Cisco Nexus 9000 シリーズ NX-OS インターフェイス構成ガイド、リリース 10.6(x)

最終更新：2026 年 2 月 2 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、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x | y]	いずれか1つを選択できる省略可能なキーワードや引数は、角かっこで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。

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

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の 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。

https://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。

通信、サービス、およびその他の情報

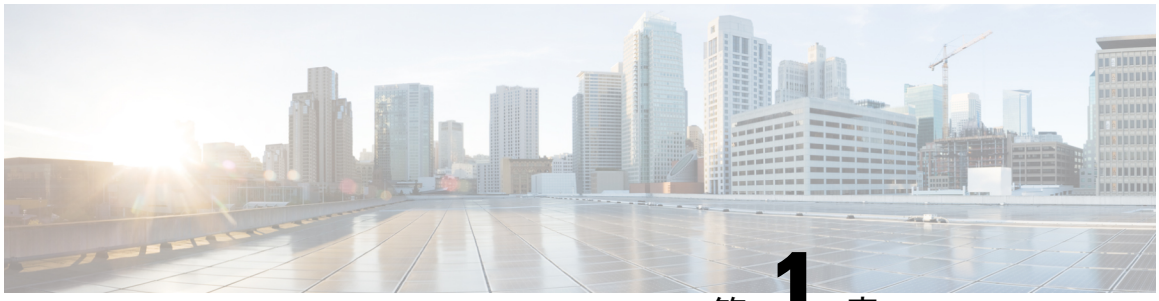
- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet [英語] にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press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

Cisco バグ検索ツール

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

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。



第 1 章

新機能と更新情報

次の表は、*Cisco Nexus 9000* シリーズ *NX-OS* インターフェイス設定ガイド リリース *10.6(x)*に記載されている新機能および変更機能をまとめたものです。それぞれの説明が記載されている箇所も併記されています。

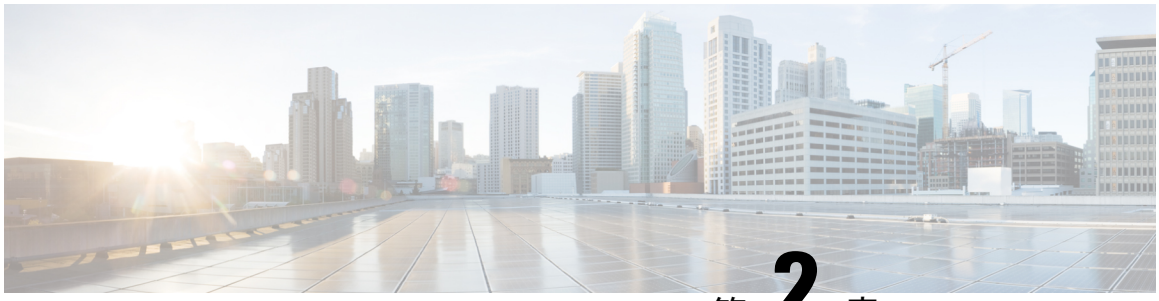
- 新機能および変更された機能に関する情報 （1 ページ）

新機能および変更された機能に関する情報

表 *1*: 新機能および変更された機能

特長	説明	変更が行われたリリース	参照先
Support for Layer 3 interfaces on Cisco Nexus 93C64E-SG2-Q スイッチ	レイヤ 3 インターフェイスのサポートが追加されました。	10.5(3)F	レイヤ 3 インターフェイスの注意事項および制約事項
での BFD のサポート Cisco Nexus 93C64E-SG2-Q スイッチ	シングルホップ BFD、BFD エコー機能、および非同期 BFD のサポートが追加されました。	10.5(3)F	ガイドラインと制約事項
での 800G ブレークアウト モードのサポート Cisco Nexus 93C64E-SG2-Q スイッチ • ブレークアウト 2x400G ポート • ブレークアウト 8x100G ポート	2x400G および 8x100G ブレークアウト モードのサポートが追加されました。	10.5(3)F	ガイドラインと制約事項

特長	説明	変更が行われたリリース	参照先
Cisco Nexus 93C64E-SG2-Q スイッチでの新しい光モジュールのサポート。	次の光学系のサポートが追加されました。 • QDD-8X100G-FR • QDD-8x100G-LR • QDD-2X400G-FR4 • QDD-2x400G-LR4 • QDD-800G CU 1 M • QDD-800G CU 1.5 M • QDD-800G CU 2M	10.5(3)F	ガイドラインと制約事項
IP アンナンバードを備えた N9800 スパイン	Cisco Nexus 9808 および 9804 スイッチにアンナンバード IP を追加	10.5（2）F	レイヤ 3 インターフェイスの注意事項および制約事項 （141 ページ）
SVI 統計レート	**hardware profile svi-and-si flex-stats-enable** コマンドが有効になっている場合、SVI 統計レートがサポートされます。	10.5（2）F	SVI およびサブインターフェイスの入力/出力ユニキャストカウンタの設定 （161 ページ） レイヤ 3 インターフェイスの設定例 （167 ページ）
VLAN マッピングでの入力としての予約済み VLAN の使用の許可	VLAN マッピングの入力 VLAN範囲を VLAN 1 ～ 3967 から VLAN 1 ～ 4094 に増やすサポートが追加されました。	10.5(1)F	VLAN 上のポート VLAN マッピングの構成 （422 ページ）



第 2 章

概要

ライセンス要件

Cisco NX-OSを動作させるには、機能とプラットフォームの要件に従って適切なライセンスを取得し、インストールする必要があります。

- 基本（Essential）ライセンスとアドオンライセンスが、さまざまな機能セットに使用できます。
- ライセンスは、製品および購入オプションに応じて、永続的、一時的、または評価可能な場合があります。
- 高度な機能を使用するには、基本ライセンス以外の追加の機能ライセンスが必要です。
- 高度な機能を使用するには、基本ライセンス以外の追加ライセンスが必要です。
- ライセンスの適用と管理は、デバイスのコマンドライン インターフェイス（CLI）を介して行われます。

ハードウェアの取り付け手順の詳細については、 *Cisco NX-OS* ライセンス ガイド および を参照してください*Cisco NX-OS* ライセンシング オプション ガイド。

サポートされるプラットフォーム

Nexus スイッチ プラットフォーム サポート マトリックスには、次のものがリストされています。

- サポートされているCisco Nexus 9000 および 3000 スイッチ モデル

- NX- OS ソフトウェア リリース バージョン

プラットフォームと機能の完全なマッピングについては、 Nexus Switch Platform Support Matrix を参照してください。

インターフェイス パラメータ

インターフェイス パラメータは、

- ネットワーク インターフェイスの動作特性を定義し、
- 管理者が特定のロールに合わせてインターフェイスの動作を調整できるようにし
- は、パフォーマンス、セキュリティ、および接続の拡張をサポートする構成設定です。

Cisco NX-OS は、サポート対象の各インターフェイス タイプの複数の構成パラメータをサポートします。これらのパラメータの大部分がこのガイドで説明されています。一部のパラメータは他のドキュメントで説明されています

次の表に、構成可能なインターフェイス パラメータに関する詳細情報のソースを示します。

表 *2:* インターフェイスのパラメータ

機能	パラメータ	解説場所
基本パラメータ	説明、デュプレックス、エラー ディセーブル、フロー制御、MTU、ビーコン	「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、仮想ルーティングおよび転送（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、リンク集約制御プロトコル（LACP）	『ポート チャネルの設定』
セキュリティ	イーサネット OAM 単方向（EOU）	『*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*』

イーサネット インターフェイスのベスト プラクティス

イーサネット インターフェイスには、次の特性があります。

- 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。
- N9K-C9316D-GX の場合：ポート 1 ー 16 は QSA で 400G、100G、40G および 10G をサポートします。

Cisco Nexus N9K-C9364C-GX および N9K-C93600CD-GX でのクアッドグループ設定のベストプラクティス

これらのガイドラインを活用、Cisco Nexus N9K-C9364C-GX および N9K-C93600CD-GX スイッチでクワッド グループを設定します。

- 4 つのインターフェイスの連続したグループ（1 ～ 4、5 ～ 8、9 ～ 12 など）は、クワッド グループを形成します。

  クワッド グループ内でリンク速度を混在させて使用することはサポートされていません。これは、N9K-C93600CD-GX のポート 1 ～ 24 および N9K-C9364C-GX のすべてのポートに適用されます。

- クワッド グループでは一度に 1 つの速度のみがアクティブになります。クワッド グループで最初にアップするリンクによって速度が設定されます。他の速度のポートはダウンし、**[リンクが接続されていません（Link not connected）]**と表示されます。
- クワッド グループで異なる速度を混在させると、動作速度は記録されません。一致しないトランシーバを挿入して起動すると、グループ内のすべてのポートがリセットされます。リセット後にアップになる最初のリンクによって、クワッド グループの速度が決まります。既存のリンクはシャットダウンする可能性があります。一致していないトランシーバを削除して回復します。
- FC-FEC は、50Gx2 ブレークアウト ポートの 2 番目のレーンではサポートされません。50Gx2 ブレークアウトが設定されている場合、2 番目のブレークアウト ポートはアップしません。50Gx2 ブレークアウトで RS-FEC を構成します。
- Cisco Nexus NX-OS Release 10.1（2）以降では、NRZ モードの NX-OS N9K-C93600CD-GX、N9K-C9316D-GX、および N9K-C9364C-GX の速度 40G および 100G で自動ネゴシエーションがサポートされています。
- Cisco Nexus NX-OS Release 10.4(3) F 以降の、N9K-C93600CD-GX および N9K-C9316D-GX では、100G 銅線 PAM4 リンクでの自動ネゴシエーションはサポートされていません。リンクをアップにするには、ピア側で **speed 100000** を構成する必要があります。
- Cisco Nexus NX-OS リリース 10.4(3)F 以降、N9K-C93600CD-GX では、100G PAM4 リンクはポート 29 ー 36 でのみサポートされます。

