Cisco Nexus 3600 NX-OS インターフェイス設定ガイド、リリース 9.3(x)

初版：2019 年 7 月 20 日

最終更新：2019 年 12 月 23 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

© 2019 Cisco Systems, Inc. All rights reserved.

目 次

はじめに

この前書きは、次の項で構成されています。

対象読者

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

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
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、角かっこで囲んで示しています。
[x | y]	いずれか1つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。

表記法	説明
[x {y | z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

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

Cisco Nexus 3600 プラットフォーム スイッチの関連資料

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

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

マニュアルに関するフィードバック

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

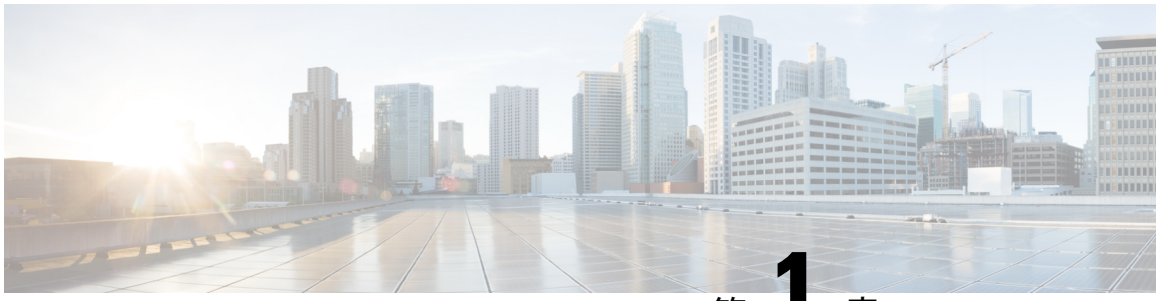
通信、サービス、およびその他の情報

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

Cisco バグ検索ツール

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

通信、サービス、およびその他の情報



第 1 章

新機能および変更された機能に関する情報

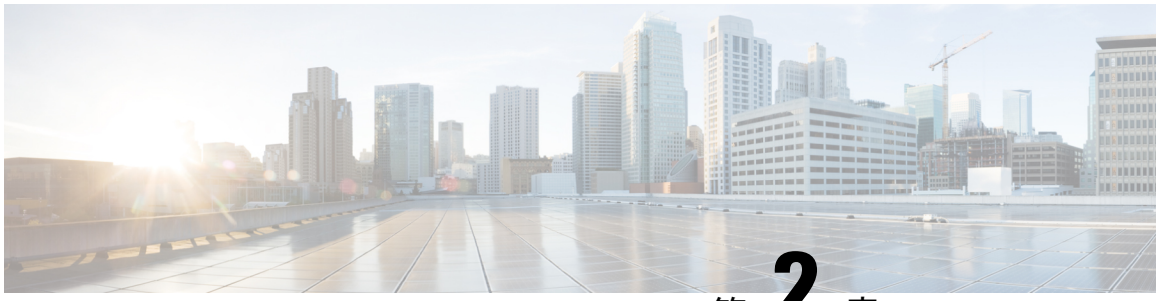
次の表では、このコンフィギュレーションガイドでの重要な変更点の概要を示します。この表は、このマニュアルのすべての変更点、または特定のリリースのすべての新機能をまとめたリストではありません。

新機能および変更された機能に関する情報

表 *1 : NX-OS* リリース *9.3(x)* の新機能および変更された機能

機能	説明	変更が行われたリリース	参照先
MTU	管理インターフェイスで、最大 9216 バイトの MTU サイズを設定することができるようになりました。	9.3(1)	MTU 設定 （10 ページ）

新機能および変更された機能に関する情報



第 2 章

レイヤ 2 インターフェイスの設定

ライセンス要件

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

イーサネット インターフェイスの概要

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

イーサネット インターフェイスはデフォルトでイネーブルです。

インターフェイス コマンド

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

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

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

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

UDLD パラメータ

シスコ独自の単一方向リンク検出（UDLD）プロトコルでは、光ファイバまたは銅線（たとえば、カテゴリ 5 のケーブル）のイーサネット ケーブルで接続されているポートでケーブルの物理的な構成をモニタリングし、単一方向リンクの存在を検出できます。スイッチが単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。

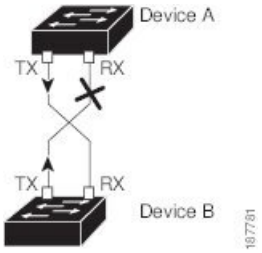
リンク上でローカルデバイスから送信されたトラフィックはネイバーで受信されるのに対し、ネイバーから送信されたトラフィックはローカルデバイスで受信されない場合には常に、単方向リンクが発生します。対になっているファイバ ケーブルのいずれかの接続が切断された場合、自動ネゴシエーションがアクティブであれば、そのリンクは存続できません。この場合、論理リンクは不定であり、UDLD は何の処理も行いません。レイヤ 1 で両方の光ファイバが正常に動作している場合は、レイヤ 2 で UDLD が、これらの光ファイルが正しく接続されているかどうか、および正しいネイバー間でトラフィックが双方向に流れているかを調べます。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。プロトコルが単一方向リンクを正しく識別

してディセーブルにするには、リンクの両端のデバイスで UDLD をサポートする必要があります。

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

Figure 1: 単方向リンク



UDLD のデフォルト設定

次の表は、UDLD のデフォルト設定を示したものです。

Table 2: UDLD のデフォルト設定

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

UDLD アグレッシブ モードと非アグレッシブ モード

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

スパニング ツリー ループを防止するため、間隔がデフォルトの 15 秒である非アグレッシブな UDLD でも、（デフォルトのスパニング ツリー パラメータを使用して）ブロッキング ポートがフォワーディング ステートに移行する前に、単方向リンクをシャットダウンすることができます。

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

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

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

レイヤ 2 インターフェイスの注意事項および制約事項

レイヤ 2 インターフェイスの設定には次の注意事項と制約事項があります。

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

インターフェイスの速度

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

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

表 *3:* ブレークアウト モードのサポート マトリックス

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

40 ギガビット イーサネット インターフェイスの速度

Cisco Nexus 3600 プラットフォーム ポートでは、QSFP ポートを 40 ギガビット イーサネット モードまたは 4x10 ギガビット イーサネット モードで動作させることができます。デフォルトでは、49 ー 54 の番号が付けられた 6 つの QSFP インターフェイスポートがあり、40 ギガビット イーサネット モードで動作できます。これらの 40 ギガビット イーサネット ポートには、2 タプルの命名規則で番号が割り当てられます。たとえば、2 番目の 40 ギガビット イーサネット ポートには 1/50 という番号が割り当てられます。40 ギガビット イーサネットから 10 ギガビット イーサネットに設定を変更するプロセスは「ブレイクアウト」と呼ばれ、10 ギガビット イーサネットからギガビット イーサネットに設定を変更するプロセスは「ブレイクイン」と呼ばれます。40 ギガビット イーサネット ポートを 10 ギガビット イーサネット ポートにブレイクアウトする場合、得られたポートには 3 タプルの命名規則を使用して番号が割り当てられます。たとえば、2 番目の 40 ギガビット イーサネット ポートのブレイクアウト ポートには 1/49/1、1/49/2、1/49/3、1/49/4 という番号が割り当てられます。

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

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

（注） 新しい QSFP + 40 Gb トランシーバは、Cisco Nexus 3600 プラットフォーム スイッチでサポートされています。新しい QSFP+（40-Gb）トランシーバは、4 個の 10Gb SFP-10G-LR トランシーバに分岐するケーブルを備えています。これを使用するには、ポートが 4x10G モードである必要があります。ブレークアウト ケーブルを使用する場合は、40G ポートを 4x10G モードで動作させる必要があります。

40 ギガビット イーサネット ポートを 4 個の 10 ギガビット イーサネット ポートに動的にブレイクアウトする機能および 4 個の 10 ギガビット イーサネット ポートを 40 ギガビット イーサネット ポートに動的にブレイクインする機能により、任意のブレイクアウト対応ポートを使用して、それらを永続的に定義することなく、40 ギガビット イーサネット モードまたは 10 ギガビット イーサネット モードを利用できます。

SVI 自動ステート

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

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

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

Cisco Discovery Protocol

Cisco Discovery Protocol（CDP）は、すべてのシスコ デバイス（ルータ、ブリッジ、アクセス サーバ、およびスイッチ）のレイヤ 2（データリンク層）で動作するデバイス検出プロトコルです。ネットワーク管理アプリケーションは CDP を使用することにより、既知のデバイスのネイバーであるシスコデバイスを検出することができます。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。

Table 4: CDP のデフォルト設定

機能	デフォルト設定
CDP インターフェイス ステート	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 err-disable 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。

タイム可変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。

errdisabled ステートからインターフェイスのリカバリをディセーブルにするには、**no errdisable recovery cause** コマンドを使用します。

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

- all：すべての原因からタイマーが回復できるようにします。
- bpduguard：ブリッジ プロトコル データ ユニット（BPDU）ガードの error-disabled ステートからタイマーが回復できるようにします。
- failed-port-state：スパニングツリープロトコル（STP）のポート状態設定障害からタイマーが回復できるようにします。
- link-flap：リンクステート フラッピングからタイマーが回復できるようにします。

- pause-rate-limit：ポーズ レート リミットの error-disabled ステートからタイマーが回復できるようにします。
- udld：単方向リンク検出（UDLD）の error-disabled ステートからタイマーが回復できるようにします。
- loopback：ループバックの error-disabled ステートからタイマーが回復できるようにします。

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 err-disable ステートは解消され、すべての原因がタイムアウトになった段階で動作を再試行できるようになります。エラーの原因を表示する場合は、**show interface status err-disabled** コマンドを使用します。

デフォルト インターフェイス

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

デバウンス タイマー パラメータ

デバウンスタイマーを設定するとリンク変更の通知が遅くなり、ネットワークの再設定によるトラフィック損失が減少します。デバウンス タイマーはイーサネット ポートごとに個別に設定します。遅延時間はミリ秒単位で指定できます。遅延時間の範囲は0～5000 ミリ秒です。デフォルトでは、このパラメータはデバウンスタイマーが作動しない100 ミリ秒に設定されています。このパラメータが0 ミリ秒に設定されると、デバウンスタイマーがディセーブルになります。

⚠

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

MTU 設定

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

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

管理インターフェイスでは、最大9216バイトのMTUサイズを設定することができます。設定の変更により、エンドデバイスで一時的なリンク フラップがトリガーされることがあります。

カウンタの値

設定、パケットサイズ、増加するカウンタの値、およびトラフィックに関する次の情報を参照してください。

設定	パケット サイズ	増加するカウンタ	Traffic
L2 ポート：MTU 設定なし	6400 および 10000	Jumbo、Giant、および Input error	Dropped
L2 ポート：ネットワーク QoS 設定にジャンボ MTU 9216 あり	6400	Jumbo	Forwarded
L2 ポート：ネットワーク QoS 設定にジャンボ MTU 9216 あり	10000	Jumbo、Giant、および Input error	Dropped
レイヤ 3 ポート：ネットワーク QoS 設定にデフォルト レイヤ 3 MTU およびジャンボ MTU 9216 あり	6400	Jumbo	パケットは、CPU にパントされ（CoPP 設定の対象）、断片化された後に、ソフトウェアによって転送される。
レイヤ 3 ポート：ネットワーク QoS 設定にデフォルト レイヤ 3 MTU およびジャンボ MTU 9216 あり	6400	Jumbo	パケットは、CPU にパントされ（CoPP 設定の対象）、断片化された後に、ソフトウェアによって転送される。
レイヤ 3 ポート：ネットワーク QoS 設定にデフォルト レイヤ 3 MTU およびジャンボ MTU 9216 あり	10000	Jumbo、Giant、および Input error	Dropped

設定	パケット サイズ	増加するカウンタ	Traffic
レイヤ 3 ポート：ネットワーク QoS 設定にジャンボ レイヤ 3 MTU およびジャンボ MTU 9216 あり	6400	Jumbo	断片化なしで転送される。
レイヤ 3 ポート：ネットワーク QoS 設定にジャンボ レイヤ 3 MTU およびジャンボ MTU 9216 あり	10000	Jumbo、Giant、および Input error	Dropped
レイヤ 3 ポート：ジャンボ レイヤ 3 MTU およびデフォルト L2 MTU 設定あり	6400 および 10000	Jumbo、Giant、および Input error	Dropped

（注）
- 適切な CRC を持つ 64 バイト未満のパケット：ショート フレーム カウンタが増加します。
- 不適切な CRC を持つ 64 バイト未満のパケット：ラント カウンタが増加します。
- 不適切な CRC を持ち 64 バイトを超えるパケット：CRC カウンタが増加します。

