Cisco Nexus 9000 シリーズ NX-OS インターフェイス コンフィギュレーション ガイド リリース 7.x

初版：2015 年 01 月 27 日

最終更新：2016 年 07 月 20 日

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

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

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、角カッコで囲んで示しています。
[x | y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。

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

例では、次の表記法を使用しています。

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

Cisco Nexus 9000 シリーズ スイッチの関連資料

Cisco Nexus 9000 シリーズ 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/en/US/products/ps13386/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。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『*What's New in Cisco Product Documentation*』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html から入手できます。

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

第 1 章

新機能および変更された機能に関する情報

この章では、『*Cisco Nexus 9000* シリーズ *NX-OS* インターフェイス コンフィギュレーション ガイド』に記載されている新機能および変更された各機能について、リリース固有の情報を示します。

新機能および変更された機能に関する情報

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

表 *1*：新機能および変更された機能

機能	説明	変更されたリリース	参照先
SFP+ アダプタ モジュール	CVR-2QSFP28-8SFP アダプタに Cisco Nexus 9236C スイッチの 100G ポートの 25G 光ファイバ サポートが追加されました。	7.0(3)I4(2)	Cisco SFP+ アダプタ モジュールのサポート，（24 ページ）
SVI の VRF メンバーシップ変更のサポート	SVI の VRF メンバーシップ変更のサポートが追加されました。	7.0(3)I4(1)	インターフェイスの VRF メンバーシップの変更
ポート プロファイルのサポート	ポート プロファイルのサポートが追加されました。	7.0(3)I4(1)	ポート プロファイル

新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
vPC での PIM SSM のサポート	vPC での PIM SSM のサポートが追加されました。	7.0(3)I4(1)	vPC マルチキャスト：PIM、IGMP、および IGMP スヌーピング
In Service Software Upgrade（ISSU）の NAT サポート	In Service Software Upgrade（ISSU）の NAT サポートが追加されました。	7.0(3)I4(1)	スタティック NAT の注意事項および制約事項
Cisco Nexus C9332PQ スイッチのブレークアウト および FEX サポート	Cisco Nexus C9332PQ スイッチのブレークアウト および FEX サポートが追加されました（TOR スイッチ）。	7.0(3)I3(1)	Cisco Nexus C9332PQ スイッチ
Cisco Nexus 92160YC スイッチのブレークアウト サポート	Cisco Nexus 92160YC スイッチのブレークアウト サポートが追加されました（TOR スイッチ）。	7.0(3)I3(1)	Cisco Nexus C92160YC スイッチ
Cisco Nexus 9272Q スイッチのブレークアウト サポート	Cisco Nexus 9272Q スイッチのブレークアウト サポートが追加されました（TOR スイッチ）。	7.0(3)I3(1)	Cisco Nexus C9272Q スイッチ
ip unnumbered コマンド	IP unnumbered コマンドのサポートが追加されました。	7.0(3)I3(1)	IP アンナンバード
レイヤ 2 データセンター相互接続	レイヤ 2 データセンター相互接続のサポートが追加さました。	7.0(3)I2(2)	レイヤ 2 データセンター相互接続の設定
vPC domain コマンド の **shut** および **no shut** サポート	**vPC domain** コマンドの **shut** および **no shut** のサポートが追加されました。	7.0(3)I2(2)	vPC の設定
DHCP Client	Cisco Nexus 9500 シリーズ スイッチのサポートが追加されました。	7.0(3)I2(2)	DHCP Client
スイッチポート分離のサポート	switchport isolated コマンドのサポートが追加されました。	7.0(3)I2(1)	スイッチポートの分離による 4K VLAN 設定の有効化

新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
DHCP Client	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の DHCP クライアントの IPv4 または IPv6 アドレス設定のサポートが追加されました。	7.0(3)I2(1)	DHCP Client
GRE トンネル拡張機能	v4 トンネル経由の GRE v6 ペイロードと v6 トンネル経由の GRE v4 ペイロードのサポートが追加されました。	7.0(3)I2(1)	GRE トンネルの設定
送信元インターフェイスのサポート	IPv4 や IPv6 のインバンドまたはアウトバンド送信元 IP アドレスを設定するための source-interface コマンド オプションのサポートが追加されました。	7.0(3)I2(1)	注意事項と制約事項
正規表現のサポート	一連のインターフェイスをアドレス指定するための正規表現のサポートが追加されました。	7.0(3)I2(1)	注意事項と制約事項
BFD 起動タイマー	この機能が導入されました。	7.0(3)I2(1)	グローバルな BFD パラメータの設定
スタティックおよびダイナミック NAT 変換のサポート	スタティックおよびダイナミック NAT 変換のサポートが追加されました。	7.0(3)I2(1)	スタティック NAT とダイナミック NAT 変換の設定
スイッチ仮想インターフェイスおよび自動ステート動作のサポート	スイッチ仮想インターフェイスおよび自動ステート動作のサポートが追加されました。	7.0(3)I2(1)	スイッチ仮想インターフェイスおよび自動ステート動作
IP-in-IP トンネル マスクのサポート	IP-in-IP トンネル マスクのサポートが追加されました。	7.0(3)I2(1)	トンネル インターフェイスの作成
Q-in-Q VLAN トンネルのサポート	Q-in-Q VLAN トンネルのサポートが追加されました。	7.0(3)I2(1)	Q-in-Q VLAN トンネルの設定

新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
MAC 組み込み IPv6（MEv6）アドレス	この機能が導入されました。	7.0(3)I2(1)	MAC 組み込み IPv6 アドレス
vPC フォークリフト アップグレードのサポート	vPC トポロジ内の Nexus 9000 スイッチのペアから異なる Nexus 9000 シリーズ スイッチのペアへのアップグレードのサポートが追加されました。	7.0(3)I1(2)	vPC フォークリフト アップグレードのシナリオ
遅延 LACP のサポート	遅延 LACP 機能により、LACP PDU が受信されるまでポート チャネル メンバーの起動を遅延させることができます。	7.0(3)I1(2)	遅延 LACP
negotiate auto コマンドのサポート	イーサネット インターフェイスの速度、デュプレックス、および自動フロー制御を設定できます。	7.0(3)I1(2)	注意事項と制約事項
IP-in-IP トンネルのサポート	トンネルを作成するためにパケットをカプセル化およびカプセル化解除できます。	7.0(3)I1(2)	ポイントツーポイント IP-in-IP トンネルのカプセル化およびカプセル化解除
ポートチャネル インターフェイスでのサブインターフェイスのサポート	ポートチャネル インターフェイスでの 1 つまたは複数のサブインターフェイスのサポートが追加されました。	7.0(3)I1(2)	ポートチャネル インターフェイスでのサブインターフェイスの設定
ダイナミック ブレークアウトのサポート	高帯域幅ポートを 4 つのブレークアウト ポートに分割できます。	7.0(3)I1(1)	ダイナミック ブレークアウト（個別ポート レベルのブレークアウト）
対称ハッシュのサポート	ポート チャネル上で対称ハッシュを有効にすると、双方向トラフィックが確実に同じ物理インターフェイスを使用するようになります。	7.0(3)I1(1)	対称ハッシュ

機能	説明	変更されたリリース	参照先
追加の **show interface tunnel** コマンドのサポート	インターフェイス カウンタに関する統計情報のサポートが追加されました。	7.0(3)I1(1)	IP トンネル設定の確認
BFDv6 のサポート	BFDv6 のサポートが追加されました。	7.0(3)I1(1)	双方向フォワーディング検出の設定, （131 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

概要

インターフェイスについて

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

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

表 *2*：インターフェイスのパラメータ

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

機能	パラメータ（Parameters）	解説場所
セキュリティ	EOU	『*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*』

Ethernet Interfaces

イーサネット インターフェイスには、ルーテッド ポートが含まれます。

Access Ports

アクセス ポートは 1 つの VLAN のトラフィックを送受信します。このポートのタイプはレイヤ 2 インターフェイスだけです。

ルーテッド ポートの詳細については、「アクセス インターフェイスとトランク インターフェイスについて」の項を参照してください。

Routed Ports

ルーテッド ポートは、IP トラフィックを他のデバイスにルーティングできる物理ポートです。ルーテッド ポートはレイヤ 3 インターフェイスだけです。

ルーテッド ポートの詳細については、「ルーテッド インターフェイス」の項を参照してください。

管理インターフェイス

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

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

ポートチャネル インターフェイス

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

サブインターフェイス

レイヤ 3 インターフェイスとして設定した親インターフェイスに仮想サブインターフェイスを作成できます。親インターフェイスは物理ポートでかまいません。親インターフェイスはサブインターフェイスによって複数の仮想インターフェイスに分割されます。これらの仮想インターフェイスに IP アドレスやダイナミック ルーティング プロトコルなど固有のレイヤ 3 パラメータを割り当てることができます。

ループバック インターフェイス

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

ブレークアウト インターフェイス

Cisco NX-OS は、モジュール レベルまたは個別ポート レベルでの高帯域幅 40G インターフェイスのブレークアウトをサポートしています。

モジュール レベルのブレークアウト

モジュール レベルのブレークアウトでは、**interface breakout** コマンドにより、モジュールの高帯域幅 40G インターフェイスが 4 つの 10G インターフェイスに分割されます。コマンドが実行されると、モジュールがリロードされ、インターフェイスの設定は削除されます。

次に、コマンドの例を示します。

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

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

ダイナミック ブレークアウト（個別ポート レベルのブレークアウト）

ダイナミック ブレークアウト（個別ポート レベルのブレークアウト）では、**interface breakout** コマンドにより、高帯域幅の 40G ポートが 4 つの 10G ブレークアウト ポートに分割されます。ブレークアウト ポートは、「**Ethernet** *<slot>/<front-panel-port>/<breakout-port>*」として識別されます。たとえば、個別ポート レベルのブレークアウト ポートは **Ethernet 1/2/1**、**Ethernet 1/2/2**、**Ethernet 1/2/3**、および **Ethernet 1/2/4** として識別される場合があります。

モジュールの 1 つまたは複数の 40G インターフェイスが個別ポート レベルでブレークアウトされる場合、コマンドの実行時にインターフェイスの設定が削除されます。

（注） 個別ポート レベルのブレークアウトでは、モジュールのリロードは不要です。

次に、1 つのブレークアウト ポートを設定する例を示します。

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

次に、複数のブレークアウト ポートを設定する例を示します。

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

no interface breakout コマンドにより、ブレークアウト ポートを取り消すことができます。

次に、ブレークアウト ポートを取り消す例を示します。

```
switch(config)# no interface breakout module 1 port 1 map 10g-4x
switch(config)#
```

レーン セレクタについて

レーン セレクタは、Cisco Nexus スイッチ上にある（前面パネルの左側にあり「LS」というラベルが付いている）押しボタン式のスイッチと 4 つの LED です。この押しボタン式のスイッチと LED は、ポートのステータスを確認するために使用されます。レーン セレクタは、Cisco Nexus 9000 シリーズ スイッチと Cisco Nexus 3164 および 3232 スイッチでサポートされています。

デフォルトでは、この LED によって、1 x 40G 設定のリンク/アクティビティ ステータスが示されます。ポートが 4 x 10G として設定されている場合は、このレーン セレクタを使用して各 10G ポートのリンク ステータスを個別に確認できます。

レーン セレクタの押しボタンを押すと、選択したレーンのリンク/アクティビティ ステータスがポート LED に表示されます。押しボタンを押すと、1 回目には最初の LED に最初のポートのステータスが表示されます。2 回目には 2 番目のポートのステータスが示され、以降同様です。押しボタンをこのように押すことで、4 つのポートのステータスを個別に確認できます。

たとえば、ポート 60 が 4 x 10G として設定されている場合、レーン セレクタの押しボタンを 1 回押すと、60/1/1 のリンク ステータスが表示されます。押しボタンをもう一度押すと、60/1/2 のリンク ステータスが表示されます。

最後のポートのステータスが表示された後に押しボタンを押すと、4 つの LED がすべて消灯します。これは、レーン セレクタがデフォルトの 1 x 40G 設定のステータスを表示する状態に戻ったことを示します。

（注） 10Gブレイクアウト ポートに対してビーコン機能が設定されている場合は、そのポートのLED が点滅します。

（注） ポートが 10G ブレークアウト モードになるように設定されており、レーンが選択されていないときは、いずれかの 10G ブレイクアウト ポートだけが稼働している場合でも、40G ポートの LED が緑色で点灯します。

ブレークアウト インターフェイスに関する注意事項

注意事項

- ブレークアウト ポートをポートチャネルの一部として設定する場合は、そのポートチャネルの有効性を確保するために、設定を 2 回（write-erase/reload の実行後に）適用する必要があります。

高帯域幅インターフェイス

高帯域幅インターフェイスのブレークアウト（モジュール レベルまたは個別ポート レベル）は、次でのみサポートされます。

- Cisco Nexus 9500 シリーズ スイッチの X9636PQ、X9432PQ、および X9536PQ ライン カード
- Cisco Nexus 9332PQ スイッチ
- Cisco Nexus 3164Q スイッチ

Cisco Nexus C92160YC スイッチ

7.0(3)I3(1) 以降、Cisco Nexus C92160YC スイッチは、2 つの異なる動作モードを提供しています。

- モード 1：48 X 10G/25G + 4 X 40G + 2 X 100G（デフォルト設定）
  - ハードウェア プロファイル ポートモード 48x25G + 2x100G + 4x40G
  - ブレークアウトは 2 つの 100G ポートでサポート
- モード 2：48 X 10G/25G + 4 X 100G
  - ハードウェア プロファイル ポートモード 48x25G + 4x100G
  - ブレークアウトは 4 つの 100G ポートでサポート

現在の動作モードを表示するには、**show running-config | grep portmode** コマンドを使用します。

例：

```
switch(config-if-range)# show running-config | grep portmode
hardware profile portmode 48x25G+2x100G+4x40G
```

詳細については、Cisco Nexus C92160YC スイッチのインストレーション ガイドを参照してください（Install and Upgrade Guides for Cisco Nexus 9000 Series Switches）。

Cisco Nexus C92160YC スイッチを使用している場合は、2つのブレークアウト モードがあります。

- 40G から 4 X 10G へのブレークアウト ポート
  - 40G ポートから 4 X 10G ポートへのブレークアウトを有効にします。
  - **interface breakout module 1 port*x*map 10g-4x** コマンドを使用します。
- 100G から 4 X 25G へのブレークアウト ポート
  - 100G ポートから 4 X 25G ポートへのブレークアウトを有効にします。
  - **interface breakout module 1 port*x*map 25g-4x** コマンドを使用します。

Cisco Nexus C9272Q スイッチ

7.0(3)I3(1) 以降、Cisco Nexus C9272Q スイッチは、72 の 40G ポートを提供しています。ポート 37 ~ 71 は、ブレークアウト インターフェイスをサポートしています。

ブレークアウト インターフェイスを設定するには、**interface breakout module 1 port*x*map 10g-4x** コマンドを使用します。

例：

```
switch(config)# interface breakout module 1 port 38 map 10g-4x
switch(config)# show interface ethernet 1/38 capabilities | grep -i break

      Breakout capable:      yes
```

Cisco Nexus C9332PQ スイッチ

7.0(3)I3(1) 以降、Cisco Nexus C9332PQ スイッチは、ブレークアウト モードをサポートし、FEX の 4 つの 10G NIF ポートに接続できる、24 の 40G ポートを提供しています。ポート 1 ~ 12 とポート 15 ~ 26 がサポートされています（ポート 13 および 14 は予約されており、ブレークアウト モードには使用できません）。

（注） すべての FEX がサポートされています。

（注） Cisco Nexus 9332PQ スイッチだけが、FEX ファブリック インターフェイスのインターフェイス ブレークアウト サポートを提供しています（7.0(3)I3(1) 以降）。

仮想デバイス コンテキスト

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

インターフェイスのハイ アベイラビリティ

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

第 3 章

基本インターフェイス パラメータの設定

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

基本インターフェイス パラメータについて

説明

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

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

ビーコン

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

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

エラー ディセーブル化

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

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

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

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

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

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

インターフェイス ステータス エラー ポリシー

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

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

いように情報が保存されます。このプロセスにより、システムに不要な中断が生じるのを避けることができます。

ポート MTU サイズ

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

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

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

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

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

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

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

帯域幅

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

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

スループット遅延

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

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

Administrative Status

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

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

UDLD パラメータ

UDLD の概要

シスコ独自の単方向リンク検出（UDLD）プロトコルにより、光ファイバまたは銅線（カテゴリ 5 ケーブルなど）イーサネット ケーブルを使用して接続されたデバイスで、ケーブルの物理構成をモニタし、単一方向リンクの存在を検出することができます。デバイスで単一方向リンクが検出されると、UDLDが関係のあるLANポートをシャットダウンし、ユーザに通知します。単一方向リンクは、さまざまな問題を引き起こす可能性があります。

UDLD は、ネイバーの ID の検知、誤って接続された LAN ポートのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 の検出が動作して、物理的な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。対になったファイバ ケーブルのうち一方の接続が切断された場合、自動ネゴシエーションがアクティブである限り、そのリンクはアップ状態が維持されなくなります。この場合、論理リンクは不定であり、UDLD は何の処理も行いません。レイヤ 1 で両方のファイバが

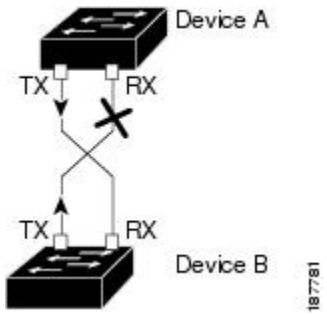
正常に動作していれば、UDLD はそれらのファイバが正しく接続しているかどうか、また、トラフィックが適切なネイバー間で双方向に流れているかどうかを判別します。自動ネゴシエーションはレイヤ 1 で動作するため、このチェックは、自動ネゴシエーションでは実行できません。

Cisco Nexus 9000 シリーズのデバイスは、UDLD をイネーブルにした LAN ポート上のネイバー デバイスに定期的に UDLD フレームを送信します。一定の時間内にフレームがエコーバックされてきて、特定の確認応答（echo）が見つからなければ、そのリンクは単一方向のフラグが立てられ、そのLANポートはシャットダウンされます。UDLDプロトコルにより単方向リンクが正しく識別されその使用が禁止されるようにするためには、リンクの両端のデバイスでUDLDがサポートされている必要があります。UDLDフレームの送信間隔は、グローバル単位でも指定されたインターフェイスにも設定できます。

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

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

図 *1*：単方向リンク



UDLD のデフォルト設定

次の表に、UDLD のデフォルト設定を示します。

表 *3*：*UDLD* のデフォルト設定

機能	デフォルト値
UDLD グローバル イネーブル ステート	グローバルにディセーブル
ポート別のUDLDイネーブル ステート（光ファイバ メディア用）	すべてのイーサネット光ファイバ LAN ポートでイネーブル

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

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

UDLD アグレッシブ モードと非アグレッシブ モード

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

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

リンクの一方にポート スタックが生じる（送受信どちらも）

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

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

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

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

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

ポート チャネル パラメータ

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

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

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

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

ポート プロファイル

7.0(3)I4(1) 以降、Cisco Nexus 9300 シリーズ スイッチでは、たくさんのインターフェイス コマンドを含むポートプロファイルを作成して、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適用できます。ポート プロファイルはそれぞれ特定のタイプのインターフェイスにだけ適用できます。次のインターフェイスから選択できます。

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

インターフェイス タイプにイーサネットまたはポート チャネルを選択する場合、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 つのレベルの継承がサポートされています。任意の数のポート プロファイルで同じポート プロファイルを継承できます。

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。

（注） Session Manager にポート プロファイルは使用できません。Session Manager の詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。

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

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

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

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

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

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

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

Cisco QSFP+ to SFP+ アダプタ モジュールのサポート

Cisco QSFP+ to SFP+ アダプタ（QSA）モジュールは、特定の Cisco Nexus 9300 デバイスの Cisco Nexus M6PQ および Cisco Nexus M12PQ アップリンク モジュールの一部である 40G アップリンク ポートに 10G サポートを提供します。

M6PQ または M12PQ アップリンク モジュールの 6 つの連続するポートは、QSA/QSFP モジュールを使用するために同じ速度（40G または 10G）で稼動している必要があります。

- Cisco Nexus 9396PX デバイスでは、2/1-6 ポートは最初のポート速度グループを形成し、残りの 2/7-12 ポートが 2 番目のポート速度グループを形成します。
- Cisco Nexus 93128PX/TX デバイスでは、2/1-6 ポートは最初のポート速度グループを形成し、残りの 2/7-8 ポートが 2 番目のポート速度グループを形成します。
- Cisco Nexus 937xPX/TX デバイスでは、1/49-54 ポートがただ 1 つのポート速度グループを形成します。

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

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

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

（注） Cisco QSFP+ to SFP+ アダプタ（QSA）モジュールは、Cisco Nexus 9500 デバイス用の 40G ライン カードに対して 10G のサポートを提供しません。

Cisco SFP+ アダプタ モジュールのサポート

Cisco NX-OS Release 7.0(3)I4(2) 以降では、Cisco Nexus 9236C スイッチの 100 ギガビット ポートで 25 ギガビット光ファイバをサポートするために、CVR-2QSFP28-8SFP アダプタを使用できます。

このスイッチの 100G インターフェイスを 4 つの 25G インターフェイスに分割するには、**interface breakout module** コマンドを使用します。このコマンドを入力した後に、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する必要があります。

ライセンス要件

次の表に、この機能のライセンス要件を示します。

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

注意事項と制約事項

基本インターフェイス パラメータの設定には次の注意事項と制約事項があります。

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

  デフォルトでは、どのポートもレイヤ 3 インターフェイスです。

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

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

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

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

- QSFP-40G-CR4 ケーブルを使用して N9K-C9332PQ 非 ALE ポートと N9K-C9372PX ALE ポートを接続する場合は、速度を 40000 に手動で設定する必要があります。
- Base-T銅線ポートの場合は、固定速度が設定されていても、自動ネゴシエーションがイネーブルになります。
- 7.0(3)I2(1) 以降では、**regex** コマンド オプションにより、正規表現を使用した一連のインターフェイスのアドレス指定がサポートされています。**regex** コマンド オプションは、すべてのインターフェイス コマンドで使用できる拡張機能です。

例：

```
switch(config-if-range)# interface ethernet regex [2]/
switch(config-if-range)# where
  conf; interface Ethernet2/1-8      admin@switch%default
switch(config-if-range)# interface ethernet regex [1]/2[2-4]
switch(config-if-range)# where
  conf; interface Ethernet1/22-24      admin@switch%default
```

- 7.0(3)I2(1) 以降では、source-interface コマンド オプションにより、管理アプリケーションが copy コマンドおよびその他のプロセス（tacacs、ntp、ping/ping6、icmp-error、traceroute など）のために IPv4 や IPv6 のインバンドまたはアウトバンド送信元 IP アドレスを設定することがサポートされています。

  - コンフィギュレーション コマンド

    ip*services***source-interface***interface***vrf***vrf name***

    例：

    - `ip ftp source-interface ethernet 8/1 vrf management`
    - `ip http source-interface loopback 1 vrf blue`
    - `ip ssh source-interface ethernet ethernet 5/1`
      `/*This command executes in the VRF context.*/`
    - `ip ping source-interface ethernet 8/1 vrf blue`
    - `ip traceroute source-interface ethernet 8/1 vrf red`
    - `ip icmp-errors source-interface ethernet 8/1`
      `/*This command executes in the VRF context.*/`

  - show コマンド：

    show ip copy*services***source-interface***interface***vrf***vrf name***

    - `show ip ftp source-interface ethernet 8/1 vrf management`
    - `show ip http source-interface loopback 1 vrf blue`
    - `show ip ssh source-interface ethernet ethernet 5/1`
      `/*This command executes in the VRF context.*/`
    - `show ip ping source-interface ethernet 8/1 vrf blue`
    - `show ip traceroute source-interface ethernet 8/1 vrf red`
    - `show ip icmp-errors source-interface ethernet 8/1`
      `/*This command executes in the VRF context.*/`

  - service コマンド：

    copy*service*://username@hostname/*path***filesource-interface***interface name*

    例：

- copy ftp://username@hostname/usr/local/bin file source-interface ethernet 8/1
- copy scp://username@hostname/usr/local/bin file source-interface ethernet 8/1
- copy tftp://username@hostname/usr/local/bin file source-interface ethernet 8/1
- copy http://username@hostname/usr/local/bin file source-interface ethernet 8/1
- copy sftp://username@hostname/usr/local/bin file source-interface ethernet 8/1

- ポート プロファイルは Cisco Nexus 9500 スイッチではサポートされていません（7.0(3)I4(1) 以降）。

デフォルト設定

次の表に、基本インターフェイス パラメータのデフォルト設定を示します。

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

パラメータ	デフォルト
エラー ディセーブル回復間隔	300 秒
バッファ ブースト	イネーブル （注） N9K-X9564TX および N9K-X9564PX ライン カードおよび Cisco Nexus 9300 シリーズ デバイスで使用可能な機能。

基本インターフェイス パラメータの設定

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

設定するインターフェイスの指定

はじめる前に

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

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

表 *4*：設定するインターフェイスの識別に必要な情報

Interface Type	Identity
イーサネット	I/O モジュールのスロット番号およびモジュールのポート番号
管理	0（ポート 0）

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

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

次に、連続しているインターフェイス範囲の設定例を示します。

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

次に、不連続なインターフェイス範囲の設定例を示します。

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

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

次の例は、ブレークアウト ケーブルを設定する方法を示しています。

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

手順の概要

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

手順の詳細

	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***interface*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
	
	例：
	`switch(config)# interface mgmt0`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス タイプと ID を指定できます。イーサネット ポートの場合は、**ethernet***slot/port* を使用します。管理インターフェイスの場合は、**mgmt0** を使用します。
		例：
		• 最初の例は、スロット 2、ポート 1 イーサネット インターフェイスの指定する方法を示します。
		• 2 つ目の例は、管理インターフェイスを指定する方法を示します。
		（注） インターフェイス タイプと ID（ポートまたはスロット/ポート番号）の間にスペースを追加する必要はありません。たとえば、イーサネット スロット 4、ポート 5 インターフェイスの場合は、「ethernet 4/5」または「ethernet4/5」と指定できます。管理インターフェイスは「mgmt0」または「mgmt 0」となります。
		インターフェイス コンフィギュレーション モードの場合、コマンドを入力するとこのモードに指定したインターフェイスが設定されます。

説明の設定

イーサネットおよび管理インターフェイスの説明を文字で設定します。

手順の概要

1. **configure terminal**
2. **interface***interface*
3. **description***text*
4. **show interface***interface*
5. **exit**
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***interface*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
	
	例：
	`switch(config)# interface mgmt0`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス タイプと ID を指定できます。イーサネット ポートの場合は、**ethernet***slot/port* を使用します。管理インターフェイスの場合は、**mgmt0** を使用します。
		例：
		• 最初の例は、スロット 2、ポート 1 イーサネット インターフェイスの指定する方法を示します。
		• 2 つ目の例は、管理インターフェイスを指定する方法を示します。

ステップ 3	**description***text*
	
	例：
	`switch(config-if)# description Ethernet port 3 on module 1`
	`switch(config-if)#`
		インターフェイスの説明を指定します。

	コマンドまたはアクション	目的
ステップ 4	**show interface***interface* 例： `switch(config)# show interface ethernet 2/1`	（任意）インターフェイス ステータスを表示します。説明パラメータもあわせて表示します。

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

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

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

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

ビーコン モードの設定

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

手順の概要

1. **configure terminal**
2. **interface ethernet***slot/port*
3. [**no**] **beacon**
4. **show interface ethernet***slot/port*
5. **exit**
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 ethernet***slot/port*
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	[**no**] **beacon**
	
	例：
	`switch(config)# beacon`
	`switch(config-if)#`
		ビーコン モードをイネーブルにします。またはビーコン モードをディセーブルにします。デフォルト モードはディセーブルです。

ステップ 4	**show interface ethernet***slot/port*
	
	例：
	`switch(config)# show interface ethernet 2/1`
	`switch(config-if)#`
		（任意）ビーコン モード ステートなど、インターフェイスのステータスを表示します。

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

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

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

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

```
switch# configure terminal
switch(config)# interface ethernet 4/17, ethernet 4/19, ethernet 4/21, ethernet 4/23
switch(config-if)# shutdown
switch(config-if)# interface ethernet 4/17
switch(config-if)# no shutdown
switch(config-if)#
```

Error-Disabled ステートの設定

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

Error-Disable 検出のイネーブル化

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

手順の概要

1. **configure terminal**
2. **errdisable detect cause** {**acl-exception** | **all** | **link-flap** | **loopback**}
3. シャットダウン
4. **no shutdown**
5. **show interface status err-disabled**
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。

	コマンドまたはアクション	目的

ステップ 2	**errdisable detect cause** {**acl-exception** | **all** | **link-flap** | **loopback**}
	
	例：
	`switch(config)# errdisable detect cause all`
	`switch(config-if)#`
		インターフェイスを error-disabled ステートにする条件を指定します。デフォルトではイネーブルになっています。

ステップ 3	シャットダウン
	
	例：
	`switch(config-if)# shutdown`
	`switch(config)#`
		インターフェイスを管理ダウンさせます。インターフェイスを error-disabled ステートから手動で回復させるには、最初にこのコマンドを入力します。

ステップ 4	**no shutdown**
	
	例：
	`switch(config-if)# no shutdown`
	`switch(config)#`
		インターフェイスを管理アップし、error-disabled ステートから手動で回復させるインターフェイスをイネーブルにします。

ステップ 5	**show interface status err-disabled** 例： `switch(config)# show interface status err-disabled`	（任意）error-disabled インターフェイスに関する情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

errdisable ステート回復のイネーブル化

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

手順の概要

1. **configure terminal**
2. **errdisable recovery cause {all | bpduguard | failed-port-state | link-flap | loopback | miscabling | psecure-violation | security-violation | storm-control | udld | vpc-peerlink}**
3. **show interface status err-disabled**
4. **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	**errdisable recovery cause {all | bpduguard | failed-port-state | link-flap | loopback | miscabling | psecure-violation | security-violation | storm-control | udld | vpc-peerlink}**
	
	例：
	`switch(config)# errdisable recovery cause all`
	`switch(config-if)#`
		インターフェイスが error-disabled ステートから自動的に回復する条件を指定すると、デバイスはインターフェイスを再びアップします。デバイスは 300 秒待機してからリトライします。デフォルトではディセーブルになっています。

ステップ 3	**show interface status err-disabled**
	
	例：
	`switch(config)# show interface status err-disabled`
	`switch(config-if)#`
		（任意）error-disabled インターフェイスに関する情報を表示します。

ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

errdisable ステート回復間隔の設定

error-disabled 回復タイマーの値を設定できます。

手順の概要

1. **configure terminal**
2. **errdisable recovery interval***interval*
3. **show interface status err-disabled**
4. **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	**errdisable recovery interval***interval*
	
	例：
	`switch(config)# errdisable recovery interval 32`
	`switch(config-if)#`
		インターフェイスが error-disabled ステートから回復する間隔を指定します。有効範囲は 30 ～ 65535 秒で、デフォルトは 300 秒です。

ステップ 3	**show interface status err-disabled**
	
	例：
	`switch(config)# show interface status err-disabled`
	`switch(config-if)#`
		（任意）error-disabled インターフェイスに関する情報を表示します。

ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

MTU サイズの設定

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

ト）またはシステム ジャンボ MTU サイズ（デフォルト サイズは 9216 バイト）の MTU を設定できます。

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

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

switchport コマンドを使用して、ポート モードを変更できます。

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

インターフェイス MTU サイズの設定

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

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

レイヤ 2 インターフェイスに別のシステム ジャンボ MTU サイズを使用する必要がある場合は、「システム ジャンボ MTU サイズの設定」の項を参照してください。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot/port*
3. [**switchport** | **no switchport**]
4. **mtu***size*
5. **show interface ethernet***slot/port*
6. **exit**
7. **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。

	コマンドまたはアクション	目的

ステップ 2	**interface ethernet***slot/port*
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		設定するイーサネット インターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	[**switchport** | **no switchport**]
	
	例：
	`switch(config-if)# no switchport`
	`switch(config-if)#`
		レイヤ 3 を使用するように指定します。

ステップ 4	**mtu***size*
	
	例：
	`switch(config-if)# mtu 9216`
	`switch(config-if)#`
		レイヤ 3 インターフェイスでは、576 ～ 9216 の任意の偶数を指定します。

ステップ 5	**show interface ethernet***slot/port* 例： `switch(config)# show interface ethernet 2/1`	（任意）インターフェイス ステータスを表示します。MTU サイズもあわせて表示します。

ステップ 6	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

システム ジャンボ MTU サイズの設定

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

（注） FEX モジュールのジャンボ フレームを設定するには、FEX モジュールで必要な MTU サイズによって FEX ファブリック ポートチャネル インターフェイスを設定します。

手順の概要

1. **configure terminal**
2. **system jumbomtu***size*
3. **show running-config all**
4. **interface***typeslot/port*
5. **mtu***size*
6. **exit**
7. **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	**system jumbomtu***size*
	
	例：
	`switch(config)# system jumbomtu 8000`
	`switch(config)#`
		システム ジャンボ MTU サイズを指定します。1500 ～ 9216 の偶数を使用します。
		（注） 一般的に受け入れられている方法では、ジャンボ フレームは、9000 バイトを超える MTU サイズを持つと見なされます。

ステップ 3	**show running-config all** 例： `switch(config)# show running-config all | include jumbomtu`	（任意）現在の動作設定を表示します。システム ジャンボ MTU サイズもあわせて表示します。

ステップ 4	**interface***typeslot/port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

ステップ 5	**mtu***size*
	
	例：
	`switch(config-if)# mtu 1500`
	`switch(config-if)#`
		レイヤ 2 インターフェイスでは、デフォルト MTU サイズ（1500）または以前指定したシステム ジャンボ MTU サイズを指定します。
		レイヤ 3 インターフェイスでは、576 ～ 9216 の任意の偶数サイズを指定します。

	コマンドまたはアクション	目的

ステップ 6	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

```
switch# configure terminal
switch(config)# system jumbomtu 8000
switch(config)# show running-config
switch(config)# interface ethernet 2/2
switch(config-if)# switchport
switch(config-if)# mtu 1500
switch(config-if)#
```

帯域幅の設定

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

手順の概要

1. **configure terminal**
2. **interface ethernet***slot/port*
3. **bandwidth***kbps*
4. **show interface ethernet***slot/port*
5. **exit**
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 ethernet***slot/port*
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		設定するイーサネットインターフェイスを指定します。インターフェイスコンフィギュレーションモードを開始します。

ステップ 3	**bandwidth***kbps*
	
	例：
	`switch(config-if)# bandwidth 1000000`
	`switch(config-if)#`
		情報用としてのみ 1 ～ 100,000,000 の値を帯域幅に指定します。

ステップ 4	**show interface ethernet***slot/port* 例： `switch(config)# show interface ethernet 2/1`	（任意）インターフェイス ステータスを表示します。帯域幅の値もあわせて表示します。

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

スループット遅延の設定

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

手順の概要

1. **configure terminal**
2. **interface ethernet***slot/port*
3. **delay***value*
4. **show interface ethernet***slot/port*
5. **exit**
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 ethernet***slot/port*
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		設定するイーサネット インターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**delay***value*
	
	例：
	`switch(config-if)# delay 10000`
	`switch(config-if)#`
		遅延時間を 10 マイクロ秒単位で指定します。1 ～ 16777215 の範囲の情報値を 10 マイクロ秒単位で設定できます。

ステップ 4	**show interface ethernet***slot/port*
	
	例：
	`switch(config)# show interface ethernet 3/1`
	`switch(config-if)#`
		（任意）インターフェイス ステータスを表示します。スループット遅延時間もあわせて表示します。

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

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

インターフェイスのシャットダウンおよび再開

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

手順の概要

1. **configure terminal**
2. **interface***interface*
3. シャットダウン
4. **show interface***interface*
5. **no shutdown**
6. **show interface***interface*
7. **exit**
8. **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***interface*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
	
	`switch(config)# interface mgmt0`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス タイプと ID を指定できます。イーサネット ポートの場合は、*ethernet slot/port* を使用します管理インターフェイスの場合は、*mgmt0* を使用します。
		例：
		• 最初の例は、スロット 2、ポート 1 イーサネット インターフェイスの指定する方法を示します。
		• 2つ目の例は、管理インターフェイスを指定する方法を示します。

ステップ 3	シャットダウン
	
	例：
	`switch(config-if)# shutdown`
	`switch(config-if)#`
		インターフェイスをディセーブルにします。

ステップ 4	**show interface***interface*
	
	例：
	`switch(config-if)# show interface ethernet 2/1`
	`switch(config-if)#`
		（任意）インターフェイス ステータスを表示します。管理ステータスもあわせて表示します。

ステップ 5	**no shutdown**
	
	例：
	`switch(config-if)# no shutdown`
	`switch(config-if)#`
		インターフェイスを再びイネーブルにします。

ステップ 6	**show interface***interface*
	
	例：
	`switch(config-if)# show interface ethernet 2/1`
	`switch(config-if)#`
		（任意）インターフェイス ステータスを表示します。管理ステータスもあわせて表示します。

ステップ 7	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

	コマンドまたはアクション	目的
ステップ 8	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

UDLD モードの設定

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

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

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

表 *5*：異なるインターフェイスで *UDLD* をイネーブルおよびディセーブルにする *CLI* 詳細

説明	ファイバ ポート	銅線またはファイバ以外のポート
デフォルト設定	イネーブル	Disabled
enable UDLD コマンド	**no udld disable**	**udld enable**
disable UDLD コマンド	**udld disable**	**no udld enable**

はじめる前に

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

手順の概要

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

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	[**no**] **feature udld**
	
	例：
	`switch(config)# feature udld`
	`switch(config)#`
	`switch(config)# no feature udld`
	`switch(config)#`
		デバイスの UDLD をイネーブル/ディセーブルにします。

ステップ 3	**udld message-time***seconds*
	
	例：
	`switch(config)# udld message-time 30`
	`switch(config)#`
		（任意）UDLD メッセージを送信する間隔を指定します。有効な範囲は 7 ～ 90 秒で、デフォルトは 15 秒です。

ステップ 4	**udld aggressive**
	
	例：
	`switch(config)# udld aggressive`
	`switch(config)#`
		（任意）UDLD モードをアグレッシブに指定します。
		（注） 銅インターフェイスの場合、UDLD アグレッシブ モードに設定するインターフェイスのインターフェイス コマンド モードを入力し、インターフェイス コマンド モードでこのコマンドを発行します。

ステップ 5	**interface ethernet***slot/port*
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		（任意）設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 6	**udld** [**enable** | **disable**]
	
	例：
	`switch(config-if)# udld enable`
	`switch(config-if)#`
		（任意）指定した銅線ポートの UDLD をイネーブルにしたり、指定したファイバ ポートの UDLD をディセーブルにします。
		銅線ポートで UDLD をイネーブルにするには、**udld enable** コマンドを入力します。ファイバ ポートで UDLD をイネーブルにするには、**no udld disable** コマンドを入力します。

ステップ 7	**show udld** [**ethernet***slot/port* | **global** | **neighbors**]
	
	例：
	`switch(config)# show udld`
	`switch(config)#`
		（任意）UDLD のステータスを表示します。

ステップ 8	**exit**
	
	例：
	`switch(config-if-range)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 9	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、デバイスの UDLD をイネーブルにする例を示します。

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

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

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

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

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if-range)# no udld enable
switch(config-if-range)# exit
```

次に、デバイスの UDLD をディセーブルにする例を示します。

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

デバウンス タイマーの設定

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

（注） **link debounce time** コマンドは、物理イーサネット インターフェイスにだけ適用できます。

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

手順の概要

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

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 ethernet***slot/port*
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		設定するイーサネットインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**link debounce time***time*
	
	例：
	`switch(config-if)# link debounce time 1000`
	`switch(config-if)#`
		指定した時間（1 ～ 5,000 ミリ秒）でデバウンス タイマーをイネーブルにします。
		0 ミリ秒を指定すると、デバウンス タイマーがディセーブルになります。

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

```
switch# configure terminal
```

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

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

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

ポート プロファイルの設定

7.0(3)I4(1) では、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。
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	**show port-profile**	（任意） ポート プロファイル設定を表示します。
ステップ 5	**copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

```
switch# configure terminal
switch(config)# port-profile type ethernet test
switch(config-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。
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	**show port-profile**	（任意） ポート プロファイル設定を表示します。
ステップ 5	**copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

次に、イーサネット インターフェイス 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	**show port-profile**	（任意） ポート プロファイル設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

```
switch# configure terminal
switch(config)# port-profile type ethernet test
switch(config-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	**show port-profile**	（任意） ポート プロファイル設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

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

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

次の例は、イーサネット インターフェイス 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	**show port-profile**	（任意） ポート プロファイル設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

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

基本インターフェイス パラメータの確認

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

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

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

インターフェイス カウンタのモニタリング

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

インターフェイス統計情報の表示

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

手順の概要

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

手順の詳細

	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 ether***slot/port*
	
	例：
	`switch(config)# interface ether 4/1`
	`switch(config)#`
		インターフェイスを指定します。

ステップ 3	**load-interval counters** [**1** | **2** | **3**] *seconds*
	
	例：
	`switch(config)# load-interval counters 1 100`
	`switch(config)#`
		ビットレートおよびパケットレートの統計情報を収集する最大 3 つのサンプリング間隔を設定します。各カウンタのデフォルト値は、次のとおりです。
		1：30 秒（VLAN の場合は 60 秒）
		2：300 秒
		3：未設定

ステップ 4	**show interface***interface*
	
	例：
	`switch(config)# show interface ethernet 2/2`
	`switch#`
		（任意）インターフェイス ステータスを表示します。カウンタもあわせて表示します。

ステップ 5	**exit**
	
	例：
	`switch(config-if-range)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

インターフェイス カウンタのクリア

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**clear counters interface** [**all** | **ethernet***slot/port* | **loopback***number* | **mgmt***number* | **port channel***channel-number*]
	
	例：
	`switch# clear counters ethernet 2/1`
	`switch#`
		インターフェイス カウンタをクリアします。

ステップ 2	**show interface***interface*
	
	例：
	`switch# show interface ethernet 2/1`
	`switch#`
		（任意）インターフェイスのステータスを表示します。

ステップ 3	**show interface** [**ethernet***slot/port* | **port channel***channel-number*] **counters**
	
	例：
	`switch# show interface ethernet 2/1 counters`
	`switch#`
		（任意）インターフェイス カウンタを表示します。

次に、イーサネット ポート 5/5 のカウンタをクリアする例を示します。

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

QSA の設定例

Cisco Nexus 9396PX：

- ポート 2/1 のデフォルト設定を使用して、ポート グループ 2/1-6 のすべての QSFP は速度 40G になります。ポート グループ 2/1-6 に QSA モジュールがある場合は、error disabled になります。
- **speed-group** [**10000** | **40000**] コマンドを使用してポート 2/7 を設定し、ポート グループ 2/7-12 内のすべての QSA を 10G または 40G の速度にします。ポート グループ 2/7-12 に QSFP モジュールがある場合は、error disabled になります。

次の例は、Cisco Nexus 9396PX の速度グループの最初のポートに関して QSA を設定する方法を示したものです。

```
switch# conf t
switch(config)# interface ethernet 2/7
switch(config-if)# speed-group 10000
```

第 4 章

レイヤ 2 インターフェイスの設定

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

（注）

レイヤ 2 ポートは、次のいずれかとして機能できます。

- トランク ポート
- アクセス ポート

（注）

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

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

（注）

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

アクセスインターフェイスとトランクインターフェイスについて

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

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

アクセス インターフェイスとトランク インターフェイスについて

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

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

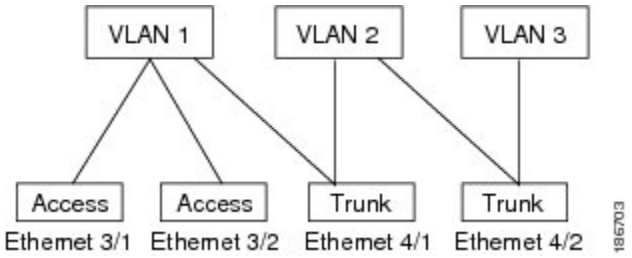
デフォルトでは、デバイスのポートはすべてレイヤ 3 ポートです。

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

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

次の図は、ネットワークにおけるトランク ポートの使い方を示したものです。トランク ポートは、2 つ以上の VLAN のトラフィックを伝送します。

図 *2*：トランクおよびアクセス ポートと *VLAN* トラフィック



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

複数の VLAN に接続するトランク ポートのトラフィックを正しく伝送するために、デバイスは IEEE 802.1Q カプセル化（タギング方式）を使用します（詳細については、「IEEE 802.1Q カプセル化」の項を参照）。

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

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

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

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

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

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

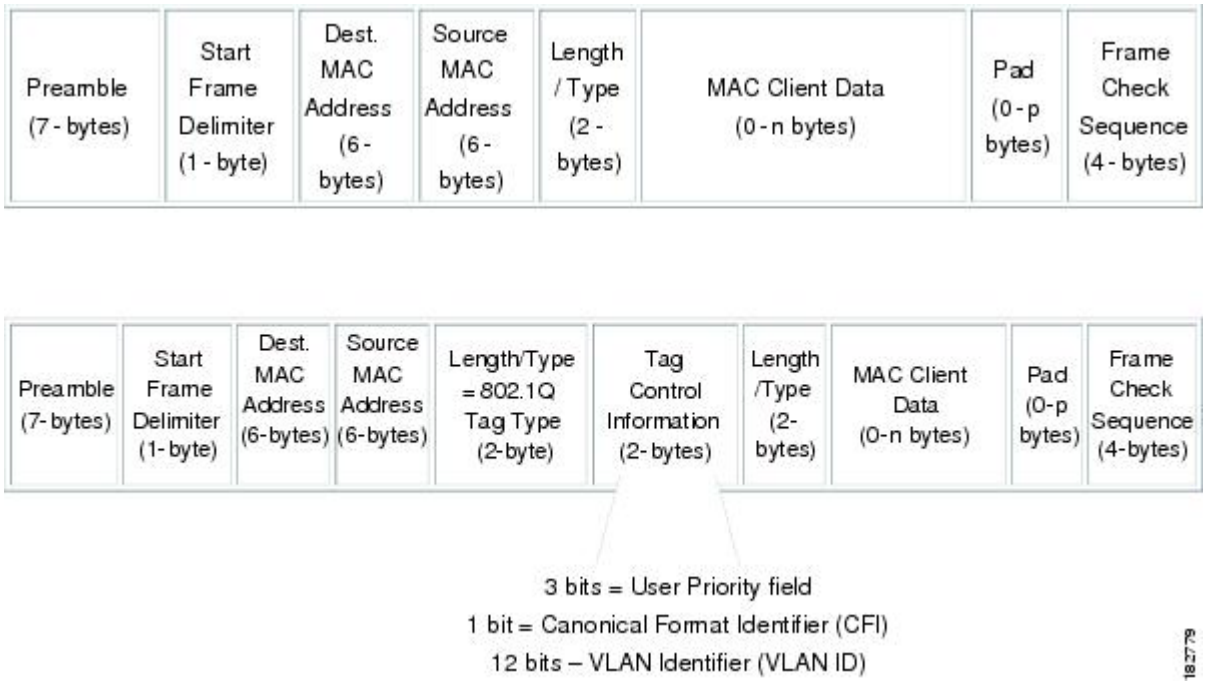
IEEE 802.1Q カプセル化

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

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

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

図 *3*：*802.1Q* タグなしヘッダーと *802.1Q* タグ付きヘッダー



アクセス VLAN

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

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

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

トランク ポートのネイティブ VLAN ID

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

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

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

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

ネイティブ VLAN トラフィックのタギング

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

ただし、デバイスを通過するすべてのパケットに 802.1Q タグがあり、トランクのネイティブ VLAN の値と一致する場合はタギングが取り除かれ、タグなしパケットとしてトランク ポートから出力

されます。トランク ポートのネイティブ VLAN でパケットのタギングを保持したい場合は、この点が問題になります。

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

Allowed VLANs

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

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

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

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

スイッチポートの分離による 4K VLAN 設定の有効化

7.0(3)I4(1) では、スイッチポート分離機能により、インターフェイス上の STP を無効化できます。この機能を使用すると、最大 VLAN 4K X 48 の仮想ポートを使用できます。スイッチポート分離機能を設定すると、そのポートのすべての 4K VLAN がフォワーディング ステートになります（VLAN を削除しても論理ポートはダウンしません）。

この機能は MSTP モードでサポートされています。また、物理インターフェイスおよびポートチャネル（vPC を含む）でもサポートされています。

（注） スイッチポート分離機能は、MSTP モードの 4K VLAN により最大 48 のポートをサポートします。

vPC 設定では、vPC ピア間でタイプ 1 整合性検査が実行されます。検査結果が不整合の場合、セカンダリ vPC はダウンしますが、プライマリ vPC はアップ状態が維持されます。

（注） スイッチポート分離機能を使用している場合は論理ポートがアップまたはダウンしてもスパニング ツリーが通知されません。

デフォルト インターフェイス

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

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

スイッチ仮想インターフェイスおよび自動ステート動作

Cisco NX-OS では、スイッチ仮想インターフェイス（SVI）は、デバイスの VLAN のブリッジング機能とルーティング機能間の論理インターフェイスを表します。

このインターフェイスの動作状態は、その対応する VLAN 内のさまざまなポートの状態によって決まります。VLAN の SVI インターフェイスは、その VLAN 内の少なくとも 1 個のポートがスパニングツリー プロトコル（STP）のフォワーディング ステートにある場合に稼働します。同様に、このインターフェイスは最後の STP 転送ポートがダウンするか、別の STP 状態になったとき、ダウンします。

SVI 自動ステート除外

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

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

SVI 自動ステートのディセーブル化

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

ハイ アベイラビリティ

ソフトウェアは、レイヤ 2 ポートのハイ アベイラビリティをサポートします。

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

仮想化のサポート

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

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（Configuration）	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	ジャンボ、Giant、および入力エラー	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	ジャンボ、Giant、および入力エラー	Dropped

設定（Configuration）	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	ジャンボ、Giant、および入力エラー	Dropped
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	ジャンボ、Giant、および入力エラー	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	ジャンボ、Giant、および入力エラー	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。

レイヤ 2 ポート モードのライセンス要件

次の表に、この機能のライセンス要件を示します。

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

ライセンス 2 インターフェイスの前提条件

ライセンス 2 インターフェイスには次の前提条件があります。

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

レイヤ 2 インターフェイスの注意事項および制約事項

VLAN トランキングには次の設定上の注意事項と制限事項があります。

- **show** コマンドで **internal** キーワードを指定することは、サポートされていません。
- Release 7.0(3)I2(1) 以降、Cisco Nexus 9300 シリーズ スイッチでは、SVI へのユニキャスト ARP 要求は VLAN 内の他のポートにフラッディングされます。
- ポートはレイヤ 2 またはレイヤ 3 インターフェイスのいずれかです。両方が同時に成立することはありません。
- レイヤ 3 ポートをレイヤ 2 ポートに変更する場合またはレイヤ 2 ポートをレイヤ 3 ポートに変更する場合は、レイヤに依存するすべての設定は失われます。アクセスまたはトランク

ポートをレイヤ 3 ポートに変更すると、アクセス VLAN、ネイティブ VLAN、許容 VLAN などの情報はすべて失われます。

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

トはスパニングツリー「ポート不一致」状態になり、トラフィックはポートを通過しません。

- トランク ポートをポートチャネル グループに含めることができますが、そのグループのトランクはすべて同じ設定にする必要があります。グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。パラメータの設定を変更すると、許容VLANやトランク ステータスなど、デバイスのグループのすべてのポートにその設定を伝えます。たとえば、ポート グループのあるポートがトランクになるのを中止すると、すべてのポートがトランクになるのを中止します。
- トランク ポートで 802.1X をイネーブルにしようとすると、エラー メッセージが表示され、802.1Xはイネーブルになりません。802.1x 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
- 入力ユニキャスト パケット カウンタだけが SVI カウンタでサポートされます。
- MAC アドレスが clear mac address-table dynamic コマンドによって VLAN でクリアされると、その VLAN のダイナミック ARP（Address Resolution Protocol）エントリが更新されます。
- VLAN にスタティック ARP エントリがあり、ポート マッピングへの MAC アドレスが存在しない場合、MAC アドレスを学習するためにスーパーバイザによって ARP 要求が生成される可能性があります。MAC アドレスが学習されると、隣接関係により、正しい物理ポートへのポイントがエントリされます。
- Cisco NX-OS は、いずれかの SVI が BIA MAC（Burned-In MAC Address）を使用して Cisco Nexus 9000 上に存在する場合、2 つの VLAN 間のトランスペアレント ブリッジングをサポートしません。これは、SVI/VLAN 間で BIA MAC が共有されるときに発生します。

  SVI ではトランスペアレント ブリッジングを正しく動作させるために BIA MAC とは異なる MAC を設定できます。
- ポート ローカル VLAN は、ファブリック エクステンダ（FEX）をサポートしません。

レイヤ 2 インターフェイスのデフォルト設定

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

表 *6*：デフォルトのアクセスおよびトランク ポート モード パラメータ（*7.0(3)I1(2)* 以前）

パラメータ（Parameters）	デフォルト
スイッチポート モード	アクセス
Allowed VLANs	1 ～ 3967、4048 ～ 4094
アクセス VLAN ID	VLAN1
Native VLAN ID	VLAN1

パラメータ（Parameters）	デフォルト
ネイティブ VLAN ID タギング	ディセーブル
管理状態	閉じる

表 *7*：デフォルトのアクセスおよびトランク ポート モード パラメータ（*7.0(3)I2(1)* 以降）

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

アクセスインターフェイスとトランクインターフェイスの設定

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

アクセスおよびトランク インターフェイスの設定に関する注意事項

トランクのすべての VLAN は同じ VDC であることが必要です。

レイヤ 2 アクセス ポートとしての VLAN インターフェイスの設定

レイヤ 2 ポートをアクセス ポートとして設定できます。アクセス ポートは、パケットを、1 つのタグなし VLAN 上だけで送信します。インターフェイスが伝送する VLAN トラフィックを指定し

ます。これがアクセス VLAN になります。アクセス ポートの VLAN を指定しない場合、そのインターフェイスはデフォルト VLAN のトラフィックだけを伝送します。デフォルトの VLAN は VLAN 1 です。

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

はじめる前に

レイヤ 2 インターフェイスを設定することを確認します。

手順の概要

1. **configure terminal**
2. **interface ethernet** {{*type slot/port*} | {**port-channel***number*}}
3. **switchport mode** [**access** | **trunk**]
4. **switchport access vlan***vlan-id*
5. **exit**
6. **show interface**
7. **no shutdown**
8. **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 ethernet** {{*type slot/port*}	{**port-channel***number*}}
		
		例：
		`switch(config)# interface ethernet 3/1`
		`switch(config-if)#`
			設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**switchport mode** [**access**	**trunk**] 例： `switch(config-if)# switchport mode access`	インターフェイスを、非トランキング、タグなし、シングル VLAN レイヤ 2 インターフェイスとして設定します。アクセス ポートは、1 つの VLAN のトラフィックだけを伝送できます。デフォルトでは、アクセス ポートは VLAN1 のトラフィックを伝送します。異なる VLAN のトラフィックを伝送するようにアクセス ポートを設定するには、**switchport access vlan** コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 4	**switchport access vlan***vlan-id* 例： `switch(config-if)# switchport access vlan 5`	このアクセス ポートでトラフィックを伝送する VLAN を指定します。このコマンドを入力しないと、アクセス ポートは VLAN1 だけのトラフィックを伝送します。このコマンドを使用して、アクセス ポートがトラフィックを伝送する VLAN を変更できます。

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 6	**show interface** 例： `switch# show interface`	（任意）インターフェイスのステータスと内容を表示します。

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

ステップ 8	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

アクセス ホスト ポートの設定

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

端末に接続されたアクセス ポートでのパフォーマンスを最適化するには、そのポートをホスト ポートとしても設定します。アクセス ホスト ポートはエッジ ポートと同様に STP を処理し、ブロッキング ステートおよびラーニング ステートを通過することなくただちにフォワーディング

ステートに移行します。インターフェイスをアクセスホストポートとして設定すると、そのインターフェイス上でポート チャネル動作がディセーブルになります。

（注） ポートチャネル インターフェイスについては、「ポート チャネルの設定」の項および『*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

はじめる前に

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

手順の概要

1. **configure terminal**
2. **interface ethernet***type slot/port*
3. **switchport host**
4. **exit**
5. **show interface**
6. **no shutdown**
7. **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 ethernet***type slot/port*
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**switchport host** 例： switch(config-if)# switchport host	インターフェイスをアクセス ホスト ポートとして設定します。このポートはただちに、スパニングツリーフォワーディング ステートに移行し、このインターフェイスのポート チャネル動作をディセーブルにします。 （注） このコマンドは端末だけに適用します。

	コマンドまたはアクション	目的

ステップ 4	**exit**
	
	例：
	`switch(config-if-range)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 5	**show interface** 例： `switch# show interface`	（任意）インターフェイスのステータスと内容を表示します。

ステップ 6	**no shutdown**
	
	例：
	`switch# configure terminal`
	`switch(config)# int e3/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

トランク ポートの設定

レイヤ 2 ポートをトランク ポートとして設定できます。トランク ポートは、1 つの VLAN の非タグ付きパケットと、複数の VLAN のカプセル化されたタグ付きパケットを伝送します（カプセル化については、「IEEE 802.1Q カプセル化」の項を参照）。

（注） デバイスは 802.1Q カプセル化だけをサポートします。

はじめる前に

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

手順の概要

1. **configure terminal**
2. **interface** {*type slot/port* | **port-channel***number*}
3. **switchport mode** [**access** | **trunk**]
4. **exit**
5. **show interface**
6. **no shutdown**
7. **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** {*type slot/port* | **port-channel***number*}
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**switchport mode** [**access** | **trunk**] 例： `switch(config-if)# switchport mode trunk`	インターフェイスをレイヤ 2 トランク ポートとして設定します。トランク ポートは、同じ物理リンクで 1 つ以上の VLAN 内のトラフィックを伝送できます（各 VLAN はトランキングが許可された VLAN リストに基づいています）。デフォルトでは、トランク インターフェイスはすべての VLAN のトラフィックを伝送できます。指定したトランクで特定の VLAN のみが許可されるように指定するには、**switchport trunk allowed vlan** コマンドを使用します。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 5	**show interface** 例： `switch# show interface`	（任意）インターフェイスのステータスと内容を表示します。

	コマンドまたはアクション	目的

ステップ 6	**no shutdown**
	
	例：
	`switch# configure terminal`
	`switch(config)# int e3/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

802.1Q トランク ポートのネイティブ VLAN の設定

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

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

手順の概要

1. **configure terminal**
2. **interface** {{*type slot/port*} | {**port-channel***number*}}
3. **switchport trunk native vlan***vlan-id*
4. **exit**
5. **show vlan**
6. **no shutdown**
7. **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** {{*type slot/port*} | {**port-channel***number*}}
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**switchport trunk native vlan***vlan-id* 例： `switch(config-if)# switchport trunk native vlan 5`	802.1Q トランクのネイティブ VLAN を設定します。指定できる範囲は 1 ～ 4094 です（ただし、内部使用に予約されている VLAN は除きます）。デフォルト値は VLAN 1 です。

ステップ 4	**exit**
	
	例：
	`switch(config-if-range)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	**show vlan** 例： `switch# show vlan`	（任意）VLAN のステータスと内容を表示します。

ステップ 6	**no shutdown**
	
	例：
	`switch# configure terminal`
	`switch(config)# int e3/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、ネイティブ VLAN をイーサネット 3/1 に設定し、レイヤ 2 トランク ポートを VLAN5 に設定する例を示します。

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