Nexus N9K-X9400-16W のブレークアウト ポートに関する考慮事項

これらは、 Cisco Nexus 9408シャーシおよび Cisco N9K-X9400-16W（16x200G line-Ccrd 拡張モジュール（LEM））のブレークアウトポートの制限です。

- ネイティブ ポートは、すべてのポートで 100G、40G、10G をサポートします。
- ブレークアウト ポートは 4x10G、4x25G をサポートしますが、次の制限があります。
  1. 4x10G、4x25G ブレークアウト ポートは、奇数ポートでのみサポートされます。
  2. ブレークアウト x4 が奇数ポートに構成されている場合、対応する偶数ポートが自動的に消去されます。
- ブレークアウト ポートは、次の制限付きで 2x50G をサポートします。
  1. 2x50G ブレークアウトは、奇数ポートと偶数ポートでサポートされます。
  2. 2x50G ブレークアウトが奇数または偶数ポートで構成されている場合、対応する偶数または奇数ポートは自動的に 2x50G にブレークアウトされます。
- QSA を使用した 10G は、次の制限付きですべてのポートでサポートされます。
  1. 10G、40G、100G トランシーバがリンクアップ状態の奇数または偶数ポートに存在する場合、対応する偶数または奇数ポートでは他の速度は許可されません。

     不一致の XCVR に関する警告または syslog が出力され、後で挿入された XCVR ポートのポート ステータスが**速度不一致**状態に変更されます。

     ポートのステータスは、 **show interface brief** および **show interface status** コマンドの出力に示されます。
  2. 奇数ポートに 40G または 100G があり、対応する偶数ポートに 10Gトランシーバがあるか、またはその逆で、 **admin shut** 状態にある場合、これらの条件が当てはまります。
     - ポートが admin shut のままである限り、優先順位は決定されません。no **shutdown** として構成されているポートが優先されます。
     - 両方のポートが同時に **no shutdown** として設定されている場合、ソフトウェアによって最初に検出されたポートが優先され、その他のポートは **xcvr 不一致** 状態になります。

       スイッチがリロードされる場合、ブートアップ時にソフトウェアによって最初に検出されたポートが優先され、残りは**速度不一致**状態になります。

Cisco Nexus NX-OSリリース 10.5(1)F 以降では、これらの注意事項と制約事項が適用されます：

- ポート 1 ～ 16 の場合、ポートのすべてのペア（1,2 | 3,4 | 5,6 | 7,8 | 9,10 | 11,12 | 13,14 | 15,16）はクワッド グループを形成します 。
- クワッド内のすべてのポートは、QSA の 10G、または 40G、100G、または 200G で動作します。

- これらの例外を除き、同じクワッド内では混合速度はサポートされません。
  - 40G と 100G の混合速度は、クワッドでサポートされます。
  - ただし、100G-CR2 を、クワッド内で 40G または他のタイプの 100G 光学系と混在させることはできません。
- 光学系の挿入と取り外しシーケンスでは、クワッド速度の不一致チェックが行われます。クワッド グループに最初に挿入されたトランシーバにより、クワッド グループの速度が決まります。

  サポートされていない速度のポートは、**XCVR速度の不一致**としてダウンします。サポートされていない混合速度では、クワッド グループで一度に 1 つの速度のみがアップします。
- 特定のポートを起動して機能させるには、そのクワッドのすべてのポートからすべての光ファイバまたはケーブルを取り外し、起動する必要があるポートに光またはケーブルを接続してから、他の光学系またはケーブルを接続します。 。
- 特定の速度不一致ポートを稼働させて機能させるには、そのクワッドの他のすべてのポートから光学系またはケーブルを取り外し、必要なポートをフラップしてから、他のポートを接続します。
- ポート状態を保持するように構成（copy running start-up）を保存します。
- 一致しないトランシーバがクワッドに接続されると、syslog が生成されます。

```
Interface Ethernet1/X is down (Reason: Inserted transceiver speed mismatch with quad
 speed Y)
```

- ascii のリロード後、インターフェイスが検出された順序によってポートの状態が変わる場合がある
- 中断や不確定な状態を避けるために、クワッドでは必ず同じ速度のトランシーバのみを使用してください。

（注） 光モジュールの取り外しまたは挿入を行う前に、LEM の電源がオンでオンラインであることを確認してください。電源がオフまたはオフラインのときに光ファイバの取り外しまたは取り付けを行うと、ソフトウェアが光ファイバを検出せず、ポート状態に矛盾が生じる可能性があります。

ポートに関する考慮事項 Cisco Nexus N9K-X9400-22L

Cisco Nexus NX-OS リリース 10.5(1) 以降では、次の注意事項と制約事項が適用されます：

- ポート 1 ～ 22 では、連続する 4 つのポート（1 ～ 4、5 ～ 8、11 ～ 14、15 ～ 18、19 ～ 22）と 2 つのポート（9 ～ 10）の各グループがクワッド グループと呼ばれます。
- クワッド内のすべてのポートは、10G、または 25G、または 50G で動作します。

- これらの例外を除き、同じクワッド内では混合速度はサポートされません。
  - 10G と 25G の混合速度は、クワッドでサポートできます。
- 光学系の挿入と取り外しシーケンスでは、クワッド速度の不一致チェックが行われます。クワッド グループに最初に挿入されたトランシーバにより、クワッド グループの速度が決まります。

  サポートされていない速度のポートは、**XCVR 速度の不一致**としてダウンします。サポートされていない混合速度では、クワッド グループで一度に 1 つの速度のみがアップします。
- 特定のポートを機能させるには、そのクワッドの各ポートからすべての光ファイバまたはケーブルを取り外します。まず、光ファイバまたはケーブルを目的のポートに差し込み、その他を接続します。
- 速度の不一致を持つポートを機能させるには、そのクワッド内の他のポートから光ファイバまたはケーブルを取り外します。必要なポートをフラップし、他のポートを接続します。
- ポート状態を永続的にするために、構成を保存（copy running startup）します。
- クワッドにミスマッチのトランシーバを接続すると、syslog に**Interface Ethernet1 / X is down**（**Reason**：**Inserted Transceiver Speed Mismatch with Quad Speed Y** と記録されます。
- ポートの状態は、ASCII のリロード時に永続的ではない可能性があります。ポートの状態は、ASCII のリロード時に検出されたインターフェースの順序に依存します。
- 中断や不確定な状態を避けるために、クワッドでは必ず同じ速度のトランシーバのみを使用してください。
- 1 つのクワッド内のすべてのデュアル スピード オプティクスがデフォルト以外の速度に設定され、**reload acii** が実行されると、**xcvr speed mismatch**により一部のポートがダウンする可能性があります。

  これらのポートで **shut** コマンドと **no shut** コマンドを活用、それらを起動して機能させます。

（注） LEM の電源がオフまたはオフラインのときに、光ファイバを取り外したり、取り付けたりしないでください。そうした場合、ソフトウェアは光ファイバを検出できず、ポートの状態が不整合になる可能性があります。

アクセス ポート

アクセス ポートは、単一のVLAN のトラフィックだけを伝送するレイヤ 2 スイッチ ポートです。このポートのタイプはレイヤ 2 インターフェイスだけです。

アクセス ポートの詳細については、「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。

ルーテッド ポート

ルーテッド ポートは、（仮想インターフェイスではなく）物理スイッチ ポート上に設定するレイヤ 3 インターフェイスです。IP トラフィックを別のデバイスにルーティングします。

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」のセクションを参照してください。

管理インターフェイス

管理インターフェイスは、

- デバイス管理専用の接続を提供し、
- データ トラフィック インターフェイスから独立して動作し、
- Telnet や SNMP などのリモート アクセス プロトコルをサポートするネットワーク インターフェイスです。

接続タイプを自動的に検出するには、管理インターフェイス（通常は mgmt0 とラベル付けされます）を使用します。全二重モードをサポートし、10、100、または 1000 メガビット/秒の速度で動作します。

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。

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論理的なネットワーク インターフェイスで、

- 複数の物理インターフェイスを単一のチャネルに集約し、
- 帯域幅を増やし、冗長性を強化し、
- 最大 32 のバンドルされたイーサネット リンクをサポートします。

最大 32 の物理ポート)への個別リンク(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 チャネルの構成」のセクションを参照してください。

サブインターフェイス

サブインターフェイスは、

- 親の物理またはポートチャネル インターフェイスで動作し、

- IPアドレス、ルーティングプロトコルなどの一意のレイヤ3パラメータの割り当てが可能で、
- を使用すると、1 つの物理インターフェイスを、独立して設定された複数のリモート対応インターフェイスに分割できる仮想インターフェイスです。

レイヤ3インターフェイスとして構成した親インターフェイスに仮想サブ使用作成できます。

ループバック インターフェイス

リモート対応ループバック インターフェイスは、

- 単一のエンドポイントがあり、常に動作していて、
- 送信したパケットをただちに受信し、
- は、外部デバイスに接続しなくても物理インターフェイスの動作をエミュレートします。

ループバック インターフェイスは、ハードウェアの状態に関係なくインターフェイスがアクティブになることが保証されるため、テスト、診断、または内部ルーティングの目的でよく使用されます。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

ブレークアウト インターフェイスは、

- 単一の高帯域物理ポートを複数の低速論理的なインターフェイスに分割し、
- スイッチまたはルータを複数の低速デバイスに同時に接続でき、
- ネットワーク構成の柔軟性を高めることにより、ポートの使用率を最大化する高速ネットワーク ポート機能です。

Cisco NX-OS は、モジュールレベルまたはポート単位のレベルで、1 つ以上の低帯域幅インターフェイスへの高帯域幅インターフェイスのブレークアウトをサポートします。