ダウンリンク遅延

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

リロード時に、指定されたタイムアウト時間が経過した後にのみハードウェアのダウンリンク RJ-45 ポートを有効にするタイマーを設定できます。このプロセスにより、アップリンク SFP+ ポートを最初に使用可能にすることができます。このタイマーは、管理上有効なポートについてのみ、ハードウェアで有効になります。

ダウンリンク遅延はデフォルトでは無効になっており、明示的に有効にする必要があります。有効になっている場合、遅延タイマーが指定されないと、デフォルトの 20 秒の遅延に設定されます。

物理イーサネットのデフォルト設定

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

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

イーサネット インターフェイスの設定に関するガイドライン

Cisco Nexus 3000 シリーズ スイッチでのインターフェイス イーサネット コマンドの設定における動作の変更があります。たとえば、**sh int ethernet Eth1/1 transceiver** コマンドは機能しなくなりました。コマンドを **sh int ethernet 1/1 transceiver** のように設定する必要があります。

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。

Note 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。

SUMMARY STEPS

1. switch# **configure terminal**

2. switch(config)# **feature udld**
3. switch(config)# **no feature udld**
4. switch(config)# **show udld global**
5. switch(config)# **interface** *type slot*/*port*
6. switch(config-if)# **udld** {**enable** | **disable** | **aggressive**}
7. switch(config-if)# **show udld** *interface*

DETAILED STEPS

	Command or Action	Purpose
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** *type slot*/*port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	switch(config-if)# **udld** {**enable** | **disable** | **aggressive**}	ノーマル UDLD モードをイネーブルにするか、UDLD をディセーブルにするか、またはアグレッシブ UDLD モードをイネーブルにします。
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。

Example

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
```

リンク ステート整合性チェッカのトリガー

リンク ステート整合性チェッカを手動でトリガーして、インターフェイスのハードウェアおよびソフトウェア リンク ステータスを比較し、その結果を表示することができます。リンク ステート整合性チェッカを手動でトリガーして結果を表示するには、次のコマンドを特定のモードで使用します。

手順の概要

1. switch# **show consistency-checker link-state module** *slot*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **show consistency-checker link-state module** *slot*	指定されたモジュールのリンク ステート整合性検査を開始し、その結果を表示します。

例

次に、リンク ステート整合性検査をトリガーして結果を表示する例を示します。

```
switch# show consistency-checker link-state module 1
Link State Checks: Link state only
Consistency Check: FAILED
No inconsistencies found for:
   Ethernet1/1
   Ethernet1/2
   Ethernet1/3
   Ethernet1/4
   Ethernet1/5
   Ethernet1/6
   Ethernet1/7
   Ethernet1/8
   Ethernet1/9
   Ethernet1/10
   Ethernet1/12
```

```
   Ethernet1/13
   Ethernet1/14
   Ethernet1/15
Inconsistencies found for following interfaces:
   Ethernet1/11
```

インターフェイス速度の設定

最初の 48 ポートは 1 G/10 G/25 G をサポートし、残りの 6 ポートは40 G/100 G をサポートします。

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

表 *5:*

ポート グループ	**Ports**
Port-Group 1	ポート 1 ～ 4
Port-Group 2	ポート 5 ー 8
Port-Group 3	ポート 9 ー 12
Port-Group 4	ポート 13 ー 16
Port-Group 5	* ポート 17 ～ 20
Port-Group 6	ポート 21 ー 24
Port-Group 7	ポート 25 ー 28
Port-Group 8	ポート 29 ー 32
Port-Group 9	ポート 33 ー 36
Port-Group 10	ポート 37 ー 40
Port-Group 11	ポート 41 ー 44
Port-Group 12	ポート 45 ～ 48

（注） インターフェイスとトランシーバの速度が一致しない場合、 **show interface ethernet** *slot*/*port* コマンドを入力すると、SFP 検証失敗メッセージが表示されます。たとえば、**speed 1000** コマンドを設定せずに 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 Gbps です。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **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*	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。
ステップ 3	switch(config-if)# **speed** *speed*	インターフェイスの速度を設定します。 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。*speed* 引数には次のいずれかを設定できます。 • 10 Mbps • 100 Mbps • 1 Gbps • 10 Gbps • automatic

例

次に、1 ギガビット イーサネット ポートの速度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
```

QSFP 40 ギガビット イーサネット インターフェイスのブレイクアウトの設定

ポートを 10-GbE モードにブレイクアウトする場合、最初の QSFP ポートと SFP+ ポート 1 ～ 4 を切り替えることができます。最初の QSFP ポートまたは 4 個の SFP+ ポートのいずれかを、

いつでもアクティブにできます。QSFPは、インターフェイス速度が40 Gbpsのデフォルト ポートです。

最初の QSFP ポートが 40-GbE モードの場合、ポートを 4 個の SFP+ ポートに切り替えることはできず、ポートを 10-GbE モードにブレイクアウトするまで最初の QSFP ポートはアクティブです。これは、SFP+ ポートが 40-GbE モードをサポートしないためです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface breakout module** *module number* **port** *port range***map 10g-4x**
3. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **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 breakout module** *module number* **port** *port range***map 10g-4x**	モジュールを 10g モードで設定できるようにします。ポート モードを QSFP から SFP+ に変更する場合、**hardware profile front portmode** コマンドは、このコマンドに表示されている 最初の QSFP ポートがブレイクアウトされた後にのみ有効になります。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

40 ギガビット イーサネット インターフェイスのブレークアウトを設定する例を示します。

```
switch# show int e1/49 tranceiver
Ethernet1/49transceiver is present
type is QSFP-4X10G-AOC1M
name is CISCO-AVAGO
part number is AFBR-7IER01Z-CS2
revision is 01
serial number is AVE20421070
nominal bitrate is 10300 MBit/sec per channel
Link length supported for copper is 1 m
cisco id is 13
cisco extended id number is 16
cisco part number is 10-2932-02
cisco product id is QSFP-4X10G-AOC1M
cisco vendor id is V02

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

```
switch(config)# interface breakout module 1 port 49 map 10g-4x
switch(config)# exit


switch# show interface ethernet 1/49/1-4 br

--------------------------------------------------------------------------------
Ethernet VLAN Type Mode Status Reason Speed Port
Interface Ch #
--------------------------------------------------------------------------------
Eth1/49/1 1 eth access up none 10G(D) --
Eth1/49/2 1 eth access up none 10G(D) --
Eth1/49/3 1 eth access up none 10G(D) --
Eth1/49/4 1 eth access up none 10G(D) --
```

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。デフォルトの場合、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。デフォルトの場合、自動ネゴシエーションは Cisco Nexus 3064 スイッチおよび Cisco Nexus 3064-X スイッチではイネーブル、Cisco Nexus 3048 スイッチではディセーブルです。1 ギガビット ポートでは自動ネゴシエーションをディセーブルにできません。

デフォルトでは、自動ネゴシエーションはすべての 1G SFP+ および 40G QSFP ポートではイネーブル、10G SFP+ ポートではディセーブルです。自動ネゴシエーションは、デフォルトで、すべての 1G および 10G Base-T ポートでイネーブルです。1G および 10G Base-T ポートではディセーブルにできません。

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

Release 6.0(2)U5(1) 以降では、すべての 40G インターフェイスで自動ネゴシエーションをディセーブルにできます。すべての 40G インターフェイスで自動ネゴシエーションをディセーブルにするために、新しい CLI コマンドの **no system default interface 40g auto-negotation** が導入されました。この新しい CLI コマンドは 40G インターフェイスについてのみ有効で、1G また 10G インターフェイスには影響を与えません。CR4 ケーブルの場合は、起動するリンクの両方のエンド デバイスで自動ネゴシエーション設定が同じである必要があります。

（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
```

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet** *slot*/*port*
3. switch(config-if)# **no negotiate auto**

4. （任意） switch(config-if)# **negotiate auto**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **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。
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	（任意） switch(config-if)# **negotiate auto**	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。

例

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)#
```

SVI 自動ステートのディセーブル化

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

自動ステートの動作を有効または無効にすると、SVI ごとに自動ステートを設定しない限り、スイッチのすべての SVI に適用されます。

（注） 自動ステートの動作はデフォルトでイネーブルです。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **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**	インターフェイス VLAN 機能をイネーブルにします。
ステップ 3	必須: switch(config)# **[no]system default interface-vlan autostate**	自動ステートのデフォルト動作をイネーブルまたはディセーブルにするようにシステムを設定します。
ステップ 4	（任意） switch(config)# **interface vlan** *interface-vlan-number*	VLAN インターフェイスを作成します。number の範囲は 1 ～ 4094 です。
ステップ 5	（任意） switch(config-if)# [**no**] **autostate**	SVI ごとに自動ステートの動作をイネーブルまたはディセーブルにします。
ステップ 6	（任意） switch(config)# **show interface-vlan** *interface-vlan*	SVI のイネーブルまたはディセーブルになっている自動ステートの動作を表示します。
ステップ 7	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、スイッチのすべての SVI に対してシステムの自動ステートのデフォルトをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature interface-vlan
switch(config)# system default interface-vlan no autostate
switch(config)# interface vlan 50
switch(config-if)# no autostate
switch(config)# copy running-config startup-config
```

次に、システムの自動ステート設定を有効にする例を示します。

```
switch(config)# show interface-vlan 2
Vlan2 is down, line protocol is down, autostate enabled
Hardware is EtherSVI, address is 547f.ee40.a17c
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec
```

デフォルト インターフェイスの設定

デフォルトインターフェイス機能によって、イーサネット、ループバック、管理、VLAN、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。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **default interface** *type interface number*
3. switch(config)# **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **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** *type interface number*	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。サポートされるインターフェイスは次のとおりです。 • **ethernet** • **loopback** • **mgmt** • **port-channel** • **vlan**
ステップ 3	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了します。

例

次に、イーサネット インターフェイスの設定を削除し、デフォルト設定に戻す例を示します。

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

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 アドバタイズメントを送信するかどうかを設定することができます。

SUMMARY STEPS

1. switch# **configure terminal**
2. (Optional) switch(config)# [**no**] **cdp advertise** {**v1** | **v2** }
3. (Optional) switch(config)# [**no**] **cdp format device-id** {**mac-address** | **serial-number** | **system-name**}
4. (Optional) switch(config)# [**no**] **cdp holdtime** *seconds*
5. (Optional) switch(config)# [**no**] **cdp timer** *seconds*

DETAILED STEPS

	Command or Action	Purpose
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	(Optional) switch(config)# [**no**] **cdp advertise** {**v1**	**v2** }	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	(Optional) switch(config)# [**no**] **cdp format device-id** {**mac-address**	**serial-number**	**system-name**}	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	(Optional) switch(config)# [**no**] **cdp holdtime** *seconds*	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。

	Command or Action	Purpose
		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	(Optional) switch(config)# [**no**] **cdp timer** *seconds*	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。

Example

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。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot*/*port*
3. switch(config-if)# **cdp enable**
4. switch(config-if)# **no cdp enable**

DETAILED STEPS

	Command or Action	Purpose
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*	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。
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。

	Command or Action	Purpose
		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。

Example

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。

手順の概要

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

手順の詳細

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

例

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）。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **errdisable recovery cause** {*all* | *udld* | *bpduguard* | *link-flap* | *failed-port-state* | *pause-rate-limit* | *loopback*}
3. switch(config)# **show interface status err-disabled**
4. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

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

例

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 loopback
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。

手順の概要

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

手順の詳細

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

例

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
```

error-disabled リカバリのディセーブル化

err-disabled ステートからのインターフェイスのリカバリを無効にできます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **no errdisable recovery cause** {*all* | *udld* | *bpduguard* | *link-flap* | *failed-port-state* | *pause-rate-limit* | *loopback*}
3. （任意） switch(config)# **show interface status err-disabled**
4. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **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 errdisable recovery cause** {*all* | *udld* | *bpduguard* | *link-flap* | *failed-port-state* | *pause-rate-limit* | *loopback*}	インターフェイスがデフォルトの err-disabled ステートに戻る条件を指定します。
ステップ 3	（任意） 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。

	コマンドまたはアクション	目的
ステップ 4	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、err-disabled リカバリをディセーブルにする例を示します。

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

デバウンス タイマーの設定

イーサネット ポートのデバウンス タイマーは、デバウンス時間をミリ秒単位（ms）で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。デフォルトでは、デバウンス タイマーは、デバウンス タイマーが作動しない 100 ミリ秒に設定されています。

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。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot/port*
3. switch(config-if)# **link debounce time** *milliseconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **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*	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。
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。

例

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