```
switch(config-if)# switchport trunk native vlan 5
switch(config-if)#
```

トランキング ポートの許可 VLAN の設定

特定のトランク ポートで許可されている VLAN の ID を指定できます。

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

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

はじめる前に

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

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

手順の概要

1. **configure terminal**
2. **interface** {**ethernet***slot/port* | **port-channel***number*}
3. **switchport trunk allowed vlan** {*vlan-list***add***vlan-list* | **all** | **except***vlan-list* | **none** | **remove***vlan-list*}
4. **exit**
5. **show vlan**
6. **no shutdown**
7. **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。

	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***number*} 例： `switch(config)# interface ethernet 3/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport trunk allowed vlan** {*vlan-list***add***vlan-list* | **all** | **except***vlan-list* | **none** | **remove***vlan-list*} 例： `switch(config-if)# switchport trunk allowed vlan add 15-20#`	トランク インターフェイスの許可 VLAN を設定します。デフォルトでは、トランク インターフェイス上のすべての VLAN（1 ～ 3967 および 4048 ～ 4094）が許可されます。VLAN 3968 ～ 4047 は、内部で使用するデフォルトで予約されている VLAN です。デフォルトでは、すべてのトランク インターフェイスですべての VLAN が許可されます。 デフォルトの予約済み VLAN は 3968 ～ 4094 で、予約 VLAN のブロックを変更できます。詳細については、『*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。 （注） 内部で割り当て済みの VLAN を、トランク ポート上の許可 VLAN として追加することはできません。内部で割り当て済みの VLAN を、トランク ポートの許可 VLAN として登録しようとすると、メッセージが返されます。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 5	**show vlan** 例： `switch# show vlan`	（任意）VLAN のステータスと内容を表示します。

ステップ 6	**no shutdown**
	
	例：
	`switch# configure terminal`
	`switch(config)# int e3/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

スイッチポート分離の設定

7.0(3)I2(1) では、スイッチポート分離機能がサポートされています。

（注） スイッチポート分離機能は、FEX インターフェイスまたはポートチャネル メンバーをサポートしていません。

（注） ポートチャネルでは、異なるスイッチポート分離設定を持つ物理インターフェイスは許可されません。

手順の概要

1. **configure terminal**
2. **interface** {{**ethernet***slot/port*} | {**port-channel***number*}}
3. **switchport isolated**
4. **show running-config interface port-channel***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** {{**ethernet***slot/port*}	{**port-channel***number*}}
		
		例：
		`switch(config)# interface ethernet 3/1`
		`switch(config-if)#`
			設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**switchport isolated** 例： `switch(config-if)# switchport isolated`	スイッチポート分離機能を有効にします。

	コマンドまたはアクション	目的
ステップ 4	**show running-config interface port-channel***port-channel-number*	（任意）インターフェイスのステータスと内容を表示します。

デフォルト インターフェイスの設定

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

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

手順の概要

1. **configure terminal**
2. **default interface***int-if* [**checkpoint***name*]
3. **exit**
4. **show interface**
5. **no shutdown**

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	**default interface***int-if* [**checkpoint***name*] 例： `switch(config)# default interface ethernet 3/1 checkpoint test8`	インターフェイスの設定を削除しデフォルトの設定を復元します。**?**キーワードを使用して、サポートされるインターフェイスを表示します。 **checkpoint** キーワードを使用して、設定を消去する前にインターフェイスの実行コンフィギュレーションのコピーを保存します。

	コマンドまたはアクション	目的

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch(config)#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show interface** 例： `switch# show interface`	（任意）インターフェイスのステータスと内容を表示します。

ステップ 5	**no shutdown**
	
	例：
	`switch# configure terminal`
	`switch(config)# int e3/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

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

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

SVI 自動ステート除外の設定

7.0(3)I2(1) 以降では、イーサネット インターフェイスまたはポート チャネルに SVI 自動ステート除外機能を設定できます。自動ステート除外オプションを使用して、ポートが SVI 計算を稼働または停止したり、それを選択したポートでイネーブルのすべての VLAN に適用するのをイネーブルまたはディセーブルにすることができます。また、SVI 自動ステート除外 VLAN 機能を使用して、VLAN を自動ステート除外インターフェイスから除外することができます。

手順の概要

1. **configure terminal**
2. **interface** {{*type slot/port*} | {**port-channel***number*}}
3. **switchport**
4. [**no**] **switchport autostate exclude**
5. [**no**] **switchport autostate exclude vlan** {*vlan id* | **all** | **except}**
6. **exit**
7. **show running-config interface** {{*type slot/port*} | {**port-channel***number*}}
8. **no shutdown**
9. **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** {{*type slot/port*} | {**port-channel***number*}}
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**switchport** 例： `switch(config-if)# switchport`	インターフェイスをレイヤ 2 インターフェイスとして設定します。
ステップ 4	[**no**] **switchport autostate exclude** 例： `switch(config-if)# switchport autostate exclude`	VLANに複数のポートがあるときに、VLANインターフェイスのリンクアップ計算からポートを除外します。 デフォルト設定に戻すには、このコマンドのno形式を使用します。
ステップ 5	[**no**] **switchport autostate exclude vlan** {*vlan id* | **all** | **except}** 例： `switch(config-if)# switchport autostate exclude vlan 10`	（任意）自動ステート除外インターフェイスから vlan または vlan のセットを除外します。これにより、システムの中断を最小限に抑えることができます。 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 6	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 7	**show running-config interface** {{*type slot/port*} | {**port-channel***number*}} 例： `switch(config)# show running-config interface ethernet 3/1`	（任意）指定されたインターフェイスに関する設定情報を表示します。

ステップ 8	**no shutdown**
	
	例：
	`switch# configure terminal`
	`switch(config)# int e3/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよびVLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

	コマンドまたはアクション	目的
ステップ 9	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

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

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

次に、自動除外インターフェイスから VLAN を除外する例を示します。

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

システムの SVI 自動ステートのディセーブル化の設定

SVI 自動ステート機能によって SVI を管理できます。SVI 自動ステートのディセーブル化機能を設定して、対応する VLAN 内にアップ状態のインターフェイスがない場合でも SVI をアップ状態に保持することができます。（同様に、SVI 自動ステートのイネーブル化機能を設定すると、対応する VLAN 内にアップ状態のインターフェイスがない場合に SVI がダウン状態になります）。システム全体にこの機能を設定するには、次の手順を使用します。

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

手順の概要

1. **configure terminal**
2. **[no] system default interface-vlan autostate**
3. **no shutdown**
4. **show running-config [all]**

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	[**no**] **system default interface-vlan autostate** 例： `switch(config)# no system default interface-vlan autostate`	デバイスに対するデフォルトの自動ステート動作をディセーブルにします。 （注） デバイスの自動ステート動作をイネーブルにするには、**system default interface-vlan autostate** コマンドを使用します。

ステップ 3	**no shutdown**
	
	例：
	`switch# configure terminal`
	`switch(config)# int e3/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 4	**show running-config** [**all**] 例： `switch(config)# show running-config`	（任意）実行コンフィギュレーションを表示します。 デフォルト情報および設定情報を表示するには、**all** キーワードを使用します。

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

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

SVI 単位の SVI 自動ステートのディセーブル化の設定

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

手順の概要

1. **configure terminal**
2. **feature interface-vlan**
3. **interface vlan***vlan-id*
4. [**no**] **autostate**
5. **exit**
6. **show running-config interface vlan***vlan-id*
7. **no shutdown**
8. **show startup-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	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**feature interface-vlan** 例： `switch(config)# feature interface-vlan`	VLAN インターフェイス モードをイネーブルにします。

ステップ 3	**interface vlan***vlan-id*
	
	例：
	`switch(config-if)# interface vlan10`
	
	`switch(config)#`
		VLAN インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。範囲は、1 ～ 4094 です。

ステップ 4	[**no**] **autostate** 例： `switch(config-if)# no autostate`	デフォルトでは、指定されたインターフェイスの SVI 自動ステート機能をイネーブルにします。 デフォルト設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 6	**show running-config interface vlan***vlan-id* 例： `switch(config)# show running-config interface vlan10`	（任意）特定の VLAN インターフェイスの実行コンフィギュレーションを表示します。

	コマンドまたはアクション	目的

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

ステップ 8	**show startup-config interface vlan***vlan-id* 例： `switch(config)# show startup-config interface vlan10`	（任意）スタートアップ コンフィギュレーションの VLAN 設定を表示します。

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

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

ネイティブ VLAN トラフィックにタグを付けるためのデバイス設定

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

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

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

手順の概要

1. **configure terminal**
2. **vlan dot1q tag native**
3. **exit**
4. **show vlan**
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	**vlan dot1q tag native** 例： `switch(config)# vlan dot1q tag native`	802.1Q トランキング ネイティブ VLAN ID インターフェイスの動作を変更します。このインターフェイスは、ネイティブ VLAN ID の値と一致して、すべての非タグ付きトラフィックをドロップするタグを使って入るすべてのパケットのタギングを維持します。この場合も、制御トラフィックはネイティブ VLAN を通過します。デフォルトではディセーブルになっています。

ステップ 3	**exit**
	
	例：
	`switch(config-if-range)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 4	**show vlan** 例： `switch# show vlan`	（任意）VLAN のステータスと内容を表示します。

ステップ 5	**no shutdown**
	
	例：
	`switch# configure terminal`
	`switch(config)# int e3/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

システムのデフォルト ポート モードをレイヤ 2 に変更

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

手順の概要

1. **configure terminal**
2. **system default switchport** [**shutdown**]
3. **exit**
4. **show interface brief**
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	**system default switchport** [**shutdown**] 例： switch(config-if)# system default switchport	システムのすべてのインターフェイスに対するデフォルトのポート モードをレイヤ 2 アクセス ポート モードに設定し、インターフェイス コンフィギュレーション モードを開始します。デフォルトでは、すべてのインターフェイスがレイヤ 3 です。 （注） **system default switchport shutdown** コマンドが発行されると、次のようになります。 • **no shutdown** で設定されていない FEX HIF はシャットダウンされます。シャットダウンを回避するには、**no shut** で FEX HIF を設定します。 • **no shutdown** で明示的に設定されていないレイヤ 2 ポートはシャットダウンされます。シャットダウンを回避するには、**no shut** でレイヤ 2 ポートを設定します。

ステップ 3	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 4	**show interface brief** 例： `switch# show interface brief`	（任意）インターフェイスのステータスと内容を表示します。

ステップ 5	**no shutdown**
	
	例：
	`switch# configure terminal`
	`switch(config)# int e3/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

インターフェイス コンフィギュレーションの確認

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

コマンド	目的
show interface ethernet*slot/port* [**brief** | | **counters** | **debounce** | **description** | **flowcontrol** | **mac-address** | **status** | **transceiver**]	インターフェイスの設定を表示します。
show interface brief	インターフェイス設定情報を、モードも含めて表示します。
show interface switchport	アクセスおよびトランクインターフェイスも含めて、すべてのレイヤ2インターフェイスの情報を表示します。
show interface trunk [**module***module-number* | **vlan***vlan-id*]	トランク設定情報を表示します。

コマンド	目的
show interface capabilities	インターフェイスの機能に関する情報を表示します。
show running-config [**all**]	現在の設定に関する情報を表示します。 **all** コマンドを使用すると、デフォルトの設定と現在の設定が表示されます。
show running-config interface ethernet*slot/port*	指定されたインターフェイスに関する設定情報を表示します。
show running-config interface port-channel*slot/port*	指定されたポートチャネルインターフェイスに関するコンフィギュレーション情報を表示します。
show running-config interface vlan*vlan-id*	指定された VLAN インターフェイスに関するコンフィギュレーション情報を表示します。

レイヤ 2 インターフェイスのモニタリング

レイヤ 2 インターフェイスを表示するには、次のコマンドを使用します。

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

アクセス ポートおよびトランク ポートの設定例

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

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

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

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

関連資料

関連資料	マニュアル タイトル
レイヤ 3 インターフェイスの設定	「レイヤ 2 インターフェイスの設定」の項
ポート チャネル	「ポート チャネルの設定」の項
VLAN、プライベート VLAN、STP	『*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*』
システム管理	『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』
ハイ アベイラビリティ	『*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*』
ライセンス	『*Cisco NX-OS Licensing Guide*』
リリース ノート	『*Cisco Nexus 9000 Series NX-OS Release Notes*』

関連資料

第 5 章

レイヤ 3 インターフェイスの設定

レイヤ 3 インターフェイスについて

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

ルーテッド インターフェイス

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

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

（注） デフォルトの動作は、スイッチのタイプ（Cisco Nexus 9300、Cisco Nexus 9500、または Cisco Nexus 3164）によって異なります。

（注） Cisco Nexus 9300 シリーズ スイッチ（Cisco Nexus 9332 スイッチを除く）には、レイヤ 2 デフォルト モードがあります。

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

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

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

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

サブインターフェイス

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

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

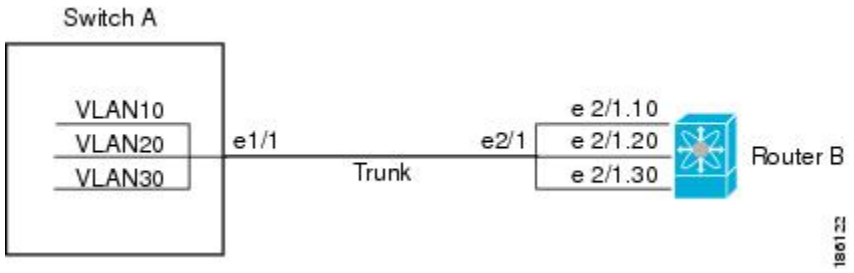
サブインターフェイスの名前は、親インターフェイスの名前（たとえば Ethernet 2/1）+ ピリオド（.）+そのインターフェイス独自の番号です。たとえば、イーサネット インターフェイス 2/1 に Ethernet 2/1.1 というサブインターフェイスを作成できます。この場合、.1 はそのサブインターフェイスを表します。

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

サブインターフェイスを使用すると、親インターフェイスがサポートするそれぞれの仮想ローカル エリア ネットワーク（VLAN）に独自のレイヤ 3 インターフェイスを実現できます。この場合、親インターフェイスは別のデバイスのレイヤ 2 トランキング 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 *4*：*VLAN* のサブインターフェイス



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

サブインターフェイスの制限事項

サブインターフェイスの制限事項は次のとおりです。

- サブインターフェイスの統計情報はサポートされていません。

VLAN Interfaces

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

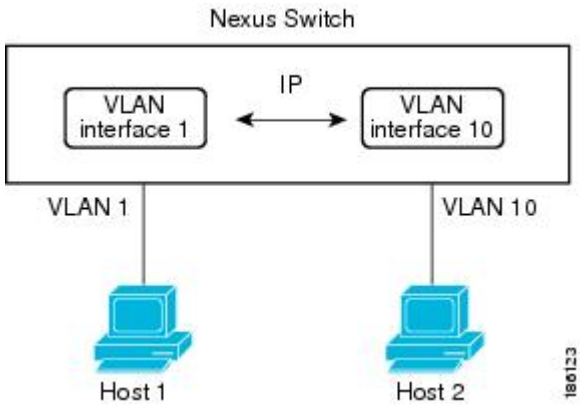
設定の前に VLAN ネットワーク インターフェイス機能をイネーブルにする必要があります。システムはこの機能をディセーブルにする前のチェックポイントを自動的に取得するため、このチェックポイントにロールバックできます。ロールバックとチェックポイントの詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。

（注） VLAN 1 の VLAN インターフェイスは削除できません。

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

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 *5*：*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（7.0(3)I4(1) 以降）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**]、**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 インターフェイスを通過するパケットはこのインターフェイスでただちに受信されます。ループバック インターフェイスは物理インターフェイスをエミュレートします。0 ～ 1023 の番号のループバック インターフェイスを最大 1024 個の設定できます。

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

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。7.0(3)I3(1) 以降、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。

MAC 組み込み IPv6 アドレス

BGP により IPv4 プレフィックスを IPv6 ネクスト ホップで伝送できます。IPv6 ネクスト ホップは、ネットワークからネイバー探索（ND）関連トラフィックを削除するために活用されます。これを行うために（7.0(3)I2(1) 以降）、MAC アドレスが IPv6 アドレスに組み込まれています。このようなアドレスは、MAC 組み込み IPv6（MEv6）アドレスと呼ばれます。ルータは、ND を経由せずに、MEv6 アドレスから MAC アドレスを直接取得します。ローカル インターフェイスおよびネクスト ホップの MAC アドレスは、IPv6 アドレスから取得されます。

MEv6 が有効になっている IPv6 インターフェイスでは、MEv6 から取得される同じ MAC アドレスが IPv4 トラフィックにも使用されます。MEv6 は、スイッチ仮想インターフェイス（SVI）を除くすべてのレイヤ 3 対応インターフェイスでサポートされます。

重要 MEv6 がインターフェイスで有効になっている場合、そのインターフェイスでは IPv6 リンク ローカル アドレス、OSPFv3、および BFDv6 への ping6 はサポートされません。

ハイ アベイラビリティ

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

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

仮想化のサポート

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

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

DHCP Client

7.0(3)I2(1) 以降、Cisco NX-OS は、SVI、物理イーサネット、および管理インターフェイス上の IPv4 アドレスと IPv6 アドレスに関して DHCP クライアントをサポートしています。**ip address dhcp** または **ipv6 address dhcp** コマンドを使用することにより、DHCP クライアントの IP アドレスを設定できます。これらのコマンドにより、DHCP サーバから IPv4 または IPv6 アドレスを得るための要求が DHCP クライアントから DHCP サーバに送信されます。Cisco Nexus スイッチ上の DHCP クライアントは、それ自体を DHCP サーバに識別させます。DHCP サーバは、この ID を使用して、DHCP クライアントに IP アドレスを返信します。

DHCP クライアントが SVI で DHCP サーバ送信ルータおよび DNS オプションによって設定されている場合、スイッチで **ip route** 0.0.0.0/0 *router-ip* コマンドと **ip name-server***dns-ip* コマンドが自動的に設定されます。

インターフェイスでの DHCP クライアントの使用に関する制限事項

次に、インターフェイスでの DHCP クライアントの使用に関する制限事項を示します。

- この機能は、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、および SVI でのみサポートされます。
- この機能は、非デフォルトの Virtual Routing and Forwarding（VRF）インスタンスでサポートされます。
- **copy running-config startup-config** コマンドを入力すると、DNS サーバおよびデフォルト ルータ オプション関連の設定がスタートアップ コンフィギュレーションに保存されます。スイッチをリロードするとき、この設定が適切ではない場合は、この設定を削除しなければならない可能性があります。
- スイッチで設定できる DNS サーバは最大 6 つです。これは、スイッチの制限です。この最大数には、DHCP クライアントによって設定される DNS サーバと手動で設定される DNS サーバが含まれます。

  スイッチで 7 つ以上の DNS サーバが設定されている場合、DNS オプション セットによって SVI の DHCP オファーを取得すると、IP アドレスは SVI に割り当てられません。

- Cisco Nexus 9000 シリーズ スイッチは、最大 10 の IPv4 DHCP クライアントと最大 10 の IPv6 DHCP クライアントをサポートしています（7.0(3)I4(1) 以降）。
- DHCP リレーの設定と DHCP クライアントの設定には互換性がなく、同じスイッチではサポートされません。インターフェイスで DHCP クライアントを設定する前に DHCP リレーの設定を削除する必要があります。
- VLAN で DHCP スヌーピングが有効になっている場合、その VLAN の SVI が DHCP クライアントによって設定されているときは、DHCP スヌーピングが SVI DHCP クライアントで実行されません。
- IPv6 DHCP クライアントを設定する場合は、まず **ipv6 address use-link-local-only** コマンドによって設定する必要があります。その後に、**ipv6 address dhcp** コマンドを使用します。

レイヤ 3 インターフェイスのライセンス要件

次の表に、この機能のライセンス要件を示します。

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

ライセンス 3 インターフェイスの前提条件

ライセンス 3 インターフェイスには次の前提条件があります。

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

注意事項と制約事項

レイヤ 3 インターフェイスの設定には次の注意事項と制約事項があります。

- **show** コマンドで **internal** キーワードを指定することは、サポートされていません。
- ポートチャネルインターフェイスでのサブインターフェイスの設定はサポートされていません。（7.0(3)I1(1)）
- 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。（7.0(3)I1(2) 以降）

- 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。（7.0(3)I1(2) 以降）
- ポートチャネル インターフェイスでサブインターフェイスを設定する場合、Dynamic Host Configuration Protocol（DHCP）オプションはサポートされていません。
- IP アンナンバード インターフェイスが設定されている場合、ループバック インターフェイスは IP アンナンバード インターフェイスと同じ VRF にある必要があります。（7.0(3)I3(1) 以降）
- **admin-shutdown** コマンドをループバック インターフェイスで実行する場合、このループバック インターフェイスがナンバード インターフェイスであるときは、IP アンナンバード インターフェイスはダウンしません。これは、IP アンナンバードインターフェイス経由で動作するルーティング プロトコルがアップ状態を維持することを意味します。（7.0(3)I3(1) 以降）
- IP アンナンバード インターフェイス経由で動作するスタティック ルートは固定されたスタティック ルートを使用する必要があります。（7.0(3)I3(1) 以降）

（注） ルートの解決に使用される IP アンナンバード インターフェイスが指定される必要があります。

- IP アンナンバードインターフェイスは物理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。（7.0(3)I3(1) 以降）
- ループバック インターフェイスだけがアンナンバード インターフェイスをナンバード インターフェイスとして使用できます。（7.0(3)I3(1) 以降）
- IP アンナンバード インターフェイス経由の OSPF がサポートされています。（7.0(3)I3(1) 以降）
- IP アンナンバード インターフェイス経由の ISIS がサポートされています。（7.0(3)I3(1) 以降）
- IP アンナンバード インターフェイスをオーバーレイ インターフェイスとして使用するループバック インターフェイス経由の BGP がサポートされています。（7.0(3)I3(1) 以降）
- IP アンナンバード インターフェイスによってデフォルトと非デフォルトの VRF がサポートされています。（7.0(3)I3(1) 以降）
- スイッチのユーザ定義 MAC アドレス（MEv6/スタティック）は 16 に制限されています。この制限を超えて設定すると、CSCux84428 に記述されている問題が発生する可能性があります。

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

デフォルト設定

次の表に、レイヤ 3 インターフェイス パラメータのデフォルト設定を示します。

表 *8*：レイヤ *3* インターフェイスのデフォルト パラメータ

パラメータ（Parameters）	デフォルト
管理ステート	閉じる

レイヤ 3 インターフェイスの設定

ルーテッド インターフェイスの設定

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

手順の概要

1. **configure terminal**
2. **interface ethernet***slot/port*
3. **no switchport**
4. [**ip address***ip-address/length* | **ipv6 address***ipv6-address/length*]
5. **show interfaces**
6. **no shutdown**
7. **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 ethernet***slot/port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**no switchport** 例： `switch(config-if)# no switchport`	そのインターフェイスを、レイヤ 3 インターフェイスとして設定します。

ステップ 4	[**ip address***ip-address/length* | **ipv6 address***ipv6-address/length*]
	
	例：
	`switch(config-if)# ip address 192.0.2.1/8`
	
	例：
	`switch(config-if)# ipv6 address 2001:0DB8::1/8`
		• このインターフェイスの IP アドレスを設定します。IP アドレスの詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。
		• このインターフェイスの IPv6 アドレスを設定します。IPv6 アドレスの詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

ステップ 5	**show interfaces** 例： `switch(config-if)# show interfaces ethernet 2/1`	（任意）レイヤ 3 インターフェイスの統計情報を表示します。

ステップ 6	**no shutdown**
	
	例：
	`switch#`
	`switch(config-if)# int e2/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーに対応するインターフェイスのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）設定の変更を保存します。

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

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

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

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

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

- 次に、ルーテッド インターフェイスを設定する例を示します。

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

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

ルーテッドインターフェイスでのサブインターフェイスの設定

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

はじめる前に

親インターフェイスをルーテッド インターフェイスとして設定します。

「ルーテッド インターフェイスの設定」の項を参照してください。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot/port.number*
3. [**ip address***ip-address/length* | **ipv6 address***ipv6-address/length*]
4. **encapsulation dot1Q***vlan-id*
5. **show interfaces**
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 ethernet***slot/port.number*
	
	例：
	`switch(config)# interface ethernet 2/1.1`
	`switch(config-subif)#`
		サブインターフェイスを作成し、サブインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	[**ip address***ip-address/length* | **ipv6 address***ipv6-address/length*]
	
	例：
	`switch(config-subif)# ip address 192.0.2.1/8`
	
	例：
	`switch(config-subif)# ipv6 address 2001:0DB8::1/8`
		• このサブインターフェイスの IP アドレスを設定します。IP アドレスの詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。
		• このサブインターフェイスの IPv6 アドレスを設定します。IPv6 アドレスの詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

ステップ 4	**encapsulation dot1Q***vlan-id* 例： `switch(config-subif)# encapsulation dot1Q 33`	サブインターフェイス上の IEEE 802.1Q VLAN カプセル化を設定します。範囲は 2 ～ 4093 です。
ステップ 5	**show interfaces** 例： `switch(config-subif)# show interfaces ethernet 2/1.1`	（任意）レイヤ 3 インターフェイスの統計情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）設定の変更を保存します。

- 次に、サブインターフェイスを作成する例を示します。

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

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

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

ポートチャネル インターフェイスでのサブインターフェイスの設定

ポートチャネル インターフェイスに 1 つまたは複数のサブインターフェイスを設定できます。

（注） ポートチャネル インターフェイス上のサブインターフェイスポートは、マルチキャスト ルーティング、ルータ ACL、QoS、ポリシーベース ルーティング（PBR）、SPAN、または ERSPAN をサポートしません。

はじめる前に

親インターフェイスをポートチャネル インターフェイスとして設定します（7.0(3)I1(2) 以降）。

「ポート チャネルの設定」の章を参照してください。

手順の概要

1. **configure terminal**
2. **interface port-channel***channel-id.number*
3. [**ip address***ip-address/length* | **ipv6 address***ipv6-address/length*]
4. **encapsulation dot1Q***vlan-id*
5. **show interfaces**
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。

	コマンドまたはアクション	目的

ステップ 2	**interface port-channel***channel-id.number*
	
	例：
	`switch(config)# interface port-channel 100.1`
	`switch(config-subif)#`
		サブインターフェイスを作成し、サブインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	[**ip address***ip-address/length* | **ipv6 address***ipv6-address/length*]
	
	例：
	`switch(config-subif)# ip address 192.0.2.1/8`
	
	例：
	`switch(config-subif)# ipv6 address 2001:0DB8::1/8`
		• このサブインターフェイスの IP アドレスを設定します。IP アドレスの詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。
		• このサブインターフェイスの IPv6 アドレスを設定します。IPv6 アドレスの詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

ステップ 4	**encapsulation dot1Q***vlan-id* 例： `switch(config-subif)# encapsulation dot1Q 33`	サブインターフェイス上の IEEE 802.1Q VLAN カプセル化を設定します。範囲は 2 ～ 4093 です。
ステップ 5	**show interfaces** 例： `switch(config-subif)# show interfaces ethernet 2/1.1`	（任意）レイヤ 3 インターフェイスの統計情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）設定の変更を保存します。

次に、サブインターフェイスを作成する例を示します。

```
switch# configure terminal
switch(config)# interface port-channel 115.3
switch(config-subif)# ip address 141.143.101.2/24
switch(config-subif)# encapsulation dot1q 3
switch(config-subif)# copy running-config startup-config
```

VLAN インターフェイスの設定

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

手順の概要

1. **configure terminal**
2. **feature interface-vlan**
3. **interface vlan***number*
4. [**ip address***ip-address/length* | **ipv6 address***ipv6-address/length*]
5. **show interface vlan***number*
6. **no shutdown**
7. **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)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**feature interface-vlan** 例： `switch(config)# feature interface-vlan`	VLAN インターフェイス モードをイネーブルにします。

ステップ 3	**interface vlan***number*
	
	例：
	`switch(config)# interface vlan 10`
	`switch(config-if)#`
		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 4	[**ip address***ip-address/length* | **ipv6 address***ipv6-address/length*]
	
	例：
	`switch(config-if)# ip address 192.0.2.1/8`
	
	例：
	`switch(config-if)# ipv6 address 2001:0DB8::1/8`
		• この VLAN インターフェイスの IP アドレスを設定します。IP アドレスの詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。
		• この VLAN インターフェイスの IPv6 アドレスを設定します。IPv6 アドレスの詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

ステップ 5	**show interface vlan***number* 例： `switch(config-if)# show interface vlan 10`	（任意）レイヤ 3 インターフェイスの統計情報を表示します。

	コマンドまたはアクション	目的

ステップ 6	**no shutdown**
	
	例：
	`switch(config)# int e3/1`
	`switch(config)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーに対応するインターフェイスのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 7	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）設定の変更を保存します。

次に、VLAN インターフェイスを作成する例を示します。

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

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`	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。

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

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

はじめる前に

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

手順の概要

1. **configure terminal**
2. **interface loopback***instance*
3. [**ip address***ip-address/length* | **ipv6 address***ipv6-address/length*]
4. **show interface loopback***instance*
5. **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)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface loopback***instance*
	例：
	`switch(config)# interface loopback 0`
	`switch(config-if)#`
		ループバック インターフェイスを作成します。範囲は 0 ～ 1023 です。

ステップ 3	[**ip address***ip-address/length* | **ipv6 address***ipv6-address/length*] 例： `switch(config-if)# ip address 192.0.2.1/8`	• このインターフェイスの IP アドレスを設定します。IP アドレスの詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

	コマンドまたはアクション	目的
	例： `switch(config-if)# ipv6 address 2001:0DB8::1/8`	• このインターフェイスの IPv6 アドレスを設定します。IPv6 アドレスの詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。
ステップ 4	**show interface loopback***instance* 例： `switch(config-if)# show interface loopback 0`	（任意）ループバック インターフェイスの統計情報を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）設定の変更を保存します。

次に、ループバック インターフェイスを作成する例を示します。

```
switch# configure terminal
switch(config)# interface loopback 0
switch(config-if)# ip address 192.0.2.1/8
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*
3. **mediump2p**
4. **ip unnumbered***typenumber*

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*
	
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**mediump2p** 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***typenumber* 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）

IP アンナンバード インターフェイスの OSPF の設定

IP アンナンバード ループバック インターフェイスの OSPF を設定できます。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot/port*
3. **encapsulation dot1Q***vlan-id*
4. **mediump2p**
5. **ip unnumbered***typenumber*
6. （任意） **ip ospf authentication**
7. （任意） **ip ospf authentication-key***password*
8. **ip router ospf***instance***area***area-number*
9. **no shutdown**
10. **interface loopback***instance*
11. **ip address***ip-address/length*
12. **ip router ospf***instance***area***area-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 ethernet***slot/port*
	
	例：
	`switch(config)# interface ethernet 1/20.1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**encapsulation dot1Q***vlan-id* 例： `switch(config-if)# encapsulation dot1Q 100`	サブインターフェイス上の IEEE 802.1Q VLAN カプセル化を設定します。範囲は 2 ～ 4093 です。
ステップ 4	**mediump2p** 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 5	**ip unnumbered***typenumber* 例： `switch(config-if)# ip unnumbered loopback 101`	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）
ステップ 6	**ip ospf authentication** 例： `switch(config-if)# ip ospf authentication`	（任意） インターフェイスの認証タイプを指定します。
ステップ 7	**ip ospf authentication-key***password* 例： `switch(config-if)# ip ospf authentication 3 b7bdf15f62bbd250`	（任意） OSPF 認証のパスワードを指定します。

	コマンドまたはアクション	目的
ステップ 8	**ip router ospf***instance***area***area-number* 例： `switch(config-if)# ip router ospf 100 area 0.0.0.1`	インターフェイス上で IP のルーティング プロセスを設定して、エリアを指定します。 （注） アンナンバード インターフェイスとナンバード インターフェイスの両方に **ip router ospf** コマンドが必要です。
ステップ 9	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスをアップにします（管理に関して）。
ステップ 10	**interface loopback***instance* 例： `switch(config)# interface loopback 101`	ループバック インターフェイスを作成します。範囲は 0 ～ 1023 です。
ステップ 11	**ip address***ip-address/length* 例： `switch(config-if)# 192.168.101.1/32`	インターフェイスに IP アドレスを設定します。
ステップ 12	**ip router ospf***instance***area***area-number* 例： `switch(config-if)# ip router ospf 100 area 0.0.0.1`	インターフェイス上で IP のルーティング プロセスを設定して、エリアを指定します。 （注） アンナンバード インターフェイスとナンバード インターフェイスの両方に **ip router ospf** コマンドが必要です。

IP アンナンバード インターフェイスの ISIS の設定

IP アンナンバード ループバック インターフェイスの ISIS を設定できます。

手順の概要

1. **configure terminal**
2. **feature isis**
3. **router isis***area-tag*
4. **net***network-entity-title*
5. **end**
6. **interface ethernet***slot/port*
7. **encapsulation dot1Q***vlan-id*
8. **mediump2p**
9. **ip unnumbered***typenumber*
10. **ip router isis***area-tag*
11. **no shutdown**

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	**feature isis** 例： `Switch(config)# feature isis`	ISIS をイネーブルにします。
ステップ 3	**router isis***area-tag* 例： `Switch(config)# router isis 100`	タグを IS-IS プロセスに割り当て、ルータ 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	**net***network-entity-title* 例： `Switch(config-router)# net 49.0001.0100.0100.1001.00`	デバイスでネットワーク エンティティ タイトル（NET）を設定します。
ステップ 5	**end** 例： `Switch(config-router)# end`	ルータ コンフィギュレーション モードを終了します。
ステップ 6	**interface ethernet***slot/port* 例： `switch(config)# interface ethernet 1/20.1`	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 7	**encapsulation dot1Q***vlan-id* 例： `switch(config-subif)# encapsulation dot1Q 100`	サブインターフェイス上の IEEE 802.1Q VLAN カプセル化を設定します。範囲は 2 ～ 4093 です。
ステップ 8	**mediump2p** 例： `switch(config-subif)# 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 9	**ip unnumbered***typenumber* 例： `switch(config-if)# ip unnumbered loopback 101`	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）
ステップ 10	**ip router isis***area-tag* 例： `switch(config-subif)# ip router isis 100`	アンナンバード インターフェイスで ISIS をイネーブルにします。
ステップ 11	**no shutdown** 例： `switch(config-subif)# no shutdown`	インターフェイスをアップにします（管理に関して）。

VRF へのインターフェイスの割り当て

VRF にレイヤ 3 インターフェイスを追加できます。

手順の概要

1. **configure terminal**
2. **interface***interface-typenumber*
3. **vrf member***vrf-name*
4. **ip address***ip-prefix/length*
5. **show vrf** [*vrf-name*] **interface***interface-typenumber*
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)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface***interface-typenumber*
	
	例：
	`switch(config)# interface loopback 0`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**vrf member***vrf-name* 例： `switch(config-if)# vrf member RemoteOfficeVRF`	このインターフェイスを VRF に追加します。
ステップ 4	**ip address***ip-prefix/length* 例： `switch(config-if)# ip address 192.0.2.1/16`	このインターフェイスの IP アドレスを設定します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。
ステップ 5	**show vrf** [*vrf-name*] **interface***interface-typenumber* 例： `switch(config-vrf)# show vrf Enterprise interface loopback 0`	（任意）VRF 情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）設定の変更を保存します。

次に、VRF にレイヤ 3 インターフェイスを追加する例を示します。

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

MAC 組み込み IPv6 アドレスの設定

7.0(3)I2(1) 以降では、MAC 組み込み IPv6（MEv6）アドレスを設定できます。

手順の概要

1. **configure terminal**
2. **interface***type slot/port*
3. **no switchport**
4. **mac-address ipv6-extract**
5. **ipv6 address***ip-address/length*
6. **ipv6 nd mac-extract** [**exclude nud-phase**]
7. （任意） **show ipv6 icmp interface***type slot/port*
8. （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**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface***type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/3`
	`switch(config-if)#`
		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	**no switchport** 例： `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	**mac-address ipv6-extract** 例： `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	**ipv6 address***ip-address/length* 例： `switch(config-if)# ipv6 address 2002:1::10/64`	このインターフェイスの IPv6 アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 6	**ipv6 nd mac-extract** [**exclude nud-phase**] 例： `switch(config-if)# ipv6 nd mac-extract`	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** 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	**show ipv6 icmp interface***type slot/port* 例： `switch(config-if)# show ipv6 icmp interface ethernet 1/3`	（任意） 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。
ステップ 8	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、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
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
```

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
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
```

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 IPv4 または IPv6 アドレスを設定できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interfaceethernet***typeslot/port* | **mgmt***mgmt-interface-number* | **vlan***vlan id*
3. switch(config-if)# [**no**] **ipv6 address use-link-local-only**
4. switch(config-if)# [**no**] [**ip** | **ipv6]address dhcp**
5. （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)# **interfaceethernet***typeslot/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**] **ipv6 address use-link-local-only**	DHCP サーバへの要求を準備します。 （注） このコマンドは、IPv6 アドレスの場合にのみ必要です。
ステップ 4	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 5	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、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 use-link-local-only
switch(config-if)# ipv6 address dhcp
```

レイヤ 3 インターフェイス設定の確認

レイヤ 3 の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
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。

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

コマンド	目的
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。
show ip interface brief	インターフェイスアドレスとインターフェイスステータス（ナンバード/アンナンバード）を表示します。
show ip route	OSPF または ISIS を介して取得されたルートを表示します（最適なユニキャストおよびマルチキャスト ネクストホップのアドレスが含まれる）。

レイヤ 3 インターフェイスのモニタリング

レイヤ 3 統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
load- interval {**interval***seconds* {**1** | **2** | **3**}}	Cisco Nexus 9000 シリーズ デバイスは、ビットレートおよびパケットレートの統計情報に 3 種類のサンプリング インターバルを設定します。 VLAN ネットワーク インターフェイスでの範囲は 60 ～ 300 秒であり、レイヤ インターフェイスでの範囲は 30 ～ 300 秒です。
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**	レイヤ 3 インターフェイスの入力および出力カウンタを表示します。
show interface ethernet errors*slot/port***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 errors*slot/port***counters errors**	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。

コマンド	目的
show interface ethernet errors*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。
show interface ethernet*slot/port.number***counters**	サブインターフェイスの統計情報（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。
show interface port-channel*channel-id.number***counters**	ポート チャネル サブインターフェイスの統計情報（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。
show interface loopback*number***counters**	ループバック インターフェイスの入力および出力カウンタ（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。
show interface loopback*number***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***countersdetailed** [**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*number***counterssnmp**	SNMP MIB から報告された VLAN インターフェイス カウンタを表示します。

レイヤ 3 インターフェイスの設定例

次に、イーサネット サブインターフェイスを設定する例を示します。

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

次に、ループバック インターフェイスを設定する例を示します。

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

インターフェイスの VRF メンバーシップ変更の例

- VRF メンバーシップを変更する場合はレイヤ 3 設定の保持を有効にします。

```
switch# configure terminal
switch(config)# system vrf-member-change retain-l3-config

Warning: Will retain L3 configuration when vrf member change on interface.
```

- レイヤ 3 の保持を確認します。

```
switch# show running-config | include vrf-member-change

system vrf-member-change retain-l3-config
```

- レイヤ 3 設定によって SVI インターフェイスを VRF の「blue」として設定します。

```
switch# configure terminal
switch(config)# show running-config interface vlan 2002

interface Vlan2002
description TESTSVI
no shutdown
mtu 9192
vrf member blue
no ip redirects
ip address 192.168.211.2/27
ipv6 address 2620:10d:c041:12::2/64
ipv6 link-local fe80::1
ip router ospf 1 area 0.0.0.0
ipv6 router ospfv3 1 area 0.0.0.0
hsrp version 2
hsrp 2002
preempt delay minimum 300 reload 600
priority 110 forwarding-threshold lower 1 upper 110
ip 192.168.211.1
hsrp 2002 ipv6
preempt delay minimum 300 reload 600
priority 110 forwarding-threshold lower 1 upper 110
ip 2620:10d:c041:12::1
```

- SVI インターフェイスの VRF を「red」に変更します。

```
switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface vlan 2002
switch(config-if)# vrf member red

Warning: Retain-L3-config is on, deleted and re-added L3 config on interface Vlan2002
```

- VRF の変更後に SVI インターフェイスを確認します。

