にするため、一部の出力が削除されています）。

```
switch# show interface debounce
```

Port	Debounce time	Value(ms)
Eth1/1	enable	100
Eth1/2	enable	100
Eth1/3	enable	100

次に、CDP ネイバーを表示する例を示します。



(注) 上の例にあるように、CDP アドバタイズメントのためのデフォルトのデバイス ID フィールドはホスト名とシリアル番号です。

```

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

Device ID         Local Intrfce   Hldtme   Capability   Platform   Port ID
dl3-dist-1        mgmt0          148      S I          WS-C2960-24TC  Fas0/9
n5k(FLC12080012)  Eth1/5         8        S I s        N5K-C5020P-BA  Eth1/5

```

物理イーサネットのデフォルト設定

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

パラメータ	デフォルト設定
デバウンス	イネーブル、100 ミリ秒
デュプレックス	オート（全二重）
カプセル化	ARPA
MTU ¹	1500 バイト
ポート モード	アクセス
速度	オート（10000）

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



第 3 章

レイヤ 3 インターフェイスの設定

この章の内容は、次のとおりです。

- [レイヤ 3 インターフェイスについて, 37 ページ](#)
- [レイヤ 3 インターフェイスのライセンス要件, 40 ページ](#)
- [レイヤ 3 インターフェイスの注意事項および制約事項, 41 ページ](#)
- [レイヤ 3 インターフェイスのデフォルト設定, 41 ページ](#)
- [レイヤ 3 インターフェイスの設定, 41 ページ](#)
- [レイヤ 3 インターフェイス設定の確認, 47 ページ](#)
- [レイヤ 3 インターフェイスのモニタリング, 49 ページ](#)
- [レイヤ 3 インターフェイスの設定例, 50 ページ](#)
- [レイヤ 3 インターフェイスの関連資料, 51 ページ](#)
- [レイヤ 3 インターフェイスの MIB, 51 ページ](#)
- [レイヤ 3 インターフェイスの標準, 51 ページ](#)

レイヤ 3 インターフェイスについて

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

ルーテッド インターフェイス

ポートをレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスとして設定できます。ルーテッドインターフェイスは、IP トラフィックを他のデバイスにルーティングできる物理ポートで

す。ルーテッドインターフェイスはレイヤ3インターフェイスだけで、スパニングツリー プロトコル (STP) などのレイヤ2プロトコルはサポートしません。

イーサネット ポートはすべて、デフォルトではスイッチドインターフェイスです。このデフォルト動作は、CLI セットアップ スクリプトまたは **system default switchport** コマンドを使用して変更できます。

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。

レイヤ3インターフェイスにスタティック MAC アドレスを割り当てることができます。MAC アドレスの設定については、を参照してください。

ルーテッドインターフェイスからレイヤ3 ポート チャンネルも作成できます。

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

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

サブインターフェイス

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

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

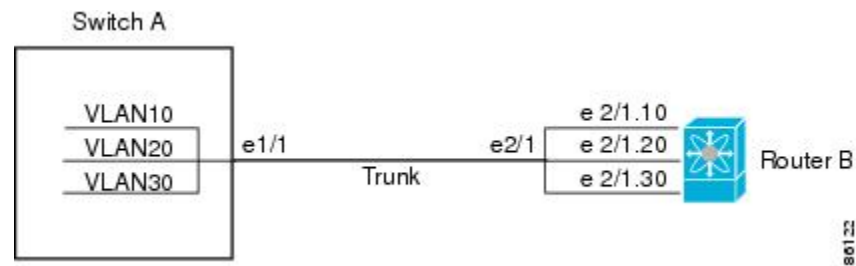
サブインターフェイスの名前は、親インターフェイスの名前（たとえば **Ethernet 2/1**）+ピリオド（.）+そのインターフェイス独自の番号です。たとえば、イーサネット インターフェイス 2/1 に **Ethernet2/1.1** というサブインターフェイスを作成できます。この場合、.1はそのサブインターフェイスを表します。

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

サブインターフェイスを使用すると、親インターフェイスがサポートする各 VLAN に独自のレイヤ3インターフェイスを実現できます。この場合、親インターフェイスは別のデバイスのレイヤ2 トランッキング ポートに接続します。サブインターフェイスを設定したら 802.1Q トランッキング を使って VLAN ID に関連付けます。

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

図 2: VLAN のサブインターフェイス



VLAN インターフェイス

VLAN インターフェイスまたはスイッチ仮想インターフェイス (SVI) は、デバイス上の VLAN を同じデバイス上のレイヤ3ルーティング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。ロールバックおよびチェックポイントについては、を参照してください。



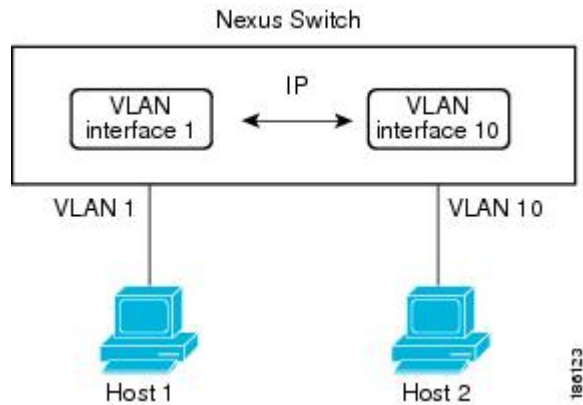
(注) VLAN 1 の VLAN インターフェイスは削除できません。

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 アドレスおよび IP ルーティングの詳細については、を参照してください。

次の図に、デバイス上の2つの VLAN に接続されている2つのホストを示します。VLAN ごとに VLAN インターフェイスを設定し、VLAN 間の IP ルーティングを使ってホスト1とホスト2を通

信させることができます。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 3: VLAN インターフェイスによる 2つの VLAN の接続



ループバック インターフェイス

ループバック インターフェイスは、常にアップ状態にある単独のエンドポイントを持つ仮想インターフェイスです。ループバック インターフェイス経由で送信されたパケットはすべて、このインターフェイスでただちに受信されます。ループバック インターフェイスは物理インターフェイスをエミュレートします。

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

トンネル インターフェイス

Cisco NX-OS は、IP トンネルとしてトンネル インターフェイスをサポートします。IP トンネルを使うと、同じレイヤまたは上位レイヤのプロトコルをカプセル化して、2 台のルータ間で作成されたトンネルを通じて IP の結果を転送できます。

レイヤ 3 インターフェイスのライセンス要件

この機能にはライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

レイヤ3インターフェイスの注意事項および制約事項

レイヤ3インターフェイスの設定には次の注意事項と制約事項があります。

- レイヤ3インターフェイスをレイヤ2インターフェイスに変更する場合、Cisco NX-OS はインターフェイスをシャットダウンしてインターフェイスを再度イネーブルにし、レイヤ3固有の設定をすべて削除します。
- レイヤ2インターフェイスをレイヤ3インターフェイスに変更する場合、Cisco NX-OS はインターフェイスをシャットダウンしてインターフェイスを再度イネーブルにし、レイヤ2固有の設定をすべて削除します。

レイヤ3インターフェイスのデフォルト設定

レイヤ3管理状態のデフォルト設定は Shut です。

レイヤ3インターフェイスの設定

ルーテッドインターフェイスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface ethernet slot/port	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# no switchport	インターフェイスをレイヤ3インターフェイスとして設定し、このインターフェイス上のレイヤ2に固有の設定をすべて削除します。 (注) レイヤ3インターフェイスを元のレイヤ2インターフェイスに変換するには、 switchport コマンドを使用します。
ステップ 4	switch(config-if)# [ip ipv6] [<i>ip-address/length</i>]	このインターフェイスの IPv4 アドレスまたは IPv6 アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 5	switch(config-if)# medium {broadcast p2p}	(任意) 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。
ステップ 6	switch(config-if)# show interfaces	(任意) レイヤ3 インターフェイスの統計情報を表示します。
ステップ 7	switch(config-if)# copy running-config startup-config	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、IPv4 ルーテッド レイヤ 3 インターフェイスを設定する例を示します。

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

サブインターフェイスの設定

はじめる前に

- 親インターフェイスをルーテッド インターフェイスとして設定します。
- このポート チャネル上にサブインターフェイスを作成するには、ポート チャネル インターフェイスを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config-if)# copy running-config startup-config	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレー

	コマンドまたはアクション	目的
		ションにコピーして、変更を永続的に保存します。
ステップ 2	<code>switch(config)# interface ethernet slot/port.number</code>	インターフェイス コンフィギュレーション モードを開始します。 <i>slot</i> の範囲は 1 ～ 255 です。 <i>port</i> の範囲は 1 ～ 128 です。
ステップ 3	<code>switch(config-if)#[ip ipv6] address ip-address/length</code>	このインターフェイスの IPv4 アドレスまたは IPv6 アドレスを設定します。
ステップ 4	<code>switch(config-if)# encapsulation dot1Q vlan-id</code>	サブインターフェイス上の IEEE 802.1Q VLAN カプセル化を設定します。 <i>vlan-id</i> の範囲は 2 ～ 4093 です。
ステップ 5	<code>switch(config-if)# show interfaces</code>	(任意) レイヤ3インターフェイスの統計情報を表示します。
ステップ 6	<code>switch(config-if)# copy running-config startup-config</code>	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、サブインターフェイスを作成する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# encapsulation dot1Q 33
switch(config-if)# copy running-config startup-config
```

インターフェイスでの帯域幅の設定

ルーテッドインターフェイス、ポートチャネル、またはサブインターフェイスに帯域幅を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	<code>switch# configure terminal</code>	グローバル コンフィギュレーション モードを開始します。

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

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

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

VLAN インターフェイスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	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。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# interface vlan <i>number</i>	VLAN インターフェイスを作成します。 <i>number</i> の範囲は 1 ～ 4094 です。
ステップ 4	switch(config-if)# [ip ipv6] address <i>ip-address/length</i>	このインターフェイスの IPv4 アドレスまたは IPv6 アドレスを設定します。
ステップ 5	switch(config-if)# show interface vlan <i>number</i>	(任意) VLAN インターフェイスの統計情報を表示します。 <i>number</i> の範囲は 1 ～ 4094 です。
ステップ 6	switch(config-if)# copy running-config startup-config	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

次に、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

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface loopback <i>instance</i>	ループバック インターフェイスを作成します。 <i>instance</i> の範囲は 0 ～ 1023 です。
ステップ 3	switch(config-if)# [ip ipv6] address <i>ip-address/length</i>	このインターフェイスの IPv4 アドレスまたは IPv6 アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 4	switch(config-if)# show interface loopback instance	(任意) ループバック インターフェイスの統計情報を表示します。 <i>instance</i> の範囲は 0 ～ 1023 です。
ステップ 5	switch(config-if)# copy running-config startup-config	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

次に、ループバック インターフェイスを作成する例を示します。

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

VRF へのインターフェイスの割り当て

はじめる前に

VRF 用のインターフェイスを設定した後で、トンネル インターフェイスに IP アドレスを割り当てます。

手順

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

	コマンドまたはアクション	目的
ステップ 5	switch(config-if)# show vrf [vrf-name] interface interface-type number	(任意) VRF 情報を表示します。
ステップ 6	switch(config-if)# show interfaces	(任意) レイヤ3 インターフェイスの統計情報を表示 します。
ステップ 7	switch(config-if)# copy running-config startup-config	(任意) リブートおよびリスタート時に実行コンフィ ギュレーションをスタートアップコンフィギュ レーションにコピーして、変更を永続的に保 存します。

次に、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

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show interface ethernet slot/port	レイヤ3 インターフェイスの設定情報、ステータス、カウンタ（インバウンドおよびアウトバウンド パケット レートおよびバイト レートが 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。
show interface ethernet slot/port brief	レイヤ3 インターフェイスの動作ステータスを表示します。
show interface ethernet slot/port capabilities	レイヤ3 インターフェイスの機能（ポートタイプ、速度、およびデュプレックスを含む）を表示します。
show interface ethernet slot/port description	レイヤ3 インターフェイスの説明を表示します。

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

レイヤ3インターフェイスのモニタリング

次のいずれかのコマンドを使用して、機能に関する統計情報を表示します。

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

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

レイヤ3 インターフェイスの設定例

次に、イーサネット サブインターフェイスを設定する例を示します。

```
switch# configuration terminal
switch(config)# interface ethernet 2/1.10
switch(config-if)# no switchport
switch(config-if)# description Layer 3 for VLAN 10
switch(config-if)# encapsulation dot1q 10
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# copy running-config startup-config
```

次に、VLAN インターフェイスを設定する例を示します。

```
switch# configuration terminal
switch(config)# interface vlan 100
switch(config-if)# no switchport
switch(config-if)# ipv6 address 33:0DB::2/8
switch(config-if)# copy running-config startup-config
```

次に、ループバック インターフェイスを設定する例を示します。