```
switch# configure terminal
switch(config)# interface ethernet 3/1
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 3/1
switch(config-if)# link debounce time 0
```

説明パラメータの設定

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
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*	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。
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。

Example

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。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot/port*
3. switch(config-if)# **shutdown**
4. switch(config-if)# **no shutdown**

DETAILED STEPS

	Command or Action	Purpose
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*	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。
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。

Example

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
```

VLAN での MAC アドレス制限の設定

Cisco Nexus 3600 シリーズ スイッチでは、ライン カード拡張モジュール（LEM）の MAC アドレス テーブル内に存在できる MAC アドレスの数の上限を設定できます。制限はシステム、VLAN、ポート、トランク、およびトンネル レベルで設定できます。たとえば、指定された VLAN での制限が 2000 の MAC アドレスである場合、レイヤ 2 フォワーディング マネージャ

（L2FM）は、受信した最初の2000のMACアドレスを受け入れ、残りのMACを拒否します。VLANでMACアドレス制限を設定するには、次の手順を実行します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **mac address-table limit system** *value*
3. switch(config)# **mac address-table limit vlan** *value*
4. switch(config)# **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **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)# **mac address-table limit system** *value*	システム レベルでの MAC 学習の上限を指定します。
ステップ 3	switch(config)# **mac address-table limit vlan** *value*	VLAN レベルでの MAC 学習の上限を指定します。
ステップ 4	switch(config)# **exit**	設定モードを終了します。

例

次に、システムおよび VLAN レベルで MAC 学習の上限を設定する例を示します。

```
switch# configure terminal
switch(config)# mac address-table limit system 10000
Configuring Mac address limit will result in flushing existing Macs in the specified
VLAN/System.Proceed(yes/no)? [no] yes
switch(config)# mac address-table limit vlan 30 3000
Configuring Mac address limit will result in flushing existing Macs in the specified
VLAN/System.Proceed(yes/no)? [no] yes
switch(config)# exit
```

次に、MAC アドレスの制限を表示する例を示します。

```
switch# configure terminal
switch(config)# sh mac address-table limit

System Limit: 10000


Vlan    Learning Limit
----    ----------
1       196000
20      196000
30      3000
100     196000
switch(config)# exit
```

カスタム EtherType またはタグ プロトコル識別子（TPID）の設定

スイッチは、802.1Q および Q-in-Q カプセル化に 0x8100 のデフォルトの ethertype を使用します。スイッチポート インターフェイスで **dot1q ethertype** コマンドを有効にすることで、ポート単位で EtherType 0x9100、0x9200、および 0x88a8 を設定できます。802.1Q タグ付きまたは 802.1p タグ付きフレームの標準 0x8100 EtherType フィールド値を使用しないネットワーク デバイスをサポートするように、ポートでカスタム EtherType フィールド値を設定できます。

（注） 二重タグ フレームを伝送する出力トランク インターフェイスだけに EtherType を設定する必要があります。設定した EtherType 値は、（Q-in-Q パケットおよび 802.1Q パケットの両方で）インターフェイスから出るすべてのタグ付きパケットに影響します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet** *slot/port*
3. switch(config-if)# **switchport**
4. switch(config-if)# **switchport mode**
5. switch(config-if)# **switchport dot1q ethertype** *value*
6. （任意） switch(config-if)# **switchport access vlan** *value*
7. switch(config-if)# **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **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*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **switchport**	インターフェイスをレイヤ 2 スイッチング ポートとして設定します。
ステップ 4	switch(config-if)# **switchport mode**	インターフェイスをレイヤ 2 スイッチング ポート モードとして設定します。
ステップ 5	switch(config-if)# **switchport dot1q ethertype** *value*	ポート上の Q-in-Q トンネル用に EtherType を設定します。
ステップ 6	（任意） switch(config-if)# **switchport access vlan** *value*	インターフェイスのアクセス VLAN を設定します。
ステップ 7	switch(config-if)# **exit**	設定モードを終了します。

例

次の例では、802.1Q トンネル ポート用にカスタム ethertype を設定する方法を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# switchport
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# switchport dot1q ethertype 0x9100
switch(config-if)# switchport access vlan 30
switch(config-if)# exit
switch(config)# exit
```

ダウンリンク遅延の設定

SFP+ポートが有効になるまでハードウェアの RJ-45 ポートの有効化を遅延させることにより、Cisco Nexus 3048 スイッチのリロード後、ダウンリンク RJ-45 ポートの前にアップリンク SFP+ ポートを動作上有効にできます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **downlink delay enable** | **disable** [**timeout** *time-out*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **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)# **downlink delay enable** | **disable** [**timeout** *time-out*]	ダウンリンク遅延を有効または無効にして、タイムアウトを設定します。

例

次に、スイッチでダウンリンク遅延を有効にして遅延タイムアウトを設定する例を示します。

```
switch# configure terminal
switch(config)# downlink delay enable timeout 45
```

インターフェイス情報の表示

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

コマンド	目的
switch# **show interface** *type slot*/*port*	指定したインターフェイスの詳細設定が表示されます。
switch# **show interface** *type slot*/*port* **capabilities**	指定したインターフェイスの機能に関する詳細情報が表示されます。このオプションは、物理インターフェイスに関してのみ使用可能です。
switch# **show interface** *type slot*/*port* **transceiver**	指定したインターフェイスに接続されているトランシーバに関する詳細情報が表示されます。このオプションは、物理インターフェイスに関してのみ使用可能です。
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。

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

次に、物理イーサネット インターフェイスを表示する例を示します。

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

```
    0 output CRC 0 ecc
    0 underrun 0 if down drop     0 output error 0 collision 0 deferred
    0 late collision 0 lost carrier 0 no carrier
    0 babble
    0 Rx pause 8031547972 Tx pause 0 reset
```

次に、物理イーサネットの機能を表示する例を示します。

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

次に、物理イーサネット トランシーバを表示する例を示します。

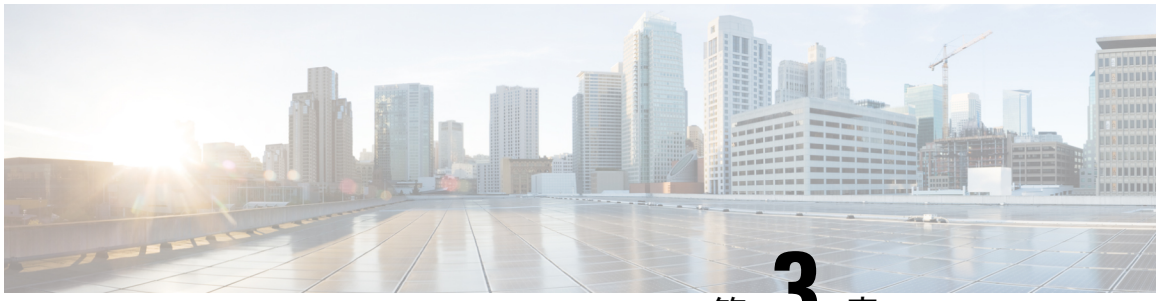
```
switch# show interface ethernet 1/1 transceiver
Ethernet1/1
    sfp is present
    name is CISCO-EXCELIGHT
    part number is SPP5101SR-C1
    revision is A
    serial number is ECL120901AV
    nominal bitrate is 10300 MBits/sec
    Link length supported for 50/125mm fiber is 82 m(s)
    Link length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

次に、インターフェイス ステータスの要約を表示する例を示します（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、CDP ネイバーを表示する例を示します。

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



第 3 章

レイヤ 3 インターフェイスの設定

レイヤ 3 インターフェイスについて

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

ポートに IP アドレスを割り当て、ルーティングをイネーブルにし、このルーテッド インターフェイスにルーティング プロトコル特性を割り当てることができます。

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

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

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

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

サブインターフェイス

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

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

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

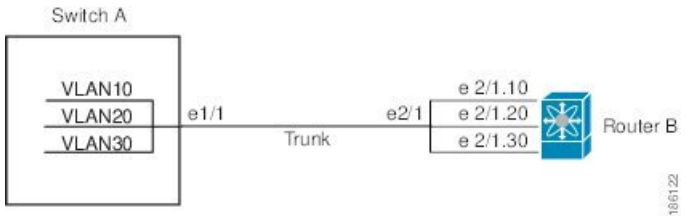
2/1 に Ethernet 2/1.1 というサブインターフェイスを作成できます。この場合、.1 はそのサブインターフェイスを表します。

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

サブインターフェイスを使用すると、親インターフェイスがサポートする各 VLAN に独自のレイヤ 3 インターフェイスを実現できます。この場合、親インターフェイスは別のデバイスのレイヤ 2 トランキング 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有効にすると、Cisco NX-OS によってデフォルト VLAN（VLAN 1）に VLAN インターフェイスが作成され、リモート スイッチ管理が許可されます。

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。

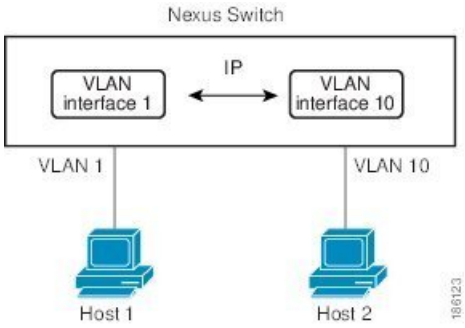
（注） VLAN 1 の VLAN インターフェイスは削除できません。

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



インターフェイスの VRF メンバーシップの変更

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

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

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

レイヤ 3 設定の保持を無効にするには、**no system vrf-member-change retain-l3-config** コマンドを使用します。このモードでは、VRF メンバーの変更時にレイヤ 3 設定が保持されません。

インターフェイスの VRF メンバーシップの変更に関する注意事項

- VRF 名の変更時に瞬間的なトラフィック損失が発生する可能性があります。

- **system vrf-member-change retain-l3-config** コマンドを有効にすると、インターフェイス レベルでの設定だけが処理されます。VRF 変更後にルーティング プロトコルに対応するための設定があれば、ルータ レベルで手動により処理する必要があります。
- **system vrf-member-change retain-l3-config** コマンドは、次によるインターフェイス レベルの設定をサポートしています。
  - CLI サーバによって保持されるレイヤ 3 設定（**ip address** および **ipv6 address**（セカンダリ）やインターフェイス設定で使用可能なすべての OSPF/ISIS/EIGRP CLI など）
  - HSRP
  - DHCP リレー エージェント CLI（ **ip dhcp relay address** [**use-vrf**] や **ipv6 dhcp relay address** [**use-vrf**] など）。
- DHCP の場合
  - ベスト プラクティスとして、クライアントおよびサーバ VRF インターフェイスを一度に 1 つずつ変更する必要があります。そのようにしないと、DHCP パケットをリレー エージェントで交換できません。
  - クライアントとサーバが異なる VRF にある場合は、 **ip dhcp relay address** [**use-vrf**] コマンドを使用して、異なる VRF 経由でリレー エージェントの DHCP パケットを交換します。

ループバック インターフェイス

ループバック インターフェイスは、常にアップ状態にある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。

IP アンナンバード

IP アンナンバード機能により、ポイントツーポイント（p2p）インターフェイスで一意の IP アドレスを明示的に設定しなくても、そのインターフェイスで IP パケットを処理することが可能になります。このアプローチでは、別のインターフェイスから IP アドレスを借りて、ポイントツーポイント リンクのアドレス空間を節約します。

ポイントツーポイント モードに準拠する任意のインターフェイスを、IP アンナンバード インターフェイスとして使用できます。IP アンナンバード機能はイーサネット インターフェイスとサブインターフェイスでのみサポートされています。借りられたインターフェイスはループバック インターフェイスとしてのみ使用され、ナンバード インターフェイスと呼ばれます。

ループバック インターフェイスは、常に機能的にアップ状態であるため、ナンバードインターフェイスとして最適です。ただし、ループバック インターフェイスはスイッチ/ルータに対してローカルであるため、最初にアンナンバードインターフェイスの到達可能性が、スタティック ルートを通じて、または内部ゲートウェイ プロトコル（OSPF、ISIS など）を使用することにより、確立される必要があります。

IP アンナンバード機能はポート チャネル インターフェイスおよびサブインターフェイスでサポートされます。借りられたインターフェイスはループバック インターフェイスとしてのみ使用され、ナンバード インターフェイスと呼ばれます。