ポートのモジュール 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は、

- 特定の高密度ポートを複数の低帯域幅ポートに分割できます。
- ネットワーク構成の柔軟性を向上させ、
- 4x10G、4x25G、4x50G などのさまざまなポート内訳オプションをサポートしています。

interface breakout コマンドを設定して、モジュールの高帯域幅幅インターフェイスを複数の低速ポートに分割できます。

一部のモジュールは、すべてのポートを 4x10G、4x25G、4x50G、4x100G、2x50G、または 2x100G の構成に分割します。

例：モジュール レベルのブレークアウト

たとえば、モジュール レベルのブレークアウト 4X10G は、4 つの 10G インターフェイスに分割されていることを意味します。コマンドを実行すると、モジュールがリロードされ、既存のインターフェイス設定が削除されます。

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

ブレークアウトを取り消すには、 **no interface breakout module** *module_number* コマンドを使用します。これにより、ポートを元の設定に復元し、以前のブレークアウト設定を削除します。

レーン セレクタ

レーン セレクタは、コントロール パネルの機能です。

- は、押しボタンスイッチと 4 つの LED で構成されています。
- ユーザーがスイッチポートのリンクまたはアクティビティステータスを表示できるようにし、
- 互換性のあるCisco Nexus 9000 シリーズ スイッチおよびCisco Nexus 3164 および 3232 スイッチでの 1 x 40G と 4 x 10G 構成間のスイッチングをサポートします。

その他の情報

レーン セレクタは、 Cisco Nexus スイッチの前面パネルの左側にあり、「LS」というラベルが付いています。

デフォルトでは、この LED によって、1 x 40G 構成のリンク/アクティビティ ステータスが示されます。4 x 10G に構成されている場合、押しボタンを押すと、各 10G ポートのステータスの LED が切り替わります。最後に押すと、すべての LED が消灯し、ディスプレイはデフォルト モードにリセットされます。

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。押しボタンを2回目に押すと、2番目のポートのステータスが示され、以降同様です。4つのポートのそれぞれのステータスを表示するには、説明に従って押しボタンを押します。

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。

例

ポート 60 が 4 x 10G として設定されている場合、レーン セレクタを 1 回押すと、60/1/1 のリンク ステータス、60/1/2 については 2 回表示されます。

（注） レーン セレクタは、リンク/アクティビティのモニタリング用に設定されていないポートを管理しません。

ガイドライン

ポートが 10G ブレークアウト モードであり、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。

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。

Cisco Nexus スイッチのブレークアウト ポートのサポート

このマトリックスは、Cisco Nexus スイッチおよびライン カード プラットフォームでサポートされているブレークアウト モード（たとえば、4x10G、4x25G、2x50G など）に関する詳細情報を提供します。詳細については、「Cisco Nexus データ シート」を参照してください。

表 *3:* ブレークアウト モードのサポート マトリックス

スイッチ	4x10G	4x25G	2x50G	2x100G	2x200G	2 x 400G	4 X 50G	4x100G	8x100G
Nexus 9300-FX3 プラットフォーム スイッチ N9K-C93108TC-FX3 N9K-C93108TC-FX3P N9K-C93180YC-FX3 N9K-C9348GC-FX3 N9K-C9348GC-FX3P	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応
N9K-C9364C-H1	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応
N9K-C93400LD-H1	○	○	○	○	○	非対応	○	○	非対応
N9K-C9332D-H2R	○	○	○	○	○	非対応	○	○	非対応
N9K-X9736C-FX3	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応
N9K-X9636C-RX	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応

スイッチ	4x10G	4x25G	2x50G	2x100G	2x200G	2 x 400G	4 X 50G	4x100G	8x100G
N9K-X9636C-R	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応
N9K-X9636Q-R	○	非対応	非対応	非対応	非対応	非対応	非対応	非対応	非対応
N9K-X96136YC-R	非対応	非対応	非対応	非対応	非対応	非対応	非対応	非対応	非対応
N3K-C3636C-R	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応
N3K-C36180YC-R	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応
N9K-93108TC-FX3P	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応
N9K-93108TC-EX	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応
N9K-93180YC-EX	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応
N9K-93108TC-FX	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応
N9K-93180YC-FX	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応
N9K-9348GC-FXP	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応
N9K-X9736C-FX	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応
N9K-X9736Q-FX	○	非対応	非対応	非対応	非対応	非対応	非対応	非対応	非対応
N9K-X9788TC-FX	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応
N9K-X9732C-FX	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応
N9K-C9348GC-FXP	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応
N9K-C9336C-FX2	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応
N9K-C93216TC-FX2	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応
N9K-C93360YC-FX2	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応
N9K-C9364C-GX	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応
N9K-C9316D-GX	○	○	○	○	○	非対応	○	○	非対応
N9K-C93600CD-GX	○	○	○	○	○	非対応	○	○	非対応
N9K-X9716D-GX	○	○	○	○	○	非対応	○	○	非対応
N9K-C9364D-GX2A	○	○	○	○	○	非対応	○	○	非対応
N9K-C9332D-GX2B	○	○	○	○	○	非対応	○	○	非対応

スイッチ	4x10G	4x25G	2x50G	2x100G	2x200G	2 x 400G	4 X 50G	4x100G	8x100G
N9K-C9348D-GX2A	○	○	○	○	○	非対応	○	○	非対応
N9K-X9400-16W	○	○	○	○	非対応	非対応	○	非対応	非対応
N9K-X9400-8D	○	○	○	○	○	非対応	○	○	非対応
N9K-X98900CD-A	○	○	非対応	○	○	非対応	○	○	非対応
N9K-X9836DM-A	○	○	非対応	○	○	非対応	○	○	非対応
N9364E-SG2-Q	非対応	非対応	非対応	非対応	非対応	○	非対応	○	○

ブレークアウトの注意事項と制約事項

- Cisco Nexus 9516スイッチは、モジュール8ー16のブレークアウトをサポートしていません。
- Cisco NX-OS リリース 7.0(3)F2(1) 以降では、36 ポート 100 ギガビット イーサネット QSFP28 ライン カード（N9K-X9636C-R）および 36 ポート 40 ギガビット イーサネット QSFP + ライン カード（N9K-X9636Q- R）は 4x10G をサポートします。
- Cisco NX-OS リリース 9.2(1) 以降、N9K-9636C-R、N9K-X9636Q-R、および N9K-X9636C-RX ライン カードは、40G ポートの 4x10G への分割をサポートします。
- Cisco NX-OS リリース 9.2(2) 以降では、N9K-X9636C-R および N9K-X9636C-RX ライン カードは、100G ポートの 4x25G への分割をサポートします。N9K-C9636C-R は RS-FEC をサポートしていません。

  Cisco NX-OS リリース9.3(3) 以降では、N9K-X9636C-R および N9K-X9636C-RX のデフォルト FEC モードは 25Gx4 および 50Gx2 の FC-FEC です。

  N9K-X9636C-RX を N9K-X9636C-R に接続する場合は、RS-FEC がサポートされていないため、N9K-X9636C-RX で FC-FEC を設定する必要があります。

  N9K-X96136YC-R ライン カードはブレークアウトをサポートしていません。
- Cisco NX-OS リリース 9.3(3) 以降、これらのスイッチはブレークアウトをサポートします。

  Cisco Nexus 93600CD-GX スイッチおよびCisco Nexus 9500 R シリーズ スイッチは、100G ポートを 2 x 50G にブレークアウトすることをサポートしています。

  N9K-X9636C-R および N9K-X9636C-RX ライン カードを搭載した Nexus 9500 R シリーズスイッチでは、特定の光入出力（QSFP-100G-PSM4-S、QSFP-100G-AOC、QSFP-100G-CU1M、および CU3M）のみが、2x50G および 4x25G へのブレイクアウトをサポートしています。

  詳細については、『*Cisco IPICS Compatibility Matrix*』を参照してください。

- Cisco NX-OSリリース 10.4(3) 以降、Cisco N9K-X98900CD-A スイッチは、4 x 25G ポートでのブレークアウトをサポートします。

  Cisco NX-OSリリース 10.4(3) よりも前のリリースでは、ブレークアウトは 4 x 25G ポートでサポートされていません。

手動ブレークアウト構成のベストプラクティス

Cisco Nexusデバイスで手動ブレークアウトを実行する場合は **interface breakout module** *module number port port range* **map** *breakout mapping* コマンドを使用する必要があります。

- Cisco Nexus 9000 デバイスを Cisco NX-OS リリース 7.0(3)I7(2) 以降にアップグレードすると、QSA を使用して手動でブレイクアウトを設定したインターフェイスはサポートされなくなります。構成を削除し、影響を受けるインターフェイスのブレークアウト設定を手動で再設定する必要があります。

（注） Cisco NX-OS リリース 7.0(3)I7(2) では、QSA ポートの手動ブレークアウトはサポートされていません。

（注） この動作は、次のプラットフォームでは手動ブレークアウトがサポートされていません：N9K-C93128TX、N9K-9332、N9K-C9396PX、N9K-C9396TX、N9K-C9372PX、N9K-C9372TX、N9K-C9332PQ、N9K-9432PQ、N9K-9536PQ、N9K-9636PQ、N9K-X9632PC-QSFP100、N9K-X9432C-S、N3K-C3132Q-V、N3K-C3164Q、N3K-C3132C、N3K-C3232C、N3K-C3264Q、N3K-C3264C、N3K-3064Q、N3K-3016、N3K-3172：これらのプラットフォームでは手動ブレークアウトがサポートされているためです。

- 次のプラットフォームでは自動ブレークアウトが正常に実行されないため、手動ブレークアウトがサポートされています。N9K-C93128TX、N9K-9332、N9K-C9396PX、N9K-C9396TX、N9K-C9372PX、N9K-C9372TX、N9K-C9332PQ、N9K-C93120TX、N9K-9432PQ、N9K-9536PQ、N9K-9636PQ、N9K-X9632PC-QSFP100、N9K-X9432C-S、N3K-C3132Q-V、N3K-C3164Q、N3K-C3132C、N3K-C3232C、N3K-C3264Q、N3K-C3264C、N3K-3064Q、N3K-3016、N3K-3172。