```
switch# configuration terminal
switch(config)# interface loopback 3
switch(config-if)# no switchport
switch(config-if)# ip address 192.0.2.2/32
switch(config-if)# copy running-config startup-config
```


レイヤ3インターフェイスの関連資料

関連トピック	参照先
コマンド構文	『Cisco Nexus 5000 Series NX-OS Interfaces Command Reference』
IP	『Cisco Nexus 5000 Series NX-OS Unicast Routing Configuring Guide』の「Configuring IP」の章
VLAN	『Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide』の「Configuring VLANs」の章

レイヤ3インターフェイスの MIB

MIB	MIB のリンク
IF-MIB	MIBを検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
CISCO-IF-EXTENSION-MIB	
ETHERLIKE-MIB	

レイヤ3インターフェイスの標準

この機能で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。



第 4 章

ポート チャネルの設定

この章の内容は、次のとおりです。

- [ポート チャネルについて, 53 ページ](#)
- [ポート チャネルの設定, 63 ページ](#)
- [ポート チャネルの設定の確認, 74 ページ](#)
- [ロードバランシングの発信ポート ID の確認, 75 ページ](#)

ポート チャネルについて

ポート チャネルは、最大 32 の個別インターフェイスを 1 つのグループに集約して、帯域幅と冗長性の向上を実現します。これらの集約された各物理インターフェイス間でトラフィックのロード バランシングも行います。ポート チャネルの物理インターフェイスが少なくとも 1 つ動作していれば、そのポート チャネルは動作しています。

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

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

プロトコルが関連付けられていない場合でもスタティックポートチャネルを使用して設定を簡略化できます。より効率的にポートチャネルを使用するには、IEEE 802.3ad に規定されているリンクアグリゲーション制御プロトコル (LACP) を使用します。LACPを使用すると、リンクによってプロトコルパケットが渡されます。

関連トピック

[LACP の概要, \(60 ページ\)](#)

ポートチャネルの概要

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

最大 16 のポートを 1 つのスタティックポートチャネルに集約するか、またはリンクアグリゲーション制御プロトコル (LACP) をイネーブルにできます。LACP でポートチャネルを設定する場合、スタティックポートチャネルを設定する場合とは若干異なる手順が必要です。



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

ポートチャネルは、個別リンクをまとめて 1 つのチャネルグループに入れ、最大 16 の物理リンクの帯域幅を集約した単一の論理リンクを作ります。ポートチャネル内のメンバポートに障害が発生すると、障害が発生したリンクで伝送されていたトラフィックはポートチャネル内のその他のメンバポートに切り替わります。

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



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

ポートチャネルインターフェイスを作成すると、ポートチャネルを直接作成できます。またはチャネルグループを作成して個別ポートをバンドルに集約させることができます。インターフェイスをチャネルグループに関連付けると、ポートチャネルがまだ存在していない場合は、対応するポートチャネルが Cisco NX-OS によって自動的に作成されます。最初にポートチャネルを作成することもできます。このインスタンスで、Cisco NX-OS は、ポートチャネルと同じチャネル番号で空のチャネルグループを作成し、デフォルトの設定を採用します。



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

ポートチャネルの設定に関する注意事項および制約事項

ポートチャネルは、グローバルコンフィギュレーションモードまたはスイッチプロファイルモードの 2 つの方法のいずれかで設定できます。ポートチャネルを Cisco NX-OS の設定同期機能で設定する場合は、次の注意事項および制約事項を考慮してください。

- ポートチャネルがスイッチプロファイルモードを使用して設定した後は、グローバルコンフィギュレーション (config terminal) モードを使用して設定できません。



(注) いくつかのポートチャネルサブコマンドは、スイッチプロファイルモードで設定できません。これらのコマンドはグローバルコンフィギュレーションモードで設定できます。ポートチャネルがスイッチプロファイルモードで作成されて設定された場合も同様です。

たとえば、次のコマンドはグローバルコンフィギュレーションモードでだけ設定できます。

switchport private-vlan association trunk primary-vlan secondary-vlan

- shutdown および no shutdown はグローバルコンフィギュレーションモードまたはスイッチプロファイルモードで設定できます。
- ポートチャネルがグローバルコンフィギュレーションモードで作成されている場合、メンバインターフェイスを含むチャネルグループも、グローバルコンフィギュレーションモードを使用して作成する必要があります。
- スイッチプロファイルモードで設定されたポートチャネルでは、スイッチプロファイルの内側と外側の両方にメンバを持つ場合があります。
- スイッチプロファイルにメンバインターフェイスをインポートする場合は、メンバインターフェイスと対応するポートチャネルもスイッチプロファイル内に存在する必要があります。

スイッチプロファイルの詳細については、『Cisco NX-OS 5000 System Management Configuration Guide』を参照してください。

互換性要件

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

互換性チェックの対象となる動作属性は次のとおりです。

- ポートモード
- アクセス VLAN
- トランクネイティブ VLAN
- 許可 VLAN リスト
- 速度
- 802.3x フロー制御設定

- MTU

Cisco Nexus 5000 シリーズ スイッチは、システム レベルの MTU だけをサポートします。この属性を個々のポートごとに変更できません。

- ブロードキャスト/ユニキャスト/マルチキャスト ストーム制御設定
- プライオリティ フロー制御
- タグなし CoS

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

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

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

- 帯域幅
- MAC アドレス
- STP

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

- 説明
- CDP
- LACP ポート プライオリティ
- デバウンス

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

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

- インターフェイスがポートチャネルに参加するか脱退しても、次のパラメータは影響を受けません。
 - ビーコン
 - 説明
 - CDP
 - LACP ポート プライオリティ
 - デバウンス
 - UDLD
 - シャットダウン
 - SNMP トラップ

ポートチャネルを使ったロードバランシング

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

- レイヤ 2 フレームの場合は、送信元および宛先の MAC アドレスを使用します。
- レイヤ 3 フレームの場合は、送信元および宛先の MAC アドレスと送信元および宛先の Internet Protocol (IP) アドレスを使用します。
- レイヤ 4 フレームの場合は、送信元および宛先の MAC アドレスと送信元および宛先の IP アドレスを使用します。



(注) レイヤ 4 フレームの場合、送信元ポートと宛先ポート番号を含めるオプションがあります。

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

- 宛先 MAC アドレス
- 送信元 MAC アドレス
- 送信元および宛先 MAC アドレス
- 宛先 IP アドレス
- 送信元 IP アドレス

- 送信元および宛先 IP アドレス
- 宛先 Transmission Control Protocol (TCP) /User Datagram Protocol (UDP) ポート番号
- 送信元 TCP/UDP ポート番号
- 送信元および宛先 TCP/UDP ポート番号

表 4: ポートチャネルロードバランシング基準

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

ファブリックエクステンダは個別に設定できません。ファブリックエクステンダ設定は Nexus 5000 シリーズで定義されます。次の表で、ポートチャネルロードバランシングプロトコルの場合に、Nexus 5000 シリーズで実行される設定の結果としてファブリックエクステンダモジュールで自動的に設定されるポートチャネルロードバランシングオプションについて説明します。

次の表に、各設定で使用する基準を示します。

表 5: Cisco Nexus 2232 および Cisco Nexus 2248 ファブリック エクステンダのポートチャネル ロードバランシング基準

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

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

LACP の概要

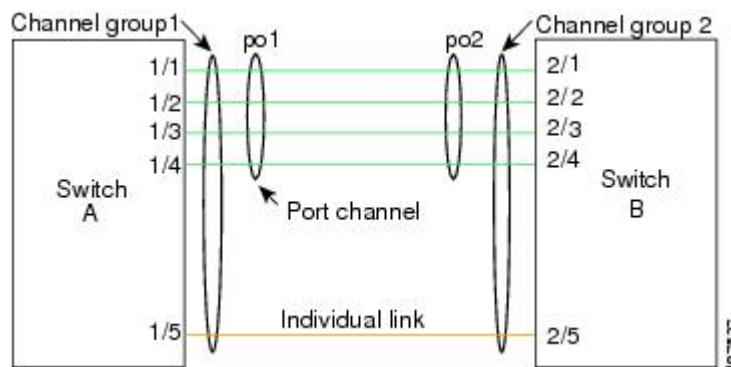
LACP の概要



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

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

図 4：個別リンクをポートチャネルに組み込む



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



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

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

LACP ID パラメータ

LACP では次のパラメータを使用します。

- LACP システム プライオリティ：LACP を稼働している各システムは、LACP システム プライオリティ値を持っています。このパラメータのデフォルト値である 32768 をそのまま使用するか、1 ～ 65535 の範囲で値を設定できます。LACP は、このシステム プライオリティと MAC アドレスを組み合わせてシステム ID を生成します。また、システム プライオリティを他のデバイスとのネゴシエーションにも使用します。システム プライオリティ値が大きいほど、プライオリティは低くなります。



(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各ポートには、LACP ポート プライオリティが割り当てられます。デフォルト値である 32768 をそのまま使用するか、1 ~ 65535 の範囲で値を設定できます。LACP はポート プライオリティとポート番号を使用してポート ID を形成します。また、互換性のあるポートのうち一部を束ねることができない場合に、どのポートをスタンバイ モードにし、どのポートをアクティブ モードにするかを決定するのに、ポート プライオリティを使用します。LACP では、ポート プライオリティ値が大きいほど、プライオリティは低くなります。指定ポートが、より低い LACP プライオリティを持ち、ホット スタンバイ リンクではなくアクティブ リンクとして選択される可能性が最も高くなるように、ポート プライオリティを設定できます。
- **LACP 管理キー** : LACP は、LACP を使用するように設定された各ポート上のチャネルグループ番号に等しい管理キー値を自動的に設定します。管理キーは、他のポートと集約されるポートの機能を定義します。他のポートと集約されるポート機能は、次の要因によって決まります。
 - ポートの物理特性 (データレート、デュプレックス機能、ポイントツーポイントまたは共有メディア ステートなど)
 - ユーザが作成した設定に関する制限事項

チャネル モード

ポートチャネルの個別インターフェイスは、チャネルモードで設定します。プロトコルを使用せずにスタティックポートチャネルを実行すると、チャネルモードは常に **on** に設定されます。デバイス上で LACP をグローバルにイネーブルにした後、各チャネルの LACP をイネーブルにします。それには、各インターフェイスのチャネルモードを **active** または **passive** に設定します。LACP チャネルグループを構成する個々のリンクについて、どちらかのチャネルモードを設定できます。



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

次の表に、各チャネルモードについて説明します。

表 6: ポートチャネルの個別リンクのチャネルモード

チャネルモード	説明
passive	ポートをパッシブなネゴシエーション状態にする LACP モード。この状態では、ポートは受信した LACP パケットに応答はしますが、LACP ネゴシエーションを開始することはありません。
active	LACP モード。ポートをアクティブネゴシエーションステートにします。ポートは LACP パケットを送信して、他のポートとのネゴシエーションを開始します。
on	すべてのスタティックポートチャネル、つまり LACP を稼働していないポートチャネルは、このモードのままになります。LACP をイネーブルにする前にチャネルモードを active または passive に変更しようとする、デバイスがエラーメッセージを返します。 チャネルで LACP をイネーブルにするには、そのチャネルのインターフェイスでチャネルモードを active または passive に設定します。LACP は、on 状態のインターフェイスとネゴシエートする場合、LACP パケットを受信しないため、そのインターフェイスと個別のリンクを形成します。つまり、LACP チャネルグループには参加しません。

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

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

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

- on モードのポートは LACP を実行していません。

LACP マーカー レスポンダ

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

LACP がイネーブルのポートチャネルとスタティックポートチャネルの相違点

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

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

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

ポートチャネルの設定

ポートチャネルの作成

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



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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# interface port-channel channel-number	設定するポートチャネルインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。指定できる範囲は1～4096です。チャネルグループがまだ存在していなければ、Cisco NX-OS によって自動的に作成されます。
ステップ 3	switch(config)# no interface port-channel channel-number	ポートチャネルを削除し、関連するチャネルグループを削除します。

次の例は、ポートチャネルの作成方法を示しています。

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

ポートチャネルへのポートの追加

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



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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# interface type slot/port	チャネルグループに追加するインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 3	switch(config-if)# switchport mode trunk	(任意) トランクポートとしてインターフェイスを設定します。

	コマンドまたはアクション	目的
ステップ 4	<code>switch(config-if)# switchport trunk {allowed vlan vlan-id native vlan vlan-id}</code>	(任意) トランクポートに必要なパラメータを設定します。
ステップ 5	<code>switch(config-if)# channel-group channel-number</code>	チャネルグループ内にポートを設定し、モードを設定します。 channel-number の指定できる範囲は 1 ～ 4096 です。Cisco NX-OS では、このチャネルグループに関連付けられたポートチャネルがなければ作成されます。これはポートチャネルの暗黙的作成と呼ばれます。
ステップ 6	<code>switch(config-if)# no channel-group</code>	(任意) チャネルグループからポートを削除します。チャネルグループから削除されたポートは元の設定に戻ります。

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

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

ポートチャネルを使ったロードバランシングの設定

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



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

手順

	コマンドまたはアクション	目的
ステップ 1	<code>switch# configure terminal</code>	コンフィギュレーションモードを開始します。
ステップ 2	<code>switch(config)# port-channel load-balance ethernet</code> <code>{[destination-ip destination-mac destination-port source-dest-ip source-dest-mac source-dest-port source-ip </code>	デバイスのロードバランシングアルゴリズムを指定します。指定可能なアルゴリズムはデバイスによって異なります。デフォルトは source-dest-mac です。 Cisco NX-OS Release 5.0(3)N2(1) 以降、Cisco Nexus 5500 プラットフォームスイッチはハッシュパラメー

	コマンドまたはアクション	目的
	source-mac source-port] crc-poly}	タでの圧縮に使用できる 8 個のハッシュ多項式をサポートします。ポートチャネルからの出力トラフィックフローのハッシュパラメータの種類によっては、多項式ごとに異なる負荷分散の結果となることがあります。デフォルトのハッシュ多項式は CRC8a です。変数は、次のように設定できます。 <ul style="list-style-type: none"> • CRC8a • CRC8b • CRC8c • CRC8d • CRC8e • CRC8f • CRC8g
ステップ 3	switch(config)# no port-channel load-balance ethernet	(任意) source-dest-mac のデフォルトのロードバランシングアルゴリズムを復元します。
ステップ 4	switch# 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。

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

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



(注) source-dest-ip、source-dest-mac、source-dest-port の各キーワードは、Cisco NX-OS の 4.0 (1a) N1 より以前のリリースの場合、それぞれ source-destination-ip、source-destination-mac、source-destination-port です。

マルチキャストトラフィックのハードウェアハッシュの設定

スイッチのいずれのポートにある入力マルチキャストトラフィックでも、デフォルトで、特定のポートチャネルメンバが選択され、トラフィックが出力されます。潜在的な帯域幅の問題を減らし、入力マルチキャストトラフィックの効率的なロードバランシングを提供するために、マルチキャストトラフィックにハードウェアハッシュを設定できます。ハードウェアハッシュをイ

ネーブルにするには、**hardware multicast hw-hash** コマンドを使用します。デフォルトに戻すには、**no hardware multicast hw-hash** コマンドを使用します。

手順

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

次に、ポートチャネルでハードウェアハッシュを設定する例を示します。

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

次に、ポートチャネルからハードウェアハッシュを削除する例を示します。

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

LACP のイネーブル化

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

LACP は、LAN ポートグループの機能を動的に学習し、残りの LAN ポートに通知します。LACP は、正確に一致しているイーサネットリンクを識別すると、これらのリンクを 1 つのポートチャネルとして容易にまとめます。次に、ポートチャネルは単一ブリッジポートとしてスパンニングツリーに追加されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# feature lacp	スイッチ上で LACP をイネーブルにします。
ステップ 3	switch(config)# show feature	(任意) イネーブルにされた機能を表示します。

次に、LACP をイネーブルにする例を示します。

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

ポートのチャネルモードの設定

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

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

はじめる前に

LACP 機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# interface type slot/port	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# channel-group channel-number [force] [mode {on active passive}]	<p>ポートチャネルのリンクのポートモードを指定します。LACP をイネーブルにしたら、各リンクまたはチャネル全体を active または passive に設定します。</p> <p>force : LAN ポートをチャネル グループに強制的に追加することを指定します。このオプションは、Cisco NX-OS Release 5.0(2)N2(1) で使用できます。</p> <p>mode : インターフェイスのポート チャネル モードを指定します。</p>

	コマンドまたはアクション	目的
		<p>active : LACP をイネーブルにすると、このコマンドは、指定されたインターフェイスで LACP をイネーブルにすることを指定します。インターフェイスはアクティブなネゴシエーション状態になります。この状態では、ポートは LACP パケットを送信して他のポートとネゴシエーションを開始します。</p> <p>on : (デフォルト モード) LACP を実行していないすべてのポートチャネルがこのモードを維持することを指定します。</p> <p>passive : LACP デバイスが検出された場合にだけ、LACP をイネーブルにします。インターフェイスはパッシブなネゴシエーション状態になります。この状態では、ポートは受信した LACP パケットに応答しますが、LACP ネゴシエーションを開始しません。</p> <p>関連するプロトコルを使用せずにポートチャネルを実行する場合、チャネル モードは常に on です。</p>
ステップ 4	<code>switch(config-if)# no channel-group number mode</code>	指定インターフェイスのポート モードを on に戻します

次に、チャネル グループ 5 のイーサネット インターフェイス 1/4 で、LACP がイネーブルなインターフェイスを active ポート チャネル モードに設定する例を示します。

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

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

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

LACP 高速タイマー レートの設定

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

はじめる前に

LACP 機能がイネーブルになっていることを確認します。

手順

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

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

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

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

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

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

LACP のシステム プライオリティおよびシステム ID の設定

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

はじめる前に

LACP 機能がイネーブルになっていることを確認します。

手順

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

	コマンドまたはアクション	目的
ステップ 3	switch# show lacp system-identifier	(任意) LACP システム識別子を表示します。

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

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

LACP ポート プライオリティの設定

ポート プライオリティに LACP ポート チャネルの各リンクを設定できます。

はじめる前に

LACP 機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface type slot/port	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# lacp port-priority priority	LACP で使用するポート プライオリティを設定します。指定できる範囲は 1 ～ 65535 で、値が大きいほどプライオリティは低くなります。デフォルト値は 32768 です。

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

はじめる前に

- LACP 機能をイネーブルにします。
- ポートチャネルが管理上ダウン状態であることを確認します。
- 正しい VDC を使用していることを確認します。正しい VDC に切り替えるには、**switchto vdc** コマンドを入力します。

手順

	コマンドまたはアクション	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>number</i> 例 : <pre>switch(config)# interface port-channel 1 switch(config) #</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。
ステップ 3	shutdown 例 : <pre>switch(config-if)# shutdown switch(config-if) #</pre>	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 : <pre>switch(config-if)# no lacp graceful-convergence switch(config-if) #</pre>	指定したポートチャネルの LACP グレースフル コンバージェンスをディセーブルにします。
ステップ 5	no shutdown 例 : <pre>switch(config-if)# no shutdown switch(config-if) #</pre>	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 : <pre>switch(config-if)# copy running-config startup-config</pre>	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

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例を示します。