トンネル インターフェイス

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

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

レイヤ 3 インターフェイスの注意事項および制約事項

レイヤ 3 インターフェイスの設定には次の注意事項と制約事項があります。

- 設定を削除しても、VLAN/SVI はレイヤ 3 インターフェイス テーブルから削除されません。VLAN 自体をレイヤ 3 インターフェイス テーブルから削除する必要があります。
- レイヤ 3 インターフェイスをレイヤ 2 インターフェイスに変更する場合、Cisco NX-OS はインターフェイスをシャットダウンしてインターフェイスを再度イネーブルにし、レイヤ 3 固有の設定をすべて削除します。
- レイヤ 2 インターフェイスをレイヤ 3 インターフェイスに変更する場合、Cisco NX-OS はインターフェイスをシャットダウンしてインターフェイスを再度イネーブルにし、レイヤ 2 固有の設定をすべて削除します。

レイヤ 3 インターフェイスのデフォルト設定

レイヤ 3 管理状態のデフォルト設定は Shut です。

SVI 自動ステートのディセーブル化

SVI 自動ステート ディセーブル化機能により、スイッチ仮想インターフェイス（SVI）は、対応する VLAN に「アップ」ステートのインターフェイスがない場合でも、「アップ」ステートになることができます。

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もあります。VLANのポートによって、対応するSVIの動作ステートが決定されます。VLAN の SVI インターフェイスは、対応する VLAN 内の少なくとも 1 個のポートがスパニングツリー プロトコル（STP）のフォワーディング ステートである場合に「アップ」になります。同様に、SVIインターフェイスは、最後のSTP転送ポートがダウンするか別のステートになったときに、「ダウン」になります。SVIのこの特性は、「自動ステート」と呼ばれます。

VLAN 上のレイヤ 2 またはレイヤ 3 境界を定義するためや、SVI インターフェイスを使用してデバイスを管理するために SVI を作成できます。2 番目のシナリオでは、SVI 自動ステート ディセーブル化機能により、対応する VLAN に「アップ」ステートのインターフェイスがない場合でも SVI インターフェイスが「アップ」ステートになることが保証されます。

レイヤ 3 インターフェイスの設定

ルーテッド インターフェイスの設定

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **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。

	コマンドまたはアクション	目的
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	（任意） switch(config-if)# **medium** {**broadcast** | **p2p**}	インターフェイス メディアをポイント ツー ポイントまたはブロードキャストのどちらかとして設定します。 （注） デフォルト設定は broadcast であり、この設定はどの **show** コマンドにも表示されません。ただし、**p2p** に設定を変更した場合、**show running-config** コマンドを入力すると、この設定が表示されます。
ステップ 6	（任意） switch(config-if)# **show interfaces**	レイヤ 3 インターフェイスの統計情報を表示します。
ステップ 7	（任意） switch(config-if)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、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

始める前に

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	（任意） switch(config-if)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。
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。
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	（任意） switch(config-if)# **show interfaces**	レイヤ 3 インターフェイスの統計情報を表示します。
ステップ 6	（任意） switch(config-if)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、サブインターフェイスを作成する例を示します。

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

インターフェイスでの帯域幅の設定

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

手順の概要

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

手順の詳細

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

例

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

```
switch# configure terminal
switch(config)# interface ethernet 2/1
```

```
switch(config-if)# bandwidth 80000
switch(config-if)# copy running-config startup-config
```

VLAN インターフェイスの設定

手順の概要

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

手順の詳細

	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。
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	（任意） switch(config-if)# **show interface vlan** *number*	VLAN インターフェイスの統計情報を表示します。*number* の有効範囲は 1 ～ 4094 です。
ステップ 7	（任意） switch(config-if)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、VLAN インターフェイスを作成する例を示します。

```
switch# configure terminal
switch(config)# feature interface-vlan
switch(config)# interface vlan 10
```

```
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# copy running-config startup-config
```

VRF メンバーシップ変更時のレイヤ 3 保持の有効化

次の手順により、インターフェイスでの VRF メンバーシップ変更時のレイヤ 3 設定の保持を有効にすることができます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**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	**system vrf-member-change retain-l3-config**
	例：
	`switch(config)# system vrf-member-change retain-l3-config`
	`Warning: Will retain L3 configuration when vrf member change on interface.`
		VRF メンバーシップ変更時のレイヤ 3 設定の保持を有効にします。
		（注） レイヤ 3 設定の保持を無効にするには、**no system vrf-member-change retain-l3-config** コマンドを使用します。

ループバック インターフェイスの設定

始める前に

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

手順の概要

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

手順の詳細

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

例

次に、ループバック インターフェイスを作成する例を示します。

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

イーサネット インターフェイスでの IP アンナンバードの設定

イーサネット インターフェイスで IP アンナンバード機能を設定できます。

手順の概要

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

手順の詳細

	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。

	コマンドまたはアクション	目的

ステップ 2	**interface ethernet** *slot/port* **port-channel**
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
	`switch(config)# interface port-channel 1/1`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。イーサネットおよびポートチャネルをサポート

ステップ 3	**medium p2p** 例： `switch(config-if)# medium p2p`	インターフェイス メディアをポイント ツー ポイントとして設定します。
ステップ 4	**ip unnumbered** *type number* 例： `switch(config-if)# ip unnumbered loopback 100`	明示的な IP アドレスをインターフェイスに割り当てずにインターフェイス上の IP 処理をイネーブルにします。 *type* および *number* は、IP アドレスが割り当てられているルータ上の別のインターフェイスを指定します。指定したインターフェイスを別のアンナンバードインターフェイスに設定することはできません。 （注） *type* は **loopback** に制限されます。（7.0(3)I3(1) 以降）

VRF へのインターフェイスの割り当て

始める前に

VRF 用のインターフェイスを設定した後で、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。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** *interface-typenumber*
3. switch(conifg-if)#**vrf member** *vrf-name*
4. switch(config-if)# FID cleanup[**ip** | **ipv6**]*ip-address/length*
5. （任意） switch(config-if)# **show vrf** [*vrf-name*] **interface** *interface-type number*
6. （任意） switch(config-if)# **show interfaces**
7. （任意） switch(config-if)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **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)# FID cleanup[**ip** | **ipv6**]*ip-address/length*	このインターフェイスの IP アドレスを設定します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。
ステップ 5	（任意） switch(config-if)# **show vrf** [*vrf-name*] **interface** *interface-type number*	VRF 情報を表示します。
ステップ 6	（任意） switch(config-if)# **show interfaces**	レイヤ 3 インターフェイスの統計情報を表示します。
ステップ 7	（任意） switch(config-if)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、VRF にレイヤ 3 インターフェイスを追加する例を示します。

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

インターフェイス MAC アドレスの設定

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

手順の概要

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

4. switch(config-if)# **show interface ethernet** *slot/port*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface ethernet** *slot/port*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# [**no**] **mac-address** *static router MAC address*	インターフェイス MAC アドレスを設定します。設定を削除するには、このコマンドの **no** 形式を使用します。次の 4 つのサポートされる形式のいずれでも MAC アドレスを入力できます。 • E.E.E • EE-EE-EE-EE-EE-EE • EE:EE:EE:EE:EE:EE • EEEE.EEEE.EEEE 次の無効なMACアドレスを入力しないでください。 • ヌル MAC アドレス：0000.0000.0000 • ブロードキャスト MAC アドレス：FFFF.FFFF.FFFF • マルチキャスト MAC アドレス：0100.DAAA.ADDD
ステップ 4	switch(config-if)# **show interface ethernet** *slot/port*	（任意）インターフェイスのすべての情報を表示します。

例

次に、インターフェイス MAC アドレスを設定する例を示します。

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

MAC 組み込み IPv6 アドレスの設定

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot/port*

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **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*	指定したインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **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)# **mac-address ipv6-extract**	インターフェイスで設定された IPv6 アドレスに組み込まれている MAC アドレスを取得します。 （注） MEv6 設定は、現時点では、IPv6 アドレスの EUI-64 形式でサポートされません。
ステップ 5	switch(config-if)# **ipv6 address** *ip-address/length*	このインターフェイスの IPv6 アドレスを設定します。
ステップ 6	switch(config-if)# **ipv6 nd mac-extract** [**exclude nud-phase**]	ネクストホップ IPv6 アドレスに組み込まれているネクストホップ MAC アドレスを取得します。 **exclude nud-phase** オプションにより、ND フェーズでのみパケットがブロックされます。**exclude nud-phase**（NUD）オプションが指定されていない場合は、ND フェーズと近隣到達不能検出（NUD）フェーズの両方でパケットがブロックされます。
ステップ 7	（任意） switch(config)# **show ipv6 icmp interface** *type slot/port*	IPv6 Internet Control Message Protocol バージョン 6（ICMPv6）インターフェイスの情報を表示します。

例

次に、ND MAC 取得を有効にして MAC 組み込み IPv6 アドレスを設定する例を示します。

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

次に、ND MAC 取得を有効（NUD フェーズを除く）にして MAC 組み込み IPv6 アドレスを設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# mac-address ipv6-extract
switch(config-if)# ipv6 address 2002:2::10/64
switch(config-if)# ipv6 nd mac-extract exclude nud-phase
switch(config-if)# show ipv6 icmp interface ethernet 1/5
ICMPv6 Interfaces for VRF "default"
Ethernet1/5, Interface status: protocol-up/link-up/admin-up
  IPv6 address: 2002:2::10
  IPv6 subnet:  2002:2::/64
```

```
  IPv6 interface DAD state:  VALID
  ND mac-extract : Enabled (Excluding NUD Phase)
  ICMPv6 active timers:
      Last Neighbor-Solicitation sent: 00:06:45
      Last Neighbor-Advertisement sent: 00:06:46
      Last Router-Advertisement sent: 00:02:18
      Next Router-Advertisement sent in: 00:02:24
  Router-Advertisement parameters:
      Periodic interval: 200 to 600 seconds
      Send "Managed Address Configuration" flag: false
      Send "Other Stateful Configuration" flag: false
      Send "Current Hop Limit" field: 64
      Send "MTU" option value: 1500
      Send "Router Lifetime" field: 1800 secs
      Send "Reachable Time" field: 0 ms
      Send "Retrans Timer" field: 0 ms
      Suppress RA: Disabled
      Suppress MTU in RA: Disabled
  Neighbor-Solicitation parameters:
      NS retransmit interval: 1000 ms
  ICMPv6 error message parameters:
      Send redirects: true
      Send unreachables: false
  ICMPv6-nd Statisitcs (sent/received):
      RAs: 6/0, RSs: 0/0, NAs: 2/0, NSs: 7/0, RDs: 0/0
      Interface statistics last reset: never
switch(config-if)#
```

SVI 自動ステートのディセーブル化の設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **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] system default interface-vlan autostate**	VLAN のスイッチング仮想インターフェイス（SVI）でシステムのデフォルトの自動ステート動作を再度

	コマンドまたはアクション	目的
		イネーブルにします。SVI での自動ステータス動作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 3	switch(config)# **feature interface-vlan**	VLAN インターフェイス SVI の作成をイネーブルにします。
ステップ 4	switch(config)# **interface vlan** *vlan id*	VLAN インターフェイスをディセーブルにして、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。
ステップ 5	(config-if)# [**no**] **autostate**	VLAN インターフェイスで SVI のデフォルトの自動ステート動作をディセーブルにします。
ステップ 6	(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config interface vlan** *vlan id*	（任意）特定のポートチャネルの実行コンフィギュレーションを表示します。

例

次に、SVI 自動ステートのディセーブル化機能を設定する例を示します。

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

インターフェイスでの DHCP クライアントの設定

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

手順の概要

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

手順の詳細

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

例

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

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

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

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

レイヤ 3 インターフェイス設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show interface ethernet *slot/port*	レイヤ3インターフェイスの設定情報、ステータス、カウンタ（インバウンドおよびアウトバウンドパケット レートおよびバイト レートが 5 分間に指数関数的に減少した平均値を含む）を表示します。
show interface ethernet *slot/port* **brief**	レイヤ 3 インターフェイスの動作ステータスを表示します。

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

レイヤ 3 インターフェイスのモニタリング

次のいずれかのコマンドを使用して、機能に関する統計情報を表示します。

コマンド	目的
load-interval *seconds* | **counter** {**1** | **2** | **3**} *seconds*	ビットレートとパケットレートの統計情報に対して 3 つの異なるサンプリング間隔を設定します。範囲は 5 ～ 300 秒です。
show interface ethernet *slot*/*port* **counters**	レイヤ 3 インターフェイスの統計情報を表示します（ユニキャスト、マルチキャスト、ブロードキャスト）。
show interface ethernet *slot*/*port* **counters brief** *load-interval-id*	レイヤ 3 インターフェイスの入力および出力カウンタを表示します。 load-interval-id は、入力および出力レートを表示するための単一のロードインターバル ID を指定します。 ロードインターバル ID の範囲は 1 ~ 3.です。
show interface ethernet *slot*/*port* **counters detailed** [**all**]	レイヤ 3 インターフェイスの統計情報を表示します。オプションとして、32 ビットと 64 ビットのパケットおよびバイトカウンタ（エラーを含む）をすべて含めることができます。
show interface ethernet *slot*/*port* **counters error**	レイヤ 3 インターフェイスの入力および出力エラーを表示します。
show interface ethernet *slot*/*port* **counters snmp**	SNMP MIB から報告されたレイヤ 3 インターフェイスカウンタを表示します。これらのカウンタはクリアできません。
show interface ethernet *slot*/*port*.*number* **counters**	サブインターフェイスの統計情報（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。
show interface port-channel *channel-id*.*number* **counters**	ポートチャネルサブインターフェイスの統計情報（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。

コマンド	目的
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)# copy running-config startup-config
```