ブレークアウト ポートの前方誤り訂正（FEC）設定

FEC は、1 m および 2 m のパッシブ銅ケーブルを除くすべてのケーブルタイプで必要です。Cisco スイッチはデフォルトでFC -FEC CL74 を使用します。RS-FEC Consortium 1.6、RS-FEC IEEE、および他の FEC アルゴリズムを設定できます。

（注） Auto-FEC は Cisco NX-OS Release 7.0(3)I7(x) ではサポートされていません。

ブレークアウト ポートを構成する場合は、リンクがアップ状態になるように FEC が一致していることを確認します。

25G イーサネットで使用される 2 つのプライマリ FEC アルゴリズムがあります。

- • **FC-FEC** （「FireCode」、「BASE-R」、または「Clause 74」とも呼ばれる）は、バーストエラー修正に最適化された低遅延エラー保護（100 ナノ秒未満）を提供します。3 メートルおよび 5 メートルのパッシブ銅線ケーブル、および最大 10 メートルのアクティブ光 25G ケーブルで使用されます。この FEC タイプは、すべての 100G インターフェイスでも使用されます。

  • **RS-FEC** （「Reed Somon」、「Clause 91」、「Clause 108」とも呼ばれる）は、より優れたエラー保護を提供します。最大 100 メートルの距離をサポートする、Cisco SFP-25G- SR -S などの 25G マルチモード光ファイバ（MMF）トランシーバに必要です。RS-FEC は、10 メートルを超えるアクティブ光ケーブルにも必要な場合があります。

すべての 25G デバイスは、デフォルトで FC -FEC をサポートします。Cisco Nexus 9300-FX シリーズは RS-FEC をサポートしています。

Cisco NX-OS リリース 7.0(3)I7(3) 以降では、 **rs-cons16** および **rs-ieee** など IEEE 標準に従って、FEC を設定するための 2 つの追加オプションが表示されます。

高速イーサネットインターフェイスで RS-FEC エラー訂正を実装するには、 Cisco Nexus 9000 スイッチで **fec rs-ieee** コマンドを使用して RS FEC IEEE （25G）を有効にします。

```
switch# (config-if)# fec ?
auto FEC auto
fc-fec CL74(25/50G)off Turn FEC off
rs-cons16 RS FEC Consortium 1.6 (25G)
rs-fec CL91(100G) or Consortium 1.5 (25/50G)
rs-ieee RS FEC IEEE (25G)
```

- Cisco NX-OS リリース 7.0(3)I7(7) 以降では、FECインターフェイス情報の管理および動作ステータスを **show interface fec** コマンドで表示できます。

  例：

```
switch# show interface fec
-------------------------------------------------------------------------------------------------
Name  Ifindex Admin-fec  Oper-fec    Status  Speed  Type
-------------------------------------------------------------------------------------------------
Eth1/1   0x1a000000 auto  auto connected     10G  SFP-H10GB-AOC2M
Eth1/2   0x1a000200      Rs-fec    notconneced    auto QSFP-100G-AOC3M
Eth1/3/1 0x38014000 auto  auto disabled auto QSFP-H40G-AOC3M
Eth1/3/2 0x38015000 auto  auto disabled auto QSFP-H40G-AOC3M
Eth1/3/3 0x38016000 auto  auto disabled auto QSFP-H40G-AOC3M
Eth1/3/4 0x38017000 auto  auto disabled auto QSFP-H40G-AOC3M
```

Cisco Nexus C9364C-H1 スイッチのブレークアウトモード

Cisco NX-OS リリース 10.2（2）F 以降、Cisco Nexus C9364C-H1 スイッチはブレークアウトモードをサポートします。

ブレイクアウトモードは、Cisco Nexus C9364C-H1 スイッチにおける

- ポート構成設定であり、単一のポートを複数の論理インターフェイス（例：2x50G、4x25G、または4x10G）に分割することを可能にします。
- このモードは、各フロントポートクワッドグループ内の最初のポート（例：ポート1、5、9、...）でのみ利用可能です。

（注） インターフェイスのブレークアウト中は、隣接する 3 つの前面ポートが削除され、インターフェイス検証または構成コマンドでは表示されません。

Cisco Nexus 9000 C93180LC-EXスイッチ：動作モードとブレークアウト モード

動作モードとブレークアウトモードは、スイッチ構成プロファイルです。これらのプロファイルを使用して、ポートをグループ化および設定したり、高速物理ポートを複数の低速論理的なポートに分割したり、各モードで使用できる機器とケーブルのタイプを特定したりできます。

Cisco Nexus 9000 C93180LC-EX スイッチ

動作モードは、次のスイッチ構成プロファイルで、

- 使用可能な帯域幅とポートのグループを決定し、
- さまざまなブレークアウト機能をイネーブルにし、
- モードを切り替えるために個別の設定手順を使用する必要があります。

7.0(3)I7(1) 以降では、Cisco Nexus 9000 C93180LC-EX スイッチは 3 つの異なる動作モードを提供します。

- **モード 1**：**28 x 40G + 4 x 40G/100G（デフォルト設定）**

  これは、ハードウェア プロファイル ポートモード 4x100g＋28x40g ポートです。次の ACL をサポートします。

  - 10x4 ブレークアウトは、1ー27 の上部ポート（ポート 1、3、5、7 ... 27）でサポートされます。

    上部ポートのいずれかが故障すると、対応する下部のポートは動作しなくなります。

    たとえば、ポート 1 が故障すると、ポート 2 が動作しなくなります。

  - 1 ギガビットおよび 10 ギガビット QSA は、ポート 29、30、31、および 32 でサポートされます。ただし、上部および下部の前面パネル ポートの QSA は同じ速度である必要があります。

- ポート 29、30、31、および 32 は、10x4、25x4、および 50x2 のブレークアウトをサポートします。

- **モード 2**：**24 x 40G + 6 x 40G/100G**

  このハードウェア プロファイルのポート モードは、6 x 100G + 24 x 40G ポートです。次の ACL をサポートします。

  - 10x4 ブレークアウトは、1ー23 の上部ポート（ポート 1、3、5、7 ... 23）でサポートされます。上部ポートのいずれかが故障すると、対応する下部のポートは動作しなくなります。
  - ポート 25、27、29、30、31、および 32 は、10x4、25x4、および 50x2 のブレークアウトをサポートします。
  - 1 ギガビットおよび 10 ギガビット QSA は、ポート 29、30、31、および 32 でサポートされます。ただし、上部および下部の前面パネル ポートの QSA は同じ速度である必要があります。

- **モード 3**：**18 x 40G/100G**

  このハードウェアプロファイルは、そのポートの 18 x 100G をポート モードにします。次の ACL をサポートします。

  - 10x4、25x4、および 50x2 のブレークアウトは、1ー27 のトップ ポート（ポート 1、3、5、7 ... 27）およびポート 29、30、31、32 でサポートされます。
  - 1 ギガビットおよび 10 ギガビット QSA は、18 ポートすべてでサポートされます。

モード 3 から別のモードに変更するには、 **copy running-config startup-config** コマンドの後に **reload** コマンドを入力して有効にします。ただし、モード 1 と 2 の間を移動するには、 **copy running-config startup-config** コマンドを入力するだけです。

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。

```
switch(config-if-range)# show running-config | grep portmode

hardware profile portmode 4x100G+28x40G
```

ブレークアウト モード

Cisco Nexus C93180LC-EX スイッチには、3 つのブレークアウト モードがあります。

- 40G ー 4x10G ブレークアウト ポートのサポート
  - このモードでは、40G ポートから 4x10G ポートへのブレークアウトをイネーブルにします。

- このモードを構成するには、 **interface breakout module 1 port** *x* **map 10g-4x** コマンドを使用します。

- 100G ー 4x25G ブレークアウト ポートのサポート
  - このモードは、100G ポートから 4x25G ポートへのブレークアウトをイネーブルにします。
  - このモードを構成するには、 **interface breakout module 1 port** *x* **map 25g-4x** コマンドを使用します。

- 100G から 2x50G へのブレークアウト ポートのサポート
  - このモードは、100G ポートから 2x50G ポートへのブレークアウトをイネーブルにします。
  - このモードを構成するには、 **interface breakout module 1 port** *x* **map 50g-2x** コマンドを使用します。

Cisco Nexus 9000 C9364C-GX スイッチのブレークアウト考慮事項

以下は、Cisco Nexus N9K-C9364C-GX スイッチのブレークアウトの考慮事項です。

- 奇数番号のポートでのみ、ブレークアウトモード（1 ー 64、2 x 50G、4 x 25G、および 4 x 10G）を設定します。

（注） 偶数番号のポートでブレークアウトを試行しないでください。

- 奇数番号のポートをブレークアウトすると、そのクワッド内の偶数番号のポートは自動的に削除され、もう一方の奇数ポートは同じブレークアウト速度に設定されます。

  たとえば、ポート 1 またはポート 3 が 2 x 50、4 x 25G、または 4 x 10G に分割されている場合、そのクワッドのもう一方の奇数ポートは自動的に同じ速度に分割され、そのクワッドのポート 2 および 4 は削除されます。上記のブレークアウト設定が削除されると、そのクワッドのすべてのポートがデフォルトに戻ります。

- クワッドをデフォルトのポート ステータスに戻すには、クワッドの両方の奇数ポートからブレークアウト設定を削除します。

- QSFP28（100G）トランシーバは、4 x 25G ブレークアウト機能をサポートします。Cisco NX-OS Release 9.3(5) 以降では、2 x 50G ブレークアウト機能がサポートされます。

- QSFP +（40G）トランシーバは、4 x 10G ブレークアウト機能をサポートします。

- interface **breakout module 1 port x map 50g-2x**コマンドを使用して、すべての奇数番号ポートで、100G ポートから 2 X 50G 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** コマンドを活用、40G ポートの 4 x 10G ポートへのブレークアウトブレークアウトを有効にします。