```
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
switch(config-if) #
```

LACP グレースフル コンバージェンスの再イネーブル化

はじめる前に

- LACP 機能をイネーブルにします。
- ポート チャネルが管理上ダウン状態であることを確認します。
- 正しい VDC を使用していることを確認します。正しい VDC に切り替えるには、**switchto vdc** コマンドを入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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) #	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) #	ポートチャネルを管理シャットダウンします。
ステップ 4	lacp graceful-convergence 例 : switch(config-if)# lacp graceful-convergence switch(config-if) #	指定したポートチャネルの 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。

	コマンドまたはアクション	目的
ステップ 5	no shutdown 例 : <pre>switch(config-if)# no shutdown switch(config-if) #</pre>	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 : <pre>switch(config-if)# copy running-config startup-config</pre>	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

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例を示します。

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

ポートチャネルの設定の確認

ポートチャネルの設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
switch# show interface port-channel <i>channel-number</i>	ポートチャネルインターフェイスのステータスを表示します。
switch# show feature	イネーブルにされた機能を表示します。
switch# show resource	システムで現在使用可能なリソースの数を表示します。
switch# show lacp {counters interface type <i>slot/port</i> neighbor port-channel system-identifier}	LACP 情報を表示します。
switch# 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。
switch# show port-channel database [interface port-channel <i>channel-number</i>]	1つ以上のポートチャネルインターフェイスの集約状態を表示します。

コマンド	目的
switch# show port-channel summary	ポートチャネルインターフェースの概要を表示します。
switch# 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。
switch# 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。
switch# show port-channel database	現在実行中のポートチャネル機能に関する情報を表示します。
switch# show port-channel load-balance	ポートチャネルを使用したロードバランシングに関する情報を表示します。

ロードバランシングの発信ポート ID の確認

コマンドのガイドライン

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



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

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

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

例

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

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

