Cisco Nexus 5500 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 7.x

初版：2014 年 01 月 15 日

最終更新：2014 年 03 月 06 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/

Text Part Number: OL-30891-01

【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。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号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、ネットワーク トポロジ図、およびその他の図は、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および電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco 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)

© 2016 Cisco Systems, Inc. All rights reserved.

目 次

はじめに xi

対象読者 xi

表記法 xi

Cisco Nexus 5500 シリーズ NX-OS ソフトウェアの関連資料 xiii

マニュアルに関するフィードバック xv

マニュアルの入手方法およびテクニカル サポート xv

新機能および変更された機能に関する情報 17

レイヤ 2 インターフェイスの設定 1

イーサネット インターフェイスの概要 1

インターフェイス コマンド 1

ユニファイド ポートについて 3

ユニファイド ポートに関する注意事項および制約事項 3

UDLD パラメータ 4

UDLD のデフォルト設定 5

UDLD アグレッシブ モードと非アグレッシブ モード 5

インターフェイスの速度 6

Cisco Discovery Protocol 6

CDP のデフォルト設定 6

error-disabled ステート 7

ポート プロファイルについて 7

ポート プロファイルに関する注意事項と制約事項 9

デバウンス タイマー パラメータ 9

MTU 設定 10

デフォルト インターフェイスに関する情報 10

物理イーサネットのデフォルト設定 10

イーサネット インターフェイスの設定 11

Cisco Nexus デバイスにおけるレイヤ 3 インターフェイスの設定 11
ユニファイド ポートの設定 12
UDLD モードの設定 13
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 16
CDP の特性の設定 17
CDP のイネーブル化/ディセーブル化 19
errdisable ステート検出のイネーブル化 19
errdisable ステート回復のイネーブル化 20
errdisable ステート回復間隔の設定 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
デフォルト インターフェイスの設定 32
説明パラメータの設定 33
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 33
低速ドレイン デバイスの検出と輻輳回避の設定 34
ファイバ チャネルの低速ドレイン デバイスの検出と輻輳回避：概要 34
スタック フレーム タイムアウト値の設定 35
No-Credit タイムアウト値の設定 35
クレジット ロス カウンタの表示 36
クレジット ロス イベントの表示 37
タイムアウト ドロップの表示 37
平均 Credit Not Available ステータスの表示 37
ポート モニタリング 38

ポート モニタのイネーブル化 38
ポート モニタ ポリシーの設定 38
ポート モニタ ポリシーのアクティブ化 40
ポート モニタ ポリシーの表示 40
FCoE 低速ドレイン デバイスの検出と輻輳回避 41
ポーズ フレーム タイムアウト値の設定 42
インターフェイス情報の表示 44
レイヤ 3 インターフェイスの設定 47
レイヤ 3 インターフェイスについて 47
ルーテッド インターフェイス 47
サブインターフェイス 48
VLAN インターフェイス 49
ループバック インターフェイス 50
プライベート VLAN での IP アドレッシング方式 50
レイヤ 3 インターフェイスのライセンス要件 51
レイヤ 3 インターフェイスの注意事項および制約事項 51
レイヤ 3 インターフェイスのデフォルト設定 52
レイヤ 3 インターフェイスの設定 52
ルーテッド インターフェイスの設定 52
サブインターフェイスの設定 53
インターフェイスでの帯域幅の設定 54
VLAN インターフェイスの設定 55
プライマリ VLAN のレイヤ 3 VLAN インターフェイスへのセカンダリ VLAN のマッピング 56
ループバック インターフェイスの設定 59
VRF へのインターフェイスの割り当て 60
レイヤ 3 インターフェイス設定の確認 61
レイヤ 3 インターフェイスのモニタリング 63
レイヤ 3 インターフェイスの設定例 65
レイヤ 3 インターフェイスの関連資料 65
レイヤ 3 インターフェイスの MIB 66
レイヤ 3 インターフェイスの標準 66

BFD の設定 67

BFD の概要 67

非同期モード 68

障害検出 68

BFD エコー機能 69

セキュリティ 70

仮想化のサポート 70

BFD のライセンス要件 70

前提条件 70

注意事項と制約事項 71

BFD のデフォルト設定 72

BFD の設定 73

BFD 設定階層 73

BFD 設定のタスク フロー 73

BFD 機能のイネーブル化について 73

BFD 機能のイネーブル化 73

グローバル BFD パラメータの設定について 74

グローバルな BFD パラメータの設定 74

インターフェイスでの BFD の設定について 76

インターフェイスでの BFD の設定 76

ポート チャネルの BFD の設定について 78

ポート チャネルの BFD の設定 78

BFD エコー機能の設定について 80

BFD エコー機能の設定 80

サブインターフェイスの BFD の最適化について 81

サブインターフェイスの BFD の最適化 82

ルーティング プロトコルに対する BFD サポートの設定 83

BGP 上での BFD の設定について 83

BGP での BFD の設定 83

EIGRP 上での BFD の設定について 84

EIGRP 上での BFD の設定 85

OSPF 上での BFD の設定について 86

OSPF での BFD の設定 86
HSRP 上での BFD の設定について 87
HSRP での BFD の設定 88
VRRP 上での BFD の設定について 89
VRRP での BFD の設定 89
スタティック ルートでの BFD の設定について 90
スタティック ルートでの BFD の設定 90
PIM 上での BFD の設定について 92
PIM 上での BFD の設定 92
インターフェイスにおける BFD のディセーブル化 93
すべての IS-IS インターフェイスでの FabricPath BFD の設定 93
特定のインターフェイスでの FabricPath BFD の設定 94
BFD 設定の確認 95
BFD のモニタ 95
BFD の設定例 96
関連資料 96
関連の標準 97
ポート チャネルの設定 99
ポート チャネルについて 99
ポート チャネルの概要 100
ポート チャネルの設定に関する注意事項と制約事項 101
互換性要件 101
ポート チャネルを使ったロード バランシング 103
LACP の概要 106
LACP の概要 106
LACP ID パラメータ 106
チャネル モード 107
LACP マーカー レスポンダ 109
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 109
LACP ポートチャネルの最小リンクおよび MaxBundle 109
ポート チャネルの設定 110

デフォルト設定 110
ポート チャネルの作成 111
ポート チャネルへのポートの追加 112
ポート チャネルを使ったロード バランシングの設定 113
マルチキャスト トラフィックに対するハードウェア ハッシュの設定 114
LACP のイネーブル化 115
ポートに対するチャネル モードの設定 115
LACP ポート チャネル最小リンク数の設定 117
LACP ポートチャネル MaxBundle の設定 118
LACP 高速タイマー レートの設定 119
LACP ショート タイムアウトの設定 120
LACP のシステム プライオリティおよびシステム ID の設定 121
LACP ポート プライオリティの設定 121
LACP グレースフル コンバージェンスのディセーブル化 122
LACP グレースフル コンバージェンスの再イネーブル化 123
ポート チャネル設定の確認 125
ロードバランシング発信ポート ID の確認 126
ポート チャネル設定の機能履歴 126
仮想ポート チャネルの設定 129
vPC について 129
vPC の概要 129
用語 131
vPC の用語 131
ファブリック エクステンダの用語 132
サポートされている vPC トポロジ 132
Cisco Nexus デバイスの vPC トポロジ 132
シングル ホーム ファブリック エクステンダの vPC トポロジ 132
デュアル ホーム ファブリック エクステンダの vPC トポロジ 133
vPC ドメイン 134
ピアキープアライブ リンクとメッセージ 135
vPC ピア リンクの互換パラメータ 136
同じでなければならない設定パラメータ 136

同じにすべき設定パラメータ 137
グレースフル タイプ 1 検査 138
VLAN ごとの整合性検査 138
vPC 自動リカバリ 138
vPC ピア リンク 139
vPC ピア リンクの概要 139
vPC 番号 140
vPC を介したレイヤ 3 141
vPC を介したレイヤ 3：サポートされている設計 142
vPC を介したレイヤ 3：サポートされていない設計 144
その他の機能との vPC の相互作用 149
vPC ピア リンクおよびコアへのリンクの設定 149
vPC と LACP 151
vPC ピア リンクと STP 152
vPC と ARP 152
CFSoE 153
vPC ピア スイッチ 153
VRF に関する注意事項と制約事項 154
vPC の設定 155
vPC のイネーブル化 155
vPC のディセーブル化 155
vPC ドメインの作成 156
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 157
vPC ピア リンクの作成 160
設定の互換性の検査 160
vPC 自動リカバリのイネーブル化 162
復元遅延時間の設定 163
vPC ピア リンク障害発生時における VLAN インターフェイスのシャットダウン回避 164
VRF 名の設定 164
vPC への VRF インスタンスのバインド 165
vPC のゲートウェイ MAC アドレスを宛先とするレイヤ 3 転送のイネーブル化 166

vPC トポロジにおけるセカンダリ スイッチの孤立ポートの一時停止 166
EtherChannel ホスト インターフェイスの作成 168
他のポート チャネルの vPC への移行 169
vPC ドメイン MAC アドレスの手動での設定 170
システム プライオリティの手動での設定 171
vPC ピア スイッチのロールの手動による設定 172
vPC ピア スイッチの設定 173
純粋な vPC ピア スイッチ トポロジの設定 173
ハイブリッド vPC ピア スイッチ トポロジの設定 175
vPC を介したレイヤ 3 の設定 177
vPC 複合からのスイッチの分離と復元 178
vPC シャットダウンの設定 178
vPC シャットダウン スイッチの復元 179
vPC 設定の確認 179
グレースフル タイプ 1 検査ステータスの表示 180
グローバル タイプ 1 不整合の表示 181
インターフェイス別タイプ 1 不整合の表示 182
VLAN ごとの整合性ステータスの表示 183
vPC の設定例 185
デュアル ホーム ファブリック エクステンダにおける vPC の設定例 185
シングル ホーム ファブリック エクステンダにおける vPC の設定例 187
vPC のデフォルト設定 189

はじめに

ここでは、次の項について説明します。

- 対象読者，xi ページ
- 表記法，xi ページ
- Cisco Nexus 5500 シリーズ NX-OS ソフトウェアの関連資料，xiii ページ
- マニュアルに関するフィードバック，xv 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，xv ページ

対象読者

このマニュアルは、Cisco Nexus デバイスおよび Cisco Nexus 2000 シリーズ ファブリック エクステンダのコンフィギュレーションおよびメンテナンスを担当するネットワーク管理者を対象としています。

表記法

（注） お客様のニーズを満たすためにドキュメントを更新するという継続的な取り組みの一環として、シスコでは設定タスクの文書化方法を変更しました。そのため、本ドキュメントには、従来とは異なるスタイルでの設定タスクが説明されている部分もあります。ドキュメントに新たに組み込まれるようになったセクションは、新しい表記法に従っています。

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。

表記法	説明
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角カッコで囲んで示しています。
[x | y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波カッコで囲み、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。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、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に記載されていない参照資料を紹介しています。

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

Cisco Nexus 5500 シリーズ NX-OS ソフトウェアの関連資料

Cisco NX-OS 5500 シリーズ全体のマニュアル セットは、次の URL から入手できます。

http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/tsd-products-support-series-home.html

リリース ノート

リリース ノートは、次の URL から入手できます。

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

コンフィギュレーション ガイド

これらのマニュアルは、次の URL から入手できます。

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

このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 5500 Series NX-OS Adapter-FEX Configuration Guide*』
- 『*Cisco Nexus 5500 Series NX-OS FabricPath Configuration Guide*』
- 『*Cisco Nexus 5500 Series NX-OS FCoE Configuration Guide*』
- 『*Cisco Nexus 5500 Series NX-OS Fundamentals Configuration Guide*』
- 『*Cisco Nexus 5500 Series NX-OS Interfaces Configuration Guide*』
- 『*Cisco Nexus 5500 Series NX-OS Layer 2 Switching Configuration Guide*』
- 『*Cisco Nexus 5500 Series NX-OS Multicast Routing Configuration Guide*』
- 『*Cisco Nexus 5500 Series NX-OS Quality of Service Configuration Guide*』
- 『*Cisco Nexus 5500 Series NX-OS SAN Switching Configuration Guide*』
- 『*Cisco Nexus 5500 Series NX-OS Security Configuration Guide*』
- 『*Cisco Nexus 5500 Series NX-OS System Management Configuration Guide*』

- 『*Cisco Nexus 5500 Series NX-OS Unicast Routing Configuration Guide*』

インストレーション ガイドおよびアップグレード ガイド

これらのマニュアルは、次の URL から入手できます。

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

このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 5500 Series NX-OS Software Upgrade and Downgrade Guides*』

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-ossw_lisns.html から入手できます。

コマンド リファレンス

これらのマニュアルは、次の URL から入手できます。

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

このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 5500 Series NX-OS Fabric Extender Command Reference*』
- 『*Cisco Nexus 5500 Series NX-OS FabricPath Command Reference*』
- 『*Cisco Nexus 5500 Series NX-OS Fundamentals Command Reference*』
- 『*Cisco Nexus 5500 Series NX-OS Interfaces Command Reference*』
- 『*Cisco Nexus 5500 Series NX-OS Layer 2 Interfaces Command Reference*』
- 『*Cisco Nexus 5500 Series NX-OS Multicast Routing Command Reference*』
- 『*Cisco Nexus 5500 Series NX-OS Quality of Service Command Reference*』
- 『*Cisco Nexus 5500 Series NX-OS Security Command Reference*』
- 『*Cisco Nexus 5500 Series NX-OS System Management Command Reference*』
- 『*Cisco Nexus 5500 Series NX-OS TrustSec Command Reference*』
- 『*Cisco Nexus 5500 Series NX-OS Unicast Routing Command Reference*』
- 『*Cisco Nexus 5500 Series NX-OS Virtual Port Channel Command Reference*』

テクニカル リファレンス

『*Cisco Nexus 5500 Series NX-OS MIB Reference*』は http://www.cisco.com/en/US/docs/switches/datacenter/nexus5500/sw/mib/reference/NX5500_MIBRef.html から入手できます。

エラー メッセージおよびシステム メッセージ

『*Cisco Nexus 5500 Series NX-OS System Message Guide*』は、http://www.cisco.com/en/US/docs/switches/datacenter/nexus5500/sw/system_messages/reference/sl_nxos_book.html から入手できます。

トラブルシューティング ガイド

『*Cisco Nexus 5500 Series NX-OS Troubleshooting Guide*』は http://www.cisco.com/en/US/docs/switches/datacenter/nexus5500/sw/troubleshooting/guide/N5K_Troubleshooting_Guide.html から入手できます。

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（ciscodfa-docfeedback@cisco.com）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、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『What's New in Cisco Product Documentation』を参照してください。

新しく作成された、または改訂されたシスコのテクニカル コンテンツをお手元で直接受け取るには、『What's New in Cisco Product Documentation』RSS フィードをご購読ください。RSS フィードは無料のサービスです。

新機能および変更された機能に関する情報

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

（注） 新機能および変更された機能に関する情報のトピックが Cisco Nexus Release 7.3(0)N1(1) 以降の構成ガイドに追加されました。

Cisco NX-OS リリース番号	サポートされるプラットフォーム	新機能/拡張機能	文書化されている章/トピック
7.3(0)N1(1)	Cisco Nexus 5500、5600、および 6000 シリーズ スイッチ	vPC を介したレイヤ 3 のサポート	vPC を介したレイヤ 3

第 1 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，1 ページ
- デフォルト インターフェイスに関する情報，10 ページ
- 物理イーサネットのデフォルト設定，10 ページ
- イーサネット インターフェイスの設定，11 ページ
- 低速ドレイン デバイスの検出と輻輳回避の設定，34 ページ
- FCoE 低速ドレイン デバイスの検出と輻輳回避，41 ページ
- インターフェイス情報の表示，44 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。

イーサネット インターフェイスはデフォルトでイネーブルです。

インターフェイス コマンド

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

- インターフェイス タイプ：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）。
- ポート番号：グループ内のポート番号。

QSFP+汎用拡張モジュール（GEM）が拡張スロットのどれかに入っている場合、次が適用されます。

- インターフェイスタイプ：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。
- 5548P および 5548UP の場合、スロット番号は次のとおりです。
  - スロット 1：すべての固定ポートを含みます。
  - スロット 2：GEM（実装されている場合）上の QSFP+ ポート
- 5596UP および 5596T の場合、スロット番号は次のとおりです。
  - スロット 1：すべての固定ポートを含みます。
  - スロット 2：GEM（実装されている場合）上の QSFP+ ポート
  - スロット 3：GEM（実装されている場合）上の QSFP+ ポート
  - スロット 4：GEM（実装されている場合）上の QSFP+ ポート
- QSFP-モード：これは GEM ブレークアウト ポート モードを識別するために使用されます。
- ポート番号：グループ内のポート番号。

QSFP+ GEM のコマンド構文は次のとおりです。

- switch(config)# **interfaceethernet***slot*/*QSFP-module*/*port*

Cisco Nexus 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)# **interfaceethernet** [*chassis*/]*slot*/*port*

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

ユニファイド ポートについて

Cisco Nexus のユニファイド ポートを使用すると、Cisco Nexus デバイス スイッチの物理ポートを 1/10 ギガビット イーサネット ポート、Fibre Channel over Ethernet（FCoE）ポート、ネイティブ 2 ギガビット ファイバ チャネル ポート、ネイティブ 4 ギガビット ファイバ チャネル ポート、またはネイティブ 8 ギガビット 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。

最近では、さまざまなタイプのネットワークに対応できるように 2 つのタイプのスイッチを備えたネットワークがほとんどです。たとえば、イーサネット トラフィックを Catalyst まで伝送するための LAN スイッチと、FC トラフィックをサーバから MDS スイッチへ伝送するための Nexus スイッチを備えたネットワークなどはその一例です。ユニファイドポートテクノロジーを使用すると、ユニファイド プラットフォーム、ユニファイド デバイス、およびユニファイド ワイヤの方式を導入することができます。ユニファイド ポートでは、LAN ポート オプションや SAN ポート オプションを選択する既存の分離プラットフォーム方式から、単一のユニファイドファブリックへ移行することができます。ユニファイド ファブリックは透過的であり、従来の運用方法や管理ソフトウェアにも対応しています。ユニファイド ファブリックの構成要素は次のとおりです。

- ユニファイド プラットフォーム：同一のハードウェア プラットフォームおよび同一のソフトウェア コード レベルをまとめて、LAN 環境および SAN 環境に対応できるようにしたものです。
- ユニファイド デバイス：同一のプラットフォーム スイッチ上で LAN サービスおよび SAN サービスが実行されます。ユニファイド デバイスでは、イーサネット ケーブルやファイバ チャネル ケーブルを同一のデバイスに接続することができます。
- ユニファイド ワイヤ：LAN ネットワークおよび SAN ネットワークをただ 1 つの統合ネットワーク アダプタ（CNA）で集約し、それらをサーバに接続します。

ユニファイド ファブリックでは、イーサネット機能や FCoE 機能を、既存の Cisco ツールとは独立に管理することができます。

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、モジュールの先頭のポートから設定する必要があります。

  この順序に従って設定が行われていない場合は、次のような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 から始めてポート 1/32 まで順に設定されます。ファイバ チャネル ポートは、ポート 1/32 から始めてポート 1/1 まで順に設定されます。

- 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。

UDLD パラメータ

シスコ独自の単一方向リンク検出（UDLD）プロトコルでは、光ファイバまたは銅線（たとえば、カテゴリ 5 のケーブル）のイーサネット ケーブルで接続されているポートでケーブルの物理的な構成をモニタリングし、単一方向リンクの存在を検出できます。スイッチが単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。単方向リンクは、スパニングツリー トポロジ ループをはじめ、さまざまな問題を引き起こす可能性があります。

UDLD は、レイヤ 1 プロトコルと協調してリンクの物理ステータスを検出するレイヤ 2 プロトコルです。レイヤ 1 では、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。

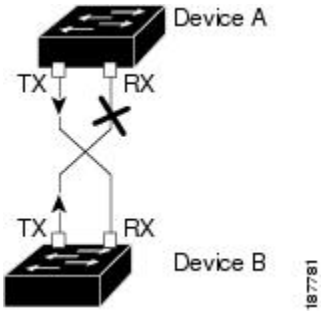
リンク上でローカル デバイスから送信されたトラフィックはネイバーで受信されるのに対し、ネイバーから送信されたトラフィックはローカル デバイスで受信されない場合には常に、単方向リンクが発生します。対になっているファイバ ケーブルのいずれかの接続が切断された場合、自動ネゴシエーションがアクティブであれば、そのリンクは存続できません。この場合、論理リンクは不定であり、UDLD は何の処理も行いません。レイヤ 1 で両方の光ファイバが正常に動作している場合は、レイヤ 2 で UDLD が、これらの光ファイルが正しく接続されているかどうか、および正しいネイバー間でトラフィックが双方向に流れているかを調べます。自動ネゴシエーションはレイヤ 1 で動作するため、このチェックは、自動ネゴシエーションでは実行できません。

Cisco Nexus デバイスは、UDLD がイネーブルになっている LAN ポート上のネイバー デバイスに定期的に UDLD フレームを送信します。一定の時間内にフレームがエコーバックされてきて、特定の確認応答（echo）が見つからなければ、そのリンクは単一方向のフラグが立てられ、その LAN ポートはシャットダウンされます。UDLD プロトコルにより単方向リンクが正しく識別されその使用が禁止されるようにするためには、リンクの両端のデバイスで UDLD がサポートされている必要があります。

次の図は、単方向リンクが発生した状態の一例を示したものです。デバイス B はこのポートでデバイス A からのトラフィックを正常に受信していますが、デバイス A は同じポート上でデバイス

B からのトラフィックを受信していません。UDLD によって問題が検出され、ポートがディセーブルになります。

図 *1*：単方向リンク



UDLD のデフォルト設定

次の表は、UDLD のデフォルト設定を示したものです。

表 *1*： *UDLD* のデフォルト設定

機能	デフォルト値
UDLD グローバル イネーブル ステート	グローバルにディセーブル
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）	イネーブル

UDLD アグレッシブ モードと非アグレッシブ モード

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

スパニングツリー ループを防止するため、間隔がデフォルトの 15 秒である非アグレッシブな UDLD でも、（デフォルトのスパニングツリー パラメータを使用して）ブロッキング ポートが

フォワーディング ステートに移行する前に、単方向リンクをシャットダウンすることができます。

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

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

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

インターフェイスの速度

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

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

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

CDP が設定された各デバイスはマルチキャストアドレスに定期的にメッセージを送信して、SNMP メッセージを受信可能なアドレスを 1 つまたは複数アドバタイズします。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

次の表は、CDP のデフォルト設定を示したものです。

表 *2*： ***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

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 error-disabled（err-disabled）ステートです。たとえば、UDLD が単方向リンクを検出した場合、そのインターフェイスは実行時にシャットダウンされます。ただし、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 err-disabled として表示されます。いったん err-disabled ステートになったインターフェイスは、手動でイネーブルにする必要があります。ただし、自動回復までのタイムアウト値を設定することもできます。err-disabled 検出はすべての原因に対してデフォルトでイネーブルです。自動回復はデフォルトでは設定されていません。

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

time 変数の変更によって起きる特定の err-disabled に対しては自動 err-disabled 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 秒後に自動回復します。回復までの時間を変更する場合は、**errdisable recovery interval** コマンドを使用して、タイムアウト時間を指定します。指定できる値は 30 ～ 65535 秒です。

原因に対する err-disabled 回復をイネーブルにしない場合、そのインターフェイスは **shutdown** コマンドおよび **no shutdown** コマンドが入力されるまで err-disabled ステートのままです。原因に対して回復をイネーブルにすると、そのインターフェイスの errdisable ステートは解消され、すべての原因がタイムアウトになった段階で動作を再試行できるようになります。エラーの原因を表示する場合は、**show interface status err-disabled** コマンドを使用します。

ポート プロファイルについて

さまざまなインターフェイス コマンドを含むポート プロファイルを作成し、そのポート プロファイルを Cisco Nexus デバイスのインターフェイス（複数可）の範囲に適用することができます。ポート プロファイルは、次のようなタイプのインターフェイスに適用できます。

- 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部でも設定することができます。ポートプロファイルの新しい設定と、ポートプロファイル外部の既存の設定が競合する場合は、ポート プロファイル内のコマンドよりも、インターフェイスに対して設定端末モードで設定されたコマンドの方が優先されます。ポート プロファイルの適用後に変更したインターフェイス設定が、そのポート プロファイルの設定と競合した場合は、インターフェイス設定が優先されます。

単独のインターフェイスまたはある範囲に属する複数のインターフェイスに適用されているポートプロファイルは継承することができます。ポートプロファイルを単独のインターフェイスまたはある範囲に属する複数のインターフェイスに適用した場合も、ポート プロファイルを継承した場合も、スイッチではそのポート プロファイル内のすべてのコマンドがインターフェイスに適用されます。

ポートプロファイルには、別のポートプロファイルの設定を継承することができます。別のポート プロファイルを継承した場合、最初のポート プロファイルでは、それを継承した第 2 のポート プロファイルに含まれるすべてのコマンドは、最初のポート プロファイルとは競合していないものと見なされます。4 つのレベルの継承がサポートされています。任意の数のポート プロファイルで同じポート プロファイルを継承できます。

ポートプロファイル設定をインターフェイスに適用するには、そのポートプロファイルをイネーブルにする必要があります。ポート プロファイルをイネーブルにする前に、インターフェイス（複数可）に対してそのポート プロファイルを設定および継承することができます。そのうえでポート プロファイルをイネーブルにすると、指定したインターフェイスにその設定内容が反映されます。

ポート プロファイルをインターフェイス（複数可）から削除する場合は、スイッチでは最初にインターフェイスの設定が無効にされ、その後でポート プロファイルのリンクそのものが削除されます。また、ポート プロファイルを削除すると、スイッチではインターフェイス設定の確認が行われた後、直接入力されたインターフェイス コマンドにより無効になったポート プロファイル コマンドがスキップされるか、またはそれらのコマンドがデフォルト値に戻されます。

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

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

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

単独のインターフェイスまたはある範囲に属する複数のインターフェイスに対してポート プロファイルを継承した後、特定の設定値を削除すると、それらのインターフェイスではそのポート プロファイル設定が機能しなくなります。

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

ポート プロファイルをイネーブル化、継承、または変更しようとすると、スイッチによりチェックポイントが作成されます。ポート プロファイル設定が正常に実行されなかった場合は、その前の設定までロールバックされ、エラーが返されます。ポート プロファイルは部分的にだけ適用されることはありません。