```
switch# configure terminal
switch(config)# show running-config interface vlan 2002

interface Vlan2002
description TESTSVI
no shutdown
```

```
mtu 9192
vrf member red
no ip redirects
ip address 192.168.211.2/27
ipv6 address 2620:10d:c041:12::2/64
ipv6 link-local fe80::1
ip router ospf 1 area 0.0.0.0
ipv6 router ospfv3 1 area 0.0.0.0
hsrp version 2
hsrp 2002
preempt delay minimum 300 reload 600
priority 110 forwarding-threshold lower 1 upper 110
ip 192.168.211.1
hsrp 2002 ipv6
preempt delay minimum 300 reload 600
priority 110 forwarding-threshold lower 1 upper 110
ip 2620:10d:c041:12::1
```

（注）

- VRF を変更する場合、レイヤ 3 設定の保持は次に影響します。
  - Physical Interface
  - ループバック インターフェイス
  - SVI インターフェイス
  - Sub-interface
  - トンネル インターフェイス
  - ポート チャネル
- VRF を変更する場合、既存のレイヤ 3 設定が削除され、再適用されます。すべてのルーティング プロトコル（OSPF/ISIS/EIGRP/HSRP）が古い VRF でダウンし、新しい VRF でアップします。
- ダイレクトおよびローカル IPv4/IPv6 アドレスが古い VRF から削除され、新しい VRF にインストールされます。
- VRF 変更時にトラフィック損失が発生する可能性があります。

関連資料

関連資料	マニュアル タイトル
IP	『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』
VLANs	『*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*』

第 6 章

双方向フォワーディング検出の設定

BFD について

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

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

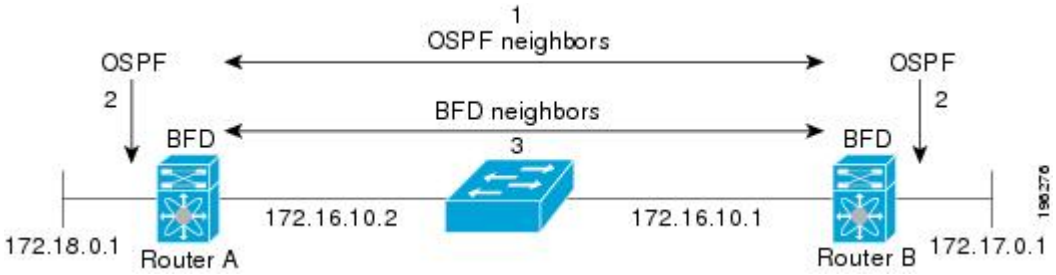
非同期モード

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

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

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

図 *6*：*BFD* ネイバー関係の確立



BFD の障害検出

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

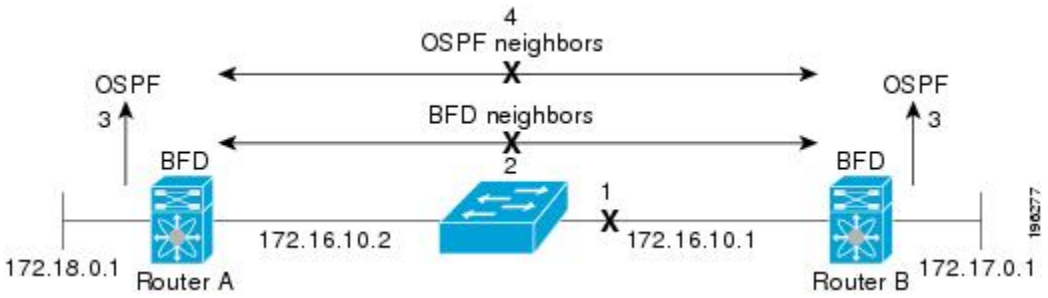
BFD は転送パスに障害を検出したとき、障害検出通知を BFD 対応プロトコルに送信します。ローカル デバイスは、プロトコル再計算プロセスを開始してネットワーク全体の収束時間を削減できます。

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

（注）

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

図 *7*：*OSPF* ネイバー関係の解除



分散型動作

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

BFD エコー機能

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

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

セキュリティ

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

BFD パケットの SHA-1 認証を設定できます。

ハイ アベイラビリティ

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

仮想化のサポート

BFD は、仮想ルーティングおよび転送（VRF）インスタンスをサポートしています。VRF は仮想化デバイス コンテキスト（VDC）内にあります。デフォルトでは、Cisco NX-OS はデフォルト VDC とデフォルト VRF に配置します。

BFD のライセンス要件

次の表に、この機能のライセンス要件を示します。

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

BFD の前提条件

BFD には、次の前提条件があります。

- BFD 機能をイネーブルにする必要があります。
- BFD 対応インターフェイスでインターネット制御メッセージ プロトコル（ICMP）リダイレクト メッセージをディセーブルにします。

- 同一の IP 送信元アドレスおよび宛先アドレスを調べる IP パケット検証チェックをディセーブルにします。
- 設定作業とともに一覧表示されているその他の詳細な前提条件を参照してください。

注意事項と制約事項

BFD 設定時の注意事項と制約事項は次のとおりです。

- **show** コマンドで **internal** キーワードを指定することは、サポートされていません。
- BFD は BFD バージョン 1 をサポートします。
- BFD は IPv4 と IPv6 をサポートします。
- BFD は OSPFv3 をサポートします。
- BFD は IS ISv6 をサポートします。
- BFD は BGPv6 をサポートします。
- BFD は EIGRPv6 をサポートします。
- BFD は、インターフェイスごとのアドレス ファミリ 1 つにつき 1 セッションだけサポートします。
- BFD は、シングルホップ BFD をサポートします。
- ボーダー ゲートウェイ プロトコル（BGP）の BFD は、シングルホップ External BGP（EBGP）および Internal BGP（iBGP）ピアをサポートしています。
- BFD は、キー付き SHA-1 認証をサポートします。
- BFD は、次のレイヤ 3 インターフェイスをサポートします。物理インターフェイス、ポート チャネル、サブインターフェイス、および VLAN インターフェイス。
- BFD はレイヤ 3 隣接情報に応じて、レイヤ 2 のトポロジ変更を含むトポロジ変更を検出します。レイヤ 3 隣接情報が使用できない場合、VLAN インターフェイス（SVI）の BFD セッションはレイヤ 2 トポロジのコンバージェンス後に稼働しない可能性があります。
- 2 台のデバイス間のスタティック ルート上の BFD については、両方のデバイスが BFD をサポートする必要があります。デバイスの一方または両方が BFD をサポートしていない場合、スタティック ルートはルーティング情報ベース（RIB）でプログラミングされません。
- ポート チャネル設定の制限事項
  - BFD で使用されるレイヤ 3 ポート チャネルでは、ポート チャネルの LACP をイネーブルにする必要があります。
  - SVI のセッションで使用されるレイヤ 2 ポート チャネルでは、ポート チャネルの LACP をイネーブルにする必要があります。
- SVI の制限事項

- ASIC リセットにより他のポートのトラフィックが中断されます。このイベントは、その他のポートの SVI セッションがフラップする原因になることがあります。ASIC がリセットする既存のトリガーには、VDC をリロードしている VDC 間のポート移動があります。また、キャリア インターフェイスが仮想ポート チャネル（vPC）の場合、BFD は SVI インターフェイスではサポートされません。
- トポロジを変更すると（たとえば、VLAN へのリンクの追加または削除、レイヤ 2 ポート チャネルからのメンバの削除など）、SVI セッションが影響を受ける場合があります。SVIセッションはダウンした後、トポロジディスカバリの終了後に起動する場合があります。
- BFD セッションが仮想ポート チャネル（vPC）ピア リンク（BCM ベース ポートまたは GEM ベース ポートのいずれか）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** コマンドを使用して、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。

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

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

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

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

- **clear** {**ip** | **ipv6**} **route***prefix* コマンドでネイバーにプレフィックスを指定すると、BFD エコー セッションがフラップします。
- **clear** {**ip** | **ipv6**} **route *** コマンドにより、BFD エコー セッションがフラップします。
- IPv4 に対する HSRP は、BFD でサポートされます。
- Cisco NX-OS デバイスのラインカードによって生成される BFD パケットは COS 6/DSCP CS6 とともに送信されます。BFD パケットの DSCP/COS 値は、ユーザが設定可能な値ではありません。
- BFDv6 を no-bfd-echo モードで設定する場合は、乗数 3 の 150 ミリ秒のタイマーを使用することをお勧めします。

- BFDv6 は VRRPv3 および HSRP for v6 ではサポートされていません。
- IPv6 **eigrp bfd** はインターフェイスでディセーブルにできません。
- ポート チャネル設定の注意事項
  - BFD per-link モードが設定されている場合、BFD エコーの機能はサポートされません。**bfd per-link** コマンドを設定する前に、**no bfd echo** コマンドを使用して BFD エコー機能をディセーブルにする必要があります。
  - リンクローカルによる BFD per-link の設定はサポートされていません。

デフォルト設定

次の表に、BFD パラメータのデフォルト設定を示します。

表 *9*：デフォルトの *BFD* パラメータ

パラメータ（Parameters）	デフォルト
BFD 機能	ディセーブル
必要最小受信間隔	50 ミリ秒
目的の最小送信間隔	50 ミリ秒
検出乗数	3
エコー機能	イネーブル
モード	非同期
Port-channel	論理モード（送信元/宛先ペアのアドレスごとに 1 セッション）
slow timer	2000 ミリ秒
起動タイマー（7.0(3)I2(1) 以降）	5 秒

BFD の設定

設定階層

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

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

BFD 設定のタスク フロー

BFD を設定するには、以下の項にある次の手順に従います。

- BFD 機能のイネーブル化
- グローバルな BFD パラメータを設定またはインターフェイスでの BFD の設定

BFD 機能のイネーブル化

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

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

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

手順の概要

1. **configure terminal**
2. **feature bfd**
3. **show feature | include bfd**
4. **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)#`
		コンフィギュレーションモードに入ります。

ステップ 2	**feature bfd** 例： `switch(config)# feature bfd`	BFD 機能をイネーブルにします。
ステップ 3	**show feature | include bfd** 例： `switch(config)# show feature | include bfd`	（任意）イネーブルおよびディセーブルにされた機能を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）設定の変更を保存します。

グローバルな BFD パラメータの設定

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

インターフェイスでこれらのグローバルなセッション パラメータを上書きするには、「インターフェイスでの BFD の設定」の項を参照してください。

はじめる前に

BFD 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **bfd interval***mintx***min_rx***msec***multiplier***value***
3. **bfd slow-timer** [*interval*]
4. [**no**] **bfd startup-timer** [*seconds*]
5. **bfd echo-interface loopback***interfacenumber*
6. **show running-config bfd**
7. **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)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**bfd interval***mintx***min_rx***msec***multiplier***value*** 例： `switch(config)# bfd interval 50 min_rx 50 multiplier 3`	デバイスのすべての BFD セッションの BFD セッション パラメータを設定します。インターフェイスで BFD セッション パラメータを設定することにより、このコマンドでこれらの値を無効にすることができます。*mintx* および *msec* の範囲は 50 ～ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ～ 50 です。乗数のデフォルトは 3 です。
ステップ 3	**bfd slow-timer** [*interval*] 例： `switch(config)# bfd slow-timer 2000`	エコー機能で使用される slow timer を設定します。この値はエコー機能がイネーブルの場合、BFD が新しいセッションを開始する速度および非同期セッションが BFD 制御パケットに使用する速度を決定します。slow-timer 値は新しい制御パケット間隔として使用されますが、エコー パケットは設定された BFD 間隔を使用します。エコーパケットはリンク障害検出に使用されますが、低速の制御パケットは BFD セッションを維持します。指定できる範囲は 1000 ～ 30000 ミリ秒です。デフォルトは 2000 です。
ステップ 4	[**no**] **bfd startup-timer** [*seconds*] 例： `switch(config)# bfd startup-timer 20`	BFD 起動タイマーを設定します。BFD 起動タイマーは、BFD セッションの起動時間を遅らせることにより、ローカルおよびリモート ルータで使用されているルートがハードウェアに固定されるまでの時間を作ります。この機能を使用すると、より大規模なシナリオで BFD のフラップを防止できます。範囲は 0 ～ 30 秒です。デフォルトは 5 秒です。 **bfd startup-timer 0** コマンドは、BFD 起動タイマーをディセーブルにします。 **no bfd startup-timer** コマンドは、BFD 起動タイマーを 5 秒（デフォルト値）に設定します。 **重要** **bfd startup-timer** コマンドは 7.0(3)I2(1) 以降に適用されます。
ステップ 5	**bfd echo-interface loopback***interfacenumber* 例： `switch(config)# bfd echo-interface loopback 1 3`	双方向フォワーディング検出（BFD）のエコーフレームに使用するインターフェイスを設定します。このコマンドは、指定されたループバック インターフェイスで設定されるアドレスに、エコーパケットの送信元アドレスを変更します。指定できるインターフェイス番号の範囲は 0 ～ 1023 です。

	コマンドまたはアクション	目的
ステップ 6	**show running-config bfd** 例： `switch(config)# show running-config bfd`	（任意）BFD 実行コンフィギュレーションを表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）設定の変更を保存します。

インターフェイスでの BFD の設定

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

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

はじめる前に

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

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

手順の概要

1. **configure terminal**
2. **interface***int-if*
3. **bfd interval***mintx***min_rx***msec***multiplier***value***
4. **bfd authentication keyed-sha1 keyid***id***key***ascii_key***
5. **show running-config bfd**
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)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface***int-if*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。?キーワードを使用して、サポートされるインターフェイスを表示します。

ステップ 3	**bfd interval***mintx***min_rx***msec***multiplier***value*** 例： `switch(config-if)# bfd interval 50 min_rx 50 multiplier 3`	デバイスのすべての BFD セッションの BFD セッション パラメータを設定します。インターフェイスで BFD セッション パラメータを設定することにより、このコマンドでこれらの値を無効にすることができます。*mintx* および *msec* の範囲は 50 ～ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ～ 50 です。乗数のデフォルトは 3 です。
ステップ 4	**bfd authentication keyed-sha1 keyid***id***key***ascii_key*** 例： `switch(config-if)# bfd authentication keyed-sha1 keyid 1 ascii_key cisco123`	（任意）インターフェイス上のすべての BFD セッションの SHA-1 認証を設定します。*ascii_key* 文字列は BFD ピア間で共有される秘密キーです。0 ～ 255 の数値の *id* 値が、この特定の *ascii_key* に割り当てられます。BFD パケットは *id* でキーを指定し、複数のアクティブ キーが使用できます。 インターフェイスの SHA-1 認証をディセーブルにするには、コマンドの **no** 形式を使用します。
ステップ 5	**show running-config bfd** 例： `switch(config-if)# show running-config bfd`	（任意）BFD 実行コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）設定の変更を保存します。

ポート チャネルの BFD の設定

ポート チャネルのすべての BFD セッションの BFD セッション パラメータを設定できます。パーリンク モードがレイヤ 3 ポート チャネルに使用される場合、BFD により、ポート チャネルの各

リンクのセッションが作成され、集約結果がクライアント プロトコルへ提供されます。たとえば、ポート チャネルの 1 つのリンクの BFD セッションが稼働している場合、OSPF などのクライアント プロトコルにポート チャネルが稼働していることが通知されます。BFD セッション パラメータは、スリーウェイ ハンドシェイクの BFD ピア間でネゴシエートされます。

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

はじめる前に

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

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

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

手順の概要

1. **configure terminal**
2. **interface port-channel***number*
3. **bfd per-link**
4. **bfd interval***mintx***min_rx***msec***multiplier***value***
5. **bfd authentication keyed-sha1 keyid***id***key***ascii_key***
6. **show running-config bfd**
7. **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 2`
	`switch(config-if)#`
		ポートチャネル コンフィギュレーション モードを開始します。**?** キーワードを使用して、サポートされる数値の範囲を表示します。

ステップ 3	**bfd per-link** 例： `switch(config-if)# bfd per-link`	ポートチャネルのリンクごとに BFD セッションを設定します。

	コマンドまたはアクション	目的
ステップ 4	**bfd interval***mintx***min_rx***msec***multiplier***value* 例： `switch(config-if)# bfd interval 50 min_rx 50 multiplier 3`	（任意）ポートチャネルのすべてのBFDセッションのBFDセッションパラメータを設定します。BFDセッションパラメータを設定することにより、このコマンドでこれらの値を無効にすることができます。*mintx* および *msec* の範囲は 50 ～ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ～ 50 です。乗数のデフォルトは 3 です。
ステップ 5	**bfd authentication keyed-sha1 keyid***id***key***ascii_key* 例： `switch(config-if)# bfd authentication keyed-sha1 keyid 1 ascii_key cisco123`	（任意）インターフェイス上のすべての BFD セッションの SHA-1 認証を設定します。*ascii_key* 文字列は BFD ピア間で共有される秘密キーです。0 ～ 255 の数値の *id* 値が、この特定の *ascii_key* に割り当てられます。BFD パケットは *id* でキーを指定し、複数のアクティブ キーが使用できます。 インターフェイスのSHA-1認証をディセーブルにするには、コマンドの **no** 形式を使用します。
ステップ 6	**show running-config bfd** 例： `switch(config-if)# show running-config bfd`	（任意）BFD 実行コンフィギュレーションを表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）設定の変更を保存します。

BFD エコー機能の設定

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

はじめる前に

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

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

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

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

手順の概要

1. **configure terminal**
2. **bfd slow-timer***echo-interval*
3. **interface***int-if*
4. **bfd echo**
5. **show running-config bfd**
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)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**bfd slow-timer***echo-interval* 例： `switch(config)# bfd slow-timer 2000`	エコー機能で使用される slow timer を設定します。この値はBFDが新しいセッションを開始する速度を決定し、BFDエコー機能がイネーブルの場合に非同期セッションの速度を低下させるために使用されます。この値は、エコー機能がイネーブルの場合、必要最小受信間隔より優先されます。指定できる範囲は 1000 ～ 30000 ミリ秒です。デフォルトは 2000 です。

ステップ 3	**interface***int-if*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。?キーワードを使用して、サポートされるインターフェイスを表示します。

ステップ 4	**bfd echo** 例： `switch(config-if)# bfd echo`	エコー機能をイネーブルにします。デフォルトではイネーブルになっています。
ステップ 5	**show running-config bfd** 例： `switch(config-if)# show running-config bfd`	（任意）BFD実行コンフィギュレーションを表示します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）設定の変更を保存します。

ルーティング プロトコルに対する BFD サポートの設定

BGP での BFD の設定

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

はじめる前に

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

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

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

手順の概要

1. **configure terminal**
2. **router bgp***as-number*
3. **neighbor** (*ip-address* | *ipv6-address*) **remote-as***as-number*
4. **bfd**
5. **show running-config bgp**
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)#`
		コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的

ステップ 2	**router bgp***as-number*
	
	例：
	`switch(config)# router bgp 64496`
	`switch(config-router)#`
		BGP をイネーブルにして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。

ステップ 3	**neighbor** (*ip-address* | *ipv6-address*) **remote-as***as-number*
	
	例：
	`switch(config-router)# neighbor 209.165.201.1 remote-as 64497`
	`switch(config-router-neighbor)#`
		リモート BGP ピアの IPv4 アドレスまたは IPv6 アドレスおよび AS 番号を設定します。*ip-address* の形式は x.x.x.x です。*ipv6-address* の形式は A:B::C:D です。

ステップ 4	**bfd** 例： `switch(config-router-neighbor)# bfd`	この BGP ピアの BFD をイネーブルにします。
ステップ 5	**show running-config bgp** 例： `switch(config-router-neighbor)# show running-config bgp`	（任意）BGP 実行コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-router-neighbor)# copy running-config startup-config`	（任意）設定の変更を保存します。

EIGRP 上での BFD の設定

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

はじめる前に

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

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

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

手順の概要

1. **configure terminal**
2. **router eigrp***instance-tag*
3. **bfd** [**ipv4** | **ipv6**]
4. **interface***int-if*
5. **ip eigrp***instance-tag***bfd**
6. **show ip eigrp** [**vrf***vrf-name*] [**interfaces***if*]
7. **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)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**router eigrp***instance-tag*
	
	例：
	`switch(config)# router eigrp Test1`
	`switch(config-router)#`
		インスタンス タグを設定して、新しい EIGRP プロセスを作成します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
		AS 番号であると認められていないインスタンス タグを設定する場合は、**autonomous-system** を使用 して AS 番号を明示的に設定する必要があります。そうしないと、この EIGRP インスタンスはシャットダウン状態のままになります。

ステップ 3	**bfd** [**ipv4**	**ipv6**] 例： `switch(config-router-neighbor)# bfd ipv4`	（任意）すべての EIGRP インターフェイスの BFD をイネーブルにします。

ステップ 4	**interface***int-if*
	
	例：
	`switch(config-router-neighbor)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。**?**キーワードを使用して、サポートされるインターフェイスを表示します。

ステップ 5	**ip eigrp***instance-tag***bfd** 例： `switch(config-if)# ip eigrp Test1 bfd`	（任意）EIGRP インターフェイスの BFD をイネーブルまたはディセーブルにします。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。 デフォルトではディセーブルになっています。

	コマンドまたはアクション	目的
ステップ 6	**show ip eigrp** [**vrf***vrf-name*] [**interfaces***if*] 例： `switch(config-if)# show ip eigrp`	（任意）EIGRP に関する情報を表示します。*vrf-name* には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。
ステップ 7	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）設定の変更を保存します。

OSPF での BFD の設定

Open Shortest Path First で BFD を設定できます。

はじめる前に

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

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

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

手順の概要

1. **configure terminal**
2. **router ospf***instance-tag*
3. **bfd** [**ipv4** | **ipv6**]
4. **interface***int-if*
5. **ip ospf bfd**
6. **show ip ospf** [**vrf***vrf-name*] [**interfaces***if*]
7. **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。

	コマンドまたはアクション	目的

ステップ 2	**router ospf***instance-tag*
	
	例：
	`switch(config)# router ospf 200`
	`switch(config-router)#`
		インスタンス タグを設定して、新しい OSPF インスタンスを作成します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。

ステップ 3	**bfd** [**ipv4** | **ipv6**] 例： `switch(config-router)# bfd`	（任意）すべての OSPF インターフェイスの BFD をイネーブルにします。

ステップ 4	**interface***int-if*
	
	例：
	`switch(config-router)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。**?** キーワードを使用して、サポートされるインターフェイスを表示します。

ステップ 5	**ip ospf bfd** 例： `switch(config-if)# ip ospf bfd`	（任意）OSPF インターフェイスの BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 6	**show ip ospf** [**vrf***vrf-name*] [**interfaces***if*] 例： `switch(config-if)# show ip ospf`	（任意）OSPF に関する情報を表示します。*vrf-name* には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。
ステップ 7	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）設定の変更を保存します。

BFD の設定例

- IPv4 および IPv6 アドレス ファミリで BFD が有効になる IS-IS の設定例

```
configure terminal
  router isis isis-1
    bfd
    address-family ipv6 unicast
    bfd
```

- 非デフォルト VRF（vrf3 の OSPFv3 ネイバー）で BFD が有効になる設定例

```
configure terminal
  router ospfv3 10
    vrf vrf3
    bfd
```

- インターフェイスごとに BFD が無効になる設定例

```
configure terminal
  interface port-channel 10
    no ip redirects
    ip address 22.1.10.1/30
    ipv6 address 22:1:10::1/120
    no ipv6 redirects
    ip router ospf 10 area 0.0.0.0
    ip ospf bfd disable        /*** disables IPv4 BFD session for OSPF
    ospfv3 bfd disable         /*** disables IPv6 BFD session for OSPFv3
```

- インターフェイス スタティック BFD ネイバーに関して BFD が有効になる設定例

```
configure terminal
  interface Ethernet1/15
    ip address 25.7.1.1/30
    ipv6 address 25:7:1::1/120
    no ip redirects
    no ipv6 redirects
    bfd neighbor src-ip 25.7.1.1 dest-ip 25.7.1.2   /*** simulates IPv4 BFD client
    bfd neighbor src-ip 25:7:1::1 dest-ip 25:7:1::2 /*** simulates IPv6 BFD client
    no shutdown
```

IS-IS での BFD の設定

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

はじめる前に

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

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

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

手順の概要

1. **configure terminal**
2. **router isis***instance-tag*
3. **bfd** [**ipv4** | **ipv6**]
4. **interface***int-if*
5. **isis bfd**
6. **show isis** [**vrf***vrf-name*] [**interface***if*]
7. **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	**router isis***instance-tag*
	
	例：
	`switch(config)# router isis 100`
	`switch(config-router)# net 49.0001.1720.1600.1001.00`
	`switch(config-router)# address-family ipv6 unicast`
		instance tag を設定して、新しい IS-IS インスタンスを作成します。

ステップ 3	**bfd** [**ipv4** | **ipv6**] 例： `switch(config-router)# bfd`	（任意）すべての OSPF インターフェイスの BFD をイネーブルにします。

ステップ 4	**interface***int-if*
	
	例：
	`switch(config-router)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。**?** キーワードを使用して、サポートされるインターフェイスを表示します。

ステップ 5	**isis bfd** 例： `switch(config-if)# isis bfd`	（任意）IS-IS インターフェイスの BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 6	**show isis** [**vrf***vrf-name*] [**interface***if*] 例： `switch(config-if)# show isis`	（任意）IS-IS に関する情報を表示します。*vrf-name* には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。
ステップ 7	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）設定の変更を保存します。

HSRP での BFD の設定

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

HSRP ルータが動作していないことを検知すると、スタンバイ HSRP はこのイベントをアクティブ タイマー失効として取り扱いアクティブ HSRP ルータとして役割を引き継ぎます。

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

はじめる前に

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

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

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

手順の概要

1. **configure terminal**
2. **hsrp bfd all-interfaces**
3. **interface***int-if*
4. **hsrp bfd**
5. **show running-config hsrp**
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	**hsrp bfd all-interfaces** 例： `switch# hsrp bfd all-interfaces`	（任意）すべての HSRP インターフェイスで BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。

ステップ 3	**interface***int-if*
	
	例：
	`switch(config-router)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。**?** キーワードを使用して、サポートされるインターフェイスを表示します。

ステップ 4	**hsrp bfd** 例： `switch(config-if)# hsrp bfd`	（任意）HSRP インターフェイスの BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。

	コマンドまたはアクション	目的
ステップ 5	**show running-config hsrp** 例： `switch(config-if)# show running-config hsrp`	（任意）HSRP 実行コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）設定の変更を保存します。

VRRP での BFD の設定

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

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

はじめる前に

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

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

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

手順の概要

1. **configure terminal**
2. **interface***int-if*
3. **vrrp***group-no*
4. **vrrp bfd***address*
5. **show running-config vrrp**
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***int-if*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。**?** キーワードを使用して、サポートされるインターフェイスを表示します。

ステップ 3	**vrrp***group-no* 例： `switch(config-if)# vrrp 2`	VRRP グループ番号を指定します。
ステップ 4	**vrrp bfd***address* 例： `switch(config-if)# vrrp bfd`	VRRP インターフェイスで BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 5	**show running-config vrrp** 例： `switch(config-if)# show running-config vrrp`	（任意）VRRP 実行コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）設定の変更を保存します。

PIM での BFD の設定

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

はじめる前に

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

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

手順の概要

1. **configure terminal**
2. **ip pim bfd**
3. **interface***int-if*
4. **ip pim bfd-instance** [**disable**]
5. **show running-config pim**
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	**ip pim bfd** 例： `switch(config)# ip pim bfd`	PIM の BFD をイネーブルにします。

ステップ 3	**interface***int-if*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。**?** キーワードを使用して、サポートされるインターフェイスを表示します。

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

スタティック ルートでの BFD の設定

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

はじめる前に

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

手順の概要

1. **configure terminal**
2. **vrf context***vrf-name*
3. **ip route***routeinterface* {*nh-address* | *nh-prefix*}
4. **ip route static bfd***interface* {*nh-address* | *nh-prefix*}
5. **show ip route static** [**vrf***vrf-name*]
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	**vrf context***vrf-name*
	
	例：
	`switch(config)# vrf context Red`
	`switch(config-vrf)#`
		（任意）VRF コンフィギュレーション モードを開始します。

ステップ 3	**ip route***routeinterface* {*nh-address*	*nh-prefix*} 例： `switch(config-vrf)# ip route 192.0.2.1 ethernet 2/1 192.0.2.4`	スタティック ルートを作成します。**?** キーワードを使用して、サポートされているインターフェイスを表示します。
ステップ 4	**ip route static bfd***interface* {*nh-address*	*nh-prefix*} 例： `switch(config-vrf)# ip route static bfd ethernet 2/1 192.0.2.4`	インターフェイスのすべてのスタティック ルートの BFD をイネーブルにします。**?** キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 5	**show ip route static** [**vrf***vrf-name*] 例： `switch(config-vrf)# show ip route static vrf Red`	（任意）スタティック ルートを表示します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `switch(config-vrf)# copy running-config startup-config`	（任意）設定の変更を保存します。

インターフェイスにおける BFD のディセーブル化

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

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

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

BFD 相互運用性の設定

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

手順の概要

1. **configure terminal**
2. **interface port-channel***int-if*
3. **ip ospf bfd**
4. **no ip redirects**
5. **bfd interval***mintx***min_rx***msec***multiplier***value***
6. **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	**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***int-if* 例： `switch(config-if)# interface ethernet 2/1`	インターフェイス コンフィギュレーション モードを開始します。**?** キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 3	**ip ospf bfd** 例： `switch(config-if)# ip ospf bfd`	OSPFv2 インターフェイスで BFD をイネーブルにします。デフォルトではディセーブルになっています。 OSPF は例として使用されています。サポートされている任意のプロトコルの BFD をイネーブルにできます。
ステップ 4	**no ip redirects** 例： `switch(config-if)# no ip redirects`	デバイスがリダイレクトを送信しないようにします。

	コマンドまたはアクション	目的
ステップ 5	**bfd interval***mintx***min_rx***msec***multiplier***value* 例： `switch(config-if)# bfd interval 50 min_rx 50 multiplier 3`	ポート チャネルのすべての BFD セッションの BFD セッション パラメータを設定します。BFD セッション パラメータを設定することにより、このコマンドでこれらの値を無効にすることができます。*mintx* および *msec* の範囲は 50 ～ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ～ 50 です。乗数のデフォルトは 3 です。
ステップ 6	**exit** 例： `switch(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、EXEC モードに戻ります。

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

手順の概要

1. **configure terminal**
2. **interface port-channel***vlanvlan-id*
3. **bfd interval***mintx***min_rx***msec***multiplier***value***
4. **no ip redirects**
5. **ip address***ip-address/length*
6. **ip ospf bfd**
7. **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	**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***vlanvlan-id*
	
	例：
	`switch(config)# interface vlan 998`
	`switch(config-if)#`
		ダイナミック スイッチ仮想インターフェイス（SVI）を作成します。

	コマンドまたはアクション	目的
ステップ 3	**bfd interval***mintx***min_rx***msec***multiplier***value* 例： `switch(config-if)# bfd interval 50 min_rx 50 multiplier 3`	デバイスのすべての BFD セッションの BFD セッション パラメータを設定します。*mintx* および *msec* の範囲は 50 ～ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ～ 50 です。乗数のデフォルトは 3 です。
ステップ 4	**no ip redirects** 例： `switch(config-if)# no ip redirects`	デバイスがリダイレクトを送信しないようにします。
ステップ 5	**ip address***ip-address/length* 例： `switch(config-if)# ip address 10.1.0.253/24`	このインターフェイスの IP アドレスを設定します。
ステップ 6	**ip ospf bfd** 例： `switch(config-if)# ip ospf bfd`	OSPFv2 インターフェイスで BFD をイネーブルにします。デフォルトではディセーブルになっています。
ステップ 7	**exit** 例： `switch(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、EXEC モードに戻ります。

論理モードの Cisco NX-OS デバイスの BFD 相互運用性の設定

手順の概要

1. **configure terminal**
2. **interface port-channel***typenumber.subinterface-id*
3. **bfd interval***mintx***min_rx***msec***multiplier***value***
4. **no ip redirects**
5. **ip ospf bfd**
6. **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	**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***typenumber.subinterface-id* 例： `switch(config-if)# interface port-channel 50.2`	ポート チャネル コンフィギュレーション モードを開始します。**?** キーワードを使用して、サポートされる数値の範囲を表示します。
ステップ 3	**bfd interval***mintx***min_rx***msec***multiplier***value*** 例： `switch(config-if)# bfd interval 50 min_rx 50 multiplier 3`	ポート チャネルのすべての BFD セッションの BFD セッション パラメータを設定します。*mintx* および *msec* の範囲は 50 ～ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ～ 50 です。乗数のデフォルトは 3 です。
ステップ 4	**no ip redirects** 例： `switch(config-if)# no ip redirects`	デバイスがリダイレクトを送信しないようにします。
ステップ 5	**ip ospf bfd** 例： `switch(config-if)# ip ospf bfd`	OSPFv2 インターフェイスで BFD をイネーブルにします。デフォルトではディセーブルになっています。 OSPF は例として使用されています。サポートされている任意のプロトコルの BFD をイネーブルにできます。
ステップ 6	**exit** 例： `switch(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、EXEC モードに戻ります。

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

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

```
switch# show bfd neighbors details
OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int
Vrf
10.1.1.1 10.1.1.2 1140850707/2147418093 Up 6393(4) Up Vlan2121
default
Session state is Up and using echo function with 50 ms interval
Local Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: None
MinTxInt: 50000 us, MinRxInt: 2000000 us, Multiplier: 3
```

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


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

BFD 設定の確認

BFD 設定情報を表示するには、次のいずれかを行います。

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

BFD のモニタリング

BFD を表示するには、次のコマンドを使用します。

コマンド	目的
show bfd neighbors [**application***name*] [**details**]	BGP や OSPFv2 などのサポートされるアプリケーションの BFD に関する情報を表示します。
show bfd neighbors [**interface***int-if*] [**details**]	インターフェイスの BGP セッションに関する情報を表示します。
show bfd neighbors [**dest-ip***ip-address*] [**src-ip***ip-address*][**details**]	インターフェイス上の指定された BGP セッションに関する情報を表示します。
show bfd neighbors [**vrf***vrf-name*] [**details**]	VRF の BFD に関する情報を表示します。
show bfd [**ipv4** | **ipv6**] [**neighbors**]	IPv4 ネイバーまたは IPv6 ネイバーに関する情報を表示します。

BFD の設定例

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

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

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

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

次に、BFDv6 設定例を示します。

```
feature bfd
feature ospfv3
router ospfv3 Test1
interface Ethernet2/7
  ipv6 router ospfv3 Test1 area 0.0.0.0
  ospfv3 bfd
  no shutdown
```

BFD の表示例

次に、**show bfd ipv6 neighbors details** コマンドの結果の例を示します。

```
#show bfd ipv6 neighbors details

OurAddr                          NeighAddr
 LD/RD                 RH/RS           Holdown(mult)     State       Int
 Vrf
cc:10::2                         cc:10::1
 1090519335/1090519260 Up             5692(3)           Up          Po1
 default


Session state is Up and using echo function with 250 ms interval
Local Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: None
MinTxInt: 250000 us, MinRxInt: 2000000 us, Multiplier: 3
Received MinRxInt: 2000000 us, Received Multiplier: 3
Holdown (hits): 6000 ms (4), Hello (hits): 2000 ms (205229)
Rx Count: 227965, Rx Interval (ms) min/max/avg: 124/1520/1510 last: 307 ms ago
Tx Count: 205229, Tx Interval (ms) min/max/avg: 1677/1677/1677 last: 587 ms ago
Registered protocols:  bgp
Uptime: 3 days 23 hrs 31 mins 13 secs
Last packet: Version: 1                - Diagnostic: 0
             State bit: Up             - Demand bit: 0
             Poll bit: 0               - Final bit: 0
             Multiplier: 3             - Length: 24
             My Discr.: 1090519260     - Your Discr.: 1090519335
             Min tx interval: 250000   - Min rx interval: 2000000
             Min Echo interval: 250000 - Authentication bit: 0
Hosting LC: 1, Down reason: None, Reason not-hosted: None
```

関連資料

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

RFC

RFC	Title
RFC 5880	双方向フォワーディング検出（*BFD*）
RFC 5881	『*BFD for IPv4 and IPv6 (Single Hop)*』

RFC

第 7 章

ポート チャネルの設定

この章では、ポート チャネルを設定し、Cisco NX-OS デバイスでポート チャネルをより有効に利用するために Link Aggregation Control Protocol（LACP）を適用して設定する手順を説明します。

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

ポート チャネルについて

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

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

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

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

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

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

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

LACP については、「LACP の概要」の項を参照してください。

ポート チャネル

ポート チャネルは、物理リンクをまとめて 1 つのチャネル グループに入れ、最大 32 の物理リンクの帯域幅を集約した単一の論理リンクを作ります。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。

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

（注） デバイスはポート チャネルに対するポート集約プロトコル（PAgP）をサポートしません。

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

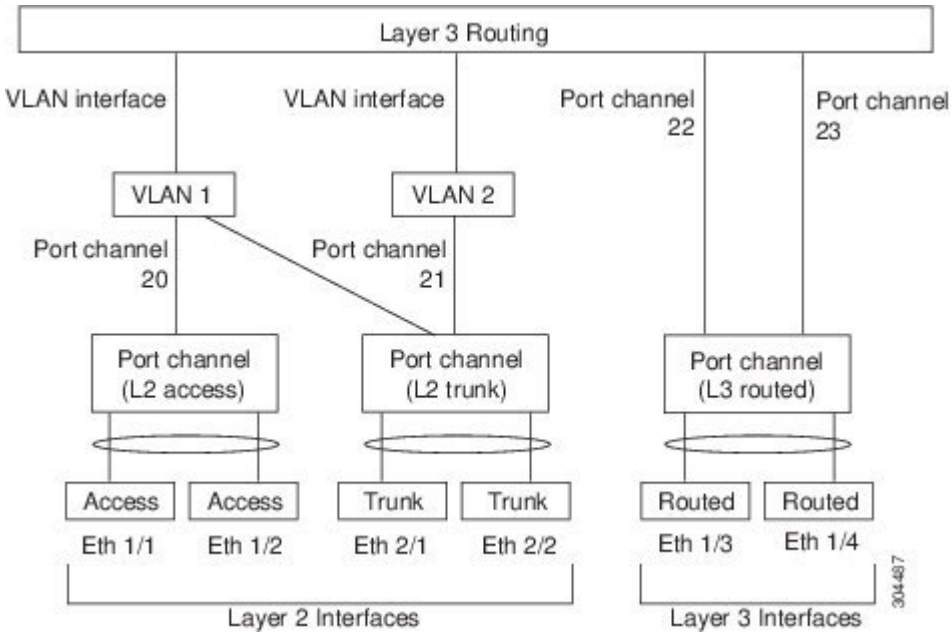
ポート チャネル インターフェイスを作成すると、ポート チャネルを直接作成できます。またはチャネル グループを作成して個別ポートをバンドルに集約させることができます。インターフェイスをチャネル グループに関連付けると、ポート チャネルがない場合は対応するポート チャネルが自動的に作成されます。この場合、ポート チャネルは最初のインターフェイスのレイヤ 2 またはレイヤ 3 設定を行います。最初にポート チャネルを作成することもできます。この場合は、Cisco NX-OS ソフトウェアがポート チャネルと同じチャネル番号の空のチャネル グループを作成してデフォルト レイヤ 2 またはレイヤ 3 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

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

ポートチャネル インターフェイス

次に、ポート チャネル インターフェイスを示します。

図 *8*：ポートチャネル インターフェイス



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

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

アクセス モードまたはトランク モードでのレイヤ 2 ポートの設定については、「レイヤ 2 インターフェイスの設定」の章を、レイヤ 3 インターフェイスおよびサブインターフェイスの設定については、「レイヤ 3 インターフェイスの設定」の章を参照してください。

Basic Settings

ポート チャネル インターフェイスには次の基本設定ができます。

- 帯域幅：この設定は情報目的で使用します。上位レベルプロトコルで使用されます。
- 遅延：この設定は情報目的で使用します。上位レベルプロトコルで使用されます。

- 説明
- Duplex
- IP アドレス
- 最大伝送単位（MTU）
- シャットダウン
- 速度

互換性要件

チャネル グループにインターフェイスを追加する場合、そのインターフェイスにチャネル グループとの互換性があるかどうかを確認するために、特定のインターフェイス属性がチェックされます。たとえば、レイヤ 2 チャネル グループにレイヤ 3 インターフェイスを追加できません。また Cisco NX-OS ソフトウェアは、インターフェイスがポート チャネル集約に参加することを許可する前に、そのインターフェイスの多数の動作属性もチェックします。

互換性チェックの対象となる動作属性は次のとおりです。

- ネットワーク層
- （リンク）速度性能
- 速度設定
- デュプレックス性能
- デュプレックス設定
- ポート モード
- アクセス VLAN
- トランク ネイティブ VLAN
- タグ付きまたは非タグ付き
- 許可 VLAN リスト
- MTU サイズ
- SPAN：SPAN の始点または宛先ポートは不可
- ストーム制御
- フロー制御性能
- フロー制御設定
- メディア タイプ、銅線またはファイバ

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

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

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

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

インターフェイスがポート チャネルに参加すると、一部のパラメータが削除され、ポート チャネルの値が次のように置き換わります。

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

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

- ビーコン
- 説明
- CDP
- LACP ポート プライオリティ

- デバウンス
- UDLD
- MDIX
- レート モード
- シャットダウン
- SNMP トラップ

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

ポート チャネル モードについては、「LACP マーカー レスポンダ」の項を参照してください。

ポート チャネルを使ったロード バランシング

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

ロード バランシング モードを設定して、デバイス全体に設定したすべてのポート チャネルに適用することができます。デバイス全体で 1 つのロード バランシング モードを設定できます。ポート チャネルごとにロード バランシング方式を設定することはできません。

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

レイヤ 3 インターフェイスのデフォルト ロード バランシング モードは、発信元および宛先 IP アドレスです。非 IP トラフィックのデフォルト ロード バランシング モードは、送信元および宛先 MAC アドレスです。チャネルグループ バンドルのインターフェイス間でロード バランシング方式を設定するには、**port-channel load-balance** コマンドを使用します。レイヤ 2 パケットのデフォルト方式は src-dst-mac です。レイヤ 3 パケットのデフォルト方式は src-dst-ip です。

次のいずれかの方式を使用するデバイスを設定し、ポートチャネル全体をロードバランシングできます。

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

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

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

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

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

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

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。

- src-dst ip
- src-dst ip-l4port

復元力のあるハッシュ

データセンターで使用される物理リンクの数が急増すると、障害物理リンクの数も増加する可能性があります。ポート チャネルまたは等コスト マルチパス（ECMP）グループのメンバー間でのフローのロードバランシングに使用される静的ハッシュ システムでは、各フローがリンクにハッシュされます。あるリンクで障害が発生すると、残りの現用リンク間ですべてのフローが再ハッシュされます。リンクへのフローのこの再ハッシュにより、障害リンクにハッシュされなかったフローであっても一部のパケットが間違った順序で配信されます。

この再ハッシュは、リンクがポート チャネルまたは等コスト マルチパス（ECMP）グループに追加された場合にも発生します。すべてのフローが、リンクの新しい番号全体にわたって再ハッシュされ、その結果として、一部のパケットが間違った順序で配信されます。復元力のあるハッシュは、ユニキャスト トラフィックだけをサポートします。

復元力のあるハッシュは、フローを物理ポートにマッピングします。リンクに障害が発生すると、障害リンクに割り当てられているフローは、現用リンク間で均等に再分配されます。現用リンクを通過する既存のフローは再ハッシュされず、それらのパケットは間違った順序で配信されません。

復元力のあるハッシュは、ECMP グループによってのみ、またポート チャネル インターフェイスでのみサポートされます。リンクがポート チャネルまたは ECMP グループに追加されると、既存のリンクにハッシュされるフローの一部が、既存のすべてのリンクにではなく、新しいリンクに再ハッシュされます。

復元力のあるハッシュは、IPv4 および IPv6 の既知のユニキャスト トラフィックをサポートしますが、IPv4 マルチキャスト トラフィックはサポートしません。

（注） 復元力のあるハッシュは、ネットワーク フォワーディング エンジン（NFE）ベースの Cisco Nexus 9300 シリーズ スイッチおよび Cisco Nexus 9500 シリーズ スイッチでサポートされています（NX-OS 7.0(3)I3(1) リリース以降）。

LACP

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

LACP の概要

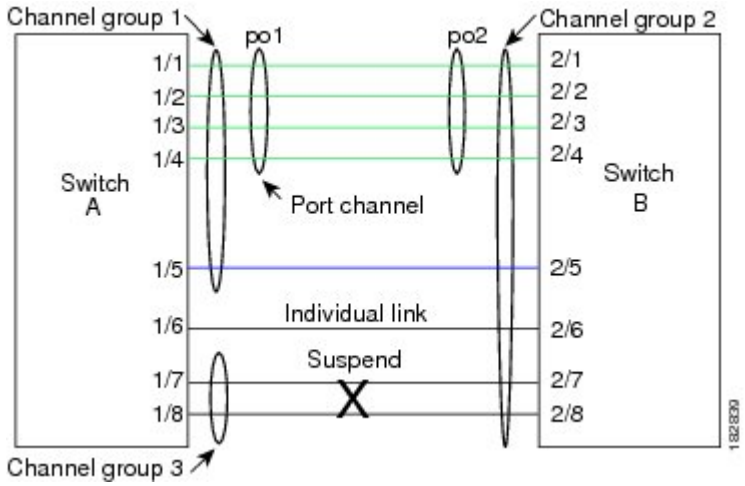
（注） LCAPは、使用する前にイネーブルにする必要があります。デフォルトでは、LACPはディセーブルです。

LACP のイネーブル化については、「LACP のイネーブル化」の項を参照してください。

システムはこの機能をディセーブルにする前のチェックポイントを自動的に取得するため、このチェックポイントにロールバックできます。ロールバックとチェックポイントの詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。

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

図 *9*：個々のリンクをポート チャネルに組み込む



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

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

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

ポートチャネル モード

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

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

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

次の図は、チャネル モードをまとめたものです。

表 *10*：ポート チャネルの個別リンクのチャネル モード

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

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

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

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

LACP ID パラメータ

ここでは、LACP パラメータについて説明します。

LACP システム プライオリティ

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

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

LACP Port Priority

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

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

LACP 管理キー

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

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

LACP マーカー レスポンダ

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

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

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

次の表に、LACP がイネーブルのポート チャネルとスタティック ポート チャネルの主な相違点を示します。

表 *11*：*LACP* がイネーブルのポート チャネルとスタティック ポート チャネル

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

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
チャネルを構成する最大リンク数	32	32

LACP 互換性の拡張

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

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

遅延 LACP

LACP ポートチャネルは、サーバとスイッチを接続すると、リンクの迅速なバンドルのために LACP PDU を交換します。ただし、PDU が受信されない場合は、リンクが中断状態になります。

7.0(3)I1(2) 以降では、遅延 LACP 機能により、LACP PDU の受信前に 1 つのポートチャネル メンバー（遅延 LACP ポート）がまず通常のポートチャネルのメンバーとしてアップできます。このメンバーが LACP モードで接続した後に、他のメンバー（補助 LACP ポート）がアップします。これにより、PDU が受信されない場合にリンクが中断状態になることが回避されます。

LACP ポート チャネルの最小リンクおよび MaxBundle

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

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

LACP ポート チャネルの最小リンク機能は次の処理を実行します。

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

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

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

LACP MaxBundle 機能では、次の処理が行われます。

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

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

LACP 高速タイマー

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

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

仮想化のサポート

メンバ ポートと他のポート チャネルに関連する設定は、ポート チャネルとメンバ ポートを持つ仮想デバイス コンテキスト（VDC）で設定します。各 VDC で 1 ～ 4096 の番号を使用してポート チャネルに番号を付けることができます。

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

（注） デフォルト VDC のポート チャネルを使用してロード バランシングを設定する必要があります。ロード バランシングの詳細については、「ポート チャネルを使用したロード バランシング」の項を参照してください。

ハイ アベイラビリティ

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

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

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

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

ポート チャネリングのライセンス要件

次の表に、この機能のライセンス要件を示します。

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

ポート チャネリングの前提条件

ポート チャネリングには次の前提条件があります。

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

注意事項と制約事項

ポート チャネリング設定時の注意事項および制約事項は、次のとおりです。

- **show** コマンドで **internal** キーワードを指定することは、サポートされていません。
- LACP ポートチャネルの最小リンクおよび maxbundle 機能は、ホスト インターフェイス ポート チャネルではサポートされていません。
- この機能を使用する前に LACP をイネーブルにする必要があります。
- デバイスに複数のポート チャネルを設定できます。
- 共有および専用ポートは同じポートチャネルに設定できません（共有ポートおよび専用ポートについては、「基本インターフェイス パラメータの設定」の章を参照）。
- レイヤ 2 ポート チャネルでは、ポートに互換性が設定されていれば、STP ポート パス コストが異なる場合でもポートチャネルを形成できます。互換性要件の詳細については、「互換性要件」の項を参照してください。
- STP では、ポートチャネルのコストはポート メンバーの集約帯域幅に基づきます。
- ポート チャネルを設定した場合、ポート チャネル インターフェイスに適用した設定はポートチャネル メンバ ポートに影響を与えます。メンバ ポートに適用した設定は、設定を適用したメンバ ポートにだけ影響します。
- LACP は半二重モードをサポートしません。LACP ポート チャネルの半二重ポートは中断ステートになります。
- ポート チャネル グループに属するポートはプライベート VLAN ポートとして設定しないでください。ポートがプライベート VLAN の設定に含まれている間は、そのポート チャネルの設定は非アクティブになります。
- チャネル 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。
- ポート チャネルは第 1 世代の 100G ライン カード（N9K-X9408PC-CFP2）または汎用拡張モジュール（N9K-M4PC-CFP2）ではサポートされていません。
- ポート チャネルは第 2 世代（以降）の 100G インターフェイスを備えたデバイスではサポートされています（7.0(3)I3(1) 以降）
- ポートチャネルは、Cisco Nexus 9300 および 9500 シリーズ デバイスのアプリケーション リーフ エンジン（ALE）アップリンク ポートに関する制約事項の影響を受ける可能性があります（ALE アップリンク ポートに関する制約事項 [英語]）。
- ポート チャネルの復元力のないハッシュは Cisco Nexus 9200 シリーズ スイッチではサポートされていません。
- Cisco NX-OS Release 7.0(3)I4(1) では、復元力のあるハッシュ（ポート チャネル ロードバランシング復元力）および VXLAN 設定は、ALE アップリンク ポートを使用した VTEP と互換性がありません。

（注） 復元力のあるハッシュはデフォルトではディセーブルになっています。

- ポートのサブインターフェイスの最大数は511です。サテライト/FEXポートのサブインターフェイスの最大数は 63 です。

デフォルト設定

次の表に、ポート チャネル パラメータのデフォルト設定を示します。

表 *12*：デフォルト ポート チャネル パラメータ

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

ポート チャネルの設定

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

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

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。関連するチャネル グループは自動的に作成されます。

（注） ポート チャネルがチャネル グループの前に作成されると、ポート チャネルは、メンバー インターフェイスが設定されるインターフェイス属性のすべてを使用して設定される必要があります。**switchport mode trunk** {*allowed vlanvlan-id* | *nativevlan-id*} コマンドを使用してメンバーを設定します。

これは、チャネル グループのメンバがレイヤ 2 ポート（switchport）およびトランク（switchport mode trunk）の場合にのみ必要です。

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

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

はじめる前に

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

手順の概要

1. **configure terminal**
2. **interface port-channel***channel-number*
3. **show port-channel summary**
4. **no shutdown**
5. **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***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。範囲は 1 ～ 4096 です。Cisco NX-OS ソフトウェアは、チャネル グループがない場合はそれを自動的に作成します。

ステップ 3	**show port-channel summary** 例： `switch(config-router)# show port-channel summary`	（任意）ポート チャネルに関する情報を表示します。

ステップ 4	**no shutdown**
	
	例：
	`switch# configure terminal`
	`switch(config)# int e3/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例は、ポート チャネルの作成方法を示しています。

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

ポート チャネルを削除したときにインターフェイス設定がどのように変わるかの詳細ついては、「互換性要件」の項を参照してください。

レイヤ 2 ポートをポート チャネルに追加

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

（注） **no channel-group** コマンドを使用して、チャネル グループからポートを削除します。

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

はじめる前に

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

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

手順の概要

1. **configure terminal**
2. **interface***typeslot/port*
3. **switchport**
4. **switchport mode trunk**
5. **switchport trunk** {**allowedvlan***vlan-id* | **native***vlan-id*}
6. **channel-group***channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]
7. **show interface***typeslot/port*
8. **no shutdown**
9. **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。

	コマンドまたはアクション	目的

ステップ 2	**interface***typeslot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		チャネル グループに追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**switchport** 例： `switch(config)# switchport`	インターフェイスをレイヤ 2 アクセス ポートとして設定します。
ステップ 4	**switchport mode trunk** 例： `switch(config)# switchport mode trunk`	（任意）インターフェイスをレイヤ 2 トランク ポートとして設定します。

ステップ 5	**switchport trunk** {**allowedvlan***vlan-id* | **native***vlan-id*}
	
	例：
	`switch(config)# switchport trunk native 3`
	`switch(config-if)#`
		（任意）レイヤ 2 トランク ポートに必要なパラメータを設定します。

ステップ 6	**channel-group***channel-number* [**force**] [**mode** {**on** | **active** | **passive**}] 例： • `switch(config-if)# channel-group 5` • `switch(config-if)# channel-group 5 force`	チャネル グループ内にポートを設定し、モードを設定します。channel-number の指定できる範囲は 1 ～ 4096 です。ポート チャネルがない場合は、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。すべてのスタティック ポート チャネル インターフェイスは、**on** モードに設定されます。すべての LACP 対応ポート チャネル インターフェイスを **active** または **passive** に設定する必要があります。デフォルト モードは **on** です。 （任意）一部の設定に互換性がないインターフェイスをチャネルに追加します。強制されるインターフェイスは、チャネル グループと同じ速度、デュプレックス、およびフロー制御設定を持っている必要があります。 （注） **force** オプションは、ポートにポート チャネルの他のメンバーとの QoS ポリシーの不一致がある場合に失敗します。
ステップ 7	**show interface***typeslot/port* 例： `switch# show interface port channel 5`	（任意）インターフェイスの内容を表示します。

	コマンドまたはアクション	目的

ステップ 8	**no shutdown**
	
	例：
	`switch# configure terminal`
	`switch(config)# int e3/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 9	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、レイヤ 2 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 5 に追加する例を示します。

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

レイヤ 3 ポートをポート チャネルに追加

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

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

（注） **no channel-group** コマンドを使用して、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。このポートの IP アドレスを再設定する必要があります。

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

はじめる前に

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

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

手順の概要

1. **configure terminal**
2. **interface***typeslot/port*
3. **no switchport**
4. **channel-group***channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]
5. **show interface***typeslot/port*
6. **no shutdown**
7. **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***typeslot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		チャネル グループに追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**no switchport** 例： `switch(config-if)# no switchport`	インターフェイスをレイヤ 3 ポートとして設定します。
ステップ 4	**channel-group***channel-number* [**force**] [**mode** {**on**	**active**	**passive**}] 例： • `switch(config-if)# channel-group 5` • `switch(config-if)# channel-group 5 force`	チャネル グループ内にポートを設定し、モードを設定します。channel-number の指定できる範囲は 1 ～ 4096 です。ポート チャネルがない場合は、このチャネル グループに関連付けられたポート チャネルが作成されます。 （任意）一部の設定に互換性がないインターフェイスをチャネルに追加します。強制されるインターフェイスは、チャネル グループと同じ速度、デュプレックス、およびフロー制御設定を持っている必要があります。
ステップ 5	**show interface***typeslot/port* 例： `switch# show interface ethernet 1/4`	（任意）インターフェイスの内容を表示します。

	コマンドまたはアクション	目的

ステップ 6	**no shutdown**
	
	例：
	`switch# configure terminal`
	`switch(config)# int e3/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