```
Missing params will be substituted by 0's.Load-balance Algorithm on switch:  
source-dest-portcrc8_hash: 204 Outgoing port id: Ethernet1/1 Param(s) used  
to calculate load-balance:  
dst-port: 1  
src-port: 0  
dst-ip: 1.225.225.225  
src-ip: 1.1.10.10  
dst-mac: 0000.0000.0000  
src-mac: aabb.ccdd.eeff
```



第 5 章

仮想ポート チャネルの設定

この章の内容は、次のとおりです。

- [vPC について, 77 ページ](#)
- [vPC の注意事項および制約事項, 92 ページ](#)
- [vPC の設定, 93 ページ](#)
- [vPC ピア スイッチの設定, 107 ページ](#)
- [vPC 設定の確認, 110 ページ](#)
- [vPC の設定例, 116 ページ](#)
- [vPC のデフォルト設定, 120 ページ](#)

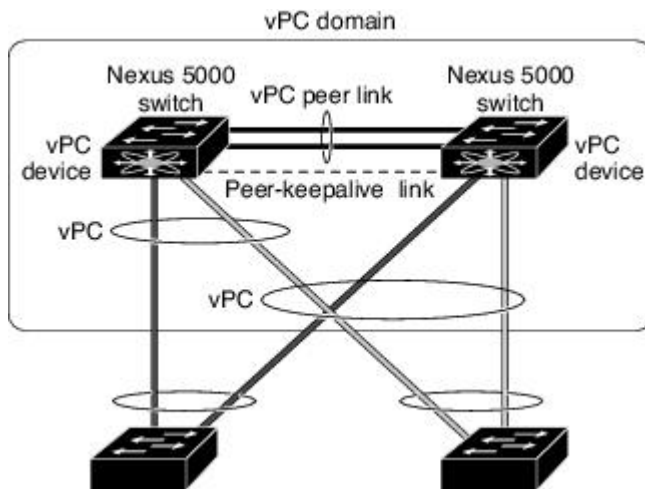
vPC について

vPC の概要

仮想ポート チャネル (vPC) は、物理的には 2 台の異なる Cisco Nexus 5000 シリーズ スイッチまたは Cisco Nexus 2000 シリーズ ファブリック エクステンダに接続されているリンクを、第 3 のデバイスには単一のポート チャネルに見えるようにします (次の図を参照)。第 3 のデバイスは、スイッチ、サーバ、またはその他の任意のネットワーキング デバイスです。Cisco NX-OS Release 4.1(3)N1(1)以降では、ファブリック エクステンダに接続された Cisco Nexus 5000 シリーズ スイッチを含むトポロジ内に vPC を設定できます。vPC では、マルチパスを提供できます。この機能で

は、ノード間の複数のパラレルパスをイネーブルにし、存在する代替パスでトラフィックのロードバランシングを行うことによって、冗長性が作成されます。

図 5: vPC のアーキテクチャ



EtherChannel の設定は、次のいずれかを使用して行います。

- プロトコルなし
- リンク アグリゲーション制御プロトコル (LACP)

vPC に EtherChannel を設定する場合 (vPC ピア リンク チャネルも含める)、各スイッチは、単一の EtherChannel 内に最大 16 個のアクティブ リンクを設定できます。ファブリック エクステンダで vPC を設定するとき、EtherChannel 内で許可されているのは 1 つのポートだけです。



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

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

vPC ピア リンクを作成するには、2 つ以上のイーサネット ポートを使用して、1 台の Cisco Nexus 5000 シリーズ スイッチ上で EtherChannel を設定します。もう 1 台のスイッチには、2 つ以上のイーサネット ポートをまた使用して別の EtherChannel を設定します。これら 2 つの EtherChannel を同時に接続すると、vPC ピア リンクが作成されます。



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

vPC ドメインには、両方の vPC ピア デバイス、vPC ピアキープアライブ リンク、vPC ピア リンク、および vPC ドメイン内にあってダウンストリーム デバイスに接続されているすべての

EtherChannel が含まれます。各 vPC ピア デバイスに設定できる vPC ドメイン ID は、1 つだけです。



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

vPC には次の利点があります。

- 単一のデバイスが 2 つのアップストリーム デバイスを介して 1 つの EtherChannel を使用することを可能にします。
- スパニングツリー プロトコル (STP) のブロック ポートをなくします。
- ループフリーなトポロジを提供します。
- 利用可能なすべてのアップリンク帯域幅を使用します。
- リンクまたはスイッチに障害が発生した場合に高速なコンバージェンスを提供します。
- リンクレベルの復元力を提供します。
- ハイ アベイラビリティを保証します。

用語

vPC の用語

vPC で使用される用語は、次のとおりです。

- **vPC** : vPC ピア デバイスとダウンストリーム デバイスの間の結合された EtherChannel。
- **vPC ピア デバイス** : vPC ピア リンクと呼ばれる特殊な EtherChannel で接続されている一対のデバイスの 1 つ。
- **vPC ピア リンク** : vPC ピア デバイス間の状態を同期するために使用されるリンク。
- **vPC メンバ ポート** : vPC に属するインターフェイス。
- **ホスト vPC ポート** : vPC に属する ファブリック エクステンダ 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 内にあってダウンストリーム デバイスに接続されているすべてのポートチャネルが含まれます。また、このドメインは、vPC グローバルパラメータを割り当てるために使用する必要があるコンフィギュレーション モードに関連付けられています。vPC ドメイン ID は両方のスイッチで同じである必要があります。
- **vPC ピア キープアライブ リンク** : ピア キープアライブ リンクは、さまざまな vPC ピア Cisco Nexus 5000 シリーズ デバイスをモニタします。ピア キープアライブ リンクは、vPC ピア デバイス間での設定可能なキープアライブ メッセージの定期的な送信を行います。

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

ファブリック エクステンダの用語

Cisco Nexus 2000 シリーズ ファブリック エクステンダ に使用される用語は、次のとおりです。

- **ファブリック インターフェイス**：ファブリック エクステンダ から親スイッチへの接続専用の 10 ギガビットイーサネット アップリンク ポート。ファブリック インターフェイスは他の目的には使用できません。親スイッチに直接接続する必要があります。
- **EtherChannel ファブリック インターフェイス**：ファブリック エクステンダ から親スイッチへの EtherChannel アップリンク接続。この接続は、単一論理チャネルにバンドルされているファブリック インターフェイスで構成されます。
- **ホスト インターフェイス**：サーバまたはホスト接続用のイーサネット インターフェイス。これらのポートは、ファブリック エクステンダのモデルに応じて、1 ギガビットイーサネット インターフェイスまたは 10 ギガビットイーサネット インターフェイスです。
- **EtherChannel ホスト インターフェイス**：ファブリック エクステンダ ホスト インターフェイスからのサーバポートへの EtherChannel ダウンリンク接続。



(注) リリース 4.1(3)N1(1) では、EtherChannel ホスト インターフェイスは 1 つのホスト インターフェイスだけで構成され、リンク アグリゲーション制御プロトコル (LACP) または非 LACP EtherChannel に設定できます。

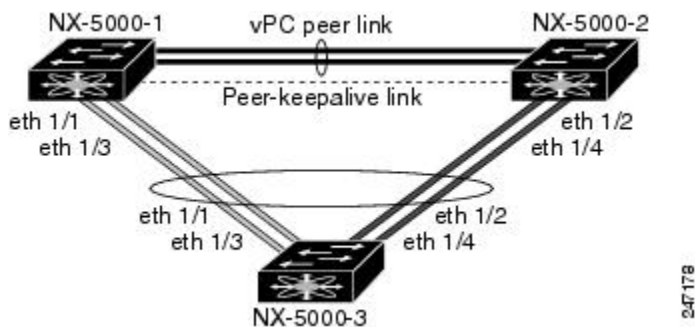
サポートされている vPC トポロジ

Cisco Nexus 5000 シリーズ スイッチ vPC トポロジ

vPC の Cisco Nexus 5000 シリーズ スイッチまたは Cisco Nexus 5500 シリーズ スイッチのペアを別のスイッチまたはサーバに直接接続できます。vPC ピアスイッチが同じタイプである必要があります。たとえば、vPC トポロジでは Nexus 5000 シリーズ スイッチのペアまたは Nexus 5500 シリーズ スイッチのペアを接続できますが、Nexus 5500 シリーズ スイッチに Nexus 5000 シリーズ スイッチを接続できません。最大 8 台のインターフェイスを各 Cisco Nexus 5000 シリーズ スイッチに接続でき、vPC のペアにバンドルされる 16 台のインターフェイスを提供できます。次の図に示す

トポロジでは、デュアル接続されたスイッチまたはサーバに 10 ギガビットまたは 1 ギガビットイーサネットアップリンクインターフェイスの vPC 機能を提供します。

図 6：スイッチ間 vPC トポロジ



(注) Cisco Nexus 5010 スイッチの最初の 8 個のポートおよび Cisco Nexus 5020 スイッチの最初の 16 個のポートは、スイッチ可能な 1 ギガビットポートと 10 ギガビットポートです。1 ギガビットモードで、これらのポート上で vPC 機能をイネーブルにできます。

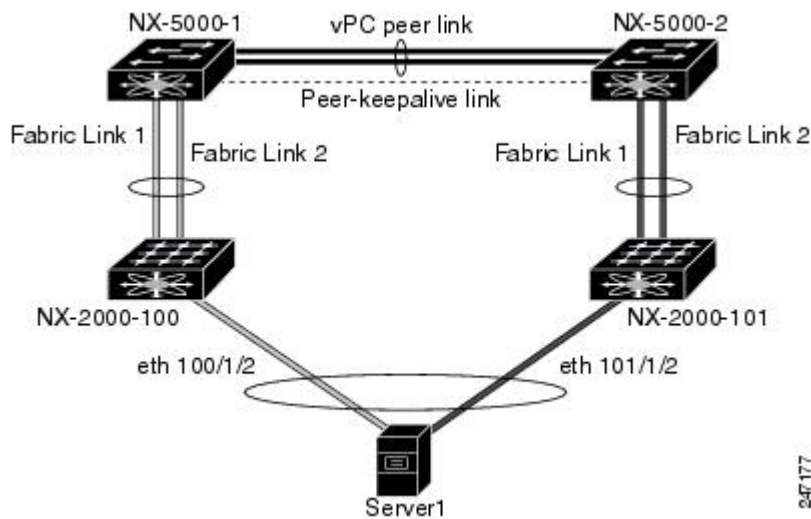
Cisco Nexus 5000 シリーズスイッチのペアに接続されたスイッチは、任意の標準ベースのイーサネットスイッチです。この設定を使用する共通環境には、Cisco Nexus 5000 シリーズスイッチのペアに接続されているデュアルスイッチを使用するブレードシャーシが含まれます。これは、vPC または Unified Computing System を介して Cisco Nexus 5000 シリーズスイッチのペアに接続されます。

シングルホーム接続ファブリック エクステンダ vPC トポロジ

次に示すように、Cisco Nexus 5000 シリーズスイッチに接続された Cisco Nexus 2000 シリーズファブリック エクステンダのペアに対して vPC で設定されたデュアルまたはクワッド以上のネットワークアダプタでサーバを接続できます。FEX モデルによっては、各ファブリック エクステンダに 1 つ以上のネットワークアダプタインターフェイスを接続できる場合があります。たとえば、図 10 に、サーバに各ファブリック エクステンダへのリンクが 1 つだけある、Cisco Nexus 2148T ファブリック エクステンダで構築されたトポロジを示します。Cisco Nexus 2248TP または Cisco Nexus 2232PP ファブリック エクステンダを含むトポロジは、サーバから単一のファブリック エクステンダへのより多くのリンクから構成できます。

次の図に示すトポロジでは、1 ギガビットイーサネットアップリンク インターフェイスを使用するデュアルホーム接続されたサーバに vPC 機能を提供します。

図 7: シングルホーム接続ファブリック エクステンダ vPC トポロジ



Cisco Nexus 5000 シリーズ スイッチはこのトポロジでシングルホーム接続のファブリック エクステンダの設定を最大 12 まで (576 ポート) サポートできます。しかし、デュアルホーム接続のホスト サーバは、この設定で vPC 内に 480 576 台だけ設定できます。



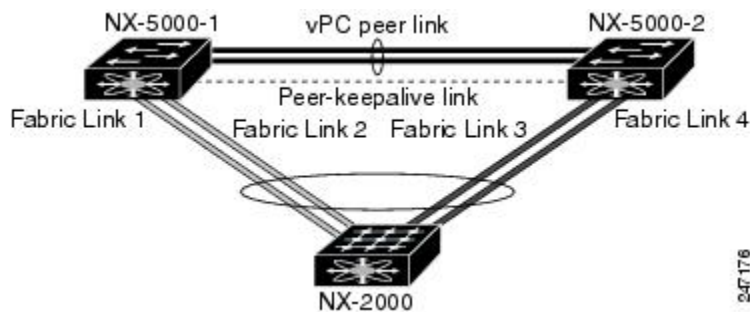
(注) Cisco Nexus 2148T ファブリック エクステンダでは、そのホストインターフェイスの EtherChannel はサポートされません。このため、各リンクが別のファブリック エクステンダに接続されたサーバからの EtherChannel では、最大 2 つのリンクが設定できます。

デュアルホーム接続ファブリック エクステンダ vPC トポロジ

Cisco Nexus 2000 シリーズ ファブリック エクステンダを 2 つのアップストリーム Cisco Nexus 5000 シリーズ スイッチおよび多数のシングルホーム接続サーバのダウンストリームに接続できます。

次の図に示すトポロジでは、1 ギガビットイーサネットアップリンクインターフェイスを使用する単一接続されたサーバに vPC 機能を提供します。

図 8：デュアルホーム接続 ファブリック エクステンダ vPC トポロジ



Cisco Nexus 5000 シリーズスイッチは、このトポロジでデュアルホーム接続の ファブリック エクステンダ を最大 12 までサポートできます。最大 576 のシングルホーム接続サーバがこの設定に接続できます。

vPC ドメイン

vPC ドメインを作成するには、まず各 vPC ピア スイッチ上で、1 ～ 1000 の値を使用して vPC ドメイン ID を作成しなければなりません。この ID は、一連の vPC ピア デバイス上で同じである必要があります。

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

vPC ピア スイッチは、設定された vPC ドメイン ID を使用して、一意の vPC システム MAC アドレスを自動的に割り当てます。各 vPC ドメインが、特定の vPC 関連操作に一意の ID として使用される一意の MAC アドレスを持ちます。ただし、スイッチは vPC システム MAC アドレスを LACP などのリンクスコープでの操作にだけ使用します。連続したネットワーク内の各 vPC ドメインを、一意のドメイン ID で作成することを推奨します。Cisco NX-OS ソフトウェアにアドレスを割り当てさせるのではなく、vPC ドメインに特定の MAC アドレスを設定することもできます。

vPC ピア スイッチは、設定された vPC ドメイン ID を使用して、一意の vPC システム MAC アドレスを自動的に割り当てます。スイッチは LACP または BPDU など、リンクスコープ操作のためだけに vPC システム MAC アドレスを使用します。vPC ドメインに特定の MAC アドレスを設定することもできます。

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

vPC ドメインを作成した後は、Cisco NX-OS ソフトウェアによって vPC ドメインのシステムプライオリティが作成されます。vPC ドメインに特定のシステムプライオリティを手動で設定することもできます。



- (注) システム プライオリティを手動で設定する場合は、必ず両方の vPC ピア スイッチ上で同じプライオリティ値を割り当てる必要があります。vPC ピア スイッチ同士が異なるシステム プライオリティ値を持っていると、vPC は稼働しません。

ピアキープアライブリンクとメッセージ

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

片方の vPC ピアスイッチに障害が発生したら、vPC ピアリンクの他方の側にある vPC ピアスイッチは、ピアキープアライブメッセージを受信しないことによってその障害を感知します。vPC ピアキープアライブメッセージのデフォルトの時間間隔は 1 秒です。間隔には 400 ミリ秒～10 秒を設定できます。タイムアウト値は、3～20 秒の範囲内で設定可能で、デフォルトのタイムアウト値は 5 秒です。ピアキープアライブのステータスは、ピアリンクがダウンした場合にだけチェックされます。

vPC ピアキープアライブは、Cisco Nexus 5000 シリーズ スイッチ上で管理 VRF またはデフォルト VRF で伝送できます。管理 VRF を使用するようにスイッチを設定するとき、キープアライブメッセージの送信元および宛先は、mgmt 0 インターフェイス IP アドレスです。デフォルト VRF を使用するようにスイッチを設定するとき、vPC ピアキープアライブメッセージの送信元アドレスおよび宛先アドレスとして機能するように SVI を作成する必要があります。ピアキープアライブメッセージに使用される送信元 IP アドレスと宛先 IP アドレスの両方が、ネットワーク上で一意であり、それらの IP アドレスがその vPC ピアキープアライブリンクに関連付けられている VRF から到達できることを確認します。



- (注) mgmt 0 インターフェイスを使用して管理 VRF で動作するように、Cisco Nexus 5000 シリーズ スイッチで vPC ピアキープアライブリンクを設定することを推奨します。デフォルト VRF を設定するときは、vPC ピアキープアライブメッセージを伝送するために vPC ピアリンクが使用されていないことを確認してください。

vPC ピアリンクの互換パラメータ

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

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

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

同じでなければならない設定パラメータ

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



(注) vPC 内のすべてのインターフェイスで、ここに示す動作パラメータおよび設定パラメータの値が同じになっていることを確認してください。

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

vPC インターフェイスのこれらのパラメータは、スイッチによって自動的に互換性がチェックされます。インターフェイスごとのパラメータは、インターフェイスごとに一貫性を保っていなければならない、グローバルパラメータはグローバルに一貫性を保っていなければならない。

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

- ポート タイプ設定
- ループ ガード
- ルート ガード
- ファブリック エクステンダ vPC トポロジでは、前述のすべてのインターフェイス レベルのパラメータは、両方のスイッチからホストインターフェイスに同じように設定する必要があります。
- EtherChannel ファブリック インターフェイスで設定された ファブリック エクステンダ FEX 番号で、ファブリック エクステンダ vPC トポロジ用です。

これらのパラメータのいずれかがイネーブルになっていなかったり、片方のスイッチでしか定義されていないと、vPC の整合性検査ではそのパラメータは無視されます。



(注) どの vPC インターフェイスもサスペンドモードになっていないことを確認するには、**show vpc brief** コマンドおよび **show vpc consistency-parameters** コマンドを入力して、syslog メッセージをチェックします。

同じにすべき設定パラメータ

次に挙げるパラメータのすべてが両方の vPC ピア スイッチ上で同じように設定されていないと、誤設定が原因でトラフィック フローに望ましくない動作が発生する可能性があります。

- MAC エージング タイマー
- スタティック MAC エントリ
- VLAN インターフェイス：vPC ピア リンク エンドにある各スイッチの VLAN インターフェイスが両エンドで同じ VLAN 用に設定されていなければならず、さらに同じ管理モードで同じ動作モードになっていなければなりません。ピア リンクの片方のスイッチだけで設定されている VLAN は、vPC またはピア リンクを使用してトラフィックを通過させることはしません。すべての VLAN をプライマリ vPC スイッチとセカンダリ vPC スイッチの両方で作成する必要があります。そうしないと、VLAN は停止します。
- プライベート VLAN 設定
- ACL のすべての設定とパラメータ
- Quality of Service (QoS) の設定とパラメータ：ローカル パラメータ、グローバル パラメータは同じでなければなりません
- STP インターフェイス設定：
 - BPDU フィルタ
 - BPDU ガード
 - コスト

- リンク タイプ
- プライオリティ
- VLAN (Rapid PVST+)

すべての設定パラメータで互換性が取れていることを確認するために、vPCの設定が終わったら、各 vPC ピア スイッチの設定を表示してみることを推奨します。

グレースフルタイプ1チェック

Cisco NX-OS Release 5.0(2)N2(1) 以降、整合性検査に失敗するとセカンダリ vPC スイッチでだけ vPC はダウンします。VLAN はプライマリ スイッチでアップのまま、タイプ 1 の設定は、トラフィックの中断なしで実行できます。この機能は、グローバルな、またインターフェイス固有のタイプ 1 不整合の場合の両方で使用されます。

この機能は、デュアルアクティブ FEX ポートではイネーブルになりません。タイプ 1 の不一致が発生した場合、VLAN は両方のスイッチのこれらのポートで中断されます。

VLAN ごとの整合性検査

Cisco NX-OS Release 5.0(2)N2(1) 以降、一部のタイプ 1 整合性検査は、スパンニングツリーが VLAN でイネーブルまたはディセーブルにされるときに VLAN ごとに行われます。整合性検査に合格しない VLAN は、プライマリ スイッチおよびセカンダリ スイッチの両方でダウンにされますが、その他の VLAN は影響を受けません。

vPC 自動リカバリ

Cisco NX-OS Release 5.0(2)N2(1) 以降、vPC 自動リカバリ機能は、次のシナリオの vPC リンクを再びイネーブルにします。

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

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

vPC 自動リカバリ機能は、デフォルトでディセーブルです。

vPC ピア リンク

vPC ピア リンクは、vPC ピア デバイス間の状態を同期するために使用されるリンクです。



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

vPC ピア リンクの概要

vPC ピアとして持てるのは 2 台のスイッチだけです。各スイッチが、他方の 1 つの vPC ピアに対してだけ vPC ピアとして機能します。vPC ピア スイッチは、他のスイッチに対する非 vPC リンクも持つことができます。

有効な設定を作成するには、各スイッチで EtherChannel を設定してから、vPC ドメインを設定します。ピア リンクとして、各スイッチの EtherChannel を割り当てます。vPC ピア リンクのインターフェイスのいずれかに障害が発生した場合に、スイッチが自動的にピア リンク内の他方のインターフェイスを使用するようにフォールバックするため、冗長性のために少なくとも 2 つの専用ポートを EtherChannel に設定することを推奨します。



- (注) トランク モードの EtherChannel を設定することを推奨します。

多くの動作パラメータおよび設定パラメータが、vPC ピア リンクによって接続されている各スイッチで同じでなければなりません。各スイッチが管理プレーンから完全に独立しているため、スイッチが重要なパラメータについて互換性があることを管理者が確認する必要があります。vPC ピア スイッチは、独立したコントロールプレーンを持っています。vPC ピア リンクを設定し終えたら、各 vPC ピア スイッチの設定を表示して、設定に互換性があることを確認します。



- (注) vPC ピア リンクによって接続されている 2 つのスイッチが、特定の同じ動作パラメータおよび設定パラメータを持っていることを確認する必要があります。

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

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

vPC リンクに学習された MAC アドレスは、ピア間でも同期されます。

設定情報は、Cisco Fabric Services over Ethernet (CFS over E) プロトコルを使用して vPC ピア リンク間を流れます。両方のスイッチ上で設定されているこれらの VLAN の MAC アドレスはすべて、vPC ピア スイッチ間で同期されています。この同期に、CFS over E が使用されます。

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

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

vPC ピア スイッチ間の設定可能なキーブアライブ メッセージの送信には、別のリンク (vPC ピア キーブアライブリンク) を使用します。vPC ピア キーブアライブリンク上のキーブアライブメッセージから、障害が vPC ピア リンク上でだけ発生したのか、vPC ピア スイッチ上で発生したのかわかります。キーブアライブ メッセージは、ピア リンク内のすべてのリンクで障害が発生した場合にだけ使用されます。

vPC 番号

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

各 vPC ピア スイッチでは、ダウンストリーム スイッチに接続する EtherChannel に同じ vPC 番号を割り当てます。vPC の作成時にトラフィックが中断されることはほとんどありません。設定を簡素化するために、各 EtherChannel に対して EtherChannel 自体と同じである vPC ID 番号を割り当てられます (つまり、EtherChannel 10 に対して vPC ID 10)。



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

その他の機能との vPC の相互作用

vPC と LACP

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

ダウンストリーム スイッチからのチャネルも含めて、すべての vPC EtherChannel 上の LACP を使用できます。LACP は、vPC ピア スイッチの各 EtherChannel 上のインターフェイスのアクティブ モードで設定することを推奨します。この設定により、スイッチ、単一方向リンク、およびマル

チホップ接続の間の互換性をより簡単に検出できるようになり、実行時の変更およびリンク障害に対してダイナミックな応答が可能になります。

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



- (注) システム プライオリティを手動で設定する場合は、必ず両方の vPC ピア スイッチ上で同じプライオリティ値を割り当てる必要があります。vPC ピア スイッチ同士が異なるシステム プライオリティ値を持っていると、vPC は稼働しません。

vPC ピア リンクと STP

最初に vPC 機能を起動したときに、STP が再収束します。STP は、vPC ピア リンクを特殊なリンクとして扱い、常に vPC ピア リンクを STP のアクティブ トポロジに含めます。

すべての vPC ピア リンク インターフェイスを STP ネットワーク ポートタイプに設定して、すべての vPC リンク上で Bridge Assurance が自動的にイネーブルになるようにすることを推奨します。また、vPC ピア リンク上では STP 拡張機能を一切イネーブルにしないことも推奨します。

パラメータのリストは、vPC ピア リンクの両サイドの vPC ピア スイッチ上で同じになるように設定する必要があります。

STP は分散しています。つまり、このプロトコルは、両方の vPC ピア スイッチ上で実行され続けます。ただし、プライマリ スイッチとして選択されている vPC ピア スイッチ上での設定が、セカンダリ vPC ピア スイッチ上の vPC インターフェイスの STP プロセスを制御します。

プライマリ vPC スイッチは、Cisco Fabric Services over Ethernet (CFS over E) を使用して、vPC セカンダリ ピア スイッチ上の STP の状態を同期させます。

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

ブリッジプロトコルデータユニット (BPDU) は、指定ブリッジ ID フィールドで、STP ブリッジ ID の vPC に設定されている MAC アドレスを使用します。vPC プライマリ スイッチが、vPC インターフェイス上でこれらの BPDU を送信します。



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

vPC と ARP

vPC ピア全体でのテーブルの同期は、Cisco Fabric Services over Ethernet (CFS over E) プロトコルの信頼性の高い転送メカニズムを使用して、Cisco NX-OS で管理されます。vPC ピア間でアドレステーブルのより高速なコンバージェンスをサポートするには、**ip arp synchronize** コマンドをイネー

ブルにする必要があります。このコンバージェンスは、ピア リンク ポート チャネルがフラップしたとき、またはvPCピアがオンラインに戻ったときのARPテーブルの復元に関連する遅延を回避することを目的にしています。

パフォーマンスを向上するためにARP同期機能をオンにすることを推奨します。デフォルトではイネーブルに設定されていません。

ARP 同期がイネーブルかどうかを確認するには、次のコマンドを入力します。