ポート プロファイルに関する注意事項と制約事項

ポート プロファイルの設定に関する注意事項および制約事項は次のとおりです。

- 各ポートプロファイルは、インターフェイスのタイプにかかわらず、ネットワーク上で一意の名前を持つ必要があります。
- 競合が発生した場合は、インターフェイス モードで入力したコマンドがポート プロファイルのコマンドに優先します。しかし、ポートプロファイルはそのコマンドをポートプロファイルに保持します。
- ポートプロファイルのコマンドに対してインターフェイスのデフォルトのコマンドを明示的に優先させない限り、ポート プロファイルのコマンドがデフォルトのコマンドに優先します。
- ポート プロフィルをインターフェイスまたはインターフェイスの範囲に継承した後、インターフェイス コンフィギュレーション レベルで新しい値を入力して、個々の設定値を上書きできます。インターフェイス コンフィギュレーション レベルで個々の設定値を削除すると、インターフェイスではポート プロファイル内の値が再度使用されます。
- ポート プロファイルに関連したデフォルト設定はありません。
- ポート プロファイル コンフィギュレーション モードでは、指定したインターフェイス タイプに応じて、特定のグループのコマンドを使用することができます。
- 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

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

Cisco Nexus デバイス スイッチは、フレームをフラグメント化しません。そのためスイッチでは、同じレイヤ 2 ドメイン内の 2 つのポートに別々の最大伝送単位（MTU）を設定することはできません。物理イーサネット インターフェイス別 MTU はサポートされていません。代わりに、MTU は QoS クラスに従って設定されます。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 は 1500 と表示され、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。

デフォルト インターフェイスに関する情報

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

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

（注） デフォルト インターフェイス機能は管理インターフェイスでサポートされますが、デバイスが到達不能になる可能性があるためお奨めしません。

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。

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 デバイスにおけるレイヤ 3 インターフェイスの設定

Cisco Nexus デバイスにレイヤ 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場合は、**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 モードに入ります。
ステップ 2	switch(config)# **interfaceethernet***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。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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。

次の例は、レイヤ 3 インターフェイスの設定方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 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
- Cisco Nexus 5672UP
- Cisco Nexus 56128 with N56-M24UP2Q GEM
- Cisco Nexus
-
-

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** コマンドが有効なことを確認します。

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*	スイッチ上のスロットを指定します。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 3	switch(config-slot) # **port***port number***type** {**ethernet** | **fc**}	ユニファイド ポートをネイティブ ファイバ チャネル ポートおよびイーサネット ポートとして設定します。 • **type**：シャーシのスロット上で設定するポートのタイプを指定します。

	コマンドまたはアクション	目的
		• **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。 （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。
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) # **slot***slot number*	スイッチ上のスロットを指定します。
ステップ 7	switch(config-slot) # **no port***port number***type fc**	ユニファイド ポートを削除します。

次の例は、20 個のポートをイーサネット ポートとして設定し、12 個のポートを FC ポートとして設定する方法を示したものです。

```
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
```

次の例は、Cisco N55-M16UP 拡張モジュールでユニファイド ポートを設定する方法を示したものです。

```
switch# configure terminal
switch(config)# slot 2
switch(config-slot)# port 1-16 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

単一方向リンク検出（UDLD）を実行するように設定されているデバイス上のイーサネット インターフェイスには、ノーマル モード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**	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 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***typeslot*/*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。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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。
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 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に **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***typeslot*/*port*	指定したインターフェイスに対してインターフェイス 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。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **speed***speed*	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。

	コマンドまたはアクション	目的
		Cisco Nexus 5500 シリーズ スイッチの場合は、*speed* 引数を次のいずれかに設定できます。 • 1000：1 Gbps • 10000：10Gbps • auto （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。 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。

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

no negotiate auto コマンドを使用することにより、リンク ネゴシエーションをディセーブルにすることができます。デフォルトでは、自動ネゴシエーションは 1 ギガビット ポートではイネーブル、10 ギガビット ポートではディセーブルです。

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

（注） 自動ネゴシエーションの設定は、10 ギガビット イーサネット ポートには適用されません。自動ネゴシエーションを 10 ギガビット ポートに設定すると、次のエラー メッセージが表示されます。

```
ERROR: Ethernet1/40: Configuration does not match the port capability
```

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*	インターフェイスを選択し、インターフェイス モードを開始します。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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）に対してリンク 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**	（任意） 選択したイーサネット インターフェイスに対してリンク ネゴシエーションをイネーブルにします。1 ギガビット イーサネット ポートに対してはデフォルトでイネーブルです。 （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。

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、情報を廃棄するまでの保持期間、およびバージョン 2 アドバタイズを送信するかどうかを設定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**	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)# [**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 のフォーマットを設定します。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） デバイスから送信された情報が受信デバイスで破棄されるまでの保持時間を指定します。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**	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***typeslot*/*port*	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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。

errdisable ステート検出のイネーブル化

アプリケーションでの errdisable ステート検出をイネーブルにすることができます。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。

（注） Cisco Nexus 5020 または 5010 スイッチと同様のポーズ レート制限により、Cisco Nexus 5500 の基本ポートは error disabled になりません。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **errdisable detect cause** {*all* | *link-flap* | *loopback*}	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。デフォルトではイネーブルになっています。
ステップ 3	switch(config)# **shutdown**	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	switch(config)# **no shutdown**	インターフェイスを管理上アップにし、err-disabled ステートから手動で回復できるようにします。
ステップ 5	switch(config)# **show interface status err-disabled**	err-disabled ステートにあるインターフェイスについての情報を表示します。
ステップ 6	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、変更を継続的に保存します。

次に、すべての場合に err-disabled 検出をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# errdisable detect cause all
switch(config)# shutdown
switch(config)# no shutdown
switch(config)# show interface status err-disabled
switch(config)# copy running-config startup-config
```

errdisable ステート回復のイネーブル化

アプリケーションを指定してインターフェイスを error-disabled（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	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)# **errdisable recovery cause** {*all* | *udld* | *bpduguard* | *link-flap* | *failed-port-state* | *pause-rate-limit*}	インターフェイスが err-disabled ステートから自動的に回復し、デバイスがそのインターフェイスを再びアップ状態にする条件を指定します。デバイスは 300 秒待機してからリトライします。デフォルトではディセーブルになっています。
ステップ 3	switch(config)# **show interface status err-disabled**	err-disabled ステートにあるインターフェイスについての情報を表示します。
ステップ 4	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、変更を継続的に保存します。

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# configure terminal
switch(config)# errdisable recovery cause all
switch(config)# show interface status err-disabled
switch(config)# copy running-config startup-config
```

errdisable ステート回復間隔の設定

下記の手順により、errdisable ステート回復のタイマー値を設定することができます。有効な範囲は 30 ～ 65535 秒です。デフォルトは 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	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)# **errdisable recovery interval***interval*	インターフェイスが errdisable 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。デフォルトは 300 秒です。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **show interface status err-disabled**	errdisable ステートにあるインターフェイスについての情報を表示します。
ステップ 4	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、変更を継続的に保存します。

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# configure terminal
switch(config)# errdisable recovery interval 32
switch(config)# show interface status err-disabled
switch(config)# copy running-config startup-config
```

ポート プロファイル

ポート プロファイルの作成

スイッチでポートプロファイルを作成することができます。各ポートプロファイルは、インターフェイスのタイプにかかわらず、ネットワーク上で一意の名前を持つ必要があります。

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 モードに入ります。

ステップ 2	**port-profile** [**type** {**ethernet** | **interface-vlan** | **port channel**}] *name*
	
	例：
	`switch(config)# port-profile type ethernet test`
	`switch(config-port-prof)#`
		指定されたタイプのインターフェイスのポート プロファイルを作成して命名し、ポートプロファイルコンフィギュレーション モードを開始します。

ステップ 3	**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 4	**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 5	**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。

次の例は、イーサネット インターフェイスに対して test という名前のポート プロファイルを作成する方法を示したものです。

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

次の例は、イーサネット インターフェイスに対して設定した 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方法を示したものです。

```
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することができます。

このコマンドの **no** 形式を使用すると、ポート プロファイルからコマンドを削除することができます。ポート プロファイルからコマンドを削除すると、それに対応するコマンドも、そのポート プロファイルが適用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：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

	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：
	`switch(config)# port-profile type ethernet test`
	`switch(config-port-prof)#`
		指定されたポート プロファイルのポート プロファイルコンフィギュレーションモードを開始し、プロファイルの設定を追加または削除できるようにします。

ステップ 3	**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 4	**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 5	**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。

次の例は、イーサネット インターフェイスに対して設定した 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方法を示したものです。

```
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：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

	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：
	`switch(config)# port-profile type ethernet test`
	`switch(config-port-prof)# no shutdown`
	`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	**state enabled** *name*
	
	例：
	`switch(config-port-prof)# state enabled`
	`switch(config-port-prof)#`
		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：
	`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。

次の例は、ポート プロファイル コンフィギュレーション モードを開始し、ポート プロファイルをイネーブルにする方法を示したものです。

```
switch# configure terminal
switch(config)# port-profile type ethernet test
switch(config-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。スイッチでは 4 つのレベルの継承がサポートされています。

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 モードに入ります。

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)#
```

次の例は、イーサネット インターフェイスに対して設定した 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方法を示したものです。

```
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)#
```

次に、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例を示します。

```
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 モードに入ります。

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： `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

単独のインターフェイスまたはある範囲に属する複数のインターフェイスにポート プロファイルを割り当てることができます。インターフェイスはすべて同じタイプであることが必要です。

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	**interface** [**ethernet** *slot/port* | **interface-vlan** *vlan-id* | **port-channel** *number*]	インターフェイスの範囲を選択します。 （注） これが QSFP+ GEMS の場合、*slot/port* 構文は *slot/QSFP-module/port* になります。
ステップ 3	**inherit port-profile** *name*	指定したポート プロファイルを、選択したインターフェイスに割り当てます。
ステップ 4	**exit**	ポート プロファイル コンフィギュレーション モードを終了します。
ステップ 5	**show port-profile** *name*	（任意） ポート プロファイルの設定を表示します。

	コマンドまたはアクション	目的
ステップ 6	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、変更を継続的に保存します。

次の例は、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方法を示したものです。

```
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)# exit
switch(config)# show port-profile adam
switch(config)# copy running-config startup-config
```

一定範囲のインターフェイスからのポート プロファイルの削除

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	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	**interface** [**ethernet** *slot/port* | **interface-vlan** *vlan-id* | **port-channel** *number*]	インターフェイスの範囲を選択します。 （注） これが QSFP+ GEMS の場合、*slot/port* 構文は *slot/QSFP-module/port* になります。
ステップ 3	**no inherit port-profile** *name*	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**	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**	（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	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

	コマンドまたはアクション	目的
		ションにコピーして、変更を継続的に保存します。

次の例は、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方法を示したものです。

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

ポート プロファイルの設定例

次の例は、ポートプロファイルを設定して、イーサネットインターフェイスでそれを継承し、さらにそのポート プロファイルをイネーブルにする方法を示したものです。

```
switch(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**	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***typeslot*/*port*	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **link debounce time***milliseconds*	指定した時間（1 ～ 5000 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
```

デフォルト 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)# **default interface** *int-if* [**checkpoint** *name*]	インターフェイスの設定を削除しデフォルトの設定を復元します。*int-if* の値は次のいずれかです。 • ethernet • loopback • mgmt • port-channel • vlan **checkpoint** キーワードを使用して、設定を消去する前にインターフェイスの実行コンフィギュレーションのコピーを保存します。
ステップ 3	**exit**	コンフィギュレーション モードを終了します。
ステップ 4	**show interface**	（任意） インターフェイスのステータスと内容を表示します。

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

```
switch# configure terminal
switch(config)# show running-config interface e1/10
!Command: show running-config interface Ethernet1/10
!Time: Tue Jul 2 10:23:50 2013

version 6.0(2)N2(1)

interface Ethernet1/10
switchport mode trunk
channel-group 1

default interface ethernet 3/1 checkpoint chk1
.......Done
switch(config)# show running-config interface e1/10
!Command: show running-config interface Ethernet1/10
!Time: Tue Jul 2 10:24:41 2013

version 6.0(2)N2(1)

interface Ethernet1/10
```

```
switch(config)#
```

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**	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***typeslot/port*	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。 （注） これが QSFP+ GEMS の場合、*slot/port* 構文は *slot/QSFP-module/port* になります。
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**	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***typeslot*/*port*	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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
```

低速ドレイン デバイスの検出と輻輳回避の設定

ファイバ チャネルの低速ドレイン デバイスの検出と輻輳回避：概要

SAN ファブリックのエンド デバイス間のすべてのデータ トラフィックは、ファイバ チャネル クラス 3、および場合によってはクラス 2 のサービスで行われ、リンク レベル、ホップごとベース、バッファ間のフロー制御が使用されます。これらのサービス クラスは、エンドツーエンド フロー制御をサポートしません。ファブリックに低速デバイスが接続されている場合、エンド デバイスは設定またはネゴシエーションされたレートのフレームを受け入れません。低速デバイスにより、これらのデバイスを宛先とするトラフィックで（Inter-Switch Link）ISL クレジット不足が発生し、リンクが輻輳します。クレジット不足は、宛先デバイスで低速ドレインが発生していなくても、ファブリック内の同じ ISL リンクを使用する無関係なフローに影響します。

この機能は、ネットワークで輻輳を引き起こしている低速ドレイン デバイスを検出するためにさまざまな機能拡張を行い、さらに輻輳回避も提供します。

この機能拡張は、ISL が塞がれる原因となっている低速ドレイン デバイスによるエッジ ポートでのフレーム スタック状況を最小化するために、主に低速ドレイン デバイスに接続されるエッジ ポートで行われます。この閉塞状態を回避するか、最小限に抑えるためには、ポートのフレーム タイムアウトを短縮します。設定されたしきい値を使用して低速ドレインが検出された後に、No-Credit タイムアウトを使用してすべてのパケットをドロップできます。フレーム タイムアウト

値を小さくすることにより、エッジ ポートで実際にタイムアウトになる時間（358 ミリ秒）より早くパケットがドロップされるため、ファブリックに影響する低速ドレイン状態が軽減されます。この機能は、ISL のバッファ領域を解放し、低速ドレイン状態が発生していない他の無関係なフローが使用できるようにします。

（注） この機能は、低速ドレイン デバイスに接続されたエッジ ポートをサポートしています。この機能は ISL にも適用できますが、エッジ F ポートにのみ適用し、ISL はデフォルト設定の E ポートおよび TE ポートのまま維持することを推奨します。この機能は、第 1 世代のモジュールではサポートされません。

スタック フレーム タイムアウト値の設定

デフォルトのスタック フレーム タイムアウト値は 358 ミリ秒です。タイムアウト値は、10 ずつ増やすことができます。ISL ではデフォルト設定を維持し、ファブリック F ポートでは 500 ミリ秒を超えない値（100 ～ 200 ミリ秒）を設定することを推奨します。

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)# **system timeout congestion-drop***seconds***mode E | F**	スタック フレーム タイムアウト値（ミリ秒単位）とスイッチのポート モードを指定します。
ステップ 3	switch(config)# **system timeout congestion-drop default mode E | F**	スイッチのデフォルトのスタック フレーム タイムアウト ポート モードを指定します。

次に、100 ミリ秒のスタック フレーム タイムアウト値を設定する例を示します。

```
switch# configure terminal
switch(config)# system timeout congestion-drop 100 mode F
switch(config)# system timeout congestion-drop default mode F
```

No-Credit タイムアウト値の設定

ポートが設定された期間のクレジットを持たない場合、そのポートで No-Credit タイムアウトをイネーブルにして、そのポートに届くすべてのフレームが出力でドロップされるようにできます。このアクションにより ISL リンクのバッファ領域が解放され、同じリンクを使用する他の無関係のフロー上のファブリックの減速と輻輳を軽減できます。

ドロップされるフレームは、スイッチに到着したばかりである場合もあれば、設定されたタイムアウト値の間スイッチに滞留していた場合もあります。これらのドロップはプリエンプティブで、輻輳を完全にクリアします。

No-Credit タイムアウト機能は、デフォルトではディセーブルです。ISL ではデフォルト設定を維持し、ファブリック F ポートでは 358 ミリ秒を超えない値（200 ～ 300 ミリ秒）を設定することを推奨します。

no system timeout no-credit-drop mode F コマンドを入力することでこの機能をディセーブルにできます。

（注） No-Credit タイムアウト値とスタック フレーム タイムアウト値は相互に関連します。No-Credit タイムアウト値は、常にスタック フレーム タイムアウト値より大きく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**	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)# **system timeout no-credit-drop***seconds***mode F**	スイッチの No-Credit タイムアウト値とポートモードを指定します。*seconds* 値はデフォルトでは 500 ミリ秒です。この値は、100 ずつ増やすことができます。
ステップ 3	switch(config)# **system timeout no-credit-drop default mode F**	スイッチのデフォルトの No-Credit タイムアウト値ポート モードを指定します。

次に、No-Credit タイムアウト値を設定する例を示します。

```
switch# configure terminal
switch(config)# system timeout no-credit-drop 100 mode F
switch(config)# system timeout no-credit-drop default mode F
```

クレジット ロス カウンタの表示

次のコマンドを使用して、最後に指定した分数、時間数、日数のモジュールごと、インターフェイスごとのクレジット ロス カウンタを表示します。

コマンド	目的
show process creditmon {credit-loss-event-history | credit-loss-events | force-timeout-events | timeout-discards-events}	オンボード障害ロギング（OBFL）のクレジット ロス ログを表示します。

クレジット ロス イベントの表示

次のいずれかのコマンドを使用して、最新の 3 つのクレジット ロス タイム スタンプを使用したインターフェイスごとのクレジット ロス イベントの総数を表示します。

コマンド	目的
show process creditmon credit-loss-events [**module***module number*]	モジュールのクレジット ロス イベントの情報を表示します。
show process creditmon credit-loss-event-history [**module***module number*]	クレジット ロス イベントの履歴情報を表示します。

タイムアウト ドロップの表示

次のコマンドを使用して、最後に指定した分数、時間数、日数のモジュールごと、インターフェイスごとのタイムアウト ドロップを表示します。

コマンド	目的
show logging onboard flow-control timeout-drops[**last***mm***minutes**] [**last***hh***hours**] [**last***dd***days**] [**module***module number*]	オンボード障害ロギング（OBFL）のタイムアウト ドロップ ログを表示します。

平均 Credit Not Available ステータスの表示

平均クレジット使用不可時間が設定されたしきい値を超えたときに、ポートのエラーをディセーブルにし、インターフェイスの詳細を備えたトラップを送信し、インターフェイスの詳細を備えた syslog を生成することができます。また、アクションを結合または追加したり、個別のアクションをオンまたはオフにすることができます。ポート モニタ機能は、しきい値およびアクションを設定するためのコマンドライン インターフェイスを提供します。しきい値は、ある間隔に対するクレジット使用不可時間のパーセンテージとして設定できます。

クレジット使用不可時間のしきい値は 0 ～ 100%（10 の倍数）、間隔は 1 秒～ 1 時間に設定できます。デフォルトは 1 秒間に 10 % で、syslog が生成されます。

次のコマンドを使用して、平均 credit-not-available ステータスを表示します。

コマンド	目的
show system internal snmp credit-not-available {**module** | **module-id**}	ポート モニタの credit-not-available カウンタ ログが表示されます。

ポート モニタリング

ポートモニタリングを使用してファブリックデバイスのパフォーマンスをモニタし、低速ドレイン サービスを検出することができます。カウンタをモニタし、ポートガードが有効か無効かに応じて必要なアクションを行うことができます。さまざまなカウンタについてしきい値を設定し、値がしきい値設定を超えた場合にイベントをトリガーできます。ポートのモニタリングにより、しきい値とアクションの設定に使用できるユーザ インターフェイスが提供されます。デフォルトでは、ポート モニタリング ポリシーでポートガードは無効になっています。

2 つのデフォルト ポリシー、default および default slowdrain が snmpd の初期化中に作成されます。スイッチがオンラインになったときに、別のポリシーがその時点でアクティブになっていない場合に default slowdrain ポリシーがアクティブになります。default slowdrain ポリシーは、credit-loss-reco カウンタと tx-credit-not-available カウンタのみをモニタします。

ポリシーを作成すると、アクセス リンクとトランク リンクの両方に作成されます。アクセス リンクは F の値、トランク リンクは E の値を持ちます。

ポート モニタのイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# [**no**] **port-monitor enable**	ポートモニタリング機能をイネーブル（デフォルト）にします。このコマンドの **no** バージョンを使用すると、ポートモニタリング機能がディセーブルになります。

ポート モニタ ポリシーの設定

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。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **port-monitor name***policyname*	ポリシーの名前を指定し、ポート モニタ ポリシー 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-port-monitor)# **port-type all**	すべてのポートに適用します。
ステップ 4	switch(config-port-monitor)# **counter** {**credit-loss-reco** | **timeout-discards** | **tx-credit-not-available** } **poll-interval***seconds* {**absolute** | **delta**} **rising-threshold***value1***event***event-id1***falling-threshold***value2***event***event-id2*	秒単位のポーリング間隔、絶対数のしきい値、次の理由でトリガーされるイベントのイベント ID を指定します。 • credit-loss-reco：クレジット ロスのリカバリ • timeout-discards：タイムアウトの廃棄 • tx-credit-not-available：平均クレジット使用不可時間
ステップ 5	switch(config-port-monitor)# [**no**] **counter** {**credit-loss-reco** | **timeout-discards** | **tx-credit-not-available** } **poll-interval***seconds* {**absolute** | **delta**} **rising-threshold***value1***event***event-id1***falling-threshold***value2***event***event-id2*	指定されたカウンタのモニタをオンにします。 このコマンドの **no** 形式は、指定されたカウンタのモニタをオフにします。

次に、タイムアウトの廃棄のポーリング間隔としきい値を指定する例を示します。

```
switch# configure terminal
switch(config)# port-monitor cisco
switch(config-port-monitor)# counter timeout-discards poll-interval 10
```

次に、クレジット損失のリカバリのポーリング間隔としきい値を指定する例を示します。

```
switch# configure terminal
switch(config)# port-monitor cisco
```

```
switch(config-port-monitor)# counter credit-loss-reco poll-interval 20 delta rising-threshold
 10 event 4 falling-threshold 3 event 4
```

ポート モニタ ポリシーのアクティブ化

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **port-monitor activate***policyname*	指定されたポート モニタ ポリシーをアクティブ化します。
ステップ 3	switch(config)# **port-monitor activate**	（任意） デフォルトのポートモニタポリシーをアクティブ化します。
ステップ 4	switch(config)# **no port-monitor activate***policyname*	（任意） 指定されたポートモニタポリシーを非アクティブ化します。

次の例では、特定のポート モニタ ポリシーをアクティブ化する方法を示します。

```
switch# configure terminal
switch(config)# port-monitor activate cisco
```

ポート モニタ ポリシーの表示

次のコマンドで、ポート モニタ ポリシーを表示できます。

コマンド	目的
switch# **show port-monitor***policyname*	指定したポート モニタ ポリシーの詳細を表示します。

次の例では、特定のポート モニタ ポリシーを表示する方法を示します。

```
switch# show port-monitor cisco

Policy Name  : cisco

Admin status : Active

Oper status  : Active

Port type    : All Ports

--------------------------------------------------------------------------------------------
```

```
Counter                 Threshold  Interval Rising Threshold event Falling Threshold  event
 Portguard     In Use

-------                 ---------  -------- ---------------- ----- ----------------  -----
 ---------     ------

Timeout Discards         Delta      60       200              4     10                 4
   Not enabled   Yes

Credit Loss Reco         Delta      5        4                4     1                  4
   Not enabled   Yes

TX Credit Not Available  Delta      30       60               4     10                 4
   Not enabled   Yes

-----------------------------------------------------------------------------------------
```

FCoE 低速ドレイン デバイスの検出と輻輳回避

Fibre Channel over Ethernet（FCoE）でのエンドデバイス間のデータ トラフィックは、リンク レベルおよび各ホップをベースとしたフロー制御を使用します。低速デバイスがファブリックに接続されている場合、エンドデバイスは、設定されたレートでフレームを受け入れません。低速デバイスの存在がリンクのトラフィック輻輳の原因となります。トラフィックの輻輳は、宛先デバイスに低速ドレインが発生していない場合でも、トラフィックに同一のスイッチ間リンク（ISL）を使用するファブリック内の無関係のフローに影響を与えます。

低速ドレイン デバイスの検出と輻輳回避がサポートされています。機能拡張は、主に低速ドレインデバイスに接続されるエッジポートにあり、エッジポート内の輻輳状態を最小限に抑えます。

低速ドレイン デバイスがネットワーク上で検出されると、エッジ ポートに対するフレーム タイムアウト値を小さな値に設定し、設定したしきい値を使用するすべてのパケットに対しタイムアウト ドロップを強制できます。フレーム タイムアウト値を小さくすることにより、エッジ ポートで実際にタイムアウトになる時間より早くパケットがドロップされるため、ファブリックに影響する低速ドレイン状態が軽減されます。タイムアウト値は、90 ミリ秒、180 ミリ秒、358 ミリ秒、716 ミリ秒、1433 ミリ秒に設定することができます。デフォルトのタイムアウト値は 358 ミリ秒です。この機能は、ISL のバッファ領域を空にし、低速ドレイン状態が発生していない他の無関係なフローが使用できるようにします。

指定されたタイムアウト値の間続いている各一時停止イベントについて、一時停止イベントが Embedded Event Manager（EEM）にパブリッシュされます。EEM はポートあたりの一時停止イベントの数を管理し、しきい値に達したときにポリシー アクションをトリガーします。

新しいしきい値とアクションでデフォルト ポリシーを上書きできます。EEM システム ポリシー _ethpm_slow_drain_edge および _ethpm_slow_drain_core の上書きを試みた場合、デフォルト アクション、デフォルト syslog も表示されます。action err-disable を指定して、この条件が発生する不良ポートを隔離することを推奨します。

EEM システム ポリシーを上書きするためのサンプル出力を次に示します。

```
event manager applet custom_edge_policy override __ethpm_slow_dain_edge
event policy-default count 5 time 360
action 1.0 syslog msg FCoE Slowdrain Policy Was Hit
exit
```

ポーズ フレーム タイムアウト値の設定

ポートのポーズフレームタイムアウト値をイネーブルまたはディセーブルにできます。システムは一時停止状態についてポートを定期的にチェックし、ポートが設定された期間に継続的な一時停止状態にある場合は、ポートのポーズフレームタイムアウトをイネーブルにします。この状況は、出力でドロップされるポートに接続するすべてのフレームで発生します。この機能により ISL リンクのバッファ領域が空になり、同じリンクを使用する他の無関係のフロー上のファブリックの減速と輻輳を軽減できます。

一時停止状態がポートでクリアされたりポートがフラップすると、システムはその特定のポート上のポーズ フレーム タイムアウトをディセーブルにします。

ポーズ フレーム タイムアウトはデフォルトでディセーブルになっています。ISL に対してはデフォルト設定を保持し、エッジ ポートに対してはデフォルト値を超えない値を設定することを推奨します。