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

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

次に、ループバック インターフェイスを設定する例を示します。

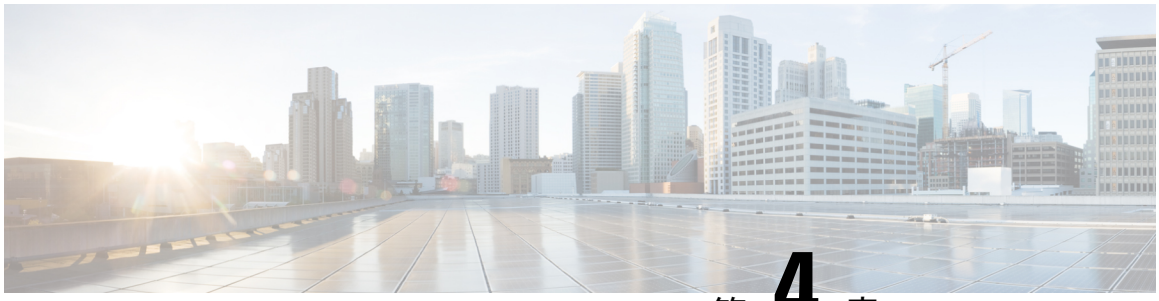
```
switch# configuration terminal
switch(config)# interface loopback 3
switch(config-if)# no switchport
switch(config-if)# ip address 192.0.2.2/32
switch(config-if)# copy running-config startup-config
```

次に、イーサネット ポートの 3 つのサンプル ロード インターバルを設定する例を示します。

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

レイヤ 3 インターフェイスの関連資料

関連項目	マニュアル タイトル
コマンド構文	『*Cisco Nexus 3600 NX-OS Command Reference*』
IP	『*Cisco Nexus 3600 NX-OS Unicast Routing Configuration Guide*』の「Configuring IP」の章
VLAN	『*Cisco Nexus 3600 NX-OS Layer 2 Switching Configuration Guide*』の「Configuring VLANs」の章



第 4 章

ポート チャネルの設定

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

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

変更した設定をポート チャネルに適用すると、そのポート チャネルのメンバー 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。For more efficient use of the port channel, you can use LACP, which is defined in IEEE 802.3ad. LACP を使用すると、リンクによってプロトコル パケットが渡されます。

Related Topics

LACP の概要 （72 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Link Aggregation Control Protocol（LACP）をイネーブルにできます。LACPによるポートチャネルを設定する手順は、スタティック ポート チャネルの場合とは若干異なります。ポート チャネル設定の制約事項については、プラットフォームの『*Verified Scalability*』マニュアルを参照してください。ロード バランシングの詳細については、ポート チャネルを使ったロード バランシング, on page 69を参照してください。

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

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

各ポートにはポート チャネルが 1 つだけあります。ポート チャネル内のすべてのポートには互換性が必要です。つまり、回線速度が同じであり、かつ全二重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。

Note チャネル モードを、ON から Active、または ON から Passive に変更することはできません。

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

Note 少なくともメンバー 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。

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
- 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
- Debounce

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

- インターフェイスがポート チャネルに参加すると、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
  - Debounce

- UDLD
- シャットダウン
- SNMP トラップ

ポート チャネルを使ったロード バランシング

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

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

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

Table 6: **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	Destination MAC	宛先 MAC、宛先 IP	宛先 MAC、宛先 IP
Source IP	Source MAC	送信元 MAC、送信元 IP	送信元 MAC、送信元 IP
送信元/宛先 IP	送信元/宛先MAC	送信元/宛先MAC、送信元/宛先 IP	送信元/宛先MAC、送信元/宛先 IP

設定	レイヤ 2 基準	レイヤ 3 基準	レイヤ 4 基準
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

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。

設定されているロードバランシング アルゴリズムにかかわらず、マルチキャスト トラフィックは次の方式を使用してポート チャネルのロード バランシングを行います。

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

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

ECMP の注意事項と制限事項

レイヤ 2/レイヤ 3 GW フローでのロードバランシングは、リロード後にスイッチが最初に起動したときに、すべてのリンク間で均等にロードバランシングされないことがあります。ハードウェアの ECMP ハッシュ設定を変更するには、2 つの CLI があります。これらのコマンドは相互に排他的です。

- MAC ベースのみのハッシュの **port-channel load-balance [src | src-dst | dst] mac** コマンドを入力します。

- IP/レイヤ4ポートに基づくハッシュの場合は、**ip load-share** または **port-channel load-balance** コマンドを入力します。
- **port-channel load-balance** コマンドは **ip load-share** コマンドを上書きできます。IP パラメータと MAC パラメータの両方を設定するのに役立つ **port-channel load-balance** コマンドを入力することをお勧めします。
- IP/レイヤ4ポートに基づいてハッシュ アルゴリズムを強制するオプションはありません。デフォルトの MAC 設定は、常にポート チャネル設定の一部としてプログラムされます。

対称ハッシュ

ポート チャネル上のトラフィックを効果的にモニタするには、ポート チャネルに接続された各インターフェイスがフォワードとリバースの両方のトラフィック フローを受信することが不可欠です。通常、フォワードとリバースのトラフィック フローが同じ物理インターフェイスを使用する保証はありません。ただし、ポートチャネルで対称ハッシュを有効にすると、双方向トラフィックが同じ物理インターフェイスを使用するように強制され、ポートチャネルの各物理インターフェイスが効果的に一連のフローにマッピングされます。

対称ハッシュが有効になっている場合、ハッシュに使用されるパラメータ（送信元と宛先の IP アドレスなど）は、ハッシュ アルゴリズムに入る前に標準化されます。このプロセスにより、パラメータがリバースされる（フォワード トラフィックの送信元がリバース トラフィックの宛先になる）場合にハッシュ出力が同じになることが保証されます。このため、同じインターフェイスが選択されます。

対称ハッシュは、Cisco Nexus 3600 シリーズ スイッチでのみサポートされます。

対称ハッシュをサポートするのは、次のロードバランシング アルゴリズムのみです。

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

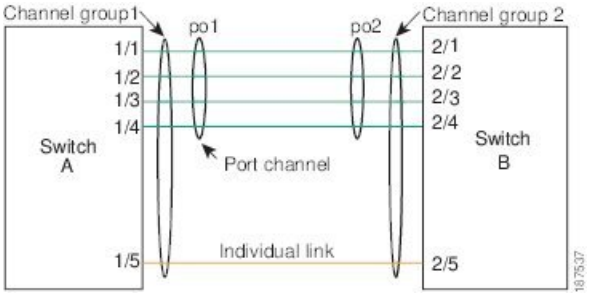
LACP の概要

LACP の概要

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

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

Figure 4: 個々のリンクをポート チャネルに組み込む



LACP を使用すると、スタティック ポート チャネルの場合と同じように、最大 32 のインターフェイスを 1 つのチャネル グループにバンドルすることができます。

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

LACP ID パラメータ

LACP では次のパラメータが使用されます。

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

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

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

チャネル モード

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

Note active または passive のチャネル モードで、個々のインターフェイスを設定するには、まず、LACP をグローバルにイネーブル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。

Table 7: 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。 デフォルトでは、LACP パケットが受信されなかった場合、LACP は中断状態になります。リンクを個別の状態にする場合は、**no lacp suspend-individual** コマンドを入力します。

passive と active のどちらのモードでも、ポート速度やトランキング 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 レスポンダをサポートしています。

LACP がイネーブルのポート チャネルとスタティック ポート チャネルの相違点

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

***Table 8: 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 チャネルにリンクし、バンドルする必要があるポート チャネル インターフェイスの最小数を設定します。
- 低帯域幅の LACP ポート チャネルがアクティブにならないようにします。
- 少数のアクティブ メンバ ポートだけが必要な最小帯域幅を提供する場合、LACP ポート チャネルが非アクティブになります。

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

- LACP ポート チャネルのバンドル ポートの上限数を定義します。

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

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

ガイドラインと制約事項

ポート チャネリング設定時の注意事項および制約事項は、次のとおりです。

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

ポート チャネルの設定

ポート チャネルの設定

ポート チャネルの作成

チャネル グループを作成する前にポート チャネルを作成します。Cisco NX-OSは自動的に、関連するチャネル グループを作成します。

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

Note チャネル メンバ ポートを発信元または宛先 SPAN ポートにできません。

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# **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。Cisco NX-OS は、チャネル グループがない場合はそれを自動的に作成します。
ステップ 3	switch(config)# **no interface port-channel** *channel-number*	ポート チャネルを削除し、関連するチャネル グループを削除します。

Example

次の例は、ポート チャネルの作成方法を示しています。

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

ポート チャネルへのポートの追加

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# **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*	チャネル グループに追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	(Optional) switch(config-if)# **switchport mode trunk**	指定したインターフェイスをトランク ポートとして設定します。
ステップ 4	(Optional) switch(config-if)# **switchport trunk** {**allowed vlan** *vlan-id* | **native vlan** *vlan-id*}	トランク ポートに必要なパラメータを設定します。
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 の範囲は 1 ～ 4096 です。ポート チャネルがない場合、Cisco NX-OS により、このチャネル グループに関連付けられたポート チャネルが作成されます。これを、暗黙的なポート チャネル作成と言います。
ステップ 6	(Optional) switch(config-if)# **no channel-group**	チャネル グループからポートを削除します。チャネル グループから削除されたポートは元の設定に戻ります。

Example

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

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

ポート チャネルを使ったロード バランシングの設定

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# **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-ip-gre**	**destination-mac**	**destination-port**	**source-dest-ip**	**source-dest-ip-gre**		デバイスのロードバランシング アルゴリズムおよびハッシュを指定します。指定可能なアルゴリズムはデバイスによって異なります。デフォルトは **source-dest-mac** です。

	Command or Action	Purpose
	source-dest-mac | **source-dest-port** | **source-ip** | **source-ip-gre** | **source-mac** | **source-port**] **symmetric** | **crc-poly**}	**Note** ハッシュ計算にNVGREキーが含まれるようにするには、オプションの **destination-ip-gre**、**source-dest-ip-gre** および **source-ip-gre** キーワードを使用します。ポート チャネルの場合、デフォルトではNVGREキーが含まれません。これらのオプションのキーワードを使用して明示的に設定する必要があります。 対称ハッシュを有効または無効にするには、オプションの **symmetric** キーワードを使用します。対称ハッシュにより、双方向のトラフィックで同じ物理インターフェイスを使用することが強制されます。対称ハッシュをサポートするのは、次のロードバランシング アルゴリズムのみです。 • source-dest-ip-only • source-dest-port-only • source-dest-ip • source-dest-port • source-dest-ip-gre
ステップ 3	(Optional) switch(config)# **no port-channel load-balance ethernet**	ロードバランシング アルゴリズムをデフォルトのsource-dest-macに戻します。
ステップ 4	(Optional) switch# **show port-channel load-balance**	ポート チャネル ロードバランシング アルゴリズムを表示します。

Example

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

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

次に、ポート チャネルの対称ハッシュを設定する例を示します。

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

LACP のイネーブル化

LACP はデフォルトではディセーブルです。LACP の設定を開始するには、LACP をイネーブルにする必要があります。LACP ポートチャネルが設定されている場合、LACP はディセーブルにできません。

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# **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	(Optional) switch(config)# **show feature**	イネーブルにされた機能を表示します。

Example

次に、LACP をイネーブルにする例を示します。

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

ポートに対するチャネル モードの設定

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

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

Before you begin

LACP 機能がイネーブルになっていることを確認します。

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
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*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]	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。