Cisco Nexus 9000 C93600CD-GX スイッチのブレークアウト機能

Cisco Nexus N9K-C93600CD-GX ブレークアウトの考慮事項を使用してください。

- Cisco Nexus N9K-C93600CD-GX では、1ー24 の 4 つのポートはすべてクワッドと呼ばれます。

（注） ブレイクアウト構成と速度は、クワッド内で同じである必要があります。

クワッドアウト機能は、クワッド内の速度またはブレイクアウト設定の不一致がある場合、期待どおりに機能しないことがあります。

6 個のクワッドは、ポート 1ー4、5ー8、9ー12、13ー16、17ー20、および 21ー24 です。

- Cisco NX-OS リリース 9.3(5) 以降では、2 つの 50G ブレークアウト機能がポート 1ー36 でサポートされます。
- 4x25G および 4x10G ブレークアウト機能は、ポート 1ー24 の間の奇数ポートでのみサポートされます。クワッド内の偶数ポートが削除されます（4 ポート）。
- クワッド内の奇数番目のポートが分離されると、そのクワッド内の偶数番目のポートは削除され、クワッド内の他の奇数番目のポートは自動的に同じ速度で分離されます。

  たとえば、ポート 1 が 4x25G または 4x10G に分割されている場合、そのクワッドのもう一方のポートは自動的に同じ速度に分割されます。そのクワッドのポート 2 と 4 が削除されます。このブレークアウト構成が削除されると、そのクワッド内のすべてのポートがデフォルト設定に戻ります。
- 2x50G ブレークアウトは、1ー24 のすべてのポートでサポートされます。クワッド内の 1 つのポートが 2x50G に分割されると、クワッド内のすべてのポートが自動的に同じ速度に分割されます。

  たとえば、ポート 2 が 2x50G に分割される場合、ポート 1、3、および 4 は自動的に 2x50G に分割されます。

（注） ポート 1ー24 の 50G 速度の両方のレーンで RS-FEC のみがサポートされます。

- Cisco NX-OS リリース 9.3(3) 以降、ポート 25ー28 は 4x10G、4x25G、および 2x50G のブレークアウト機能をサポートします。これらのブレークアウト機能は、ポート ペアでサポートされます。 例：25～26、27～28。

（注） リンクをアップするには、2x50G のレーン 2 を RS-FEC で設定する必要があります。

- Cisco NX-OS リリース 9.3(3) 以降では、ポート 29ー36 の次のブレークアウト設定を検討します。
  - QSFP-DD-400G-DR4 トランシーバは、4 x 100G ブレークアウト機能のみをサポートします。
  - QSFP-DD-400G-FR4 および QSFP-DD-400G-LR8 トランシーバは、ブレークアウト機能をサポートしていません。
  - QSFP28（100G）トランシーバは、2 x 50G および 4 x 25G ブレークアウト機能をサポートします。
  - QSFP +（40G）トランシーバは、4 x 10G ブレークアウト機能をサポートします。

Cisco Nexus C9316D-G スイッチのブレークアウトの考慮事項：

Cisco Nexus N9K-C9316D-GX スイッチのポート 1 ～ 16 には、これらのブレークアウトの考慮事項を活用します。

- QSFP-DD-400G-DR4 トランシーバは、4 x 100G および 4x10G ブレークアウト機能のみをサポートします。

（注） QSFP-DD-400G-FR4 および QSFP-DD-400G-LR8 トランシーバは、ブレークアウト機能をサポートしていません。

- QSFP28（100G）トランシーバは、2 x 50G、4 x 25G、および 4x10G ブレークアウト機能をサポートします。

Cisco Nexus 93C64E-SG2-Q スイッチ のブレークアウトの考慮事項

単一の高速ポートを複数の低速ポートに分割して回数変更可能接続を可能にするスイッチポート機能であるブレークアウトアウト機能を使用できます。

, ,以降Cisco NX-OS リリース 10.2（2）F、Cisco Nexus 93C64E-SG2-Q スイッチ は

- 2x400G および 8x100G のブレークアウト構成、
- サポートされる光学部品との互換性、および
- 柔軟なポート構成を提供します。

サポートされているブレークアウトモードは次のとおりです。

- **2x400Gブレークアウト**： 単一のポートを 2 つの 400G ポートに分割します。

- **8x100Gブレークアウト**： 単一のポートを 8 つの 100G ポートに分割します。

オプティクス

Cisco NX-OS リリース 10.2（2）F以降、 Cisco Nexus 93C64E-SG2-Q スイッチ はこれらのオプティクスをサポートします。

- QDD-8X100G-FR
- QDD-8x100G-LR
- QDD-2X400G-FR4
- QDD-2x400G-LR4

Cisco Nexus 93C64E-SG2-Q スイッチ は、64 個の QSFP-DD800 ポートもサポートしています。これにより、高密度および高速の接続が可能になります。

仮想デバイス コンテキスト

リモート対応仮想化コンテキスト（ VDC ）は、

- オペレーティングシステムとハードウェアリソースをセグメント化し、
- 物理スイッチ内の独立した論理的なスイッチをエミュレートし、
- を使用すると、コンテキストごとに個別の設定、管理、管理を実行するためのネットワーク仮想化テクノロジーです。

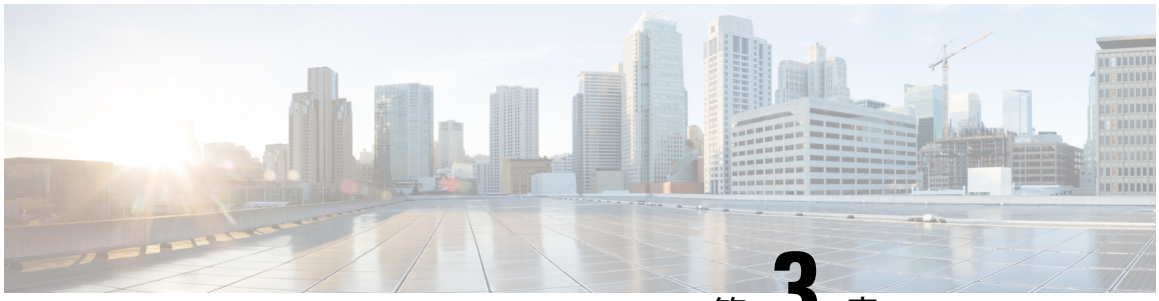
Cisco Nexus 9000 シリーズ スイッチは、複数の VDC をサポートしていません。すべてのスイッチ リソースはデフォルト VDC で管理されます。

インターフェイスの高可用性

インターフェイスの高可用性とは、

- スーパーバイザのスイッチオーバー中にインターフェイスの動作を継続できるようにし、
- ステートフルおよびステートレスの両方の再起動メカニズムをサポートするネットワーク機能です。

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

基本インターフェイス パラメータについて

インターフェイスの説明

インターフェイスの説明は、イーサネットまたは

- 管理インターフェースに識別可能な名前を割り当てる構成属性であり、
- 複数のインターフェースがリストされた状態でのインターフェースの迅速な識別を可能にし、
- 個々のインターフェースの役割や目的を区別するための固有のラベル付けを許可します。

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 チャネルの説明の構成」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、「説明の構成」の項を参照してください。

ビーコン モード

ビーコン モードは、

- ポートのリンクステート LED をアクティブにして ID に対して緑色に点滅させ、
- デフォルトではディセーブルになっていて、
- インターフェイスでビーコン パラメータを設定してイネーブルになるポート識別機能です。

ビーコンモードを使用すると、設置またはトラブルシューティング中にデバイスの物理ポートを簡単に見つけることができます。アクティブにすると、対応するポートの LED が緑色に点滅し、正確なインターフェイスを示します。複雑な環境でのケーブル トレースやポート検証などのタスクを簡素化します。

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構成については、「ビーコンモードの構成」の項を参照してください。

Error-disabled ステート

error-disabled ステートとは、ポートが管理上有効化されている

- にもかかわらず、検出された問題により実行時に無効化される動作状態を指します。
- これは自動保護機構（UDLDによる一方向リンクの検出や過剰なポートフラッピングなど）の結果として発生し、
- 正常動作を復旧するには手動介入または特定の回復設定が必要となります。

その他の情報

ポートが管理的に有効であるが（**no shutdown** コマンドを使用）、プロセスによって実行時に無効になる場合、そのポートは error-disabled（err-disabled）ステートです。

インターフェイスが errdisable ステートになった場合は、 **show interface status err-disabled** 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。

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。

（注） 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。

error-disabled の自動回復

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。

The **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。

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 回復を有効にしない場合、そのインターフェイスは **shutdown** および **no shutdown** コマンドを開始するまでerror-disabled ステートです。

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。

ガイドライン

- Embedded Event Manager（EEM）ポリシーは、障害のあるケーブルと光ファイバを検出するために、連続 420 秒（デフォルト）で 30 回のフラップの後にポートを error-disabled にします。

  Cisco NX-OS リリース 10.5(2)F 以降、より多くの起動および停止時間を必要とするシステムでは、420 秒間に 25 回のフラップが発生すると、portts は error-disabled になります。これは、これらのプラットフォームに適用されます。

  - Cisco Nexus 9800 シリーズ スイッチ
  - N9K-C9332D-GX2B
  - N9K-C9364D-GX2A
  - N9K-C9348D-GX2A
  - N9K-C9408

MDIX パラメータ

メディア依存インターフェイスクロスオーバー（MDIX）パラメータは、インターフェイス構成の設定です。

- ネットワークデバイス間のクロスオーバー接続の自動検出を有効または無効にし、
- 銅線のネットワーク インターフェイスにのみ適用され、
- デフォルトでイネーブル ステータスに設定されるため、手動での配線を考慮することなく互換性が確保されます。

この **no mdix auto** コマンドは、、N9K-C93108TC-FX、N9K-X9788TC-FX、および N9K-C9348GC-FXP デバイスでのみサポートされます。