```
switch# configure terminal
switch (config)# interface ethernet 1/5
switch(config-if)# switchport
switch(config-if)# channel-group 6
```

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

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

情報目的としての帯域幅および遅延の設定

ポート チャネルの帯域幅は、チャネル内のアクティブ リンクの合計数によって決定されます。

情報目的でポート チャネル インターフェイスに帯域幅および遅延を設定します。

手順の概要

1. **configure terminal**
2. **interface port-channel***channel-number*
3. **bandwidth***value*
4. **delay***value*
5. **exit**
6. **show interface port-channel***channel-number*
7. **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***channel-number*
	
	例：
	`switch(config)# interface port-channel 2`
	`switch(config-if)#`
		設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**bandwidth***value*
	
	例：
	`switch(config-if)# bandwidth 60000000`
	`switch(config-if)#`
		情報目的で使用される帯域幅を指定します。有効な範囲は 1 ～ 3,200,000,000 kbs です。デフォルト値はチャネル グループのアクティブ インターフェイスの合計によって異なります。

ステップ 4	**delay***value*
	
	例：
	`switch(config-if)# delay 10000`
	`switch(config-if)#`
		情報目的で使用されるスループット遅延を指定します。範囲は、1 ～ 16,777,215（10 マイクロ秒単位）です。デフォルト値は 10 マイクロ秒です。

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了し、コンフィギュレーション モードに戻ります。

ステップ 6	**show interface port-channel***channel-number* 例： `switch# show interface port-channel 2`	（任意）指定したポート チャネルのインターフェイス情報を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

ポート チャネル インターフェイスのシャットダウンと再起動

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

手順の概要

1. **configure terminal**
2. **interface port-channel***channel-number*
3. シャットダウン
4. **exit**
5. **show interface port-channel***channel-number*
6. **no shutdown**
7. **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***channel-number*
	
	例：
	`switch(config)# interface port-channel 2`
	`switch(config-if)#`
		設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	シャットダウン
	
	例：
	`switch(config-if)# shutdown`
	`switch(config-if)#`
		インターフェイスをシャットダウンします。トラフィックは通過せず、インターフェイスは管理ダウン状態になります。デフォルトはシャットダウンなしです。
		（注） インターフェイスを開くには、**no shutdown** コマンドを使用します。
		インターフェイスは管理アップとなります。操作上の問題がなければ、トラフィックが通過します。デフォルトはシャットダウンなしです。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了し、コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show interface port-channel***channel-number* 例： `switch(config-router)# show interface port-channel 2`	（任意）指定したポート チャネルのインターフェイス情報を表示します。

ステップ 6	**no shutdown**
	
	例：
	`switch# configure terminal`
	`switch(config)# int e3/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、ポート チャネル 2 のインターフェイスをアップする例を示します。

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

ポート チャネルの説明の設定

ポート チャネルの説明を設定できます。

手順の概要

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

ステップ 3	**説明**
	
	例：
	`switch(config-if)# description engineering`
	`switch(config-if)#`
		ポート チャネル インターフェイスに説明を追加できます。説明に80文字まで使用できます。デフォルトでは、説明は表示されません。このパラメータを設定してから、出力に説明を表示する必要があります。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了し、コンフィギュレーション モードに戻ります。

ステップ 5	**show interface port-channel***channel-number* 例： `switch# show interface port-channel 2`	（任意）指定したポート チャネルのインターフェイス情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、ポート チャネル 2 に説明を追加する例を示します。

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

ポート チャネル インターフェイスへの速度とデュプレックスの設定

ポート チャネル インターフェイスに速度とデュプレックスを設定できます。

手順の概要

1. **configure terminal**
2. **interface port-channel***channel-number*
3. **speed** {**10** | **100** | **1000** | **auto**}
4. **duplex** {**auto** | **full** | **half**}
5. **exit**
6. **show interface port-channel***channel-number*
7. **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***channel-number*
	
	例：
	`switch(config)# interface port-channel 2`
	`switch(config-if)#`
		設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**speed** {**10**	**100**	**1000**	**auto**}
				
				例：
				`switch(config-if)# speed auto`
				`switch(config-if)#`
					ポートチャネル インターフェイスの速度を設定します。デフォルトの自動ネゴシエーションは自動です。

ステップ 4	**duplex** {**auto**	**full**	**half**}
			
			例：
			`switch(config-if)# speed auto`
			`switch(config-if)#`
				ポート チャネル インターフェイスのデュプレックスを設定します。デフォルトの自動ネゴシエーションは自動です。

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了し、コンフィギュレーション モードに戻ります。

ステップ 6	**show interface port-channel***channel-number* 例： `switch# show interface port-channel 2`	（任意）指定したポート チャネルのインターフェイス情報を表示します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、ポート チャネル 2 に 100 Mb/s を設定する例を示します。

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

ポート チャネルを使ったロード バランシングの設定

VDC アソシエーションにかかわらず、ポート チャネルのロードバランシング アルゴリズムを設定し、デバイス全体に適用できます。

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

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

はじめる前に

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

手順の概要

1. **configure terminal**
2. **port-channelload-balance***method* {**dst ip** | **dst ip-gre** | **dst ip-l4port** | **dst ip-l4port-vlan** | **dst ip-vlan** | **dst l4port** | **dst mac** | **src ip** | **src ip-gre** | **src ip-l4port** | **src ip-l4port-vlan** | **src ip-vlan** | **src l4port** | **src mac** | **src-dst ip** | **src-dst ip-gre** | **src-dst ip-l4port** [**symmetric**] | **src-dst ip-l4port-vlan** | **src-dst ip-vlan** | **src-dst l4port** | **src-dst mac**} [**fex** {*fex-range* | *all*}] [**rotate***rotate*]
3. **show port-channel load-balance**
4. **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	**port-channelload-balance***method* {**dst ip** | **dst ip-gre** | **dst ip-l4port** | **dst ip-l4port-vlan** | **dst ip-vlan** | **dst l4port** | **dst mac** | **src ip** | **src ip-gre** | **src ip-l4port** | **src ip-l4port-vlan** | **src ip-vlan** | **src l4port** | **src mac** | **src-dst ip** | **src-dst ip-gre** | **src-dst ip-l4port** [**symmetric**] | **src-dst ip-l4port-vlan** | **src-dst ip-vlan** | **src-dst l4port** | **src-dst mac**} [**fex** {*fex-range* | *all*}] [**rotate***rotate*] 例： • `switch(config)# port-channel load-balance src-dst mac` `switch(config)#` • `switch(config)# no port-channel load-balance src-dst mac` `switch(config)#`	デバイスのロードバランシング アルゴリズムを指定します。指定可能なアルゴリズムはデバイスによって異なります。レイヤ 3 のデフォルトは IPv4 と IPv6 の両方で **src-dst ip** で、非 IP のデフォルトは **src-dst mac** です。 （注） 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。 • src-dst ip • src-dst ip-l4port
ステップ 3	**show port-channel load-balance** 例： `switch(config-router)# show port-channel load-balance`	（任意）ポート チャネル ロード バランシング アルゴリズムを表示します。
ステップ 4	**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。

LACP のイネーブル化

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

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

LACP を設定する手順は次のとおりです。

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

手順の概要

1. **configure terminal**
2. **feature lacp**
3. **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	**feature lacp** 例： `switch(config)# feature lacp`	デバイスの LACP をイネーブルにします。
ステップ 3	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、LACP をイネーブルにする例を示します。

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

LACP ポート チャネル ポート モードの設定

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

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

手順の概要

1. **configure terminal**
2. **interface***typeslot/port*
3. **channel-group***number***mode** {**active** | **on** | **passive**}
4. **show port-channel summary**
5. **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***typeslot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		チャネル グループに追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**channel-group***number***mode** {**active** | **on** | **passive**} 例： `switch(config-if)# channel-group 5 mode active`	ポート チャネルのリンクのポート モードを指定します。LACP をイネーブルにしたら、各リンクまたはチャネル全体を active または passive に設定します。 関連する集約プロトコルを使用せずにポート チャネルを実行する場合、ポートチャネル モードは常に on です。 デフォルト ポート チャネル モードは **on** です。
ステップ 4	**show port-channel summary** 例： `switch(config-if)# show port-channel summary`	（任意）ポート チャネルの概要を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

LACP ポート チャネル最少リンク数の設定

LACP の最小リンク機能を設定できます。最小リンクと 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最小リンク設定を復元するには、**no lacp min-links** コマンドを使用します。

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

はじめる前に

適切なポートチャネル インターフェイスであることを確認します。

手順の概要

1. **configure terminal**
2. **interface port-channel***number*
3. **lacp min-links***number*
4. **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指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**lacp min-links***number* 例： `switch(config-if)# lacp min-links 3`	ポート チャネル インターフェイスを指定して、最小リンクの数を設定します。指定できる範囲は 1 ～ 16 です。
ステップ 4	**show running-config interface port-channel***number* 例： `switch(config-if)# show running-config interface port-channel 3`	（任意）ポート チャネル最小リンク設定を表示します。

次に、アップ/アクティブにするポート チャネルに関して、アップ/アクティブにするポート チャネル メンバー インターフェイスの最小数を設定する例を示します。

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

LACP ポートチャネル MaxBundle の設定

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

（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。

はじめる前に

適切なポートチャネル インターフェイスであることを確認します。

手順の概要

1. **configure terminal**
2. **interface port-channel***number*
3. **lacp max-bundle***number*
4. **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指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**lacp max-bundle***number* 例： `switch(config-if)# lacp max-bundle`	ポートチャネル インターフェイスを指定して max-bundle を設定します。 ポート チャネルの max-bundle のデフォルト値は 16 です。指定できる範囲は 1 ～ 32 です。 （注） デフォルト値は 16 ですが、ポート チャネルのアクティブ メンバ数は、pc_max_links_config およびポートチャネルで許可されている pc_max_active_members の最小数です。
ステップ 4	**show running-config interface port-channel***number* 例： `switch(config-if)# show running-config interface port-channel 3`	（任意）ポートチャネル max-bundle 設定を表示します。

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

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

LACP 高速タイマー レートの設定

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

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

はじめる前に

LACP 機能がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface***typeslot/port*
3. **lacp rate fast**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**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***typeslot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定するインターフェイスを指定します。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	**lacp rate fast** 例： `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。 タイムアウト レートをデフォルトにリセットするには、コマンドの **no** 形式を使用します。

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

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

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

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

LACP システム プライオリティの設定

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

はじめる前に

LACP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **lacp system-priority***priority*
3. **show lacp system-identifier**
4. **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	**lacp system-priority***priority* 例： `switch(config)# lacp system-priority 40000`	LACP で使用するシステム プライオリティを設定します。指定できる範囲は 1 ～ 65535 で、値が大きいほどプライオリティは低くなります。デフォルト値は 32768 です。 （注） VDC ごとに LACP システム ID が異なります。これは、この設定値に MAC アドレスが追加されるためです。
ステップ 3	**show lacp system-identifier** 例： `switch(config-if)# show lacp system-identifier`	（任意）LACP システム識別子を表示します。

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

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

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

LACP ポート プライオリティの設定

LACP をイネーブルにしたら、ポート プライオリティの LACP ポート チャネルにそれぞれのリンクを設定できます。

はじめる前に

LACP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface***typeslot/port*
3. **lacp port-priority***priority*
4. **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***typeslot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		チャネル グループに追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**lacp port-priority***priority* 例： `switch(config-if)# lacp port-priority 40000`	LACP で使用するポート プライオリティを設定します。指定できる範囲は 1 ～ 65535 で、値が大きいほどプライオリティは低くなります。デフォルト値は 32768 です。
ステップ 4	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、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。

はじめる前に

LACP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface port-channel***number*
3. シャットダウン
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	**シャットダウン** 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。

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. シャットダウン
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	シャットダウン 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。

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

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

LACP の個別一時停止のディセーブル化

ポートがピアから LACP PDU を受信しない場合、LACP はポートを中断ステートに設定します。このプロセスによって、サーバの中には起動に失敗するものがあります。そのようなサーバは、LACP が論理的にポートを稼動状態にしていることを必要とするからです。

（注） エッジ ポートで **lacp suspend-individual** コマンドを入力するだけです。このコマンドを使用する前に、ポート チャネルが管理ダウン状態である必要があります。

はじめる前に

LACP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface port-channel***number*
3. シャットダウン
4. **no lacp suspend-individual**
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。

	コマンドまたはアクション	目的
ステップ 3	シャットダウン 例： `switch(config-if) shutdown`	ポート チャネルを管理シャットダウンします。
ステップ 4	**no lacp suspend-individual** 例： `switch(config-if)# no lacp suspend-individual`	ポート チャネルで LACP 個別ポートの一時停止動作をディセーブルにします。
ステップ 5	**no shutdown** 例： `switch(config-if) no shutdown`	ポート チャネルを管理アップします。
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。

次に、ポート チャネルで LACP 個別ポートの一時停止をディセーブルにする方法を示します。

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

LACP の個別一時停止の再イネーブル化

デフォルトの LACP 個別ポートの一時停止を再度イネーブルにできます。

手順の概要

1. **configure terminal**
2. **interface port-channel***number*
3. シャットダウン
4. **lacp suspend-individual**
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	シャットダウン 例： `switch(config-if) shutdown`	ポート チャネルを管理シャットダウンします。
ステップ 4	**lacp suspend-individual** 例： `switch(config-if)# lacp suspend-individual`	ポート チャネルで LACP 個別ポートの一時停止動作をイネーブルにします。
ステップ 5	**no shutdown** 例： `switch(config-if) no shutdown`	ポート チャネルを管理アップします。
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。

次に、ポート チャネルで LACP 個別ポートの一時停止を再度イネーブルにする方法を示します。

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

遅延 LACP の設定

遅延 LACP を設定するには、**lacp mode delay** コマンドを使用し、その後に LACP ポート プライオリティを設定します（7.0(3)I1(2) 以降）。

（注） vPC の場合は、両方の vPC スイッチで遅延 LACP を有効にする必要があります。

（注） 遅延 LACP は、レイヤ 3 ポート チャネル、FEX モジュール、または Cisco Nexus 9500 シリーズ スイッチではサポートされていません。

（注） vPC の場合、プライマリ スイッチに遅延 LACP ポートがあり、プライマリ スイッチが起動できないときは、動作上のプライマリ スイッチの遅延 LACP ポートチャネルで vPC 設定を削除し、新しいポートのポートチャネルをフラップして既存のポートチャネルの遅延 LACP ポートとして選択されるようにする必要があります。

（注） **no lacp suspend-individual** と遅延 LACP 機能が同じポートで設定されている場合、そのポートに属している非遅延 LACP ポートは個別の状態になります。LACP が確立されると、メンバーはアップ状態に移行します。

ベスト プラクティスとして、同じポートで **no lacp suspend-individual** を遅延 LACP 機能とともに使用しないでください。

手順の概要

1. **configure terminal**
2. **interface port-channel***number*
3. **lacp mode 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	**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 port-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。
ステップ 3	**lacp mode delay**	遅延 LACP を有効にします。 （注） 遅延 LACP を無効にするには、**no lacp mode delay** コマンドを使用します。 LACP ポート プライオリティを設定して、遅延 LACP の設定を完了します。詳細については、「LACP ポート プライオリティの設定」の項を参照してください。

	コマンドまたはアクション	目的
		LACP ポート プライオリティにより、遅延 LACP ポートの選択が決定されます。最も小さい数値のプライオリティを持つポートが選択されます。 複数のポートが最優先のプライオリティを持つ場合は、使用する vPC を決定するために VDC システムの MAC アドレスが使用されます。その後、非 vPC スイッチまたは選択された vPC スイッチ内で最小のイーサネット ポート名を持つポートが使用されます。 遅延 LACP 機能が設定してされており、ポート チャネル フラップによって有効になっている場合、遅延LACPポートは通常のポートチャネルとして動作し、サーバとスイッチの間でのデータの交換を可能にします。最初の LACP PDU を受信すると、遅延 LACP ポートは通常のポート メンバーから LACP ポート メンバーに移行します。 （注） スイッチまたはリモート サーバでポート チャネルがフラップするまでは、遅延 LACP ポートの選択は完全または有効化しません。

次に、遅延 LACP を設定する例を示します。

```
switch# config terminal
switch(config)# interface po 1
switch(config-if)# lacp mode delay


switch# config terminal
switch(config)# interface ethernet 1/1
switch(config-if)# lacp port-priority 1
switch(config-if)# channel-group 1 mode active
```

次に、遅延 LACP を無効にする例を示します。

```
switch# config terminal
switch(config)# interface po 1
switch(config-if)# no lacp mode delay
```

ポート チャネル ハッシュ分散の設定

Cisco NX-OS は、グローバル レベルとポートチャネル レベルの両方でアダプティブおよび固定のハッシュ分散の設定をサポートしています。このオプションは、メンバがアップまたはダウンしたときに Result Bundle Hash（RBH）分散の変化を最小限に抑えることにより、トラフィックの中断を最小限に抑えます。このため、変化のない RBH 値にマッピングされているフローが同じリンクを流れ続けるようになります。ポートチャネル レベルの設定はグローバル設定よりも優先されます。デフォルト設定はグローバルに適応し、各ポートチャネルの設定がないので、ISSU 中に変更はありません。コマンドが適用されたときにポートはフラップされず、設定は次のメンバー リンクの変更イベントで有効になります。どちらのモードも RBH モジュールまたは非モジュール スキームで動作します。

この機能がサポートされない下位バージョンへの ISSD 時には、固定モード コマンドがグローバルに使用されている場合や、ポートチャネル レベルの設定がある場合は、この機能を無効にする必要があります。

グローバル レベルでのポート チャネル ハッシュ分散の設定

手順の概要

1. **configure terminal**
2. **no port-channel hash-distribution** {**adaptive** | **fixed**}
3. **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	**no port-channel hash-distribution** {**adaptive**	**fixed**}
		
		例：
		`switch(config)# port-channel hash-distribution adaptive`
		`switch(config)#`
			グローバル レベルでポート チャネル ハッシュ分散を指定します。
			デフォルトはアダプティブ モードです。
			コマンドは、次のメンバー リンク イベント（link down/up/no shutdown/shutdown）まで有効になりません。（`Do you still want to continue(y/n)? [yes]`）

ステップ 3	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、グローバル レベルでハッシュ分散を設定する例を示します。

```
switch# configure terminal
switch(config)# no port-channel hash-distribution fixed
```

ポート チャネル レベルでのポート チャネル ハッシュ分散の設定

手順の概要

1. **configure terminal**
2. **interface port-channel** {*channel-number* | *range*}
3. **no port-channel port hash-distribution** {**adaptive** | **fixed**}
4. **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** {*channel-number*	*range*}
		
		例：
		`switch# interface port-channel 4`
		`switch(config-if)#`
			設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**no port-channel port hash-distribution** {**adaptive**	**fixed**}
		
		例：
		`switch(config-if)# port-channel port hash-distribution adaptive`
		`switch(config-if)`
			ポート チャネル レベルでポート チャネル ハッシュ分散を指定します。
			デフォルトはありません。
			コマンドは、次のメンバー リンク イベント（link down/up/no shutdown/shutdown）まで有効になりません。（`Do you still want to continue(y/n)? [yes]`）

ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、グローバル レベル コマンドとしてハッシュ分散を設定する例を示します。

```
switch# configure terminal
switch(config)# no port-channel hash-distribution fixed
```

ポートチャネル設定の確認

ポート チャネルの設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show interface port-channel*channel-number*	ポート チャネル インターフェイスのステータスを表示します。
show feature	イネーブルにされた機能を表示します。
load- interval {**interval***seconds* {**1** | **2** | **3**}}	ビットレートとパケットレートの統計情報に対して 3 つの異なるサンプリング間隔を設定します。
show port-channel compatibility-parameters	ポート チャネルに追加するためにメンバ ポート間で同じにするパラメータを表示します。
show port-channel database [**interface port-channel***channel-number*]	1 つ以上のポートチャネルインターフェイスの集約状態を表示します。
show port-channel load-balance	ポート チャネルで使用するロード バランシングのタイプを表示します。
show port-channel summary	ポート チャネル インターフェイスのサマリーを表示します。
show port-channel traffic	ポートチャネルのトラフィック統計情報を表示します。
show port-channel usage	使用済みおよび未使用のチャネル番号の範囲を表示します。
show lacp {**counters** [**interface port-channel***channel-number*] | [**interface***type/slot*] | **neighbor** [**interface port-channel***channel-number*] | **port-channel** [**interface port-channel***channel-number*] | **system-identifier**]]}	LACP に関する情報を表示します。
show running-config interface port-channel*channel-number*	ポートチャネルの実行コンフィギュレーションに関する情報を表示します。

ポート チャネル インターフェイス コンフィギュレーションのモニタリング

次のコマンドを使用すると、ポートチャネルインターフェイス構成情報を表示することができます。

コマンド	目的
clear counters interface port-channel*channel-number*	カウンタをクリアします。
clear lacp counters [**interface port-channel***channel-number*]	LACP カウンタをクリアします。
load- interval {**interval***seconds* {**1** | **2** | **3**}}	ビットレートとパケットレートの統計情報に対して 3 つの異なるサンプリング間隔を設定します。
show interface counters [**module***module*]	入力および出力オクテットユニキャストパケット、マルチキャストパケット、ブロードキャスト パケットを表示します。
show interface counters detailed [**all**]	入力パケット、バイト、マルチキャストおよび出力パケット、バイトを表示します。
show interface counters errors [**module***module*]	エラー パケットの数を表示します。
show lacp counters	LACP の統計情報を表示します。

ポート チャネルの設定例

次に、LACP ポート チャネルを作成し、そのポート チャネルに 2 つのレイヤ 2 インターフェイスを追加する例を示します。

```
switch# configure terminal
switch (config)# feature lacp
switch (config)# interface port-channel 5
switch (config-if)# interface ethernet 1/4
switch(config-if)# switchport
switch(config-if)# channel-group 5 mode active
switch(config-if)# lacp port priority 40000
switch(config-if)# interface ethernet 1/7
switch(config-if)# switchport
switch(config-if)# channel-group 5 mode
```

次に、チャネル グループに 2 つのレイヤ 3 インターフェイスを追加する例を示します。Cisco NX-OS ソフトウェアはポート チャネルを自動的に作成します。

```
switch# configure terminal
switch (config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# no ip address
switch(config-if)# channel-group 6 mode active
switch (config)# interface ethernet 2/5
switch(config-if)# no switchport
switch(config-if)# no ip address
switch(config-if)# channel-group 6 mode active
```

```
switch (config)# interface port-channel 6
switch(config-if)# ip address 192.0.2.1/8
```

関連資料

関連項目	マニュアル タイトル
システム管理	『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』
ハイ アベイラビリティ	『*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*』
ライセンス	『*Cisco NX-OS Licensing Guide*』

第 8 章

vPC の設定

この章では、Cisco NX-OS デバイス上で仮想ポート チャネル（vPC）を設定する方法を説明します。

vPC ピア リンクに Nexus 9000 デバイスの任意のインターフェイスを使用できます。

ポート チャネルの互換性パラメータは、物理スイッチのすべてのポート チャネル メンバーで同じである必要があります。

vPC の一部になるように共有インターフェイスを設定できません。

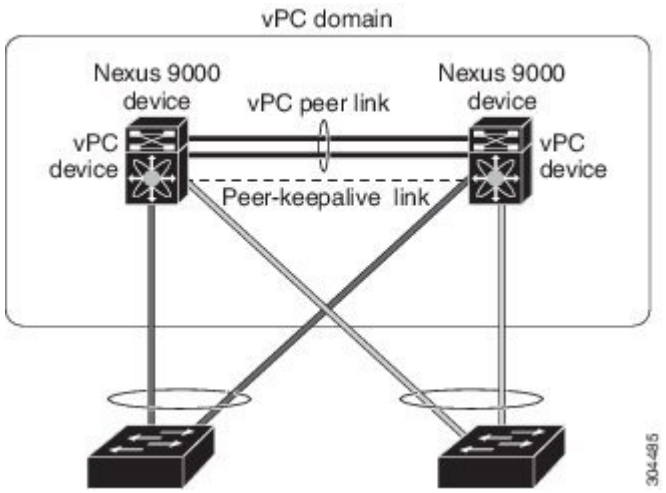
（注） ポート チャネルの互換性パラメータは、両方のピアのすべての vPC メンバ ポートでも同じでなければならないので、シャーシごとに同じタイプのモジュールを使用する必要があります。

vPC について

vPC の概要

仮想ポート チャネル（vPC）は、物理的には 2 台の異なる Cisco Nexus 9000 シリーズ デバイスに接続されているリンクを、第3のデバイスには単一のポートに見えるようにします（図を参照）。第 3 のデバイスは、スイッチ、サーバ、ポート チャネルをサポートするその他の任意のネットワーキング デバイスのいずれでもかまいません。vPC は、ノード間の複数の並列パスを可能にし、トラフィックのロード バランシングを可能にすることによって、冗長性を作り、バイセクショナルな帯域幅を増やすレイヤ 2 マルチパスを提供できます。

図 *10*：*vPC* のアーキテクチャ



vPC で使用できるのは、レイヤ 2 ポート チャネルだけです。vPC ドメインは単一の仮想デバイス コンテキスト（VDC）に関連付けられるため、同じ 1 つの vPC ドメインに所属するすべての vPC インターフェイスが同一 VDC 内で定義されていなければなりません。

ポート チャネルの設定は、次のいずれかを使用して行います。

- プロトコルなし
- リンク集約制御プロトコル（LACP）

LACP を使用せずに vPC（vPC ピア リンク チャネルも含めて）のポート チャネルを設定する場合は、各デバイスが、単一のポート チャネル内に最大 8 つのアクティブ リンクを持てます。LACP を使用して vPC（vPC ピア リンク チャネルも含めて）のポート チャネルを設定する場合は、各デバイスが、単一のポート チャネル内に 8 つのアクティブ リンクと 8 つのスタンバイ リンクを持つことができます（LACP と vPC の使用の詳細については、「その他の機能との vPC の相互作用」の項を参照）。

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

システムはこの機能をディセーブルにする前のチェックポイントを自動的に取得するため、このチェックポイントにロールバックできます。

vPC 機能をイネーブルにしたら、ピアキープアライブ リンクを作成します。このリンクは、2 つの vPC ピア デバイス間でのハートビート メッセージの送信を行います。

2 つ以上の 10 ギガビット イーサネット ポートまたは 40 ギガビット イーサネット ポートを使用することにより、1 台の Cisco Nexus 9000 シリーズ シャーシでポート チャネルを設定して vPC ピア リンクを作成できます。vPC をイネーブルにして実行するための正しいハードウェアが揃っていることを確認にするには **show hardware feature-capability** コマンドを入力します。コマンド出力で vPC の向かいに X が表示されている場合、そのハードウェアでは vPC 機能をイネーブルにできません。

vPC ピア リンク レイヤ 2 ポート チャネルは、トランクとして設定することを推奨します。もう 1 つの Cisco Nexus 9000 シリーズ シャーシで、再度 2 つ以上の 10 ギガビット イーサネット ポートまたは 40 ギガビット イーサネット ポートを専用モードで使用して、もう 1 つのポート チャネルを設定します。これらの 2 つのポート チャネルを接続すると、リンクされた 2 つの Cisco Nexus デバイスが第 3 のデバイスには 1 つのデバイスとして見える vPC ピア リンクが作成されます。第 3 のデバイス、またはダウンストリーム デバイスは、スイッチ、サーバ、vPC に接続された正規のポートチャネルを使用するその他の任意のネットワーキングデバイスのいずれでもかまいません。正しいモジュールを使用していないと、システムからエラー メッセージが表示されます。

異なるモジュールの専用ポート上で vPC ピア リンクを設定して、障害発生の可能性を下げることをお勧めします。復元力を最適にしたい環境では、少なくとも 2 つのモジュールを使用してください。

すべての vPC ピア リンクおよびコアに面したインターフェイスを 1 つのモジュール上で設定しなければならない場合、コアへのレイヤ 3 リンクに関連付けられているトラック オブジェクトおよび両方の vPC ピア デバイス上の vPC ピア リンク上のすべてのリンクを設定してください。いったんこの機能を設定したら、プライマリ vPC ピア デバイスに障害が発生した場合には、プライマリ vPC ピア デバイス上のすべての vPC リンクを、システムが自動的に停止します。システムが安定するまでは、このアクションにより、すべての vPC トラフィックが強制的にセカンダリ vPC ピア デバイスに送られます。

トラック オブジェクトを作成し、コアおよび vPC ピア リンクに接続されているプライマリ vPC ピア デバイス上のすべてのリンクにそのオブジェクトを適用できます。**track interface** コマンドに関する詳細情報については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

vPC ドメインには、両方の vPC ピア デバイス、vPC ピアキープアライブ リンク、vPC ピア リンク、および vPC ドメイン内にあってダウンストリーム デバイスに接続されているすべてのポート チャネルが含まれます。各デバイスに設定できる vPC ドメイン ID は、1 つだけです。

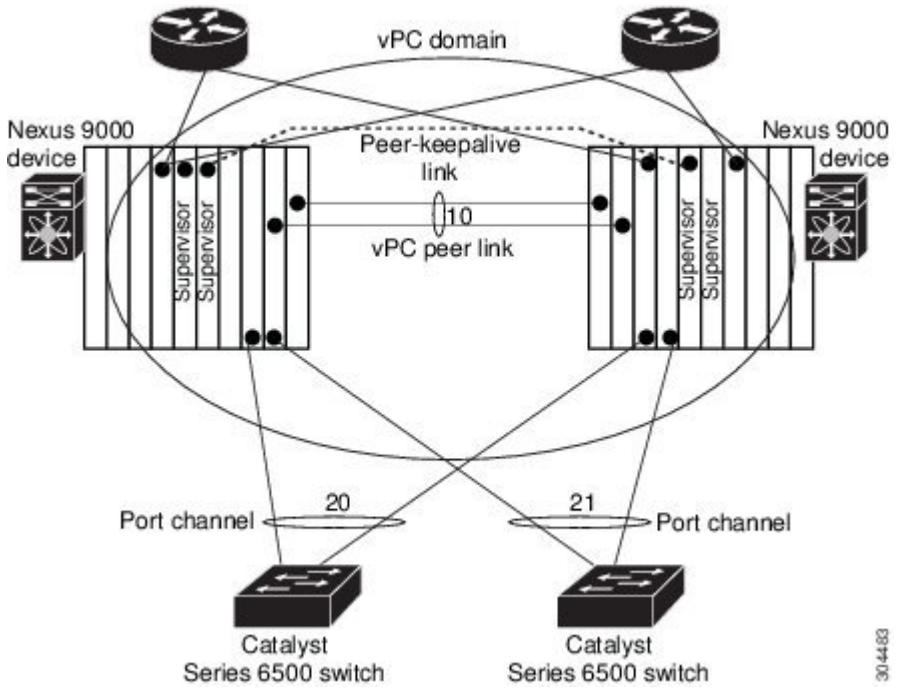
このバージョンでは、各ダウンストリームデバイスを、単一のポートチャネルを使用して単一の vPC ドメイン ID に接続できます。

（注） 常にすべての vPC デバイスを両方の vPC ピア デバイスに、ポート チャネルを使用して接続してください。

vPC（図を参照）には、次の利点があります。

- 単一のデバイスが 2 つのアップストリーム デバイスを介して 1 つのポート チャネルを使用することを可能にします。
- スパニングツリー プロトコル（STP）のブロック ポートが不要になります。
- ループフリーなトポロジが実現されます。
- 利用可能なすべてのアップリンク帯域幅を使用します。
- リンクまたはデバイスに障害が発生した場合に、ファースト コンバージェンスを提供します。
- リンクレベルの復元力を提供します。
- ハイ アベイラビリティが保証されます。

図 *11*：*1* つの *VDC* 内の *vPC* インターフェイス



vPC の用語

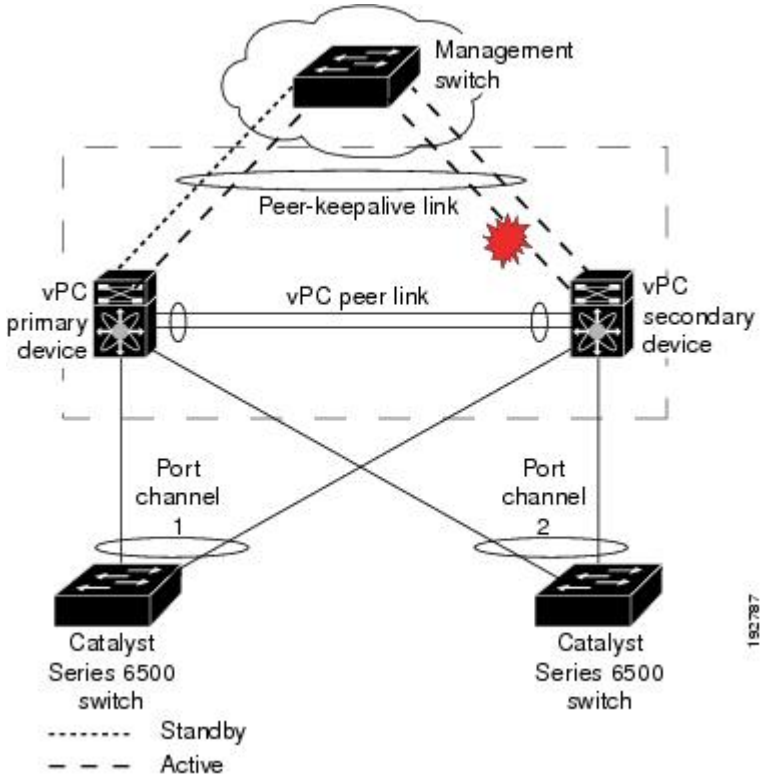
vPC で使用される用語は、次のとおりです。

- vPC：vPC ピア デバイスとダウンストリーム デバイスの間の結合されたポート チャネル。
- vPC ピア デバイス：vPC ピア リンクと呼ばれる特殊なポート チャネルで接続されている一対のデバイスの 1 つ。
- vPC ピア リンク：vPC ピア デバイス間の状態を同期するために使用されるリンク。両エンドが 10 ギガバイト イーサネットまたは 40 ギガビット イーサネット インターフェイス上になくてはなりません。
- vPC メンバ ポート：vPC に属するインターフェイス。
- ホスト vPC ポート：vPC に属するファブリック エクステンダのホスト インターフェイス。
- vPC ドメイン：このドメインには、両方の vPC ピア デバイス、vPC ピアキープアライブ リンク、vPC 内にあってダウンストリーム デバイスに接続されているすべてのポート チャネルが含まれます。また、このドメインは、vPC グローバル パラメータを割り当てるために使用する必要があるコンフィギュレーション モードに関連付けられています。
- vPC ピアキープアライブ リンク：ピアキープアライブ リンクは、さまざまな vPC ピア Cisco Nexus 9000 シリーズのデバイスをモニタします。ピアキープアライブ リンクは、vPC ピア デバイス間での設定可能なキープアライブ メッセージの定期的な送信を行います。

  ピアキープアライブ リンクを、各 vPC ピア デバイス内のレイヤ 3 インターフェイスにマッピングされている独立した仮想ルーティングおよび転送（VRF）インスタンスに関連付けることを推奨します。独立した VRF を設定しなかった場合は、デフォルトで管理 VRF が使用されます。ただし、ピアキープアライブ リンクに管理インターフェイスを使用する場合は、

各 vPC ピア デバイスのアクティブ管理ポートとスタンバイ管理ポートの両方に接続した管理スイッチを置く必要があります（図を参照）。

図 *12* : *vPC* ピアキープアライブ リンクの管理ポートを接続するための独立したスイッチが必要



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

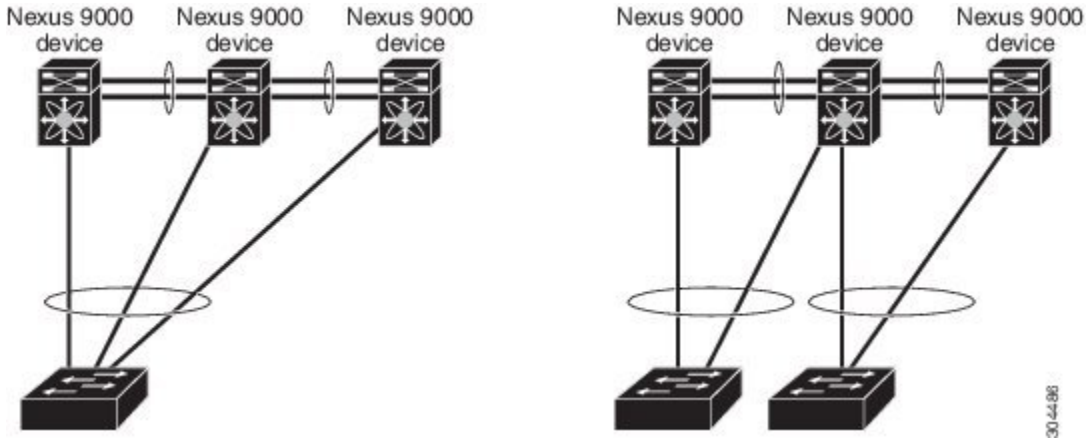
- vPC メンバ ポート：vPC に属するインターフェイス。
- デュアルアクティブ：プライマリとして動作する両方の vPC ピア。この状況は、両方のピアがまだアクティブなときにピアキープアライブとピア リンクがダウンした場合に発生します。この場合、セカンダリ vPC はプライマリ vPC が動作しないと想定し、プライマリ vPC として機能します。
- リカバリ：ピアキープアライブとピア リンクが起動すると、1 台のスイッチがセカンダリ vPC になります。セカンダリ vPC になるスイッチで、vPC リンクが停止してから復帰します。

vPC ピア リンクの概要

vPC ピアとして持てるのは 2 台のデバイスだけです。各デバイスが、他方の 1 つの vPC ピアに対してだけ vPC ピアとして機能します。vPC ピア デバイスは、他のデバイスに対する非 vPC リンクも持つことができます。

無効な vPC ピア設定については、次の図を参照してください。

図 *13*：許可されていない *vPC* ピア設定



有効な設定を作成するには、まず各デバイス上でポート チャネルを設定してから、vPC ドメインを設定します。ポート チャネルを各デバイスに、同じ vPC ドメイン ID を使用してピア リンクとして割り当てます。vPC ピア リンクのインターフェイスの片方に障害が発生した場合に、デバイスが自動的にピア リンク内の他方のインターフェイスを使用するようにフォールバックするため、冗長性のために少なくとも 2 つの専用ポートをポート チャネルに設定することを推奨します。

（注） レイヤ 2 ポート チャネルをトランク モードで設定することを推奨します。

多くの動作パラメータおよび設定パラメータが、vPC ピア リンクによって接続されている各デバイスで同じでなければなりません（「vPC インターフェイスの互換パラメータ」の項を参照）。各デバイス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デバイス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 デバイスは、個別のコントロール プレーンを持ちます。vPC ピア リンクを設定し終えたら、各 vPC ピア デバイスの設定を表示して、設定に互換性があることを確認してください。

（注） vPC ピア リンクによって接続されている 2 つのデバイスが、特定の同じ動作パラメータおよび設定パラメータを持っていることを確認する必要があります。必要な設定の一貫性の詳細については、「vPC インターフェイスの互換パラメータ」の項を参照してください。

vPC ピア リンクを設定すると、vPC ピア デバイスは接続されたデバイスの一方がプライマリ デバイスで、もう一方の接続デバイスがセカンダリ デバイスであると交渉します（「vPC の設定」の項を参照）。Cisco NX-OS ソフトウェアは、最小の MAC アドレスを使用してプライマリ デバイスを選択します。特定のフェールオーバー条件の下でだけ、ソフトウェアが各デバイス（つまり、プライマリ デバイスおよびセカンダリ デバイス）に対して異なるアクションを取ります。プライマリ デバイスに障害が発生すると、システムの回復時にセカンダリ デバイスが新しいプライマリ デバイスになり、以前のプライマリ デバイスがセカンダリ デバイスになります。

どちらの vPC デバイスをプライマリ デバイスにするか設定することもできます。vPC ピア デバイスのプライオリティを変更すると、ネットワークでインターフェイスがアップしたりダウンしたりする可能性があります。1 台の vPC デバイスをプライマリ デバイスにするよう再度ロール プライオリティを設定する場合は、プライオリティ値が低いプライマリ vPC デバイスと値が高いセカンダリ vPC デバイスの両方でロール プライオリティを設定します。次に、**shutdown コマンド**を入力して、両方のデバイスで vPC ピア リンクであるポート チャネルをシャット ダウンし、最後に **no shutdown** コマンドを入力して、両方のデバイスでポート チャネルを再度イネーブルにします。

（注） 各 vPC ピア リンクの各 vPC ピア デバイスの冗長性のために、2 つの異なるモジュールを使用することを推奨します。

ソフトウェアは、vPC ピアを介して転送されたすべてのトラフィックをローカル トラフィックとしてキープします。ポート チャネルから入ってきたパケットは、vPC ピア リンクを介して移動するのではなく、ローカル リンクの 1 つを使用します。不明なユニキャスト、マルチキャスト、およびブロードキャスト トラフィック（STP BPDU を含む）は、vPC ピア リンクでフラッディングされます。ソフトウェアが、マルチキャスト フォワーディングを両方の vPC ピア デバイス上で同期された状態に保ちます。

両方の vPC ピア リンク デバイスおよびダウンストリーム デバイスで、任意の標準ロードバランシング スキームを設定できます（ロード バランシングについては、「ポート チャネルの設定」の章を参照）。

設定情報は、Cisco Fabric Service over Ethernet（CFSoE）プロトコルを使用して vPC ピア リンクを転送されます。（CFSoE の詳細については、「vPC および孤立ポート」の項を参照）。

両方のデバイス上で設定されているこれらの VLAN の MAC アドレスはすべて、vPC ピア デバイス間で同期されています。この同期に、CFSoE が使用されます（CFSoE の詳細については、「vPC および孤立ポート」の項を参照）。

vPC ピア リンクに障害が発生した場合は、ソフトウェアが、両方のデバイスが稼働していることを確認するための vPC ピア デバイス間のリンクであるピアキープアライブ リンクを使用して、リモート vPC ピア デバイスのステータスをチェックします。vPC ピア デバイスが稼働している場合は、セカンダリ vPC デバイスは、ループやトラフィックの消失あるいはフラッディングを防ぐために、そのデバイス上のすべての vPC ポートをディセーブルにします。したがって、データは、ポート チャネルの残っているアクティブなリンクに転送されます。

（注） 独立した VRF を作成して設定し、その vPC ピアキープアライブ リンクのための VRF 内の各 vPC ピア デバイス上でレイヤ 3 ポートを設定することを推奨します。ピアキープアライブのデフォルト ポートとデフォルト VRF は、管理ポートと管理 VRF です。

ソフトウェアは、ピアキープアライブ リンクを介したキープアライブ メッセージが返されない場合に、vPC ピア デバイスに障害が発生したことを学習します。

vPC ピア デバイス間の設定可能なキープアライブ メッセージの送信には、独立したリンク（vPC ピアキープアライブ リンク）を使用します。vPC ピアキープアライブ リンク上のキープアライブ メッセージから、障害が vPC ピア リンク上でだけ発生したのか、vPC ピア デバイス上で発生したのかがわかります。キープアライブ メッセージは、ピア リンク内のすべてのリンクで障害が発生した場合にだけ使用されます。キープアライブ メッセージについては、「ピアキープアライブ リンクとメッセージ」の項を参照してください。

プライマリおよびセカンダリ デバイス上で手動で設定する必要がある機能

各 vPC ピア デバイスのプライマリ/セカンダリ マッピングに従うために、次の機能を手動で設定する必要があります。

- STP ルート：プライマリ vPC ピア デバイスを STP プライマリ ルート デバイスとして設定し、vPC セカンダリ デバイスを STP セカンダリ ルート デバイスとして設定します。vPC および STP の詳細については、「vPC ピア リンクと STP」の項を参照してください。
  - Bridge Assurance がすべての vPC ピア リンク上でイネーブルになるように、vPC ピア リンク インターフェイスを STP ネットワーク ポートとして設定することを推奨します。
  - VLAN 単位の高速スパニングツリー（PVST+）を設定してプライマリ デバイスがすべての VLAN のルートになるようにし、マルチ スパニングツリー（MST）を設定してプライマリ デバイスがすべてのインスタンスのルートになるようにすることを推奨します。
- レイヤ 3 VLAN ネットワーク インターフェイス：両方のデバイスから同じ VLAN の VLAN ネットワーク インターフェイスを設定することにより、各 vPC ピア デバイスのレイヤ 3 接続を設定します。
- HSRP アクティブ：vPC ピア デバイス上でホットスタンバイ ルータ プロトコル（HSRP）と VLAN インターフェイスを使用する場合は、プライマリ vPC ピア デバイスを HSRP アクティブの最も高いプライオリティで設定します。セカンダリ デバイスを HSRP スタンバイになるように設定し、各 vPC デバイスの VLAN インターフェイスが同じ管理/動作モードにあることを確認します（vPC および HSRP の詳細については、「vPC ピア リンクとルーティング」の項を参照）。

vPC ピア リンクの両側で単方向リンク検出（UDLD）を設定することを推奨します。UDLD の設定については、「UDLD モードの設定」の項を参照してください。

vPC ピア リンクのレイヤ 3 バックアップ ルートの設定

HSRP や PIM などのアプリケーションを使用するネットワークのレイヤ 3 にリンクするために、vPC ピア デバイス上の VLAN ネットワーク インターフェイスを使用できます。ただし、この目的には VLAN ネットワーク インターフェイスを使用するよりも、vPC ピア デバイスからのルーティングのためのレイヤ 3 リンクを別途設定することを推奨します。

各ピアデバイス上でVLANネットワークインターフェイスが設定されており、そのインターフェイスが各デバイス上で同じVLANに接続されていることを確認してください。また、各VLANインターフェイスが、同じ管理/動作モードになっていなければなりません。VLANネットワークインターフェイスの設定の詳細については、「レイヤ 3 インターフェイスの設定」の章を参照してください。

vPC ピア リンクでフェールオーバーが発生すると、vPC ピア デバイス上の VLAN インターフェイスも影響を受けます。vPC ピア リンクに障害が発生すると、セカンダリ vPC ピア デバイス上の関連付けられている VLAN インターフェイスがシステムによって停止されます。

vPC ピア リンクに障害が発生したときに特定の VLAN インターフェイスが vPC セカンダリ デバイス上で停止しないようにできます。

この機能を設定するには、**dual-active exclude interface-vlan** コマンドを使用します。

（注） vPC ドメインにレイヤ 3 デバイスを接続した場合、vPC ピア リンク上でも送信される VLAN を使用したルーティング プロトコルのピアリングはサポートされません。vPC ピア デバイスおよび汎用レイヤ 3 デバイスの間でルーティング プロトコルの隣接関係が必要な場合は、相互接続に物理的にルーティングされたインターフェイスを使用する必要があります。vPC ピアゲートウェイ機能の使用では、この要件は変わりません。

ピアキープアライブ リンクとメッセージ

Cisco NX-OS ソフトウェアは、vPC ピア間でピアキープアライブ リンクを使用して、設定可能なキープアライブ メッセージを定期的に送信します。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 接続がなくてはなりません。ピアキープアライブ リンクが有効になって稼働していないと、システムは vPC ピア リンクを稼働させることができません。

（注） vPC ピアキープアライブ リンクを、各 vPC ピア デバイス内のレイヤ 3 インターフェイスにマッピングされている独立した VRF に関連付けることを推奨します。独立した VRF を設定しなかった場合は、デフォルトで管理 VRF と管理ポートが使用されます。vPC ピアキープアライブ メッセージの送受信にピア リンク自体を使用することはしないでください。

片方の vPC ピア デバイスに障害が発生したら、vPC ピア リンクの他方の側にある vPC ピア デバイスは、ピアキープアライブ メッセージを受信しなくなることによってその障害を感知します。

vPC ピアキープアライブ メッセージのデフォルトの間隔は、1 秒です。この間隔は、400 ミリ秒 ～ 10 秒の範囲内で設定可能です。

ホールドタイムアウト値は、3 ～ 10 秒の範囲内で設定可能で、デフォルトのホールドタイムアウト値は 3 秒です。このタイマーは、vPC ピア リンクが停止した時点で開始します。セカンダリ vPC ピア デバイスは、ネットワークの収束が確実に発生してから vPC アクションが発生するようにするために、このホールドタイムアウト期間の間は vPC ピアキープアライブ メッセージを無視します。ホールドタイムアウト期間の目的は、誤ったポジティブ ケースを防ぐことです。

タイムアウト値は、3 ～ 20 秒の範囲内で設定可能で、デフォルトのタイムアウト値は 5 秒です。このタイマーは、ホールドタイムアウト間隔が終了した時点で開始します。このタイムアウト期間の間は、セカンダリ vPC ピア デバイスは、プライマリ vPC ピア デバイスから vPC ピアキープアライブ hello メッセージが送信されてこないかチェックします。セカンダリ vPC ピア デバイスが 1 つの hello メッセージを受信したら、そのデバイスは、セカンダリ vPC ピア デバイス上のすべての vPC インターフェイスをディセーブルにします。

ホールドタイムアウト パラメータとタイムアウト パラメータの相違点は、次のとおりです。

- ホールドタイムアウトの間は、vPC セカンダリ デバイスは、受信したキープアライブ メッセージに基づいてアクションを起こしません。それにより、たとえばスーパーバイザがピア リンクがダウンした数秒後に失敗した場合などに、キープアライブが一時的に受信される可能性がある場合に、システムがアクションを起こすのを回避できます。
- タイムアウト中は、vPC セカンダリ デバイスは、設定された間隔が終了するまでにキープアライブ メッセージを受信できないと、vPC プライマリ デバイスになるというアクションを取ります。

キープアライブ メッセージへのタイマーの設定については、「vPC の設定」の項を参照してください。

（注） ピアキープアライブ メッセージに使用される送信元 IP アドレスと宛先 IP アドレスがどちらもネットワーク上で一意であり、かつそれらの IP アドレスがその vPC ピアキープアライブ リンクに関連付けられている VRF から到達可能であることを確認してください。

コマンドライン インターフェイス（CLI）を使用して、vPC ピアキープアライブ メッセージを使用するインターフェイスを信頼できるポートとして設定してください。優先順位をデフォルト（6）のままにしておくか、またはもっと高い値に設定します。次に、インターフェイスを信頼できるポートとして設定する例を示します。

```
(config)# class-map type qos match-all trust-map
(config-cmap-qos)# match cos 4-7
(config)# policy-map type qos ingresspolicy
(config-pmap-qos)# class trust-map
(config)# interface Ethernet 8/11
(config-if)# service-policy type qos input ingresspolicy
```

vPC ピア ゲートウェイ

vPC ピア デバイスを、vPC ピア デバイスの MAC アドレスに送信されるパケットに対してもゲートウェイとして機能するように設定できます。

この機能を設定するには、**peer-gateway** コマンドを使用します。

（注） vPC ピア デバイスでレイヤ 3 バックアップ ルーティングの VLAN インターフェイスを設定するときに使用される **peer-gateway exclude-vlan** コマンドはサポートされていません。

一部のネットワーク接続ストレージ（NAS）デバイスまたはロードバランサは、特定のアプリケーションのパフォーマンスを最適化するのに役立つ機能を備えている場合があります。これらの機能により、同じサブネットにローカルに接続されていないホストから送信された要求に応答するときに、デバイスはルーティング テーブルのルックアップを回避できます。このようなデバイスは、一般的な HSRP ゲートウェイではなく、送信元 Cisco Nexus 9000 シリーズ デバイスの MAC アドレスを使用して、トラフィックに応答する場合があります。この動作は、一部の基本的なイーサネット RFC 基準に準拠していません。ローカルではないルータ MAC アドレスの vPC デバイスに到達するパケットは、ピア リンクを介して送信され、最終的な宛先が他の vPC の背後にある場合には、組み込みの vPC ループ回避メカニズムによってドロップされる場合があります。

vPC ピアゲートウェイ機能は、vPC スイッチが、vPC ピアのルータ MAC アドレスを宛先とするパケットに対して、アクティブなゲートウェイとして機能することを可能にします。この機能は、このようなパケットが vPC ピア リンクを通過する必要なしにローカルに転送されることを可能にします。このシナリオでは、この機能によってピア リンクの使用が最適化され、トラフィック損失が回避されます。

ピアゲートウェイ機能の設定は、プライマリ vPC ピアとセカンダリ vPC ピアの両方で行う必要がありますが、デバイスの稼働も vPC トラフィックも中断しません。vPC ピアゲートウェイ機能は、vPC ドメイン サブモードの下でグローバルに設定できます。

この機能をイネーブルにすると、ピア ゲートウェイ ルータを介してスイッチングされたパケットの IP リダイレクト メッセージの発生を避けるために、Cisco NX-OS は vPC VLAN を介してマッピングされるすべてのインターフェイス VLAN 上で IP リダイレクトを自動的にディセーブルにします。

TTL が 1 のパケットが TTL の有効期限が原因で伝送中にドロップされるように、ピアゲートウェイ vPC デバイスに到達するパケットは、デクリメントされたパケット存続時間（TTL）を有しています。ピアゲートウェイ機能がイネーブルで、TTL が 1 のパケットを送信する特定のネットワーク プロトコルが vPC VLAN で動作する場合は、この状況を考慮する必要があります。

vPC ドメイン

vPC ドメイン ID を使用すれば、vPC ダウンストリーム デバイスに接続されている vPC ピア リンクとポートを識別できます。

vPC ドメインは、キープアライブ メッセージや他の vPC ピア リンク パラメータを、デフォルト値をそのまま使用するのではなく値を設定する場合に使用するコンフィギュレーション モードでもあります。これらのパラメータの設定の詳細については、「vPC の設定」の項を参照してください。

vPC ドメインを作成するには、まず各 vPC ピア デバイス上で、1 ～ 1000 の値を使用して vPC ドメイン ID を作成しなければなりません。VDC につき設定できる vPC ドメインは、1 つだけです。

各デバイス上で、ピア リンクとして機能させるポート チャネルを明示的に設定する必要があります。各デバイス上でピア リンクにしたポート チャネルを、1 つの vPC ドメインからの同じ vPC ドメイン ID に関連付けます。このドメイン内で、システムはループフリー トポロジとレイヤ 2 マルチパスを提供します。

これらのポート チャネルと vPC ピア リンクは、静的にしか設定できません。各 vPC ピア デバイス上の vPC 内のすべてのポートが、同じ VDC 内になくてはなりません。ポート チャネルおよび vPC ピア リンクは、LACP を使用するかまたはプロトコルなしのいずれかで設定できます。各 vPC でポート チャネルを設定するにはアクティブ モードのインターフェイスで LACP を使用することを推奨します。それにより、ポート チャネルのフェールオーバー シナリオの最適でグレースフルなリカバリが保証され、ポート チャネル間の設定不一致に対する設定検査が行われます。

vPC ピア デバイスは、設定された vPC ドメイン ID を使用して、一意の vPC システム MAC アドレスを自動的に割り当てます。各 vPC ドメインが、具体的な vPC 関連操作に ID として使用される一意の MAC アドレスを持ちます。ただし、デバイスは vPC システム MAC アドレスを LACP などのリンクスコープでの操作にしか使用しません。連続したレイヤ 2 ネットワーク内の各 vPC ドメインを、一意のドメイン ID で作成することを推奨します。Cisco NX-OS ソフトウェアにアドレスを割り当てさせるのではなく、vPC ドメインに特定の MAC アドレスを設定することもできます。

vPC MAC テーブルの表示の詳細については、「vPC および孤立ポート」の項を参照してください。

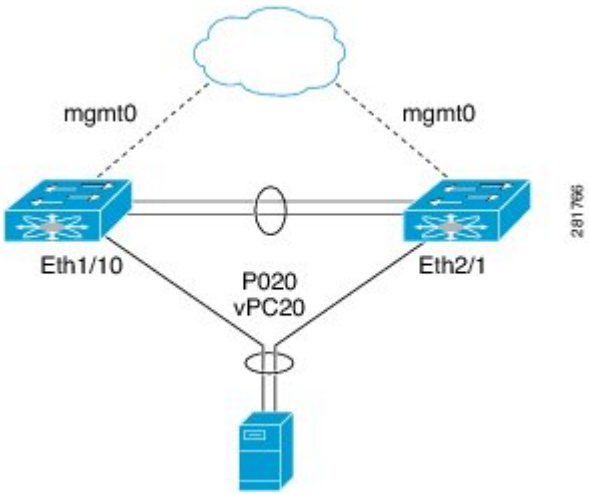
vPC ドメインを作成した後は、Cisco NX-OS ソフトウェアによって vPC ドメインのシステム プライオリティが作成されます。vPC ドメインに特定のシステム プライオリティを設定することもできます。

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

vPC トポロジ

次の図は、Cisco Nexus 9000 シリーズ デバイス ポートが別のスイッチまたはホストに直接接続され、vPC の一部となるポート チャネルの一部として設定される基本設定を示しています。

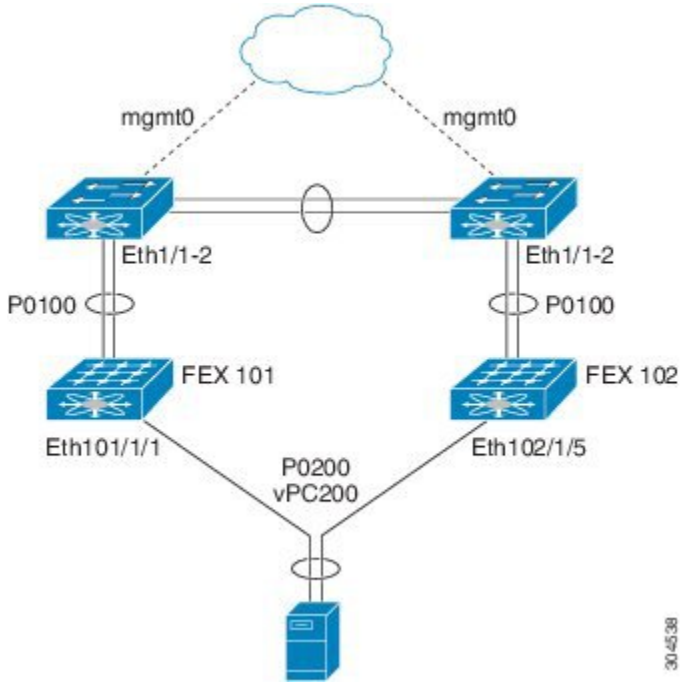
図 *14*：スイッチ *vPC* トポロジ



この図では、vPC 20 がポート チャネル 20 で設定され、最初のデバイスには Eth1/10 が、2 番目のデバイスには Eth2/1 がメンバ ポートとしてあります。

図で示されるように、ファブリック エクステンダ（FEX）を通してピア デバイスから vPC を設定できます。

図 *15*：*FEX Straight-Through* トポロジ（ホスト *vPC*）



図では、各 FEX は Cisco Nexus 9000 シリーズ デバイスがあるシングル ホーム接続（Straight-Through FEX トポロジ）です。この FEX 上のホスト インターフェイスはポート チャネルとして設定され、それらのポート チャネルは vPC として設定されています。Eth101/1/1 および Eth102/1/5 は、PO200 のメンバーとして設定され、PO200 は vPC 200 に対し設定されます。

どちらのトポロジでも、ポート チャネル P020 および P0200 をピア スイッチ上でまったく同じように設定する必要があります。その後、設定の同期を使用して vPC スイッチの設定を同期します。

FEX ポートの設定に関する詳細は、『*Cisco Nexus 2000 Series NX-OS Fabric Extender Configuration Guide for Cisco Nexus 9000 Series Switches*』を参照してください。

vPC インターフェイスの互換パラメータ

多くの設定パラメータおよび動作パラメータが、vPC 内のすべてのインターフェイスで同じでなければなりません。vPC ピア リンクに使用するレイヤ 2 ポート チャネルはトランク モードに設定することを推奨します。

vPC 機能をイネーブルにし、さらに両方の vPC ピア デバイス上でピア リンクを設定すると、シスコ ファブリック サービス（CFS）メッセージにより、ローカル vPC ピア デバイスに関する設定のコピーがリモート vPC ピア デバイスへ送信されます。これにより、システムが 2 つのデバイス

上で異なっている重要な設定パラメータがないか調べます（CFS の詳細については、「vPC および孤立ポート」の項を参照）。

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

vPC の互換性チェックプロセスは、正規のポート チャネルの互換性チェックとは異なります。正規のポート チャネルについては、「ポート チャネルの設定」の章を参照してください。

同じでなければならない設定パラメータ

このセクションの設定パラメータは、vPC ピア リンクの両方のデバイスで同じに設定する必要があります。そうしないと、vPC は一時停止モードに完全にまたは部分的に移動します。

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

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

vPC インターフェイスでのこれらのパラメータの一部は、デバイスによって自動的に互換性がチェックされます。インターフェイスごとのパラメータは、インターフェイスごとに一貫性を保っていなければならず、グローバル パラメータはグローバルに一貫性を保っていなければなりません。

- ポートチャネル モード：オン、オフ、またはアクティブ（ただし、ポートチャネル モードは vPC ピアの各サイドでアクティブ/パッシブにできます）
- チャ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
- Multiple Spanning Tree 用の STP リージョン コンフィギュレーション

- VLAN ごとのイネーブル/ディセーブル状態
- STP グローバル設定：
  - ブリッジ保証設定
  - ポート タイプ設定
  - ループ ガード設定
- STP インターフェイス設定：
  - ポート タイプ設定
  - ループ ガード
  - ルート ガード
- 最大伝送単位（MTU）

これらのパラメータのいずれかがイネーブルになっていなかったり、片方のデバイスでしか定義されていないと、vPC の一貫性チェックではそのパラメータは無視されます。

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

同じにすべき設定パラメータ

次の挙げるパラメータのいずれかが両方の vPC ピア デバイス上で同じように設定されていないと、誤設定が原因でトラフィック フローに望ましくない動作が発生する可能性があります。

- MAC エージング タイマー
- スタティック MAC エントリ
- VLAN インターフェイス：vPC ピア リンク エンドにある各デバイスの VLAN インターフェイスが両エンドで同じ VLAN 用に設定されていなければならず、さらに同じ管理モードで同じ動作モードになっていなければなりません。ピア リンクの片方のデバイスだけで設定されている VLAN は、vPC またはピア リンクを使用してトラフィックを通過させることはしません。すべての VLAN をプライマリ vPC デバイスとセカンダリ vPC デバイスの両方で作成する必要があります。そうなっていない VLAN は、停止します。
- ACL のすべての設定とパラメータ
- Quality of Service（QoS）の設定とパラメータ
- STP インターフェイス設定：
  - BPDU Filter

- BPDU ガード
- コスト
- リンク タイプ
- プライオリティ
- VLAN（Rapid PVST+）

- ポート セキュリティ
- Cisco Trusted Security（CTS）
- ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピング
- ネットワーク アクセス コントロール（NAC）
- ダイナミック ARP インスペクション（DAI）
- IP ソース ガード（IPSG）
- インターネット グループ管理プロトコル（IGMP）スヌーピング
- ホット スタンバイ ルーティング プロトコル（HSRP）
- プロトコルに依存しないマルチキャスト（PIM）
- すべてのルーティング プロトコル設定

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

パラメータの不一致によってもたらされる結果

稼動中の vPC で不一致が発生した場合にセカンダリ ピア デバイス上のリンクのみを一時停止する、グレースフル整合性検査機能を設定できます。この機能は CLI のみで設定可能で、デフォルトでイネーブルになっています。

この機能を設定するには、graceful consistency-check コマンドを使用します。

一致しなければならないパラメータのリストのすべてのパラメータに関する整合性検査の一部として、システムはすべての VLAN の一貫性をチェックします。

vPC は稼動を継続し、矛盾した VLAN のみがダウンします。この VLAN 単位の整合性検査機能はディセーブルにできず、マルチ スパニングツリー（MST）VLAN には適用されません。

vPC 番号

vPC ドメイン ID と vPC ピア リンクを作成し終えたら、ダウンストリーム デバイスを各 vPC ピア デバイスに接続するためのポート チャネルを作成します。つまり、プライマリ vPC ピア デバイスからダウンストリーム デバイスへのポート チャネルを 1 つ作成し、もう 1 つ、セカンダリ ピア デバイスからダウンストリーム デバイスへのポート チャネルも作成します。

（注） スイッチとしてもブリッジとしても機能しないホストまたはネットワーク デバイスに接続されているダウンストリーム デバイス上のポートは、STP エッジ ポートとして設定することを推奨します。

各 vPC ピア デバイス上で、ダウンストリーム デバイスに接続するポート チャネルに vPC 番号を割り当てます。vPC の作成時にトラフィックが中断されることはほとんどありません。すべてのポート番号に、ポート チャネル自体と同じ vPC ID 番号を割り当てると（つまり、ポート チャネル 10 には vPC ID 10）、設定が簡単になります。

（注） vPC ピア デバイスからダウンストリーム デバイスに接続するためにポート チャネルに割り当てる vPC 番号は、両方の vPC ピア デバイスで同じである必要があります。

他のポート チャネルの vPC への移行

（注） ダウンストリーム デバイスは、ポート チャネルを使用して両方の vPC ピア デバイスに接続する必要があります。

ダウンストリームデバイスを接続するために、プライマリ vPC ピアデバイスからダウンストリーム デバイスへのポート チャネルを作成し、セカンダリ ピア デバイスからダウンストリーム デバイスへのもう 1 つのポート チャネルを作成します。各 vPC ピア デバイス上で、ダウンストリームデバイスに接続するポートチャネルに vPC 番号を割り当てます。vPC の作成時にトラフィックが中断されることはほとんどありません。

単一モジュール上での vPC ピア リンクとコアへのリンクの設定

（注） 異なるモジュールの専用ポート上で vPC ピア リンクを設定して、障害発生の可能性を下げることをお勧めします。復元力を最適にしたい環境では、少なくとも2つのモジュールを使用してください。

すべての vPC ピア リンクとコアに面するインターフェイスを単一モジュール上で設定しなければならない場合は、両方の vPC ピア デバイス上のすべての vPC ピア リンク上にあり、コアへのレイヤ 3 リンクに関連付けられているトラック オブジェクトとトラック リストをコマンドライン インターフェイスを使用して設定してください。トラック リスト上のすべてのトラッキング対象オブジェクトが停止した場合、システムは次のように動作するため、この設定を使用すれば、その特定のモジュールが停止した場合のトラフィックのドロップを避けることができます。

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

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

コアに対するすべてのリンクおよびすべての vPC ピア リンクを含むトラック リストを、そのオブジェクトとして作成する必要があります。このトラック リストの指定した vPC ドメインに対して、トラッキングをイネーブルにします。この同じ設定を他方の vPC ピア デバイスにも適用します。オブジェクト トラッキングおよびトラック リストの詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

（注） 次の例では、Boolean OR を追跡リストで使用し、完全なモジュール障害の場合にのみすべてのトラフィックが vPC ピア デバイスへ流れるよう強制します。コア インターフェイスまたはピア リンクがダウンしたときにスイッチオーバーをトリガーする場合は、次のトラック リストでブール AND を使用します。

単一モジュール上の関連するすべてのインターフェイスが故障したときに vPC をリモート ピアに切替えるように追跡リストを設定するには、次の手順に従います。

1. インターフェイス上（コアへのレイヤ 3）およびポート チャネル上（vPC ピア リンク）でトラック オブジェクトを設定します。