	Command or Action	Purpose
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

Example

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

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

LACP ポート チャネルの MinLink の設定

MinLink 機能は、LACP ポート チャネルだけで動作します。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。

重要 LACP ポート チャネルの両側（つまり、両方のスイッチ）で LACP MinLink 機能を設定することを推奨します。ポート チャネルの片側だけで **lacp min-links** コマンドを設定すると、リンクフラッピングが発生する可能性があります。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **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ます。
ステップ 3	switch(config-if)# [**no**] **lacp min-links** *number*	最小リンクの数を設定します。 *number* のデフォルト値は、1 です。指定できる範囲は 1 ～ 32 です。 この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

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

例

次に、全体として *up* とラベル付けされたバンドルに対してアップしている必要があるリンクの最小数を設定する例を示します。

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

LACP ポートチャネル MaxBundle の設定

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

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

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

始める前に

適切なポートチャネル インターフェイスであることを確認します。

手順の概要

1. **configure terminal**
2. **interface port-channel** *number*
3. **lacp max-bundle** *number*
4. **show running-config interface port-channel** <*number*>

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *number*
	例：
	`switch(config)# interface port-channel 3`
	`switch(config-if)#`
		設定するインターフェイスを選択します。

ステップ 3	**lacp max-bundle** *number* 例： `switch(config-if)# lacp max-bundle <number>`	ポート チャネルで許可されるアクティブなバンドル LACP ポートの最大数を設定します。 ポート チャネルの max-bundle のデフォルト値は 32 です。指定できる範囲は 1 ～ 32 です。 （注） デフォルト値は 16 ですが、ポート チャネルのアクティブ メンバー数は、ポートチャネルで許可されている *pc_max_links_config* および *pc_max_active_members* の最小数です。
ステップ 4	**show running-config interface port-channel** <*number*> 例： `switch(config-if)# show running-config interface port-channel 3`	（オプション）インターフェイスのポート チャネル設定を表示します。

例

次に、アクティブなバンドル LACP ポートの最大数を設定する例を示します。

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

LACP 高速タイマー レートの設定

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

始める前に

LACP 機能がイネーブルになっていることを確認します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **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*	設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **lacp rate fast**	LACP がサポートされているインターフェイスに LACP 制御パケットを送信する際のレートとして高速レート（1 秒）を設定します。

例

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

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

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

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

LACP のシステム プライオリティおよびシステム ID の設定

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

Before you begin

LACP 機能がイネーブルになっていることを確認します。

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# **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	(Optional) switch# **show lacp system-identifier**	LACP システム識別子を表示します。

Example

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

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

LACP ポート プライオリティの設定

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

Before you begin

LACP 機能がイネーブルになっていることを確認します。

SUMMARY STEPS

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

DETAILED STEPS

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

Example

次に、イーサネット インターフェイス 1/4 の LACP ポート プライオリティを 40000 に設定する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# lacp port priority 40000
```

LACP グレースフル コンバージェンスのディセーブル化

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

（注） このコマンドを使用する前に、ポート チャネルが管理ダウン状態である必要があります。

始める前に

LACP をイネーブルにします。

手順の概要

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

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

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *number*
	例：
	`switch(config)# interface port-channel 1`
	`switch(config-if)#`
		設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**shutdown** 例： `switch(config-if) shutdown`	ポート チャネルを管理シャットダウンします。
ステップ 4	**no lacp graceful-convergence** 例： `switch(config-if)# no lacp graceful-convergence`	ポート チャネルの LACP グレースフル コンバージェンスをディセーブルにします。
ステップ 5	**no shutdown** 例： `switch(config-if) no shutdown`	ポート チャネルを管理的にアップします。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

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

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

LACP グレースフル コンバージェンスの再イネーブル化

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

手順の概要

1. **configure terminal**
2. **interface port-channel** *number*
3. **shutdown**
4. **lacp graceful-convergence**
5. **no shutdown**
6. **copy running-config startup-config**

手順の詳細

	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-if)#`
		設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**shutdown** 例： `switch(config-if) shutdown`	ポート チャネルを管理シャットダウンします。
ステップ 4	**lacp graceful-convergence** 例： `switch(config-if)# lacp graceful-convergence`	ポート チャネルの LACP グレースフル コンバージェンスをイネーブルにします。
ステップ 5	**no shutdown** 例： `switch(config-if) no shutdown`	ポート チャネルを管理アップします。
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。

例

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

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

ポート チャネル設定の確認

次のコマンドを使用すると、ポート チャネル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** *type slot*/*port* | **neighbor** | **port-channel** | **system-identifier**}	LACP 情報を表示します。
show port-channel compatibility-parameters	ポート チャネルに追加するためにメンバー ポート間で同じにするパラメータを表示します。
show port-channel database [**interface port-channel** *channel-number*]	1 つ以上のポート チャネル インターフェイスの集約状態を表示します。
show port-channel summary	ポート チャネル インターフェイスの概要を表示します。
show port-channel traffic	ポート チャネルのトラフィック統計情報を表示します。
show port-channel usage	使用済みおよび未使用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。

ポートチャネルメンバシップ整合性チェッカのトリガー

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **show consistency-checker membership port-channels**	ポート チャネルのメンバー ポートに対するポート チャネル メンバーシップ整合性検査を開始して結果を表示します。

例

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

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

ロードバランシング発信ポート ID の確認

コマンドに関する注意事項

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

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

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

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-ip src-ip dst-mac src-mac l4-src-port** *port-id* **l4-dst-port** *port-id* **ether-type** *ether-type* **ip-proto** *ip-proto*	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 プロファイル

多くのインターフェイス コマンドを含むポート プロファイルを作成し、一定範囲のインターフェイスにそのポート プロファイルを適用することができます。ポート プロファイルはそれぞれ特定のタイプのインターフェイスにだけ適用できます。次のインターフェイスから選択できます。

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

インターフェイス タイプにイーサネットまたはポート チャネルを選択する場合、ポート プロファイルはデフォルトモードになります。デフォルトモードはレイヤ3です。ポートプロファイルをレイヤ 2 モードに変更するには、**switchport** コマンドを入力します。

ポートプロファイルをインターフェイスまたはインターフェイスの範囲にアタッチするときにポート プロファイルを継承します。ポート プロファイルをインターフェイスまたはインターフェイスの範囲にアタッチ、または継承する場合、そのポートプロファイルのすべてのコマンドがインターフェイスに適用されます。また、ポートプロファイルには、別のポートプロファイルの設定を継承することができます。別のポートプロファイルを継承した場合、最初のポート プロファイルでは、それを継承した第 2 のポート プロファイルに含まれるすべてのコマンドは、最初のポートプロファイルとは競合していないものと見なされます。4つのレベルの継承に対応しています。任意の数のポート プロファイルで同じポート プロファイルを継承できます。

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

- 競合が発生した場合は、インターフェイス モードで入力したコマンドがポート プロファイルのコマンドに優先します。しかし、ポート プロファイルはそのコマンドをポート プロファイルに保持します。
- ポート プロファイルのコマンドは、port-profile コマンドがデフォルト コマンドで明示的に上書きされていない限り、インターフェイスのデフォルト コマンドに優先します。
- 一定範囲のインターフェイスが2つ目のポートプロファイルを継承すると、矛盾がある場合、最初のポート プロファイルのコマンドが 2 つ目のポート プロファイルのコマンドを無効にします。
- ポートプロフ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。

指定するインターフェイス タイプにより、コマンドのサブセットが port-profile コンフィギュレーション モードで使用できます。

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

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

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

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

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

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

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

インターフェイスまたはインターフェイスの範囲のポートプロファイルを継承し、特定の設定値を削除した後、その port-profile コンフィギュレーションは指定のインターフェイスでは動作しません。

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、システムによりエラーが返されます。

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

ポート プロファイルの設定

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

ポート プロファイルの作成

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

（注） ポート プロファイル名には、次の文字のみを使用できます。

- a ～ z
- A ～ Z
- 0 ～ 9
- 特殊文字は、以下を除き使用できません。
  - .
  - -
  - _

手順の概要

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

手順の詳細

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

例

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

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

ポート プロファイル コンフィギュレーション モードの開始およびポート プロファイルの修正

ポート プロファイル コンフィギュレーション モードを開始し、ポート プロファイルを修正できます。ポート プロファイルを修正するには、ポート プロファイル コンフィギュレーション モードを開始する必要があります。

手順の概要

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

手順の詳細

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

例

次に、指定されたポート プロファイルのポート プロファイル コンフィギュレーション モードを開始し、すべてのインターフェイスを管理アップする例を示します。

```
switch# configure terminal
switch(config)# port-profile type ethernet test
switch(config-ppm)# no shutdown
switch(config-ppm)#
```

一定範囲のインターフェイスへのポートプロファイルの割り当て

単独のインターフェイスまたはある範囲に属する複数のインターフェイスにポートプロファイルを割り当てることができます。すべてのインターフェイスが同じタイプである必要があります。

手順の概要

1. **configure terminal**
2. **interface** [**ethernet** *slot/port* | **interface-vlan** *vlan-id* | **port-channel** *number*]
3. **inherit port-profile** *name*
4. **exit**
5. （任意） **show port-profile**
6. （任意） **copy running-config startup-config**

手順の詳細

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

例

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

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

特定のポート プロファイルのイネーブル化

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

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

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

手順の概要

1. **configure terminal**

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

手順の詳細

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

例

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

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

ポート プロファイルの継承

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

手順の概要

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

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**port-profile** *name*	指定されたポート プロファイルに対して、ポート プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**inherit port-profile** *name*	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**	ポート プロファイル コンフィギュレーション モードを終了します。
ステップ 5	（任意） **show port-profile**	ポート プロファイル設定を表示します。
ステップ 6	（任意） **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

例

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

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

一定範囲のインターフェイスからのポートプロファイルの削除

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
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。
ステップ 3	**no inherit port-profile** *name*	選択したインターフェイスへの指定したポート プロファイルの割り当てを解除します。
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	（任意） **show port-profile**	ポート プロファイル設定を表示します。
ステップ 6	（任意） **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

例

次の例は、イーサネット インターフェイス 7/3 ～ 7/5、10/2、および 11/20 ～ 11/25 への adam という名前のポート プロファイルの割り当てを解除する方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 7/3-5, 10/2, 11/20-25
switch(config-if)# no inherit port-profile adam
switch(config-if)#
```

継承されたポート プロファイルの削除

継承されたポート プロファイルを削除できます。この設定は、ポート プロファイル モードで行います。

手順の概要

1. **configure terminal**
2. **port-profile** *name*
3. **no inherit port-profile** *name*
4. **exit**
5. （任意） **show port-profile**
6. （任意） **copy running-config startup-config**

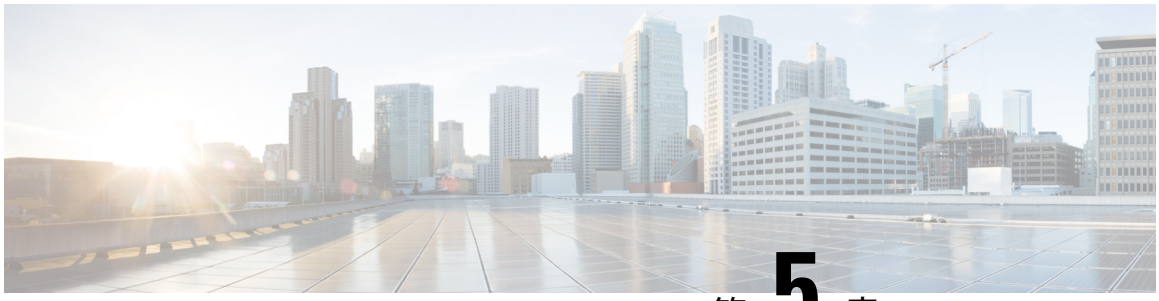
手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**port-profile** *name*	指定されたポート プロファイルに対して、ポート プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**no inherit port-profile** *name*	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**	ポート プロファイル コンフィギュレーション モードを終了します。
ステップ 5	（任意） **show port-profile**	ポート プロファイル設定を表示します。
ステップ 6	（任意） **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