MDIX パラメータの設定については、「MDIX パラメータの設定」のセクションを参照してください。

インターフェイス ステータス エラー ポリシー

インターフェイス ステータス エラー ポリシーは、

- ポリシーのプッシュが失敗した場合にインターフェイスがアクティブ化されないようにし、
- エラー状態情報を保存して中断の繰り返しを回避し、
- ポリシーとハードウェア構成の一貫性を確保するネットワークポリシーの適用メカニズムです。

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。このデータベースでは、各ポリシーがコマンド ライン インターフェイスを通じて定義されます。

インターフェイスにポリシーを設定すると、そのポリシーがハードウェアポリシーと一致することが保証されます。ハードウェアポリシーと一致しないポリシーがプッシュされると、インターフェイスはerror-disabledポリシー状態に設定されます。エラー状態が維持され、今後ポートが起動しないように情報が保存されるため、ポリシー違反の繰り返しやシステムの中断が回避されます。

エラーをクリアしてプログラミングを再試行するには、 **no shutdown** コマンドを使用します。

インターフェイス MTU サイズ

最大伝送ユニット（MTU）サイズは、次のネットワーク インターフェイスのパラメータです。

- それはイーサネット ポートが処理できる最大のフレーム サイズを決定し、
- 設定されたサイズを超えるフレームのドロップを強制します。

追加情報

デフォルトでは、それぞれのインターフェイスのMTUは1500バイトで、イーサネット フレームに関する IEEE 802.3 標準です。

ジャンボ フレームと呼ばれるMTUサイズを大きくすると、処理効率が向上します。ジャンボ フレームは通常、最大 9216 バイトです。

Cisco NX-OSプラットフォームでは、インターフェイスごとまたはプロトコル スタックのさまざまなレベルで MTU を調整できます。

CloudScale スイッチは、ハードウェアでの追加のカプセル化に対応するために、構成された MTU を超える 166 バイトを許可します（デフォルト）。

（注） 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。

インターフェイスタイプ別の MTU 構成

MTU はインターフェイスごとに設定されます。インターフェイスをレイヤ 2 またはレイヤ 3 インターフェイスに変更できます。

- **レイヤ 2 インターフェイス**

  MTU サイズは、システムのデフォルト MTU 値またはシステム ジャンボ MTU 値の 2 つの値のいずれかで設定できます。

  システム デフォルトの MTU サイズは 1500 バイトです。各レイヤ 2 インターフェイスは、デフォルトでこの値を使用します。デフォルトのシステム ジャンボ MTU 値（9216 バイト）を使用してインターフェイスを設定できます。

  1500 ～ 9216 のMTU値を許可するには、最初にシステム ジャンボMTUを設定します。次に、それに応じてインターフェイス MTU を調整します。

（注） システム ジャンボ MTU サイズを変更できます。値が変更されると、システム ジャンボ MTU 値を使用するレイヤ 2 インターフェイスは新しいシステム ジャンボ MTU 値に自動的に変更します。

- **レイヤ 3 インターフェイス**

  レイヤ 3 インターフェイスには、レイヤ 3 物理インターフェイス (スイッチポートなしで設定)、スイッチ仮想インターフェイス（SVI）、およびサブインターフェイスが含まれます。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。

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。

ガイドライン

- Cisco Nexus 9300-FX2 および 9300-GX デバイスで、MTU が 9216 未満の入力インターフェイスを設定すると、FTE は入力エラーをキャプチャせず、イベントも表示しません。入力 MTU を9216 に設定すると、FTE はすべてのイベントを表示します。

帯域幅

帯域幅は、

- ネットワーク接続の最大データ転送速度を測定し、
- デバイス間のリンクの容量を定義し、
- は、イーサネットポートの物理層に固定されたまま（たとえば、1,000,000 Kb）になるネットワーク パフォーマンス メトリックスです。

イーサネットポートでは、物理帯域幅は常に固定です（1,000,000 Kb など）。レイヤ 3 プロトコルでは、内部メトリック計算にのみ設定可能な帯域幅の値が使用されます。このパラメータ

を変更しても、ルーティングプロトコルの動作にのみ影響があり、接続のキャパシティは物理的に変更されません。

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。

帯域幅パラメータの構成については、「帯域幅の構成」の項を参照してください。

スループット遅延値

スループット遅延は、インターフェイス構成パラメータで、

- レイヤ 3 プロトコルが動作を決定するために使用する値を提供し、
- インターフェイスの実際のスループット遅延に影響を与えず、
- 10 マイクロ秒単位で設定されます。

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。

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構成については、「スループット遅延の構成」セクションを参照してください。

管理ステータス パラメータ

管理ステータス パラメータは、次のようなネットワーク インターフェイスの設定です。

- インターフェイスが管理上アップまたはダウン状態であるかを示します。
- インターフェイスがデータを送信する機能を有効または無効にします。

管理ステータスがダウンに設定されると、インターフェイスはディセーブルになり、データを送信できません。up に設定すると、インターフェイスはイネーブルになります。

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。

単方向リンク検出

UDLD

単一方向リンク検出（UDLD）は、

- 接続されたデバイス間の光ファイバおよび銅線イーサネットケーブルの物理構成を監視し、
- はこれらの接続上の単方向リンクの存在を検出し、
- 影響を受ける LAN ポートを自動的にシャットダウンして、ネットワークの問題を防止するためのネットワーク プロトコルです。

UDLDは、単一方向リンクと呼ばれる接続で一方向にのみトラフィックが通過するときに発生する問題を特定して軽減するように設計されたシスコ独自プロトコルです。このような状態は、ネットワークループを作成し、データ損失やプロトコルの誤動作を引き起こす可能性があります。

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。フレームが特定の時間枠内にエコーバックされても確認応答（エコー）がない場合、リンクは単方向としてフラグが付けられます。LAN ポートがシャットダウンします。

単一方向リンクが識別されディセーブルされるようにするには、リンクの両端のデバイスで UDLD プロトコル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、グローバル単位または指定されたインターフェイスに設定できます。

追加情報

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。

単一方向リンクは、ローカル デバイスから送信されたトラフィックがネイバーで受信されるが、ネイバーからのトラフィックがローカル デバイスで受信されない場合に発生します。

ペアのファイバ 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と、そのリンクのアップ状態は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。両方のファイバーがレイヤー1で正常に動作している場合、UDLDはそれらが正しく接続されているかどうか、およびトラフィックが正しいネイバー間で双方向に流れているかどうかを確認します。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。

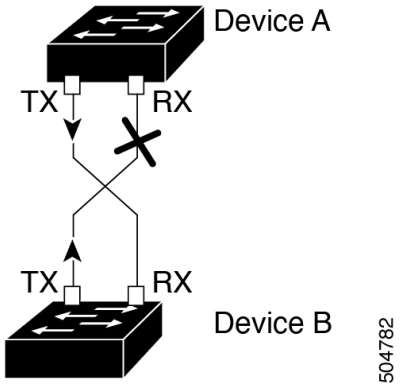
（注） UDLD は、銅線の LAN ポート上では、このタイプのメディアでの不要な制御トラフィックの送信を避けるために、ローカルでデフォルトでディセーブルになっています。

例

デバイスAとデバイスBは光ファイバケーブルで接続されています。ケーブルの切断により、デバイス B はデバイス A からトラフィックを受信できますが、デバイス A はデバイス B から

トラフィックを受信できません。UDLDはこの単方向の状態を検出し、影響を受けるポートをディセーブルにすることで、ネットワークの問題を防ぎます。

図 *1:* 単方向リンク



類推

UDLD は、参加者双方が相手の声を定期的に確認できる、双方向の会話に似ています。1 人の参加者が応答を停止すると、誤解を防ぐためにカンバセーションが一時停止します。同様に、双方向通信が失敗した場合に UDLD がポートをディセーブルにします。

UDLD のデフォルト構成の状態

UDLD 構成の状態は、システム定義の設定で、

- UDLD がグローバルに動作するか、または特定のポートで動作するかを指定し、
- UDLD が標準規格モードとアグレッシブモードのどちらで動作しているかを決定し、
- UDLDプロトコル動作のメッセージ間隔を制御します。

UDLD は、ポート メディア タイプに応じて異なるデフォルトを適用します。

- イーサネット光ファイバ ポート上では、UDLD はデフォルトでイネーブルに設定されています。
- イーサネットツイストペア（銅線）ポートでは、UDLD はデフォルトでディセーブルになっています。UDLD を使用する場合は、UDLD をイネーブルにする必要があります。

UDLD のデフォルト構成の状態

次の表に、UDLD のデフォルト構成を示します。

表 *4: UDLD* のデフォルト構成の状態

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

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

UDLD モードはリンクをモニターし、単方向リンク障害を検出して対応する方法を決定します。

UDLD は、通常モードまたはアグレッシブ モードで使用できます。

- **通常モード**：UDLD 通常モードでは、ピア ポート間でパケットを交換してリンク ヘルスを検出します。
- **アグレッシブモード**：UDLDアグレッシブモードは、応答しないネイバーとのコンタクトの再確立を試行します。8 回の再試行後、リンクが応答しないままの場合、UDLD は、検出されない一方向の障害がネットワークの問題を引き起こすのを防ぐために、影響を受けるポートを積極的にディセーブルにします。

その他の情報

スイッチがリンク エラー（空のエコー パケット、単方向の障害、TX または RX ループ、ネイバーの不一致など）を検出すると、その状態にフラグを立てますが、ポートをディセーブルにはしない場合があります。

UDLDはデフォルトでは通常モードで動作し、アグレッシブモードはユーザがイネーブルにしない限りディセーブルになります。

UDLDアグレッシブモードをグローバルにイネーブルにすると、このモードはすべての光ファイバポートでアクティブになります。特定の個々の光ファイバポートでアクティブにすることもできます。

（注） これは、個々の銅線インターフェイスで設定する必要があります。

UDLDアグレッシブモードは、両方がサポートしているネットワーク デバイス間だけで活用します。このモードは、ポイントツーポイント リンクでのみ活用します。

このような場合、UDLDアグレッシブモードでポートをディセーブルにして、トラフィック損失を防止します。

- 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

ガイドライン

- ラインカードをISSU中にアップグレードする場合、UDLDアグレッシブモードがイネーブルになっているレイヤ2ポートチャネルに一部のポートが含まれていると、リモートポートをシャットダウンすると、UDLD によってローカル ポートが err-disabled ステートになります。これは予期されている動作です。