低速ドレイン デバイスの動作から迅速にリカバリするには、ポーズ フレーム タイムアウト値を設定する必要があります。それは、フレームが輻輳したタイムアウトのスイッチにあるかどうかにかかわらず、低速ドレインに直面しているエッジ ポート内のすべてのフレームがドロップされるためです。このプロセスにより、ISL 内の輻輳がすぐにクリアされます。輻輳を完全にクリアするには、輻輳フレーム タイムアウト値を設定する代わりにポーズ フレーム タイムアウト値を設定する必要があります。

no system default interface pause timeout milliseconds mode {core | edge} コマンドを使用して、エッジ ポートに対するポーズ フレーム タイムアウト値をディセーブルにします。デフォルトのポーズ タイムアウト値は 358 ミリ秒です。

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# **system default interface pause timeout***milliseconds***mode** {**core** | **edge**}	デバイスに対する新しいポーズフレーム タイムアウト値（ミリ秒）およびポート モードを設定します。
ステップ 3	switch# **system default interface pause mode** {**core** | **edge**}	デバイスに対するデフォルトのポーズフレーム タイムアウト値（ミリ秒）およびポート モードを設定します。
ステップ 4	switch# **no system default interface pause timeout** *milliseconds***mode** {**core** | **edge**}	デバイスに対するポーズフレーム タイムアウトをディセーブルにします。
ステップ 5	switch# **no system default interface pause mode** {**core** | **edge**}	デバイスに対するデフォルトのポーズフレーム タイムアウトをディセーブルにします。

	コマンドまたはアクション	目的
ステップ 6	switch# **show logging onboard flow-control pause-event**	（任意） 1 インターフェイス 1 モジュールごとの一時停止イベントの総数を表示します。
ステップ 7	switch# **show logging onboard flow-control timeout-drop**	（任意） タイムスタンプ情報を使用して1インターフェイス 1 モジュールごとのタイムアウト ドロップを表示します。

次に、ポーズ フレーム タイムアウト値を設定する例を示します。

```
switch# configure terminal
switch(config)# system default interface pause timeout 358 mode core
switch(config)# system default interface pause mode edge
switch(config)# no system default interface pause timeout 358 mode core
switch(config)# no system default interface pause mode edge
switch(config)# end
switch# show logging onboard flow-control pause-event
switch# show logging onboard flow-control timeout-drop
```

次に、スイッチ全体のポーズ イベントの総数を表示する例を示します。

```
switch# show logging onboard flow-control pause-events
List of Pause Events
----------------------------------------------------
Ethernet      Timestamp
Interface
----------------------------------------------------
 1/1          01/01/2009 10:15:20.262951
 1/1          01/01/2009 10:15:21.462869
 1/1          01/01/2009 10:15:22.173349
 1/1          01/01/2009 10:15:22.902929
 1/1          01/01/2009 10:15:23.642984
 1/1          01/01/2009 10:15:24.382961
 1/1          01/01/2009 10:15:25.100497
 1/1          01/01/2009 10:15:25.842915
```

次に、スーパーバイザ CLI に関するタイムスタンプ情報を使用したインターフェイスごとのタイムアウト ドロップを表示する例を示します。

```
switch# show logging onboard flow-control timeout-drops
Number of Pause Events per Port
----------------------------
Ethernet   Number of
Interface  Pause Events
----------------------------
1/1        38668
1/15       232
2/16       2233
2/17       2423
```

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***typeslot*/*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。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
switch# **show interface***typeslot*/*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関してのみ使用可能です。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
switch# **show interface***typeslot*/*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関してのみ使用可能です。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
switch# **show interface brief**	すべてのインターフェイスのステータスが表示されます。
switch# **show interface flowcontrol**	すべてのインターフェイスでフロー制御設定の詳細なリストを表示します。
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。
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することができます。引数を入力せずにこのコマンドを実行すると、スイッチ内に設定されたすべてのインターフェイスの情報が表示されます。

次に、物理イーサネット インターフェイスを表示する例を示します。

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

次に、物理イーサネットの機能を表示する例を示します。

```
switch# show interface ethernet 1/1 capabilities
Ethernet1/1
  Model:                 734510033
  Type:                  10Gbase-(unknown)
  Speed:                 1000,10000
  Duplex:                full
  Trunk encap. type:     802.1Q
  Channel:               yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:           rx-(off/on),tx-(off/on)
  Rate mode:             none
  QOS scheduling:        rx-(6q1t),tx-(1p6q0t)
  CoS rewrite:           no
  ToS rewrite:           no
  SPAN:                  yes
  UDLD:                  yes
  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      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                    Ch #
--------------------------------------------------------------------------------
Eth1/1        200    eth  trunk  up      none                        10G(D) --
Eth1/2        1      eth  trunk  up      none                        10G(D) --
Eth1/3        300    eth  access down    SFP not inserted            10G(D) --
Eth1/4        300    eth  access down    SFP not inserted            10G(D) --
Eth1/5        300    eth  access down    Link not connected         1000(D) --
Eth1/6        20     eth  access down    Link not connected          10G(D) --
Eth1/7        300    eth  access down    SFP not inserted            10G(D) --
...
```

次に、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） 上記の例のとおり、CDP アドバタイズメントのデバイス ID フィールドには、デフォルトでホスト名とシリアル番号が表示されます。

```
switch# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device ID             Local Intrfce   Hldtme  Capability  Platform      Port ID
d13-dist-1              mgmt0           148     S I      WS-C2960-24TC  Fas0/9
n5k(FLC12080012)        Eth1/5          8       S I s    N5K-C5020P-BA  Eth1/5
```

第 2 章

レイヤ 3 インターフェイスの設定

この章の内容は、次のとおりです。

- レイヤ 3 インターフェイスについて，47 ページ
- レイヤ 3 インターフェイスのライセンス要件，51 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，51 ページ
- レイヤ 3 インターフェイスのデフォルト設定，52 ページ
- レイヤ 3 インターフェイスの設定，52 ページ
- レイヤ 3 インターフェイス設定の確認，61 ページ
- レイヤ 3 インターフェイスのモニタリング，63 ページ
- レイヤ 3 インターフェイスの設定例，65 ページ
- レイヤ 3 インターフェイスの関連資料，65 ページ
- レイヤ 3 インターフェイスの MIB，66 ページ
- レイヤ 3 インターフェイスの標準，66 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、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、パケットを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静的 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、デバイスの『Layer 2 Switching Configuration Guide』を参照してください。

ルーテッド インターフェイスからレイヤ 3 ポート チャネルも作成できます。

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

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

サブインターフェイス

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

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

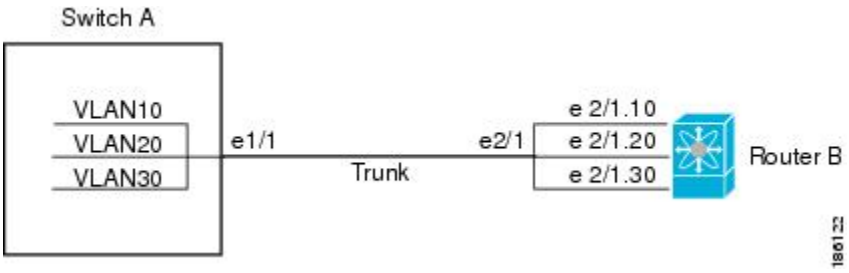
サブインターフェイスの名前は、親インターフェイスの名前（たとえば Ethernet 2/1）+ ピリオド（.）+そのインターフェイス独自の番号です。たとえば、イーサネット インターフェイス 2/1 に Ethernet 2/1.1 というサブインターフェイスを作成できます。この場合、.1 はそのサブインターフェイスを表します。

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

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

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

設定の前に VLAN ネットワーク インターフェイス機能をイネーブルにする必要があります。システムはこの機能をディセーブルにする前のチェックポイントを自動的に取得するため、このチェックポイントにロールバックできます。ロールバックとチェックポイントの詳細については、デバイスの『System Management Configuration Guide』を参照してください。

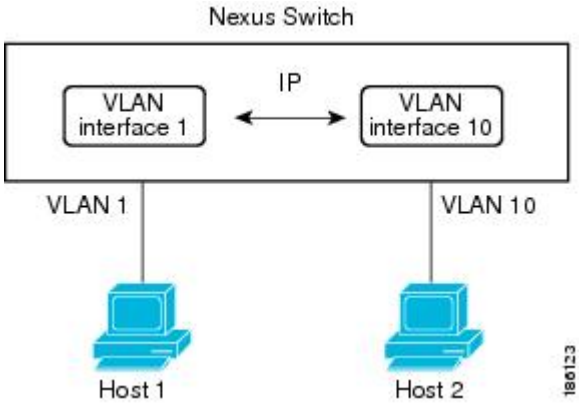
（注） VLAN 1 の VLAN インターフェイスは削除できません。

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

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

信させることができます。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。

プライベート VLAN での IP アドレッシング方式

それぞれのカスタマーに別々の VLAN を割り当てると、次のように非効率的な IP アドレス指定方式が作成されます。

- カスタマー VLAN にアドレスのブロックを割り当てると、未使用 IP アドレスが発生することがあります。
- VLAN におけるデバイス数が増加する場合、割り当て済みアドレス数が増加に対応できるだけ十分に大きくないことがあります。

この問題は、プライベート VLAN を使用すると軽減します。プライベート VLAN では、プライベート VLAN のすべてのメンバーが、プライマリ VLAN に割り当てられている共通アドレス空間を共有するためです。ホストはセカンダリ VLAN に接続され、プライマリ VLAN に割り当てられているアドレスのブロックから IP アドレスが DHCP サーバによってホストに割り当てられます

が、同一プライマリ VLAN 内のセカンダリ VLAN には割り当てられません。さまざまなセカンダリ VLAN のカスタマー デバイスには後続 IP アドレスが割り当てられます。新しいデバイスを追加すると、サブネットアドレスの巨大プールから次に使用できるアドレスが、DHCP サーバによって割り当てられます。

レイヤ3インターフェイスのライセンス要件

レイヤ3ライセンスのインストール後、次のガイドラインと制限事項がデバイスに適用されます。

- イン サービス ソフトウェア アップグレード（ISSU）はサポートされません。
- 一時的なレイヤ3機能ライセンスはサポートされていません（レイヤ3ベース サービス パッケージのライセンスの猶予期間は 0 です）。
- 管理スイッチ仮想インターフェイス（SVI）は、レイヤ3ベース サービス パッケージ ライセンスなしでサポートされ、ISSU は設定された管理 SVI で実行できます。
- レイヤ 3 ベース サービス パッケージ ライセンスがインストールされていない場合、すべての SVI（管理キーワードが設定されているかどうかにかかわらず）が動作上アップ状態です。レイヤ 3 ベース サービス パッケージ機能ライセンスのインストール後、ルーティングされた SVI は動作上いったんダウンにされた後、アップに戻されます。このリロードは、ルーティングされた SVI がレイヤ 3 ベース サービス パッケージ機能ライセンスのインストール前の管理 SVI のように動作し、ハードウェアに保存されたインターフェイス状態が転送情報ベース（FIB）の SVI ルートのプログラミングに続いてクリアされる必要があるためです。
- レイヤ 3 ライセンスをクリアした後、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、デバイスをリロードする必要があります。続いて、無停止で ISSU を実行できます。
- レイヤ 3 ライセンスをクリアした後、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、デバイスをリロードする必要があります。続いて、無停止で ISSU を実行できます。
- レイヤ 3 ライセンスをクリアする前に HSRP および VRRP を消去する必要はありませんが、それらのコンフィギュレーションもクリアすることを推奨します。
- VRRP と HSRP はレイヤ 3 ライセンスなしで設定できますが、レイヤ 3 ライセンスなしでは動作しません。それらが設定されている場合、無停止での ISSU はサポートされません。

レイヤ3インターフェイスの注意事項および制約事項

レイヤ 3 インターフェイスの設定には次の注意事項と制約事項があります。

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

- レイヤ 2 インターフェイスをレイヤ 3 インターフェイスに変更する場合、Cisco NX-OS はインターフェイスをシャットダウンしてインターフェイスを再度イネーブルにし、レイヤ 2 固有の設定をすべて削除します。
-
- Cisco Nexus 5500 シリーズ スイッチは、59 台のレイヤ 3 物理インターフェイスのみをサポートしています。

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。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 3	switch(conifg-if)# **no switchport**	インターフェイスをレイヤ 3 インターフェイスとして設定し、このインターフェイス上のレイヤ 2 固有の設定を削除します。 （注） レイヤ 3 インターフェイスを元のレイヤ 2 インターフェイスに変換するには、**switchport** コマンドを使用します。
ステップ 4	switch(config-if)# [**ip**|**ipv6**]*ip-address/length*	このインターフェイスの IP アドレスを設定します。
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。

	コマンドまたはアクション	目的
		（注） デフォルト設定は broadcast であり、この設定はどの **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、変更を継続的に保存します。

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 コンフィギュレーションにコピーして、変更を継続的に保存します。
ステップ 2	switch(config)# **interface ethernet** *slot/port.number*	インターフェイス コンフィギュレーション モードを開始します。*slot* の範囲は 1 ～ 255 です。*port* の範囲は 1 ～ 128 です。

	コマンドまたはアクション	目的
		（注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# [**ip** | **ipv6**] **address** *ip-address/length*	このインターフェイスの IP アドレスを設定します。
ステップ 4	switch(config-if)# **encapsulation dot1Q** *vlan-id*	サブインターフェイス上の IEEE 802.1Q VLAN カプセル化を設定します。*vlan-id* の範囲は 2 ～ 4093 です。
ステップ 5	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 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、変更を継続的に保存します。

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	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。*slot* の範囲は 1 ～ 255 です。*port* の範囲は 1 ～ 128 です。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。

	コマンドまたはアクション	目的
ステップ 3	switch(conifg-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。 • *value*：帯域幅のサイズ（KB 単位）。指定できる範囲は 1 ～ 10000000 です。 • **inherit**：このインターフェイスのすべてのサブインターフェイスが、帯域幅の値（値が指定されている場合）または親インターフェイスの帯域幅（値が指定されていない場合）のどちらかを継承することを示します。
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、変更を継続的に保存します。

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。
ステップ 3	switch(config)# **interface vlan** *number*	VLANインターフェイスを作成します。*number* の有効範囲は 1 ～ 4094 です。

	コマンドまたはアクション	目的
ステップ 4	switch(config-if)# [**ip** | **ipv6**] **address** *ip-address/length*	このインターフェイスの IP アドレスを設定します。
ステップ 5	switch(config-if)# **no shutdown**	インターフェイスを管理上アップさせます。
ステップ 6	switch(config-if)# **show interface vlan** *number*	（任意） VLAN インターフェイスの統計情報を表示します。*number* の有効範囲は 1 ～ 4094 です。
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、変更を継続的に保存します。

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
```

プライマリ VLAN のレイヤ 3 VLAN インターフェイスへのセカンダリ VLAN のマッピング

セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングして、プライベート VLAN 入力トラフィックのレイヤ 3 スイッチングを可能にするには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	Router(config)#**interface-vlan***primary_vlan_ID*	プライマリ VLAN 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。

	コマンドまたはアクション	目的
		（注） 独立 VLAN およびコミュニティ VLAN は、ともにセカンダリ VLAN と呼ばれます。
ステップ 2	Router(config-if)# **private-vlan mapping** {*secondary_vlan_list*|**add***secondary_vlan_list*|**remove***secondary_vlan_list*}	セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングして、プライベート VLAN 入力トラフィックのレイヤ 3 スイッチングを可能にします。 セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングする際は、次の情報に注意してください。 • **private-vlan mapping** インターフェイス コンフィギュレーション コマンドは、レイヤ 3 スイッチングされるプライベート VLAN 入力トラフィックにのみ影響します。 • *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート

	コマンドまたはアクション	目的
		VLAN ID、またはハイフンで連結したプライベート VLAN ID の範囲です。 • セカンダリ VLAN をプライマリ VLAN にマッピングするには、*secondary_vlan_list* パラメータを入力するか、*secondary_vlan_list* パラメータに **add** キーワードを使用します。 • セカンダリ VLAN とプライマリ VLAN のマッピングを解除するには、**remove** キーワードを指定した *secondary_vlan_list* を使用します。
ステップ 3	Router(config-if)# **no private-vlan mapping**	セカンダリ VLAN とプライマリ VLAN の間のマッピングを消去します。
ステップ 4	Router(config-if)# **end**	設定モードを終了します。
ステップ 5	Router **show interface private-vlan mapping**	設定を確認します。

次に、プライベート VLAN 303 ～ 307、309、および 440 からのセカンダリ VLAN 入力トラフィックのルーティングを許可して、設定を確認する例を示します。

```
Router# configure terminal
 Router(config)# interface vlan 202
 Router(config-if)# private-vlan mapping add 303-307,309,440
```

```
Router(config-if)# end
Router# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan202   303            community
vlan202   304            community
vlan202   305            community
vlan202   306            community
vlan202   307            community
vlan202   309            community
vlan202   440            isolated
Router#
```

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** *instance*	ループバック インターフェイスを作成します。*instance* の範囲は 0 ～ 1023 です。
ステップ 3	switch(config-if)# [**ip** | **ipv6**] **address** *ip-address/length*	このインターフェイスの IP アドレスを設定します。
ステップ 4	switch(config-if)# **show interface loopback** *instance*	（任意） ループバック インターフェイスの統計情報を表示します。*instance* の範囲は 0 ～ 1023 です。
ステップ 5	switch(config-if)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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(conifg-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**]*ip-address/length*	このインターフェイスの IP アドレスを設定します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。
ステップ 5	switch(config-if)# **show vrf** [*vrf-name*] **interface***interface-typenumber*	（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、変更を継続的に保存します。

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。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
show interface ethernet*slot/port***status**	レイヤ 3 インターフェイスの管理ステータス、ポート モード、速度、およびデュプレックスを表示します。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。

コマンド	目的
show interface ethernet*slot/port***.***number*	サブインターフェイスの設定情報、ステータス、カウンタ（インバウンドおよびアウトバウンド パケット レートおよびバイト レートが 5 分間に指数関数的に減少した平均値を含む）を表示します。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
show interface port-channel *channel-id***.***number*	ポート チャネル サブインターフェイスの設定情報、ステータス、カウンタ（インバウンドおよびアウトバウンド パケット レートおよびバイト 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*number*	ループバック インターフェイスの設定情報、ステータス、カウンタを表示します。
show interface loopback*number***brief**	ループバック インターフェイスの動作ステータスを表示します。
show interface loopback*number***description**	ループバック インターフェイスの説明を表示します。
show interface loopback*number***status**	ループバック インターフェイスの管理ステータスおよびプロトコル ステータスを表示します。
show interface vlan*number*	VLAN インターフェイスの設定情報、ステータス、カウンタを表示します。
show interface vlan*number***brief**	VLAN インターフェイスの動作ステータスを表示します。
show interface vlan*number***description**	VLAN インターフェイスの説明を表示します。
show interface vlan*number***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*number***status**	VLAN インターフェイスの管理ステータスおよびプロトコル ステータスを表示します。

レイヤ 3 インターフェイスのモニタリング

次のいずれかのコマンドを使用して、機能に関する統計情報を表示します。

コマンド	目的
show interface ethernet*slot*/*port***counters**	レイヤ 3 インターフェイスの統計情報を表示します（ユニキャスト、マルチキャスト、ブロードキャスト）。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
show interface ethernet*slot*/*port***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。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
show interface ethernet*slot*/*port***counters detailed** [**all**]	レイヤ 3 インターフェイスの統計情報を表示します。オプションとして、32 ビットと 64 ビットのパケットおよびバイトカウンタ（エラーを含む）をすべて含めることができます。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
show interface ethernet*slot*/*port***counters error**	レイヤ 3 インターフェイスの入力および出力エラーを表示します。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
show interface ethernet*slot*/*port***counters snmp**	SNMP MIB から報告されたレイヤ 3 インターフェイス カウンタを表示します。これらのカウンタはクリアできません。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。

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

レイヤ 3 インターフェイスの設定例

次に、イーサネット サブインターフェイスを設定する例を示します。

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

次に、VLAN インターフェイスを設定する例を示します。

```
switch# configuration terminal
switch(config)# interface vlan 100
switch(config-if)# 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

関連項目	マニュアル タイトル
コマンド構文	コマンド構文の詳細については、ご使用のデバイスのコマンドリファレンスを参照してください。
IP	ご使用のデバイスの『Unicast Routing Configuration Guide』の「Configuring IP」の章
VLAN	『Layer 2 Switching Configuration Guide』の「Configuring VLANs」の章

レイヤ 3 インターフェイスの MIB

MIB	MIB Link
IF-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 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 3 章

BFD の設定

この章の内容は、次のとおりです。

- BFD の概要，67 ページ
- BFD のライセンス要件，70 ページ
- 前提条件，70 ページ
- 注意事項と制約事項，71 ページ
- BFD のデフォルト設定，72 ページ
- BFD の設定，73 ページ
- BFD 設定の確認，95 ページ
- BFD のモニタ，95 ページ
- BFD の設定例，96 ページ
- 関連資料，96 ページ
- 関連の標準，97 ページ

BFD の概要

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

BFD では、レイヤ 3 Hello メッセージの隣接検出を単一プロセスにオフロードすることによってすべてのルーティングおよびコントロール プレーンの CPU 使用率を低くします。BFD プロセスはすべてのアプリケーションに対して均等に実行され、1 秒未満の間隔で障害を検出します。

fabricpath インターフェイスには、BFD グローバル コンフィギュレーション コマンドが使用できます。`config-farbicpath-isis` コマンド モードの **bfd** キーワードは、すべての FabricPath インターフェイスで BFD をイネーブルにします。インターフェイス固有のコマンドは、グローバル値を上書きします。

FabricPath BFD では、fabricpath-isis がクライアントです。FabricPath-ISIS は、機能セット fabricpath の一部です。

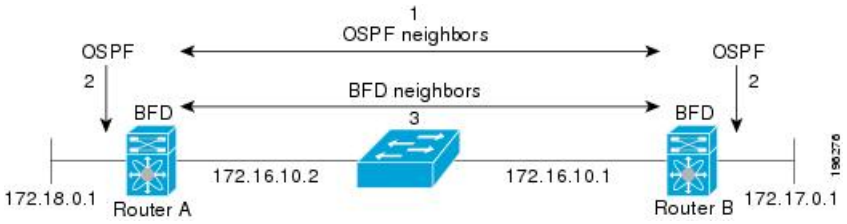
非同期モード

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

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

次の図は、BFD セッションがどのように確立されているかを示します。この図は、Open Shortest Path First（OSPF）と BFD を実行する 2 台のルータがある単純なネットワークを示します。OSPF がネイバーを検出すると（1）、OSPF 隣接ルータで BFD ネイバー セッションを開始する要求が、ローカル BFD プロセスに送信されます（2）。OSPF ネイバー ルータとの BFD ネイバー セッションが確立されました（3）。

図 *4*：*BFD* ネイバー関係の確立



障害検出

BFD セッションが確立され、タイマー ネゴシエーションが終了すると、BFD ネイバーは、より速い速度の場合を除き IGP Hello プロトコルと同じ動作をする BFD 制御パケットを送信し、活性度

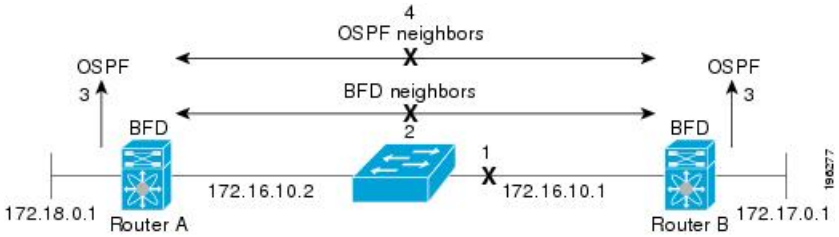
を検出します。BFD は障害を検出しますが、プロトコルが障害の発生したピアをバイパスするための処置を行う必要があります。

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

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

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

図 *5*：*OSPF* ネイバー関係の解除



BFD エコー機能

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

エコー機能は BFD ネイバーの両方がエコー機能を実行しているときに非対称です。

（注） ユニキャスト リバース パス転送チェック（uRPF）はデフォルトではディセーブルです。これを BFD のあるインターフェイス機能でイネーブルにする必要がある場合は、BFD エコー機能がディセーブルになっている必要があります。

セキュリティ

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

BFD パケットの SHA-1 認証を設定できます。

仮想化のサポート

BFD は、仮想ルーティングおよび転送（VRF）インスタンスをサポートします。

BFD のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	BFD には、LAN Base Services ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『*Cisco NX-OS Licensing Guide*』を参照してください。

前提条件

BFD には、次の前提条件があります。

- BFD 機能をイネーブルにする必要があります。BFD 機能のイネーブル化, （73 ページ）を参照してください。
- BFD をイネーブルにする任意のクライアント プロトコルでは、そのクライアント プロトコルの BFD をイネーブルにします。ルーティング プロトコルに対する BFD サポートの設定, （83 ページ）を参照してください。
- Cisco Nexus 5548 および Cisco Nexus 5596 プラットフォームの BFD レイヤ 3 インターフェイスで ICMPv4 および ICMPv6 リダイレク トメッセージをディセーブルにします。
- 設定作業とともに一覧表示されているその他の詳細な前提条件を参照してください。

注意事項と制約事項

BFD では、Cisco Nexus 5500 シリーズ スイッチについて次の注意事項と制約事項があります。

- BFD は BFD バージョン 1 をサポートします。
- BFD は IPv4 をサポートします。
- BFD は、シングルホップ BFD をサポートします。
- BFD は Border Gateway Protocol（BGP）をサポートします。
- BGP の BFD は、シングル ホップ External Border Gateway Protocol（EBGP）および internal Border Gateway Protocol（iBGP）ピアをサポートします。
- BFD は、Enhanced Interior Gateway Routing Protocol（EIGRP）をサポートします。
- BFD は、Open Shortest Path First（OSPF）ルーティング プロトコルをサポートします。
- BFD は、キー付き SHA-1 認証をサポートします。
- BFD は、物理インターフェイス、ポート チャネル、サブインターフェイス、および VLAN インターフェイスのレイヤ 3 インターフェイスをサポートします。
- BFD はレイヤ 3 隣接情報に応じて、レイヤ 2 のトポロジ変更を含むトポロジ変更を検出します。レイヤ 3 隣接情報が使用できない場合、VLAN インターフェイス（SVI）の BFD セッションはレイヤ 2 トポロジのコンバージェンス後に稼働しない可能性があります。
- ポート チャネル設定の制限は次のとおりです。
  - BFD で使用されるレイヤ 3 ポート チャネルでは、ポート チャネルの Link Aggregation Control Protocol（LACP）をイネーブルにする必要があります。
  - SVI のセッションで使用されるレイヤ 2 ポート チャネルでは、ポート チャネルの LACP をイネーブルにする必要があります。
- BFD は、仮想ポート チャネル（vPC）、vPC ピア リンク、および FabricPath リンク全体に形成されている SVI インターフェイス上でサポートされます。
- SVI の制限は次のとおりです。
  - ASIC をリセットすると、別のポートのトラフィックの中断の原因となり、別のポートの SVI セッションがフラップする原因となる可能性があります。
  - トポロジを変更すると（たとえば、VLAN へのリンクを追加または削除するとき、またはレイヤ 2 ポート チャネルからのメンバーを削除するとき）、SVI セッションが影響を受ける場合があります。SVI セッションはダウンした後、トポロジディスカバリの終了後に起動する場合があります。