例

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

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



第 5 章

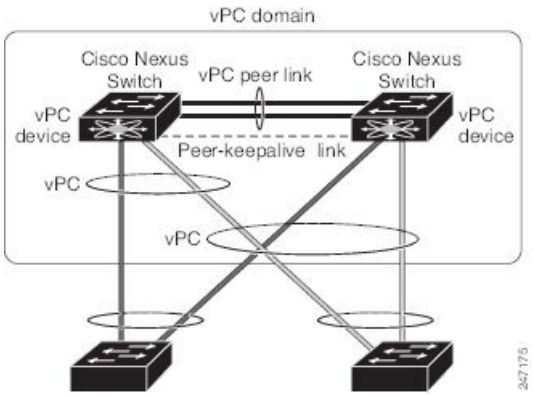
仮想ポート チャネルの設定

vPC について

vPC の概要

仮想ポート チャネル（vPC）を使用すると、物理的には 2 台の異なる Cisco Nexus デバイスに接続されている複数のリンクを、第 3 のデバイスからは単一のポートチャネルとして認識されるようにすることができます（次の図を参照）。第 3 のデバイスには、スイッチやサーバなどあらゆるネットワーキングデバイスが該当します。vPC では、マルチパス機能を使用することができます。この機能では、ノード間の複数のパラレルパスをイネーブルにし、さらには存在する代替パスでトラフィックのロード バランシングを行うことにより、冗長性が確保されます。

Figure 5: vPC のアーキテクチャ



EtherChannel の設定は、次のいずれかを使用して行います。

- プロトコルなし
- リンク集約制御プロトコル（LACP）

vPC に EtherChannel を設定する場合（vPC ピア リンク チャネルも含める）、各スイッチは、単一の EtherChannel 内に最大 32 個のアクティブ リンクを設定できます。

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

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

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

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

vPC ドメインには、両方の vPC ピア デバイス、vPC ピアキープアライブ リンク、vPC ピア リンク、および vPC ドメイン内にあ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。

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

vPC には次のような特長があります。

- 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。
- 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。

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。

Note システム プライオリティを手動で設定する場合は、必ず両方の vPC ピア スイッチ上に同じプライオリティ値を割り当てるようにしてください。両側の vPC ピア スイッチに異なるシステム プライオリティ値が割り当てられている場合、vPC は稼働しません。

ピアキープアライブ リンクとメッセージ

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

一方の vPC ピア スイッチに障害が発生すると、vPC ピア リンクのもう一方の側にある vPC ピア スイッチでは、ピアキープアライブ メッセージを受信しなくなることによってその障害を検知します。vPC ピアキープアライブ メッセージのデフォルトの時間間隔は 1 秒です。この時間間隔は、400 ミリ秒～ 10 秒の範囲で設定することができます。タイムアウト値は、3 ～ 20 秒の範囲内で設定可能で、デフォルトのタイムアウト値は 5 秒です。ピアキープアライブのステータスの確認は、ピアリンクがダウンした場合にのみ行われます。

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

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

vPC ピア リンクの互換パラメータ

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

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

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

vPC ポート チャネルでの新しいタイプ 2 整合性検査

vPC ポート チャネルのスイッチポート MAC 学習設定を検証するために、新しいタイプ 2 整合性検査が追加されました。CLI の **show vpc consistency-check vPC <vpc no.>** は、スイッチポート MAC 学習設定のローカル値とピア値を表示するように拡張されました。これはタイプ 2 チェックであるため、vPCは、ローカル値とピア値の間に不一致がある場合でも動作上アップ状態になりますが、この不一致は CLI 出力から表示できます。

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

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

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

同じでなければならない設定パラメータ

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

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

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

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

- ポートチャネル モード：オン、オフ、またはアクティブ
- チャネル単位のリンク速度
- チャネル単位のデュプレックス モード
- チャネルごとのトランク モード：
  - ネイティブ VLAN
  - トランク上で許可される VLAN
  - ネイティブ VLAN トラフィックのタギング
- スパニング ツリー プロトコル（STP）モード
- マルチ スパニングツリーの STP 領域コンフィギュレーション（MST）
- VLAN ごとのイネーブル/ディセーブル状態
- STP グローバル設定：
  - ブリッジ保証設定
  - ポート タイプ設定：vPCインターフェイスはすべて標準ポートとして設定することが推奨されます
  - ループ ガード設定
- STP インターフェイス設定：
  - ポート タイプ設定
  - ループ ガード
  - ルート ガード

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

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

同じにすべき設定パラメータ

次に挙げるパラメータのいずれかが両方の 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。
- ACL のすべての設定とパラメータ
- Quality of Service（QoS）の設定およびパラメータ：ローカル パラメータです。グローバル パラメータは同じであることが必要です
- STP インターフェイス設定：
  - BPDU フィルタ
  - BPDU ガード
  - コスト
  - リンク タイプ
  - プライオリティ
  - VLAN（Rapid PVST+）

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

VLAN ごとの整合性検査

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

vPC 自動リカバリ

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

ピア リンクの障害に伴ってセカンダリ vPC スイッチ上の vPC がディセーブルになり、さらにプライマリ vPC スイッチで障害が発生するか、またはトラフィックが転送できなくなると、セカンダリ スイッチでは vPC が再イネーブル化されます。このシナリオの場合、vPC ではキープアライブが 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 自動リカバリ機能は、デフォルトでイネーブルです。

vPC ピア リンク

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

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

vPC ピア リンクの概要

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

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

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

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

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

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

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

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

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

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

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

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

vPC 番号

vPC ドメイン ID と vPC ピア リンクを作成すると、ダウンストリーム スイッチを各 vPC ピア スイッチに接続するための EtherChannel を作成することができます。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、ダウンストリーム スイッチに接続された EtherChannel に同じ vPC 番号を割り当てます。vPC の作成時にトラフィックが中断されることはほとんどありません。設定を簡素化するため、各 EtherChannel に対してその EtherChannel と同じ番号の vPC ID 番号を割り当てることもできます（EtherChannel 10 に対しては vPC ID 10 を割り当てるなど）。

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

その他の機能との vPC の相互作用

vPC と LACP

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

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

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

Note システム プライオリティを手動で設定する場合は、必ず両方の vPC ピア スイッチ上に同じプライオリティ値を割り当てるようにしてください。vPC ピア スイッチ同士が異なるシステム プライオリティ値を持っていると、vPC は稼働しません。

vPC ピア リンクと STP

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。

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

CFSoE

Cisco Fabric Services over Ethernet（CFSoE）は、vPC ピア デバイスの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。

Note **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 フォークリフト アップグレードのシナリオ

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

vPC フォークリフト アップグレードに関する考慮事項：

- vPC ロールの選択とスティッキビット

  2 つの vPC システムの組み合わせによって vPC ドメインが形成される場合は、プライオリティによって、どちらのデバイスが vPC プライマリで、どちらのデバイスが vPC セカンダリかが決定されます。プライマリ デバイスがリロードされると、システムがオンラインに戻り、vPC セカンダリ デバイス（現在、動作上のプライマリ）への接続が復元されます。セカンダリ デバイス（動作上のプライマリ）の動作ロールは変更されません（不要な

中断を防ぐため）。この動作は、スティッキビットによって実現されます。スティッキビットでは、スティッキ情報がスタートアップ コンフィギュレーションに保存されません。この方式では、稼働中のデバイスがリロードされたデバイスよりも優先されます。そのため、vPC プライマリは動作上の vPC セカンダリになります。ピア リンクとピアキープアライブがダウンしてvPCノードが起動し、自動復旧期間後にプライマリになるときにも、スティッキビットが設定されます。

- vPC の遅延復元

  遅延復元タイマーは、ピアの隣接がすでに確立されている場合に、リロード後に復元した vPC ピア デバイスでの vPC の起動を遅らせるために使用されます。

  復元した vPC ピア デバイス上の VLAN インターフェイスが起動するのを遅延するには、**interfaces-vlan** オプションを **delay restore** のオプション コマンドに使用します。

- vPC 自動リカバリ

  データセンターで停電が発生し、両方の vPC ピア スイッチがダウンした場合、スイッチが 1 つだけ復元すると、そのスイッチが自動回復機能によってプライマリ スイッチのロールを負い、vPC リンクが自動復旧期間後に起動します。デフォルトの自動復旧期間は 240 秒です。

次の例は、vPC ピア ノードの Node1 と Node2 を New_Node1 と New_Node2 に置き換える移行シナリオです。

	移行手順	予想される動作	Node1 の設定済みロール（例：ロール プライオリティ 100）	Node1 の動作ロール	Node2 の設定済みロール（例：ロール プライオリティ 200）	Node2 の動作ロール
1	初期状態です。	トラフィックは Node1 と Node2 の両方の vPC ピアによって転送されます。 Node1 がプライマリで、Node2 がセカンダリです。	プライマリ	プライマリ スティッキビット：False	セカンダリ	セカンダリ スティッキビット：False

	移行手順	予想される動作	Node1 の設定済みロール（例：ロール プライオリティ 100）	Node1 の動作ロール	Node2 の設定済みロール（例：ロール プライオリティ 200）	Node2 の動作ロール
2	Node2 を置き換えます。Node2 のすべての vPC とアップリンクを停止させます。ピア リンクと vPC ピアキープアライブが管理アップ状態になります。	トラフィックはプライマリ vPC ピア Node1 に収束します。	プライマリ	プライマリ スティッキビット：False	セカンダリ	セカンダリ スティッキビット：False
3	Node2 を削除します。	Node1 は引き続きトラフィックを転送します。	プライマリ	プライマリ スティッキビット：False	該当なし	該当なし
4	New_Node2 を設定します。コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。vPC ピア リンクとピアキープアライブが管理アップ状態になります。 New_Node2 の電源をオフにします。 すべての接続を行います。 New_Node2 の電源をオンにします。	New_Node2 はセカンダリとして起動します。Node1 は引き続きプライマリになります。 トラフィックは引き続き Node01 で転送されます。	プライマリ	プライマリ スティッキビット：False	セカンダリ	セカンダリ スティッキビット：False

	移行手順	予想される動作	Node1 の設定済みロール（例：ロール プライオリティ 100）	Node1 の動作ロール	Node2 の設定済みロール（例：ロール プライオリティ 200）	Node2 の動作ロール
5	New_Node2 のすべての vPC とアップリンク ポートを起動します。	トラフィックは Node1 と New_Node2 の両方によって転送されます。	プライマリ	プライマリ スティッキビット：False	セカンダリ	セカンダリ スティッキビット：False
6	Node1 を置き換えます。 Node1 の vPC とアップリンクを停止させます。	トラフィックは New_Node2 に収束します。	プライマリ	プライマリ スティッキビット：False	セカンダリ	セカンダリ スティッキビット：False
7	Node1 を削除します。	New_Node2 がセカンダリ（動作上のプライマリ）になり、スティッキビットが True に設定されます。	該当なし	該当なし	セカンダリ	プライマリ スティッキビット：True
8	New_Node1 を設定します。実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。 New_Node1 の電源をオフにします。すべての接続を行います。 New_Node1 の電源をオンにします。	New_Node1 はプライマリ（動作上のセカンダリ）として起動します。	プライマリ	セカンダリ スティッキビット：False	セカンダリ	プライマリ スティッキビット：True

	移行手順	予想される動作	Node1 の設定済みロール（例：ロール プライオリティ 100）	Node1 の動作ロール	Node2 の設定済みロール（例：ロール プライオリティ 200）	Node2 の動作ロール
9	New_Node1 のすべての vPC とアップリンク ポートを起動します。	トラフィックは New_Node1 と New_Node2 の両方によって転送されます。	プライマリ	セカンダリ スティッキビット：False	セカンダリ	プライマリ スティッキビット：True

（注） 設定されたセカンダリ ノードを動作上のセカンダリ、設定されたプライマリ ノードを動作上のプライマリとして使用するには、Node2 を移行の最後にリロードします。これはオプションであり、機能には影響を与えません。

vPC に関する注意事項と制約事項

vPC 設定時の注意事項と制限事項は次のとおりです。

- vPC は、異なるタイプの Cisco Nexus 3000 シリーズ スイッチ間ではサポートされません。
- VPC ピアには、VXLAN 用に予約した同一の VLAN が必要です。ピアで予約した VLAN が異なると、VXLAN によって望ましくない動作が発生する可能性があります。
- CLI コマンドの **sh vpc brief** の出力に、Delay-restore status と Delay-restore SVI status の 2 つの追加のフィールドが表示されます。
- vPC ピアリンクおよび vPC インターフェイスを設定する場合は、あらかじめ vPC 機能をイネーブルにしておく必要があります。
- システムにおいて vPC ピア リンクを構成するためには、その前にピアキープアライブ 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。
- 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 に使用できるのは、ポート チャネルのみです。vPC は標準ポート チャネル（スイッチ間の vPC トポロジ）およびポート チャネル ホスト インターフェイス（ホスト インターフェイスの vPC トポロジ）で設定できます。
- 両側の vPC ピア スイッチを設定する必要があります。ただし vPC ピア デバイス間で設定が自動的に同期化されることはありません。
- 必要な設定パラメータが、vPC ピア リンクの両側で互換性を保っているかチェックしてください。
- vPC の設定中に、最小限のトラフィックの中断が発生する可能性があります。
- アクティブ モードのインターフェイスで LACP を使用して vPC のすべてのポート チャネルを設定する必要があります。
- vPC の最初のメンバが起動すると、トラフィックが中断する可能性があります。
- OSPF over vPC および BFD with OSPF は、Cisco Nexus 3000 シリーズ スイッチでサポートされます。