```
switch(config-if)# track 35 interface ethernet 8/35 line-protocol
switch(config-track)# track 23 interface ethernet 8/33 line-protocol
switch(config)# track 55 interface port-channel 100 line-protocol
```

2. ブール OR を使って追跡リスト内のすべてのインターフェイスを含むトラック リストを作成して、すべてのオブジェクトに障害が発生したときにトリガーします。

```
switch(config)# track 44 list boolean OR
switch(config-track)# object 23
switch(config-track)# object 35
switch(config-track)# object 55
switch(config-track)# end
```

3. このトラック オブジェクトを vPC ドメインに追加します。

```
switch(config)# vpc domain 1
switch(config-vpc-domain)# track 44
```

4. トラック オブジェクトを表示します。

```
switch# show vpc brief
```

```
Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id : 1
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
Configuration consistency status: success
vPC role : secondary
Number of vPCs configured : 52
Track object : 44
vPC Peer-link status
---------------------------------------------------------------------
id Port Status Active vlans
-- ---- ------ --------------------------------------------------
1 Po100 up 1-5,140
vPC status
----------------------------------------------------------------------
id Port Status Consistency Reason Active vlans
-- ---- ------ ----------- ------------------------ ------------
1 Po1 up success success 1-5,140
```

次に、オブジェクト トラッキングに関する情報を表示する例を示します。

```
switch# show track brief
Track Type Instance Parameter State Last
Change
23 Interface Ethernet8/33 Line Protocol UP 00:03:05
35 Interface Ethernet8/35 Line Protocol UP 00:03:15
44 List ----- Boolean
or UP 00:01:19
55 Interface port-channel100 Line Protocol UP 00:00:34
```

その他の機能との vPC の相互作用

vPC と LACP

LACP は、vPC ドメインのシステム MAC アドレスを使用して、vPC の LACP Aggregation Group（LAG）ID を形成します（LAG-ID および LACP については、「ポート チャネルの設定」の章を参照）。

ダウンストリーム デバイスからのチャネルも含めて、すべての vPC ポート チャネル上の LACP を使用できます。LACP は、vPC ピア デバイスの各ポート チャネル上のインターフェイスのアクティブ モードで設定することを推奨します。この設定により、デバイス、単方向リンク、およびマルチホップ接続の間の互換性をより簡単に検出できるようになり、実行時の変更およびリンク障害に対してダイナミックな応答が可能になります。

vPC ピア リンク デバイスのシステム プライオリティを手動で設定して、vPC ピア リンク デバイスが、接続されているダウンストリーム デバイスより確実に高い LACP プライオリティを持つようにすることを推奨します。システム プライオリティの値が低いほど、高い LACP プライオリティを意味します。

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

vPC ピア リンクと STP

vPC はループフリーなレイヤ 2 トポロジを提供しますが、それでもやはり、誤った配線やケーブルの欠陥、誤設定などから保護するためのフェールセーフ メカニズムを STP が提供する必要があります。vPC を初めて稼働させたときに、STP による再コンバージェンスが発生します。STP は、vPC ピア リンクを特殊なリンクとして扱い、常に vPC ピア リンクを STP のアクティブ トポロジに含めます。

すべての vPC ピア リンク インターフェイスを STP ネットワーク ポート タイプに設定して、すべての vPC リンク上で Bridge Assurance が自動的にイネーブルになるようにすることを推奨します。また、vPC ピア リンク上ではどの STP 拡張機能もイネーブルにしないことも推奨します。STP 拡張がすでに設定されている場合、その拡張が vPC ピア リンクの問題の原因となることはありません。

MST と Rapid PVST+ の両方を実行している場合は、必ず PVST シミュレーション機能を正しく設定してください。

STP 拡張機能および PVST シミュレーションについては、『*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

（注） パラメータのリストは、vPC ピア リンクの両サイドの vPC ピア デバイス上で同じになるように設定する必要があります。このような一致が必要な設定については、「vPC インターフェイスの互換パラメータ」の項を参照してください。

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

プライマリ vPC デバイスは、Cisco Fabric Services over Ethernet（CFSoE）を使用して、vPC セカンダリ ピア デバイス上の STP の状態を同期させます。CFSoE の詳細については、「vPC および孤立ポート」の項を参照してください。

vPC の STP プロセスも、ピア リンク上で接続されているデバイスの 1 つに障害が発生したときにそれを検出するために、定期的なキープアライブ メッセージに依存しています。これらのメッセージについては、「ピアキープアライブ リンクとメッセージ」の項を参照してください。

vPC マネージャが、vPC ピア デバイス間で、プライマリ デバイスとセカンダリ デバイスを設定して 2 つのデバイスを STP 用に調整する提案/ハンドシェイク合意を実行します。その後、プライマリ vPC ピア デバイスが、プライマリ デバイスとセカンダリ デバイス両方での STP プロトコルの制御を行います。プライマリ vPC ピア デバイスを STP プライマリ ルート デバイスとして設定し、

セカンダリ VPC デバイスを STP セカンダリ ルート デバイスになるように設定することを推奨します。

プライマリ vPC ピア デバイスがセカンダリ vPC ピア デバイスにフェールオーバーした場合、STP トポロジには何の変化も発生しません。

BPDU は、代表ブリッジ ID フィールドで、STP ブリッジ ID の vPC に設定されている MAC アドレスを使用します。vPC プライマリ デバイスが、vPC インターフェイス上でこれらの BPDU を送信します。

次のパラメータについて同じ STP 設定を使用して、vPC ピア リンクの両エンドを設定する必要があります。

- STP グローバル設定：
  - STP モード
  - MST のための STP リージョン設定
  - VLAN ごとのイネーブル/ディセーブル状態
  - ブリッジ保証設定
  - ポート タイプ設定
  - ループ ガード設定
- STP インターフェイス設定：
  - ポート タイプ設定
  - ループ ガード
  - ルート ガード

（注） これらのパラメータのいずれかに誤設定があった場合、Cisco NX-OS ソフトウェアが vPC 内のすべてのインターフェイスを停止します。syslog をチェックし、**show vpc brief** コマンドを入力して、vPC インターフェイスが停止していないか確認してください。

次の STP インターフェイス設定が、vPC ピア リンクの両側で同じになっていることを確認します。そうなっていないと、トラフィック フローに予測不能な動作が発生する可能性があります。

- BPDU Filter
- BPDU ガード
- コスト
- リンク タイプ
- プライオリティ
- VLAN（PVRST+）

（注） vPC ピア リンクの両側での設定を表示して、設定が同じであることを確認してください。

この機能がイネーブルになっている場合は、**show spanning-tree** コマンドで vPC に関する情報を表示できます。例については、『*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

（注） ダウンストリームデバイスのポートは、STPエッジポートとして設定することを推奨します。スイッチに接続されているすべてのホスト ポートを STP エッジ ポートとして設定してくださいSTP ポート タイプの詳細については、『*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

vPC ピア スイッチ

vPC ピア スイッチ機能は、STP コンバージェンスに関連するパフォーマンス上の問題を解決するために、Cisco NX-OS に追加されました。この機能は、一対の Cisco Nexus 9000 シリーズ デバイスがレイヤ2トポロジ内で1つのSTPルートとして現れることを可能にします。この機能は、STPルートをvPCプライマリ スイッチに固定する必要性をなくし、vPCプライマリ スイッチに障害が発生した場合の vPC コンバージェンスを向上させます。

ループを回避するために、vPC ピア リンクは STP 計算からは除外されます。vPC ピア スイッチ モードでは、ダウンストリーム スイッチでの STP BPDU タイムアウトに関連した問題（この問題は、トラフィックの中断につながります）を避けるために、STP BPDU が両方の vPC ピア デバイスから送信されます。

この機能は、すべてのデバイス vPC に属する純粋なピア スイッチ トポロジで使用できます。

（注） ピア スイッチ機能は、vPCを使用するネットワークでサポートされ、STPベースの冗長性はサポートされません。ハイブリッド ピア スイッチ設定で vPC ピア リンクに障害が発生すると、トラフィックが失われる場合があります。このシナリオでは、vPC ピアは同じ STP ルート ID や同じブリッジ ID を使用します。アクセス スイッチのトラフィックは 2 つに別れ、その半分が最初の vPC ピアに、残りの半分が 2 番目の vPC ピアに転送されます。ピア リンク障害は、南北のトラフィックには影響がありませんが、東西のトラフィックが失われます。

STP 拡張機能および Rapid PVST+ については、『*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

vPC および ARP または ND

Cisco Fabric Service over Ethernet（CFSoE）プロトコルの信頼性が高いトランスポート メカニズムを使用した、vPC ピア間のテーブル同期に対応する機能が Cisco NX-OS に追加されました。**ip arp synchronize** および **ipv6 nd synchronize** コマンドをイネーブルにし、vPC ピア間のアドレス テー

ブルのコンバージェンスの高速化をサポートする必要があります。このコンバージェンスにより、ピア リンク ポート チャネルがフラップしたり、vPC ピアがオンラインに戻るときに、IPv4 の場合は ARP テーブルの復元でまたは IPv6 の場合は ND テーブルの復元で発生する遅延を解消できます。

vPC マルチキャスト：PIM、IGMP、および IGMP スヌーピング

Nexus 9000 シリーズ デバイス対応の Cisco NX-OS ソフトウェアは、vPC での次をサポートします。

- PIM Any Source Multicast（ASM）
- PIM Source-Specific Multicast（SSM）（7.0(3)I4(1) 以降）

（注） Cisco NX-OS ソフトウェアは、vPC での 双方向（BIDR）をサポートしません。

ソフトウェアが、マルチキャスト フォワーディングを両方の vPC ピア デバイス上で同期された状態に保ちます。vPC ピア デバイス上の IGMP スヌーピング プロセスは、学習したグループ情報を vPC ピア リンクを通じて他の vPC ピア デバイスと共有します。マルチキャスト状態は、常に両方の vPC ピア デバイス上で同期されます。vPC モードでの PIM プロセスは、1 つの vPC ピア デバイスだけが受信者に向けてマルチキャスト トラフィックを転送する状態を確保します。

各 vPC ピアは、レイヤ 2 またはレイヤ 3 デバイスです。マルチキャスト トラフィックは 1 つの vPC ピア デバイスだけから伝送されます。次のシナリオで、重複したパケットが観察される場合があります。

- 孤立ホスト
- 送信元と受信者が、マルチキャスト ルーティングのイネーブルになった異なる VLAN 内のレイヤ 2 vPC クラウド内にあり、vPC メンバ リンクが停止している場合。

次のシナリオで、ごくわずかなトラフィック損失が観察される場合があります。

- トラフィックを転送している vPC ピア デバイスをリロードした場合。
- トラフィックを転送している vPC ピア デバイスの PIM を再起動した場合。

必ずすべてのレイヤ 3 デバイスを両方の vPC ピア デバイスにデュアル接続してください。片方の vPC ピア デバイスが停止した場合、他方の vPC ピア デバイスが、通常どおりにすべてのマルチキャスト トラフィックを転送し続けます。

次に、vPC PIM および vPC IGMP/IGMP スヌーピングについて説明します。

- vPC PIM：vPC モードの PIM プロセスは、1 台の vPC ピア デバイスのみがマルチキャスト トラフィックを転送する状態を確保します。vPC モードの PIM プロセスは、送信元の状態を両方の vPC ピア デバイスと同期させ、トラフィックを転送する vPC ピア デバイスを選出します。

- vPC IGMP/IGMP スヌーピング：vPC モードの IGMP プロセスは、両方の vPC ピア デバイスで指定ルータ（DR）情報を同期させます。デュアル DR は、vPC モードのときに IGMP で利用可能です。デュアル DR は、vPC モードでない場合は利用できません。これは、両方の vPC ピア デバイスがピア間のマルチキャスト グループ情報を保持するためです。

（注） vPC VLAN（vPC ピア リンクで伝送される VLAN）とダウンストリーム vPC が接続されたレイヤ 3 デバイス間の PIM ネイバー関係はサポートされません。それによりマルチキャスト パケットのドロップが生じる場合があります。PIM ネイバー関係がダウンストリーム レイヤ 3 デバイスで必要な場合、物理レイヤ 3 インターフェイスを vPC インターフェイスの代わりに使用する必要があります。

IGMP スヌーピングは、両方の vPC ピア デバイス上で同じようにイネーブルにしたりディセーブルにしたりする必要があり、すべての機能設定を同じにする必要があります。IGMP スヌーピングは、デフォルトで有効になっています。

（注） 次のコマンドは、vPC モードでサポートされていません。

- **ip pim spt-threshold infinity**
- **ip pim use-shared-tree-only**

マルチキャストの詳細については、『*Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide*』を参照してください。

マルチキャスト PIM デュアル DR（プロキシ DR）

デフォルトでは、マルチキャスト ルータは該当する受信先が存在する場合のみ PIM ジョインをアップストリームに送信します。これらの該当する受信先は、IGMP ホスト（IGMP レポートを通じて通信します）または他のマルチキャスト ルータ（PIM ジョインを通じて通信します）のどちらかの場合があります。

Cisco NX-OS vPC 実装では、PIM はデュアル指定ルータ（DR）モードで動作します。つまり、vPC デバイスが vPC SVI の発信インターフェイス（OIF）上の DR である場合、そのピアは自動的にプロキシ DR ロールを引き継ぎます。IGMP は、OIF が DR である場合、OIF（レポートはその OIF で学習されます）をフォワーディングに追加します。デュアル DR では、両方の vPC デバイスには、次の例に示すように、vPC SVI OIF に対して同一のエントリ (*,G) があります。

```
VPC Device1:
------------
(*,G)
oif1 (igmp)
VPC Device2:
------------
(*,G)
oif1 (igmp)
```

IP PIM PRE-BUILD SPT

マルチキャスト ソースがレイヤ 3 クラウド（vPC ドメイン外）にある場合、1 つの vPC ピアが送信元のフォワーダとして選定されます。このフォワーダの選択は、送信元に到達するためのメトリックに基づきます。関係がある場合、vPC プライマリはフォワーダとして選択されます。フォワーダのみがその関連する (S,G) 内に vPC OIF を持っており、非フォワーダ (S,G) は 0 OIF を持っています。したがって、フォワーダのみがこの例に示すように、送信元へ PIM (S,G) ジョインを送信します。

```
VPC Device1 (say this is Forwarder for Source 'S'):
------------
(*,G)
oif1 (igmp)
(S,G)
oif1 (mrib)
VPC Device2:
------------
(*,G)
oif1 (igmp)
(S,G)
NULL
```

障害が発生した場合（たとえば、フォワーダのレイヤ 3 リバース パス転送（RPF）リンクが動作しない、またはフォワーダがリロードされるなど）、現在の非フォワーダが最終的にフォワーダになる場合は、トラフィック取得するために送信元への (S,G) に対する PIM ジョインの送信を開始をする必要があります。送信元に到達するホップ数によって、この操作には時間がかかる場合があります（PIM はホップバイホップ プロトコルです）。

この問題を排除し、より優れたコンバージェンスを取得するには、**ip pim pre-build-spt** コマンドを使用します。 このコマンドにより、マルチキャスト ルートに 0 OIF があっても PIM はジョインを送信できます。vPC デバイスでは、非フォワーダは送信元へ PIM (S,G) ジョインをアップストリームに送信します。欠点は、非フォワーダからのリンク帯域幅のアップストリームが最終的にそれによってドロップされるトラフィックに使用されることです。コンバージェンスの向上によるメリットは、リンク使用帯域幅をはるかに上回っていることです。 したがって、vPC を使用する場合は、このコマンドを使用することを推奨します。

vPC ピア リンクとルーティング

First Hop Redundancy Protocol（FHRP）は、vPC と相互運用できます。Hot Standby Routing Protocol（HSRP）、および Virtual Router Redundancy Protocol（VRRP）のすべてが、vPC と相互運用できます。すべてのレイヤ 3 デバイスを両方の vPC ピア デバイスにデュアル接続することを推奨します。

プライマリ FHRP デバイスは、たとえセカンダリ vPC デバイスがデータ トラフィックを転送したとしても、ARP 要求に応答します。

プライマリ vPC ピア デバイスを FHRP アクティブ ルータの最も高いプライオリティで設定しておくと、初期の設定確認と vPC/HSRP のトラブルシューティングを簡単にできます。

さらに、if-hsrp コンフィギュレーション モードで priority コマンドを使用して、vPC ピア リンク上でイネーブルになっているグループの状態がスタンバイになっているか、またはリッスン状態

になっている場合のフェールオーバーのしきい値を設定できます。インターフェイスがアップまたはダウンするのを防ぐために下限および上限しきい値を設定できます。

VRRP は、vPC ピア デバイス上で実行されている場合に HSRP とよく似た動作を示します。VRRP は、HSRP を設定したのと同じ方法で設定してください。

プライマリ vPC ピア デバイスに障害が発生した場合は、セカンダリ vPC ピア デバイスにフェールオーバーされ、FHRP トラフィックはシームレスに流れ続けます。

バックアップ ルーティング パスとして機能するように 2 台の vPC ピア デバイス間にルーティング隣接を設定することを推奨します。1 台の vPC ピア デバイスがレイヤ 3 アップリンクを失うと、その vPC はルーテッド トラフィックを他の vPC ピア デバイスにリダイレクトでき、そのアクティブ レイヤ 3 アップリンクを活用できます。

次の方法で、バックアップのルーティング パス用のスイッチ間リンクを設定できます。

- 2 台の vPC ピア デバイス間でレイヤ 3 リンクを作成します。
- 専用の VLAN インターフェイスを持つ非 VPC VLAN トランクを使用します。
- 専用の VLAN インターフェイスを持つ vPC ピア リンクを使用します。

vPC 環境での HSRP の焼き付け MAC アドレス オプション（use-bia）の設定、および任意の FHRP プロトコルのための仮想 MAC アドレスの手動での設定は、推奨できません。これらの設定は、vPC ロード バランシングに不利な影響を与えるためです。HSRP use-bia オプションは、vPC ではサポートされていません。カスタム MAC アドレスを設定する際には、両方の vPC ピア デバイスに同じ MAC アドレスを設定する必要があります。

delay restore コマンドを使用して、ピアの隣接関係が確立され VLAN インターフェイスが再びアップ状態になるまで vPC の再稼働を遅延させるための復元タイマーを設定することができます。この機能により、vPC が再びトラフィックの受け渡しをし始める前にルーティング テーブルが収束できなかった場合のパケットのドロップを回避できます。この機能を設定するには、**delay restore** コマンドを使用します。

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

FHRP およびルーティングに関する詳細情報については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

レイヤ 3 および vPC 設定のベスト プラクティス

ここでは、vPC でレイヤ 3 を使用し、設定するためのベスト プラクティスについて説明します。

レイヤ 3 および vPC 設定の概要

レイヤ 3 デバイスは、vPC を介して vPC ドメインに接続すると、次のようになります。

- レイヤ 2 では、レイヤ 3 デバイスは vPC ピア デバイスによって提供された一意のレイヤ 2 スイッチを認識します。

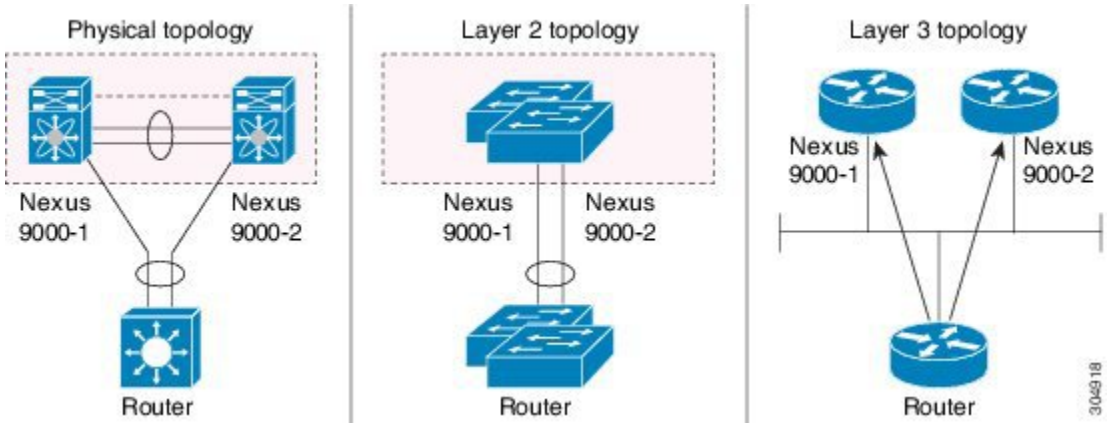
- レイヤ 3 では、レイヤ 3 デバイスは 2 台の異なるレイヤ 3 デバイス（vPC ピア デバイスごとに 1 台）を認識します。

vPC はレイヤ 2 仮想化技術であるため、レイヤ 2 では、両方の vPC ピア デバイスがネットワークの他の部分に対して一意の論理デバイスとして機能します。

レイヤ 3 には仮想化技術がないため、各 vPC ピア デバイスがネットワークの他の部分で別の レイヤ 3 デバイスと見なされます。

次の図は、vPC による 2 つの異なるレイヤ 2 およびレイヤ 3 ビューを示しています。

図 *16*：*vPC* ピア デバイスの異なるビュー



レイヤ 3 および vPC 設定に関する注意事項

vPC ドメインにレイヤ 3 デバイスを接続するには、レイヤ 3 デバイスのレイヤ 3 リンクを使用して各 vPC ピア デバイスを接続します。

（注） vPC ループ回避ルールにより、vPC を使用してレイヤ 3 デバイスを vPC ドメインに接続することは許可されません。

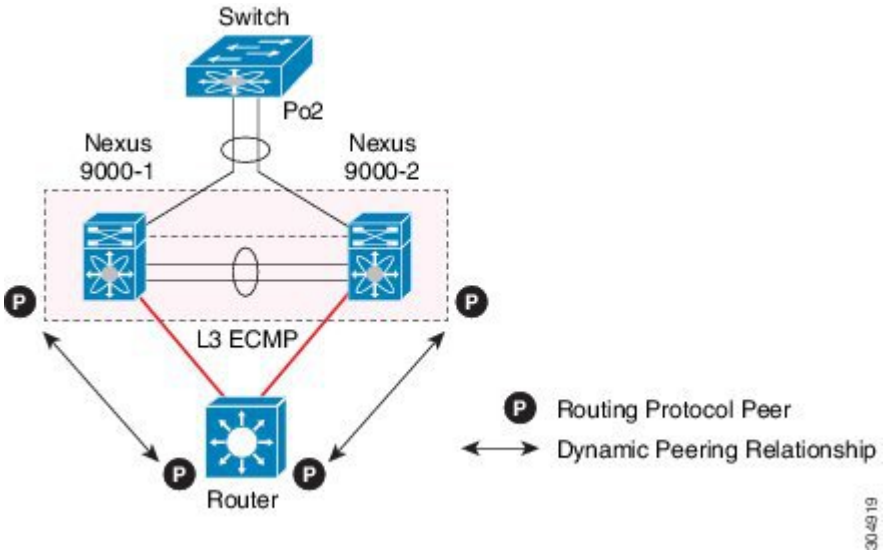
レイヤ 3 デバイスは、両方の vPC ピア デバイスとのレイヤ 3 ルーティング プロトコルの隣接関係を開始できます。

1 つまたは複数のレイヤ 3 リンクを、各 vPC ピア デバイスにレイヤ 3 デバイスを接続ために使用できます。Cisco Nexus 9000 シリーズ デバイスは、プレフィックスごとに最大 16 のハードウェア ロード シェアリング パスでレイヤ 3 Equal Cost Multipathing（ECMP）をサポートします。vPC ピア デバイスからレイヤ 3 デバイスへのトラフィックを、2 台のデバイスを相互接続するすべてのレイヤ 3 リンクにロードバランスできます。

レイヤ 3 デバイスでレイヤ 3 ECMP を使用すると、このデバイスから vPC ドメインへのすべてのレイヤ 3 リンクを効果的に使用できます。レイヤ 3 デバイスから vPC ドメインへのトラフィックを、2 つのエンティティを相互接続するすべてのレイヤ 3 リンクにロードバランスできます。

vPC ドメインに対するレイヤ 3 デバイスのサポートされる接続モデルは、次の図に示されています。

図 *17*：別のレイヤ *3* リンクを使用した *vPC* ドメインへの *L3* デバイスの接続



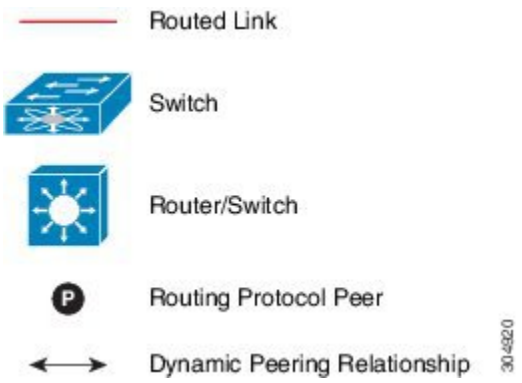
レイヤ 3 デバイスを vPC ドメインに接続する際は、次の注意事項に従ってください。

- レイヤ 3 デバイスを vPC ドメインに接続するには、独立したレイヤ 3 リンクを使用します。
- レイヤ 3 デバイスが vPC ピア デバイスで設定された HSRP アドレスにスタティックにルーティングできない場合は、vPC ドメインにレイヤ 3 デバイスを接続するのにレイヤ 2 の vPC を使用しないでください。
- ルーテッド トラフィックとブリッジド トラフィックの両方が必要な場合は、ルーテッド トラフィックに個々のレイヤ 3 リンクを使用し、ブリッジド トラフィックには別のレイヤ 2 ポート チャネルを使用します。
- 両方のデバイスからの同じ VLAN に対して VLAN ネットワーク インターフェイスを設定するか、2 台のピア デバイス間に専用レイヤ 3 リンクを使用することにより（レイヤ 3 バックアップ ルーティング パスのため）、vPC ピア デバイス間のレイヤ 3 接続をイネーブルにします。

レイヤ 3 および vPC のトポロジの例

ここでは、レイヤ 3 および vPC のネットワーク トポロジの例を示します。

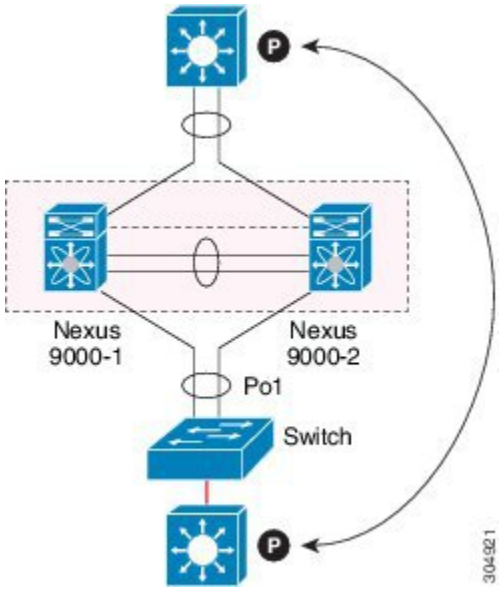
図 *18*：凡例



ルータ間のピアリング

この例では、vPC がレイヤ 2 中継パスとして使用されています。レイヤ 3 デバイスから vPC ピア デバイスへの直接的なルーティング プロトコル ピアリング隣接がないため、このトポロジはサポートされます。

図 *19*：ルータ間のピアリング

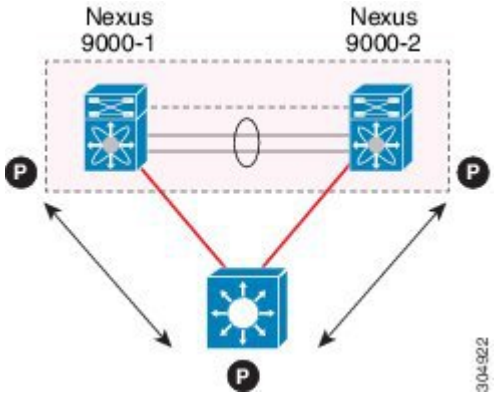


レイヤ *3* リンクを使用した外部ルータとのピアリング

この例は、レイヤ 3 リンクを使用してレイヤ 3 デバイスを vPC ドメインに接続するトポロジを示しています。

（注） この方法で 2 つのエンティティを相互接続することは、ベスト プラクティスです。

図 *20*：レイヤ *3* リンクを使用した外部ルータとのピアリング

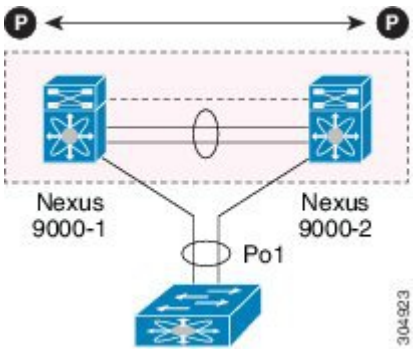


バックアップ ルーティング パス用の *vPC* ピア デバイス間のピアリング

この例は、レイヤ 3 バックアップ ルーティング パスによる 2 台の vPC ピア デバイス間のピアリングを示しています。vPC ピア デバイス 1 または vPC ピア デバイス 2 のレイア 3 アップリンクに障害が発生した場合、2 台のピア デバイス間のパスを使用して、アップ ステートのレイヤ 3 アップリンクを持つスイッチにトラフィックがリダイレクトされます。

レイヤ 3 バックアップ ルーティング パスは、vPC ピア リンク上の専用インターフェイス VLAN（SVI など）を使用するか、2 台の vPC ピア デバイス間の専用レイヤ 2 またはレイヤ 3 リンクを使用して実装できます。

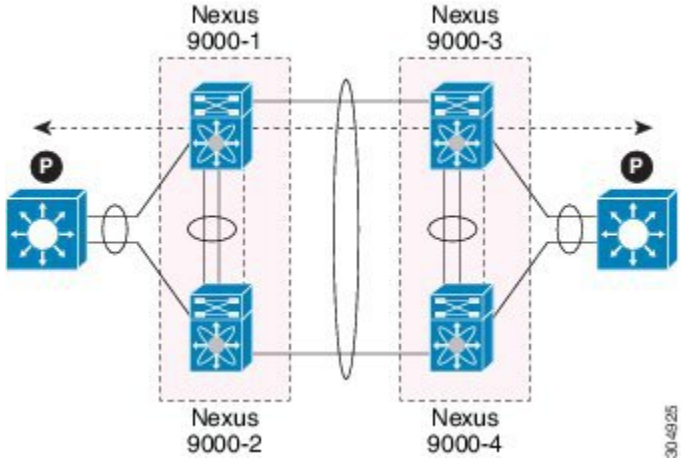
図 *21*：バックアップ ルーティング パス用の *vPC* ピア デバイス間のピアリング



中継スイッチとして *vPC* デバイスを使用した *2* ルータの間のピアリング

この例は、「ルータ間のピアリング」トポロジと似ています。異なる点は、vPC ドメインがレイヤ 2 中継パスとしてのみ使用されていることです。

図 *22*：中継スイッチとして *vPC* デバイスを使用した *2* ルータの間のピアリング



パラレル相互接続ルーテッド ポートでの外部ルータとのピアリング

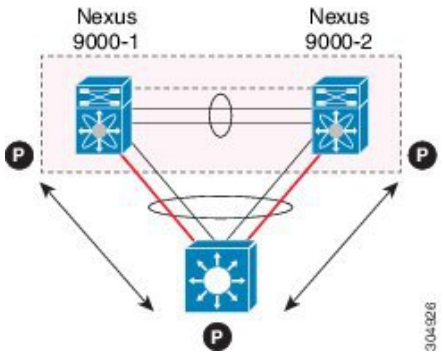
この例は、2 つの異なるリンク タイプ（レイヤ 2 リンクとレイヤ 3 リンク）を使用して vPC ドメインに接続されたレイヤ 3 デバイスを示しています。

レイヤ 2 リンクは、ブリッジド トラフィック（同じ VLAN に保持されるトラフィック）または VLAN 間トラフィック（vPC ドメインがインターフェイス VLAN と関連 HSRP コンフィギュレーションをホストすることが前提）に使用されます。

レイヤ 3 リンクは、各 vPC ピア デバイスとのルーティング プロトコル ピアリング隣接に使用されます。

このトポロジの目的は、レイヤ 3 デバイスを通過するように特定のトラフィックを誘導することです。レイヤ 3 リンクは、レイヤ 3 デバイスから vPC ドメインにルーテッド トラフィックを伝送するのにも使用されます。

図 *23*：パラレル相互接続ルーテッド ポートでの外部ルータとのピアリング

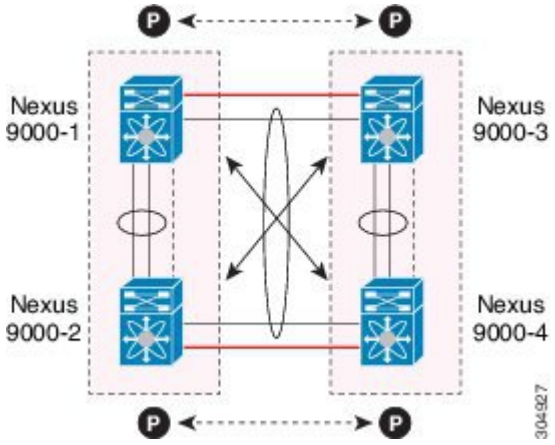


パラレル相互接続ルーテッド ポートでの *vPC* 相互接続を介したピアリング

ルーティング プロトコル ピアリング隣接を 2 つのデータセンター間で確立する必要がある場合、ベスト プラクティスは、この例に示すように 2 サイト間に専用レイヤ 3 リンクを追加することです。

2 つのデータセンター間の vPC リンクはブリッジド トラフィックまたは VLAN 間トラフィックを伝送し、専用レイヤ 3 リンクは 2 サイト間でルーテッド トラフィックを伝送します。

図 *24*：パラレル相互接続ルーテッド ポートでの *vPC* 相互接続を介したピアリング

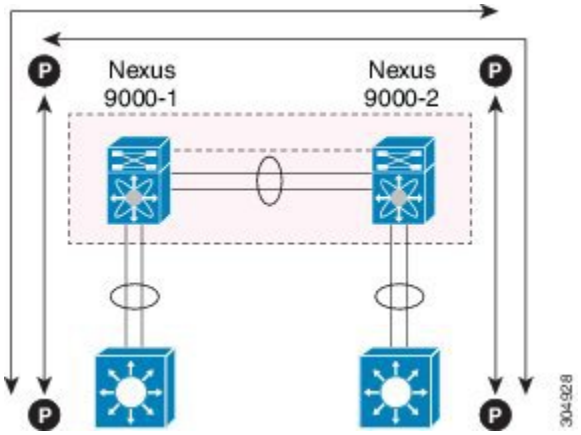


非 *vPC VLAN* を使用する *PC* 相互接続および専用スイッチ間リンクを介したピアリング

この例は、レイヤ 3 デバイスが vPC ドメインにシングル接続されている場合に、専用スイッチ間リンクで非 vPC VLAN を使用して、レイヤ 3 デバイスと各 vPC ピア デバイスとの間でルーティング プロトコル ピアリング隣接を確立できることを示しています。ただし、非 vPC VLAN は、vPC VLAN とは異なるスタティック MAC を使用するように設定する必要があります。

（注） この目的のために vPC VLAN（および vPC ピア リンク）を設定することはサポートされていません。

図 *25*：非 *vPC VLAN* を使用する *PC* 相互接続および専用スイッチ間リンクを介したピアリング



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される信頼性の高い状態転送メカニズムです。CFSoE は、vPC にリンクされている、STP、IGMP などの多くの機能のメッセージとパケットを伝送します。情報は、CFS/CFSoE プロトコル データ ユニット（PDU）に入れて伝送されます。

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

CFSoE 転送は、各 VDC にローカルです。

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

（注） **no cfs eth distribute** コマンドと **no cfs distribute** コマンドは入力しないでください。CFSoE for vPC 機能のための CFSoE をイネーブルにしなければなりません。vPC をイネーブルにしてこれらのコマンドのいずれかを入力すると、エラー メッセージが表示されます。

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

CFS は、TCP/IP を介したデータも転送します。IP 経由の CFS の詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。

（注） CFS リージョンはサポートされていません。

vPC および孤立ポート

vPC 対応でないデバイスが各ピアに接続するとき、接続されたポートは vPC のメンバではないため、孤立ポートと称されます。一方のピアへのデバイスのリンクがアクティブ（フォワーディング）になり、他方のリンクは STP のためスタンバイ（ブロッキング）になります。

ピア リンク障害またはリストアが発生すると、孤立ポートの接続は vPC 障害または復元プロセスにバインドされる可能性があります。たとえば、デバイスのアクティブな孤立ポートがセカンダリ vPC ピアに接続する場合、ピア リンク障害が発生し、vPC ポートがセカンダリ ピアによって一時停止されると、そのデバイスはプライマリ ピアを経由する接続を失います。セカンダリ ピアがアクティブな孤立ポートも一時停止した場合は、デバイスのスタンバイ ポートがアクティブになり、プライマリ ピアへの接続が提供され、接続が復元されます。セカンダリ ピアが vPC ポートを一時停止するときに特定の孤立ポートがそのピアによって一時停止され、vPC が復元されるとそのポートが復元されるように CLI で設定できます。

仮想化のサポート

1 つの vPC 内のすべてのポートが、同じ VDC 内になくてはなりません。このバージョンのソフトウェアは、VDC ごとに 1 つの vPC ドメインしかサポートしません。各 VDC で 1 ～ 4096 の番号を使用して vPC に番号を付けることができます。

停電後の vPC リカバリ

データセンターの停電時には、vPC を含む両方の Cisco Nexus 9000 シリーズ デバイスがリロードされます。場合によっては、1 つのピアのみが復元される場合があります。機能するピアキープアライブまたはピア リンクがないと、vPC は正常に機能することができません。しかし、Cisco NX-OS リリースによっては、vPC サービスが機能するピアのローカル ポートのみを使用するようにする方法が利用可能です。

自動リカバリ

Cisco Nexus 9000 シリーズ デバイスは、**auto-recovery** コマンドを使用して、そのピアがオンラインになるのに失敗した場合に vPC サービスを復元するように設定できます。この設定は、スタートアップ コンフィギュレーションに保存しなければなりません。リロード時に、ピア リンクがダウンし、3 回連続してピアキープアライブ メッセージが失われた場合、セカンダリ デバイスはプライマリ STP ロールとプライマリ LACP ロールを引き継ぎます。ソフトウェアが vPC を初期化し、そのローカル ポートを稼働させ始めます。ピアがないため、ローカル vPC ポートの一貫性チェックはバイパスされます。デバイスは、自身をそのロール プライオリティに関係なく STP プライマリに選出し、LACP ポート ロールのマスターとしても機能します。

リカバリ後の vPC ピア ロール

ピア デバイスのリロードが完了し、隣接が形成されたら、次のプロセスが発生します。

1. 最初の vPC ピアがその現在のロールを維持して、その他のプロトコルへの任意の移行リセットを回避します。ピアが、他の可能なロールを受け入れます。
2. 隣接が形成されたら、整合性検査が実行され、適切なアクションが取られます。

ハイ アベイラビリティ

In-Service Software Upgrade（ISSU）では、最初の vPC デバイス上のソフトウェア リロード プロセスが、vPC 通信チャネルを介した CFS メッセージングを使用して、その vPC ピア デバイスをロックします。1 度に 1 つのデバイスだけアップグレードできます。最初のデバイスは、そのアップグレードが完了したら、そのピア デバイスのロックを解除します。次に、2 つ目のデバイスが、最初のデバイスが行ったのと同じように最初のデバイスをロックして、アップグレード プロセスを実行します。アップグレード中は、2 つの vPC デバイスが一時的に異なるリリースの Cisco NX-OS を実行することになりますが、その下位互換性サポートにより、システムは正常に機能します。

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

vPC 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 9000 シリーズ スイッチのペアから異なる Cisco Nexus 9000 シリーズ 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。一般に、このシナリオによって、Cisco Nexus 9508 vPC ピア ノードのペアから Cisco Nexus 9516 スイッチのペアに移行できます。

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稼働するのを遅延するには、**interfaces-vlan** オプションを **delay restore** コマンドに使用します。

- 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	Primary スティッキビット：False	セカンダリ	セカンダリ（Secondary） スティッキビット：False
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	Primary スティッキビット：False	セカンダリ	セカンダリ（Secondary） 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
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	Primary スティッキビット：False	n/a	n/a
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	Primary スティッキビット：False	セカンダリ	セカンダリ（Secondary） スティッキビット：False
5	New_Node2 のすべての vPC とアップリンク ポートを起動します。	トラフィックは Node1 と New_Node2 の両方によって転送されます。	プライマリ	Primary スティッキビット：False	セカンダリ	セカンダリ（Secondary） 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	Primary スティッキビット：False	セカンダリ	セカンダリ（Secondary） 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
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。	n/a	n/a	セカンダリ	Primary 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（Secondary） スティッキビット：False	セカンダリ	Primary スティッキビット：True
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（Secondary） スティッキビット：False	セカンダリ	Primary 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 のライセンス要件

次の表に、この機能のライセンス要件を示します。

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

注意事項と制約事項

vPC 設定時の注意事項と制限事項は次のとおりです。

- **show** コマンドで **internal** キーワードを指定することは、サポートされていません。
- vPC ピアは、アップグレードまたはダウングレード プロセス中に、異なるバージョンの NX-OS ソフトウェアのみを稼働できます。
- アップグレード/ダウングレード期間外に異なるバージョンを実行する vPC ピアはサポートされません。
- 1 つの vPC のすべてのポートが、同じ VDC 内になくてはなりません。
- vPC を設定するには、まず vPC をイネーブルにする必要があります。
- システムが vPC ピア リンクを形成するには、その前にピアキープアライブ リンクとピアキープアライブ メッセージを設定する必要があります。
- vPC に入れられるのは、レイヤ 2 ポート チャネルだけです。
- 両方の vPC ピア デバイスを設定しなければなりません。設定が片方のデバイスから他方へ送信されることはありません。
- マルチレイヤ（バックツーバック）vPC を設定するには、それぞれの vPC に一意の vPC ドメイン ID を割り当てる必要があります。
- 必要な設定パラメータが、vPC ピア リンクの両側で互換性を保っているかチェックしてください。互換性の推奨については、「vPC インターフェイスの互換パラメータ」の項を参照してください。
- vPC の設定中に、最小限のトラフィックの中断が発生する可能性があります。
- vPC 上での BIDR PIM はサポートされていません。
- vPC 環境での DHCP スヌーピング、DAI、IPSG はサポートされていません。DHCP リレーはサポートされています。
- CFS リージョンはサポートされていません。

- ポート チャネル上でのポート セキュリティは、サポートされていません。
- vPC 内の LACP を使用するすべてのポート チャネルを、アクティブ モードのインターフェイスで設定することを推奨します。
- この目的には VLAN ネットワーク インターフェイスを使用するよりも、vPC ピア デバイスからのルーティングのためのレイヤ 3 リンクを別途設定してください。
- バックツーバックのマルチレイヤ vPC トポロジでは、それぞれの vPC に一意のドメイン ID が必要です。
- vPC 経由の レイヤ 3 の設定は、サポートされていません。
- ダブルサイド vPC 上のすべてのノードで同じ Hot Standby Router Protocol（HSRP）/Virtual Router Redundancy Protocol（VRRP）グループを持つことは、Cisco NX-OS 7.0(3)I2(1) 以降のリリースでサポートされています。
- スパイン ノードのペアから Cisco Nexus 9000 デバイスのペアに移行する場合は、Cisco Nexus 9000 vPC ピアがアクティブ/スタンバイ状態になるように HSRP プライオリティを設定する必要があります。HSRP 状態の Cisco Nexus 9000 vPC をアクティブ/リッスン状態またはスタンバイ/リッスン状態にすることはサポートされていません（7(0)I2(2) 以降）。
- vPC を使用する場合は、FHRP（HSRP、VRRP）にデフォルトのタイマーを使用し、PIM 設定を行うことを推奨します。アグレッシブ タイマーを vPC 設定で使用すると、コンバージェンス時間のメリットがありません。
- vPC 環境で open shortest path first（OSPF）を設定する場合は、コア スイッチ上でルータ コンフィギュレーション モードで次のタイマー コマンドを使用することにより、vPC ピア リンクがシャットダウンしたときに OSPF の高速コンバージェンスを実現します。

```
switch (config-router)# timers throttle spf 1 50 50
switch (config-router)# timers lsa-arrival 10
```

  OSPF に関する詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。
- HSRP の BFD は、vPC 環境ではサポートされていません。
- STP ポート コストは、vPC 環境で 200 に固定されています。
- ジャンボ フレームは、vPC ピア リンクではデフォルトでイネーブルです。
- vPC がダウンし、トラフィックがピアリンクを通過する必要があるときに、増加するトラフィックに対応するためのベストプラクティスは、ピアリンクのラインカードを横断して複数の高帯域幅インターフェイス（Cisco Nexus 9000 の 40G インターフェイスなど）を使用することです。
- **vpc orphan-ports suspend** コマンドは、非 vPC VLAN のポートおよびレイヤ 3 ポートにも適用されます。ただし、VPC VLAN のポートで使用することをお勧めします。
- FEX vPC は、FEX（任意のモデル）と親スイッチとしての Cisco Nexus 9300（TOR）および Cisco Nexus 9500（EOR）シリーズ スイッチの間ではサポートされません。

- NX-OS 7.0(3)I2(2) 以降では、以前に ip pim pre-build-spt コマンドによって提供されていた動作がデフォルトで自動的にイネーブルになっており、ディセーブルにはできません。
- NX-OS 7.0(3)I2(2) 以降では、個別の状態で動作する vPC ポートチャネル メンバー リンクが、VLAN の不整合の検査時にフラップされます。サーバのプロビジョニング時にリンクがフラップされることを回避するには、**no graceful consistency-check** コマンドによって vPC グレースフル整合性検査をディセーブルにします。

  次に、vPC グレースフル整合性検査をディセーブルにする例を示します。