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

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

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

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

BFD のデフォルト設定

次の表に、BFD パラメータのデフォルト設定を示します。

パラメータ	デフォルト
BFD 機能	ディセーブル
必要最小受信間隔	250 ミリ秒
目的の最小送信間隔	250 ミリ秒
検出乗数	3
エコー機能	イネーブル
モード	非同期
ポート チャネル	論理モード（送信元/宛先ペアのアドレスごとに 1 セッション）
slow timer	2000 ミリ秒
サブインターフェイスの最適化	ディセーブル

BFD の設定

BFD 設定階層

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

ポート チャネルのメンバーである物理ポートについては、メンバー ポートはマスター ポート チャネルの BFD 設定を継承します。メンバー ポート サブインターフェイスは、サブインターフェイスの最適化がイネーブルになっていない限りマスター ポート チャネルの BFD 設定より優先することができます。

BFD 設定のタスク フロー

手順

ステップ 1 BFD 機能をイネーブルにします。

ステップ 2 インターフェイス上に、グローバルな BFD パラメータを設定するかまたは BFD を設定します。

ステップ 3 ルーティング プロトコルをサポートする BFD を設定します。

BFD 機能のイネーブル化について

BFD 機能のイネーブル化

はじめる前に

デバイス VRF 内のインターフェイスおよびプロトコルで BFD を設定する前に、BFD 機能をイネーブルにする必要があります。

（たとえば、OSPF または BGP に対して）プロトコル グローバル レベルで BFD を変更するときに正しい VRF を使用しているかどうかを確認します。

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)# **feature bfd**	BFD をイネーブルにします。
ステップ 3	switch(config)# **show feature | include bfd**	（任意） イネーブルおよびディセーブルにされた機能を表示します。
ステップ 4	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、変更を継続的に保存します。

次に、BFD をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature bfd
switch(config)# show feature | include bfd
switch(config)# copy running-config startup-config
```

グローバル BFD パラメータの設定について

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

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

グローバルな BFD パラメータの設定

はじめる前に

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

インターフェイスでグローバルなセッション パラメータを上書きするには、インターフェイスでの BFD の設定, （76 ページ）を参照してください。

正しい VRF を使用していることを確認します。

BFD 機能をイネーブルにします。BFD 機能のイネーブル化, （73 ページ）を参照してください。

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)# **bfd** [**fabricpath**] **interval***mintx***min_rx***msec***multiplier***value*	デバイスのすべての BFD セッションの BFD セッション パラメータを設定します。インターフェイスで BFD セッション パラメータを設定することにより、これらの値を無効にすることができます。fabricpath BFD セッションのグローバル パラメータを設定するには、オプションの **fabricpath** キーワードを使用します。*mintx* および **min_rx***msec* の範囲は 250 ～ 999 ミリ秒で、デフォルトは 250 です。**multiplier***value* の範囲は、3 ～ 50 です。乗数のデフォルトは 3 です。
ステップ 3	switch(config)# **bfd** [**fabricpath**] **slow-timer** [*milliseconds*]	エコー機能で使用される slow timer を設定します。この値はエコー機能がイネーブルの場合、BFD が新しいセッションを開始する速度および非同期セッションが BFD 制御パケットに使用する速度を決定します。slow-timer 値は新しい制御パケット間隔として使用されますが、エコーパケットは設定された BFD 間隔を使用します。エコーパケットはリンク障害検出に使用されますが、低速の制御パケットは BFD セッションを維持します。指定できる範囲は 1000 ～ 30000 ミリ秒です。デフォルトは 2000 です。
ステップ 4	switch(config)# **bfd echo-interface loopback***interface number*	BFD のエコーフレームに使用するインターフェイスを設定します。このコマンドは、指定されたループバック インターフェイスで設定されるアドレスに、エコーパケットの送信元アドレスを変更します。指定できるインターフェイス番号の範囲は 0 ～ 1023 です。
ステップ 5	switch(config)# **show running-config bfd**	（任意） BFD の実行コンフィギュレーションを表示します。
ステップ 6	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、変更を継続的に保存します。

	コマンドまたはアクション	目的

次に、グローバル BFD パラメータを設定する例を示します。

```
switch# configure terminal
switch(config)# bfd interval 250 min_rx 250 multiplier 3
switch(config)# bfd slow-timer 2000
switch(config)# bfd echo-interface loopback 1 3
switch(config-if)# show running-config bfd
switch(config-if)# copy running-config startup-config
```

インターフェイスでの BFD の設定について

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

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

インターフェイスでの BFD の設定

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

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

（注） fabricpath モードのインターフェイスで **bfd** [**fabricpath**] コマンドを使用することができます。fabricpath モードをイネーブルにするには、インターフェイスが **switchport mode fabricpath** を使用して設定されている必要があります。

はじめる前に

正しい VRF を使用していることを確認します。

BFD 機能をイネーブルにします。BFD 機能のイネーブル化, （73 ページ）を参照してください。

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***int-if*	インターフェイス コンフィギュレーション モードを開始します。? キーワードを使用し

	コマンドまたはアクション	目的
		て、サポートされるインターフェイスを表示します。
ステップ 3	switch(config-if)# **bfd** [**fabricpath**]	インターフェイス レベルで fabricpath BFD をイネーブルにします。
ステップ 4	switch(config-if)# **bfd** [**fabricpath**] **interval***mintx***min_rx***msec***multiplier***value*	インターフェイスのすべての BFD セッションの BFD セッション パラメータを設定します。この値はグローバルな BFD セッション パラメータより優先されます。fabricpath BFD セッションのグローバル パラメータを設定するには、オプションの **fabricpath** キーワードを使用します。*mintx* および *msec* の範囲は 50 ～ 999 ミリ秒で、デフォルトは 250 です。乗数の範囲は 3 ～ 50 です。乗数のデフォルトは 3 です。
ステップ 5	switch(config-if)# **bfd** [**fabricpath**] **authenticationkeyed-SHA1 key-id** *id* {**hex-key***hex-key* | **key***ascii-key* }	（任意） インターフェイスですべての BFD セッションの SHA-1 認証を設定します。*ascii_key* 文字列は BFD ピア間で共有される秘密キーです。0 ～ 255 の数値の *id* 値が、この特定の *ascii_key* に割り当てられます。BFD パケットは、複数のアクティブ キーの使用を許可する ID でキーを指定します。インターフェイスの SHA-1 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 6	switch(config-if)# **show running-config bfd**	（任意） BFD の実行コンフィギュレーションを表示します。
ステップ 7	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、変更を継続的に保存します。

次に、インターフェイスで BFD を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# bfd interval 250 min_rx 250 multiplier 3
switch(config-if)# bfd authentication keyed-SHA1 key-id 1 key cisco123
switch(config-if)# show running-config bfd
switch(config-if)# copy running-config startup-config
```

ポート チャネルの BFD の設定について

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

この設定は、設定されたポートチャネルのグローバルセッションパラメータより優先されます。ポート チャネルのメンバー ポートはメンバー ポートのサブインターフェイス レベルで BFD パラメータを設定しない限り、ポート チャネルの BFD セッション パラメータを継承します。その場合、サブインターフェイス最適化がイネーブルにされていなければ、メンバー ポート サブインターフェイスはサブインターフェイス BFD コンフィギュレーションを使用します。詳細については、「サブインターフェイスの BFD の最適化」を参照してください。

ポート チャネルの BFD の設定

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

この設定は、設定されたポートチャネルのグローバルセッションパラメータより優先されます。ポート チャネルのメンバー ポートはメンバー ポートのサブインターフェイス レベルで BFD パラメータを設定しない限り、ポート チャネルの BFD セッション パラメータを継承します。その場合、サブインターフェイス最適化がイネーブルにされていなければ、メンバー ポート サブインターフェイスはサブインターフェイス BFD コンフィギュレーションを使用します。詳細については、サブインターフェイスの BFD の最適化, （82 ページ）を参照してください。

はじめる前に

正しい VRF を使用していることを確認します。

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

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」を参照してください。

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 port-channel***number*	ポート チャネル コンフィギュレーション モードを開始します。?キーワードを使用して、サポートされる数値の範囲を表示します。
ステップ 3	switch(config-if)# **bfd** [**fabricpath**] **interval***mintx***min_rx***msec***multiplier***value*	（任意） ポート チャネルのすべての BFD セッションの BFD セッション パラメータを設定します。この値はグローバルな BFD セッション パラメータより優先されます。fabricpath BFD セッションのグローバル パラメータを設定するには、オプションの **fabricpath** キーワードを使用します。*mintx* および **min_rx***msec* の範囲は 250 ～ 999 ミリ秒で、デフォルトは 250 です。乗数の範囲は 1 ～ 50 です。乗数のデフォルトは 3 です。
ステップ 4	switch(config-if)# **bfd** [**fabricpath**] **authenticationkeyed-SHA1 key-id** *id* {**hex-key***hex-key* | **key***ascii-key* }	（任意） インターフェイスですべての BFD セッションの SHA-1 認証を設定します。*ascii_key* 文字列は BFD ピア間で共有される秘密キーです。0 ～ 255 の数値の *id* 値が、この特定の *ascii_key* に割り当てられます。BFD パケットは、複数のアクティブ キーの使用を許可する ID でキーを指定します。インターフェイスの SHA-1 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 5	switch(config-if)# **show running-config bfd**	（任意） BFD の実行コンフィギュレーションを表示します。
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、変更を継続的に保存します。

次に、ポート チャネルに BFD を設定する例を示します。

```
switch# configure terminal
switch(config)# interface port-channel 2
switch(config-if)# bfd interval 250 min_rx 250 multiplier 3
switch(config-if)# bfd authentication keyed-SHA1 key-id 1 key cisco123
switch(config-if)# show running-config bfd
switch(config-if)# copy running-config startup-config
```

BFD エコー機能の設定について

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

（注） BFD エコーは、fabricpath インターフェイスではイネーブルにできません。

BFD エコー機能の設定

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

fabricpath モードでデフォルト VLAN（VLAN 1）が設定されている場合は、任意の VLAN に属する任意のポートで fabricpath（L2）BFD セッションを設定することができます。起動する fabricpath BFD セッションのデフォルト VLAN 1 が fabricpath モードであることが必要です。

（注） エコー モードは、fabricpath インターフェイスではサポートされません。

はじめる前に

正しい VRF を使用していることを確認します。

BFD 機能をイネーブルにします。BFD 機能のイネーブル化, （73 ページ）を参照してください。

BFD セッション パラメータを設定します。グローバルな BFD パラメータの設定, （74 ページ）またはインターフェイスでの BFD の設定, （76 ページ）を参照してください。

ICMP のリダイレクト メッセージが BFD 対応インターフェイスでディセーブルであることを確認します。インターフェイスで **no ip redirects** コマンドまたは **no ipv6 redirects** コマンドを使用します。

同一の送信元アドレスおよび宛先アドレスを調べる IP パケット検証チェックがディセーブルになっていることを確認します。

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)# **bfd** [**fabricpath**] **slow-timer**[*milliseconds*]	エコー機能で使用される slow timer を設定します。この値は BFD が新しいセッションを開始する速度を決定し、BFD エコー機能がイネーブルの場合に非同期セッションの速度を低下させるために使用されます。この値は、エコー機能がイネーブルの場合、必要最小受信間隔より優先されます。指定できる範囲は 1000 ～ 30000 ミリ秒です。デフォルトは 2000 です。
ステップ 3	switch(config)# **interface** *int-if*	インターフェイス コンフィギュレーション モードを開始します。? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 4	switch(config-if)# **bfd echo**	エコー機能をイネーブルにします。デフォルトではイネーブルになっています。
ステップ 5	switch(config-if)# **show running-config bfd**	（任意） BFD の実行コンフィギュレーションを表示します。
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、変更を継続的に保存します。

次に、BFD エコー機能を設定する例を示します。

```
switch# configure terminal
switch(config)# bfd slow-timer 2000
switch(config)# interface ethernet 2/1
switch(config-if)# bfd echo
switch(config-if)# show running-config bgp
switch(config-if)# copy running-config startup-config
```

サブインターフェイスの BFD の最適化について

サブインターフェイスでBFDを最適化できます。BFDにより、設定されているすべてのサブインターフェイスのセッションが作成されます。BFD により、設定されている最小の VLAN ID を持つサブインターフェイスがマスター サブインターフェイスとして設定され、そのサブインターフェイスは親インターフェイスのBFDセッションパラメータを使用します。残りのサブインターフェイスは slow timer を使用します。最適化されたサブインターフェイス セッションでエラーが

検出されると、BFD により、その物理インターフェイスのすべてのサブインターフェイスがダウンとマークされます。

サブインターフェイスの BFD の最適化

サブインターフェイスでBFDを最適化できます。BFDにより、設定されているすべてのサブインターフェイスのセッションが作成されます。BFD により、設定されている最小の VLAN ID を持つサブインターフェイスがマスター サブインターフェイスとして設定され、そのサブインターフェイスは親インターフェイスのBFDセッション パラメータを使用します。残りのサブインターフェイスは slow timer を使用します。最適化されたサブインターフェイス セッションでエラーが検出されると、BFD により、その物理インターフェイスのすべてのサブインターフェイスがダウンとマークされます。

はじめる前に

正しい VRF を使用していることを確認します。

BFD 機能をイネーブルにします。BFD 機能のイネーブル化, （73 ページ）を参照してください。

BFD セッション パラメータを設定します。グローバルな BFD パラメータの設定, （74 ページ）またはインターフェイスでの BFD の設定, （76 ページ）を参照してください。

これらのサブインターフェイスが別の Cisco NX-OS デバイスに接続するようにしてください。この機能は、Cisco NX-OS でだけサポートされます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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***int-if*	インターフェイス コンフィギュレーション モードを開始します。? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 3	switch(config-if)# **bfd optimize subinterface**	BFD 対応インターフェイスのサブインターフェイスを最適化します。デフォルトではディセーブルになっています。
ステップ 4	switch(config-if)# **show running-config bfd**	（任意） BFD の実行コンフィギュレーションを表示します。
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、変更を継続的に保存します。

次の例では、インターフェイスで BFD を最適化する方法を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# bfd optimize subinterface
switch(config-if)# show running-config bfd
switch(config-if)# copy running-config startup-config
```

ルーティング プロトコルに対する BFD サポートの設定

Cisco Nexus 5500 では、以下のルーティング プロトコルの BFD サポートを提供しています。

- Border Gateway Protocol（BGP）
- Enhanced Interior Gateway Routing Protocol（EIGRP）
- Open Shortest Path First バージョン 2（OSPFv2）
- ホットスタンバイ ルータ プロトコル（HSRP）
- 仮想ルータ冗長プロトコル（VRRP）
- スタティック ルート
- プロトコル独立型マルチキャスト（PIM）
- Intermediate System to Intermediate System（IS-IS）の FabricPath

BGP 上での BFD の設定について

Border Gateway Protocol（BGP）の BFD を設定できます。

BGP での BFD の設定

Border Gateway Protocol（BGP）の BFD を設定できます。

はじめる前に

BFD 機能をイネーブルにします。BFD 機能のイネーブル化，（73 ページ）を参照してください。

BFD セッション パラメータを設定します。グローバルな BFD パラメータの設定，（74 ページ）またはインターフェイスでの BFD の設定，（76 ページ）を参照してください。

BGP 機能をイネーブルにします。

詳細については、『*Cisco Nexus 5500 Switch NX-OS Unicast Routing Configuration Guide, Release 6.x*』を参照してください。

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)# **router bgp***as-number*	BGP をイネーブルにして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。
ステップ 3	switch(config-router)# **neighbor** {*ip-address*} **remote-as***as-number*	リモート BGP ピアの IPv4 アドレスおよび AS 番号を設定します。*ip-address* の形式は x.x.x.x です。
ステップ 4	switch(config-router-neighbor)# **bfd**	この BGP ピアの BFD をイネーブルにします。
ステップ 5	switch(config-router-neighbor)# **update-source** *interface-type number*	この BGP ピアに対する BFD を起動します。
ステップ 6	switch(config-router-neighbor)# **show running-config bgp**	（任意） BGP の実行コンフィギュレーションを表示します。
ステップ 7	switch(config-router-neighbor)# **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、変更を継続的に保存します。

次に、BGP 上で BFD を設定する例を示します。

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router)# neighbor 209.165.201.1 remote-as 64497
switch(config-router-neighbor)# bfd
switch(config-router-neighbor)# update-source ethernet 2/1
switch(config-router-neighbor)# show running-config bgp
switch(config-router-neighbor)# copy running-config startup-config
```

EIGRP 上での BFD の設定について

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

EIGRP 上での BFD の設定

はじめる前に

正しい VRF を使用していることを確認します。

BFD 機能をイネーブルにします。BFD 機能のイネーブル化, （73 ページ）を参照してください。

BFD セッション パラメータを設定します。グローバルな BFD パラメータの設定, （74 ページ）またはインターフェイスでの BFD の設定, （76 ページ）を参照してください。

EIGRP 機能をイネーブルにします。

詳細については、『*Cisco Nexus 5500 Switch NX-OS Unicast Routing Configuration Guide, Release 6.x*』を参照してください。

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)# **router eigrp***instance-tag*	インスタンス タグを設定して、新しいEIGRPプロセスを作成します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。 AS 番号であると認められていない *instance-tag* を設定する場合は、**autonomous-system** コマンドを使用して AS番号を明示的に設定する必要があります。そうしないと、このEIGRPインスタンスはシャットダウン状態のままになります。
ステップ 3	switch(config-router)# **bfd**	（任意） この EIGRP ルータの BFD をイネーブルにします。
ステップ 4	switch(config-router)# **interface***int-if*	インターフェイス コンフィギュレーション モードを開始します。? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 5	switch(config-if)# **ip eigrp***instance-tag***bfd**	（任意） EIGRP インターフェイスで BFD をイネーブルまたはディセーブルにします。インスタンス タグには最大20文字の英数字を使用できます。大文字と小文字を区別します。 デフォルトではディセーブルになっています。

	コマンドまたはアクション	目的
ステップ 6	switch(config-if)# **show ip eigrp** [**vrf***vrf-name*] [**interface** *if*]	（任意） EIGRP の実行コンフィギュレーションを表示します。
ステップ 7	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、変更を継続的に保存します。

次に、EIGRP 上で BFD を設定する例を示します。

```
switch# configure terminal
switch(config)# router eigrp Test1
switch(config-router)# bfd
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip eigrp Test1 bfd
switch(config-if)# show ip eigrp
switch(config-if)# copy running-config startup-config
```

OSPF 上での BFD の設定について

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

OSPF での BFD の設定

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

はじめる前に

BFD 機能をイネーブルにします。BFD 機能のイネーブル化，（73 ページ）を参照してください。

BFD セッション パラメータを設定します。グローバルな BFD パラメータの設定，（74 ページ）またはインターフェイスでの BFD の設定，（76 ページ）を参照してください。

OSPF 機能をイネーブルにします。

詳細については、『*Cisco Nexus 5500 Switch NX-OS Unicast Routing Configuration Guide, Release 6.x*』を参照してください。

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)# **router ospf***instance-tag*	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
ステップ 3	switch(config-router)# **bfd**	（任意） この OSPFv2 インスタンスの BFD をイネーブルにします。また、各 OSPFv2 インターフェイスはイネーブルかディセーブルである必要があります。
ステップ 4	switch(config-router)# **interface***int-if*	インターフェイス コンフィギュレーション モードを開始します。? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 5	switch(config-if)# **ip ospf bfd**	（任意） OSPFv2 インターフェイスで BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 6	switch(config-if)# **show ip ospf** [**vrf***vrf-name*] [**interface** *if*]	（任意） OSPF の実行コンフィギュレーションを表示します。
ステップ 7	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、変更を継続的に保存します。

次に、OSPF 上で BFD を設定する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# bfd
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip ospf bfd
switch(config-if)# show ip ospf
switch(config-if)# copy running-config startup-config
```

HSRP 上での BFD の設定について

Hot Standby Router Protocol（HSRP）の BFD を設定できます。アクティブおよびスタンバイの HSRP ルータは BFD を介して相互に追跡しています。

スタンバイ HSRP ルータ上の BFD がアクティブ HSRP ルータが動作していないことを検知すると、スタンバイ HSRP はこのイベントをアクティブ タイマー失効として取り扱い、アクティブ HSRP ルータとして役割を引き継ぎます。show hsrp detail では、このイベントが BFD@Act-down または BFD@Sby-down として表示されます。

HSRP での BFD の設定

Hot Standby Router Protocol（HSRP）の BFD を設定できます。アクティブおよびスタンバイの HSRP ルータは BFD を介して相互に追跡しています。

スタンバイ HSRP ルータ上の BFD がアクティブ HSRP ルータが動作していないことを検知すると、スタンバイ HSRP はこのイベントをアクティブ タイマー失効として取り扱い、アクティブ HSRP ルータとして役割を引き継ぎます。**show hsrp detail** コマンドでは、このイベントが BFD@Act-down または BFD@Sby-down として表示されます。

はじめる前に

正しい VRF を使用していることを確認します。

BFD 機能をイネーブルにします。BFD 機能のイネーブル化, （73 ページ）を参照してください。

BFD セッション パラメータを設定します。グローバルな BFD パラメータの設定, （74 ページ）またはインターフェイスでの BFD の設定, （76 ページ）を参照してください。

HSRP 機能をイネーブルにします。詳細については、『*Cisco Nexus 5500 Series NX-OS Unicast Routing Configuration Guide, Release 6.x*』を参照してください。

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)# **hsrp bfd all-interfaces**	（任意） HSRP インターフェイスですべての BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 3	switch(config)# **interface***int-if*	インターフェイス コンフィギュレーション モードを開始します。? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 4	switch(config-if)# **hsrp bfd**	（任意） HSRP インターフェイスで BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 5	switch(config-if)# **show running-config hsrp**	（任意） HSRP の実行コンフィギュレーションを表示します。

	コマンドまたはアクション	目的
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、変更を継続的に保存します。

次に、HSRP 上で BFD を設定する例を示します。

```
switch# configure terminal
switch(config)# hsrp bfd all-interfaces
switch(config)# interface ethernet 2/1
switch(config-if)# hsrp bfd
switch(config-if)# show running-config hsrp
switch(config-if)# copy running-config startup-config
```

VRRP 上での BFD の設定について

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

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

VRRP での BFD の設定

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

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

はじめる前に

正しい VRF を使用していることを確認します。

BFD 機能をイネーブルにします。BFD 機能のイネーブル化, （73 ページ）を参照してください。

BFD セッション パラメータを設定します。グローバルな BFD パラメータの設定, （74 ページ）またはインターフェイスでの BFD の設定, （76 ページ）を参照してください。

VRRP 機能をイネーブルにします。

詳細については、『*Cisco Nexus 5500 Series NX-OS Unicast Routing Configuration Guide, Release 6.x*』を参照してください。

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** *int-if*	インターフェイス コンフィギュレーション モードを開始します。? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 3	switch(config-if)# **vrrp***group-no*	VRRP グループ番号を指定します。
ステップ 4	switch(config-if-vrrp)# **vrrp bfd***address*	VRRP インターフェイスで BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 5	switch(config-if-vrrp)# **show running-config vrrp**	（任意） VRRP の実行コンフィギュレーションを表示します。
ステップ 6	switch(config-if-vrrp)# **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、変更を継続的に保存します。

次に、VRRP 上で BFD を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# vrrp 1
switch(config-if-vrrp)# vrrp bfd 10.0.0.10
switch(config-if-vrrp)# show running-config vrrp
switch(config-if-vrrp)# copy running-config startup-config
```

スタティック ルートでの BFD の設定について

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

スタティック ルートでの BFD の設定

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

はじめる前に

正しい VRF を使用していることを確認します。
BFD 機能をイネーブルにします。BFD 機能のイネーブル化, （73 ページ）を参照してください。

BFD セッション パラメータを設定します。グローバルな BFD パラメータの設定, （74 ページ）またはインターフェイスでの BFD の設定, （76 ページ）を参照してください。

HSRP 機能をイネーブルにします。詳細については、『*Cisco Nexus 5500 Series NX-OS Unicast Routing Configuration Guide, Release 6.x*』を参照してください。

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)# **vrf context***vrf-name*	（任意） VRF 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-vrf)# **ip route route interface** {*nh-address*|*nh-prefix*}	スタティック ルートを作成します。? キーワードを使用して、サポートされているインターフェイスを表示します。
ステップ 4	switch(config-vrf)# **ip route static bfd interface** {*nh-address*|*nh-prefix*}	インターフェイスのすべてのスタティック ルートの BFD をイネーブルにします。? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 5	switch(config-vrf)# **show ip route static**[**vrf***vrf-name*]	（任意） スタティック ルートを表示します。
ステップ 6	switch(config-vrf)# 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、設定を永続的に保存します。

次に、スタティック ルート上で BFD を設定する例を示します。

```
switch# configure terminal
switch(config)# vrf context Red
switch(config-vrf)# ip route route interface 192.0.2.1 ethernet 2/1 192.0.2.4
switch(config-vrf)# ip route static bfd ethernet 2/1 192.0.2.4
switch(config-vrf)# show ip route static vrf Red
switch(config-vrf)# copy running-config startup-config
```

PIM 上での BFD の設定について

PIM（Protocol Independent Multicast）プロトコルの BFD を設定できます。

PIM 上での BFD の設定

PIM（Protocol Independent Multicast）プロトコルの BFD を設定できます。

はじめる前に

正しい VRF を使用していることを確認します。

BFD 機能をイネーブルにします。BFD 機能のイネーブル化, （73 ページ）を参照してください。

BFD セッション パラメータを設定します。グローバルな BFD パラメータの設定, （74 ページ）またはインターフェイスでの BFD の設定, （76 ページ）を参照してください。

PIM 機能をイネーブルにします。詳細については、『*Cisco Nexus 5500 Series NX-OS Multicast Routing Configuration Guide, Release 6.x*』を参照してください。

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)# **ip pim bfd**	PIM の BFD をイネーブルにします。
ステップ 3	switch(config)# **interface***int-if*	インターフェイス コンフィギュレーション モードを開始します。?キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 4	switch(config-if)# **ip pim bfd-instance** [**disable**]	（任意） PIM インターフェイスの BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 5	switch(config-if)# **show running-config pim**	（任意） PIM の実行コンフィギュレーションを表示します。
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、設定を永続的に保存します。