```
switch# show running
```

ARP 同期をイネーブルにするには、次のコマンドを入力します。

```
switch(config-vpc-domain) # ip arp synchronize
```

CFSSoE

Cisco Fabric Services over Ethernet (CFSSoE) は、vPC ピア デバイスのアクションを同期化するために使用する信頼性の高い状態転送メカニズムです。CFSSoE 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/CFSSoE プロトコル データ ユニット (PDU) に入れて伝送されます。

CFSSoE 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 CFSSoE 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。CFSSoE 機能が vPC 上で正常に機能するために必要な設定は一切ありません。

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



(注) **no cfs eth distribute** コマンドまたは **no cfs distribute** コマンドを入力しないでください。CFSSoE は、vPC機能に対してイネーブルにする必要があります。vPCをイネーブルにしてこれらのコマンドのいずれかを入力すると、エラー メッセージがシステムによって表示されます。

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

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するパフォーマンス上の問題に対処します。この機能により、一対の Cisco Nexus 5000 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 リンクに障害が発生すると、北南のトラフィックに影響はありませんが、東西のトラフィックが失われます (ブラックホール化されます)。

STP 拡張機能および Rapid PVST+ については、『Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。

vPC の注意事項および制約事項

vPC には、次の注意事項と制約事項があります。

- vPC ピア リンクおよび vPC インターフェイスを設定する前に、vPC 機能をイネーブルにする必要があります。
- システムが vPC ピア リンクを形成するには、その前にピア キープアライブ リンクを設定する必要があります。
- vPC ピア リンクは、少なくとも 2 台の 10 ギガビット イーサネット インターフェイスを使用して形成する必要があります。
- vPC の Cisco Nexus 5000 シリーズ スイッチのペアまたは Cisco Nexus 5500 シリーズ スイッチのペアを別のスイッチまたはサーバに直接接続できます。vPC ピア スイッチが同じタイプである必要があります。たとえば、vPC トポロジでは Nexus 5000 シリーズ スイッチのペアまたは Nexus 5500 シリーズ スイッチのペアを接続できますが、Nexus 5500 シリーズ スイッチに Nexus 5000 シリーズ スイッチを接続できません。
- vPC に入れられるのは、ポートチャネルだけです。通常のポートチャネル (スイッチ間 vPC トポロジ)、ポートチャネル ファブリック インターフェイス (ファブリック エクステンダ vPC トポロジ)、およびポートチャネル ホスト インターフェイス (ホスト インターフェイス vPC トポロジ) で vPC を設定できます。
- ファブリック エクステンダ はホスト インターフェイス vPC トポロジまたはファブリック エクステンダ vPC トポロジのメンバになれますが、両方で同時にはなれません。
- 両方の vPC ピア スイッチを設定する必要があります。設定は、vPC ピア デバイス間で自動的に同期されません。
- 必要な設定パラメータが、vPC ピア リンクの両側で互換性を保っているかチェックしてください。
- vPC の設定中に、最小限のトラフィックの中断が発生する可能性があります。

- アクティブ モードのインターフェイスで LACP を使用して vPC のすべてのポート チャネルを設定する必要があります。
- **peer-switch** コマンドが設定されており、vPC キープアライブメッセージが管理インターフェイスではなく SVI 経由で交換された場合は、追加のスパニングツリー プロトコル (STP) の設定が必要です。vPC ピア間のキープアライブ トラフィックを伝送する専用リンクで STP をディセーブルにする必要があります。専用リンクの両端で STP BPDUfilter を設定することによって、専用リンクで STP をディセーブルにできます。vPC キープアライブ SVI の VLAN を相互接続専用リンクでのみ許可し、その他のすべてのリンク (ピアリンクを含む) では禁止することを推奨します。

vPC の設定

vPC のイネーブル化

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# feature vpc	スイッチで vPC をイネーブルにします。
ステップ 3	switch# show feature	(任意) スイッチ上でイネーブルになっている機能を表示します。
ステップ 4	switch# 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
```

vPC のディセーブル化

vPC 機能をディセーブルにできます。



(注) vPC 機能をディセーブルにすると、Cisco Nexus 5000 シリーズ スイッチがすべての vPC 設定をクリアします。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# no feature vpc	スイッチの vPC をディセーブルにします。
ステップ 3	switch# show feature	(任意) スイッチ上でイネーブルになっている機能を表示します。
ステップ 4	switch# 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
```

vPC ドメインの作成

両方の vPC ピア デバイスで、同じ vPC ドメイン ID を作成する必要があります。このドメイン ID は、vPC システム MAC アドレスを自動的に形成するために使用されます。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# vpc domain domain-id	スイッチで 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。デフォルト domain-id はありません。範囲は 1 ～ 1000 です。

	コマンドまたはアクション	目的
		(注) 既存の vPC ドメインの vpc-domain コンフィギュレーション モードを開始するには、 vpc domain コマンドも使用できます。
ステップ 3	switch# show vpc brief	(任意) 各 vPC ドメインに関する要約情報を表示します。
ステップ 4	switch# 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
```

vPC キープアライブリンクと vPC キープアライブメッセージの設定

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

Cisco NX-OS Release 5.0(3)N1(1) 以降、Cisco Nexus 5500 プラットフォーム スイッチは、レイヤ 3 モジュールを使用する VRF Lite で、基本または LAN-Enterprise ライセンスがインストールされた VRF Lite をサポートします。この機能により、VRF を作成し、VRF に特定のインターフェイスを割り当てることができます。このリリースよりも前は、VRF 管理と VRF デフォルトの 2 つの VRF がデフォルトで作成されます。mgmt0 インターフェイスとすべての SVI インターフェイスが VRF の管理と VRF デフォルトに存在します。