```
switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.

switch(config)# vpc domain 1
switch(config-vpc-domain)# no graceful consistency-check
```

デフォルト設定

次の表は、vPC パラメータのデフォルト設定をまとめたものです。

表 *13*：デフォルト *vPC* パラメータ

パラメータ（Parameters）	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

（注） vPC ピア リンクの両側のデバイス両方でこれらの手順を使用する必要があります。両方の vPC ピア デバイスをこの手順で設定します。

ここでは、コマンドライン インターフェイス（CLI）を使用して vPC を設定する方法を説明します。

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

vPC のイネーブル化

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

手順の概要

1. **configure terminal**
2. **feature vpc**
3. **exit**
4. **show feature**
5. **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	**feature vpc** 例： `switch(config)# feature vpc`	デバイス上で vPC をイネーブルにします。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show feature** 例： `switch# show feature`	（任意）デバイス上でイネーブルになっている機能を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例は、vPC 機能をイネーブルにする方法を示します。

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

vPC のディセーブル化

（注） vPC 機能をディセーブルにすると、デバイス上のすべての vPC 設定がクリアされます。

手順の概要

1. **configure terminal**
2. **no feature vpc**
3. **exit**
4. **show feature**
5. **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	**no feature vpc** 例： `switch(config)# no feature vpc`	デバイスの vPC をディセーブルにします。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show feature** 例： `switch# show feature`	（任意）デバイス上でイネーブルになっている機能を表示します。

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

次の例は、vPC 機能をディセーブルにする方法を示します。

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

vPC ドメインの作成と vpc-domain モードの開始

vPC ドメインを作成し、両方の vPC ピア デバイス上で vPC ピア リンク ポート チャネルを同じ vPC ドメイン内に置くことができます。1 つの VDC 全体を通じて一意の vPC ドメイン番号を使用してください。このドメイン ID は、vPC システム MAC アドレスを自動的に形成するのに使用されます。

このコマンドを使用して、vpc-domain コマンド モードを開始することもできます。

手順の概要

1. **configure terminal**
2. **vpc domain***domain-id* [**shut** | **no shut**]
3. **exit**
4. **show vpc brief**
5. **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	**vpc domain***domain-id* [**shut**	**no shut**]
		
		例：
		`switch(config)# vpc domain 5`
		`switch(config-vpc-domain)#`
			デバイス上に vPC ドメインを作成し、設定目的で vpc-domain コンフィギュレーション モードを開始します。デフォルトはありません。指定できる範囲は 1 ～ 1000 です。

	コマンドまたはアクション	目的

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		vpc-domain コンフィギュレーション モードを終了します。

ステップ 4	**show vpc brief** 例： `switch# show vpc brief`	（任意）各 vPC ドメインに関する簡単な情報を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、vpc-domain コマンド モードを開始して、既存の vPC ドメインを設定する例を示します。

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

vPC キープアライブ リンクと vPC キープアライブ メッセージの設定

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

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

（注） vPC ピアキープアライブ リンクを使用する際は、個別の VRF インスタンスを設定して、各 vPC ピア デバイスからその VRF にレイヤ 3 ポートを接続することを推奨します。ピア リンク自体を使用して vPC ピアキープアライブ メッセージを送信しないでください。VRF の作成および設定方法については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。ピアキープアライブ メッセージに使用される送信元と宛先の両方の IP アドレスがネットワーク内で一意であることを確認してください。管理ポートと管理 VRF が、これらのキープアライブ メッセージのデフォルトです。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain***domain-id* [**shut** | **no shut**]
3. **peer-keepalivedestination***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. **exit**
5. **show vpc statistics**
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	**vpc domain***domain-id* [**shut**	**no shut**]
		
		例：
		`switch(config)# vpc domain 5`
		`switch(config-vpc-domain)#`
			デバイスで vPC ドメインを作成し、vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**peer-keepalivedestination***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**}] 例： `switch(config-vpc-domain)# peer-keepalive destination 172.28.230.85` `switch(config-vpc-domain)#`	vPC ピアキープアライブ リンクのリモート エンドの IPv4 アドレスを設定します。 （注） vPC ピアキープアライブ リンクを設定するまで、vPC ピア リンクは構成されません。 管理ポートと VRF がデフォルトです。 （注） 独立した VRF を設定し、vPC ピアキープアライブ リンクのための VRF 内の各 vPC ピア デバイスからのレイヤ 3 ポートを使用することを推奨します。VRF の作成および設定の詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

	コマンドまたはアクション	目的

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 5	**show vpc statistics** 例： `switch# show vpc statistics`	（任意）キープアライブ メッセージの設定に関する情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

VRF の設定方法については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

次の例は、vPC ピアキープアライブ リンクの宛先と送信元の IP アドレスおよび VRF を設定する方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 100
switch(config-vpc-domain)# peer-keepalive destination 172.168.1.2 source 172.168.1.1 vrf
vpc-keepalive
switch(config-vpc-domain)# exit
switch#
```

vPC ピア リンクの作成

vPC ピア リンクを作成するには、指定した vPC ドメインのピア リンクとするポート チャネルを各デバイス上で指定します。冗長性を確保するため、トランク モードで vPC ピア リンクとして指定したレイヤ 2 ポート チャネルを設定し、各 vPC ピア デバイス上の個別のモジュールで 2 つのポートを使用することを推奨します。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

手順の概要

1. **configure terminal**
2. **interface port-channel***channel-number*
3. **switchport mode trunk**
4. **switchport trunk allowed vlan***vlan-list*
5. **vpc peer-link**
6. **exit**
7. **show vpc brief**
8. **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***channel-number*
	
	例：
	`switch(config)# interface port-channel 20`
	`switch(config-if)#`
		このデバイスの vPC ピア リンクとして使用するポート チャネルを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**switchport mode trunk** 例： `switch(config-if)# switchport mode trunk`	（任意）このインターフェイスをトランク モードで設定します。
ステップ 4	**switchport trunk allowed vlan***vlan-list* 例： `switch(config-if)# switchport trunk allowed vlan 1-120,201-3967`	（任意）許容 VLAN リストを設定します。

ステップ 5	**vpc peer-link**
	
	例：
	`switch(config-if)# vpc peer-link`
	`switch(config-vpc-domain)#`
		選択したポート チャネルを vPC ピア リンクとして設定し、vpc-domain コンフィギュレーション モードを開始します。

ステップ 6	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		vpc-domain コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 7	**show vpc brief** 例： `switch# show vpc brief`	（任意）各 vPC に関する情報を表示します。vPC ピア リンクに関する情報も表示されます。
ステップ 8	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例は、vPC ピア リンクを設定する方法を示します。

```
switch# configure terminal
switch(config)# interface port-channel 20
switch(config-if)# switchport mode
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1-120,201-3967
switch(config-if)# vpc peer-link
switch(config-vpc-domain)# exit
switch(config)#
```

vPC ピアゲートウェイの設定

vPC ピア デバイスを、vPC ピア デバイスの MAC アドレスに送信されるパケットに対してゲートウェイとして機能するように設定できます。

（注） vPC ドメインにレイヤ 3 デバイスを接続した場合、vPC ピアリンク上でも送信される VLAN を使用したルーティング プロトコルのピアリンクはサポートされません。vPC ピア デバイスおよび汎用レイヤ 3 デバイスの間でルーティング プロトコルの隣接関係が必要な場合は、相互接続に物理的にルーティングされたインターフェイスを使用する必要があります。vPC ピアゲートウェイ機能の使用では、この要件は変わりません。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain***domain-id* [**shut** | **no shut**]
3. **peer-gateway**
4. **exit**
5. **show vpc brief**
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	**vpc domain***domain-id* [**shut** | **no shut**]
	
	例：
	`switch(config-if)# vpc domain 5`
	`switch(config-vpc-domain)#`
		vPC ドメインがまだ存在していない場合はそれを作成し、vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**peer-gateway** 例： `switch(config-vpc-domain)# peer-gateway` （注） この機能を正常に動作させるために、この vPC ドメインのすべてのインターフェイス VLAN 上で IP リダイレクトをディセーブルにします。	ピアのゲートウェイ MAC アドレスを宛先とするパケットのレイヤ 3 フォワーディングをイネーブルにします。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		vpc-domain コンフィギュレーション モードを終了します。

ステップ 5	**show vpc brief** 例： `switch# show vpc brief`	（任意）各 vPC に関する情報を表示します。vPC ピア リンクに関する情報も表示されます。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

グレースフル整合性検査の設定

デフォルトでイネーブルになるグレースフル整合性検査機能を設定できます。この機能がイネーブルでない場合、必須互換性パラメータの不一致が動作中の vPC で導入されると、vPC は完全に一時停止します。この機能がイネーブルの場合、セカンダリ ピアデバイスのリンクだけが一時停止します。vPC での一貫した設定については、「vPC インターフェイスの互換パラメータ」の項を参照してください。

手順の概要

1. **configure terminal**
2. **vpc domain***domain-id* [**shut** | **no shut**]
3. **graceful consistency-check**
4. **exit**
5. **show vpc brief**

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	**vpc domain***domain-id* [**shut**	**no shut**]
		
		例：
		`switch(config-if)# vpc domain 5`
		`switch(config-vpc-domain)#`
			vPC ドメインがまだ存在していない場合はそれを作成し、vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**graceful consistency-check** 例： `switch(config-vpc-domain)# graceful consistency-check`	必須互換性パラメータで不一致が検出された場合に、セカンダリ ピア デバイスのリンクのみが一時停止するということを指定します。 この機能をディセーブルにする場合は、このコマンドの **no** 形式を使用します。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		vpc-domain コンフィギュレーション モードを終了します。

ステップ 5	**show vpc brief** 例： `switch# show vpc brief`	（任意）vPC に関する情報を表示します。

次に、グレースフル整合性検査機能をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# graceful consistency-check
switch(config-vpc-domain)# exit
switch(config)#
```

vPC ピア リンクの設定の互換性チェック

両方の vPC ピア デバイス上の vPC ピア リンクを設定した後に、すべての vPC インターフェイスで設定が一貫していることをチェックします。vPC での一貫した設定については、「vPC インターフェイスの互換パラメータ」の項を参照してください。

手順の概要

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

ステップ 2	**show vpc consistency-parameters** {**global** | **interface port-channel***channel-number*}
	
	例：
	`switch(config)# show vpc consistency-parameters global`
	`switch(config)#`
		（任意）すべての vPC インターフェイス全体で一貫している必要があるパラメータのステータスを表示します。

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

```
switch# configure terminal
switch(config)# show vpc consistency-parameters global
switch(config)#
```

（注） vPC インターフェイス設定の互換性に関するメッセージが syslog にも記録されます。

他のポート チャネルの vPC への移行

冗長性を確保するために、vPC ドメイン ダウンストリーム ポート チャネルを 2 つのデバイスに接続することを推奨します。

ダウンストリーム デバイスに接続するには、ダウンストリーム デバイスからプライマリ vPC ピア デバイスへのポート チャネルを作成し、ダウンストリーム デバイスからセカンダリ ピア デバ

イスへのもう 1 つのポート チャネルを作成します。各 vPC ピア デバイス上で、ダウンストリームデバイスに接続するポート チャネルに vPC 番号を割り当てます。vPC の作成時にトラフィックが中断されることはほとんどありません。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

レイヤ 2 ポート チャネルを使用していることを確認します。

手順の概要

1. **configure terminal**
2. **interface port-channel***channel-number*
3. **vpc***number*
4. **exit**
5. **show vpc brief**
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***channel-number*
	
	例：
	`switch(config)# interface port-channel 20`
	`switch(config-if)#`
		ダウンストリーム デバイスに接続するために vPC に入れるポート チャネルを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**vpc***number*
	
	例：
	`switch(config-if)# vpc 5`
	`switch(config-vpc-domain)#`
		選択したポート チャネルを vPC に入れてダウンストリーム デバイスに接続するように設定します。これらのポート チャネルには、デバイス内の任意のモジュールを使用できます。有効な範囲は 1 ～ 4096 です。
		（注） vPC ピア デバイスからダウンストリーム デバイスに接続されているポート チャネルに割り当てる vPC 番号は、両方の vPC デバイスで同じでなければなりません。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		vpc-domain コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 5	**show vpc brief** 例： `switch# show vpc brief`	（任意）vPC に関する情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、ダウンストリーム デバイスに接続するポート チャネルを設定する例を示します。

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

vPC ドメイン MAC アドレスの手動での設定

vPC ドメインを作成すると、Cisco NX-OS ソフトウェアが自動的に vPC システム MAC アドレスを作成します。このアドレスは、LACP など、リンク スコープに制限される操作に使用されます。ただし、vPC ドメインの MAC アドレスを手動で設定するように選択することもできます。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain***domain-id* [**shut** | **no shut**]
3. **system-mac***mac-address*
4. **exit**
5. **show vpc role**
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	**vpc domain***domain-id* [**shut** | **no shut**]
	
	例：
	`switch(config)# vpc domain 5`
	`switch(config-vpc-domain)#`
		設定する vPC ドメインの番号を入力します。システムは、vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**system-mac***mac-address*
	
	例：
	`switch(config-vpc-domain)# system-mac 23fb.4ab5.4c4e`
	`switch(config-vpc-domain)#`
		指定した vPC ドメインに割り当てる MAC アドレスを aaaa.bbbb.cccc の形式で入力します。

ステップ 4	**exit**
	
	例：
	`switch(config-vpc-domain)# exit`
	`switch#`
		vpc-domain コンフィギュレーション モードを終了します。

ステップ 5	**show vpc role** 例： `switch# show vpc brief`	（任意）vPC システム MAC アドレスを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例は、vPC ドメイン MAC アドレスを手動で設定する方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# system-mac 13gb.4ab5.4c4e
switch(config-vpc-domain)# exit
switch(config)#
```

システム プライオリティの手動での設定

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

（注） LACP の実行時には、vPC ピア デバイスが LACP のプライマリ デバイスになるように、vPC システム プライオリティを手動で設定することを推奨します。システム プライオリティを手動で設定する場合には、必ず同じプライオリティ値を両方の vPC ピア デバイスに設定します。これらの値が一致しないと、vPC は起動しません。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain***domain-id* [**shut** | **no shut**]
3. **system-priority***priority*
4. **exit**
5. **show vpc role**
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	**vpc domain***domain-id* [**shut**	**no shut**]
		
		例：
		`switch(config)# vpc domain 5`
		`switch(config-vpc-domain)#`
			設定する vPC ドメインの番号を入力します。システムは、vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**system-priority***priority*
	
	例：
	`switch(config-vpc-domain)# system-priority 4000`
	`switch(config-vpc-domain)#`
		指定した vPC ドメインに割り当てるシステム プライオリティを入力します。指定できる値の範囲は、1 ～ 65535 です。デフォルト値は 32667 です。

ステップ 4	**exit**
	
	例：
	`switch(config-vpc-domain)# exit`
	`switch#`
		vpc-domain コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 5	**show vpc role** 例： `switch# show vpc role`	（任意）vPC システム プライオリティを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例は、vPC ドメインのシステム プライオリティを手動で設定する方法を示します。

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

vPC ピア デバイス ロールの手動での設定

デフォルトでは、vPC ドメインと、vPC ピア リンクの両端を設定すると、Cisco NX-OS ソフトウェアはプライマリとセカンダリの vPC ピア デバイスを選択します。ただし、vPC のプライマリ デバイスとして、特定の vPC ピア デバイスを選択することもできます。選択したら、プライマリ デバイスにする vPC ピア デバイスに、他の vPC ピア デバイスより小さいロール値を手動で設定します。

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

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain***domain-id* [**shut** | **no shut**]
3. **role priority***priority*
4. **exit**
5. **show vpc role**
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	**vpc domain***domain-id* [**shut** | **no shut**]
	
	例：
	`switch(config)# vpc domain 5`
	`switch(config-vpc-domain)#`
		設定する vPC ドメインの番号を入力します。システムは、vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**role priority***priority*
	
	例：
	`switch(config-vpc-domain)# role priority 4`
	`switch(config-vpc-domain)#`
		vPC システム プライオリティとして使用するロール プライオリティを指定します。値の範囲は 1 ～ 65636 で、デフォルト値は 32667 です。低い値は、このスイッチがプライマリ vPC になる可能性が高いということを意味します。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		vpc-domain コンフィギュレーション モードを終了します。

ステップ 5	**show vpc role** 例： `switch# show vpc role`	（任意）vPC システム プライオリティを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例は、vPC ピア デバイスのロール プライオリティを手動で設定する方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# role priority 4
switch(config-vpc-domain)# exit
switch(config)#
```

シングルモジュール vPC でのトラッキング機能の設定

すべての vPC ピア リンクとコアに面するインターフェイスを単一モジュール上で設定しなければならない場合は、両方のプライマリ vPC ピア デバイス上の vPC ピア リンクのすべてのリンク上

にあり、コアへのレイヤ 3 リンクに関連付けられているトラック オブジェクトとトラック リストを設定しなければなりません。いったんこの機能を設定したら、プライマリ vPC ピア デバイスに障害が発生した場合には、プライマリ vPC ピア デバイス上のすべての vPC リンクを、システムが自動的に停止します。システムが安定するまでは、このアクションにより、すべての vPC トラフィックが強制的にセカンダリ vPC ピア デバイスに送られます。

この設定は、両方の vPC ピア デバイスに置かなければなりません。さらに、いずれの vPC ピア デバイスも機能上のプライマリ vPC ピア デバイスになる場合があるため、両方の vPC ピア デバイスに同じ設定を置いておく必要があります。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

トラック オブジェクトとトラック リストが設定済みであることを確認します。コアおよび vPC ピア リンクに接続されているすべてのインターフェイスが両方の vPC ピア デバイス上のトラック リンク オブジェクトに割り当てられていることを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain***domain-id* [**shut** | **no shut**]
3. **track***track-object-id*
4. **exit**
5. **show vpc brief**
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	**vpc domain***domain-id* [**shut**	**no shut**]
		
		例：
		`switch(config)# vpc domain 5`
		`switch(config-vpc-domain)#`
			設定する vPC ドメインの番号を入力し、vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**track***track-object-id*
	
	例：
	`switch(config-vpc-domain)# track object 23`
	`switch(config-vpc-domain)#`
		以前に関連するインターフェイスで設定されたトラック リスト オブジェクトを vPC ドメインに追加します。オブジェクト トラッキングおよびトラック リストの詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

	コマンドまたはアクション	目的

ステップ 4	**exit**
	
	例：
	`switch(config-vpc-domain)# exit`
	`switch#`
		vpc-domain コンフィギュレーション モードを終了します。

ステップ 5	**show vpc brief** 例： `switch# show vpc brief`	（任意）追跡対象オブジェクトに関する情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、以前に設定されたトラック リスト オブジェクトを、vPC ピア デバイス上の vPC ドメインに配置する例を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# track object 5
switch(config-vpc-domain)# exit
switch(config)#
```

停電後のリカバリの設定

停電が発生すると、vPC はピア隣接がスイッチ リロード時に形成するのを待ちます。この状況は、許容範囲内に収まらないほど長いサービスの中断に至る場合があります。Cisco Nexus 9000 シリーズ デバイスは、そのピアがオンラインになるのに失敗した場合に vPC サービスを復元するように設定できます。

リロード復元の設定

ここで説明されている **reload restore** コマンドおよび手順は廃止されます。「自動リカバリの設定」で説明されている **auto-recovery** コマンドおよび手順を使用することを推奨します。

Cisco Nexus 9000 シリーズ デバイスは、**reload restore** コマンドを使用して、そのピアがオンラインになるのに失敗した場合に vPC サービスを復元するように 設定できます。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain***domain-id* [**shut** | **no shut**]
3. **reload restore** [**delay***time-out*]
4. **exit**
5. **show running-config vpc**
6. **show vpc consistency-parameters interface port-channel***number*
7. **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	**vpc domain***domain-id* [**shut**	**no shut**]
		
		例：
		`switch(config)# vpc domain 5`
		`switch(config-vpc-domain)#`
			設定する vPC ドメインの番号を入力し、vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**reload restore** [**delay***time-out*] 例： `switch(config-vpc-domain)# reload restore`	vPC がそのピアが機能しないことを前提として vPC を稼働させ始めるように設定します。デフォルト遅延値は240秒です。タイムアウト遅延は240 ～ 3600秒の間で設定できます。 vPC をデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

ステップ 4	**exit**
	
	例：
	`switch(config-vpc-domain)# exit`
	`switch#`
		vpc-domain コンフィギュレーション モードを終了します。

ステップ 5	**show running-config vpc** 例： `switch# show running-config vpc`	（任意）vPC に関する情報、特にリロード ステータスを表示します。
ステップ 6	**show vpc consistency-parameters interface port-channel***number* 例： `switch# show vpc consistency-parameters interface port-channel 1`	（任意）指定したインターフェイスの vPC の一貫性パラメータに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： switch# **copy running-config startup-config**	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。 （注） リロード機能がイネーブルになっていることを確認するには、この手順を実行します。

次に、vPC リロード復元機能を設定し、それをスイッチのスタートアップ コンフィギュレーションに保存する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vpc domain 5
switch(config-vpc-domain)# reload restore

Warning:
Enables restoring of vPCs in a peer-detached state after reload, will wait for 240
seconds (by default) to determine if peer is un-reachable

switch(config-vpc-domain)# exit
switch(config)# exit
switch# copy running-config startup-config
switch# show running-config vpc

!Command: show running-config vpc
!Time: Wed Mar 24 18:43:54 2010
version 5.0(2)
feature vpc
logging level vpc 6
vpc domain 5
reload restore
```

次の例は、一貫性パラメータを確認する方法を示します。

```
switch# show vpc consistency-parameters interface port-channel 1

Legend:
Type 1 : vPC will be suspended in case of mismatch
Name Type Local Value Peer Value
------------- ---- ----------- ---------------
STP Port Type 1 Default -
STP Port Guard 1 None -
STP MST Simulate PVST 1 Default -
mode 1 on -
Speed 1 1000 Mb/s -
Duplex 1 full -
Port Mode 1 trunk -
Native Vlan 1 1 -
MTU 1 1500 -
Allowed VLANs - 1-3967,4048-4093
Local suspended VLANs
```

自動リカバリの設定

Cisco Nexus 9000 シリーズ デバイスは、auto-recovery コマンドを使用して、そのピアがオンラインになるのに失敗した場合に vPC サービスを復元するように設定できます。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain***domain-id* [**shut** | **no shut**]
3. **auto-recovery** [**reload-delay***time*]
4. **exit**
5. **show running-config vpc**
6. **show vpc consistency-parameters interface port-channel***number*
7. **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	**vpc domain***domain-id* [**shut**	**no shut**]
		
		例：
		`switch(config)# vpc domain 5`
		`switch(config-vpc-domain)#`
			設定する vPC ドメインの番号を入力し、vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**auto-recovery** [**reload-delay***time*]
	
	例：
	`switch(config-vpc-domain)#`
	`auto-recovery`
		vPC がそのピアが機能しないことを前提として vPC を稼働させ始めるように設定し、vPC を復元するためのリロード後に待機する時間を指定します。デフォルト遅延値は 240 秒です。240 ~ 3600 秒の遅延を設定できます。
		vPC をデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

ステップ 4	**exit**
	
	例：
	`switch(config-vpc-domain)# exit`
	`switch#`
		vpc-domain コンフィギュレーション モードを終了します。

ステップ 5	**show running-config vpc** 例： `switch# show running-config vpc`	（任意）vPC に関する情報、特にリロード ステータスを表示します。

	コマンドまたはアクション	目的
ステップ 6	**show vpc consistency-parameters interface port-channel***number* 例： `switch# show vpc consistency-parameters interface port-channel 1`	（任意）指定したインターフェイスの vPC の一貫性パラメータに関する情報を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。 （注） 自動リカバリ機能がイネーブルになっていることを確認するには、この手順を実行します。

次に、vPC 自動リカバリ機能を設定し、それをスイッチのスタートアップ コンフィギュレーションに保存する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vpc domain 5
switch(config-vpc-domain)# auto-recovery

Warning:
Enables restoring of vPCs in a peer-detached state after reload, will wait for 240
seconds to determine if peer is un-reachable

switch(config-vpc-domain)# exit
switch(config)# exit
switch# copy running-config startup-config
```

孤立ポートの一時停止の設定

vPC 対応でないデバイスが各ピアに接続するとき、接続されたポートは vPC のメンバではないため、孤立ポートと称されます。ピア リンクまたはピア キープアライブ障害に応えてセカンダリ ピアが vPC ポートを一時停止するときに、セカンダリ ピアによって一時停止（シャットダウン）される孤立ポートとして物理インターフェイスを明示的に宣言できます。孤立ポートは vPC が復元されたときに復元されます。

（注） vPC 孤立ポートの一時停止は、ポート チャネルのメンバ ポートではなく、物理ポートでのみ設定できます。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

手順の概要

1. **configure terminal**
2. **show vpc orphan-ports**
3. **interface***type slot/port*
4. **vpc orphan-ports suspend**
5. **exit**
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	**show vpc orphan-ports** 例： `switch# show vpc orphan-ports`	（任意）孤立ポートのリストを表示します。

ステップ 3	**interface***type slot/port*
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 4	**vpc orphan-ports suspend** 例： `switch(config-if)# vpc orphan-ports suspend`	選択したインターフェイスを vPC 障害時にセカンダリ ピアにより一時停止される vPC 孤立ポートとして設定します。

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、インターフェイスを vPC 障害時にセカンダリ ピアにより一時停止される vPC 孤立ポートとして設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# vpc orphan-ports suspend
switch(config-if)# exit
switch(config)#
```

vPC ピア スイッチの設定

Cisco Nexus 9000 シリーズ デバイスは、一対の vPC デバイスがレイヤ 2 トポロジ内で 1 つの STP ルートとして現れるように設定することができます。

純粋な vPC ピア スイッチ トポロジの設定

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

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

（注） VPC ピア間の非 VPC 専用トランク リンクを使用する場合は、STP が VLAN をブロックするのを防ぐために、非 VPC VLAN はピアによって異なるグローバル プライオリティが必要です。

手順の概要

1. **configure terminal**
2. **vpc domain***domain-id* [**shut** | **no shut**]
3. **peer-switch**
4. **spanning-tree vlan***vlan-range***priority***value*
5. **exit**
6. **show spanning-tree summary**
7. **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。

	コマンドまたはアクション	目的

ステップ 2	**vpc domain***domain-id* [**shut** | **no shut**]
	
	例：
	`switch(config)# vpc domain 5`
	`switch(config-vpc-domain)#`
		設定する vPC ドメインの番号を入力し、vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**peer-switch** 例： `switch(config-vpc-domain)# peer-switch`	vPC スイッチ ペアがレイヤ 2 トポロジ内で 1 つの STP ルートとして現れるようにします。 ピア スイッチ vPC トポロジをディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 4	**spanning-tree vlan***vlan-range***priority***value* 例： `switch(config)# spanning-tree vlan 1 priority 8192`	VLAN のブリッジ プライオリティを設定します。有効な値は、4096 の倍数です。デフォルト値は 32768 です。

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

ステップ 6	**show spanning-tree summary** 例： `switch# show spanning-tree summary`	（任意）スパニングツリー ポートの状態の概要を表示します。これに、vPC ピア スイッチも含まれます。
ステップ 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vpc domain 5
switch(config-vpc-domain)# peer-switch

2010 Apr 28 14:44:44 switch %STP-2-VPC_PEERSWITCH_CONFIG_ENABLED: vPC peer-switch
configuration is enabled. Please make sure to configure spanning tree "bridge" priority as
per recommended guidelines to make vPC peer-switch operational.

switch(config-vpc-domain)# spanning-tree vlan 1 priority 8192
switch(config-vpc-domain)# exit
switch(config)#
```

ハイブリッド vPC ピア スイッチ トポロジの設定

spanning-tree pseudo-information コマンドを使用して STP VLAN ベースのロード バランシング条件を満たすように代表ブリッジ ID を変更した後、ルート ブリッジ ID を最高のブリッジ プライオリティよりもよい値に変更することにより、ハイブリッド vPC または非 vPC ピア スイッチ トポロジを設定することができます。次に、ピア スイッチをイネーブルにします。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

VPC ピア間の非 VPC 専用トランク リンクを使用する場合は、STP が VLAN をブロックするのを防ぐために、非 VPC VLAN はピアによって異なる疑似ルート プライオリティが必要です。

手順の概要

1. **configure terminal**
2. **spanning-tree pseudo-information**
3. **vlan***vlan-id***designated priority***priority*
4. **vlan***vlan-id***root priority***priority*
5. **vpc domain***domain-id* [**shut** | **no shut**]
6. **peer-switch**
7. **exit**
8. **show spanning-tree summary**
9. **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	**spanning-tree pseudo-information**
	
	例：
	`switch(config)# spanning-tree pseudo-information`
	`switch(config-pseudo)#`
		スパニングツリー疑似情報を設定します。

ステップ 3	**vlan***vlan-id***designated priority***priority* 例： `switch(config-pseudo)# vlan 1 designated priority 8192`	VLANの指定ブリッジプライオリティを設定します。有効な値は、0 ～ 61440 の範囲内の 4096 の倍数です。

	コマンドまたはアクション	目的
ステップ 4	**vlan***vlan-id***root priority***priority* 例： `switch(config-pseudo)# vlan 1 root priority 4096`	VLAN のルート ブリッジ プライオリティを設定します。有効な値は、0 ～ 61440 の範囲内の 4096 の倍数です。

ステップ 5	**vpc domain***domain-id* [**shut** | **no shut**]
	
	例：
	`switch(config)# vpc domain 5`
	`switch(config-vpc-domain)#`
		設定する vPC ドメインの番号を入力し、vpc-domain コンフィギュレーション モードを開始します。

ステップ 6	**peer-switch** 例： `switch(config-vpc-domain)# peer-switch`	vPC スイッチ ペアがレイヤ 2 トポロジ内で 1 つの STP ルートとして現れるようにします。 ピア スイッチ vPC トポロジをディセーブルにするには、このコマンドの **no** 形式を使用します。

ステップ 7	**exit**
	
	例：
	`switch(config-vpc-domain)# exit`
	`switch#`
		vpc-domain コンフィギュレーション モードを終了します。

ステップ 8	**show spanning-tree summary** 例： `switch# show spanning-tree summary`	（任意）スパニングツリー ポートの状態の概要を表示します。これに、vPC ピア スイッチも含まれます。
ステップ 9	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

vPC 設定の確認

vPC 設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show feature	vPC がイネーブルになっているかどうかを表示します。
show vpc brief	vPC に関する要約情報を表示します。
show vpc consistency-parameters	すべての vPC インターフェイス全体で一貫している必要があるパラメータのステータスを表示します。
show running-config vpc	vPC の実行コンフィギュレーションの情報を表示します。
show port-channel capacity	設定されているポートチャネルの数、およびデバイス上でまだ使用可能なポートチャネル数を表示します。
show vpc statistics	vPC に関する統計情報を表示します。
show vpc peer-keepalive	ピアキープアライブ メッセージに関する情報を表示します。
show vpc role	ピア ステータス、ローカルデバイスのロール、vPC システム MAC アドレスとシステム プライオリティ、およびローカル vPC デバイスの MAC アドレスとプライオリティを表示します。

vPC のモニタリング

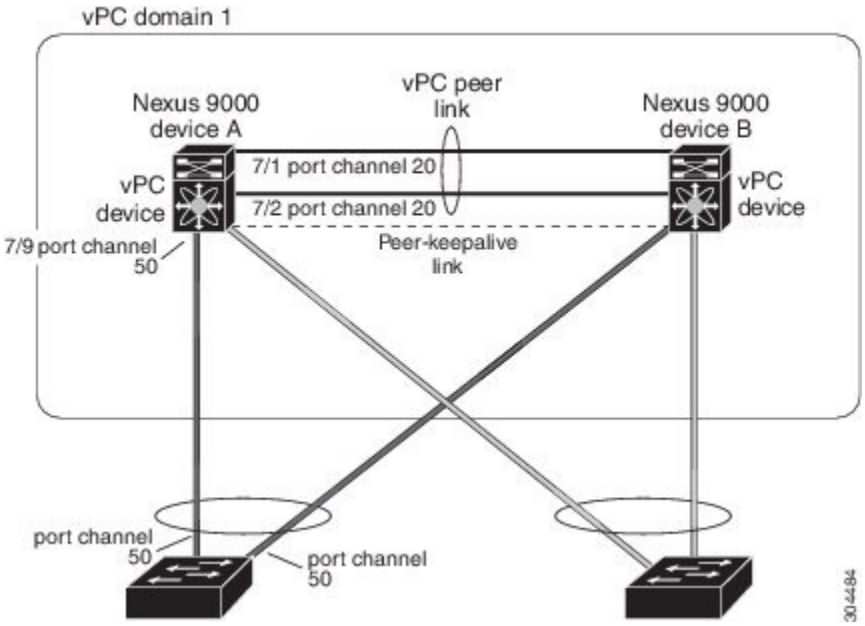
vPC 統計情報を表示するには、**show vpc statistics** コマンドを使用します。

（注） このコマンドは、現在作業している vPC ピア デバイスの vPC 統計情報しか表示しません。

vPC の設定例

次の例は、図に示すように、デバイス A 上で vPC を設定する方法を示します。

図 *26*：*vPC* の設定例



1 vPC および LACP をイネーブルにします。

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

2 （任意）ピア リンクにするインターフェイスの 1 つを専用モードに設定します。

```
switch(config)# interface ethernet 7/1,
ethernet 7/3, ethernet 7/5. ethernet 7/7
switch(config-if)# shutdown
switch(config-if)# exit
switch(config)# interface ethernet 7/1
switch(config-if)# rate-mode dedicated
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)#
```

3 （任意）ピア リンクにする 2 つ目の冗長インターフェイスを専用ポート モードに設定します。

```
switch(config)# interface ethernet 7/2, ethernet 7/4,
ethernet 7/6. ethernet 7/8
switch(config-if)# shutdown
switch(config-if)# exit
switch(config)# interface ethernet 7/2
switch(config-if)# rate-mode dedicated
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)#
```

4 ピア リンクに入れる 2 つのインターフェイス（冗長性のために）をアクティブ レイヤ 2 LACP ポート チャネルに設定します。

```
switch(config)# interface ethernet 7/1-2
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1-50
switch(config-if)# switchport trunk native vlan 20
switch(config-if)# channel-group 20 mode active
switch(config-if)# exit
```

5 VLAN を作成し、イネーブルにします。

```
switch(config)# vlan 1-50
switch(config-vlan)# no shutdown
switch(config-vlan)# exit
```

6 vPC ピアキープアライブ リンク用の独立した VEF を作成し、レイヤ 3 インターフェイスをその VRF に追加します。

```
switch(config)# vrf context pkal
switch(config-vrf)# exit
switch(config)# interface ethernet 8/1
switch(config-if)# vrf member pkal
switch(config-if)# ip address 172.23.145.218/24
switch(config-if)# no shutdown
switch(config-if)# exit
```

7 vPC ドメインを作成し、vPC ピアキープアライブ リンクを追加します。

```
switch(config)# vpc domain 1
switch(config-vpc-domain)# peer-keepalive
 destination 172.23.145.217 source 172.23.145.218 vrf pkal
switch(config-vpc-domain)# exit
```

8 vPC ピア リンクを設定します。

```
switch(config)# interface port-channel 20
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1-50
switch(config-if)# vpc peer-link
switch(config-if)# exit
switch(config)#
```

9 vPC のダウンストリーム デバイスへのポート チャネルのインターフェイスを設定します。

```
switch(config)# interface ethernet 7/9
switch(config-if)# switchport mode trunk
switch(config-if)# allowed vlan 1-50
switch(config-if)# native vlan 20
switch(config-if)# channel-group 50 mode active
switch(config-if)# exit
switch(config)# interface port-channel 50
switch(config-if)# vpc 50
switch(config-if)# exit
switch(config)#
```

10 設定を保存します。

```
switch(config)# copy running-config startup-config
```

（注） まずポート チャネルを設定する場合は、それがレイヤ 2 ポート チャネルであることを確認してください。

関連資料

関連項目	関連項目
システム管理	システム管理
ハイ アベイラビリティ	ハイ アベイラビリティ
リリース ノート	リリース ノート

第 9 章

IP トンネルの設定

この章では、Cisco NX-OS デバイスで Generic Route Encapsulation（GRE）を使って IP トンネルを設定する手順について説明します。

IP トンネルについて

IP トンネルを使うと、同じレイヤまたは上位層プロトコルをカプセル化して、2 台のデバイス間で作成されたトンネルを通じて IP に結果を転送できます。

IP トンネルの概要

IP トンネルは次の 3 つの主要コンポーネントで構成されています。

- パッセンジャ プロトコル：カプセル化する必要があるプロトコル。パッセンジャ プロトコルの例には IPv4 があります。
- キャリア プロトコル：パッセンジャ プロトコルをカプセル化するために使用するプロトコル。Cisco NX-OS はキャリア プロトコルとして GRE をサポートします。

- トランスポートプロトコル：カプセル化したプロトコルを伝送するために使用するプロトコル。トランスポートプロトコルの例には IPv4 があります。IP トンネルは IPv4 などのパッセンジャ プロトコルを使用し、このプロトコルを GRE などのキャリア プロトコル内にカプセル化します。次に、このキャリア プロトコルは IPv4 などのトランスポート プロトコルを通じてデバイスから送信されます。

対応する特性を持つトンネル インターフェイスをトンネルの両端にそれぞれ設定します。

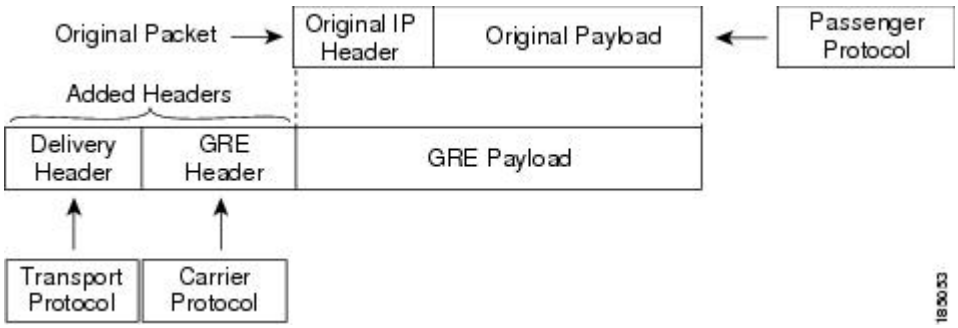
設定の前にトンネル機能をイネーブルにする必要があります。システムはこの機能をディセーブルにする前のチェックポイントを自動的に取得するため、このチェックポイントにロールバックできます。ロールバックとチェックポイントの詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。

GRE トンネル

Generic Routing Encapsulation（GRE）をさまざまなパッセンジャ プロトコルのキャリア プロトコルとして使用できます。

次の図は、GRE トンネルの IP トンネルのコンポーネントを示しています。オリジナルのパッセンジャ プロトコル パケットは GRE ペイロードとなり、デバイスはパケットに GRE ヘッダーを追加します。次にデバイスはトランスポートプロトコルヘッダーをパケットに追加して送信します。

図 *27*：*GRE PDU*



ポイントツーポイント IP-in-IP トンネルのカプセル化およびカプセル化解除

6.1(2)I3(4)、7.0(3)I1(2) 以降では、ポイントツーポイント IP-in-IP の encapsulation および decapsulation は、送信元トンネルインターフェイスから宛先トンネルインターフェイスにカプセル化されたパケットを送信するために作成できるトンネルのタイプです。このタイプのトンネルは、着信トラフィックと発信トラフィックの両方を伝送します。

（注） PBR ポリシーに基づく IP-in-IP トンネルの選択はサポートされません

マルチポイント IP-in-IP トンネルのカプセル化解除

6.1(2)I3(4)、7.0(3)I1(2) 以降では、マルチポイント IP-in-IP の decapsulate-any は、任意の数の IP-in-IP トンネルから 1 つのトンネル インターフェイスにパケットのカプセル化を解除するために作成できるトンネルのタイプです。このトンネルは発信トラフィックを伝送しません。ただし、任意の数のリモート トンネル エンドポイントが、このように設定されたトンネルを宛先として使用することができます。

『Path MTU Discovery』

パス最大伝送単位（MTU）ディスカバリ（PMTUD）は、パケットの発信元から宛先へのパスに沿って最小 MTU を動的に決定することで、2 つのエンドポイント間のパスのフラグメンテーションを防ぎます。PMTUD は、パケットにフラグメンテーションが必要であるという情報がインターフェイスに届くと、接続に対する送信 MTU 値を減らします。

PMTUD をイネーブルにすると、インターフェイスはトンネルを通過するすべてのパケットに Don't Fragment（DF）ビットを設定します。トンネルに入ったパケットがそのパケットの MTU 値よりも小さい MTU 値を持つリンクを検出すると、リモート リンクはそのパケットをドロップし、パケットの送信元にインターネット制御メッセージプロトコル（ICMP）メッセージを返します。このメッセージには、フラグメンテーションが要求されたこと（しかし許可されなかったこと）と、パケットをドロップしたリンクの MTU が含まれています。

（注） トンネル インターフェイスの PMTUD は、トンネル エンドポイントがトンネルのパスでデバイスによって生成される ICMP メッセージを受信することを要求します。ファイアウォール接続を通じて PMTUD を使用する前に、ICMP メッセージが受信できることを確認してください。

ハイ アベイラビリティ

IP トンネルはステートフル再起動をサポートします。ステートフル再起動はスーパーバイザ切り替え時に発生します。切り替え後、Cisco NX-OS は実行時の設定を適用します。

IP トンネルのライセンス要件

次の表に、この機能のライセンス要件を示します。

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

IP トンネルの前提条件

IP トンネルには次の前提条件があります。

- IP トンネルを設定するための TCP/IP に関する基礎知識があること。
- スイッチにログインしている。
- IP トンネルを設定してイネーブルにする前にデバイスのトンネリング機能をイネーブルにしておくこと。

注意事項と制約事項

IP トンネルの設定に関する注意事項と制約事項は次のとおりです。

- **show** コマンドで **internal** キーワードを指定することは、サポートされていません。
- Cisco NX-OS は、次のプロトコルだけをサポートします。
  - IPv4 パッセンジャー プロトコル
  - GRE キャリア プロトコル
- Cisco NX-OS は、次の最大数のトンネルをサポートします。
  - IP トンネル：8 トンネル
  - GRE および IP-in-IP 標準トンネル：8 トンネル（7.0(3)I1(2) 以降）
- アクセス コントロール リスト（ACL）または QoS ポリシーは IP トンネルでサポートされません。
- Cisco NX-OS は、IETF RFC 2784 に定義されている GRE ヘッダーをサポートします。Cisco NX-OS は、トンネル キーと IETF RFC 1701 のその他のオプションをサポートしません。
- Cisco NX-OS は、GRE トンネル キープアライブをサポートしません。
- すべてのユニキャスト ルーティング プロトコルが IP トンネルでサポートされます。
- IP トンネル インターフェイスは、SPAN 送信元または宛先には設定できません。

- IP トンネルは、PIM またはその他のマルチキャスト機能およびプロトコルをサポートしません（7.0(3)I1(2) 以降）。
- PBR ポリシーに基づく IP-in-IP トンネルの選択はサポートされません（7.0(3)I1(2) 以降）。
- IP トンネルは、デフォルトの **system routing** モードでのみサポートされ、その他のモードではサポートされません（7.0(3)I1(2) 以降）。
- トンネル インターフェイスを **ipip mode** に設定する場合、最大 MTU 値は 9192（7.0(3)I2(2) 以前）または 9196（7.0(3)I3(1) 以降）です。

  NX-OS 7.0(3)I3(1) 以降のリリースから以前のリリースにダウングレードする場合、MTU 値が 9196 の **ipip mode** のトンネル インターフェイスを使用しているときは、ダウングレード操作の結果として MTU 設定が失われます。ベスト プラクティスとしては、MTU 設定が失われることを回避するために、ダウングレードを開始する前に MTU 値を 9192 に調整します。
- トンネル インターフェイスを **ipip mode** に設定する場合、デフォルトの MTU 値は 1476（7.0(3)I3(1) 以前）または 1480（7.0(3)I4(1) 以降）です。

  NX-OS 7.0(3)I4(1) 以降のリリースから以前のリリースにダウングレードする場合、明示的な MTU 設定のない **ipip mode** のトンネル インターフェイスを使用しているときは、ダウングレード操作の結果として MTU 値が 1480 から 1476 に変更されます。ベスト プラクティスとしては、MTU 値が変更されることを回避するために、ダウングレードを開始する前に MTU 値を 1476 に調整します。

  NX-OS 7.0(3)I3(1) 以前のリリースから NX-OS 7.0(3)I4(1) 以降のリリースにアップグレードする場合、明示的な MTU 設定のない **ipip mode** のトンネル インターフェイスを使用しているときは、アップグレード操作の結果として MTU 値が 1476 から 1480 に変更されます。ベスト プラクティスとしては、MTU 値が変更されることを回避するために、アップグレードを開始する前に MTU 値を 1480 に調整します。
- Cisco Nexus 9200 シリーズ スイッチでは、IP-in-IP トンネルで受信される GRE パケットが予想通りにドロップされず、パケット宛先に転送されます。
- スイッチから送信される Tx パケット（制御パケットなど）は、Tx 統計情報には含まれません。
- 別のトンネル経由で到達可能なトンネル宛先は、サポートされません。
- トンネル経由のルートについては整合性チェッカがサポートされません。
- 非 IP ルーティング プロトコル（isis など）は、IP-in-IP トンネル経由ではサポートされません。
- RFC5549 は、トンネル経由ではサポートされません。

デフォルト設定

次の表に、IP トンネル パラメータのデフォルト設定を示します。

IP トンネルの設定

表 *14*：デフォルトの *IP* トンネル パラメータ

パラメータ（**Parameters**）	デフォルト
Path MTU Discovery 経過時間タイマー	10 分
パス MTU ディスカバリの最小 MTU	64
トンネル機能	ディセーブル

IP トンネルの設定

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

トンネリングのイネーブル化

IP トンネルを設定する前にトンネリング機能をイネーブルにする必要があります。

手順の概要

1. **configure terminal**
2. **feature tunnel**
3. **exit**
4. **show feature**
5. **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	**feature tunnel**
	
	例：
	`switch(config)# feature tunnel`
	`switch(config-if)#`
		新しいトンネル インターフェイスを作成できます。
		トンネル インターフェイス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 3	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch#`
		インターフェイスモードを終了し、コンフィギュレーション モードに戻ります。

ステップ 4	**show feature** 例： `switch(config-if)# show feature`	（任意）デバイス上でイネーブルされている機能に関する情報を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

トンネル インターフェイスの作成

トンネル インターフェイスを作成して、この論理インターフェイスを IP トンネルに設定できます。

（注） Cisco NX-OS は、最大 8 つの IP トンネルをサポートしています。

（注） トンネル インターフェイスおよび関連するすべての設定を削除するには、**no interface tunnel** コマンドを使用します。

コマンド	目的
no interface tunnel*number* 例： `switch(config)# no interface tunnel 1`	トンネル インターフェイスおよび関連する設定を削除します。
description*string* 例： `switch(config-if)# description GRE tunnel`	トンネルの説明を設定します。
mtu*value* 例： `switch(config-if)# mtu 1400`	インターフェイスで送信される IP パケットの MTU を設定します。
tunnel ttl*value* 例： `switch(config-if)# tunnel ttl 100`	トンネルの存続可能時間を設定します。範囲は 1 ～ 255 です。

（注） トンネルの宛先の **use-vrf** とは異なるトンネル インターフェイス VRF を使用する GRE トンネルまたは IP-in-IP トンネルを設定することは、サポートされていません。トンネル インターフェイスとトンネルの宛先で同じ VRF を使用する必要があります。

はじめる前に

異なる VRF でトンネル送信元およびトンネル宛先を設定できます。トンネリング機能がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface tunnel***number*
3. **tunnel mode** {**gre ip** | **ipip** {**ip** | **decapsulate-any**}}
4. **tunnel source** {*ip-address* |*interface-name*}
5. **tunnel destination** {*ip-address* |*host-name*}
6. **tunnel use-vrf***vrf-name*
7. **show interfaces tunnel***number*
8. **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 tunnel***number*
	
	例：
	`switch(config)# interface tunnel 1`
	`switch(config-if)#`
		新しいトンネル インターフェイスを作成します。

ステップ 3	**tunnel mode** {**gre ip** | **ipip** {**ip** | **decapsulate-any**}}	このトンネル モードを GRE、ipip、または ipip decapsulate-only に設定します。 **gre** キーワードおよび **ip** キーワードは、IP での GRE カプセル化の使用を指定します。 **ipip** キーワードは、IP-in-IP カプセル化の使用を指定します。オプションの **decapsulate-any** キーワードは、あるトンネル インターフェイスの IP-in-IP トンネルを終了させます。このキーワードは、発信トラフィックを伝送しないトンネルを作成します。ただし、リモート トンネル エンドポイントは、設定されたトンネルを宛先として使用できます。
ステップ 4	**tunnel source** {*ip-address* |*interface-name*} 例： `switch(config-if)# tunnel source ethernet 1/2`	この IP トンネルの送信元アドレスを設定します。送信元は、IP アドレスまたは論理インターフェイス名によって指定できます。
ステップ 5	**tunnel destination** {*ip-address* |*host-name*} 例： `switch(config-if)# tunnel destination 192.0.2.1`	この IP トンネルの宛先アドレスを設定します。宛先は、IP アドレスまたは論理ホスト名によって指定できます。
ステップ 6	**tunnel use-vrf***vrf-name* 例： `switch(config-if)# tunnel use-vrf blue`	（任意）設定された VRF をトンネルの IP 宛先アドレスの検索に使用します。
ステップ 7	**show interfaces tunnel***number* 例： `switch# show interfaces tunnel 1`	（任意）トンネル インターフェイス統計情報を表示します。

	コマンドまたはアクション	目的
ステップ 8	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

次に、トンネル 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 tunnel 1
switch(config-if)# tunnel source ethenet 1/2
switch(config-if)# tunnel destination 192.0.2.1
switch(config-if)# copy running-config startup-config
```

ネットマスクを使用した IP-in-IP トンネルの作成

ネットマスクを使用して IP-in-IP トンネルを作成すると、トンネル送信元サブネットおよびトンネル宛先サブネットを指定することと、一致するパケットのカプセル化を解除することが可能になります。（7.0(3)I2(1) 以降）

- IP-in-IP decap-any トンネルは、任意の数の IP-in-IP トンネルからカプセル化されたパケットを受信します。
- ネットマスク機能により、スイッチは、ネットマスクに適合する IP アドレスからのパケットを受信します。

ネットマスク機能に関する注意事項

- ルーティング プロトコルは、ネットマスクを使用して作成された IP-in-IP トンネルではサポートされません。
- カプセル化はネットマスク機能ではサポートされていません。同じサブネットの一連の送信元からのカプセル化解除だけがサポートされています。

手順の概要

1. **configure terminal**
2. **interface tunnel***number*
3. **tunnel modeipip** [**ip**]
4. **tunnel source***ip-address* / *mask_length*
5. **tunnel source***ip-address* / *mask_length*
6. （任意） **no shut**
7. **ip address***ip-prefix*/*length*

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 tunnel***number*
	
	例：
	`switch(config)# interface tunnel 5`
	`switch(config-if)#`
		新しいトンネル インターフェイスを作成します。

ステップ 3	**tunnel mode ipip** [**ip**]	このトンネル モードを ipip に設定します。 **ipip** キーワードは、IP-in-IP カプセル化の使用を指定します。
ステップ 4	**tunnel source***ip-address* / *mask_length* 例： `switch(config-if)# tunnel source 33.1.1.1 255.255.255.0`	この IP トンネルの送信元アドレスを設定します。送信元は、IP アドレスとマスクの長さによって指定されます。
ステップ 5	**tunnel source***ip-address* / *mask_length* 例： `switch(config-if)# tunnel destination 33.1.1.2 255.255.255.0`	この IP トンネルの宛先アドレスを設定します。宛先は、IP アドレスとマスクの長さによって指定されます。
ステップ 6	**no shut**	（任意） インターフェイスを消去します。
ステップ 7	**ip address***ip-prefix*/*length* 例： `switch(config-if)# ip address 50.1.1.1/24`	このインターフェイスの IP アドレスを設定します。

次に、ネットマスクを使用して IP-in-IP トンネルを作成する例を示します。

```
switch(config)# interface tunnel 10
switch(config-if)# tunnel mode ipip
switch(config-if)# tunnel source 33.1.1.2/24
switch(config-if)# tunnel destination 33.1.1.1/24
switch(config-if)# no shut
switch(config-if)# ip address 10.10.10.10/24
switch(config-if)# end
switch# show interface tunnel 10
Tunnel10 is up
    Admin State: up
    Internet address is 10.10.10.10/24
    MTU 1476 bytes, BW 9 Kbit
    Tunnel protocol/transport IPIP/IP
```