次に、PIM 上で BFD を設定する例を示します。

```
switch# configure terminal
switch(config)# ip pim bfd
switch(config)# interface ethernet 2/1
switch(config-if)# ip pim bfd-instance
switch(config-if)# show running-config pim
switch(config-if)# copy running-config startup-config
```

インターフェイスにおける BFD のディセーブル化

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config)# **ip eigrp** *instance-tag* **bfd disable** 例： `switch(config)# ip eigrp Test1 bfd disable`	EIGRP インターフェイスで BFD をディセーブルにします。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
ステップ 2	switch(config-if)# **ip ospf bfd disable** 例： `switch(config-if)# ip ospf bfd disable`	OSPFv2 インターフェイスで BFD をディセーブルにします。

すべての IS-IS インターフェイスでの FabricPath BFD の設定

はじめる前に

正しい VRF を使用していることを確認します。

BFD 機能をイネーブルにします。BFD 機能のイネーブル化, （73 ページ）を参照してください。

BFD セッション パラメータを設定します。グローバルな BFD パラメータの設定, （74 ページ）またはインターフェイスでの BFD の設定, （76 ページ）を参照してください。

ISIS 機能は、**feature-set fabricpath** コマンドを入力したときにデフォルトでイネーブルになります。

詳細については、『*Cisco Nexus 5500 Switch NX-OS Unicast Routing Configuration Guide, Release 7.x*』を参照してください。

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)# **fabricpath domain default**	グローバル FabricPath レイヤ 2 Intermediate System to Intermediate System（IS-IS）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-fabricpath-isis)# **bfd**	すべての IS-IS インターフェイスで FabricPath BFD をイネーブルにします。

次に、すべての IS-IS インターフェイスで FabricPath BFD を設定する例を示します。

```
switch# configure terminal
switch(config)# fabricpath domain default
switch(config-fabricpath-isis)# bfd
```

特定のインターフェイスでの FabricPath BFD の設定

はじめる前に

BFD 機能をイネーブルにします。BFD 機能のイネーブル化, （73 ページ）を参照してください。

BFD セッション パラメータを設定します。グローバルな BFD パラメータの設定, （74 ページ）またはインターフェイスでの BFD の設定, （76 ページ）を参照してください。

ISIS 機能は、**feature-set fabricpath** コマンドを入力したときにデフォルトでイネーブルになります。

詳細については、『*Cisco Nexus 5500 Switch NX-OS Unicast Routing Configuration Guide, Release 7.x*』を参照してください。

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)# **[no] bfd fabricpath encap-ce**	ユーザがセッションごとに L2BFD フレームのカプセル化モードを選択できるようにします。コマンドをイネーブルにすると、Fabricpath のカプセル化なしでフレームを送信します。デフォルト モードでは、Fabricpath カプセル化を使用してフレームを送信します。

	コマンドまたはアクション	目的
ステップ 3	switch(config-if)# **fabricpath isis bfd**	インターフェイスで FabricPath BFD をイネーブルにします。

次に、特定のインターフェイスで FabricPath BFD を設定する例を示します。

```
switch# configure terminal
switch(config)# [no] bfd fabricpath encap-ce
switch(config-if)# fabricpath isis bfd
```

BFD 設定の確認

BFD を確認するには、次のコマンドを使用します。

コマンド	目的
switch# **show running-config bfd**	BGP や OSPFv2 などのサポートされるアプリケーションの BFD に関する情報を表示します。
switch# **show startup-config bfd**	起動時に適用される BFD コンフィギュレーションに関する情報を表示します。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 5500 Series NX-OS Interfaces Command Reference*』を参照してください。

BFD のモニタ

BFD をモニタするには、次のコマンドを使用します。

コマンド	目的
switch# **show bfd neighbors** [**application***name*] [**details**]	BGP や OSPFv2 などのサポートされるアプリケーションの BFD に関する情報を表示します。
switch# **show bfd neighbors** [**interface***int-if*] [**details**]	指定したインターフェイスでの BFD に関する情報を表示します。
switch# **show bfd neighbors** [**dest-ip***ip-address*] [**src-ip***ip-address*] [**details**]	指定したインターフェイスでのセッションの BFD に関する情報を表示します。
switch# **show bfd neighbors** [**vrf***vrf-name*] [**details**]	VRF の BFD に関する情報を表示します。

コマンド	目的
switch# **show bfd neighbors** [**fabricpath**] [**dest-ip***ip-address*] [**src-ip***ip-address*] [**details**]	指定したインターフェイスでのセッションの BFD に関する情報を表示します。オプションの **fabricpath** キーワードを使用して特定の fabricpath ネイバーに関する情報を表示します。
switch# **show bfd neighbors** [**dest-sys-id***dest-sys-id-value*]	特定の FabricPath ネイバーに関する情報を表示します。

詳細については、『*Cisco Nexus 5500 Series NX-OS Switch Interfaces Command Reference*』を参照してください。

BFD の設定例

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

```
switch# configure terminal
switch(config)# feature bfd
switch(config)# feature ospf
switch(config)# router ospf Test1
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip ospf bfd
switch(config-if)# no shutdown
```

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

```
switch# configure terminal
switch(config)# feature bfd
switch(config)# feature eigrp
switch(config)# bfd interval 250 min_rx 250 multiplier 4
switch(config)# router eigrp Test2
switch(config-router)# bfd
```

関連資料

関連項目	マニュアル タイトル
BFD コマンド	詳細については、『*Cisco Nexus 5500 Switch NX-OS Unicast Routing Command Reference, Release 6.x*』を参照してください。

関連の標準

以下の業界標準は双方向フォワーディング検出に対応しています。

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

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，99 ページ
- ポート チャネルの設定，110 ページ
- ポート チャネル設定の確認，125 ページ
- ロードバランシング発信ポート ID の確認 ，126 ページ
- ポート チャネル設定の機能履歴，126 ページ

ポート チャネルについて

ポート チャネルは、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。

ポート チャネルは、互換性のあるインターフェイスをバンドルすることによって作成します。スタティック ポート チャネルのほか、Link Aggregation Control Protocol（LACP）を実行するポート チャネルを設定して稼働させることができます。

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

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

関連トピック

LACP の概要, （106 ページ）

ポート チャネルの概要

Cisco NX-OS は、ポート チャネルを使用することにより、広い帯域幅、冗長性、チャネル全体のロード バランシングを実現しています。

ポートを 1 つのスタティック ポート チャネルに集約するか、またはリンク集約制御プロトコル（LACP）をイネーブルにできます。LACP によるポート チャネルを設定する手順は、スタティック ポート チャネルの場合とは若干異なります。ポート チャネル設定の制約事項については、プラットフォームの『*Verified Scalability*』マニュアルを参照してください。ロード バランシングの詳細については、ポート チャネルを使ったロード バランシング, （103 ページ）を参照してください。

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

ポート チャネルは、個々のリンクを 1 つのチャネル グループにバンドルしたもので、それによりいくつかの物理リンクの帯域幅を集約した単一の論理リンクが作成されます。ポート チャネル内のメンバー ポートに障害が発生すると、障害が発生したリンクで伝送されていたトラフィックはポート チャネル内のその他のメンバー ポートに切り替わります。

各ポートにはポート チャネルが 1 つだけあります。ポート チャネル内のすべてのポートには互換性が必要です。つまり、回線速度が同じであり、かつ全二重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ことで、ポート チャネルを直接作成することができます。またチャネル グループを作成して個々のポートを 1 つに集約することもできます。インターフェイスをチャネル グループに関連付ける際、ポート チャネルがなければ、Cisco NX-OS では対応するポート チャネルが自動的に作成されます。最初にポート チャネルを作成することもできます。その場合、Cisco NX-OS では、ポート チャネルと同じチャネル数で空のチャネル グループが作成され、デフォルトの設定が適用されます。

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

ポート チャネルの設定に関する注意事項と制約事項

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 モードのいずれかで設定することができます。Cisco NX-OS の設定同期化機能を介してポート チャネルの設定を行う際には、次の注意事項および制約事項を考慮してください。

- いったんスイッチ プロファイル モードで設定したポート チャネルを、グローバル コンフィギュレーション（config terminal）モードで設定することはできません。

（注） ポート チャネルに関する一部のサブコマンドは、スイッチ プロファイル モードでは設定できません。ただしこれらのコマンドは、ポート チャネルがスイッチ プロファイル モードで作成、設定されている場合でも、グローバル コンフィギュレーション モードからであれば設定することができます。

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 モードでのみ設定可能です。

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 モードとスイッチ プロファイル モードのどちらでも設定できます。
- ポート チャネルをグローバル コンフィギュレーション モードで作成した場合は、メンバー 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 チャネルには、スイッチ プロファイルの内部と外部どちらからもメンバーにすることができます。
- メンバーインターフェイスをスイッチプロファイルにインポートする場合は、そのメンバーインターフェイスに対応するポート チャネルがスイッチ 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、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 では、そのインターフェイスとチャネル グループとの互換性が確保されるように、特定のインターフェイス属性のチェックが行われます。また Cisco NX-OS では、インターフェイスがポート チャネル集約に加えられることを許可する場合にも、事前にそのインターフェイスに関するさまざまな動作属性のチェックが行われます。

互換性チェックの対象となる動作属性は次のとおりです。

- ポート モード

- アクセス VLAN
- トランク ネイティブ VLAN
- 許可 VLAN リスト
- 速度
- 802.3x フロー制御設定
- MTU

  Cisco Nexus デバイスは、システム レベル 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場合は、**show port-channel compatibility-parameters** コマンドを使用します。

チャネル モード セットを on に設定したインターフェイスだけをスタティック ポート チャネルに追加できます。また LACP を実行するポート チャネルには、チャネル モードが active または passive に設定されたインターフェイスだけを追加することもできますこれらの属性は個別のメンバー ポートに設定できます。

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

- 帯域幅
- MAC アドレス
- スパニングツリー プロトコル

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

- 説明
- CDP
- LACP ポート プライオリティ
- デバウンス

channel-group force コマンドを使用して、ポートをチャネル グループへ強制的に追加できるようにした場合、パラメータは次のように処理されます。

- インターフェイスがポートチャネルに参加すると、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 チャネルに追加またはポート チャネルから削除されても、次のパラメータはそのまま維持されます。
  - ビーコン
  - 説明
  - CDP
  - LACP ポート プライオリティ
  - デバウンス
  - UDLD
  - シャットダウン
  - SNMP トラップ

ポート チャネルを使ったロード バランシング

Cisco NX-OS では、フレーム内のアドレスから生成されたバイナリ パターンの一部を数値に圧縮変換し、それを基にチャネル内のリンクを 1 つ選択することによって、ポート チャネルを構成するすべての動作中インターフェイス間でトラフィックのロード バランシングが行われます。ポート チャネルはデフォルトでロード バランシングを備えています。

基本設定では、次の基準を使用し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 Internet Protocol（IP）アドレスを使用します。

（注） レイヤ 4 フレームに対しては、必要に応じて送信元および宛先のポート番号を指定することもできます。

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

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

表 *3*：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 エクステンダの設定は個別には行えません。ファブリック エクステンダの設定は、Cisco Nexus デバイスで定義されます。ポート チャネル ロード バランシング プロトコルにおいて、Cisco Nexus デバイスで実行された設定の結果に応じてファブリック エクステンダ モジュール上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は下記の表を参照してください。

次の表は、各設定の基準をまとめたものです。

表 4： ***Cisco Nexus 2232*** ファブリック エクステンダおよび ***Cisco Nexus 2248*** ファブリック エクステンダにおけるポート チャネルでのロードバランシングの基準

設定	レイヤ 2 基準	レイヤ 3 基準	レイヤ 4 基準
宛先 MAC	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

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

（注） ハードウェア マルチキャスト hw-hash コマンドは、Cisco Nexus 3500 シリーズ スイッチではサポートされません。これらのスイッチではこのコマンドを設定しないことを推奨します。

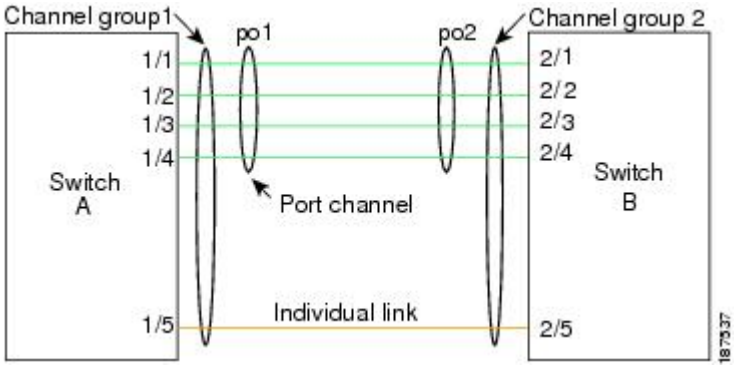
LACP の概要

LACP の概要

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

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

図 *6*： 個々のリンクをポート チャネルに組み込む



LACP を使用すると、スタティック ポート チャネルの場合と同じように、最大 16 個のインターフェイスを 1 つのチャネル グループにバンドルすることができます。

（注） ポート チャネルを削除すると、関連付けられたチャネル グループも Cisco NX-OS によって自動的に削除されます。すべてのメンバー 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が使用されます。

- LACP システム プライオリティ：LACP を稼働している各システムは、LACP システム プライオリティ値を持っています。このパラメータのデフォルト値である 32768 をそのまま使用するか、1 ～ 65535 の範囲で値を設定できます。LACP は、このシステム プライオリティと MAC アドレスを組み合わせてシステム 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 では、ポート プライオリティおよびポート番号によりポート ID が構成されます。また、互換性のあるポートのうち一部を束ねることができない場合に、どのポートをスタンバイ モードにし、どのポートをアクティブ モードにするかを決定するのに、ポート プライオリティを使用します。LACP では、ポート プライオリティ値が大きいほど、プライオリティは低くなります。指定ポートが、より低い LACP プライオリティを持ち、ホット スタンバイ リンクではなくアクティブ リンクとして選択される可能性が最も高くなるように、ポート プライオリティを設定できます。
- LACP 管理キー：LACP は、LACP を使用するように設定された各ポート上のチャネル グループ番号に等しい管理キー値を自動的に設定します。管理キーにより、他のポートとともに集約されるポートの機能が定義されます。他のポートとともに集約されるポートの機能は、次の要因によって決まります。
  - ポートの物理特性（データ レート、デュプレックス機能、ポイントツーポイントまたは共有メディア ステートなど）
  - ユーザが作成した設定に関する制約事項

チャネル モード

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

（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。

次の図は、チャネル モードをまとめたものです。

表 5: ポート チャネルの個別リンクのチャネル モード

チャネル モード	説明
passive	ポートをパッシブなネゴシエーション状態にする LACP モード。この状態では、ポートは受信した LACP パケットに応答はしますが、LACP ネゴシエーションを開始することはありません。
active	ポートをアクティブ ネゴシエーション ステートにする LACP モード。この場合ポートでは LACPパケットを送信することにより、他のポートとのネゴシエーションが開始されます。
on	すべてのスタティック ポート チャネル（つまり LACP を稼働していないポート チャネル）は、このモードのままになります。LACP をイネーブルにする前にチャネル モードを active または passive に変更しようとすると、デバイスがエラー メッセージを返します。 チャネルで LACP をイネーブルにするには、そのチャネルのインターフェイスでチャネル モードを active または passive に設定します。LACP 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 と active のどちらのモードでも、ポート速度やトランキング ステートなどの基準に基づいてポート チャネルを構成可能かどうかを判定するため、LACP によるポート間のネゴシエーションが行われます。passive モードは、リモート システム、つまり、パートナーが、LACP をサポートしているかどうかが不明な場合に便利です。

次の例に示したとおり、ポートは、異なる LACP モードであっても、それらのモード間で互換性があれば、LACP ポート チャネルを構成することができます。

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

LACP マーカー レスポンダ

ポート チャネルを使用すると、リンク障害やロード バランシング動作に伴って、データ トラフィックが動的に再配信される場合があります。LACP では、マーカー プロトコルを使用して、こうした再配信によってフレームが重複したり順序が変わったりしないようにします。Cisco NX-OS は、マーカー レスポンダ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

次の表は、LACP がイネーブルのポート チャネルとスタティック ポート チャネルとの主な相違点をまとめたものです。設定の最大制限値の詳細については、デバイスの『*Verified Scalability*』マニュアルを参照してください。

表 *6* : *LACP* がイネーブルのポート チャネルとスタティック ポート チャネル

構成	LACP がイネーブルのポート チャネル	スタティック ポート チャネル
適用されるプロトコル	グローバルにイネーブル化	なし。
リンクのチャネル モード	次のいずれか。 • Active • Passive	on モードのみ

LACP ポートチャネルの最小リンクおよび MaxBundle

ポート チャネルは、同様のポートを集約し、単一の管理可能なインターフェイスの帯域幅を増加させます。

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

LACP ポートチャネルの MinLink 機能は次の処理を実行します。

- LACP ポート チャネルにリンク アップし、バンドルする必要があるポートの最小数を設定します。
- 低帯域幅の LACP ポート チャネルがアクティブにならないようにします。

- 必要な最小帯域幅を提供するアクティブ メンバー ポートが少数の場合、LACP ポート チャネルが非アクティブになります。

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

LACP MaxBundle 機能では、次の処理が行われます。

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

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

LACP の最小リンクと maxbundle の設定は、FEX HIF ポート チャネルには適用できません。

最小リンクまたは maxbundle の設定を非 LACP HIF PO に適用することはできますが、機能は動作しません。LACP HIF PO で最小リンクまたは maxbundle の設定を行うことは許可されておらず、拒否されます。

ポート チャネルの設定

デフォルト設定

表 7: デフォルト ポート チャネル パラメータ

パラメータ	デフォルト
ポート チャネル	管理アップ
レイヤ3インターフェイスのロードバランシング方式	送信元および宛先 IP アドレス
レイヤ2インターフェイスのロードバランシング方式	送信元および宛先 MAC アドレス
モジュールごとのロード バランシング	ディセーブル
RBH モジュロ モード	ディセーブル
LACP	ディセーブル

パラメータ	デフォルト
チャネル モード	on
LACP システム プライオリティ	32768
LACP ポート プライオリティ	32678
LACP の最小リンク	1
FEX ファブリック ポート チャネル用最小リンク数	1
Maxbundle	16

ポート チャネルの作成

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	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 port-channel***channel-number*	設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。範囲は 1 ～ 4096 です。チャネル グループがまだ存在していなければ、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。ポート チャネルがない場合は、Cisco NX-OS によってこのチャネル グループに関連付けられたポート チャネルが作成されます。

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

手順

	コマンドまたはアクション	目的
ステップ 1	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***typeslot*/*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。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **switchport mode trunk**	（任意） 指定したインターフェイスをトランク ポートとして設定します。
ステップ 4	switch(config-if)# **switchport trunk** {**allowed vlan***vlan-id* | **native vlan***vlan-id*}	（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	switch(config-if)# **channel-group***channel-number*	チャネル グループ内にポートを設定し、モードを設定します。channel-number の指定できる範囲は 1 ～ 4096 です。ポート チャネルがない場合は、Cisco NX-OS によってこのチャネル グループに関連付けられたポート チャネルが作成されます。これを、暗黙的なポート チャネル作成と言います。
ステップ 6	switch(config-if)# **no channel-group**	（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 チャネルを使用する場合は、LACP をイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# **port-channel load-balance ethernet** {[**destination-ip** | **destination-mac** | **destination-port** | **source-dest-ip** | **source-dest-mac** | **source-dest-port** | **source-ip** | **source-mac** | **source-port**] | **crc-poly**}	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。（注） Cisco Nexus 5500 プラットフォーム スイッチはハッシュ パラメータの圧縮に使用できる 8 種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に対するハッシュ パラメータの種類によっては、多項式が異なると負荷分散の結果も異なる場合があります。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。 • CRC8a • CRC8b • CRC8c • CRC8d • CRC8e • CRC8f • CRC8g

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **no port-channel load-balance ethernet**	（任意） ロードバランシング アルゴリズムをデフォルトの source-dest-mac に戻します。
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。

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

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

マルチキャスト トラフィックに対するハードウェア ハッシュの設定

デフォルトでは、スイッチのどのポートにおける入力マルチキャスト トラフィックでも、特定のポートチャネルメンバーが選択され、トラフィックが出力されます。マルチキャスト トラフィックのハードウェア ハッシュを設定して、帯域幅の問題が発生する可能性を減らし、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行うことができます。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。デフォルトに戻す場合は、**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**	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 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)# **[no] hardware multicast hw-hash**	指定したポートチャネルに対してハードウェア ハッシュを設定します。

次の例は、ポート チャネルに対してハードウェア ハッシュを設定する方法を示したものです。

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

次の例は、ポート チャネルからハードウェア ハッシュを削除する方法を示したものです。

```
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 では、適合する複数のイーサネット リンクが検出されると、これらのリンクが 1 つのポート チャネルにグループ化されます。次に、ポート チャネルは単一ブリッジ ポートとしてスパニングツリーに追加されます。

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 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
```

ポートに対するチャネル モードの設定

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

関連するプロトコルを使用せずにポート チャネルを設定すると、リンク両端のすべてのインターフェイスでは on チャネル モードが維持されます。

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**	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***typeslot*/*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。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]	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。 **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。 **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。 **active**：これを指定すると、LACP をイネーブルにした時点で、指定したインターフェイス上で LACP がイネーブルになります。インターフェイスはアクティブ ネゴシエーション ステートになります。この場合ポートでは、LACP パケットを送信することにより、他のポートとのネゴシエーションが開始されます。 **on**：（デフォルト モード）これを指定すると、LACP を実行していないすべてのポート チャネルに対して、このモードが維持されます。 **passive**：LACP 装置が検出された場合に限り、LACP をイネーブルにします。インターフェイスはパッシブ ネゴシエーション ステートになります。この場合ポートでは、受信した LACP パケットへの応答は行われますが、LACP ネゴシエーションは開始されません。 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。
ステップ 4	switch(config-if)# **no channel-group***number***mode**	指定インターフェイスのポート モードを on に戻します

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
```

次の例は、チャネル グループ 5 にインターフェイスを強制的に追加する方法を示したものです。

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

LACP ポート チャネル最小リンク数の設定

LACP の最小リンク機能を設定できます。最小リンク数機能は LACP でのみ機能しますが、非 LACP ポート チャネルに対してこの機能の CLI コマンドを入力することができます。しかし、このコマンドは処理されません。

はじめる前に

適切なポートチャネル インターフェイスであることを確認します。

手順

	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 port-channel***number*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **lacp min-links***number*	ポート チャネル インターフェイスを指定して、最小リンク数を設定し、インターフェイス コンフィギュレーション モードを開始します。指定できる範囲は 1 ～ 16 です。
ステップ 4	switch(config-if)# **show running-config interface port-channel***number*	（任意） ポートチャネル最小リンク数のコンフィギュレーションを表示します。 （注） 以前の Cisco NX-OS リリースから Cisco NX-OS リリース 7.2(1)N1(1) 以降のリリースにアップグレードすると、追加の設定行 **no lacp suspend-individual** が **show running-config interface port-channel***number* コマンドの **show** コマンド出力に表示されます。

次に、LACP ポート チャネル最小リンク数を設定する例を示します。

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

LACP ポートチャネル MaxBundle の設定

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

はじめる前に

適切なポートチャネル インターフェイスであることを確認します。

手順

	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 port-channel***number*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **lacp max-bundle***number*	ポートチャネルインターフェイスを指定して、max-bundle を設定し、インターフェイス コンフィギュレーション モードを開始します。 ポート チャネルの max-bundle のデフォルト値は 16 です。指定できる範囲は 1 ～ 16 です。 （注） デフォルト値は 16 ですが、ポート チャネルのアクティブ メンバー数は、pc_max_links_config およびポートチャネルで許可されている pc_max_active_members の最小数です。最小リンク機能と最大バンドル機能は、ポート チャネルの両側が同じ値で設定されている場合に適切に機能します。最小/最大バンドル値の不一致は、ポートのフラップ、トラフィックのドロップ、不必要なポートの停止につながる可能性があります。
ステップ 4	switch(config-if)# **show running config interface port-channel***number*	

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

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

LACP 高速タイマー レートの設定

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

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**	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***typeslot*/*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。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **lacp rate fast**	LACP がサポートされているインターフェイスに LACP 制御パケットを送信する際のレートとして高速レート（1 秒）を設定します。

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

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

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

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

LACP ショート タイムアウトの設定

lacp rate fast コマンドの LACP ショート タイムアウト値を変更して、LACP 高速レート タイムアウトの期間を変更することができます。**lacp rate fast** コマンドを使用すれば、LACP がサポートされているインターフェイスに LACP 制御パケットを送信する際の高速レートを設定できます。ショート タイムアウト値を 15 秒（デフォルト タイムアウト）から 3 秒（IEEE802.3ad で推奨される標準）に変更できます。

（注） **lacp short-timeout** コマンドは、LACP がイネーブルになっているインターフェイスでのみサポートされます。

LACP ショート タイムアウトが設定されている場合、BFD 機能はサポートされません。

vPC Multichassis EtherChannel トランク（MCT）ポートでは LACP レート高速は推奨されません。

はじめる前に

LACP レート高速機能がイネーブルになっていることを確認します。

手順

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)# **lacp short-timeout**
LACP がサポートされているインターフェイスに LACP 制御パケットを送信する際の LACP 高速レートのショート タイムアウト値を設定します。有効な値の範囲は 3 ～ 15 秒です。デフォルトのショート タイムアウト値は 15 秒です。

（注） LACP ショートタイムアウトのデフォルト設定は実行コンフィギュレーションには表示されません。

ステップ 3 （任意） switch(config)# **show run | include lacp**
インターフェイス上の LACP の設定を表示します。

次に、LACP 高速レートに 3 秒の LACP ショート タイムアウト値を設定する例を示します。

```
switch# configure terminal
switch(config)# lacp short-timeout 3
```

次に、LACP 高速レートに LACP ショート タイムアウトのデフォルト タイムアウト（15 秒）を復元する例を示します。

```
switch# configure terminal
switch(config)# no lacp short-timeout
```

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**	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)# **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。
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

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

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**	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***typeslot*/*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。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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 コンバージェンスのディセーブル化

はじめる前に

- LACP 機能をイネーブルにします。
- ポート チャネルが管理上のダウン状態になってい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** *number*
	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。

	コマンドまたはアクション	目的

ステップ 3	シャットダウン
	
	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	**no lacp graceful-convergence**
	
	例：
	`switch(config-if)# no 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ディセーブルにします。

ステップ 5	**no shutdown**
	
	例：
	`switch(config-if)# no shutdown`
	`switch(config-if) #`
		ポートチャネルを管理上のアップ状態にします。

ステップ 6	**copy running-config startup-config** 例： `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、変更を継続的に保存します。

次の例は、ポートチャネルのLACPグレースフルコンバージェンスをディセーブルにする方法を示したものです。