Cisco NX-OS ソフトウェアは、vPC ピア間でピアキープアライブリンクを使用して、設定可能なキープアライブメッセージを定期的送信します。これらのメッセージを送信するには、ピアデバイス間にレイヤ 3 接続が必要です。ピアキープアライブリンクが起動および動作していないと、システムは vPC ピアリンクを開始できません。

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



- (注) vPC ピアキープアライブリンクを使用する際は、個別の VRF インスタンスを設定して、各 vPC ピアスイッチからその VRF にレイヤ 3 ポートを接続することを推奨します。ピアリンク自体を使用して vPC ピアキープアライブメッセージを送信しないでください。VRF の作成と設定については、『Cisco Nexus 5000 Series NX-OS Unicast Routing Configuration Guide, Release 5.0(3)N1(1)』を参照してください。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

システムで vPC ピアリンクを形成できるようにするには、まず vPC ピアキープアライブリンクを設定する必要があります。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# vpc domain <i>domain-id</i>	スイッチの vPC ドメインがまだない場合は作成し、 vpc-domain コンフィギュレーションモードを開始します。
ステップ 3	switch(config-vpc-domain)# peer-keepalive destination <i>ipaddress</i> [hold-timeout <i>secs</i> interval <i>msecs</i> { timeout <i>secs</i> } precedence { <i>prec-value</i> network internet critical flash-override flash immediate priority routine } tos { <i>tos-value</i> max-reliability max-throughput min-delay min-monetary-cost normal } tos-byte <i>tos-byte-value</i> } source <i>ipaddress</i> vrf { <i>name</i> management vpc-keepalive }]	vPC ピアキープアライブリンクのリモートエンドの IPv4 アドレスを設定します。 (注) vPC ピアキープアライブリンクを設定するまでは、vPC ピアリンクはシステムによって形成されません。 管理ポートと VRF がデフォルトです。
ステップ 4	switch(config-vpc-domain)# vpc peer-keepalive destination <i>ipaddress</i> source <i>ipaddress</i>	(任意) vPC ピアキープアライブリンクを使用する際は、個別の VRF インスタンスを設定して、各 vPC ピアデバイスからその VRF にレイヤ 3 ポートを接続します。
ステップ 5	switch# show vpc peer-keepalive	(任意) キープアライブメッセージのコンフィギュレーションに関する情報を表示します。
ステップ 6	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 ピアキープアライブリンクの宛先 IP アドレスを設定する例を示します。

```
switch# configure terminal
```

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

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

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

次に、vPC キープアライブ リンクに vpc_keepalive という名前の別の VRF を作成し、その新しい VRF を確認する例を示します。

次に、vPC キープアライブ リンクに vpc_keepalive という名前の別の VRF を作成し、その新しい VRF を確認する例を示します。

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

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

```
vPC keep-alive status          : peer is alive
--Peer is alive for           : (154477) seconds, (908) msec
--Send status                 : Success
--Last send at                : 2011.01.14 19:02:50 100 ms
--Sent on interface           : Vlan123
--Receive status              : Success
--Last receive at             : 2011.01.14 19:02:50 103 ms
--Received on interface       : Vlan123
--Last update from peer       : (0) seconds, (524) msec
```

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

The services provided by the switch , such as ping, ssh, telnet, radius, are VRF aware. The VRF name need to be configured or specified in order for the correct routing table to be used.

```
L3-NEXUS-2# ping 123.1.1.1 vrf vpc_keepalive
PING 123.1.1.1 (123.1.1.1): 56 data bytes
64 bytes from 123.1.1.1: icmp_seq=0 ttl=254 time=3.234 ms
64 bytes from 123.1.1.1: icmp_seq=1 ttl=254 time=4.931 ms
64 bytes from 123.1.1.1: icmp_seq=2 ttl=254 time=4.965 ms
64 bytes from 123.1.1.1: icmp_seq=3 ttl=254 time=4.971 ms
64 bytes from 123.1.1.1: icmp_seq=4 ttl=254 time=4.915 ms
```

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

vPC ピア リンクの作成

vPC ピア リンクを作成するには、指定した vPC ドメインのピア リンクとする EtherChannel を各スイッチ上で指定します。冗長性を確保するため、トランク モードで vPC ピア リンクとして指定する EtherChannel を設定し、各 vPC ピア スイッチで個別のモジュールの 2 つのポートを使用することを推奨します。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface port-channel channel-number	このスイッチの vPC ピア リンクとして使用する EtherChannel を選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# vpc peer-link	選択した EtherChannel を vPC ピア リンクとして設定し、vpc-domain コンフィギュレーション モードを開始します。
ステップ 4	switch# show vpc brief	(任意) vPC ピア リンクに関する情報など、各 vPC の情報を表示します。
ステップ 5	switch# 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)# vpc peer-link
```

設定の互換性チェック

両方の vPC ピア スイッチ上の vPC ピア リンクを設定した後に、すべての vPC インターフェイスで設定が一貫していることをチェックします。



(注) Cisco NX-OS Release 5.0(2)N1(1) 以降、次のQoS パラメータはタイプ 2 整合性検査をサポートします。

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

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

パラメータ	デフォルト設定
switch# show vpc consistency-parameters {global interface port-channel channel-number}	すべての vPC インターフェイス全体で一貫している必要があるパラメータのステータスを表示します。

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

```
switch# show vpc consistency-parameters global
```

Legend:

Type 1 : vPC will be suspended in case of mismatch

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

次に、必要な設定が EtherChannel インターフェイスと互換性があることをチェックする例を示します。

```
switch# show vpc consistency-parameters interface port-channel 20
```

Legend:
Type 1 : vPC will be suspended in case of mismatch

Name	Type	Local Value	Peer Value
-----	----	-----	-----
Fex id	1	20	20
STP Port Type	1	Default	Default
STP Port Guard	1	None	None
STP MST Simulate PVST	1	Default	Default
mode	1	on	on
Speed	1	10 Gb/s	10 Gb/s
Duplex	1	full	full
Port Mode	1	fex-fabric	fex-fabric
Shut Lan	1	No	No
Allowed VLANs	-	1,3-3967,4048-4093	1-3967,4048-4093

vPC 自動リカバリのイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# vpc domain domain-id	既存の vPC ドメインの vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	switch(config-vpc-domain)# auto-recovery reload-delay delay	自動リカバリ機能をイネーブルにし、リロード遅延期間を設定します。デフォルトはディセーブルです。

次に、vPC ドメイン 10 の自動リカバリ機能をイネーブルにし、240 秒の遅延期間を設定する例を示します。

```
switch(config)# vpc domain 10
switch(config-vpc-domain)# auto-recovery reload-delay 240
Warning:
  Enables restoring of vPCs in a peer-detached state after reload, will wait for 240 seconds
  (by default) to determine if peer is un-reachable
```

次に、vPC ドメイン 10 の自動リカバリ機能のステータスを表示する例を示します。

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

version 5.0(2)N2(1)

feature vpc
vpc domain 10
  peer-keepalive destination 10.193.51.170
  auto-recovery
```

vPC トポロジのセカンダリスイッチの孤立ポートの一時停止

vPC セカンダリ ピア リンクがダウンするときに、非仮想ポートチャネル（vPC）ポートを一時停止できます。孤立ポートとも呼ばれる非 vPC ポートは、vPC の一部ではないポートです。



(注) ポートが孤立ポートとして設定されると、そのポートはフラップします。これは、孤立ポートの制約を考慮して、そのポートをアップにできるかどうかをシステムが再評価するために発生します。たとえば、MCTはアップにする必要があるため、選択を完了する必要があります。

はじめる前に

vPC 機能をイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# interface ethernet slot/port	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# vpc orphan-port suspend	セカンダリスイッチがダウンすると、指定したポートは一時停止されます。 (注) vpc-orphan-port suspend コマンドは、物理ポート上でのみサポートされます。
ステップ 4	switch(config-if)# exit	インターフェイス コンフィギュレーション モードを終了します。
ステップ 5	switch# show vpc orphan-port	(任意) 孤立ポート設定を表示します。
ステップ 6	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、孤立ポートを一時停止する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/0
switch(config-if)# vpc orphan-port suspend
```

次に、vPC の一部ではないが、vPC の一部であるポートと同じ VLAN を共有するポートを表示する例を示します。

```
switch# configure terminal
switch(config)# show vpc orphan-ports
Note:
-----::Going through port database. Please be patient.::-----
VLAN Orphan Ports
-----
1 Po600
2 Po600
3 Po600
4 Po600
5 Po600
6 Po600
7 Po600
8 Po600
9 Po600
10 Po600
11 Po600
12 Po600
13 Po600
14 Po600
...
```

EtherChannel ホスト インターフェイスの作成

Cisco Nexus 2000 シリーズ ファブリック エクステンダからダウンストリーム サーバに接続するには、EtherChannel ホスト インターフェイスを作成します。EtherChannel ホスト インターフェイスは、ファブリック エクステンダ モデルによってはメンバとして 1 つのホスト インターフェイスだけを保持できます。Cisco Nexus 2148T では、ファブリック エクステンダごとに 1 つのインターフェイスメンバだけが許可され、より新しいファブリック エクステンダでは、単一のファブリック エクステンダ上で同じポートチャネルの最大 8 のメンバが許可されています。EtherChannel ホスト インターフェイスを作成して、ファブリック エクステンダ トポロジを使用するその上に vPC を設定する必要があります。

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。

接続されている ファブリック エクステンダ がオンラインであることを確認します。

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

手順

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

	コマンドまたはアクション	目的
ステップ 3	switch(config-if)# channel-group <i>channel-number</i> mode { active passive on }	選択されたホスト インターフェイスの EtherChannel ホスト インターフェイスを作成します。
ステップ 4	switch# show port-channel summary	(任意) 各 EtherChannel ホスト インターフェイスに関する情報を表示します。
ステップ 5	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、EtherChannel ホスト 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 101/1/20
switch(config-if)# channel-group 7 mode active
```

他のポートチャネルの vPC への移行

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# interface port-channel <i>channel-number</i>	ダウンストリームスイッチに接続するために vPC に入れるポートチャネルを選択し、インターフェイス コンフィギュレーション モードを開始します。 (注) 通常のポートチャネル（物理的な vPC トポロジ）、ポートチャネルファブリック インターフェイス（ファブリック エクステンダ vPC トポロジ）、およびポートチャネルホスト インターフェイス（ホスト インターフェイス vPC トポロジ）で vPC を設定できます。

	コマンドまたはアクション	目的
ステップ 3	switch(config-if)# vpc number	選択したポートチャネルを vPC に入れてダウンストリームスイッチに接続するように設定します。指定できる範囲は 1 ～ 4096 です。 vPC ピアスイッチからダウンストリームスイッチに接続されているポートチャネルに割り当てる vPC <i>number</i> は、両方の vPC ピアスイッチで同一である必要があります。
ステップ 4	switch# show vpc brief	(任意) 各 vPC に関する情報を表示します。
ステップ 5	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、ダウンストリームデバイスに接続されるポートチャネルを設定する方法を示します。

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

vPC ドメイン MAC アドレスの手動での設定



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

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# vpc domain domain-id	スイッチの既存の vPC ドメインを選択するか、新しい vPC ドメインを作成し、vpc-domain コンフィギュレーションモードを開始します。デフォ