  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

ポート チャネルは、複数の物理インターフェイスを

- 組み合わせて総帯域幅を増やし、少なくとも 1 つの
- アクティブである限り動作し続けることで冗長性を提供し、参加している物理インターフェイス間で
- トラフィックのバランスをとってネットワーク パフォーマンスを最適化する論理インターフェイスです。

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。ポートチャネルは、チャネル内の少なくとも1つの物理インターフェースがアクティブである限り動作を継続します。

追加情報

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。

ポート チャネルに加えられた設定の変更は、そのチャネル内の各メンバー インターフェイスに自動的に適用されます。

ポート チャネルについては、「ポート チャネルの構成」の章を参照してください。

ポート プロファイル

Cisco Nexus 9300 シリーズ スイッチの場合 、多くのインターフェイス コマンドを含むポート プロファイルを作成して、インターフェイスの範囲にそのポート プロファイルを適用できま

す。ポートプロファイルは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 チャネルを選択した場合、ポート プロファイルはデフォルトモードになります。デフォルトモードはレイヤ3です。ポートプロファイルをレイヤ 2 モードに変更するには、**switchport** コマンドを入力します。

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

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

- 競合が発生した場合は、インターフェイス モードで入力したコマンドがポート プロファイルのコマンドに優先します。しかし、ポート プロファイルはそのコマンドをポート プロファイルに保持します。
- ポートプロファイルのコマンドに対してデフォルトのコマンドを明示的に優先させない限り、ポートプロファイルのコマンドがインターフェイスのデフォルトの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。
- Cisco Nexus C9232E-B1 スイッチでは、ポートはデフォルトで 2x400G プロファイルになります。他のブレークアウト モードに変更するには、 **no interface breakout module 1 port <port#> map 400g-2x** "を構成する必要があります。そして、**interface breakout module 1 port <port#> map <map name>**を構成します。

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 とその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。

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

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

ポートプロファイルをイネーブル化、継承、または変更しようとすると、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、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

Cisco QSFP+ to SFP+アダプタ モジュール（QSA）は、次のようなネットワーク インターフェイスのアクセサリです。

- 40G QSFP+ アップリンク ポートで 10G SFP+トランシーバを使用でき、
- 指定した速度グループ内のすべてのポートが同じ速度（10G または 40G）で動作する必要があります。

Cisco QSFP+ to SFP+アダプタ（QSA）モジュールは、特定の Cisco Nexus 9300 デバイスに属する Cisco Nexus M6PQ および M12PQアップリンク モジュール内の 40G アップリンク ポートで 10G の動作を可能にします。

QSA/QSFP モジュールを使用するには、M6PQ または M12PQ アップリンク モジュール内の連続する 6 つのポートが同じ速度 (10G または 40G) で動作する必要があります。

サポートされるプラットフォームとポート グループ

これらのCisco Nexusデバイスおよびポート グループは Cisco QSFP+ to SFP+アダプタ モジュールをサポートしています。

- Cisco Nexus 9396PX：2/1 ～ 6（最初のグループ）、2/7 ～ 12（2 番目のグループ）
- Cisco Nexus 93128PX/TX: 2/1 ～ 6（最初のグループ）、2/7 ～ 8（第 2 グループ）
- Cisco Nexus 937xPX/TX：1/49 ～ 54（グループのみ）
- Cisco Nexus 93120TX：1/97 ～ 102（グループのみ）
- Cisco Nexus 9332PQ：1/27 ～ 32（グループのみ）

QSA モジュールのポート速度の構成

speed-group 10000 コマンドを使用してポート速度グループの最初のポートを設定して、グループ内のすべてのポートを 10G に設定します。デフォルトのポート速度は 40G です。

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

- Cisco NX-OS リリース 7.0(3)I7(5) を実行している Cisco Nexus 9300 シリーズ スイッチでは、アップリンク モジュールを削除しないでください。アップリンク モジュールのポートは、アップリンク用にのみ使用してください。

- Cisco NX-OS リリース 9.2(2) 以降、CWDM4 は次のスイッチおよびライン カードでサポートされます。
  - 36 ポート 100 ギガビット イーサネット QSFP28 ライン カード（N9K-X9636C-R）
  - 36 ポート 40 ギガビット イーサネット QSFP+ ライン カード（N9K-X9636Q-R）
  - 36 ポート 100 ギガビット QSFP28 ラインカード（N9K-X9636C-RX）
  - 52 ポート 100 ギガビット QSFP28 ラインカード（N9K-X96136YC-R）

速度を構成すると、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。スイッチは互換性のないモジュールをディセーブルにし、「check speed-group」config というメッセージが表示されます。

（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 Nexus 9200 および 9300-EX シリーズ スイッチおよび Cisco Nexus 3232C および 3264Q シリーズ スイッチでは、QSFP-to-SFP アダプタを使用できます。

Cisco SFP+ アダプタ モジュール

Cisco SFP+ アダプタ モジュールは、

- SFP+ 光ファイバを大容量のスイッチポートで使用するように適応させることで、高速接続が可能になるネットワーク インターフェイス デバイスです。
- これは、手動または自動速度設定による複数のイーサネット速度（10Gや25Gなど）をサポートします。

interface breakout module コマンドを使用すると、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できます。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。

Cisco NX-OS リリース 9.2(3) 以降、10/25 LR は 、N9K-X97160YC-EX、N9K-C93180YC-FX、N9K-C93240YC-FX2、および N3K-C34180YC スイッチでサポートされています。

このデュアル スピード光トランシーバはデフォルトで 25G で動作し、他の 25G LR トランシーバと相互運用します。自動速度検知はサポートされていないため、このデバイスを 10G トランシーバーで使用するには、手動で 10G 速度に設定してください。

CVR-2QSFP28-8SFP アダプタは、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します。

Cisco SFP-10G-T-X モジュール

Cisco SFP-10G-TXモジュールは、ホットスワップ可能な10ギガビットイーサネットトランシーバで、

- 標準規格のカテゴリ 6a またはカテゴリ 7 の銅線ケーブルで 10GBASE-T接続を実現し、
- インターフェイスの柔軟性を高めるために RJ-45 コネクタをサポートし、
- データセンターおよび企業アプリケーションで最大 30 メートルの到達距離を可能にします。

Cisco NX-OS リリース 9.3(5) 以降、10G BASE-T SFP+（RJ-45）は N9K-C93240YC-FX2、、N9K-C93180YC-FX、および N9K-C93360YC-FX2 デバイスでサポートされます。

デフォルトでは、Cisco SFP-10G-TX モジュールは 10G の速度で動作します。

SFP-10G-TX モジュールを使用する場合、すべての隣接ポートが空であるか、パッシブ銅線リンクを使用している必要があります。

show interface および **show interface capability** コマンドは、特定のポートでサポートされている速度を表示します。

SFP-10G-TXトランシーバを使用している場合、特定のポートでサポートされている速度として100 Mbpsと表示されることがあります。GLC- TEトランシーバの場合、サポートされている最低速度は 1 Gbps です。

管理状態が「Up」のときにメディアタイプ10G-TXで設定されたインターフェイスは、サポートされていないメディアタイプで errdisable のままになります。この状態を解消するには、インターフェイスで次のコマンドを使用します。

- **shutdown**
- **no shutdown**

次の表は、さまざまなCisco Nexusスイッチのデフォルトのポートマッピングを示しています。

表 *5:* デフォルトのポート マッピング

デバイス名	ポート マップ
Cisco Nexus 、N9K-C93180YC-FX、N9K-C93180YC-FX3 および N9K-C93180YC-FX3S	PI/PE：1、4-5、8-9、12-13、16、37、40-41、44-45、48
Cisco Nexus N9K-C93240YC-FX2	W/PI Fan/PS：2、6、8、12、14、18、20、24、26、30 32、36、38、42、44、48 W/PE Fan/PS：6、12、18、24、30、36、42、48

デバイス名	ポート マップ
Cisco Nexus N9K-C93360YC-FX2	PI/PE 1、4-5、8、41、44-45、48-49、52-53、56-57、 60-61、64-65、68-69、72-73、76-77、80-81、84-85、 88-89、92-93、96

Cisco SFP-10G-OLT20-X モジュール

Cisco SFP-10G-OLT20-X モジュールは、ホットスワップ可能な光トランシーバであり、Cisco スイッチの標準規格 SFP+ ポートに適合します。最大 20 km までの 10 ギガビットイーサネット接続をサポートしています。このモジュールは、Cisco および業界の OLT 仕様に準拠しています。

PON マネージャを活用、モジュールのモニタ、設定、管理を行います。

Cisco NX-OS リリース 10.6(1)F以降、 Cisco Nexus 9000 シリーズ スイッチはSFP-10G-OLT20-X モジュールをサポートします。

詳細については、『Transceiver Module Group (TMG) Compatibility Matrix』を参照してください。

例： SFP モジュールの詳細の表示

SFP モジュールの詳細を表示するには、 **show interface transceiver details** コマンドを使用します。

```
switch# show interface eth1/33 transceiver details
            Ethernet1/33
            transceiver is present
            type is SFP-10G-OLT20
            name is CISCO-TIBIT
            part number is SFP-10G-OLT20-X
            revision is 001
            serial number is OLT-E09B2736AAB6
            nominal bitrate is 10300 MBit/sec
            Link length supported for 9/125um fiber is 20 km
            cisco id is 3
            cisco extended id number is 4

            SFP Detail Diagnostics Information (internal calibration)
           ----------------------------------------------------------------------------

            Current              Alarms                  Warnings
            Measurement     High        Low         High          Low
           ----------------------------------------------------------------------------

            Temperature   38.00 C        80.00 C    -25.00 C     75.00 C      -20.00 C
            Voltage          N/A          3.63 V      2.96 V      3.46 V        3.13 V
            Current           N/A       120.00 mA    45.00 mA   115.00 mA      50.00
mA
            Tx Power         N/A         7.99 dBm    2.99 dBm    6.99 dBm      3.99 dBm
```

```
Rx Power          N/A        -6.00 dBm  -29.20 dBm   -7.00 dBm    -28.23 dBm

 Transmit Fault Count = 0
------------------------------------------------------------------------------

 Note: ++  high-alarm; +  high-warning; --  low-alarm; -  low-warning


 2025 Apr 29 05:00:31 switch2 vsh.bin: DIAG VALUES
temp:38000,,,volt:0,,,curr:0,tx:0, rx_pwr: 0
```