```
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 チャネルが管理上のダウン状態になってい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** *number*
	
	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	シャットダウン
	
	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。

ステップ 5	**no shutdown**
	
	例：
	`switch(config-if)# no shutdown`
	`switch(config-if) #`
		ポート チャネルを管理上のアップ状態にします。

ステップ 6	**copy running-config startup-config** 例： `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、変更を継続的に保存します。

次の例は、ポート チャネルの LACP グレースフル コンバージェンスをディセーブルにする方法を示したものです。

```
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 チャネル設定の確認

次のコマンドを使用すると、ポート チャネルの設定情報を確認できます。

コマンド	目的
show interface port channel*chennal-number*	ポート チャネル インターフェイスのステータスを表示します。
show feature	イネーブルにされた機能を表示します。
show resource	システムで現在利用可能なリソースの数を表示します。
show lacp {**counters** | **interface***typeslot*/*port* | **neighbor** | **port-channel** | **system-identifier**}	LACP 情報を表示します。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
show port-channel compatibility-parameters	ポートチャネルに追加するためにメンバーポート間で同じにするパラメータを表示します。
show port-channel database [**interface port-channel***channel-number*]	1 つ以上のポートチャネルインターフェイスの集約状態を表示します。
show port-channel summary	ポート チャネル インターフェイスの概要を表示します。
show port-channel traffic	ポートチャネルのトラフィック統計情報を表示します。
show port-channel usage	使用済みおよび未使用のチャネル番号の範囲を表示します。
show port-channel database	現在実行中のポートチャネル機能に関する情報を表示します。
show port-channel load-balance	ポートチャネルによるロードバランシングについての情報を表示します。

ロードバランシング発信ポート ID の確認

コマンドに関する注意事項

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

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

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

コマンド	目的
switch# **show port-channel load-balance forwarding-path interface port-channel***port-channel-id***vlan** vlan-id **dst-ipsrc-ipdst-macsrc-macl4-src-port***port-id* **l4-dst-port***port-id*	発信ポート ID を表示します。

例

次に、ロードバランシング発信ポート ID を表示する例を示します。

```
switch# show port-channel load-balance forwarding-path interface port-channel 10 vlan 1
dst-ip 1.225.225.225 src-ip 1.1.10.10 src-mac aa:bb:cc:dd:ee:ff
l4-src-port 0 l4-dst-port 1
Missing params will be substituted by 0's. Load-balance Algorithm on switch: source-dest-port
 crc8_hash:204 Outgoing port id: Ethernet 1/1 Param(s) used to calculate load balance:
dst-port: 0
src-port: 0
dst-ip: 1.225.225.225
src-ip: 1.1.10.10
dst-mac: 0000.0000.0000
src-mac: aabb.ccdd.eeff
```

ポート チャネル設定の機能履歴

表 *8* : ポート チャネル設定の機能履歴

機能名	リリース	機能情報
最小リンク数	6.0(2)N1(2)	この機能が導入されました。
LACP ショート タイムアウト	7.3(0)N1(1)	この機能が導入されました。

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，129 ページ
- VRF に関する注意事項と制約事項，154 ページ
- vPC の設定，155 ページ
- vPC ピア スイッチの設定，173 ページ
- vPC を介したレイヤ 3 の設定，177 ページ
- vPC 複合からのスイッチの分離と復元，178 ページ
- vPC 設定の確認，179 ページ
- vPC の設定例，185 ページ
- vPC のデフォルト設定，189 ページ

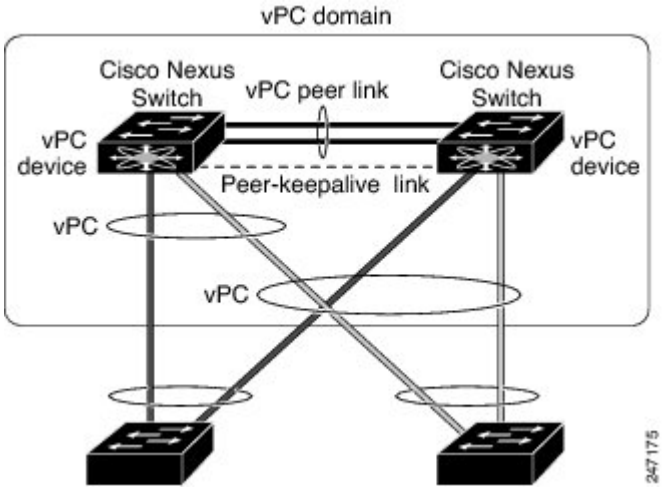
vPC について

vPC の概要

仮想ポート チャネル（vPC）を使用すると、物理的には 2 台の異なる Cisco Nexus デバイスまたは Cisco Nexus ファブリック エクステンダに接続されている複数のリンクを、第 3 のデバイスからは単一のポート チャネルとして認識されるようにすることができます（次の図を参照）。第 3 のデバイスには、スイッチやサーバなどあらゆるネットワーキングデバイスが該当します。Cisco Nexus ファブリック エクステンダに接続された Cisco Nexus デバイスを含むトポロジ内に vPC を設定できます。vPC では、マルチパス機能を使用することができます。この機能では、ノード間の複数

のパラレルパスをイネーブルにし、さらには存在する代替パスでトラフィックのロードバランシングを行うことにより、冗長性が確保されます。

図 7 : *vPC* のアーキテクチャ



EtherChannel の設定は、次のいずれかを使用して行います。

- プロトコルなし
- リンク集約制御プロトコル（LACP）

vPC ピア リンク チャネルなど、vPC で EtherChannel を設定した場合、それぞれのスイッチでは 1 つの EtherChannel に最大 16 個のアクティブ リンクをまとめることができます。ファブリック エクステンダ上で vPC を設定した場合、各 EtherChannel で使用できるポートは 1 つだけです。

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

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

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

vPC ドメインには、両方の vPC ピア デバイス、vPC ピアキープアライブ リンク、vPC ピア リンク、および vPC ドメイン内にあってダウンストリーム デバイスに接続されているすべての EtherChannel 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） EtherChannel を使用する vPC デバイスはすべて、両方の vPC ピア デバイスに接続する必要があります。

vPC には次のような特長があります。

- 単独のデバイスが、2 つのアップストリーム デバイスを介して EtherChannel を使用できるようになります。
- スパニングツリー プロトコル（STP）のブロック ポートが不要になります。
- ループフリーなトポロジが実現されます。
- 利用可能なすべてのアップリンク帯域幅を使用します。
- リンクまたはスイッチに障害が発生した場合、高速コンバージェンスが実行されます。
- リンクレベルの復元力を提供します。
- ハイ アベイラビリティが保証されます。

用語

vPC の用語

vPC で使用される用語は、次のとおりです。

- vPC：vPC ピア デバイスとダウンストリーム デバイスの間の結合された EtherChannel。
- vPC ピア デバイス：vPC ピア リンクと呼ばれる特殊な EtherChannel により接続されることで対をなす個々のデバイス。
- vPC ピア リンク：vPC ピア デバイス間の状態を同期するために使用されるリンク。
- vPC メンバー ポート：vPC に属するインターフェイス。
- ホスト vPC ポート：vPC に属するファブリック エクステンダのホスト インターフェイス。
- vPC ドメイン：両方の vPC ピア デバイス、vPC ピアキープアライブ リンク、vPC 内にあってダウンストリーム デバイスに接続されているすべてのポート チャネルが含まれるドメイン。また、このドメインは、vPC グローバル パラメータを割り当てるために使用する必要があるコンフィギュレーション モードに関連付けられています。vPC ドメイン ID は、両スイッチで同じであることが必要です。
- vPC ピアキープアライブ リンク：ピアキープアライブ リンクでは、vPC ピア Cisco Nexus デバイスの稼働力のモニタリングが行われます。ピアキープアライブ リンクは、vPC ピア デバイス間での設定可能なキープアライブ メッセージの定期的な送信を行います。

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

ファブリック エクステンダの用語

Cisco Nexus ファブリック エクステンダで使用される用語は、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に特化した 10 ギガビット イーサネットのアップリンク ポートです。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 アップリンク接続です。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：サーバ接続またはホスト接続に使用するイーサネット インターフェイスです。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 インターフェイスになる場合と、10 ギガビット イーサネット インターフェイスになる場合があります。
- 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サーバ ポートへの EtherChannel ダウンリンク接続です。

（注） EtherChannel ホスト インターフェイスは 1 個のホスト 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 として設定できます。

サポートされている vPC トポロジ

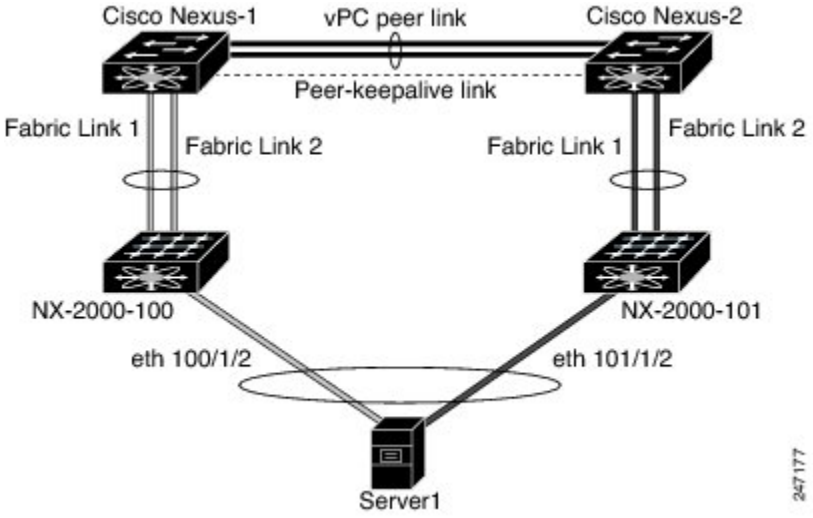
Cisco Nexus デバイスの vPC トポロジ

シングル ホーム ファブリック エクステンダの vPC トポロジ

図のように、Cisco Nexus デバイスに接続された Cisco Nexus ファブリック エクステンダのペアに、vPC で設定された 2 つまたは 4 つまたはそれ以上のネットワーク アダプタを持つサーバを接続できます。各ファブリック エクステンダには、FEX モデルに応じて、1 台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ます。次の図はその具体例として、Cisco Nexus 2148T ファブリック エクステンダを使用して構成したトポロジを示したものです。サーバから各ファブリック エクステンダへのリンクはそれぞれ 1 つだけです。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。

下図に示したトポロジでは、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持つデュアル ホーム サーバに対して vPC 機能が実現されています。

図 *8*：シングル ホーム ファブリック エクステンダの *vPC* トポロジ



Cisco Nexus デバイスは、このトポロジで最大 12 台の設定済みシングル ホーム ファブリック エクステンダ（576 ポート）をサポートできますが、この構成による vPC では 480 576 台のデュアル ホーム接続されたホスト サーバだけを設定することかできます。

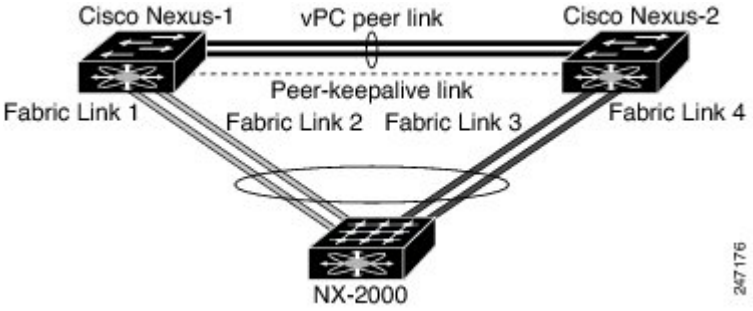
（注） Cisco Nexus 2148T ファブリック エクステンダは、ホスト インターフェイスでの EtherChannel はサポートしていません。そのため、1 つの EtherChannel で設定できるサーバからのリンクは最大 2 つで、各リンクは別々のファブリック エクステンダに接続されます。

デュアル ホーム ファブリック エクステンダの vPC トポロジ

Cisco Nexus ファブリック エクステンダを、アップストリームにある 2 台の Cisco Nexus デバイス、およびダウンストリームにある複数のシングルホームサーバに接続することができます。次の図

に示したトポロジは、1 ギガビット イーサネット アップリンク インターフェイスでそれぞれ別々に接続されたサーバに対して vPC 機能を実現したものです。

図 *9*：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 デバイスは、このトポロジで最大 12 台の設定済みデュアル ホーム接続された ファブリック エクステンダをサポートできます。この構成では、最大 576 台のシングル ホーム サーバを接続できます。

vPC ドメイン

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

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

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

vPC ピア スイッチでは、設定した vPC ドメイン ID に基づいて、一意の vPC システム MAC アドレスが自動的に割り当てられます。スイッチで vPC システム MAC アドレスが使用されるのは、LACP や BPDU などリンク関連の処理に限ります。vPC ドメインに特定の MAC アドレスを設定することもできます。

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（一方がアクセス スイッチ、もう一方が集約スイッチ）がある場合は、それぞれの vPC に固有のドメイン ID を割り当ててください。

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

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

ピアキープアライブ リンクとメッセージ

Cisco NX-OS ソフトウェアでは、vPC ピア間のピアキープアライブ リンクを使用して、設定可能なキープアライブ メッセージが定期的に送信されます。これらのメッセージを送信するためには、ピア スイッチ間にレイヤ 3 接続が必要です。ピアキープアライブ リンクがアップ状態で稼働していなければ、システムでは vPC ピア リンクをアップすることができません。

ホールドタイムアウトとタイムアウト値を同時に設定できます。

ホールドタイムアウト値：ホールドタイムアウト値の範囲は 3 ～ 10 秒です。デフォルト値は 3 秒です。このタイマーは、vPC ピア リンクが停止した時点で開始します。ホールドタイムアウト期間の目的は、誤ったポジティブ ケースを防ぐことです。

タイムアウト値よりも小さいホールドタイムアウト値を設定した場合、vPC システムはホールドタイムアウト期間の vPC ピア キープアライブ メッセージを無視し、タイムアウト期間のリマインダのメッセージを考慮します。この期間にキープアライブ メッセージを受信しなかった場合、vPC セカンダリ デバイスがプライマリ デバイスの役割を引き継ぎます。たとえば、ホールドタイムアウト値が 3 秒でタイムアウト値が 5 秒の場合、最初の 3 秒間は vPC キープアライブ メッセージが無視され（ピア リンク障害後の数秒間のスーパバイザ障害に適応する場合など）、残りのタイムアウト期間の 2 秒間はキープアライブ メッセージが考慮されます。この期間が過ぎると、キープアライブ メッセージがない場合には vPC セカンダリ デバイスがプライマリ デバイスとして引き継ぎます。

タイムアウト値：タイムアウト値の範囲は 3 ～ 20 秒です。デフォルト値は 5 秒です。このタイマーは、ホールドタイムアウト間隔が終了した時点で開始します。ホールドタイムアウト値以下のタイムアウト値を設定した場合、タイムアウト期間はホールドタイムアウト期間の後に開始されます。たとえば、タイムアウト値が 3 秒でホールドタイムアウト値が 5 秒の場合、タイムアウト期間は 5 秒後に開始されます。

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

vPC ピア リンクの互換パラメータ

多くの設定パラメータおよび動作パラメータが、vPC 内のすべてのインターフェイスで同じでなければなりません。vPC 機能をイネーブルにし、さらに両方の vPC ピア スイッチ上でピア リンクを設定すると、シスコ ファブリック サービス（CFS）メッセージにより、ローカル vPC ピア スイッチに関する設定のコピーがリモート vPC ピア スイッチへ送信されます。これによりシステムでは、2 つのスイッチ間で重要な設定パラメータに違いがないかどうか判定が行われます。

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

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

同じでなければならない設定パラメータ

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

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

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

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

- ポートチャネル モード：オン、オフ、またはアクティブ
- チャネル単位のリンク速度
- チャネル単位のデュプレックス モード
- チャネルごとのトランク モード：
  - ネイティブ VLAN
  - トランク上で許可される VLAN
  - ネイティブ VLAN トラフィックのタギング
- スパニング ツリー プロトコル（STP）モード
- マルチ スパニングツリーの STP 領域コンフィギュレーション（MST）

- VLAN ごとのイネーブル/ディセーブル状態
- STP グローバル設定：
  - ブリッジ保証設定
  - ポートタイプ設定：vPCインターフェイスはすべて標準ポートとして設定することが推奨されます
  - ループ ガード設定
- STP インターフェイス設定：
  - ポート タイプ設定
  - ループ ガード
  - ルート ガード
- ファブリック エクステンダの vPC トポロジの場合、上記のインターフェイス レベル パラメータはすべて、両側スイッチのホストインターフェイスに対して設定を同じにする必要があります。
- EtherChannel ファブリック インターフェイス上で設定されたファブリック エクステンダの FEX 番号（ファブリック エクステンダの vPC トポロジの場合）。

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

（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いずれかが両方の 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 リンクの両端にある各スイッチの VLAN インターフェイスは同じ VLAN 用に設定されている必要があり、さらにそれらの管理モードおよび動作モードも同じであることが必要です。ピア リンクの一方のスイッチでのみ設定されている VLAN では、vPC またはピア リンクを使用したトラフィックの転送は行われません。VLAN はすべて、プライマリ vPC スイッチとセカンダリ vPC スイッチの両方で作成する必要があります。両方で作成されていない場合、VLAN は停止することになります。

- 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）の設定およびパラメータ：ローカル パラメータです。グローバル パラメータは同じであることが必要です
- STP インターフェイス設定：
  - BPDU Filter
  - BPDU ガード
  - コスト
  - リンク タイプ
  - プライオリティ
  - VLAN（Rapid PVST+）

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

グレースフル タイプ 1 検査

整合性検査で不整合が検出された場合、セカンダリ vPC スイッチ上でのみ vPC がダウン状態になります。プライマリ vPC スイッチ上の VLAN はアップ状態が維持されるため、トラフィックを中断することなくタイプ 1 の設定を実行することができます。この機能は、グローバル タイプ 1 不整合の場合にも、インターフェイス別タイプ 1 不整合の場合にも使用されます。

この機能は、デュアルアクティブ FEX ポートに対しては無効です。タイプ 1 の不一致が発生すると、両側スイッチのこれらのポートでは VLAN が停止します。

VLAN ごとの整合性検査

Cisco NX-OS Release 5.0(2)N2(1) 以降では、VLAN 上でスパニングツリーのイネーブル/ディセーブルが切り替わるたびに、いくつかのタイプ 1 整合性検査が VLAN ごとに実行されます。この整合性検査に合格しない VLAN は、プライマリ スイッチおよびセカンダリ スイッチでダウン状態になりますが、その他の VLAN は影響を受けません。

vPC 自動リカバリ

Cisco NX-OS Release 5.0(2)N2(1) 以降では、次のような状況が発生すると、vPC 自動リカバリ機能により vPC リンクが再イネーブル化されます。

両側の vPC ピア スイッチでリロードが実行され、かつ一方のスイッチのみリブートした場合、自動リカバリによってそのスイッチがプライマリ スイッチとして機能し、一定時間が経過した後に

vPC リンクがアップ状態になります。このシナリオにおけるリロード遅延時間は、240 ～ 3600 秒の範囲で設定できます。

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

vPC 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 リンクを設定する場合は、あらかじめピアキープアライブ リンクを設定しておく必要があります。設定しておかないと、ピア リンクは機能しません

vPC ピア リンクの概要

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

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

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

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

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

vPC ピア リンクを設定する際、vPC ピア スイッチでは、接続されたスイッチの一方がプライマリ スイッチ、もう一方がセカンダリ スイッチとなるようにネゴシエーションが行われます。デフォルトの場合、Cisco NX-OS ソフトウェアでは、最小の MAC アドレスを基にプライマリ スイッチ

が選択されます。特定のフェールオーバー条件の下でのみ、このソフトウェアは各スイッチ（つまり、プライマリ スイッチとセカンダリ スイッチ）に対して別々の処理を行います。プライマリ スイッチに障害が発生した場合、システムが回復した時点でセカンダリ スイッチがプライマリ スイッチとして動作し、元々のプライマリ スイッチがセカンダリ スイッチとなります。

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

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

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

vPC ピア リンクに障害が発生すると、ソフトウェアでは、両方のスイッチが稼働していることを確認するため、vPC ピア スイッチ間のリンクであるピアキープアライブ リンクを使用してリモート vPC ピア スイッチのステータス確認が行われます、vPC ピア スイッチが稼働している場合は、セカンダリ vPC スイッチにあるすべて vPC ポートがディセーブルになります。さらにデータは、EtherChannel において依然アクティブ状態にあるリンクに転送されます。

ソフトウェアは、ピアキープアライブ リンクを介してキープアライブ メッセージが返されない場合、vPC ピア スイッチに障害が発生したと認識します。

vPC ピア スイッチ間では、別途用意されたリンク（vPC ピアキープアライブ リンク）を使用して、設定可能なキープアライブ メッセージが送信されます。vPC ピアキープアライブ リンク上のキープアライブ メッセージにより、障害が vPC ピア リンク上でだけ発生したのか、vPC ピア スイッチ上で発生したのかが判断されます。キープアライブ メッセージは、ピア リンク内のすべてのリンクで障害が発生した場合にだけ使用されます。

vPC 番号

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

各 vPC ピア スイッチ上では、ダウンとリーム スイッチに接続された EtherChannel に同じ vPC 番号を割り当てます。vPC の作成時にトラフィックが中断されることはほとんどありません。設定を簡素化するため、各 EtherChannel に対してその EtherChannel と同じ番号の vPC ID 番号を割り当てることもできます（EtherChannel 10 に対しては vPC ID 10 を割り当てるなど）。

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

vPC を介したレイヤ 3

Cisco NX-OS Release 7.3(0)N1(1) から、レイヤ 3（L3）デバイスは vPC ドメイン内の vPC ピアの両方とピアリング隣接関係を形成することができます。ピア リンクを介して送信されるトラフィックに TTL の減少はありません。

Cisco Nexus 5500 シリーズ スイッチは、ドーター L3 モジュールを持つ場合にのみ、この機能をサポートします。

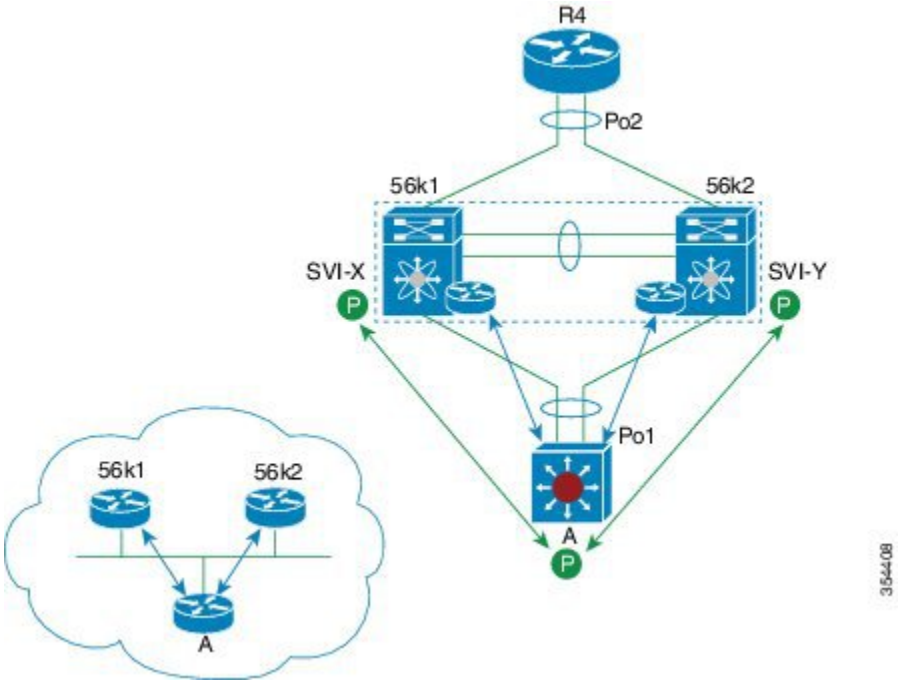
ピア ゲートウェイ機能は、vPC 機能を介してレイヤ 3 を設定する前に有効にする必要があります。

この機能を設定する利点を次に示します。

- 個別のレイヤ 3 リンクを使用せずに、レイヤ 3 デバイスと vPC ピアの間のピアの隣接関係を設定できます。ブリッジされたトラフィックとルーティングされたトラフィックの両方を同じリンクで送ることができます。
- ピアの隣接関係を vPC VLAN で形成できます。
- ピアの隣接関係は、トラフィックでリンクまたはデバイスの障害が発生した場合に高速コンバージェンスのために役立ちます。

次の図では、ピア ゲートウェイ機能が別のピア（SVI Y）の代わりにパケットを転送することを vPC ピア（SVI X）に許可しています。これにより、ピア リンクを介したトラフィックがなくなり帯域幅を節約できます。

図 *10*：*vPC* ソリューションを介したレイヤ *3*



vPC を介したレイヤ 3：サポートされている設計

次の図は、vPC を介したレイヤ 3 の設定でサポートされる設計を示しています。

図 *11*：両方の *vPC* ピアを使用するルータ ピア

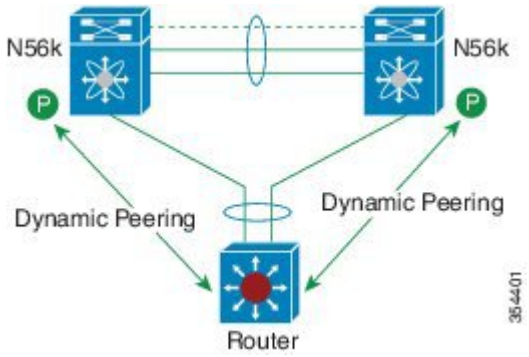
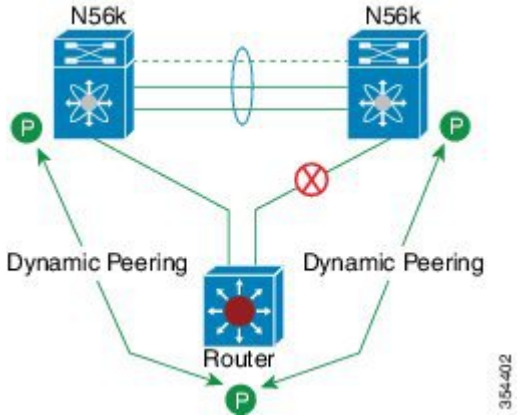


図 *12*：*vPC VLAN* を使用して *STP* の相互接続を介して確立されるピアリング



両方の vPC ピアを使用するルータ ピア。

図 *13*： 両方の *vPC* ピアを使用する孤立デバイスのルート ピアリング

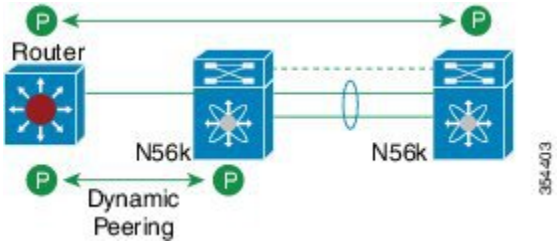
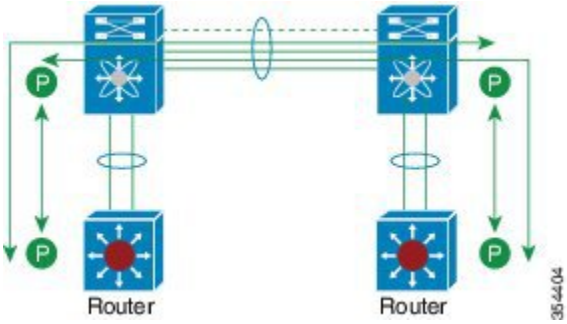
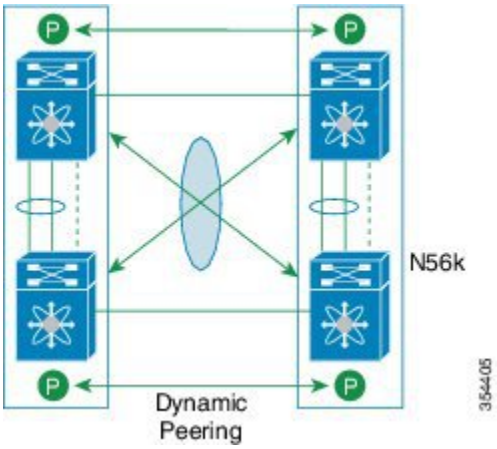


図 *14*： *vPC VLAN* を使用した *PC* の相互接続および *vPC* ピア リンクを介したピアリング



両方の vPC ピアを使用する両方のルータ ピア。

図 *15*： *vPC* の相互接続を介したピアリング（*DCI* の場合）



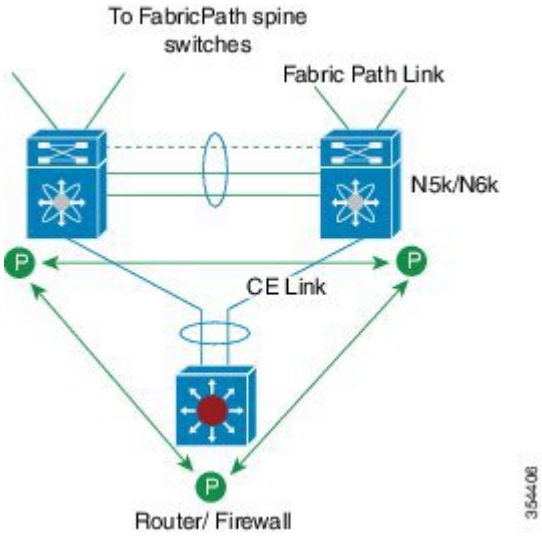
2 つの vPC ピアを使用する各 Nexus デバイス ピア。

vPC+ を使用したピアリング（Release 6.0(2)N2(1) からサポート）：

- ピア リンク ポートは FabricPath コア ポートとして設定されます。
- North facing ポートが FabricPath スパイン ポートとして機能します。

- North facing ポートは非 FabricPath トポロジのレイヤ 3 ポートとして機能することもできます。

図 *16*： *vPC+* を使用したピアリング



vPC を介したレイヤ 3：サポートされていない設計

次の図は、vPC 機能を介したレイヤ 3 の設定でサポートされない設計を示しています。

2 つの孤立デバイスの間の TTL 距離が 2 のため、次の設計はサポートされません。これは、ルーティングの隣接関係を形成する際に vPC で制御パケットが失われる原因となります。

図 *17*：*vPC* の相互接続を介した孤立デバイスのピアリング（*DCI* の場合）

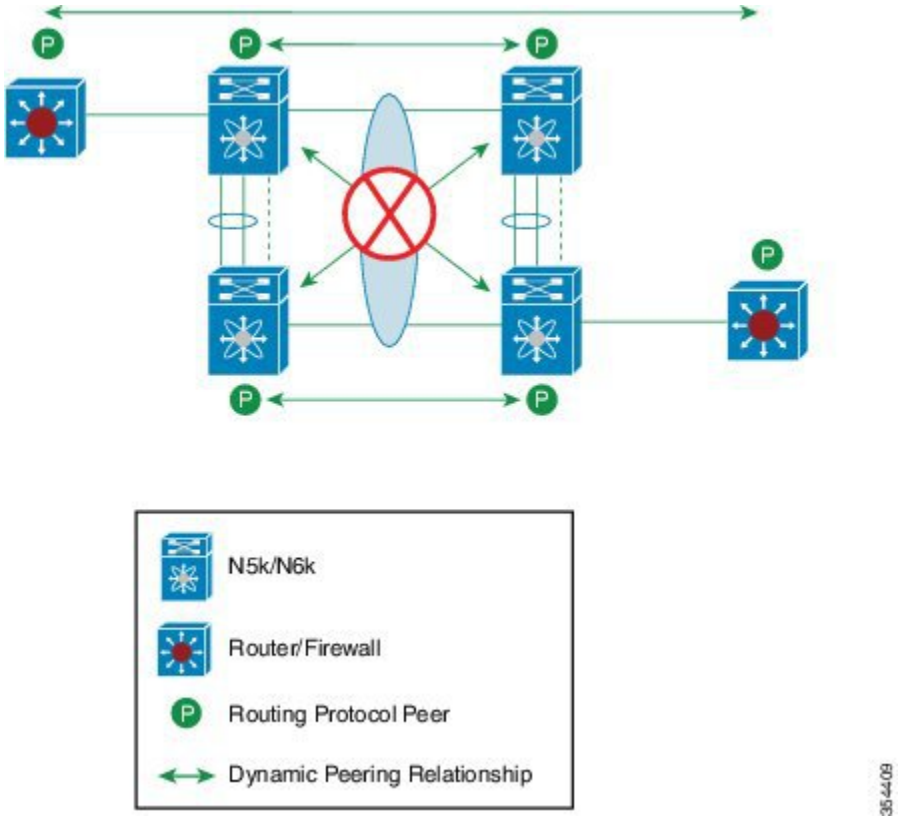


図 *18*：*FEX vPC* ホスト インターフェイスを介した *vPC* ピアを使用したピアリング

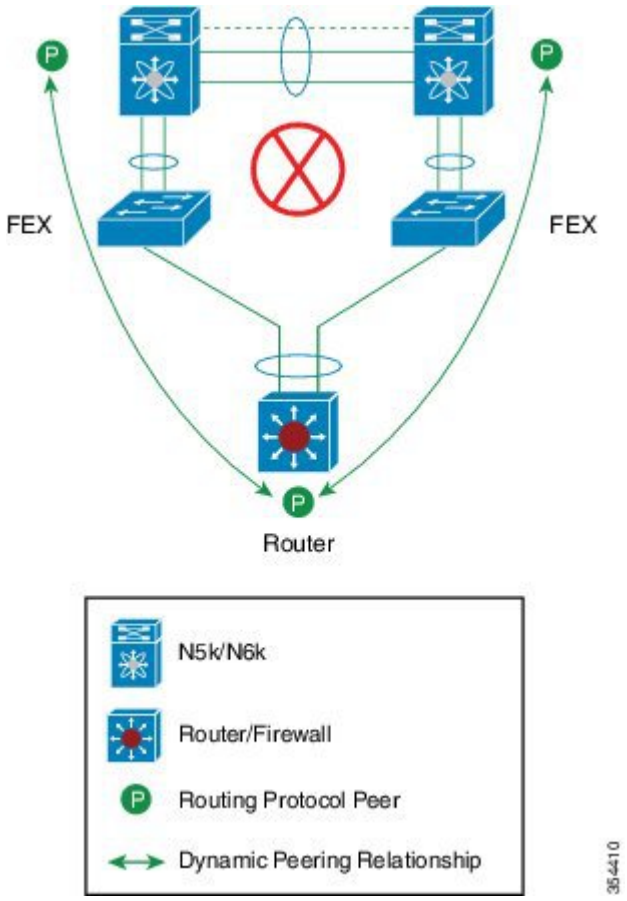


図 *19*： 不等 *L3* メトリックを使用した *vPC* インターフェイス間のピアリング

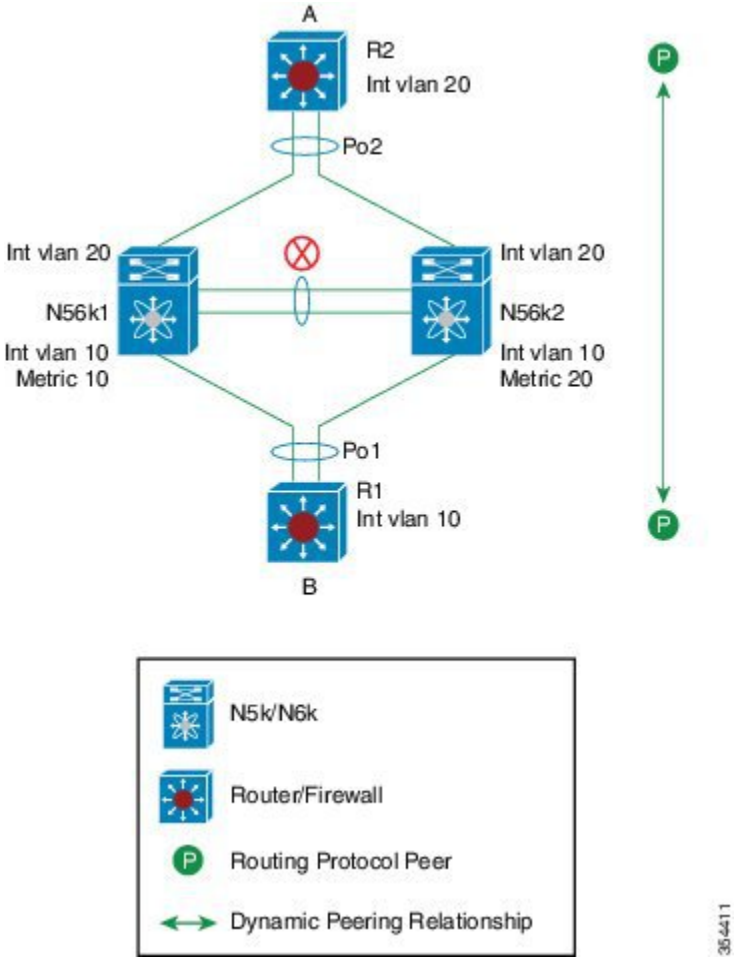


図 *20*： ***vPC+ VLAN*** を使用した ***vPC+*** ピアおよび ***STP*** の相互接続によるピアリング

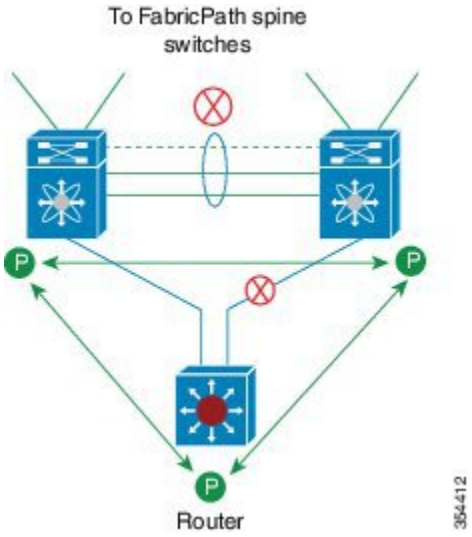


図 *21*： 両方の ***vPC+*** ピアを使用した孤立デバイスによるルート ピアリング

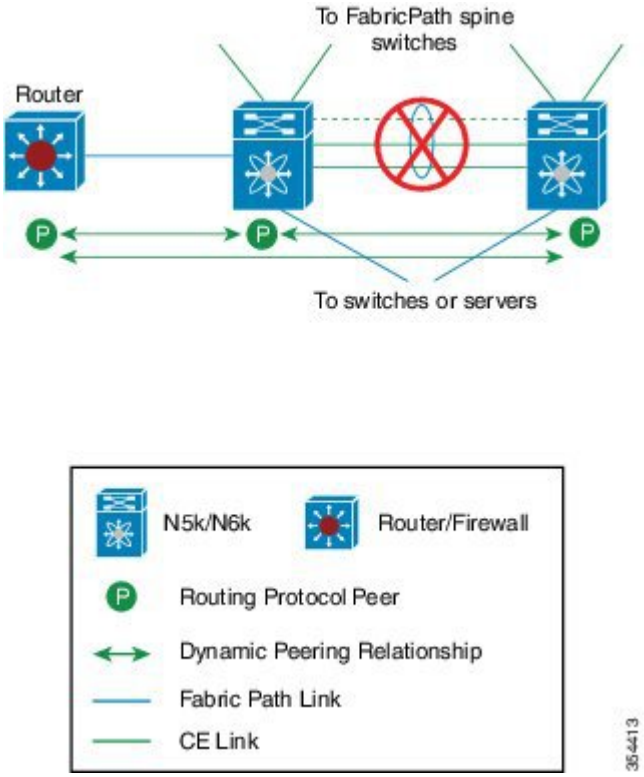
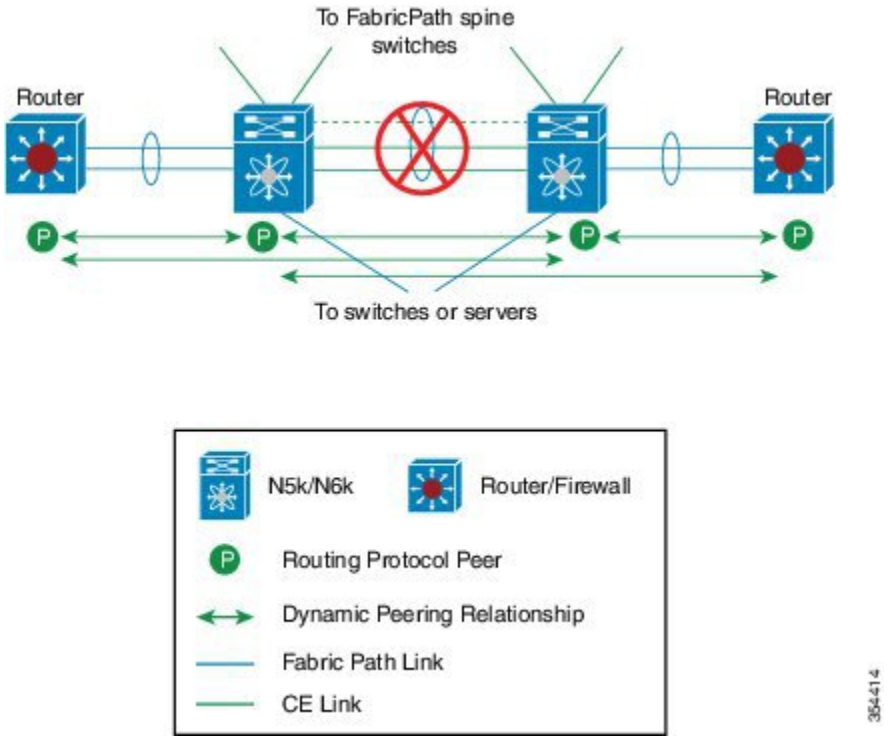


図 *22*： ***vPC VLAN*** を使用した ***PC*** の相互接続および ***vPC+*** ピア リンクを介したピアリング



その他の機能との vPC の相互作用

vPC ピア リンクおよびコアへのリンクの設定

コアおよび両方の vPC ピア デバイス上のすべての vPC ピア リンクへのレイヤ 3 リンクに関連付けられたトラック オブジェクトおよびトラック リストを使用して、コマンドライン インターフェイスを設定します。トラック リスト上のすべてのトラッキング対象オブジェクトが停止した場合、システムは次のように動作するため、この設定を使用すれば、その特定のモジュールが停止した場合のトラフィックのドロップを避けることができます。

- vPC プライマリ ピア デバイスによるピアキープアライブ メッセージの送信を停止します。これにより、vPC セカンダリ ピア デバイスが強制的に引き継がされます。
- その vPC ピア デバイス上のすべてのダウンストリーム vPC を停止させます。これにより、すべてのトラフィックが強制的に他の vPC ピア デバイスに向けてそのアクセス スイッチでルーティングされます。

いったんこの機能を設定したら、モジュールに障害が発生した場合には、システムが自動的にプライマリ vPC ピア デバイス上のすべての vPC リンクを停止させ、ピアキープアライブ メッセージを停止します。このアクションにより、vPC セカンダリ デバイスが強制的にプライマリ ロールを引き継がされ、システムが安定するまで、すべての vPC トラフィックがこの新しい vPC プライマリ デバイスに送られます。

コアに対するすべてのリンクおよびすべての vPC ピア リンクを含むトラック リストを、そのオブジェクトとして作成します。このトラック リストの指定した vPC ドメインに対して、トラッキングをイネーブルにします。この同じ設定を他方の vPC ピア デバイスにも適用します。

はじめる前に

関連するすべてのインターフェイスに障害が発生した場合にリモート ピアに vPC をスイッチオーバーするためのトラック リストを設定するには、次のように行います。

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** *type 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)# **track** *track-id* **interface** *type slot/port* **line-protocol**	インターフェイス（コアへのレイヤ 3）でトラック オブジェクトを設定します。
ステップ 4	switch(config-track)# **track** *track-id* **interface** *type slot/port* **line-protocol**	インターフェイス（コアへのレイヤ 3）のオブジェクトを追跡します。
ステップ 5	switch(config)# **track** *track-id* **interface port-channel** *port* **line-protocol**	ポート チャネル（vPC ピア リンク）でトラック オブジェクトを設定します。
ステップ 6	switch(config)# **track** *track-id* **list boolean** [**OR** | **AND**]	トラック リストのすべてのインターフェイスを含むトラック リストを作成し、ブーリアン OR を使用してすべてのオブジェクトが失敗した場合にトリガーするか、ブーリアン AND を使用していずれかのコア インターフェイスまたはピア リンクがダウンしたときにスイッチオーバーをトリガーします。
ステップ 7	switch(config-track)# **object** *number*	オブジェクト番号を指定します。
ステップ 8	switch(config-track)# **end**	トラック 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)# **vpc domain** *domain-id*	vPC ドメイン コンフィギュレーションを開始します。
ステップ 10	switch(config-vpc-domain)# **track** *number*	vPC ドメインにトラック オブジェクトを追加します。

	コマンドまたはアクション	目的
ステップ 11	switch(config)# **show vpc brief**	（任意） トラック オブジェクトを表示します。
ステップ 12	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、変更を継続的に保存します。

次に、すべてのオブジェクトで障害が発生したときにトリガーするように、ブール OR を使って追跡リストを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 8/35
switch(config-if)# track 35 interface ethernet 8/35 line-protocol
switch(config-track)# track 23 interface ethernet 8/33 line-protocol
switch(config)# track 55 interface port-channel 100 line-protocol
switch(config)# track 44 list boolean OR
switch(config-track)# object 23
switch(config-track)# object 35
switch(config-track)# object 55
switch(config-track)# end
switch(config)# vpc domain 1
switch(config-vpc-domain)# track 44
switch(config)# copy running-config startup-config
```