	コマンドまたはアクション	目的
		ルット <i>domain-id</i> はありません。範囲は 1 ～ 1000 です。
ステップ 3	switch(config-vpc-domain)# system-mac <i>mac-address</i>	指定した vPC ドメインに割り当てる MAC アドレスを <i>aaaa.bbbb.cccc</i> の形式で入力します。
ステップ 4	switch# show vpc role	(任意) vPC システム MAC アドレスを表示します。
ステップ 5	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 MAC アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-if)# system-mac 23fb.4ab5.4c4e
```

システムプライオリティの手動での設定

vPC ドメインを作成すると、vPC システムプライオリティが自動的に作成されます。ただし、vPC ドメインのシステムプライオリティは手動で設定することもできます。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# vpc domain <i>domain-id</i>	スイッチの既存の vPC ドメインを選択するか、新しい vPC ドメインを作成し、 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 <i>domain-id</i> はありません。範囲は 1 ～ 1000 です。
ステップ 3	switch(config-vpc-domain)# system-priority <i>priority</i>	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。

	コマンドまたはアクション	目的
ステップ 4	switch# show vpc brief	(任意) vPC ピア リンクに関する情報など、各 vPC の情報を表示します。
ステップ 5	switch# 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)# vpc domain 5
switch(config-if)# system-priority 4000
```

vPC ピア スイッチ ロールの手動での設定

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

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

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# vpc domain domain-id	スイッチの既存の vPC ドメインを選択するか、新しい vPC ドメインを作成し、vpc-domain コンフィギュレーション モードを開始します。デフォルト domain-id はありません。範囲は 1 ~ 1000 です。
ステップ 3	switch(config-vpc-domain)# role priority priority	vPC システム プライオリティに割り当てるロール プライオリティを入力します。指定できる値の範

	コマンドまたはアクション	目的
		囲は、1 ～ 65535 です。デフォルト値は 32667 です。
ステップ 4	switch# show vpc brief	(任意) vPC ピア リンクに関する情報など、各 vPC の情報を表示します。
ステップ 5	switch# 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)# vpc domain 5
switch(config-if)# role priority 4000
```

vPC ピア スイッチの設定

純粋な vPC ピア スイッチ トポロジの設定

純粋な vPC ピア スイッチ トポロジを設定するには、**peer-switch** コマンドを使用し、次に可能な範囲内で最高の（最も小さい）スパニングツリーブリッジプライオリティ値を設定します。



(注) スパニングツリープライオリティに適用する値は、両方の vPC ピアで同一である必要があります。

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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# vpc domain <i>domain-id</i>	設定する vPC ドメインの番号を入力します。 vpc-domain コンフィギュレーションモードを開始します。
ステップ 3	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	switch(config-vpc-domain)# spanning-tree vlan <i>vlan-range</i> priority <i>value</i>	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。 (注) この値は、両方の vPC ピアで同一である必要があります。
ステップ 5	switch(config-vpn-domain)# exit	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	switch(config)# 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。 コマンド出力で次の行を探します。 vPC peer-switch is enabled (operational)
ステップ 7	switch(config)# copy running-config startup-config	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

次の例は、純粋な vPC ピア スイッチ トポロジを設定する方法を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vpc domain 5
switch(config-vpc-domain)# peer-switch
2010 Apr 28 14:44:44 switch %STP-2-VPC_PEERSWITCH_CONFIG_ENABLED: vPC peer-switch
configuration is enabled. Please make sure to configure spanning tree "bridge" priority as

per recommended guidelines to make vPC peer-switch operational.
switch(config-vpc-domain)# exit
switch(config)# spanning-tree vlan 1 priority 8192
switch(config)# show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001-VLAN0050, VLAN0100-VLAN0149, VLAN0200-VLAN0249
VLAN0300-VLAN0349, VLAN0400-VLAN0599, VLAN0900-VLAN0999
Port Type Default is disable
Edge Port [PortFast] BPDU Guard Default is disabled
Edge Port [PortFast] BPDU Filter Default is disabled
Bridge Assurance is enabled
```

```

Loopguard Default                is disabled
Pathcost method used             is short
vPC peer-switch                 is enabled (operational)
Name                             Blocking Listening Learning Forwarding STP Active
-----
VLAN0001                        0          0          0          16          16
VLAN0002                        0          0          0          16          16
switch(config)# copy running-config startup-config
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（『Cisco Nexus 5000 Series NX-OS Layer 2 Switching Command Reference』を参照してください）を使用して STP VLAN ベースのロードバランシング基準を満たすように代表ブリッジ IC を変更した後、ルートブリッジ ID を最高のブリッジプライオリティよりもよい値に変更することにより、ハイブリッド vPC または非 vPC ピア スイッチ トポロジを設定することができます。次に、ピア スイッチをイネーブルにします。



(注)

以前にグローバル スパニングツリー パラメータを設定し、その後スパニングツリー疑似情報パラメータを設定した場合は、疑似情報パラメータがグローバル パラメータより優先されることに注意してください。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# spanning-tree pseudo-information	スパニングツリー疑似情報を設定します。 (注) この設定は、どのグローバル スパニングツリー設定よりも優先されます。
ステップ 3	switch(config-pseudo)# vlan vlan-id designated priority priority	VLAN の指定ブリッジプライオリティを設定します。有効な値は、0 ～ 61440 の範囲内の 4096 の倍数です。
ステップ 4	switch(config-pseudo)# vlan vlan-id root priority priority	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。 (注) ピア スイッチが動作するには、この値が両方の vPC ピアで同一である必要があります。

	コマンドまたはアクション	目的
ステップ 5	switch(config-pseudo)# exit	スパニングツリー疑似情報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	switch(config)# vpc domain domain-id	設定する vPC ドメインの番号を入力します。 vpc-domain コンフィギュレーションモードを開始します。
ステップ 7	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 8	switch(config-vpc-domain)# exit	vpc-domain コンフィギュレーションモードを終了します。
ステップ 9	switch(config)# 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。 コマンド出力で次の行を探します。 vPC peer-switch is enabled (operational)
ステップ 10	switch(config)# copy running-config startup-config	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

次の例は、ハイブリッド vPC ピア スイッチ トポロジを設定する方法を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# spanning-tree pseudo-information
switch(config-pseudo)# vlan 1 designated priority 8192
switch(config-pseudo)# vlan 1 root priority 4096
switch(config-pseudo)# exit
switch(config)# vpc domain 5
switch(config-vpc-domain)# peer-switch
switch(config-vpc-domain)# exit
switch(config)# copy running-config startup-config
```

vPC 設定の確認

vPC の設定情報を表示するには、次のコマンドを使用します。

コマンド	目的
switch# 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。
switch# show port-channel capacity	スイッチで設定されている EtherChannel の数、およびまだ使用可能なポートチャネル数を表示します。
switch# show running-config vpc	vPC の実行コンフィギュレーションの情報を表示します。
switch# show vpc brief	vPC に関する簡単な情報を表示します。
switch# show vpc consistency-parameters	すべての vPC インターフェイス全体で一貫している必要があるパラメータのステータスを表示します。
switch# show vpc peer-keepalive	ピアキープアライブメッセージの情報を表示します。
switch# show vpc role	ピアステータス、ローカルスイッチのロール、vPC システム MAC アドレスとシステムプライオリティ、およびローカル vPC スwitch の MAC アドレスとプライオリティを表示します。
switch# show vpc statistics	vPC に関する統計情報を表示します。 (注) このコマンドは、現在作業している vPC ピア デバイスの vPC 統計情報しか表示しません。

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

グレースフルタイプ1チェックステータスの表示

次に、グレースフルタイプ1整合性検査の現在のステータスを表示する例を示します。

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

vPC domain id           : 10
Peer status              : peer adjacency formed ok
vPC keep-alive status    : peer is alive
Configuration consistency status: success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role                 : secondary
```

```

Number of vPCs configured      : 34
Peer Gateway                   : Disabled
Dual-active excluded VLANs     : -
Graceful Consistency Check     : Enabled

```

vPC Peer-link status

id	Port	Status	Active vlans
1	Po1	up	1

グローバルタイプ1不整合の表示

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

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

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

Legend:

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

```

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

```

vPC Peer-link status

id	Port	Status	Active vlans
1	Po1	up	1-10

vPC status

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

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

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

Legend:

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

```

vPC domain id                  : 10
Peer status                    : peer adjacency formed ok
vPC keep-alive status          : peer is alive
Configuration consistency status: failed
Per-vlan consistency status    : success
Configuration consistency reason: vPC type-1 configuration incompatible - STP Mode inconsistent
Type-2 consistency status      : success
vPC role                       : primary
Number of vPCs configured      : 2

```

```

Peer Gateway                : Disabled
Dual-active excluded VLANs  : -
Graceful Consistency Check  : Enabled

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

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

```

インターフェイス固有のタイプ1不整合の表示

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

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

```

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

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

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

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

```

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

```

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

vPC domain id                : 10

```

```

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

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

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

```

VLAN ごとの整合ステータスの表示

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

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

```

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

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

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

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

```

no spanning-tree vlan 5 コマンドを入力すると、プライマリおよびセカンダリ VLAN で不整合が引き起こされます。

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


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

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

Legend:

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

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

vPC Peer-link status

id	Port	Status	Active vlans
1	Pol	up	1-4,6-10

vPC status

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

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

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

Legend:

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

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

vPC Peer-link status

id	Port	Status	Active vlans
1	Pol	up	1-4,6-10

vPC status

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

次に、STP Disabled としての不整合の例を示します。

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

Name	Type	Reason Code	Pass Vlans
STP Mode	1	success	0-4095

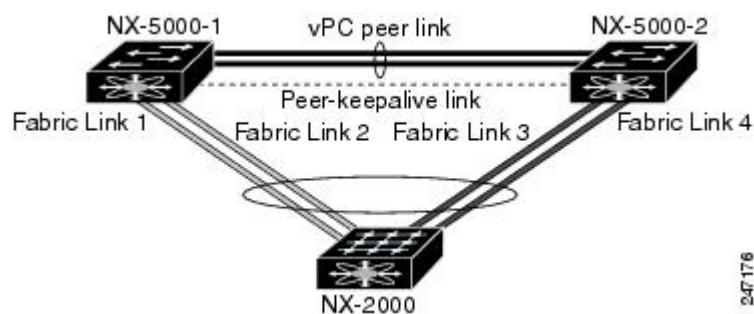
STP Disabled	1	vPC type-1 configuration incompatible - STP is enabled or disabled on some or all vlans	0-4, 6-4095
STP MST Region Name	1	success	0-4095
STP MST Region Revision	1	success	0-4095
STP MST Region Instance to VLAN Mapping	1	success	0-4095
STP Loopguard	1	success	0-4095
STP Bridge Assurance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

vPC の設定例

デュアルホーム接続ファブリック エクステンダ vPC の設定例

次に、次の図に示すように、NX-5000-1 スイッチのピアキープアライブ メッセージを伝送するために管理 VRF を使用するデュアルホーム接続 ファブリック エクステンダ vPC トポロジを設定する例を示します。

図 9 : vPC の設定例



はじめる前に

Cisco Nexus 2000 シリーズ ファブリック エクステンダ NX-2000-100 が接続され、オンラインであることを確認します。

手順

ステップ 1 vPC および LACP をイネーブルにします。

```
NX-5000-1# configure terminal
NX-5000-1(config)# feature lacp
NX-5000-1(config)# feature vpc
```

ステップ 2 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。

```
NX-5000-1(config)# vpc domain 1
NX-5000-1(config-vpc-domain)# peer-keepalive destination 10.10.10.237
NX-5000-1(config-vpc-domain)# exit
```

ステップ 3 2つのポートの EtherChannel として vPC ピア リンクを設定します。

```
NX-5000-1(config)# interface ethernet 1/1-2
NX-5000-1(config-if-range)# switchport mode trunk
NX-5000-1(config-if-range)# switchport trunk allowed vlan 20-50
NX-5000-1(config-if-range)# switchport trunk native vlan 20
NX-5000-1(config-if-range)# channel-group 20 mode active
NX-5000-1(config-if-range)# exit
NX-5000-1(config)# interface port-channel 20
NX-5000-1(config-if)# vpc peer-link
NX-5000-1(config-if)# exit
```

ステップ 4 ファブリック エクステンダ ID (たとえば、「100」) を作成します。

```
NX-5000-1(config)# fex 100
NX-5000-1(config-fex)# pinning max-links 1
NX-5000-1(fex)# exit
```

ステップ 5 ファブリック エクステンダ 100 のファブリック EtherChannel リンクを設定します。

```
NX-5000-1(config)# interface ethernet 1/20
NX-5000-1(config-if)# channel-group 100
NX-5000-1(config-if)# exit
NX-5000-1(config)# interface port-channel 100
NX-5000-1(config-if)# switchport mode fex-fabric
NX-5000-1(config-if)# vpc 100
NX-5000-1(config-if)# fex associate 100
NX-5000-1(config-if)# exit
```

ステップ 6 両方の Nexus 5000 シリーズ スイッチ上の ファブリック エクステンダ 100 の各ホスト インターフェイス ポートを他のすべての手順に従って設定します。