  SVI の制約：BFD セッションが仮想ポート チャネル（vPC）ピア リンクを使用して SVI 経由で行われる場合、BFD エコー機能はサポートされません。SVI 設定レベルで **no bfd echo** を使用して、vPC ピア ノード間で行われる SVI 経由のすべてのセッションに関して BFD エコー機能を無効にする必要があります。
- ピアキープアライブに管理インターフェイスではなくレイヤ 3 リンクが使用されている場合、CPU キューがコントロール プレーン トラフィックと輻輳すると、vPC ピアキープアライブ パケットがドロップする可能性があります。CPU トラフィックには、ルーティング プロトコル、ARP、Glean、および IPMC ミス パケットが含まれます。ピアキープアライブ インターフェイスが管理インターフェイスではなくレイヤ 3 リンクである場合、vPC ピアキープアライブ パケットは、ロープライオリティ キューで CPU に送信されます。

  vPC ピアキープアライブにレイヤ 3 リンクが使用されている場合は、次の ACL を設定して vPC ピアキープアライブを優先させます。

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

  ここで、「3200」は、キープアライブ パケットのデフォルトの UDP ポートです。デフォルト ポートが変更されている場合は、この ACL を、設定されている UDP ポートに一致させる必要があります。

vPC 設定の確認

vPC の設定情報を表示する場合は、次のコマンドを使用します。

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

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

スイッチの出力の詳細については、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
Auto-recovery status              : Disabled
Delay-restore status              : Timer is off.(timeout = 30s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
```

```
--   ----   ------ ----------------------------------------------------
1    Po1    up     1
```

グローバル タイプ 1 不整合の表示

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

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

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

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

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

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

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

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

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

```
Number of vPCs configured       : 2
Peer Gateway                    : Disabled
Dual-active excluded VLANs      : -
Graceful Consistency Check      : Enabled

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

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

インターフェイス別タイプ 1 不整合の表示

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

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

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

vPC domain id                   : 10
Peer status                     : peer adjacency formed ok
vPC keep-alive status           : peer is alive
Configuration consistency status: success
Per-vlan consistency status     : success
Type-2 consistency status       : success
vPC role                        : secondary
Number of vPCs configured       : 2
Peer Gateway                    : Disabled
Dual-active excluded VLANs      : -
Graceful Consistency Check      : Enabled
Auto-recovery status              : Disabled
Delay-restore status              : Timer is off.(timeout = 30s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)

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

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

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

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

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
Per-vlan consistency status     : success
Type-2 consistency status       : success
vPC role                          : primary
Number of vPCs configured       : 2
Peer Gateway                      : Disabled
Dual-active excluded VLANs      : -
Graceful Consistency Check      : Enabled
Auto-recovery status              : Disabled
Delay-restore status              : Timer is off.(timeout = 30s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)

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

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

VLAN ごとの整合性ステータスの表示

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

例

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

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

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

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

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

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

no spanning-tree vlan 5 コマンドを入力すると、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                     : 1
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : primary
Number of vPCs configured         : 2
Peer Gateway                      : Disabled
Dual-active excluded VLANs and BDs : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Enabled, timer is off.(timeout = 240s)
Delay-restore status              : Timer is off.(timeout = 30s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1000 up     1-5,8,11-19


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

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

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

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

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
Per-vlan consistency status       : failed
Type-2 consistency status         : success
vPC role                          : primary
Number of vPCs configured         : 2
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status               : Disabled
Delay-restore status               : Timer is off.(timeout = 30s)
Delay-restore SVI status           : Timer is off.(timeout = 10s)

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1-4,6-10

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

次に、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 のデフォルト設定

次の表は、vPC パラメータのデフォルト設定をまとめたものです。

Table 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

vPC の設定

vPC のイネーブル化

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# **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	(Optional) switch# **show feature**	スイッチ上でイネーブルになっている機能を表示します。
ステップ 4	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次の例は、vPC 機能をイネーブルにする方法を示します。

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

vPC のディセーブル化

vPC 機能をディセーブルにできます。

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# **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	(Optional) switch# **show feature**	スイッチ上でイネーブルになっている機能を表示します。
ステップ 4	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次の例は、vPC 機能をディセーブルにする方法を示します。

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

vPC ドメインの作成

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

Before you begin

vPC 機能をイネーブルにしていることを確認します。

vPC ピア リンクの両側に両方のスイッチを設定する必要があります。

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# **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。 **Note** 既存の vPC ドメインに対して vpc-domain コンフィギュレーション モードを開始する場合は、**vpc domain** コマンドを使用することもできます。
ステップ 3	(Optional) switch# **show vpc brief**	各 vPC ドメインに関する要約情報を表示します。
ステップ 4	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、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。

Note vPC ピアキープアライブ リンクを使用する際は、個別の VRF インスタンスを設定して、各 vPC ピア スイッチからその VRF インスタンスにレイヤ 3 ポートを接続することが推奨されます。ピア リンク自体を使用して vPC ピアキープアライブ メッセージを送信しないでください。

Before you begin

vPC 機能が有効なことを確認します。

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

vPC ピア リンクの両側に両方のスイッチを設定する必要があります。

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# **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。 **Note** vPC ピアキープアライブ リンクを設定するまで、vPC ピア リンクは構成されません。 管理ポートと VRF がデフォルトです。
ステップ 4	(Optional) switch(config-vpc-domain)# **vpc peer-keepalive destination** *ipaddress* **source** *ipaddress*	vPC ピアキープアライブ リンクに対し、個別の VRF インスタンスを設定して、各 vPC ピア デバイスからその VRF にレイヤ 3 ポートを接続します。
ステップ 5	(Optional) switch# **show vpc peer-keepalive**	キープアライブ メッセージのコンフィギュレーションに関する情報を表示します。
ステップ 6	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

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

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

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

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

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

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

L3-NEXUS-2# show vpc peer-keepalive

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

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

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

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

vPC ピア リンクの作成

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

Before you begin

vPC 機能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。

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# **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	(Optional) switch# **show vpc brief**	vPC ピア リンクに関する情報など、各 vPC の情報を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次の例は、vPC ピア リンクを設定する方法を示します。

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

設定の互換性の検査

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

次の QoS パラメータは、タイプ 2 整合性検査をサポートします。

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

- Output Queuing：Bandwidth および Absolute Priority

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

手順の概要

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

手順の詳細

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

例

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

```
switch# show vpc consistency-parameters global
Legend:
        Type 1 : vPC will be suspended in case of mismatch
Name                        Type  Local Value            Peer Value

------------- ----  ---------------------- -----------------------
QoS                         2     ([], [], [], [], [],   ([], [], [], [], [],
                                   [])                    [])

Network QoS (MTU)           2     (1538, 0, 0, 0, 0, 0)  (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#
```

vPC 自動リカバリのイネーブル化

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **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。

例

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



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

復元遅延時間の設定

ピアの隣接が形成され、VLANインターフェイスがバックアップされるまで、バックアップからの vPC の回復を遅らせるようにリストア タイマーを設定できます。この機能により、vPC が再びトラフィックの受け渡しをし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。

始める前に

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。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **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。
ステップ 4	（任意） switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

例

次の例は、vPC リンクに対する復元遅延時間の設定方法を示したものです。

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

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

vPC ピア リンクが失われると、vPC セカンダリ スイッチによりその vPC メンバー 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。

始める前に

VLAN インターフェイスが設定済みであることを確認します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **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。

例

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

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

VRF 名の設定

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

VRF 名を指定することができます。

手順の概要

1. switch# **ping** *ipaddress* **vrf** *vrf-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **ping** *ipaddress* **vrf** *vrf-name*	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。

例

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
```

他のポート チャネルの vPC への移行

Before you begin

vPC 機能が有効なことを確認します。

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

SUMMARY STEPS

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

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

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# **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。 **Note** 通常のポート チャネル（物理的な 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。
ステップ 3	switch(config-if)# **vpc** *number*	選択したポート チャネルを vPC に配置してダウンストリーム スイッチに接続するように設定します。範囲は 1 ～ 4096 です。 vPC ピア スイッチからダウンストリーム スイッチに接続されているポートチャネルに割り当てる vPC 番号は、両方の vPC スイッチで同じでなければなりません。
ステップ 4	(Optional) switch# **show vpc brief**	各 vPC に関する情報を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次の例は、ダウンストリームデバイスに接続されるポートチャネルを設定する方法を示します。

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

vPC ドメイン MAC アドレスの手動での設定

Note システム アドレスの設定は、オプションの設定手順です。

Before you begin

vPC 機能が有効なことを確認します。

vPC ピア リンクの両側に両方のスイッチを設定する必要があります。

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# **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。
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	(Optional) switch# **show vpc role**	vPC システムの MAC アドレスを表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

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

```
switch# configure terminal
switch(config)# vpc domain 5
```

```
switch(config-if)# system-mac 23fb.4ab5.4c4e
```

システム プライオリティの手動での設定

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

Before you begin

vPC 機能が有効なことを確認します。

vPC ピア リンクの両側に両方のスイッチを設定する必要があります。

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# **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。
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	(Optional) switch# **show vpc brief**	vPC ピア リンクに関する情報など、各 vPC の情報を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次の例は、vPC ピア リンクを設定する方法を示します。

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

vPC ピア スイッチのロールの手動による設定

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

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

Before you begin

vPC 機能が有効なことを確認します。

vPC ピア リンクの両側に両方のスイッチを設定する必要があります。

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# **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。

	Command or Action	Purpose
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	(Optional) switch# **show vpc brief**	vPC ピア リンクに関する情報など、各 vPC の情報を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次の例は、vPC ピア リンクを設定する方法を示します。

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

vPC のレイヤ 3 の設定

始める前に

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

ピア リンクがアップしていることを確認します

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	switch# **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	switch(config)# **vpc domain** *domain-id*
	例：
	`switch(config)# vpc domain 5`
	`switch(config-vpc-domain)#`
		vPC ドメインがまだ存在していない場合はそれを作成し、vpc-domain コンフィギュレーション モードを開始します。デフォルトはありません。指定できる範囲は <1 ～ 1000> です。

ステップ 3	switch(config-vpc-domain)#**layer3 peer-router**	両方のピアとのピアリング隣接関係を形成するためレイヤ 3 デバイスを有効にします。 （注） 両方のピアでこのコマンドを設定します。このコマンドをピアのうち 1 つでのみ設定するか、1 つのピアで無効にすると、レイヤ 3 ピアルータの動作状態が無効になります。動作状態に変更があると、通知が表示されます。
ステップ 4	switch(config-vpc-domain)# **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 5	（任意） switch# **show vpc brief**	各 vPC ドメインに関する要約情報を表示します。
ステップ 6	（任意） switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

例

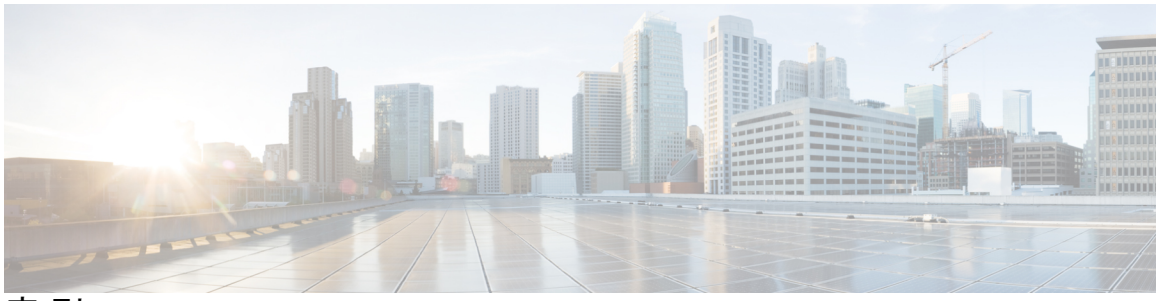
次に、vPC 機能経由でレイヤ 3 を設定する例を示します。

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

switch(config-vpc-domain)# exit

switch(config)#
```

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

```
switch# show vpc brief

vPC domain id : 5
```

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



索 引

か

さ

せ

た

ち

て

と

は

ふ

ほ

む

も

る

れ

ろ