vPC と LACP

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

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

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

（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 スイッチ上に同じプライオリティ値を割り当てるようにしてください。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。

（注） （セカンダリがプライマリになる）vPC の役割の変更中に、FEX でポートが LACP-individual 状態の場合、そのポートがフラップし、プライマリが作動する前に接続が短時間の間失われる原因となります。この問題を回避するには、ポートチャネルメンバーポートが LACP-individual 状態として設定されていないか、LACP が使用されていないことを確認します（On モード）。

vPC ピア リンクと STP

vPC 機能の初回起動時には、STP は再コンバージェンスします。STP は、vPC ピア リンクを特殊なリンクとして扱い、常に vPC ピア リンクを STP のアクティブ トポロジに含めます。

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

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

STP は分散型です。つまり、このプロトコルは、両端の vPC ピア スイッチ上で継続的に実行されます。ただし、セカンダリ vPC ピア スイッチ上の vPC インターフェイスの STP プロセスは、プライマリ スイッチとして選択されている vPC ピア スイッチ上での設定により制御されます。

プライマリ vPC スイッチでは、Cisco Fabric Services over Ethernet（CFSoE）を使用して、vPC セカンダリ ピア スイッチ上の STP 状態の同期化が行われます。

vPC ピア スイッチ間では、プライマリ スイッチとセカンダリ スイッチを設定して 2 つのスイッチを STP 用に調整する提案/ハンドシェイク合意が vPC マネージャによって実行されます。さらにプライマリ vPC ピア スイッチにより、プライマリ スイッチおよびセカンダリ スイッチの vPC インターフェイスに対する STP プロトコルの制御が行われます。

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

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

vPC と ARP

Cisco NX-OS では、Cisco Fabric Services over Ethernet（CFSoE）プロトコルが持つ信頼性の高い転送メカニズムによって、vPC ピア間のテーブルの同期が管理されます。vPC ピア間でアドレステーブルの高速コンバージェンスをサポートするためには、**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場合や vPC ピアがオンラインに戻った場合に、ARP テーブルの復元に伴う遅延の解消を目的としたものです。

パフォーマンスを向上させるためにも、ARP 同期機能はイネーブルにすることが推奨されます。デフォルトではディセーブルです。

ARP 同期がイネーブルかどうかを確認する場合は、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場合は、次のコマンドを入力します。

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

CFSoE

Cisco Fabric Services over Ethernet（CFSoE）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。CFSoE は、vPC にリンクされている、STP、IGMP などの多くの機能のメッセージとパケットを伝送します。情報は、CFS/CFSoE プロトコル データ ユニット（PDU）に入れて伝送されます。

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

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

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

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

vPC 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、Cisco Nexus デバイスのペアをレイヤ 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 拡張機能と Rapid PVST+ の詳細については、ご使用のデバイスの『*Layer 2 Switching Configuration Guide*』を参照してください。

VRF に関する注意事項と制約事項

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場合は、あらかじめ vPC 機能をイネーブルにしておく必要があります。
- システムにおいて vPC ピア リンクを構成するためには、その前にピアキープアライブ リンクを設定しておく必要があります。
- vPC ピアリンクは、少なくとも 2 つの 10 ギガビット イーサネット インターフェイスを使用して構成する必要があります。
- vPC に使用できるのは、ポート チャネルのみです。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 インターフェイスの vPC トポロジのメンバーになることもファブリック エクステンダの vPC トポロジのメンバーになることも可能ですが、同時に両方のメンバーになることはできません。
- 両側の vPC ピア スイッチを設定する必要があります。ただし vPC ピア デバイス間で設定が自動的に同期化されることはありません。
- 必要な設定パラメータが、vPC ピア リンクの両側で互換性を保っているかチェックしてください。
- vPC の設定中に、最小限のトラフィックの中断が発生する可能性があります。
- vPC 内の LACP を使用するポート チャネルはすべて、アクティブ モードのインターフェイスで設定することが推奨されます。
- **peer-switch** コマンドが設定され、vPC キープアライブ メッセージが管理インターフェイスの代わりに SVI を介して交換されている場合、追加のスパニングツリー プロトコル（STP）コンフィギュレーションが必要です。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。専用リンクの両端に STP BPDUfilter

を設定することで、専用リンク上で 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。

- ルータと vPC ピアに接続された Cisco Nexus 5500 シリーズ スイッチは、接続されているルータとの OSPF 関連付けを作成しますが、vPC ピアとは作成しません。この状況は、非 vPC VLAN が vPC ピア間の別のトランクに存在する場合に発生します。非 vPC VLAN が vPC ピア リンクにある場合、OSPF は、両方の vPC ピアのように動作します。この状況は、peer-gateway がイネーブルの場合のみです。

vPC の設定

vPC のイネーブル化

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

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 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 デバイスがすべての 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**	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)# **no feature vpc**	スイッチで 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

両側の vPC ピア スイッチに対して、同じ vPC ドメイン ID を作成する必要があります。このドメイン ID を基に、vPC システムの MAC アドレスが自動的に構成されます。

はじめる前に

vPC 機能が有効なことを確認します。

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**	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)# **vpc domain***domain-id*	スイッチに対して vPC ドメインを作成し、vpc-domain コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
		domain-id のデフォルト値はありません。指定できる値の範囲は 1 ～ 1000 です。 （注） 既存の vPC ドメインに対して vpc-domain コンフィギュレーション モードを開始する場合は、**vpc domain** コマンドを使用することもできます。
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 ソフトウェアは、vPC ピア間でピアキープアライブ リンクを使用して、設定可能なキープアライブメッセージを定期的に送信します。これらのメッセージを送信するには、ピアデバイス間にレイヤ 3 接続が必要です。ピアキープアライブ リンクが起動および動作していないと、システムは vPC ピア リンクを開始できません。

ピアキープアライブメッセージに使用される送信元と宛先の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）インスタンスから、これらの IP アドレスが到達可能であることを確認してください。

（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 インスタンスにレイヤ 3 ポートを接続することが推奨されます。ピア リンク自体を使用して vPC ピアキープアライブ メッセージを送信しないでください。VRF の作成と設定については、ご使用のデバイスの『Unicast Routing Configuration Guide』を参照してください。

はじめる前に

vPC 機能が有効なことを確認します。

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

vPC ピア リンクの両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**	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)# **vpc domain***domain-id*	スイッチ上に vPC ドメインが存在しない場合はそれを作成し、vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	switch(config-vpc-domain)# **peer-keepalive destination***ipaddress* [**hold-timeout***secs* | **interval***msecs* {**timeout***secs*} | **precedence** {*prec-value* | **network** | **internet** | **critical** | **flash-override** | **flash** | **immediate priority** | **routine**} | **tos** {*tos-value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal**} | **tos-byte***tos-byte-value*} | **source***ipaddress* | **vrf** {*name* | **management vpc-keepalive**}]	vPC ピアキープアライブ リンクのリモートエンドの IPv4 アドレスを設定します。 （注） vPC ピアキープアライブ リンクを設定するまで、vPC ピア リンクは構成されません。 管理ポートと VRF がデフォルトです。
ステップ 4	switch(config-vpc-domain)# **vpc peer-keepalive destination** *ipaddress* **source***ipaddress*	（任意） vPC ピアキープアライブ リンクに対し、個別の VRF インスタンスを設定して、各 vPC ピア デバイスからその VRF にレイヤ 3 ポートを接続します。
ステップ 5	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。