```
NX-5000-1(config)# interface ethernet 100/1/1-48
NX-5000-1(config-if)# switchport mode access
NX-5000-1(config-if)# switchport access vlan 50
NX-5000-1(config-if)# no shutdown
NX-5000-1(config-if)# exit
```

ステップ 7 設定を保存します。

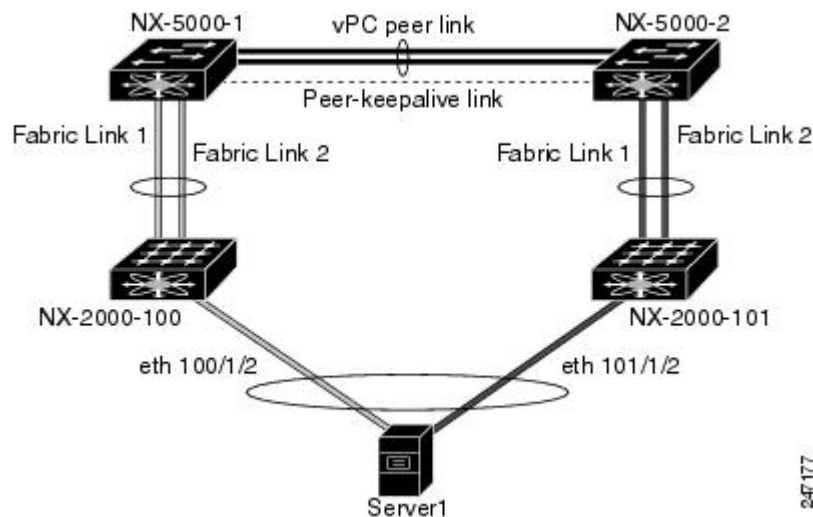
```
NX-5000-1(config)# copy running-config startup-config
```

NX-5000-2 スイッチに対して上記のすべての手順を繰り返します。

シングルホーム接続ファブリック エクステンダ vPC の設定例

次に、次の図に示すように、スイッチ NX-5000-1 のピアキーブアライブメッセージを伝送するためにデフォルト VRF を使用するシングルホーム接続 ファブリック エクステンダ vPC トポロジを設定する例を示します。

図 10 : vPC の設定例



(注) 次に、ファブリック エクステンダ NX-2000-100 に接続されている NX-5000-1 の設定だけを表示する例を示します。ファブリック エクステンダ NX-2000-101 に接続されているその vPC ピア (NX-5000-2) でこれらの手順を繰り返す必要があります。

はじめる前に

Cisco Nexus 2000 シリーズ ファブリック エクステンダ NX-2000-100 および NX-2000-101 が接続され、オンラインであることを確認します。

手順

ステップ 1 vPC および LACP をイネーブルにします。

```
NX-5000-1# configure terminal
NX-5000-1(config)# feature lacp
NX-5000-1(config)# feature vpc
```

- ステップ 2** SVI インターフェイスをイネーブルにし、vPC ピアキープアライブ リンクが使用する VLAN と SVI を作成します。

```
NX-5000-1(config)# feature interface-vlan
NX-5000-1(config)# vlan 900
NX-5000-1(config-vlan)# int vlan 900
NX-5000-1(config-if)# ip address 10.10.10.236 255.255.255.0
NX-5000-1(config-if)# no shutdown
NX-5000-1(config-if)# exit
```

- ステップ 3** vPC ドメインを作成し、デフォルト VRF の vPC ピアキープアライブ リンクを追加します。

```
NX-5000-1(config)# vpc domain 30
NX-5000-1(config-vpc-domain)# peer-keepalive destination 10.10.10.237 source 10.10.10.236
vrf default
NX-5000-1(config-vpc-domain)# exit
```

(注) vPC ピアキープアライブ メッセージを送信するので、VLAN 900 は、vPC ピア リンク間でトランッキングしないでください。vPC ピアキープアライブ メッセージの NX-5000-1 と NX-5000-2 のスイッチ間に代替パスが必要です。

- ステップ 4** 2 つのポートの EtherChannel として vPC ピア リンクを設定します。

```
NX-5000-1(config)# interface ethernet 1/1-2
NX-5000-1(config-if-range)# switchport mode trunk
NX-5000-1(config-if-range)# switchport trunk allowed vlan 20-50
NX-5000-1(config-if-range)# switchport trunk native vlan 20
NX-5000-1(config-if-range)# channel-group 30 mode active
NX-5000-1(config-if-range)# exit
NX-5000-1(config)# interface port-channel 30
NX-5000-1(config-if)# vpc peer-link
NX-5000-1(config-if)# exit
```

- ステップ 5** ファブリック エクステンダ NX-2000-100 を設定します。

```
NX-5000-1(config)# fex 100
NX-5000-1(config-fex)# pinning max-links 1
NX-5000-1(fex)# exit
```

- ステップ 6** ファブリック エクステンダ NX-2000-100 のファブリック EtherChannel リンクを設定します。

```
NX-5000-1(config)# interface ethernet 1/20-21
NX-5000-1(config-if)# channel-group 100
NX-5000-1(config-if)# exit
NX-5000-1(config)# interface port-channel 100
NX-5000-1(config-if)# switchport mode fex-fabric
NX-5000-1(config-if)# fex associate 100
NX-5000-1(config-if)# exit
```

ステップ 7 ファブリック エクステンダ NX-2000-100 の vPC サーバ ポートを設定します。

```
NX-5000-1(config-if)# interface ethernet 100/1/1
NX-5000-1(config-if)# switchport mode trunk
NX-5000-1(config-if)# switchport trunk native vlan 100
NX-5000-1(config-if)# switchport trunk allowed vlan 100-105
NX-5000-1(config-if)# channel-group 600
NX-5000-1(config-if)# no shutdown
NX-5000-1(config-if)# exit
NX-5000-1(config)# interface port-channel 600
NX-5000-1(config-if)# vpc 600
NX-5000-1(config-if)# no shutdown
NX-5000-1(config-if)# exit
```

ステップ 8 設定を保存します。

```
NX-5000-1(config)# copy running-config startup-config
```

vPC のデフォルト設定

次の表に、vPC パラメータのデフォルト設定を示します。

表 8: デフォルト vPC パラメータ

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



索引

E

EtherChannel ホスト インターフェイス [102](#)
作成 [102](#)

F

FEX [80](#)
用語 [80](#)

L

LACP [54, 60, 63, 67, 71, 72, 73](#)
 グレースフル コンバージェンス [72, 73](#)
 再イネーブル化 [73](#)
 ディセーブル化 [72](#)
システム ID [60](#)
設定 [67](#)
ポート チャネル [60](#)
ポート プライオリティ [71](#)
マーカー レスポンダ [63](#)
LACP がイネーブル対スタティック [63](#)
 ポート チャネル [63](#)
LACP の設定 [67](#)

M

MIB [51](#)
レイヤ 3 インターフェイス [51](#)

S

SFP+ トランシーバ [7](#)
Small Form-Factor Pluggable (プラス) トランシーバ [7](#)

STP [53](#)

ポート チャネル [53](#)

U

UDLD [5, 7](#)
 アグレッシブ モード [7](#)
 定義 [5](#)
 非アグレッシブ モード [7](#)
UDLD モード [14](#)
 設定 [14](#)

V

VLAN [39](#)
 インターフェイス [39](#)
VLAN インターフェイス [44](#)
 設定 [44](#)
vPC [90, 92, 103](#)
 ARP または ND を使用 [90](#)
 注意事項および制約事項 [92](#)
 ポート チャネルの移行 [103](#)
vPC トポロジ [101](#)
 孤立ポートの一時停止、セカンダリ スイッチ [101](#)
vPC ピア スイッチ [91](#)
vPC ピア スイッチ トポロジ [107, 109](#)
 純粋な [107](#)
 設定 [107](#)
 ハイブリッド [109](#)
 設定 [109](#)
VRF [46](#)
 インターフェイスの割り当て [46](#)

い

イーサネット インターフェイス [31](#)
 デバウンス タイマー、設定 [31](#)
 インターフェイス [5, 37, 39, 40, 43, 44, 45, 46, 49, 50](#)
 UDLD [5](#)
 VLAN [39, 44](#)
 設定 [44](#)
 VRF への割り当て [46](#)
 帯域幅の設定 [43](#)
 トンネル [40](#)
 ルーテッド [37](#)
 ループバック [40, 45](#)
 レイヤ 3 [37, 49, 50](#)
 設定例 [50](#)
 モニタリング [49](#)
 interface [3](#)
 オプション [3](#)
 シャーシ ID [3](#)
 インターフェイス情報、表示 [33](#)
 レイヤ 2 [33](#)
 インターフェイス速度 [7, 15](#)
 設定 [15](#)

か

確認 [47](#)
 レイヤ 3 インターフェイス設定 [47](#)
 関連資料 [51](#)
 レイヤ 3 インターフェイス [51](#)

く

グレースフル コンバージェンス [72, 73](#)
 LACP [72, 73](#)
 ポート チャネル [72, 73](#)
 LACP [72, 73](#)
 グレースフル コンバージェンス [72, 73](#)

こ

孤立ポートの一時停止、セカンダリ スイッチ [101](#)
 vPC トポロジ [101](#)

さ

サブインターフェイス [38, 42, 43](#)
 設定 [42](#)
 帯域幅の設定 [43](#)

し

新機能に関する情報 [1](#)
 説明 [1](#)

せ

設定 [41, 42, 43, 44, 45, 47](#)
 VLAN インターフェイス [44](#)
 インターフェイス帯域幅 [43](#)
 サブインターフェイス [42](#)
 ルーテッド インターフェイス [41](#)
 ループバック インターフェイス [45](#)
 レイヤ 3 インターフェイス [47](#)
 確認 [47](#)
 設定例 [50](#)
 レイヤ 3 インターフェイス [50](#)

た

帯域幅 [43](#)
 設定 [43](#)
 単一方向リンク検出 [5](#)

ち

チャネル モード [61, 68](#)
 ポート チャネル [61, 68](#)
 注意事項および制約事項 [41, 92](#)
 vPC [92](#)
 レイヤ 3 インターフェイス [41](#)

て

デバウンス タイマー [11](#)
 パラメータ [11](#)

デバウンス タイマー、設定 [31](#)
 イーサネット インターフェイス [31](#)
 デフォルト設定 [41](#)
 レイヤ 3 インターフェイス [41](#)

と

トンネル インターフェイス [40](#)

は

ハードウェア ハッシュ [66](#)
 マルチキャスト トラフィック [66](#)
 パラメータ、概要 [11](#)
 デバウンス タイマー [11](#)

ひ

標準 [51](#)
 レイヤ 3 インターフェイス [51](#)

ふ

ファブリック エクステンダ [80](#)
 用語 [80](#)
 物理イーサネットの設定 [36](#)

へ

変更された機能に関する情報 [1](#)
 説明 [1](#)

ほ

ポート チャネリング [54](#)
 ポート チャネル [43, 53, 55, 57, 60, 63, 64, 65, 66, 68, 74, 103](#)
 LACP [60](#)
 LACP がイネーブル対スタティック [63](#)
 STP [53](#)
 vPC への移行 [103](#)
 互換性要件 [55](#)
 作成 [63](#)

ポート チャネル (続き)
 設定の確認 [74](#)
 帯域幅の設定 [43](#)
 チャネル モード [68](#)
 ハードウェア ハッシュ [66](#)
 ポートの追加 [64](#)
 ロード バランシング [57, 65](#)
 ポート チャネル [57](#)
 ポート チャネルの設定 [54](#)
 注意事項および制約事項 [54](#)
 ポートの追加 [64](#)
 ポート チャネル [64](#)
 ポート プロファイル [9, 10](#)
 概要 [9](#)
 注意事項および制約事項 [10](#)
 ポート プロファイル [10](#)

ま

マルチキャスト トラフィック [66](#)
 ハードウェア ハッシュ [66](#)
 ポート チャネル [66](#)

も

モニタリング [49](#)
 レイヤ 3 インターフェイス [49](#)

ゆ

ユニファイド ポート [4, 12](#)
 設定 [12](#)

よ

用語 [80](#)
 ファブリック エクステンダ [80](#)

ら

ライセンス要件 [40](#)
 レイヤ 3 インターフェイス [40](#)

る

ルーテッド インターフェイス [37, 41, 43](#)
 設定 [41](#)
 帯域幅の設定 [43](#)
ループバック インターフェイス [40, 45](#)
 設定 [45](#)

れ

レイヤ 2 [33](#)
 インターフェイス情報、表示 [33](#)
レイヤ 2 インターフェイス [12](#)
 ユニファイド ポート [12](#)
レイヤ 3 インターフェイス [37, 40, 41, 47, 49, 50, 51](#)
 MIB [51](#)
 インターフェイス [51](#)
 レイヤ 3 [51](#)
 MIB [51](#)
 関連資料 [51](#)

レイヤ 3 インターフェイス (続き)
 インターフェイス (続き)
 レイヤ 3 (続き)
 標準 [51](#)

確認 [47](#)
関連資料 [51](#)
設定例 [50](#)
注意事項および制約事項 [41](#)
デフォルト設定 [41](#)
標準 [51](#)
モニタリング [49](#)
ライセンス要件 [40](#)
ルーテッド インターフェイスの設定 [41](#)

ろ

ロード バランシング [65](#)
 ポート チャネル [65](#)
 設定 [65](#)