```
    Tunnel source 33.1.1.2, destination 33.1.1.1
    Transport protocol is in VRF "default"
    Last clearing of "show interface" counters never
    Tx
    0 packets output, 0 bytes
    Rx
    0 packets input, 0 bytes

switch# show run interface tunnel 10

!Command: show running-config interface Tunnel10
!Time: Wed Aug 26 13:50:01 2015

version 7.0(3)I2(1)

interface Tunnel10
  ip address 10.10.10.10/24
  tunnel mode ipip ip
  tunnel source 33.1.1.2 255.255.255.0
  tunnel destination 33.1.1.1 255.255.255.0
  no shutdown
```

トンネル インターフェイスの設定

トンネル インターフェイスを GRE トンネル モード、ipip モード、または ipip decapsulate-only モードに設定できます。GRE モードがデフォルトのトンネル モードです。（7.0(3)I1(2) 以降）

はじめる前に

トンネリング機能がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface tunnel***number*
3. **tunnel mode** {**gre ip** | **ipip** {**ip** | **decapsulate-any**}}
4. **show interfaces tunnel***number*
5. **mtu***value*
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。

	コマンドまたはアクション	目的

ステップ 2	**interface tunnel***number*
	
	例：
	`switch(config)# interface tunnel 1`
	`switch(config-if)#`
		新しいトンネル インターフェイスを作成します。

ステップ 3	**tunnel mode** {**gre ip** | **ipip** {**ip** | **decapsulate-any**}}	このトンネル モードを GRE、ipip、または ipip decapsulate-only に設定します。 **gre** キーワードおよび **ip** キーワードは、IP での GRE カプセル化の使用を指定します。 ipip キーワードは、IP-in-IP カプセル化の使用を指定します。オプションの **decapsulate-any** キーワードは、あるトンネル インターフェイスの IP-in-IP トンネルを終了させます。このキーワードは、発信トラフィックを伝送しないトンネルを作成します。ただし、リモート トンネル エンドポイントは、設定されたトンネルを宛先として使用できます。
ステップ 4	**show interfaces tunnel***number* 例： `switch(config-if)# show interfaces tunnel 1`	（任意）トンネル インターフェイス統計情報を表示します。
ステップ 5	**mtu***value*	インターフェイスで送信される IP パケットの最大伝送ユニット（MTU）を設定します。 有効な範囲は 64 ～ 9192 ユニットです。 （注） **tunnel mode ipip** を設定する場合、その範囲は NX-OS のリリースによって異なります。 • 64 ~ 9192 ユニット（7.0(3)I2(2) 以前） • 64 ~ 9196 ユニット（7.0(3)I3(1) 以降）
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

次に、GRE へのトンネル 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 tunnel 1
switch(config-if)# tunnel mode gre ip
switch(config-if)# copy running-config startup-config
```

次に、ipip トンネルを作成する例を示します。

```
switch# configure terminal
switch(config)# interface tunnel 1
switch(config-if)# tunnel mode ipip
switch(config-if)# mtu 1400
switch(config-if)# copy running-config startup-config
switch(config-if)# no shut
```

GRE トンネルの設定

トンネルインターフェイスをGREトンネルモードに設定できます。（6.1(2)I3(3)および7.0(3)I1(1)）

（注） Cisco NX-OS は IPV4 over IPV4 の GRE プロトコルのみをサポートしています。

はじめる前に

トンネリング機能がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface tunnel***number*
3. **tunnel modegre ip**
4. **show interfaces tunnel***number*
5. **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 tunnel***number*
	
	例：
	`switch(config)# interface tunnel 1`
	`switch(config-if)#`
		新しいトンネルインターフェイスを作成します。

ステップ 3	**tunnel modegre ip** 例： `switch(config-if)# tunnel mode gre ip`	このトンネル モードを GRE に設定します。

	コマンドまたはアクション	目的
ステップ 4	**show interfaces tunnel***number* 例： `switch(config-if)# show interfaces tunnel 1`	（任意）トンネルインターフェイス統計情報を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

GRE トンネルの設定

GRE v6 トンネルは、IPv6 トランスポートで異なるタイプのパケットを伝送するために使用されます。GREv6 トンネルは、IPv4 ペイロードのみを伝送します。トンネルの CLI は、IPv6 トンネルを選択し、v6 トンネルの送信元と宛先を設定するために拡張されました。（7.0(3)I2(1) 以降）

トンネル インターフェイスを GRE トンネル モード、ipip モード、または ipip decapsulate-only モードに設定できます。GRE モードがデフォルトのトンネル モードです。

はじめる前に

トンネリング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 tunnel***number*
3. switch(config-if)# **tunnel mode** {**gre ip** | **ipip** {**ip** | **decapsulate-any**}}
4. switch(config-if)# **tunnel use-vrf***vrf-name*
5. switch(config-if)# **ipv6 address***IPv6 address*
6. （任意） switch(config-if)# **show interface tunnel***number*
7. switch(config-if)# **mtu***value*
8. （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。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **interface tunnel***number*	トンネルインターフェイス 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)# **tunnel mode** {**gre ip** | **ipip** {**ip** | **decapsulate-any**}}	このトンネル モードを GRE、ipip、または ipip decapsulate-only に設定します。 **gre** キーワードおよび **ip** キーワードは、IP での GRE カプセル化の使用を指定します。 ipip キーワードは、IP-in-IP カプセル化の使用を指定します。オプションの **decapsulate-any** キーワードは、あるトンネル インターフェイスの IP-in-IP トンネルを終了させます。このキーワードは、発信トラフィックを伝送しないトンネルを作成します。ただし、リモート トンネル エンドポイントは、設定されたトンネルを宛先として使用できます。
ステップ 4	switch(config-if)# **tunnel use-vrf***vrf-name*	トンネル VRF名を設定します。
ステップ 5	switch(config-if)# **ipv6 address***IPv6 address*	IPv6 アドレスを設定します。 （注） トンネルの送信元アドレスおよび宛先アドレスは同じまま（IPv4 アドレス）です。
ステップ 6	switch(config-if)# **show interface tunnel***number*	（任意） トンネル インターフェイスの統計情報を表示します。
ステップ 7	switch(config-if)# **mtu***value*	インターフェイスで送信される IP パケットの最大伝送ユニット（MTU）を設定します。
ステップ 8	switch(config-if)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、GRE v4 トンネル経由の IPv6 ペイロードを設定する例を示します。トンネルの送信元、宛先、IPv4 アドレス、IPv6 アドレスを設定し、**no shut** コマンドを実行します。GRE v4 トンネルが作成されると、トンネル経由の v4 または v6 ルートを設定できます。

```
switch# configure terminal
switch(config)# interface tunnel 10
switch(config)# tunnel source 11.1.1.1
switch(config)# tunnel destination 11.1.1.2
switch(config-if)# tunnel mode gre ip
switch(config-if)# tunnel use-vrf red
switch(config-if)# ip address 10.1.1.1/24
switch(config-if)# ipv6 address 2:2::2/64
switch(config-if)# no shut

switch(config)# ip route 50.1.1.0/24 tunnel 10
```

```
switch(config)# ipv6 route 2000:100::/64 tunnel 10
```

次に、GRE v4 トンネル インターフェイス 10 を表示し、IPv4 および IPv6 ルートを表示する例を示します。

```
switch(config)# show int tunnel 10
Tunnel 10 is up
    Admin State: up
    Internet address(es):
    10.1.1.1/24
    1010::1/64
    MTU 1476 bytes, BW 9 Kbit
    Tunnel protocol/transport GRE/IP
    Tunnel source 11.1.1.1, destination 11.1.1.2
    Transport protocol is in VRF "default"

switch#show ipv6 route
…
2000:100::/64, ubest/mbest: 1/0, attached
    *via Tunnel10, [1/0], 00:00:16, static

#show ip route
…
50.1.1.0/24, ubest/mbest: 1/0
    *via Tunnel10, [1/0], 00:03:33, static
```

次に、GRE v6 トンネル経由の IPv4 ペイロードを設定する例を示します。トンネル モードを GRE IPv6 に設定し、トンネルの v6 送信元および宛先、IPv4 アドレスを設定して、**no shut** コマンドを実行します。GRE v6 トンネルが作成されると、トンネル経由の v4 ルートを設定できます。

```
switch# configure terminal
switch(config)# interface tunnel 20
switch(config-if)# tunnel mode gre ipv6
switch(config)# tunnel source 1313::1
switch(config)# tunnel destination 1313::2
switch(config-if)# tunnel use-vrf red
switch(config-if)# ip address 20.1.1.1/24
switch(config-if)# no shut

switch(config)# ip route 100.1.1.0/24 tunnel 20
```

次に、GRE v6 トンネル インターフェイス 20 を表示する例を示します。

```
show interface tunnel 20
Tunnel 20 is up
    Admin State: up
    Internet address is 20.1.1.1/24
    MTU 1456 bytes, BW 9 Kbit
    Tunnel protocol/transport GRE/IPv6
    Tunnel source 1313::1, destination 1313::2
    Transport protocol is in VRF "default"

#show ip route
…
100.1.1.0/24, ubest/mbest: 1/0
    *via Tunnel20, [1/0], 00:01:00, static

red10# show interface brief | grep Tunnel
Tunnel10                up          10.1.1.1/24       GRE/IP           1476
Tunnel20                up          20.1.1.1/24       GRE/IPv6         1456
```

次に、ipip トンネルを作成する例を示します。

```
switch# configure terminal
switch(config)# interface tunnel 1
switch(config-if)# tunnel mode ipip
switch(config-if)# mtu 1400
switch(config-if)# copy running-config startup-config
switch(config-if)# no shut
```

Path MTU Discovery のイネーブル化

トンネルでパス MTU ディスカバリをイネーブルにするには、**tunnel path-mtu discovery** コマンドを使用します。

手順の概要

1. **tunnel path-mtu-discoveryage-timer***min*
2. **tunnel path-mtu-discoverymin-mtu***bytes*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**tunnel path-mtu-discoveryage-timer***min* 例： `switch(config-if)# tunnel path-mtu-discovery age-timer 25`	トンネル インターフェイスで Path MTU Discovery（PMTUD）をイネーブルにします。 • min：分数。有効な範囲は 10 ～ 30 です。デフォルトは 10 です。
ステップ 2	**tunnel path-mtu-discoverymin-mtu***bytes* 例： `switch(config-if)# tunnel path-mtu-discovery min-mtu 1500`	トンネル インターフェイスで Path MTU Discovery（PMTUD）をイネーブルにします。 • bytes：認識された最小 MTU。 範囲は 64 ～ 9192 です。デフォルトは 64 です。

トンネル インターフェイスへの VRF メンバーシップの割り当て

VRF にトンネル インターフェイスを追加できます。

はじめる前に

トンネリング機能がイネーブルになっていることを確認します。

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. **configure terminal**
2. **interface tunnel***number*
3. **vrf member***vrf-name*
4. **ip address***ip-prefix/length*
5. **show vrf** [*vrf-name*] **interface***interface-type number*
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 tunnel***number*
	
	例：
	`switch(config)# interface tunnel 0`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**vrf member***vrf-name* 例： `switch(config-if)# vrf member RemoteOfficeVRF`	このインターフェイスを VRF に追加します。
ステップ 4	**ip address***ip-prefix/length* 例： `switch(config-if)# ip address 192.0.2.1/16`	このインターフェイスの IP アドレスを設定します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。
ステップ 5	**show vrf** [*vrf-name*] **interface***interface-type number* 例： `switch(config-vrf)# show vrf Enterprise interface tunnel 0`	（任意）VRF 情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）この設定の変更を保存します。

次に、VRF にトンネル 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 tunnel 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
```

IP トンネル設定の確認

IP トンネルの設定情報を確認するには、次のいずれかの作業を行います。

コマンド	目的
show interface tunnel*number*	トンネルインターフェイスの設定を表示します（MTU、プロトコル、転送、および VRF）。入力および出力パケット、バイト、およびパケット レートを表示します。
show interface tunnel*number***brief**	トンネル インターフェイスの動作状態、IP アドレス、カプセル化のタイプ、MTU を表示します。
show interface tunnel*number***counters**	入力および出力パケットのインターフェイス カウンタを表示します。 （注） インターフェイス カウンタとともに表示されるバイト数には内部ヘッダー サイズが含まれます。
show interface tunnel*number***description**	トンネルインターフェイスに設定された説明を表示します。
show interface tunnel*number***status**	トンネルインターフェイスの動作ステータスを表示します。
show interface tunnel*number***status err-disabled**	トンネル インターフェイスの errdisable 状態を表示します。

IP トンネリングの設定例

次の例では、簡易 GRE トンネルを示します。イーサネット 1/2 は、ルータ A のトンネル送信元であり、ルータ B のトンネル宛先です。イーサネット インターフェイス 2/1 は、ルータ B のトンネル送信元であり、ルータ A のトンネル宛先です。

ルータ A：

```
feature tunnel
interface tunnel 0
ip address 209.165.20.2/8
tunnel source ethernet 1/2
```

```
tunnel destination 192.0.2.2
tunnel mode gre ip
tunnel path-mtu-discovery 25 1500

interface ethernet 1/2
ip address 192.0.2.55/8
```

ルータ B：

```
feature tunnel
interface tunnel 0
ip address 209.165.20.1/8
tunnel source ethernet 2/1
tunnel destination 192.0.2.55
tunnel mode gre ip

interface ethernet 2/1
ip address 192.0.2.2/8
```

関連資料

関連項目	マニュアル タイトル
IP トンネル コマンド	『*Cisco Nexus 9000 Series NX-OS Interfaces Command Reference*』

第 10 章

Q-in-Q VLAN トンネルの設定

Q-in-Q トンネルについて

この章では、Cisco NX-OS デバイス上で IEEE 802.1Q-in-Q VLAN トンネルおよびレイヤ 2 プロトコルのトンネリングを設定する方法について説明します（7.0(3)I2(1) 以降）。

Q-in-Q VLAN トンネルを使用することで、サービス プロバイダーは第 2 の 802.1Q タグをすでにタグ付けされたフレームに追加して、カスタマーに内部使用の VLAN をすべて提供しながら、インフラストラクチャ内で異なるカスタマーのトラフィックを分離することができます。

Q-in-Q トンネリング

サービス プロバイダーのビジネス カスタマーには、多くの場合、サポートする VLAN ID および VLAN の数に固有の要件があります。同一サービスプロバイダー ネットワークのさまざまなカスタマーが必要とする VLAN 範囲は重複し、インフラストラクチャを通るカスタマーのトラフィックは混合してしまうことがあります。カスタマーごとに一意の VLAN ID 範囲を割り当てると、カスタマーの設定が制限され、802.1Q 仕様の 4096 の VLAN に関する上限を容易に超えてしまいます。

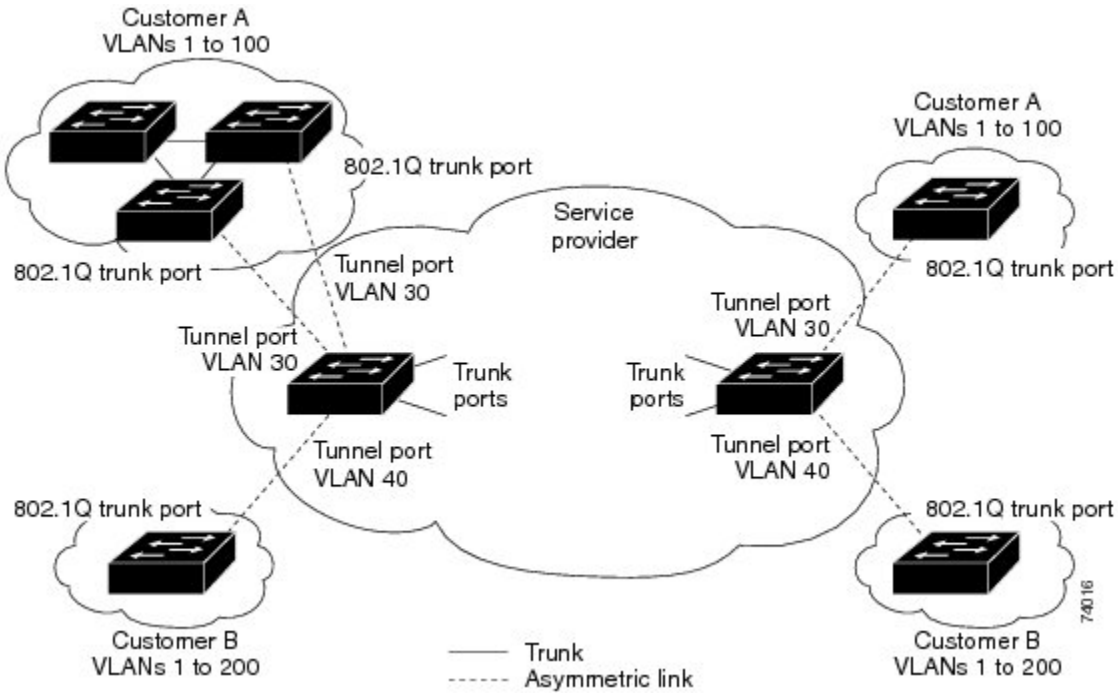
（注） Q-in-Q は、ポート チャネルでサポートされます。非対称リンクとしてポート チャネルを設定するには、ポート チャネル内のすべてのポートが同じトンネリング設定でなければなりません。

サービス プロバイダーは、802.1Q トンネリング機能を使用すると、単一の VLAN を使用して、複数の VLAN を含むカスタマーをサポートできます。同一の VLAN 上にあるように見えるときでも、サービス プロバイダー インフラストラクチャ内のカスタマーの VLAN ID を保護したり、異なるカスタマーの VLAN トラフィックを分離しておくことができます。IEEE 802.1Q トンネリングは、VLAN-in-VLAN 階層構造およびタグ付きパケットへのタギングによって、VLAN スペースを拡張します。802.1Q トンネリングをサポートするように設定されたポートは、トンネル ポートといいます。トンネリングを設定する場合、トンネリング専用の VLAN にトンネル ポートを割り当てます。カスタマーごとに個別の VLAN が必要ですが、その VLAN はカスタマーの VLAN をすべてサポートします。

カスタマー デバイスの IEEE 802.1Q トランク ポートから、通常どおりに適切な VLAN ID でタグ付けされたカスタマー トラフィックが、サービスプロバイダー エッジ スイッチのトンネル ポートに着信します。カスタマー デバイスとエッジ スイッチの間のリンクは、一方の端が 802.1Q トランク ポート、反対側がトンネル ポートとして設定されているので、非対称リンクです。それぞれのカスタマーに固有のアクセス VLAN ID には、トンネル ポート インターフェイスを割り当てます。以下の図を参照してください。

（注） 選択的 Q-in-Q トンネリングはサポートされません。トンネル ポートに着信すべてのフレームは、Q-in-Q タギングの対象となります。

図 *28* : *802.1Q-in-Q* トンネル ポート

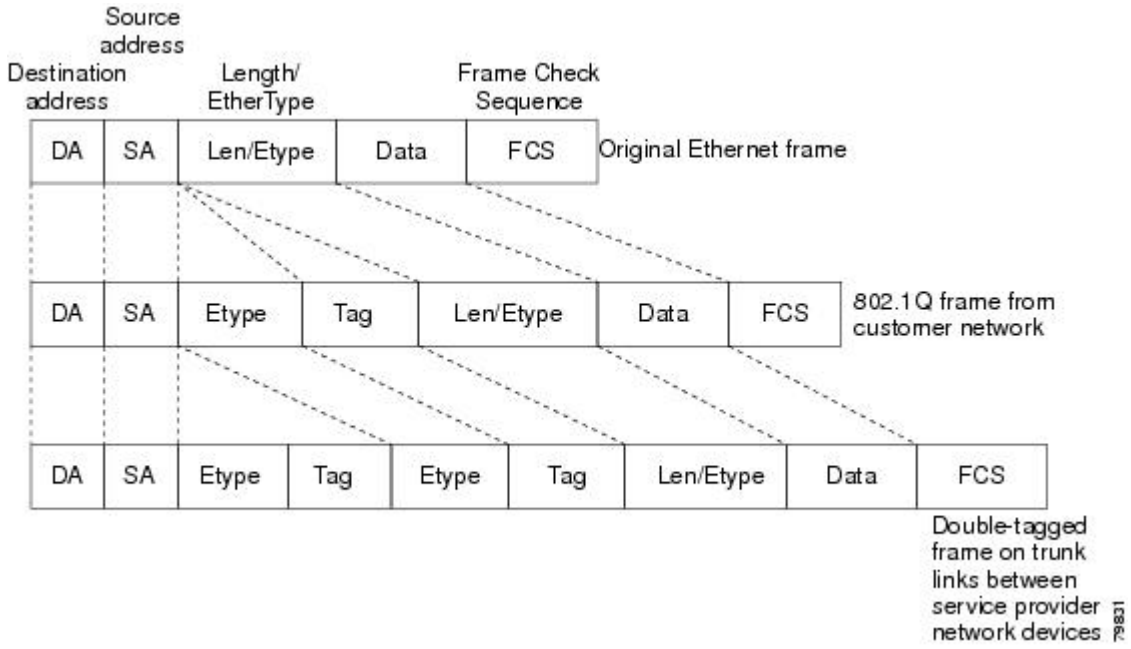


サービスプロバイダー エッジ スイッチのトンネル ポートに着信するパケット（適切な VLAN ID ですでに 802.1Q タグ付けされている）は、カスタマーに一意である VLAN ID を含む 802.1Q タグの別のレイヤでカプセル化されます。元々のカスタマーの 802.1Q タグは、カプセル化されたパケットの中に維持されます。したがって、サービスプロバイダー インフラストラクチャに着信するパケットは二重にタグ付けされます。

外部タグには、カスタマーの（サービス プロバイダーによって割り当てられた）アクセス VLAN ID が含まれます。（カスタマーによって割り当てられた）内部タグの VLAN ID は、受信トラ

フィックの VLAN です。この二重タギングは、以下の図に示すようにタグ スタック構成 Double-Q または Q-in-Q と呼ばれます。

図 *29*：タグなし、*802.1Q* タグ付き、および二重タグ付きイーサネット フレーム



この方法で、外部タグの VLAN ID スペースは内部タグの VLAN ID スペースに依存しません。単一の外部 VLAN ID は、個々のカスタマーの全体の VLAN ID スペースを表すことができます。この方法により、カスタマーのレイヤ 2 ネットワークをサービス プロバイダー ネットワーク全体に拡張して、複数のサイトに仮想 LAN インフラストラクチャを作成することも可能になります。

（注） 階層型タギング、すなわちマルチレベルの dot1q タギング Q-in-Q はサポートされていません。

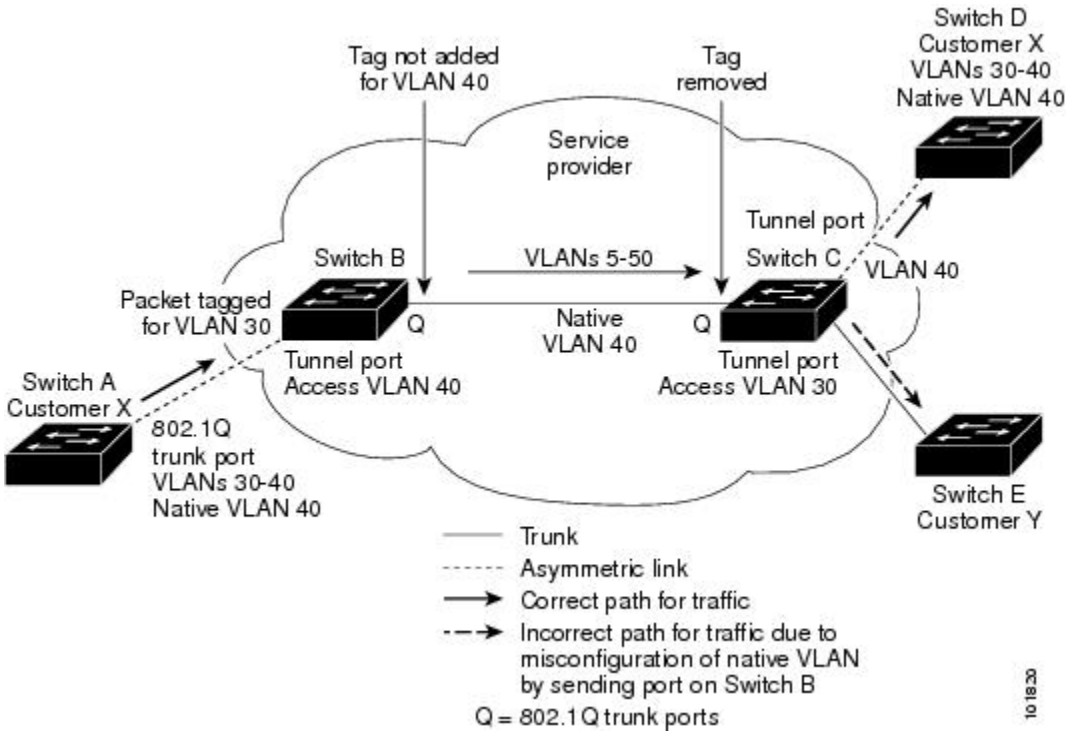
ネイティブ VLAN のリスク

エッジ スイッチで 802.1Q トンネリングを設定する場合は、サービス プロバイダー ネットワークにパケットを送信するために、802.1Q トランク ポートを使用する必要があります。ただし、サービスプロバイダー ネットワークのコアを通過するパケットは、IEEE 802.1Q トランク、ISL トランク、または非トランキング リンクで伝送される場合があります。802.1Q トランクをこれらのコア スイッチで使用する場合には、802.1Q トランクのネイティブ VLAN を、同じスイッチ上の dot1q トンネル ポートのどのネイティブ VLAN にも一致させないでください。ネイティブ VLAN 上のトラフィックが 802.1Q 送信トランク ポートでタグ付けされなくなるためです。

以下の図では、VLAN 40 は、サービスプロバイダー ネットワークの入力エッジ スイッチ（スイッチ B）において、カスタマー X からの 802.1Q トランク ポートのネイティブ VLAN として設定さ

れています。カスタマー X のスイッチ A は、VLAN 30 のタグ付きパケットを、アクセス VLAN 40 に属する、サービスプロバイダー ネットワークのスイッチ B の入力トンネル ポートに送信します。トンネル ポートのアクセス VLAN（VLAN 40）は、エッジ スイッチのトランク ポートのネイティブ VLAN（VLAN 40）と同じなので、トンネル ポートから受信したタグ付きパケットに 802.1Q タグは追加されません。パケットには VLAN 30 タグだけが付いて、サービスプロバイダー ネットワークで出力エッジ スイッチ（スイッチ C）のトランク ポートに送信され、出力スイッチ トンネルによってカスタマー Y に間違えて送信されます。

図 *30*：ネイティブ *VLAN* のリスク



ネイティブ VLAN の問題を解決する方法は 2 つあります。

- 802.1Q トランクから出るすべてのパケット（ネイティブ VLAN を含む）が、vlan dot1q tag native コマンドを使用してタグ付けされるように、エッジ スイッチを設定します。すべての 802.1Q トランクでネイティブ VLAN パケットにタグを付けるようにスイッチを設定した場合、スイッチはタグなしパケットを受信しますが、タグ付きパケットだけを送信します。

（注） **vlan dot1q tag native** コマンドは、すべてのトランク ポート上のタギング動作に影響を与えるグローバル コマンドです。

- エッジ スイッチのトランク ポートのネイティブ VLAN ID が、カスタマー VLAN 範囲に属さないようにします。たとえばトランク ポートが VLAN100 ～ 200 のトラフィックを運ぶ場合は、この範囲以外の番号をネイティブ VLAN に割り当てます。

レイヤ 2 プロトコルのトンネリングについて

サービスプロバイダー ネットワーク経由で接続される複数のサイトのカスタマーは、さまざまなレイヤ 2 プロトコルを実行して、すべてのリモート サイトおよびローカル サイトを含むようにトポロジを拡大する必要があります。スパニングツリー プロトコル（STP）が適切に稼働している必要があり、すべての VLAN で、ローカル サイトおよびサービスプロバイダー インフラストラクチャ経由のすべてのリモート サイトを含む、適切なスパニングツリーを構築する必要があります。Cisco Discovery Protocol（CDP）は、ローカルおよびリモート サイトから隣接するシスコ デバイスを検出することができる必要があり、VLAN トランキング プロトコル（VTP）は、カスタマー ネットワークのすべてのサイトを通して一貫した VLAN 設定を提供する必要があります。

プロトコル トンネリングがイネーブルになると、サービス プロバイダー インフラストラクチャの受信側にあるエッジ スイッチが、レイヤ 2 プロトコルを特別の MAC アドレスでカプセル化し、サービス プロバイダー ネットワークの端まで送信します。ネットワークのコア スイッチでは、このパケットが処理されずに通常のパケットとして転送されます。CDP、STP、または VTP のブリッジプロトコルデータユニット（BPDU）は、サービスプロバイダーインフラストラクチャを通過し、サービスプロバイダーネットワークの発信側にあるカスタマースイッチまで配信されます。同一パケットは同じ VLAN のすべてのカスタマー ポートで受信されます。

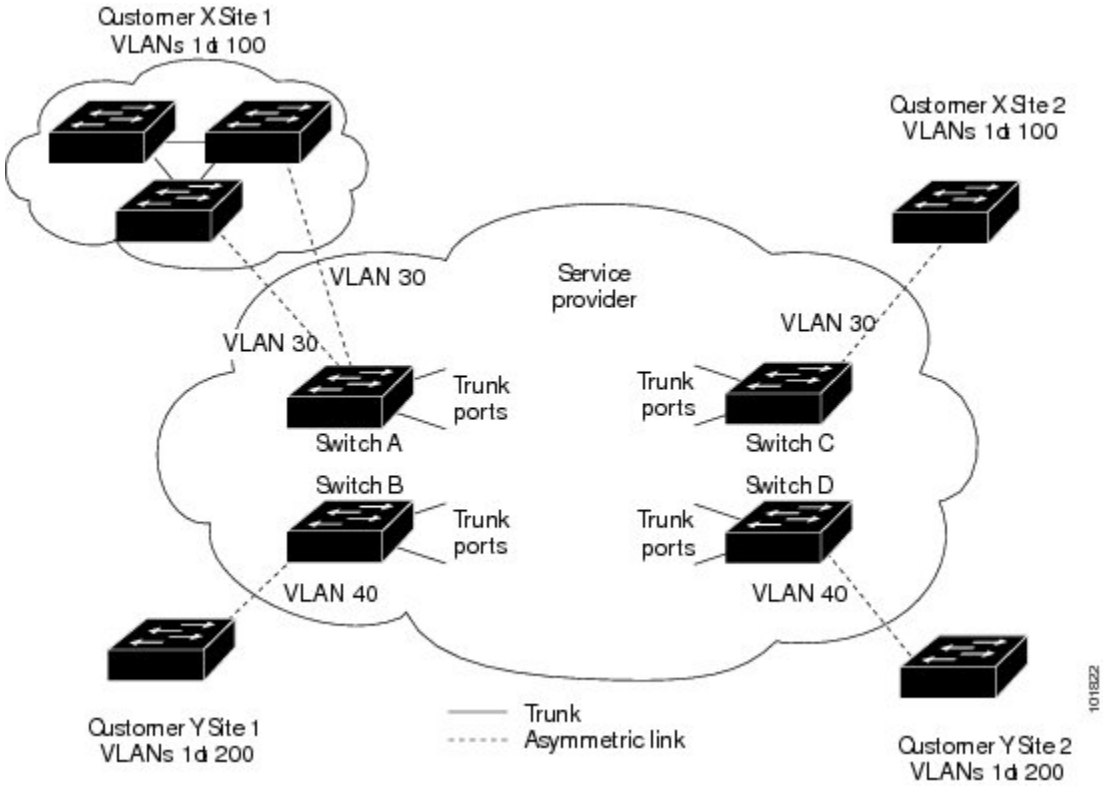
802.1Q トンネリング ポートでプロトコルのトンネリングをイネーブルにしていない場合、サービスプロバイダー ネットワークの受信側のリモート スイッチでは BPDU を受信せず、STP、CDP、802.1X、および VTP を適切に実行できません。プロトコルのトンネリングがイネーブルである場合、それぞれのカスタマー ネットワークのレイヤ 2 プロトコルは、サービスプロバイダー ネットワーク内で動作しているものから完全に区別されます。802.1Q トンネリングでサービスプロバイダーネットワークを通してトラフィックを送信する、さまざまなサイトのカスタマースイッチでは、カスタマー VLAN が完全に認識されます。

（注） レイヤ 2 プロトコルのトンネリングは、ソフトウェアで BPDU をトンネリングすることで動作します。スーパーバイザが受信する多数の BPDU により CPU の負荷が大きくなります。スーパーバイザ CPU の負荷を軽減するために、ソフトウェア レート リミッタを使用する必要がある場合があります。レイヤ 2 プロトコル トンネル ポートのしきい値の設定, （333 ページ）を参照してください。

たとえば、以下の図で、カスタマー X には、サービス プロバイダー ネットワークを介して接続された同じ VLAN に 4 台のスイッチがあります。ネットワークが BPDU をトンネリングしない

と、ネットワークの遠端のスイッチは STP、CDP、802.1X、および VTP プロトコルを正しく実行できません。

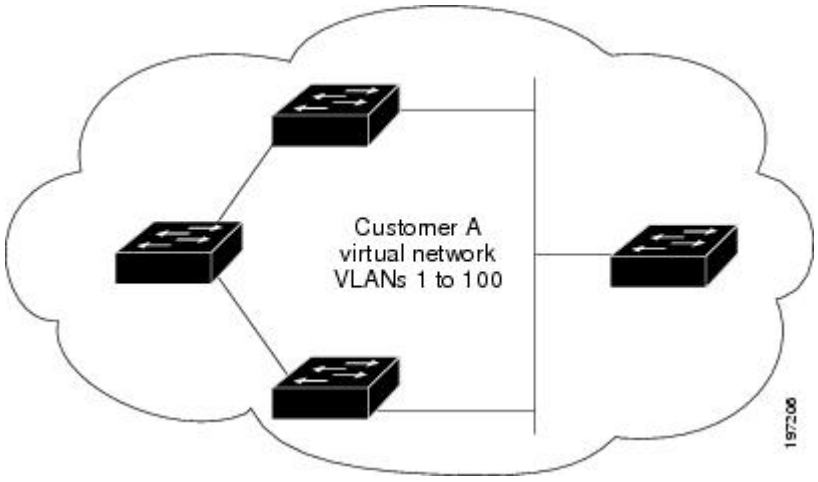
図 *31*：レイヤ *2* プロトコル トンネリング



前の例では、カスタマー X、サイト 1 のスイッチ上の VLAN で動作する STP は、カスタマー X、サイト 2 のスイッチに基づくコンバージェンス パラメータを考慮せずに、このサイトのスイッチのスパニング ツリーを構築します。

以下の図は、BPDU トンネリングがイネーブルになっていない場合の、カスタマーのネットワークでの結果トポロジを示します。

図 *32* : *BPDU* トンネリングを使用しない仮想ネットワーク トポロジ



インターフェイスのライセンス要件

IP トンネルおよび vPC には Enterprise Services ライセンスが必要です。このライセンスは IP トンネルをイネーブルにするシステムごとにインストールする必要があります。

他のインターフェイスにはライセンスが必要ありません。

注意事項と制約事項

Q-in-Q トンネリングおよびレイヤ 2 トンネリングには、次の設定に関する注意事項と制約事項があります。

- **show** コマンドで **internal** キーワードを指定することは、サポートされていません。
- サービスプロバイダー ネットワーク内のスイッチは、Q-in-Q タギングによる MTU サイズの増加に対応するように設定する必要があります。
- Q-in-Q タグ付きパケットの MAC アドレス ラーニングは、外部 VLAN（サービス プロバイダー VLAN）タグに基づいています。単一の MAC アドレスが複数の内部（カスタマー）VLAN で使用される配置においては、パケット転送の問題が発生する場合があります。
- レイヤ 3 以上のパラメータは、トンネル トラフィックでは識別できません（レイヤ 3 宛先や送信元アドレスなど）。トンネル型トラフィックはルーティングできません。
- Cisco Nexus 9000 シリーズのデバイスは、トンネル トラフィックに対する MAC レイヤ ACL/QoS（VLAN ID および送信元/宛先 MAC アドレス）のみを提供できます。
- MAC アドレスに基づくフレーム配布を使用する必要があります。

- 非対称リンクでは 1 つのポートだけがトラッキングするため、Dynamic Trunking Protocol（DTP）をサポートしません。無条件でトランクになるように、非対称リンクの 802.1Q トランク ポートを設定する必要があります。
- プライベート VLAN をサポートするように設定されたポートに 802.1Q トンネリング機能を設定することはできません。プライベート VLAN は、これらの導入には必要ではありません。
- トンネル VLAN の IGMP スヌーピングをディセーブルにする必要があります。
- コントロール プレーン ポリシング（CoPP）はサポートされません。
- ネイティブ VLAN でのタギングを維持し、タグなしトラフィックを廃棄するには、vlan dot1Q tag native コマンドを入力する必要があります。このコマンドにより、ネイティブ VLAN の設定ミスを防止できます。
- 802.1Q インターフェイスをエッジ ポートにするように手動で設定する必要があります。
- IGMP スヌーピングは内部 VLAN ではサポートされません。
- Q-in-Q は、Cisco Nexus 9332PQ、9372PX、9372TX、93120TX スイッチ、および N9K-M6PQ または N9K-M12PQ 汎用拡張モジュール（GEM）搭載の Cisco Nexus 9396PX、9396TX、93128TX スイッチのアップリンク ポートではサポートされません。
- Q-in-Q トンネルは、Cisco Nexus 9300 および 9500 シリーズ デバイスのアプリケーション リーフ エンジン（ALE）アップリンク ポートに関する制約事項の影響を受ける可能性があります（ALE アップリンク ポートに関する制約事項 [英語]）。

Q-in-Q トンネルおよびレイヤ 2 プロトコルのトンネリングの設定

802.1Q トンネル ポートの作成

switchport mode コマンドを使用して dot1q-tunnel ポートを作成します。

（注）

spanning-tree port type edge コマンドを使用して、エッジ ポートに 802.1Q トンネル ポートを設定する必要があります。ポートの VLAN メンバーシップは、**switchport access vlan***vlan-id* コマンドを使用して変更されます。

dot1q-tunnel ポートに割り当てられたアクセス VLAN の IGMP スヌーピングをディセーブルにして、マルチキャスト パケットが Q-in-Q トンネルを通過できるようにする必要があります。

はじめる前に

はじめに、スイッチ ポートとしてインターフェイスを設定する必要があります。

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 dot1q-tunnel**
5. （任意） switch(config-if)# **no switchport mode dot1q-tunnel**
6. switch(config-if)# **exit**
7. （任意） switch(config)# **show dot1q-tunnel** [**interface***if-range*]
8. （任意） switch(config)# **no shutdown**
9. （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 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 dot1q-tunnel**	ポートに 802.1Q トンネルを作成します。インターフェイス モードを変更すると、ポートはダウンし、再初期化（ポート フラップ）されます。トンネル インターフェイスでは BPDU フィルタリングがイネーブルになり、CDP がディセーブルになります。
ステップ 5	switch(config-if)# **no switchport mode dot1q-tunnel**	（任意） ポートで 802.1Q トンネルをディセーブルにします。
ステップ 6	switch(config-if)# **exit**	設定モードを終了します。
ステップ 7	switch(config)# **show dot1q-tunnel** [**interface***if-range*]	（任意） dot1q-tunnel モードにあるすべてのポートを表示します。必要に応じて、表示するインターフェイスまたはインターフェイスの範囲を指定できます。
ステップ 8	switch(config)# **no shutdown**	（任意） ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

	コマンドまたはアクション	目的
ステップ 9	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、802.1Q トンネル ポートを作成する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 7/1
switch(config-if)# switchport
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# exit
switch(config)# exit
switch# show dot1q-tunnel
```

Q-in-Q 用の EtherType の変更

Q-in-Q カプセル化に使用するように 802.1Q EtherType 値を変更できます。

（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（サービス プロバイダーに接続するトランク インターフェイス）だけに EtherType を設定する必要があります。トランクの一方で EtherType を変更した場合、トランクのもう一方でも同じ値を設定する必要があります（対称構成）。

注意 設定した EtherType 値は、（Q-in-Q パケットだけではなく）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 dot1q ethertype***value*
5. （任意） switch(config-if)# **no switchport dot1q ethertype**
6. switch(config-if)# **exit**
7. （任意） switch(config)# **no shutdown**
8. （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 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 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 5	switch(config-if)# **no switchport dot1q ethertype**	（任意） ポートの EtherType を 0x8100 のデフォルト値にリセットします。
ステップ 6	switch(config-if)# **exit**	設定モードを終了します。
ステップ 7	switch(config)# **no shutdown**	（任意） ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 8	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、802.1Q トンネル ポートを作成する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 7/1
switch(config-if)# switchport
switch(config-if)# switchport dot1q ethertype 0x9100
switch(config-if)# exit
switch(config)# exit
switch# show dot1q-tunnel
```

レイヤ 2 プロトコル トンネルのイネーブル化

802.1Q トンネル ポートでプロトコルのトンネリングをイネーブルにできます。

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 dot1q-tunnel**
5. switch(config-if)# **l2protocol tunnel** [**cdp** | **stp** | **vtp**]
6. （任意） switch(config-if)# **no l2protocol tunnel** [**cdp** | **stp** | **vtp**]
7. switch(config-if)# **exit**
8. （任意） switch(config)# **no shutdown**
9. （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 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 dot1q-tunnel**	ポートに 802.1Q トンネルを作成します。インターフェイス モードを変更すると、ポートはダウンし、再初期化（ポート フラップ）されます。トンネル インターフェイスでは BPDU フィルタリングがイネーブルになり、CDP がディセーブルになります。
ステップ 5	switch(config-if)# **l2protocol tunnel** [**cdp** | **stp** | **vtp**]	レイヤ 2 プロトコルのトンネリングをイネーブルにします。必要に応じて、CDP、STP、または VTP トンネリングをイネーブルにできます。
ステップ 6	switch(config-if)# **no l2protocol tunnel** [**cdp** | **stp** | **vtp**]	（任意） プロトコルのトンネリングをディセーブルにします。
ステップ 7	switch(config-if)# **exit**	設定モードを終了します。
ステップ 8	switch(config)# **no shutdown**	（任意） ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

	コマンドまたはアクション	目的
ステップ 9	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、802.1Q トンネル ポートでプロトコルのトンネリングをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 7/1
switch(config-if)# switchport
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# l2protocol tunnel stp
switch(config-if)# exit
switch(config)# exit
```

L2 プロトコル トンネル ポートに対するグローバル CoS の設定

トンネル ポートの入力 BPDU が指定されたクラスでカプセル化されるように、サービス クラス（CoS）の値をグローバルに指定できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **l2protocol tunnel cos***value*
3. （任意） switch(config)# **no l2protocol tunnel cos**
4. switch(config)# **exit**
5. （任意） switch# **no shutdown**
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**	グローバル 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)# **l2protocol tunnel cos***value*	すべてのレイヤ 2 プロトコルのトンネリング ポートでグローバル CoS 値を指定します。デフォルト CoS 値は 5 です。
ステップ 3	switch(config)# **no l2protocol tunnel cos**	（任意） グローバル CoS 値をデフォルト値に設定します。
ステップ 4	switch(config)# **exit**	設定モードを終了します。

	コマンドまたはアクション	目的
ステップ 5	switch# **no shutdown**	（任意） ポリシーがハードウェア ポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーはerror-disabledポリシー状態になります。
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、レイヤ 2 プロトコルのトンネリングのためのグローバル CoS 値を指定する例を示します。

```
switch# configure terminal
switch(config)# l2protocol tunnel cos 6
switch(config)# exit
```

レイヤ 2 プロトコル トンネル ポートのしきい値の設定

レイヤ2プロトコルのトンネリング ポートに対するポート ドロップおよびシャットダウン値を指定できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet***slot/port*
3. switch(config-if)# **switchport**
4. switch(config-if)# **switchport mode dot1q-tunnel**
5. switch(config-if)# **l2protocol tunnel drop-threshold** [**cdp** | **stp** | **vtp**] *packets-per-sec*
6. （任意） switch(config-if)# **no l2protocol tunnel drop-threshold** [**cdp** | **stp** | **vtp**]
7. switch(config-if)# **l2protocol tunnel shutdown-threshold** [**cdp** | **stp** | **vtp**] *packets-per-sec*
8. （任意） switch(config-if)# **l2protocol tunnel shutdown-threshold** [**cdp** | **stp** | **vtp**]
9. switch(config-if)# **exit**
10. （任意） switch(config)# **no shutdown**
11. （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 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 dot1q-tunnel**	ポートに 802.1Q トンネルを作成します。
ステップ 5	switch(config-if)# **l2protocol tunnel drop-threshold** [**cdp** | **stp** | **vtp**] *packets-per-sec*	廃棄される前にインターフェイスで処理できる最大パケット数を指定します。必要に応じて、CDP、STP、または VTP を指定できます。パケットの有効な値は 1 ～ 4096 です。
ステップ 6	switch(config-if)# **no l2protocol tunnel drop-threshold** [**cdp** | **stp** | **vtp**]	（任意） しきい値を 0 にリセットし、ドロップしきい値をディセーブルにします。
ステップ 7	switch(config-if)# **l2protocol tunnel shutdown-threshold** [**cdp** | **stp** | **vtp**] *packets-per-sec*	インターフェイスで処理できる最大パケット数を指定します。パケット数が超過すると、ポートは error-disabled ステートになります。必要に応じて、CDP、STP、または VTP を指定できます。パケットの有効な値は 1 ～ 4096 です。
ステップ 8	switch(config-if)# **l2protocol tunnel shutdown-threshold** [**cdp** | **stp** | **vtp**]	（任意） しきい値を 0 にリセットし、シャットダウンしきい値をディセーブルにします。
ステップ 9	switch(config-if)# **exit**	設定モードを終了します。
ステップ 10	switch(config)# **no shutdown**	（任意） ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 11	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。

Q-in-Q 設定の確認

コマンド	目的
clear l2protocol tunnel counters [**interface***if-range*]	すべての統計情報カウンタをクリアします。インターフェイスが指定されていない場合、すべてのインターフェイスのレイヤ2プロトコル トンネル統計情報がクリアされます。
show dot1q-tunnel [**interface***if-range*]	dot1q トンネル モードのインターフェイス範囲またはすべてのインターフェイスが表示されます。
show l2protocol tunnel [**interface***if-range* | **vlan***vlan-id*]	一定範囲のインターフェイス（特定のVLANの一部であるすべての dot1q-tunnel インターフェイスまたはすべてのインターフェイス）のレイヤ 2 プロトコル トンネル情報を表示します。
show l2protocol tunnel summary	レイヤ2プロトコル トンネルが設定されているすべてのポートのサマリーを表示します。
show running-config l2pt	現在のレイヤ2プロトコル トンネルの実行コンフィギュレーションを表示します。