次の例は、vPC ピアキープアライブ リンクの宛先 IP アドレスを設定する方法を示したものです。

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

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

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

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

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

L3-NEXUS-2# show vpc peer-keepalive

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

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

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

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

vPC ピア リンクの作成

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

はじめる前に

vPC 機能が有効なことを確認します。

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**	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 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
```

設定の互換性の検査

両側の vPC ピア スイッチに vPC ピア リンクを設定した後に、すべての vPC インターフェイスで設定に整合性があるかどうかの検査を行います。

（注） Cisco NX-OS Release 5.0(2)N1(1) 以降では、次の QoS パラメータでタイプ 2 整合性検査がサポートされています。

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

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

コマンドまたはアクション	目的
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     2     (F, F, F, F, F, F)     (100, 0, 0, 0, 0, 0)
Priority)
Output Queuing (Bandwidth)  2     (100, 0, 0, 0, 0, 0)   (100, 0, 0, 0, 0, 0)
Output Queuing (Absolute    2     (F, F, F, F, F, F)     (100, 0, 0, 0, 0, 0)
Priority)
STP Mode                    1     Rapid-PVST             Rapid-PVST
STP Disabled                1     None                   None
STP MST Region Name         1     ""                     ""
STP MST Region Revision     1     0                      0
STP MST Region Instance to  1
  VLAN Mapping

STP Loopguard               1     Disabled               Disabled
STP Bridge Assurance        1     Enabled                Enabled
STP Port Type, Edge         1     Normal, Disabled,      Normal, Disabled,
BPDUFilter, Edge BPDUGuard        Disabled               Disabled
STP MST Simulate PVST       1     Enabled                Enabled
Allowed VLANs               -     1,624                  1
Local suspended VLANs       -     624                    -
switch#
```

次の例は、1 つの EtherChannel インターフェイスについて必須設定の互換性があるかどうか検査する方法を示したものです。

```
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**	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)# **vpc domain***domain-id*	既存の vPC ドメインに対して vpc-domain コンフィギュレーション モードを開始します。
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、リロード遅延時間を設定します。デフォルトではディセーブルになっています。

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
```

復元遅延時間の設定

Cisco NX-OS Release 5.0(3)N1(1) 以降では、ピアの隣接が形成され、VLAN インターフェイスがバックアップされるまで、vPC の再稼働を遅らせるように復元タイマーを設定できます。この機能により、vPC が再びトラフィックの受け渡しをしはじめる前にルーティング テーブルが収束できなかった場合のパケットのドロップを回避できます。

はじめる前に

vPC 機能が有効なことを確認します。

vPC ピア リンクの両端にあるそれぞれのスイッチで設定を行う必要があります。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**	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)# **vpc domain***domain-id*	スイッチ上に vPC ドメインが存在しない場合はそれを作成し、vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	switch(config-vpc-domain)# **delay restore***time*	vPC が復元されるまでの遅延時間を設定します。 復元時間は、復元された vPC ピア デバイスが稼働するまで遅延時間（単位は秒）です。有効な範囲は 1 ～ 3600 です。デフォルトは 30 秒です。 （注） L3 ライセンスがインストールされている場合、復元遅延時間は 150 秒に設定されます。 16 以上のファブリック エクステンダがある場合、復元遅延時間は 90 秒に設定されます。
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 リンクに対する復元遅延時間の設定方法を示したものです。

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

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

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

はじめる前に

VLAN インターフェイスが設定済みであることを確認します。

手順

	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)# **vpc domain***domain-id*	スイッチ上に vPC ドメインが存在しない場合はそれを作成し、vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	switch(config-vpc-domain))# **dual-active exclude interface-vlan***range*	vPC ピアリンクが失われた場合でもアップ状態を維持する必要がある VLAN インターフェイスを指定します。 range：シャットダウンしないようにする VLAN インターフェイスの範囲を指定します。指定できる範囲は 1 ～ 4094 です。

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

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

VRF 名の設定

ping、ssh、telnet、radius などのスイッチ サービスは VRF 対応です。適切なルーティング テーブルを使用するためには、VRF 名を設定する必要があります。

VRF 名を指定することができます。

手順

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

次に、vpc_keepalive という名前の VRF を指定する例を示します。

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

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

vPC への VRF インスタンスのバインド

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

はじめる前に

スイッチで使用中のインターフェイスを表示する場合は、**show interfaces brief** コマンドを使用します。VRF インスタンスを vPC にバインドするには、未使用の VLAN を使用する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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)# **vpc bind-vrf***vrf-name***vlan** *vlan-id*	VRF インスタンスを vPC にバインドし、vPC にバインドする VLAN を指定します。VLAN ID の範囲は 1 ～ 3967 および 4049 ～ 4093 です。

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

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

vPC のゲートウェイ MAC アドレスを宛先とするレイヤ 3 転送のイネーブル化

vPC ピアゲートウェイ機能により、vPC ピアのルータ MAC アドレスを宛先とするパケットに対し、vPC スイッチをアクティブなゲートウェイとして使用することができます。これにより vPC ピアリンクを経由することなくローカルな転送が可能になります。このシナリオでは、この機能によってピアリンクの使用が最適化され、トラフィック損失が回避されます。

仮想ポート チャネル（vPC）のゲートウェイ MAC アドレスを宛先とするパケットに対しては、レイヤ 3 転送をイネーブルにすることかできます。

（注） この機能は、両側の vPC ピア スイッチで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***domain-id*	スイッチ上に vPC ドメインが存在しない場合はそれを作成し、vpc-domain コンフィギュレーション モードを開始します。
ステップ 3	switch(config-vpc-domain))# **peer-gateway***range*	仮想ポートチャネル（vPC）のゲートウェイ MAC アドレスを宛先とするパケットに対してレイヤ 3 転送をイネーブルにします。

次の例は、vPC ピア ゲートウェイをイネーブルにする方法を示したものです。

```
switch(config)# vpc domain 20
switch(config-vpc-domain)# peer-gateway
switch(config-vpc-domain)#
```

vPC トポロジにおけるセカンダリ スイッチの孤立ポートの一時停止

セカンダリ vPC ピア リンクがダウンした場合、非仮想ポート チャネル（vPC）ポートを一時停止することができます。非 vPC ポート（孤立ポート）とは、vPC に属していないポートです。

（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**	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*	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。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **vpc orphan-port suspend**	セカンダリ スイッチがダウンした場合に、指定したポートを一時停止します。 （注） **vpc-orphan-port suspend** コマンドは、物理ポートでのみサポートされます。また、ポート チャネル メンバー ポートではサポートされません。
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） 孤立ポートの設定を表示します。
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、変更を継続的に保存します。

次の例は、孤立ポートを一時停止する方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet ½0
switch(config-if)# vpc orphan-port suspend
```

次の例は、vPC には属していないポートのうち、vPC に属しているポートと同じ VLAN を共有するポートの表示方法を示したものです。

```
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 ファブリック エクステンダからダウンストリーム サーバに接続するため、EtherChannel ホストインターフェイスを作成することができます。ファブリックエクステンダのモデルによっては、EtherChannel ホスト インターフェイス 1 つにつきメンバーにできるホスト インターフェイスは 1 つだけです。Cisco Nexus 2148T では、個々のファブリック エクステンダに対してメンバーにできるインターフェイスは 1 つだけですが、新しいファブリック エクステンダでは、それぞれに対して同じポートチャネルを最大 8 個までメンバーにすることができます。EtherChannel ホスト インターフェイスでファブリック エクステンダのトポロジを使用する vPC を設定するためには、その EtherChannel ホスト インターフェイスを作成する必要があります。

はじめる前に

vPC 機能が有効なことを確認します。

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になっていることを確認します。

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

手順

	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***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。 （注） これが QSFP+ GEMS の場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **channel-group***channel-number***mode** {**active** | **passive** | **on**}	選択したホスト インターフェイスで EtherChannel ホスト インターフェイスを作成します。

	コマンドまたはアクション	目的
ステップ 4	switch(config-if)# **show 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(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、変更を継続的に保存します。

次の例は、EtherChannel ホスト インターフェイスの設定方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 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 機能が有効なことを確認します。

vPC ピア リンクの両端にあるそれぞれのスイッチで設定を行う必要があります。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**	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 port-channel***channel-number*	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 に配置してダウンストリーム スイッチに接続するように設定します。範囲は 1 ～ 4096 です。 vPC ピア スイッチからダウンストリーム スイッチに接続されているポート チャネルに割り当てる vPC 番号は、両方の vPC スイッチで同じでなければなりません。
ステップ 4	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） システム アドレスの設定は、オプションの設定手順です。

はじめる前に

vPC 機能が有効なことを確認します。

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**	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)# **vpc domain***domain-id*	スイッチ上にある既存の vPC ドメインを選択するか、または新規の vPC ドメインを作成して、vpc-domain コンフィギュレーション モードを開始

	コマンドまたはアクション	目的
		します。*domain-id* のデフォルト値はありません。指定できる値の範囲は 1 ～ 1000 です。
ステップ 3	switch(config-vpc-domain)# **system-mac***mac-address*	指定した vPC ドメインに割り当てる MAC アドレスを aaaa.bbbb.cccc の形式で入力します。
ステップ 4	switch# **show vpc role**	（任意） vPC システムの 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。

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

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

システム プライオリティの手動での設定

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

はじめる前に

vPC 機能が有効なことを確認します。

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**	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)# **vpc domain***domain-id*	スイッチ上にある既存の vPC ドメインを選択するか、または新規の vPC ドメインを作成して、vpc-domain コンフィギュレーション モードを開始します。*domain-id* のデフォルト値はありません。指定できる値の範囲は 1 ～ 1000 です。

	コマンドまたはアクション	目的
ステップ 3	switch(config-vpc-domain)# **system-priority***priority*	指定した vPC ドメインに割り当てるシステム プライオリティを入力します。指定できる値の範囲は、1 ～ 65535 です。デフォルト値は 32667 です。
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 スイッチのロールの手動による設定

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

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

はじめる前に

vPC 機能が有効なことを確認します。

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**	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)# **vpc domain***domain-id*	スイッチ上にある既存の vPC ドメインを選択するか、または新規の vPC ドメインを作成して、

	コマンドまたはアクション	目的
		vpc-domain コンフィギュレーション モードを開始します。*domain-id* のデフォルト値はありません。指定できる値の範囲は 1 ～ 1000 です。
ステップ 3	switch(config-vpc-domain)# **role priority***priority*	vPC システム プライオリティとして使用するロール プライオリティを指定します。指定できる値の範囲は、1 ～ 65535 です。デフォルト値は 32667 です。
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 機能が有効なことを確認します。

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)# **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 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** *vlan-range* **priority** *value*	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、変更を継続的に保存します。

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 コマンドを使用して STP VLAN ベースのロード バランシング条件を満たすように代表ブリッジ ID を変更した後、ルート ブリッジ ID を最高のブリッジ プライオリティよりも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。詳細については、ご使用のデバイスのコマンド リファレンスを参照してください。

（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 機能が有効なことを確認します。

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。

	コマンドまたはアクション	目的
		（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。
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、変更を継続的に保存します。

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 を介したレイヤ 3 の設定

はじめる前に

- 両方の vPC ピアでピア ゲートウェイ機能がイネーブルになっていて、設定されていることを確認します。
- 両方のピアが vPC を介したレイヤ 3 の機能をサポートするイメージを実行していることを確認します。

手順

ステップ 1 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。
switch# **configure terminal**

ステップ 2 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。
switch(config)# **vpc domain***domain_id*

ステップ 3 両方の vPC ピアのピア ゲートウェイをイネーブルにします。
switch(config-vpc-domain)# **peer-gateway**

ステップ 4 両方の vPC ピアのレイヤ 3 ピア ルータをイネーブルにし、両方のピアとのピアリング隣接関係を形成します。
switch(config-vpc-domain)# **layer3 peer-router**

（注） ピア ゲートウェイ機能をイネーブルにせずにレイヤ 3 ピア ルータをイネーブルにすると、次の syslog メッセージが表示されます。

「Please enable peer-gateway before configuring this feature.」

ステップ 5 vpc-domain コンフィギュレーション モードを終了します。
switch(config-vpc-domain)# **end**

ステップ 6 （オプション）各 vPC ドメインに関する簡単な情報を表示して、設定を確認します。
switch# **show vpc brief**

次に、vPC を介したレイヤ 3 を設定する例を示します。

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

次に、vPC を介したレイヤ 3 が設定されているかどうかを確認する例を示します。

```
switch# show vpc brief
vPC domain id : 1
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
Configuration consistency status : success
Per-vlan consistency status : failed
Type-2 consistency status : success
```

```
vPC role : secondary
Number of vPCs configured : 2
Peer Gateway : Enabled
Peer gateway excluded VLANs : -
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Enabled (timeout = 240 seconds)
Operational Layer3 Peer : Enabled
```

vPC 複合からのスイッチの分離と復元

vPC シャットダウンの設定

vPC 複合からスイッチを分離します。スイッチをいったん分離すると、分離されていないスイッチを通過する vPC トラフィックに影響を与えることなくそのスイッチはデバッグ、再ロード、さらに物理的に切り離すことさえ可能です。

（注） vPC スイッチが分離されるとき、分離されるスイッチと分離されないスイッチの両方で設定変更は許可されません。

分離されたスイッチでは中断を伴うアップグレードのみがサポートされます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **vpc domain** *domain-id*	スイッチに対して vPC ドメインを作成し、vpc-domain コンフィギュレーション モードを開始します。domain-id のデフォルト値はありません。指定できる値の範囲は 1 ～ 1000 です。
ステップ 3	switch(config-vpc)# **shutdown**	vPC ドメインからスイッチを分離します。
ステップ 4	switch(config-vpc)# **copy running-config startup-config**	リブート後にすべての現在のコンフィギュレーションの詳細を利用できるように、スタートアップ コンフィギュレーションファイルに実行コンフィギュレーションを保存します。

次の例では、vPC ドメイン 100 のトラフィックをシャットダウンする方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 100
switch(config-vpc)# shutdown
switch(config-vpc)# copy running-config startup-config
```

vPC シャットダウン スイッチの復元

最少の中断で vPC 複合に分離スイッチバックを組み込みます。

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)# **vpc domain** *domain-id*	スイッチに対して vPC ドメインを作成し、vpc-domain コンフィギュレーション モードを開始します。domain-id のデフォルト値はありません。指定できる値の範囲は 1 ～ 1000 です。
ステップ 3	switch(config-vpc)# **no shutdown**	vPC ドメインにスイッチを復元します。
ステップ 4	switch(config-vpc)# **copy running-config startup-config**	リブート後にすべての現在のコンフィギュレーションの詳細を利用できるように、スタートアップ コンフィギュレーションファイルに実行コンフィギュレーションを保存します。

次の例では、vPC ドメイン 100 のトラフィックを復元する方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 100
switch(config-vpc)# no shutdown
switch(config-vpc)# copy running-config startup-config
```

vPC 設定の確認

vPC の設定情報を表示する場合は、次のコマンドを使用します。

コマンド	目的
switch# **show feature**	vPC がイネーブルかどうかを表示します。
switch# **show port-channel capacity**	設定されている EtherChannel の数、およびスイッチ上でまだ使用可能な EtherChannel の数を表示します。
switch# **show running-config vpc**	vPC の実行コンフィギュレーションの情報を表示します。

コマンド	目的
switch# **show vpc brief**	vPC に関する簡単な情報を表示します。
switch# **show vpc consistency-parameters**	すべての vPC インターフェイス全体で一貫している必要があるパラメータのステータスを表示します。
switch# **show vpc peer-keepalive**	ピアキープアライブ メッセージの情報を表示します。
switch# **show vpc role**	ピア ステータス、ローカルスイッチのロール、vPC システムの MAC アドレスとシステム プライオリティ、およびローカル vPC スイッチの MAC アドレスとプライオリティを表示します。
switch# **show vpc statistics**	vPC に関する統計情報を表示します。 （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 スイッチのコマンド 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 検査ステータスの表示

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

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

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

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

グローバル タイプ 1 不整合の表示

グローバル タイプ 1 不整合が発生すると、セカンダリ スイッチの vPC はダウンします。次の例は、スパニングツリー モードでの不一致に伴って生じたこのタイプの不整合を示したものです。

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

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

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

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

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

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

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

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

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

vPC status
```

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

インターフェイス別タイプ 1 不整合の表示

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

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

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

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

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 ごとの整合性ステータスの表示

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

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    Po1    up     1-4,6-10

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

次に、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    Po1    up     1-4,6-10

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

次に、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             0-4,6-4095
                                  configuration
                                  incompatible - STP is
                                  enabled or disabled on
                                   some or all vlans
STP MST Region Name         1     success                0-4095
STP MST Region Revision     1     success                0-4095
STP MST Region Instance to  1     success                0-4095
```

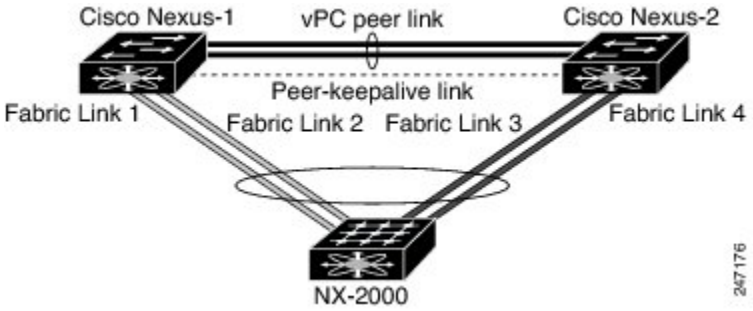
```
 VLAN Mapping
STP Loopguard               1     success                0-4095
STP Bridge Assurance        1     success                0-4095
STP Port Type, Edge         1     success                0-4095
BPDUFilter, Edge BPDUGuard
STP MST Simulate PVST       1     success                0-4095
Pass Vlans                  -                            0-4,6-4095
```

vPC の設定例

デュアル ホーム ファブリック エクステンダにおける vPC の設定例

次に、次の図に示すように、CiscoNexus-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 *23* : ***vPC*** の設定例



はじめる前に

Cisco Nexus 2000 シリーズ ファブリック エクステンダの NX-2000-100 が接続され、かつオンラインになってい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。

```
CiscoNexus-1# configure terminal
CiscoNexus-1(config)# feature lacp
CiscoNexus-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。

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

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

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

ステップ 4 ファブリック エクステンダの識別子（100 など）を作成します。

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

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

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

ステップ 6 両方の Cisco Nexus デバイス上のファブリック 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。

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

ステップ 7 設定を保存します。

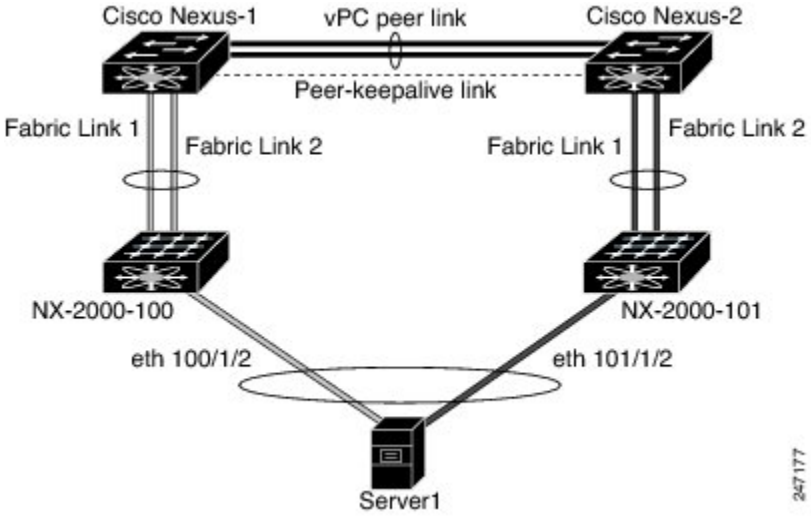
```
CiscoNexus-1(config)# copy running-config startup-config
```

CiscoNexus-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 ファブリック エクステンダにおける vPC の設定例

次に、次の図に示すように、スイッチCiscoNexus-1のピア キープアライブ 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 *24*：*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 CiscoNexus-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（CiscoNexus-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 の NX-2000-100 と 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。

```
CiscoNexus-1# configure terminal
CiscoNexus-1(config)# feature lacp
CiscoNexus-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 リンクで使用する VLAN および SVI を作成します。

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

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

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

（注） VLAN 900 は、vPC ピアキープアライブ メッセージが伝送されるため、vPC ピアリンク上をトランク**されない**ようにする必要があります。vPC ピアキープアライブ メッセージの CiscoNexus-1 と CiscoNexus-2 のスイッチ間に代替パスが必要です。

ステップ 4 vPC ピア リンクを 2 ポートの EtherChannel として設定します。

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

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

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

ステップ 6 ファブリック エクステンダの NX-2000-100 に対して、ファブリック EtherChannel リンクを設定します。

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

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

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

ステップ 8 設定を保存します。

```
CiscoNexus-1(config)# copy running-config startup-config
```

vPC のデフォルト設定

次の表は、vPC パラメータのデフォルト設定をまとめたものです。

表 *9*：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

B

BFD 68, 70, 71, 72, 73, 74, 76, 78, 80, 81, 83, 84, 86, 87, 90, 92, 93, 95, 96, 97
- BGP での設定 83
- BGP 上での設定 83
- EIGRP 上での設定 84
- HSRP 上での設定 87
- OSPF 上での設定 86
- PIM 上での設定 92
- security 70
- イネーブル化 73
- インターフェイスにおけるディセーブル化 93
- インターフェイスの設定 76
- エコー機能の設定 80
- グローバル パラメータの設定 74
- サブインターフェイスの最適化 81
- スタティック ルートでの設定 90
- デフォルト設定 72
- ポート チャネルの設定 78
- モニタリング 95
- ライセンス要件 70
- ルーティング プロトコルのサポート 83
- 仮想化サポート 70
- 関連の標準 97
- 障害検出 68
- 設定の確認 95
- 設定階層 73
- 設定例 96
- 前提条件 70
- 注意事項と制約事項 71
- 非同期モード 68

E

EtherChannel ホスト インターフェイス 168
- 作成 168

F

FEX 132
- 用語 132

L

LACP 100, 106, 109, 115, 122, 123
- グレースフル コンバージェンス 122, 123
  - ディセーブル化 122
  - 再イネーブル化 123
- システム ID 106
- ポート チャネル 106
- マーカー レスポンダ 109
- 設定 115

LACP がイネーブルとスタティック 109
- ポート チャネル 109

LACP ショート タイムアウト 120
- 設定 120

LACP の設定 115

LACP ポート プライオリティ 121
- 設定 121

LACP 高速タイマー レート 119
- 設定 119

Link Aggregation Control Protocol 100

M

MIB 66
- レイヤ 3 インターフェイス 66

S

SFP+ トランシーバ 6

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

STP 99
ポート チャネル 99

U

UDLD 4, 5
アグレッシブ モード 5
定義 4
非アグレッシブ モード 5
UDLD モード A 13
設定 13

V

VLAN 49
インターフェイス 49
VLAN インターフェイス 55
設定 55
vPC 152, 154, 169
ARP または ND を使用 152
ポート チャネルの移行 169
注意事項と制約事項 154
vPC トポロジ 166
孤立ポートの一時停止、セカンダリ スイッチ 166
vPC の用語 131
vPC ピア スイッチ 153
vPC ピア スイッチ トポロジ 173, 175
hybrid 175
設定 175
純粋な 173
設定 173
vPC ピア リンク 149
インターフェイス 149
vpc を介した L3 177
インターフェイス 177
vPC を介したレイヤ 3 141, 142, 144
VRF 60
インターフェイスの割り当て 60

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
イネーブル化 19, 20, 73
BFD 73
CDP 19
イネーブル化 *(続き)*
error-disabled の検出 19
error-disabled リカバリ 20
インターフェイス 1, 4, 47, 49, 50, 54, 55, 59, 60, 63, 65
loopback 50, 59
UDLD 4
VLAN 49, 55
設定 55
VRF への割り当て 60
オプション 1
シャーシ ID 1
ルーテッド 47
レイヤ 3 47, 63, 65
モニタリング 63
設定例 65
帯域幅の設定 54
インターフェイスの速度 6, 15
設定 15
インターフェイス情報、表示 44
レイヤ 2 44

く

グレースフル コンバージェンス 122, 123
LACP 122, 123
ポート チャネル 122, 123
LACP 122, 123
グレースフル コンバージェンス 122, 123

さ

サブインターフェイス 48, 53, 54
設定 53
帯域幅の設定 54

ち

チャネル モード 107, 115
ポート チャネル 107, 115

て

ディセーブル化 16, 19, 33, 93, 155
CDP 19
vPC 155

ディセーブル化 *(続き)*
イーサネット インターフェイス 33
インターフェイスにおける BFD 93
リンク ネゴシエーション 16
デバウンス タイマー 9
パラメータ 9
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 52
レイヤ 3 インターフェイス 52

と

トポロジ 132, 133
シングル ホーム接続ファブリック エクステンダ vPC 132
デュアル ホーム接続ファブリック エクステンダ vPC 133

は

ハードウェア ハッシュ 114
マルチキャスト トラフィック 114
ハイレベル設定タスク フロー 73
パラメータ、概要 9
デバウンス タイマー 9

ふ

ファブリック エクステンダ 132
用語 132
プライベート VLAN での IP アドレッシング方式 50

ほ

ポート チャネリング 100
ポート チャネル 54, 99, 101, 103, 106, 109, 111, 112, 113, 114, 115, 125, 169
LACP 106
LACP がイネーブルとスタティック 109
STP 99
vPC への移行 169
チャネル モード 115
ハードウェア ハッシュ 114
ポート チャネル *(続き)*
ポートの追加 112
ロード バランシング 103, 113
ポート チャネル 103
互換性要件 101
作成 111
設定の確認 125
帯域幅の設定 54
ポート チャネルの設定 101
注意事項と制約事項 101
ポート プロファイル 7, 9
概要 7
注意事項と制約事項 9
ポート プロファイル 9
ポートの追加 112
ポート チャネル 112

ま

マルチキャスト トラフィック 114
ハードウェア ハッシュ 114
ポート チャネル 114

も

モニタリング 63
レイヤ 3 インターフェイス 63

ゆ

ユニファイド ポート 3, 12
設定 12

る

ルーテッド インターフェイス 47, 52, 54
設定 52
帯域幅の設定 54
ループバック インターフェイス 50, 59
設定 59

れ

レイヤ 2 **44**
　インターフェイス情報、表示 **44**
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 **47, 51, 52, 61, 63, 65, 66**
　MIB **66**
　インターフェイス **65, 66**
　　レイヤ 3 **65, 66**
　　MIB **66**
　　関連資料 **65**
　　規格 **66**
　デフォルト設定 **52**
　モニタリング **63**
レイヤ 3 インターフェイス *(続き)*
　ルーテッド インターフェイスの設定 **52**
　確認 **61**
　関連資料 **65**
　規格 **66**
　設定例 **65**
　注意事項と制約事項 **51**

ろ

ロード バランシング **113**
　ポート チャネル **113**
　　設定 **113**