Q-in-Q およびレイヤ 2 プロトコルのトンネリングの設定例

次に、イーサネット 7/1 に着信するトラフィックに対し Q-in-Q を処理するよう設定されたサービス プロバイダーのスイッチを示します。レイヤ 2 プロトコル トンネルが STP BPDU に対してイネーブルにされます。このカスタマーは VLAN 10（外部 VLAN タグ）に割り当てられます。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vlan 10
switch(config-vlan)# no shutdown
switch(config-vlan)# no ip igmp snooping
switch(config-vlan)# exit
switch(config)# interface ethernet 7/1
switch(config-if)# switchport
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# switchport access vlan 10
switch(config-if)# spanning-tree port type edge
switch(config-if)# l2protocol tunnel stp
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# exit
switch#
```

第 11 章

スタティック NAT とダイナミック NAT 変換の設定

この章は、次の項で構成されています。

ネットワーク アドレス変換の概要

ネットワークアドレス変換（NAT）は、登録されていないIPアドレスを使用してインターネットへ接続するプライベート IP インターネットワークをイネーブルにします。NAT はデバイス（通常、2 つのネットワークを接続するもの）で動作し、パケットを別のネットワークに転送する前に、社内ネットワークの（グローバルに一意のアドレスではなく）プライベートIPアドレスを正

規の IP アドレスに変換します。NAT は、ネットワーク全体に対して 1 つの IP アドレスだけを外部にアドバタイズするように設定できます。この機能により、1 つの IP アドレスの後ろに内部ネットワーク全体を効果的に隠すことで、セキュリティが強化されます。

NAT が設定されたデバイスには、少なくとも内部ネットワークに対して 1 つ、外部ネットワークに対して 1 つのインターフェイスがあります。標準的な環境では、NAT はスタブ ドメインとバックボーンの間の出口ルータに設定されます。パケットがドメインから出て行くとき、NAT はローカルで意味のある送信元 IP アドレスをグローバルで一意の IP アドレスに変換します。パケットがドメインに入ってくる際は、NAT はグローバルで一意の宛先 IP アドレスをローカル IP アドレスに変換します。出力点が複数存在する場合、個々の点で設定された NAT は、同一の変換テーブルを持っていなければなりません。

NAT は RFC 1631 に記述されています。

7.0(3)I2(1) 以降では、スタティックおよびダイナミック NAT 変換がサポートされています。

スタティック NAT に関する情報

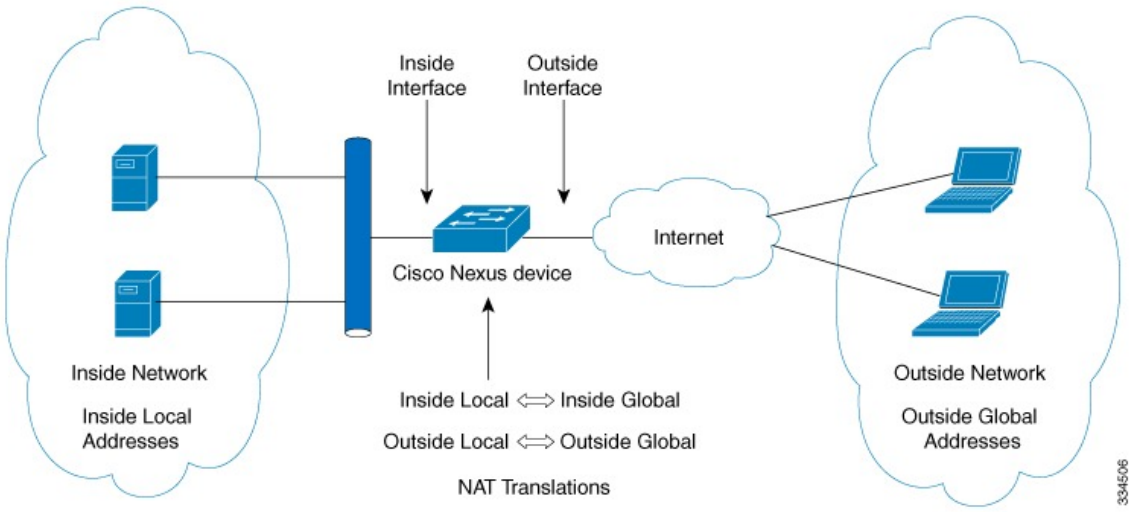
スタティック ネットワーク アドレス変換（NAT）を使用すると、ユーザは内部ローカル アドレスから外部グローバル アドレスへの 1 対 1 変換を設定することができます。これにより、内部から外部トラフィックおよび外部から内部トラフィックへの IP アドレスとポート番号の両方の変換が可能になります。Cisco Nexus デバイスはヒットレス NAT をサポートします。これは、既存の NAT トラフィック フローに影響を与えずに NAT 設定で NAT 変換を追加または削除できることを意味します。

スタティック NAT では、プライベート アドレスからパブリック アドレスへの固定変換が作成されます。スタティック NAT では 1 対 1 ベースでアドレスが割り当てられるため、プライベート アドレスと同じ数のパブリック アドレスが必要です。スタティック NAT では、パブリック アドレスは連続する各接続で同じであり、永続的な変換規則が存在するため、宛先ネットワークのホストは変換済みのホストへのトラフィックを開始できます（そのトラフィックを許可するアクセス リストがある場合）。

ダイナミック NAT およびポート アドレス変換（PAT）では、各ホストは後続する変換ごとに異なるアドレスまたはポートを使用します。ダイナミック NAT とスタティック NAT の主な違いは、スタティック NAT ではリモート ホストが変換済みのホストへの接続を開始でき（それを許可するアクセス リストがある場合）、ダイナミック NAT では開始できないという点です。

次の図に、一般的なスタティック NAT のシナリオを示します。変換は常にアクティブであるため、変換対象ホストとリモート ホストの両方で接続を生成でき、マップ アドレスは **static** コマンドによって静的に割り当てられます。

図 *33*：スタティック *NAT*



次に、スタティック NAT を理解するのに役立つ主な用語を示します。

- NAT の内部インターフェイス：プライベート ネットワークに面するレイヤ 3 インターフェイス。
- NAT の外部インターフェイス：パブリック ネットワークに面するレイヤ 3 インターフェイス。
- ローカル アドレス：ネットワークの内部（プライベート）部分に表示される任意のアドレス。
- グローバル アドレス：ネットワークの外部（パブリック）部分に表示される任意のアドレス。
- 正規の IP アドレス：Network Information Center（NIC）やサービス プロバイダーにより割り当てられたアドレス。
- 内部ローカルアドレス：内部ネットワーク上のホストに割り当てられた IP アドレス。このアドレスは正規の IP アドレスである必要はありません。
- 外部ローカル アドレス：内部ネットワークから見た外部ホストの IP アドレス。これは、内部ネットワークのルーティング可能なアドレス空間から割り当てられるため、正規のアドレスである必要はありません。
- 内部グローバルアドレス：1 つ以上の内部ローカル IP アドレスを外部に対して表すために使用できる正規の IP アドレス。

- 外部グローバルアドレス：ホスト所有者が外部ネットワーク上のホストに割り当てたIPアドレス。このアドレスは、ルート可能なアドレスまたはネットワーク空間から割り当てられた正規のアドレスです。

ダイナミック NAT の概要

ダイナミック ネットワーク アドレス変換（NAT）は、実IPアドレスのグループを宛先ネットワーク上でルーティング可能なマッピングされたIPアドレスに変換します。ダイナミックNATでは、未登録および登録 IP アドレス間の 1 対 1 のマッピングを確立しますが、マッピングは通信時に利用可能な登録済みの IP アドレスに応じて変えることができます。

ダイナミック NAT の設定は、自動的に内部ネットワークと外部ネットワーク間またはインターネット間のファイアウォールを作成します。ダイナミック NAT は、スタブ ドメイン内で生じる接続のみを許可します。外部ネットワーク デバイスは、デバイスが通信を開始しない限り、ネットワークのデバイスに接続できません。

ダイナミックNAT変換は、変換が必要なトラフィックをデバイスが受信するまで、NAT変換テーブルには存在しません。ダイナミック変換は、新しいエントリのスペースを作成するために使用されないときに、クリアまたはタイムアウトされます。通常、NAT 変換エントリは、TCAM（Ternary Content Addressable Memory）エントリが制限されている場合はクリアされます。ダイナミック NAT 変換のデフォルトの最小タイムアウトは 30 分です。

（注） Cisco NX-OS 7.0(3)I2(3) 以前のリリースでは、**ip nat translation sampling-timeout** コマンドでのサンプリングタイムアウトの最小値が 30 分から 15 分に短縮されていました。

（注） Cisco NX-OS 7.0(3)I3(1) 以降のリリースでは、**ip nat translation sampling-timeout** コマンドはサポートされていません。インストールされているNATポリシーに関して統計情報が60秒ごとに収集されます。これらの統計情報は、フローがアクティブであるかどうかを判断するために使用されます。

Cisco NX-OS 7.0(3)I2(3) 以前のリリースでは、ダイナミック NAT 変換のタイムアウトには、サンプリングタイムアウト値と TCP または UDP タイムアウト値の両方が含まれます。サンプリングタイムアウトは、デバイスがダイナミック変換のアクティビティのチェックをする時間を指定します。デフォルト値は、12 時間です。他のすべてのタイムアウトは、サンプルタイムアウトがタイムアウトになった後にのみ開始されます。サンプリングタイムアウト後、デバイスはこの変換に適合するパケットを検査します。チェックは、TCPまたはUDPタイムアウト期間中に発生します。TCP または UDP タイムアウト期間中にパケットがなければ、変換はクリアされます。アクティビティが変換で検出されると、チェックがすぐに停止され、サンプリングタイムアウト期間が開始されます。

Cisco NX-OS 7.0(3)I2(3) 以前のリリースでは、この新しいサンプリングタイムアウト期間を待機した後、デバイスはダイナミック変換のアクティビティを再度チェックします。アクティビティのチェック中に TCAM は、CPU にダイナミック NAT 変換と一致するパケットのコピーを送信しま

す。コントロール プレーン ポリシング（CoPP）が下限しきい値で設定される場合、TCP または UDP パケットは CPU に到達しない可能性があり、CPU は NAT 変換の非アクティブとしてこれを考慮します。

ダイナミック NAT は、ポートアドレス変換（PAT）およびアクセス コントロール リスト（ACL）をサポートします。オーバーロードとしても知られている PAT は、異なるポートを使用することにより、単一の登録済み IP アドレスに複数の未登録の IP アドレスをマッピングするダイナミック NAT の一形態です。NAT 設定は、同一または異なる ACL を使用して複数のダイナミック NAT 変換することができます。ただし、特定の ACL では、1 つのインターフェイスのみしか指定することができません。

タイムアウト メカニズム

Cisco NX-OS 7.0(3)I2(3) 以前のリリースでは、ダイナミック NAT 変換は作成された後、特に TCAM エントリの数が限られているため、新しい変換を作成できるように使用時にクリアする必要があります。次の NAT 変換のタイムアウト タイマーはスイッチでサポートされています。

- **timeout**：ダイナミック NAT 変換のタイムアウト値。

  タイムアウト値の範囲は、サンプリングタイムアウトを含む、60 ～ 172800 秒です。

- **sampling-timeout**：デバイスがダイナミック変換のアクティビティをチェックをする時間。

  タイムアウト値の範囲は、900 ～ 172800 秒です。

udp-timeout および **timeout** 値のタイマーは、**ip nat translation sampling-timeout** コマンドで設定されているタイムアウトの期限が切れた後にトリガーされます。

（注） Cisco NX-OS 7.0(3)I3(1) 以降のリリースでは、エージングに関して設定可能な次の 3 つの異なるオプションがあります。

- タイムアウト：これは、フローのすべてのタイプ（TCP および UDP の両方）に適用されます
- TCP タイムアウト：これは TCP フローにのみ適用されます
- UDP タイムアウト：これは UDP フローにのみ適用されます

（注） Cisco NX-OS 7.0(3)I3(1) 以降のリリースでは、設定されたタイムアウトのないダイナミック エントリを作成すると、1 時間（60 分）のデフォルトのタイムアウトが使用されます。タイムアウトを設定した後、**clear ip nat translation all** コマンドを入力すると、設定されたタイムアウトが有効になります。タイムアウトは、1 ～ 172800 秒まで設定することができます。

NAT の内部アドレスおよび外部アドレス

NAT の内部は、変換する必要がある組織が所有するネットワークを指します。NAT が設定されている場合、このネットワーク内のホストは、別の空間（グローバル アドレス空間として知られている）にあるものとしてネットワークの外側に現れる 1 つ空間（ローカル アドレス空間として知られている）内のアドレスを持つことになります。

同様に、NAT の外側は、スタブ ネットワークが接続するネットワークを指します。これらは一般に、組織の制御下にはありません。外部ネットワーク内のホストを変換の対象にすることができ、これらのホストもローカル アドレスとグローバル アドレスを持つことができます。

NAT では、次の定義が使用されます。

- ローカル アドレス：ネットワークの内部に表示されるローカル IP アドレス。
- グローバル アドレス：ネットワークの外部に表示されるグローバル IP アドレス。
- 内部ローカル アドレス：内部ネットワーク上のホストに割り当てられた IP アドレス。このアドレスは、多くの場合、Internet Network Information Center（InterNIC）やサービス プロバイダーにより割り当てられた正規の IP アドレスではありません。
- 内部グローバル アドレス：外部に向けて、1 つ以上の内部ローカル IP アドレスを表現した正規の IP アドレス（InterNIC またはサービス プロバイダーにより割り当てられたもの）。
- 外部ローカル アドレス：内部ネットワークから見た外部ホストの IP アドレス。アドレスは必ずしも正規ではありません。アドレスは、内部でルート可能なアドレス空間から割り当てられます。
- 外部グローバル アドレス：外部ネットワークに存在するホストに対して、ホストの所有者により割り当てられた IP アドレス。このアドレスは、グローバルにルート可能なアドレス、またはネットワーク空間から割り当てられます。

ダイナミック NAT のプールのサポート

Cisco NX-OS は、ダイナミック NAT のプールのサポートを提供します。ダイナミック NAT は、新しい変換のプールからグローバル アドレスを動的に割り当てるために使用できるグローバル アドレスのプールを設定できます。アドレスは、セッションが期限切れまたはクローズされた後にプールに戻されます。これは、要件に基づいてアドレスをより効率的に活用します。

PAT のサポートは、グローバル アドレス プールの使用を含みます。また、IP アドレスの使用を最適化します。PAT は、ポート番号を使用して一度に 1 つの IP アドレスを使います。ポートが該当グループで使用できない場合や、複数の IP アドレスが設定されている場合は、PAT は次の IP アドレスに移動して最初の送信元ポートを再び割り当てようとします。このプロセスは、PAT が使用できるポートと IP アドレスがなくなるまで続きます。

ダイナミック NAT および PAT では、各ホストは後続する変換ごとに異なるアドレスまたはポートを使用します。ダイナミック NAT とスタティック NAT の主な違いは、スタティック NAT では

リモートホストが変換済みのホストへの接続を開始でき（それを許可するアクセスリストがある場合）、ダイナミック NAT では開始できないという点です。

スタティックおよびダイナミック Twice NAT の概要

送信元 IP アドレスと宛先 IP アドレスの両方が、ネットワーク アドレス変換（NAT）デバイスを通過する単一パケットとして変換されると、Twice NAT と呼ばれます。Twice NAT は、スタティックおよびダイナミック変換でサポートされます。

Twice NAT は、変換グループの一部として、2 つの NAT 変換（1 つの内部および 1 つの外部）を設定することができます。これらの変換は、NAT デバイスを通して流れるように単一のパケットに適用できます。グループの一部として、2 つの変換を追加すると、個々の変換と組み合わせ変換の両方が有効になります。

NAT の内部変換では、パケットが内部から外部へ流れる際に、送信元 IP アドレスとポート番号を変更します。パケットが外部から内部に戻る際に、宛先の IP アドレスとポート番号を変更します。NAT の外部変換では、パケットが外部から内部に流れる際に、送信元 IP アドレスとポート番号を変更し、パケットが内部から外部に戻る際に、宛先 IP アドレスとポート番号を変更します。

Twice NAT を使用しない場合、変換ルールのうちの 1 つだけがパケット、送信元 IP アドレスとポート番号または宛先 IP アドレスとポート番号のいずれかに適用されます。

同じグループに属するスタティック NAT 変換は、Twice NAT 設定と見なされます。スタティック設定が、設定されたグループ ID を持っていない場合は、Twice NAT 設定では動作しません。グループ ID によって識別される単一つのグループに属するすべての内部および外部 NAT 変換は、Twice NAT 変換を形成するように対になっています。

ダイナミック Twice NAT 変換は、事前定義された **ip nat pool** または **interface overload** 設定から動的に送信元 IP アドレスとポート番号の情報を選択します。パケット フィルタリングは、ACL の設定によって実行され、ソース変換が、ダイナミック NAT ルールの使用によって実行できるように、トラフィックはダイナミック NAT 変換ルールの方向性から生成する必要があります。

ダイナミック Twice NAT は、変換グループの一部として、2 つの NAT 変換（1 つの内部および 1 つの外部）を設定することができます。1 つの変換はダイナミックである必要があり、他の変換はスタティックである必要があります。これら 2 つの変換が変換グループの一部の場合、両方の変換は、内部から外部または外部から内部のいずれかの NAT デバイスを通過するときに単一のパケットに適用できます。

VRF 対応 NAT

VRF 対応 NAT 機能は、VRF（virtual routing and forwarding instances）のアドレス空間を理解し、パケットを変換するスイッチをイネーブルにします。イネーブルにするにより、NAT 機能が 2 つの VRF 間で使用されている重複するアドレス空間のトラフィックを変換できるようになります。

VRF 対応 NAT に関する注意事項

- VRF 対応 NAT 機能は Cisco Nexus 9300 シリーズ スイッチでのみサポートされています。

- 1 つの non-default-vrf から別の non-default-vrf へ流れるトラフィックは変換されません（たとえば、vrfA を vrfB に）。
- VRF からグローバル VRF へ流れるトラフィックの場合、nat-outside コンフィギュレーションは非デフォルト VRF インターフェイスではサポートされていません。
- VRF 対応 NAT は、スタティック NAT とダイナミック NAT 設定でサポートされます。
  - トラフィックが、デフォルト以外の VRF（内部）からデフォルトの VRF（外部）に流れるように設定されている場合、**ip nat** コマンドの **match-in-vrf** オプションを 指定することはできません。
  - トラフィックが、デフォルト以外の VRF（内部）から同じデフォルト以外の VRF（外部）に流れるように設定されている場合、**ip nat** コマンドの **match-in-vrf** オプションを指定する必要があります。

    次に設定例を示します。

```
Switch(config)#ip nat inside source list <ACL_NAME>
       <[interface <INTERFACE NAME> overload] | pool <POOL NAME> [overload]]>
       [ group <1-1024> [dynamic] ] [ vrf <vrf-name> [match-in-vrf] ]
Switch(config)#ip nat inside source static [<LOCAL IP>
      <GLOBAL IP> | [tcp | udp] <LOCAL IP> <LOCAL PORT> <GLOBAL IP> <GLOBAL PORT>
 ]
       [ group <1-1024> [dynamic] ] [ vrf <vrf-name> [match-in-vrf] ]


Switch(config)#ip nat outside source list <ACL_NAME>
       <[interface <INTERFACE NAME>] | pool <POOL NAME>]>
       [ group <1-1024> [dynamic] ] [ vrf <vrf-name> [match-in-vrf] ]
Switch(config)#ip nat outside source static [<LOCAL IP>
      <GLOBAL IP> | [tcp | udp] <LOCAL IP> <LOCAL PORT> <GLOBAL IP> <GLOBAL PORT>
 ]
       [ group <1-1024> [dynamic] ] [ vrf <vrf-name> [match-in-vrf] ]
```

- VRF 対応 NAT は、フラグメント化されたパケットをサポートしていません。
- VRF 対応 NAT は、アプリケーション層の変換をサポートしていません。

  そのため、レイヤ 4 およびその他の組み込み IP は変換さず、次はエラーになります。
  - FTP
  - ICMP の障害
  - IPSec
  - HTTPS
- VRF 対応 NAT は、インターフェイスで NAT または VACL をサポートしています（ただし、両方の機能をインターフェイスで同時にサポートすることはできません）。
- VRF 対応 NAT は、元のパケットに適用され、NAT 変換済みパケットには適用されない出力 ACL をサポートしています。
- VRF 対応 NAT は、デフォルト VRF のみをサポートしています。
- VRF 対応 NAT は、MIB のサポートを提供しません。

- VRF 対応 NAT は、DCNM のサポートを提供しません。
- VRF 対応 NAT は、単一のグローバル VDC のみをサポートしています。
- VRF 対応 NAT は、アクティブ/スタンバイ スーパーバイザ モデルをサポートしていません。

スタティック NAT の注意事項および制約事項

スタティック NAT 設定時の注意事項および制約事項は、次のとおりです。

- **show** コマンドで **internal** キーワードを指定することは、サポートされていません。
- スタティック NAT 機能は Cisco Nexus 9300 シリーズ スイッチでサポートされています。
- スタティック NAT 機能は Cisco Nexus 9200 シリーズ スイッチでサポートされています。
- Cisco Nexus 9200 シリーズ スイッチでは、内部ポリシーと外部ポリシーの両方に対して **add-route** オプションが必要です。
- NAT は、スタティック NAT とダイナミック NAT の両方を含む最大 1024 の変換がサポートされています。
- NAT と sFlow は同じポートでサポートされません。
- Cisco Nexus デバイスは次のインターフェイス タイプ上の NAT をサポートしています。
  - スイッチ仮想インターフェイス（SVI）
  - ルーテッド ポート
  - レイヤ 3 およびレイヤ 3 サブインターフェイス
- NAT はデフォルトの仮想ルーティングおよびフォワーディング（VRF）テーブルのみでサポートされます。
- NAT は、IPv4 ユニキャストだけでサポートされています。
- Cisco Nexus デバイスは次をサポートしていません。
  - ソフトウェアの変換。すべての変換はハードウェアで行われます。
  - NAT および VXLAN ルーティング。
  - アプリケーション層の変換。レイヤ 4 およびその他の組み込み IP は変換されません（FTP、ICMP の障害、IPSec、HTTPS など）。
  - インターフェイス上で同時に設定された NAT および VLAN アクセス コントロール リスト（VACL）。
  - フラグメント化された IP パケットの PAT 変換。
  - ソフトウェア転送パケットの NAT 変換。たとえば、IP オプションを持つパケットは NAT 変換されません。

- デフォルトでは、NAT 機能に関して TCAM エントリが割り当てられません。他の機能の TCAM サイズを調整することにより、NAT 機能 の TCAM サイズを割り当てます。TCAM を割り当てるには、**hardware access-list tcam region nat***tcam-size* コマンドを使用します。
- HSRP および VRRP はスタティック NAT でのみサポートされます。
- IP アドレスがスタティック NAT 変換または PAT 変換に使用される場合、他の目的には使用できません。たとえば、インターフェイスに割り当てることはできません。
- スタティック NAT の場合は、外部グローバル IP アドレスが外部インターフェイス IP アドレスと異なる必要があります。
- NAT 統計情報は利用できません。
- （100 を超える）多数の変換を設定する場合、変換を設定してから NAT インターフェイスを設定する方が迅速に設定できます。
- 7.0(3)I4(1) 以降、NAT は（無中断の）In Service Software Upgrade（ISSU）をサポートしています。

ダイナミック NAT に関する制約事項

次の制限はダイナミック ネットワーク アドレス変換（NAT）に適用されます。

- **show** コマンドで **internal** キーワードを指定することは、サポートされていません。
- ダイナミック NAT 機能は Cisco Nexus 9300 シリーズ スイッチでサポートされています。
- ダイナミック NAT 機能は Cisco Nexus 9200 シリーズ スイッチでサポートされています。
- Cisco Nexus 9200 シリーズ スイッチでは、内部ポリシーと外部ポリシーの両方に対して **add-route** オプションが必要です。
- Cisco Nexus 9200 シリーズ スイッチでは、内部ポリシーと外部ポリシーの両方に対して **interface overload** オプションが必要です。
- VXLAN ルーティングは Cisco Nexus 3172 スイッチではサポートされません。
- フラグメント化されたパケットはサポートされません。
- アプリケーション レイヤ ゲートウェイ（ALG）変換はサポートされません。アプリケーション レベル ゲートウェイとしても知られている ALG は、アプリケーション パケットのペイロード内の IP アドレス情報を変換するアプリケーションです。
- 出力 ACL は、変換されたパケットには適用されません。
- デフォルト以外の Virtual Routing and Forwarding（VRF）インスタンスはサポートされません。
- MIB はサポートされていません。
- Cisco Data Center Network Manager（DCNM）はサポートされません。

- 複数のグローバル仮想デバイス コンテキスト（VDC）は、Cisco Nexus デバイスではサポートされていません。
- ダイナミック NAT 変換は、アクティブおよびスタンバイ デバイスと同期されません。
- ステートフル NAT はサポートされません。ただし、NAT と Hot Standby Router Protocol（HSRP）は共存できます。
- タイムアウト値は、設定されているタイムアウト + 119 秒になります。
- 通常、NAT の ICMP フローは、設定されたサンプリングタイムアウトと変換タイムアウトの期限後にタイムアウトになります。ただし、スイッチに存在する NAT の ICMP フローがアイドル状態になると、サンプリングタイムアウトの期限が設定された直後にタイムアウトになります。
- Cisco Nexus 9000 シリーズ スイッチで新しい変換を作成すると、フローは、変換がハードウェアでプログラムされるまでソフトウェア転送され、これには数秒かかります。この間、内部グローバル アドレスの変換エントリはありません。そのため、リターン トラフィックはドロップされます。この制限を克服するには、ループバック インターフェイスを作成し、NAT プールに属する IP アドレスを指定します。
- ダイナミック NAT の場合、外部 NAT についてはプール オーバーロードとインターフェイス オーバーロードはサポートされません。

ダイナミック Twice NAT の注意事項および制約事項

ダイナミック Twice NAT では、スタティック NAT のフローを作成する前にダイナミック NAT のフローが作成されない場合、ダイナミック Twice NAT のフローは正しく作成されません。

空の ACL が作成されると、**permit ip any any** のデフォルトのルールが設定されます。最初の ACL が空白な場合、NAT-ACL は、さらに ACL エントリと一致しません。

スタティック NAT の設定

スタティック NAT のイネーブル化

手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature nat**
3. 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 nat**	デバイス上でスタティック NAT 機能をイネーブルにします。
ステップ 3	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。

インターフェイスでのスタティック NAT の設定

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface***type slot*/*port*
3. switch(config-if)# **ip nat** {**inside** | **outside**}
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)# **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)# **ip nat** {**inside** | **outside**}	内部または外部としてインターフェイスを指定します。 （注） マーク付きインターフェイスに到着したパケットだけが変換できます。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、スタティック NAT を使用して内部のインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# ip nat inside
```

内部送信元アドレスのスタティック NAT のイネーブル化

内部送信元変換の場合、トラフィックは内部インターフェイスから外部インターフェイスに流れます。NAT は、内部ローカル IP アドレスを内部グローバル IP アドレスに変換します。リターントラフィックでは、宛先の内部グローバル IP アドレスが内部ローカル IP アドレスに変換されて戻されます。

（注） Cisco Nexus デバイスが、内部送信元 IP アドレス（Src:ip1）を外部送信元 IP アドレス（newSrc:ip2）に変換するように設定されている場合、Cisco Nexus デバイスは内部宛先 IP アドレス（newDst: ip1）への外部宛先 IP アドレス（Dst: ip2）の変換を暗黙的に追加します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip nat inside source static***local-ip-address global-ip-address* [**group***group-id*] [**vrf***vrf-name* [**match-in-vrf**]]
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)# **ip nat inside source static***local-ip-address global-ip-address* [**group***group-id*] [**vrf***vrf-name* [**match-in-vrf**]]	内部ローカル アドレスを内部グローバル アドレスに、またはその逆に（内部グローバル トラフィックを内部ローカル トラフィックに）変換するようにスタティック NAT を設定します。**group** を指定することにより、スタティック Twice NAT でこの変換が属するグループが指定されます。
ステップ 3	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、内部送信元アドレスのスタティック NAT を設定する例を示します。

```
switch# configure terminal
switch(config)# ip nat inside source static 1.1.1.1 5.5.5.5
switch(config)# copy running-config startup-config
```

外部送信元アドレスのスタティック NAT のイネーブル化

外部送信元変換の場合、トラフィックは外部インターフェイスから内部インターフェイスに流れます。NAT は、外部グローバル IP アドレスを外部ローカル IP アドレスに変換します。リターントラフィックでは、宛先の外部ローカル IP アドレスが外部グローバル IP アドレスに変換されて戻されます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip nat outside source static***global-ip-address* [**group***group-id*] [**add-route**] [**vrf***vrf-name* [**match-in-vrf**]]
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)# **ip nat outside source static***global-ip-address* [**group***group-id*] [**add-route**] [**vrf***vrf-name* [**match-in-vrf**]]	外部グローバルアドレスを外部ローカルアドレスに、またはその逆に（外部ローカルトラフィックを外部グローバルトラフィックに）変換するようにスタティック NAT を設定します。**group** を指定することにより、スタティック Twice NAT でこの変換が属するグループが指定されます。ポートなしで内部変換が設定されると、暗黙的な追加ルートが実行されます。外部変換の設定中、最初の追加ルート機能はオプションです。
ステップ 3	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、外部送信元アドレスのスタティック NAT を設定する例を示します。

```
switch# configure terminal
switch(config)# ip nat outside source static 2.2.2.2 6.6.6.6
switch(config)# copy running-config startup-config
```

内部送信元アドレスのスタティック PAT の設定

ポート アドレス変換（PAT）を使用して、特定の内部ホストにサービスをマッピングできます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip nat inside source static** {*inside-local-addressoutside-local-address* | {**tcp**| **udp**} *inside-local-address* {*local-tcp-port* | *local-udp-port*} *inside-global-address* {*global-tcp-port* | *global-udp-port*}} *global-ip-address* {**group***group-id*} {**vrf***vrf-name* {**match-in-vrf**}}
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)# **ip nat inside source static** {*inside-local-addressoutside-local-address* | {**tcp**| **udp**} *inside-local-address* {*local-tcp-port* | *local-udp-port*} *inside-global-address* {*global-tcp-port* | *global-udp-port*}} *global-ip-address* {**group***group-id*} {**vrf***vrf-name* {**match-in-vrf**}}	スタティック NAT を内部ローカル ポート、内部グローバル ポートにマッピングします。
ステップ 3	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、UDP サービスを特定の内部送信元アドレスおよび UDP ポートにマッピングする例を示します。

```
switch# configure terminal
switch(config)#  ip nat inside source static udp 20.1.9.2 63 35.48.35.48 130
switch(config)# copy running-config startup-config
```

外部送信元アドレスのスタティック PAT の設定

ポート アドレス変換（PAT）を使用して、サービスを特定の外部ホストにマッピングできます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip nat outside source static** {*outside-global-addressoutside-local-address* | {**tcp** | **udp**} *outside-global-address* {*global-tcp-port* | *global-udp-port*} *outside-local-address* {*global-tcp-port* | *global-udp-port*}} *global-ip-address* {**group***group-id*} {**add-route**} {**vrf***vrf-name* {**match-in-vrf**}}
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)# **ip nat outside source static** {*outside-global-addressoutside-local-address* | {**tcp** | **udp**} *outside-global-address* {*global-tcp-port* | *global-udp-port*} *outside-local-address* {*global-tcp-port* | *global-udp-port*}} *global-ip-address* {**group***group-id*} {**add-route**} {**vrf***vrf-name* {**match-in-vrf**}}	スタティック NAT を、外部グローバル ポート、外部ローカル ポートにマッピングします。 **group** を指定することにより、スタティック Twice NAT でこの変換が属するグループが指定されます。ポートなしで内部変換が設定されると、暗黙的な追加ルートが実行されます。外部変換の設定中、最初の追加ルート機能はオプションです。
ステップ 3	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、TCP サービスを特定の外部送信元アドレスおよび TCP ポートにマッピングする例を示します。

```
switch# configure terminal
switch(config)#  ip nat outside source static tcp 20.1.9.2 63 35.48.35.48 130
switch(config)# copy running-config startup-config
```

スタティック Twice NAT の設定

同じグループ内のすべての変換は、スタティック Twice ネットワーク アドレス 変換（NAT）ルールを作成する際に考慮されます。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **ipnatinsidesourcestatic***inside-local-ip-addressinside-global-ip-address*[**group***group-id*]
4. **ipnatoutsidesourcestatic***outside-global-ip-addressoutside-local-ip-address*[**group***group-id*] [**add-route**]
5. **interface***typenumber*
6. **ipaddress***ip-addressmask*
7. **ipnatinside**
8. **exit**
9. **interface***typenumber*
10. **ipaddress***ip-addressmask*
11. **ipnatoutside**
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `switch# configure terminal`	特権 EXEC モードを開始します。
ステップ 3	**ipnatinsidesourcestatic***inside-local-ip-addressinside-global-ip-address*[**group***group-id*] 例： `switch(config)# ip nat inside source static 10.1.1.1 192.168.34.4 group 4`	内部グローバル IP アドレスに対応する内部ローカル IP アドレスを変換するために、スタティック Twice NAT を設定します。 • **group** キーワードは、変換が属するグループを決定します。

	コマンドまたはアクション	目的
ステップ 4	**ipnatoutsidesourcestatic***outside-global-ip-addressoutside-local-ip-address*[**group***group-id*] [**add-route**] 例： `switch(config)# ip nat outside source static 209.165.201.1 10.3.2.42 group 4 add-route`	外部ローカルIPアドレスに対応する外部グローバルIPアドレスを変換するために、スタティック Twice NAT を設定します。 • **group** キーワードは、変換が属するグループを決定します。
ステップ 5	**interface***typenumber* 例： `switch(config)# interface ethernet 1/2`	インターフェイスを設定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 6	**ipaddress***ip-addressmask* 例： `switch(config-if)# ip address 10.2.4.1 255.255.255.0`	インターフェイスのプライマリIPアドレスを設定します。
ステップ 7	**ipnatinside** 例： `switch(config-if)# ip nat inside`	NAT の対象である内部ネットワークにインターフェイスを接続します。
ステップ 8	**exit** 例： `switch(config-if)# exit`	インターフェイス コンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 9	**interface***typenumber* 例： `switch(config)# interface ethernet 1/1`	インターフェイスを設定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 10	**ipaddress***ip-addressmask* 例： `switch(config-if)# ip address 10.5.7.9 255.255.255.0`	インターフェイスのプライマリIPアドレスを設定します。
ステップ 11	**ipnatoutside** 例： `switch(config-if)# ip nat outside`	NAT の対象である外部ネットワークにインターフェイスを接続します。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `switch(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

スタティック NAT および PAT の設定例

次に、スタティック NAT の設定例を示します。

```
ip nat inside source static 103.1.1.1 11.3.1.1
ip nat inside source static 139.1.1.1 11.39.1.1
ip nat inside source static 141.1.1.1 11.41.1.1
ip nat inside source static 149.1.1.1 95.1.1.1
ip nat inside source static 149.2.1.1 96.1.1.1
ip nat outside source static 95.3.1.1 95.4.1.1
ip nat outside source static 96.3.1.1 96.4.1.1
ip nat outside source static 102.1.2.1 51.1.2.1
ip nat outside source static 104.1.1.1 51.3.1.1
ip nat outside source static 140.1.1.1 51.40.1.1
```

次に、スタティック PAT の設定例を示します。

```
ip nat inside source static tcp 10.11.1.1 1 210.11.1.1 101
ip nat inside source static tcp 10.11.1.1 2 210.11.1.1 201
ip nat inside source static tcp 10.11.1.1 3 210.11.1.1 301
ip nat inside source static tcp 10.11.1.1 4 210.11.1.1 401
ip nat inside source static tcp 10.11.1.1 5 210.11.1.1 501
ip nat inside source static tcp 10.11.1.1 6 210.11.1.1 601
ip nat inside source static tcp 10.11.1.1 7 210.11.1.1 701
ip nat inside source static tcp 10.11.1.1 8 210.11.1.1 801
ip nat inside source static tcp 10.11.1.1 9 210.11.1.1 901
ip nat inside source static tcp 10.11.1.1 10 210.11.1.1 1001
ip nat inside source static tcp 10.11.1.1 11 210.11.1.1 1101
ip nat inside source static tcp 10.11.1.1 12 210.11.1.1 1201
```

例：スタティック Twice NAT の設定

次の例は、内部送信元および外部送信元のスタティック Twice NAT 設定を設定する方法を示しています。

```
Switch> enable
Switch# configure terminal
Switch(config)# ip nat inside source static 10.1.1.1 192.168.34.4 group 4
Switch(config)# ip nat outside source static 209.165.201.1 10.3.2.42 group 4
Switch(config)# interface ethernet 1/2
Switch(config-if)# ip address 10.2.4.1 255.255.255.0
Switch(config-if)# ip nat inside
switch(config-if)# exit
switch(config)# interface ethernet 1/1
switch(config-if)# ip address 10.5.7.9 255.255.255.0
switch(config-if)# ip nat outside
Switch(config-if)# end
```

スタティック NAT の設定の確認

スタティック NAT の設定を表示するには、次の作業を行います。

手順の概要

1. switch# **show ip nat translations**

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 ip nat translations**	内部グローバル、内部ローカル、外部ローカル、および外部グローバルの各 IP アドレスを示します。

次に、スタティック NAT の設定を表示する例を示します。

```
switch# sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global

--- ---                ---                51.3.1.1           104.1.1.1
--- ---                ---                95.4.1.1           95.3.1.1
--- ---                ---                96.4.1.1           96.3.1.1
--- ---                ---                51.40.1.1          140.1.1.1
--- ---                ---                51.42.1.1          142.1.2.1
--- ---                ---                51.1.2.1           102.1.2.1
--- 11.1.1.1           101.1.1.1          ---                ---
--- 11.3.1.1           103.1.1.1          ---                ---
--- 11.39.1.1          139.1.1.1          ---                ---
--- 11.41.1.1          141.1.1.1          ---                ---
--- 95.1.1.1           149.1.1.1          ---                ---
--- 96.1.1.1           149.2.1.1          ---                ---
    130.1.1.1:590      30.1.1.100:5000    ---                ---
    130.2.1.1:590      30.2.1.100:5000    ---                ---
    130.3.1.1:590      30.3.1.100:5000    ---                ---
    130.4.1.1:590      30.4.1.100:5000    ---                ---
    130.1.1.1:591      30.1.1.101:5000    ---                ---


switch# sh ip nat translations verbose
Pro Inside global      Inside local       Outside local      Outside global
any ---                ---                22.1.1.3           22.1.1.2
    Flags:0x200009 time-left(secs):-1 id:0 state:0x0 grp_id:10
any 11.1.1.130         11.1.1.3           ---                ---
    Flags:0x1 time-left(secs):-1 id:0 state:0x0 grp_id:0
any 11.1.1.133         11.1.1.33          ---                ---
    Flags:0x1 time-left(secs):-1 id:0 state:0x0 grp_id:10
any 11.1.1.133         11.1.1.33          22.1.1.3           22.1.1.2
    Flags:0x200009 time-left(secs):-1 id:0 state:0x0 grp_id:0
tcp 10.1.1.100:64490   10.1.1.2:0         20.1.1.2:0         20.1.1.2:0
    Flags:0x82 time-left(secs):43192 id:31 state:0x3 grp_id:0 vrf: default
N9300-1#
```

ダイナミック NAT の設定

ダイナミック変換および変換タイムアウトの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **ip access-list***access-list-name*
4. **permit***protocol source source-wildcard***any**
5. **deny***protocol source source-wildcard***any**
6. **exit**
7. **ipnatinsidesourcelist***access-list-name***interface***typenumber***overload** [**vrf***vrf-name* [**match-in-vrf**]]
8. **interface***typenumber*
9. **ipaddress***ip-addressmask*
10. **ipnatinside**
11. **exit**
12. **interface***typenumber*
13. **ipaddress***ip-addressmask*
14. **ipnatoutside**
15. **exit**
16. **ipnattranslationmax-entries***number-of-entries*
17. **ipnattranslationtimeout***seconds*
18. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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 3	**ip access-list***access-list-name* 例： `Switch(config)# ip access-list acl1`	アクセス リストを定義し、アクセス リスト 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	**permit***protocol source source-wildcard***any** 例： `Switch(config-acl)# permit ip 10.111.11.0/24 any`	条件に一致したトラフィックを許可する IP アクセス リストの条件を設定する。
ステップ 5	**deny***protocol source source-wildcard***any** 例： `Switch(config-acl)# deny udp 10.111.11.100/32 any`	ネットワークの入力からのパケットを拒否する IP アクセス リストの条件を設定する。
ステップ 6	**exit** 例： `Switch(config-acl)# exit`	アクセスリスト コンフィギュレーション モードを終了し、グローバル コンフィギュレーションモードに戻ります。
ステップ 7	**ipnatinsidesourcelist***access-list-name***interface***typenumber***overload** [**vrf***vrf-name* [**match-in-vrf**]] 例： `Switch(config)# ip nat inside source list acl1 interface ethernet 1/1 overload`	手順 3 で定義されたアクセス リストを指定して、ダイナミック送信元変換を設定します。
ステップ 8	**interface***typenumber* 例： `Switch(config)# interface ethernet 1/4`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**ipaddress***ip-addressmask* 例： `Switch(config-if)# ip address 10.111.11.39 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 10	**ipnatinside** 例： `Switch(config-if)# ip nat inside`	NAT の対象である内部ネットワークにインターフェイスを接続します。
ステップ 11	**exit** 例： `Switch(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーションモードに戻ります。
ステップ 12	**interface***typenumber* 例： `Switch(config)# interface ethernet 1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 13	**ipaddress***ip-addressmask* 例： `Switch(config-if)# ip address 172.16.232.182 255.255.255.240`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 14	**ipnatoutside** 例： `Switch(config-if)# ip nat outside`	外部ネットワークにインターフェイスを接続します。
ステップ 15	**exit** 例： `Switch(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 16	**ipnattranslationmax-entries***number-of-entries* 例： `Switch(config)# ip nat translation max-entries 300`	ダイナミック NAT 変換の最大数を指定します。エントリの数は、1 ～ 1023 を指定できます。
ステップ 17	**ipnattranslationtimeout***seconds* 例： `switch(config)# ip nat translation timeout 13000`	ダイナミック NAT 変換のタイムアウト値を指定します。
ステップ 18	**end** 例： `Switch(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ダイナミック NAT プールの設定

単一の **ip nat pool** コマンドで IP アドレスの範囲を定義することにより、または **ip nat pool** および **address** コマンドを使用することにより NAT プールを作成できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature nat**
3. switch(config)# **ip nat pool***pool-name* [*startipendip*] {**prefix***prefix-length* | **netmask***network-mask*}
4. （任意） switch(config-ipnat-pool)# **address***startipendip*
5. （任意） switch(config)# **no ip nat pool***pool-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# **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 nat**	デバイスで NAT 機能をイネーブルにします。
ステップ 3	switch(config)# **ip nat pool***pool-name* [*startipendip*] {**prefix***prefix-length* | **netmask***network-mask*}	グローバル IP のアドレスの範囲の NAT プールを作成します。IP アドレスは、プレフィクス長またはネットワーク マスクを使用してフィルタリングされます。
ステップ 4	switch(config-ipnat-pool)# **address***startipendip*	（任意） グローバル IP アドレスの範囲が、プールの作成中に指定されていない場合は指定します。
ステップ 5	switch(config)# **no ip nat pool***pool-name*	（任意） 指定された NAT プールを削除します。

この例では、プレフィクス長を使用した NAT プールの作成方法を示します。

```
switch# configure terminal
switch(config)# ip nat pool pool1 30.1.1.1 30.1.1.2 prefix-length 24
switch(config)#
```

この例では、ネットワーク マスクを使用した NAT プールの作成方法を示します。

```
switch# configure terminal
switch(config)# ip nat pool pool5 20.1.1.1 20.1.1.5 netmask 255.0.255.0
switch(config)#
```

この例では、**ip nat pool** および **address** コマンドを使用した NAT プールの作成およびグローバル IP アドレスの範囲の定義方法を示します。

```
switch# configure terminal
switch(config)# ip nat pool pool7 netmask 255.255.0.0
switch(config-ipnat-pool)# address 40.1.1.1 40.1.1.5
switch(config-ipnat-pool)#
```

この例では、NAT プールの削除方法を示します。

```
switch# configure terminal
switch(config)# no ip nat pool pool4
switch(config)#
```

送信元リストの設定

内部インターフェイスと外部インターフェイスの IP アドレスの送信元リストを設定できます。

はじめる前に

プールの送信元リストを設定する前に、プールの設定を確認してください。

手順の概要

1. switch# **configure terminal**
2. （任意） switch# **ip nat inside source list***list-name***pool***pool-name* [**overload**]
3. （任意） switch# **ip nat outside source list***list-name***pool***pool-name* [**add-route**]

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# **ip nat inside source list***list-name***pool***pool-name* [**overload**]	（任意） オーバーロードの有無にかかわらずプールを使用した NAT 内部送信元リストを作成します。
ステップ 3	switch# **ip nat outside source list***list-name***pool***pool-name* [**add-route**]	（任意） オーバーロードをかけずにプールを使用した NAT 外部送信元リストを作成します。

この例では、オーバーロードをかけずにプールを使用したNAT内部送信元リストを作成する方法を示します。

```
switch# configure terminal
switch(config)# ip nat inside source list list1 pool pool1
switch(config)#
```

この例では、オーバーロードをかけてプールを使用したNAT内部送信元リストを作成する方法を示します。

```
switch# configure terminal
switch(config)# ip nat inside source list list2 pool pool2 overload
switch(config)#
```

この例では、オーバーロードをかけずにプールを使用したNAT外部送信元リストを作成する方法を示します。

```
switch# configure terminal
switch(config)# ip nat outside source list list3 pool pool3
switch(config)#
```

内部送信元アドレスのダイナミック Twice NAT の設定

内部送信元アドレス変換の場合、トラフィックは内部インターフェイスから外部インターフェイスに流れます。内部送信元アドレスのダイナミック Twice NAT を設定できます。

はじめる前に

スイッチ上で NAT がイネーブルであることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip nat outside source static***outside-global-ip-addressoutside-local-ip-address* | [**tcp** | **udp**] *outside-global-ip-addressoutside-global-portoutside-local-ip-addressoutside-local-port* [**group***group-id*] [**add-route**] [**dynamic**]
3. switch(config)# **ip nat inside source list***access-list-name* [**interface***typeslot/port***overload** | **pool***pool-name*] [**group***group-id*] [**dynamic**]]
4. switch(config)# **ip nat pool***pool-name* [*startipendip*] {**prefix***prefix-length* | **netmask***network-mask*}
5. switch(config)# **interface***typeslot/port*
6. switch(config-if)# **ip nat outside**
7. switch(config-if)# **exit**
8. switch(config)# **interface***typeslot/port*
9. switch(config-if)# **ip nat inside**

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)# **ip nat outside source static***outside-global-ip-addressoutside-local-ip-address* | [**tcp** | **udp**] *outside-global-ip-addressoutside-global-portoutside-local-ip-addressoutside-local-port* [**group***group-id*] [**add-route**] [**dynamic**]	外部グローバルアドレスを内部ローカルアドレスに変換する、または内部ローカルトラフィックを内部グローバルトラフィックに変換するようにスタティック NAT を設定します。 **group** キーワードは、変換が属するグループを決定します。
ステップ 3	switch(config)# **ip nat inside source list***access-list-name* [**interface***typeslot/port***overload** | **pool***pool-name*] [**group***group-id*] [**dynamic**]]	オーバーロードの有無にかかわらずプールを使用した NAT 内部送信元リストを作成する

	コマンドまたはアクション	目的
		ことにより、ダイナミック送信元変換を確立します。 **group** キーワードは、変換が属するグループを決定します。
ステップ 4	switch(config)# **ip nat pool***pool-name* [*startipendip*] {**prefix***prefix-length* | **netmask***network-mask*}	グローバル IP のアドレスの範囲の NAT プールを作成します。IP アドレスは、プレフィクス長またはネットワークマスクを使用してフィルタリングされます。
ステップ 5	switch(config)# **interface***typeslot/port*	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	switch(config-if)# **ip nat outside**	外部ネットワークにインターフェイスを接続します。
ステップ 7	switch(config-if)# **exit**	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	switch(config)# **interface***typeslot/port*	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	switch(config-if)# **ip nat inside**	NAT の対象である内部ネットワークにインターフェイスを接続します。

次に、内部送信元アドレスのダイナミック Twice NAT 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)# ip nat outside source static 2.2.2.2 4.4.4.4 group 20 dynamic
switch(config)# ip nat inside source list acl_1 pool pool_1 overload group 20 dynamic
switch(config)# ip nat pool pool_1 3.3.3.3 3.3.3.10 prefix-length 24
switch(config)# interface Ethernet1/8
switch(config-if)# ip nat outside
switch(config-if)# exit
```

```
switch(config)# interface Ethernet1/15
switch(config-if)# ip nat inside
```

外部送信元アドレスのダイナミック Twice NAT の設定

外部送信元アドレス変換の場合、トラフィックは外部インターフェイスから内部インターフェイスに流れます。外部送信元アドレスのダイナミック Twice NAT を設定できます。

はじめる前に

スイッチ上で NAT がイネーブルであることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip nat inside source static***inside-local-ip-addressinside-global-ip-address* | [**tcp** | **udp**] *inside-local-ip-addresslocal-portinside-global-ip-addressglobal-port* [**group***group-id*] [**dynamic**]
3. switch(config)# **ip nat outside source list***access-list-name* [**interface***typeslot/port***overload** | **pool***pool-name*] [**group***group-id*] [**add-route**] [**dynamic**]
4. switch(config)# **ip nat pool***pool-name* [*startipendip*] {**prefix***prefix-length* | **netmask***network-mask*}
5. switch(config)# **interface***typeslot/port*
6. switch(config-if)# **ip nat outside**
7. switch(config-if)# **exit**
8. switch(config)# **interface***typeslot/port*
9. switch(config-if)# **ip nat inside**

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)# **ip nat inside source static***inside-local-ip-addressinside-global-ip-address* | [**tcp** | **udp**] *inside-local-ip-addresslocal-portinside-global-ip-addressglobal-port* [**group***group-id*] [**dynamic**]	内部グローバル アドレスを内部ローカル アドレスに変換する、または内部ローカル トラフィックを内部グローバル トラフィックに変換するようにスタティック NAT を設定します。 **group** キーワードは、変換が属するグループを決定します。
ステップ 3	switch(config)# **ip nat outside source list***access-list-name* [**interface***typeslot/port***overload** | **pool***pool-name*] [**group***group-id*] [**add-route**] [**dynamic**]	オーバーロードの有無にかかわらずプールを使用した NAT 外部送信元リストを作成することにより、ダイナミック送信元変換を確立します。

	コマンドまたはアクション	目的
ステップ 4	switch(config)# **ip nat pool***pool-name* [*startipendip*] {**prefix***prefix-length* | **netmask***network-mask*}	グローバル IP のアドレスの範囲の NAT プールを作成します。IP アドレスは、プレフィクス長またはネットワーク マスクを使用してフィルタリングされます。
ステップ 5	switch(config)# **interface***typeslot/port*	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	switch(config-if)# **ip nat outside**	外部ネットワークにインターフェイスを接続します。
ステップ 7	switch(config-if)# **exit**	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	switch(config)# **interface***typeslot/port*	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	switch(config-if)# **ip nat inside**	NAT の対象である内部ネットワークにインターフェイスを接続します。

次に、外部送信元アドレスのダイナミック Twice NAT 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)# ip nat inside source static 7.7.7.7 5.5.5.5 group 30 dynamic
switch(config)# ip nat pool pool_2 4.4.4.4 4.4.4.10 prefix-length 24
switch(config)# interface Ethernet1/6
switch(config-if)# ip nat outside
switch(config-if)# exit
switch(config)# interface Ethernet1/11
switch(config-if)# ip nat inside
```

ダイナミック NAT 変換のクリア

ダイナミック変換をクリアするには、次の作業を実行します。

コマンド	目的
clearipnattranslation [**all** | **inside***global-ip-addresslocal-ip-address* [**outside***local-ip-addressglobal-ip-address*] | **outside***local-ip-addressglobal-ip-address*]	すべてまたは特定のダイナミック NAT 変換を削除します。

この例では、すべてのダイナミック変換をクリアする方法を示します。

```
switch# clear ip nat translation all
```

この例では、内部および外部アドレスのダイナミック変換をクリアする方法を示します。

```
switch# clear ip nat translation inside 2.2.2.2 4.4.4.4 outside 5.5.5.5 7.7.7.7
```

ダイナミック NAT の設定の確認

ダイナミック NAT の設定を表示するには、次の作業を行います。

コマンド	目的
show ip nat translations	アクティブなネットワーク アドレス変換（NAT）を表示します。 エントリがいつ生成され、いつ使用されたかを含む各変換テーブルエントリの追加情報が表示されます。
show run nat	NAT の設定を表示します。

この例では、NAT の実行コンフィギュレーションを表示する方法を示します。

```
switch# show run nat

!Command: show running-config nat
!Time: Wed Apr 23 11:17:43 2014

version 6.0(2)A3(1)
feature nat

ip nat inside source list list1 pool pool1
ip nat inside source list list2 pool pool2 overload
ip nat inside source list list7 pool pool7 overload
ip nat outside source list list3 pool pool3
ip nat pool pool1 30.1.1.1 30.1.1.2 prefix-length 24
ip nat pool pool2 10.1.1.1 10.1.1.2 netmask 255.0.255.0
ip nat pool pool3 30.1.1.1 30.1.1.8 prefix-length 24
ip nat pool pool5 20.1.1.1 20.1.1.5 netmask 255.0.255.0
ip nat pool pool7 netmask 255.255.0.0
  address 40.1.1.1 40.1.1.5
```

この例では、アクティブ NAT 変換を表示する方法を示します。

オーバーロードをかけた内部プール

```
switch# show ip nat translation
Pro  Inside global      Inside local       Outside local      Outside global
icmp 20.1.1.3:64762     10.1.1.2:133       20.1.1.1:0         20.1.1.1:0
icmp 20.1.1.3:64763     10.1.1.2:134       20.1.1.1:0         20.1.1.1:0
```

オーバーロードをかけない外部プール

```
switch# show ip nat translation
Pro  Inside global      Inside local       Outside local      Outside global
any  ---                ---                177.7.1.1:0        77.7.1.64:0
any  ---                ---                40.146.1.1:0       40.46.1.64:0
```

```
any  ---                 ---                 10.4.146.1:0       10.4.46.64:0
```

例：ダイナミック変換および変換タイムアウトの設定

次の例では、アクセス リストを指定して、ダイナミック オーバーロード ネットワーク アドレス変換（NAT）を設定する方法を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# ip access-list acl1
Switch(config-acl)# permit ip 10.111.11.0/24 any
Switch(config-acl)# deny udp 10.111.11.100/32 any
Switch(config-acl)# exit
Switch(config)# ip nat inside source list acl1 interface ethernet 1/1 overload
Switch(config)# interface ethernet 1/4
Switch(config-if)# ip address 10.111.11.39 255.255.255.0
Switch(config-if)# ip nat inside
Switch(config-if)# exit
Switch(config)# interface ethernet 1/1
Switch(config-if)# ip address 172.16.232.182 255.255.255.240
Switch(config-if)# ip nat outside
Switch(config-if)# exit
Switch(config)# ip nat translation max-entries 300
Switch(config)# ip nat translation timeout 13000
Switch(config)# end
```

付 録 A

レイヤ 2 データセンター相互接続の設定

ここでは、仮想ポートチャネル（vPC）を使用したレイヤ 2 データセンター相互接続（DCI）の設定例を示します。

概要

データセンター相互接続（DCI）の目的は、異なるデータセンター間で特定の VLAN を拡張することです。これにより、遠く離れた場所にあるサーバとネットワーク アタッチド ストレージ（NAS）デバイスのレイヤ 2 隣接関係が提供されます。

vPC は、2 つのサイト（DCI vPC 全体にわたるブリッジ プロトコル データ ユニット（BPDU）なし）間の STP 分離というメリットを提供します。これは、データセンター間に冗長リンクが提供され、データセンターの停止がリモート データセンターに伝搬しないことを意味します。

（注） vPC は最大 2 つのデータセンターを相互接続するために使用できます。

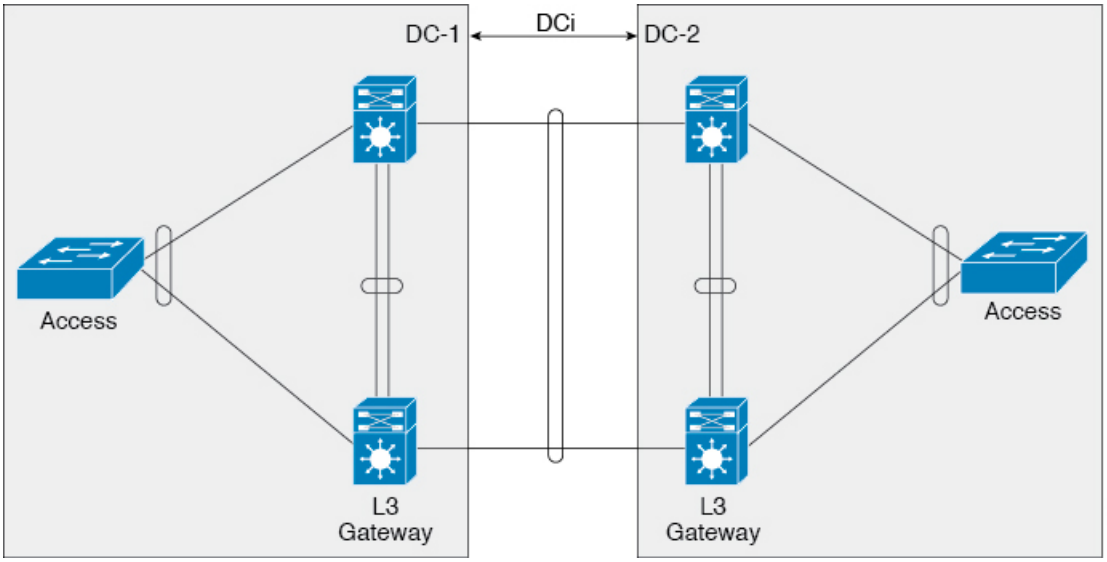
レイヤ 2 データセンター相互接続の例

次に、vPC を使用したレイヤ 2 データセンター相互接続（DCI）の設定例を示します。この例では、First Hop Redundancy Protocol（FHRP）を分離できます。

（注） vPC と Hot Standby Routing Protocol（HSRP）はすでに設定されています。

（注） DCI として機能する Link Aggregation Control Protocol（LACP）を vPC リンク で使用する必要があります。

図 *34*：デュアル レイヤ *2*/レイヤ *3* のポッド相互接続



この例では、レイヤ 3（L3）ゲートウェイが同じ vPC ペアで設定されており、DCI として機能します。Hot Standby Router Protocol（HSRP）を分離するために、DCI ポート チャネルでポート アクセス コントロール リスト（PACL）を設定し、DCI を通過する VLAN に関してスイッチ仮想インターフェイス（SVI）で HSRP Gratuitous Address Resolution Protocol（ARP）（GARP）を無効にする必要があります。

```
ip access-list DENY_HSRP_IP
  10 deny udp any 224.0.0.2/32 eq 1985
  20 deny udp any 224.0.0.102/32 eq 1985
  30 permit ip any any

interface <DCI-Port-Channel>
  ip port access-group DENY_HSRP_IP in

interface Vlan <x>
  no ip arp gratuitous hsrp duplicate
```

付 録 B

Cisco NX-OS インターフェイスがサポートする IETF RFC

ここでは、Cisco NX-OS でサポートされているインターフェイスの IETF RFC を示します。

IPv6 の RFC

RFC	Title
RFC 1981（7.0(3)I1(1) 以降）	『*Path MTU Discovery for IP version 6*』
RFC 2373	『*IP Version 6 Addressing Architecture*』
RFC 2374	『*An Aggregatable Global Unicast Address Format*』
RFC 2460	『*Internet Protocol, Version 6 (IPv6) Specification*』
RFC 2462	『*IPv6 Stateless Address Autoconfiguration*』
RFC 2464	『*Transmission of IPv6 Packets over Ethernet Networks*』
RFC 2467	『*Transmission of IPv6 Packets over FDDI Networks*』
RFC 2472	『*IP Version 6 over PPP*』
RFC 2492	『*IPv6 over ATM Networks*』
RFC 2590	『*Transmission of IPv6 Packets over Frame Relay Networks Specification*』

RFC	Title
RFC 3021	『*Using 31-Bit Prefixes on IPv4 Point-to-Point Links*』
RFC 3152	『*Delegation of IP6.ARPA*』
RFC 3162	『*RADIUS and IPv6*』
RFC 3513	『*Internet Protocol Version 6 (IPv6) Addressing Architecture*』
RFC 3596	『*DNS Extensions to Support IP version 6*』
RFC 4193	『*Unique Local IPv6 Unicast Addresses*』

付 録 C

Cisco NX-OS インターフェイスの設定制限

設定の制限は、『*Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*』に記載されています。

索 引

G

H

I

L

M

N

P

R

S

T

U

V

い

し

て

と

り