（注） コマンドは、PONポートが有効になるまで、電圧、電流、送信電力、または受信電力の値がゼロの場合、電流測定フィールドに「NA」と表示します。

show interface transceiver details コマンド出力で、Rx 電力は常に N/A と表示されます。

ガイドライン

SFPモジュールを使用する場合は、次の注意事項を活用します。

- この光ファイバの PON マネージャでは、次の推奨 SLA 値を活用します。

```
Downstream
Guaranteed Rate [kbps]: 128
Guaranteed Max Burst [bytes]: 100000
Best Effort Rate [kbps]: 10000000
Best Effort Max Burst [bytes]: 99999
Upstream
Fixed Rate [kbps]: 400
Guaranteed Rate [kbps]: 128
Guaranteed Max Burst [bytes]: 409600
Guaranteed Priority [1 Lowest, 8 Highest]: 1
Best Effort Rate [kbps]: 10000000
Best Effort Max Burst [bytes]: 409600
Best Effort Priority [1 Lowest, 8 Highest]: 1
Min Grant Period [100µs]: 0
Max Grant Period [100µs]: 10
Grant Limit [grants]: 8
Service Limit [kBytes]: 60
Service Weight [kBytes]: 0
```

- **shutdown** 操作を実行した後、OLT 光ポートで **no shutdown** を有効にした後、5 分間の設定時間を確保します。この待機期間により、さらにアクションを実行したりステータスを確認したりする前に、PON マネージャを安定させることができます。

インターフェイスの構築に関する制限

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。

- Cisco N9K-C9348GC-FXP スイッチをサードパーティ（SRX4600ファイアウォール）ファイアウォールに接続し、いずれかのスイッチポートがネットワークデバイスのコンソールポートに接続されている場合、ファイアウォールに接続されているすべてのポートでリンクが不安定になるか、 10 Mbpsで設定します。

- 銅線ポートでは、MDIX はデフォルトでイネーブルになっています。MDIX コマンドは、
- **internal** キーワードがサポートされていないため、 **show** を無効にすることはできません。
- 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。 **show interface transceivers** コマンドを使用して互換性を確認します。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構成できます。デフォルトでは、各ポートもレイヤ 3 インターフェイスです。

  switchport コマンドを使用して、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します。**no switchport** コマンドを使用して、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換します。
- 一時停止フレームでフロー制御を使用する ことはできません 。
- Cisco NX-OS リリース 9.3(1) 以降では、MTU 9216のみを FEX ファブリック ポートに設定できます。その他の値が渡された場合は、エラーが生成されます。

  スイッチを Cisco NX-OS リリース 9.3(1) にアップグレードする前に、FEX ファブリック ポートチャネルの MTU 値が 9216 に設定されていた場合、 **show running config** コマンドは MTU 値を表示しませんが、 **show running-config diff** コマンドは表示します。
- Cisco NX-OS リリース 9.3(1) 以降では、FEX ファブリック ポート チャネルはデフォルトで MTU 9216 のみをサポートします。
- これらのラインカードではリンク トレーニングを使用できません。

  Nexus 9300 モジュール：

  - N9K-M12PQ（C9396PX、C9396TX、C93128PX、C93128TX）

  Nexus 9500 モジュール：

  - X9536PQ
  - X9564PX
  - X9564TX
- 有効なインターフェース記述の最後にバックスラッシュ (\) を使用すると、パーサーはバックスラッシュを継続文字として識別し、コマンド文字列に新しい行文字「\n」を追加することにより、コマンド出力に余分な改行を追加します。これは Day-1 の動作です。
- Cisco NX-OS リリース 10.2(3)F 以降、 **link-flap error-disable count** コマンドはすべての Cisco Nexus 9000 シリーズ スイッチのすべての物理ポートで構成できます。
- Cisco NX-OSリリース 10.3(x) および 10.4(x) では、 Nexus 9000 シリーズ スイッチでインターフェイス速度を手動で 100 Mbpsに設定すると、同様に手動で 100 Mbpsに設定する特定の非 Nexus デバイスとのリンク確立を妨げる場合があります。この問題を回避するに

は、リモートデバイスで自動ネゴシエーションを有効にするか、またはリモート構成を変更できない場合の回避策として中間レイヤ 2 スイッチを使用します。

イーサネット ポート速度およびデュプレックスモードに関するガイドライン

- 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、デバイスは自動的に速度およびデュプレックス パラメータの両方を自動に設定します（**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。

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

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

- Cisco Nexus 9000 シリーズ スイッチでは、 `show interface` コマンドと `show interface capability` コマンドを実行すると、特定のポートでサポートされている速度として 100 Mbpsが表示される場合があります。ただし、この速度はSFP-10G-TXトランシーバを使用する場合にのみサポートされます。GLC-TEトランシーバを使用するポートの場合、サポートされている最低速度は 1 Gbps です。

サーバー ポートでの自動ネゴシエーションのサポート

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** コマンを使用します。

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。

- Cisco NX-OSリリース 10.1(2) 以降、これらのスイッチで 40G および 100G 速度の自動ネゴシエーションを使用できます。
  - N9K-C93600CD-GX
  - N9K-C9316D-GX
  - NRZモードのN9K-C9364C-GX
- Cisco NX-OS リリース 9.2(2) 以降、自動ネゴシエーション（40 G/100 G）は以下のポートでサポートされます。
  - Cisco Nexus 9336C-FX2 スイッチ：ポート 1 ー 6 および 33 ー 36
  - Cisco Nexus 93240YC-FX2 スイッチ：ポート 51 ー 54
  - Cisco Nexus 9788TC ライン カード：ポート 49 ー 52
  - Cisco NX-OS リリース 10.4(1)F 以降、100G/40G の自動ネゴシエーションは、Cisco Nexus 9332D-H2R プラットフォーム スイッチでサポートされます。ただし、400G はサポートされていません。
  - Cisco NX-OS リリース 10.4(2)F, 以降、100G/40G ポートの自動ネゴシエーションは、Cisco Nexus 93400LD-H1 プラットフォーム スイッチの最後の 4 つのポートでサポートされます。
  - Cisco NX-OS リリース 10.4(3)F 以降、100G/40G ポートの自動ネゴシエーションは、Cisco Nexus N9K-C9364C-H1 プラットフォーム スイッチでサポートされます。

自動ネゴシエーションの非サポート

自動ネゴシエーションは、これらのNexusスイッチの400Gおよび200G銅線リンクではサポートされて いません 。リンクをアップにするには、ピア側でそれぞれの速度を構成する必要があります。

Nexus スイッチ	銅線サポート（自動ネゴシエーションなし）	リリース
N9K-C9348D-GX2A	400G	10.2(3)F
N9K-C9348D-GX2A	200G	10.3（3）F
N9K-C9364D-GX2A	400G	10.2(3)F

Nexus スイッチ	銅線サポート（自動ネゴシエーションなし）	リリース
N9K-C9364D-GX2A	200G	10.3（3）F
N9K-C9332D-GX2B	400G	NX-OS 10.2(1q)F
N9K-C9332D-GX2B	200G	10.3（3）F
N9K-C93600CD-GX	400G	9.3(5)
N9K-C93600CD-GX	200G	10.3（3）F
N9K-C9316D-GX	400G	9.3(5)
N9K-C9316D-GX	200G	10.3（3）F
N9K-X9400-8D	400G	10.3（3）F
N9K-X9400-8D	200G	10.3（3）F
N9K-X9400-16W	200G	10.5(1)F

- 自動ネゴシエーションは、25G ブレークアウトポートではサポートされていません。
- ケーブル長が 5 m を超える場合、自動ネゴシエーションはサポートされていません。このケーブル長の制限は、銅ケーブルにのみ適用されます。光ケーブルには適用されません。
- Cisco Nexus NX-OS Release 10.4(3) 以降の、100G-CR2(PAM4)/ 4ZQ100G 銅線 PAM4 リンクでの自動ネゴシエーションはサポートされていません。

  リンクをアップにするには、ピア側で speed 100000 を構成する必要があります。

  - N9K-C93600CD-GX
  - N9K-C9316D-GX

（注） Cisco Nexus NX-OS リリース 10.4(3)F 以降、N9K-C93600CD-GX では、100G-CR2(PAM4)/4ZQ100G 銅線リンクはポート 29 ～ 36 でのみサポートされます。

- Cisco NX-OS リリース 10.4(2)F 以降では、リンクをアクティブにするには、両方の 50Gx2 ブレークアウト ポートで同じ FEC を設定する必要があります。

  FEC タイプは、ポートの自動ネゴシエーションではサポートされていません。デフォルト構成がポートで異なる場合は、両方のポートに同じ構成が存在することを確認します。
- N9K-C93108TC-FX3P スイッチが次のいずれかのスイッチに接続されている場合、自動ネゴシエーションはサポートされません。

- N9K-C9236C、N9K-C92300YC、N9K-C9232C、N9K-C92300YC、および N9K-C93180YC-FX。
- N3K-C3172TQ-XL、N3K-C3172TQ-10GT、N3K-C3172PQ-10GE、および N3K-C3132Q-40GE。

- Cisco NX-OS リリース 10.5（2）F 以降、N9K-X9736C-FX3 ライン カードを搭載した Cisco Nexus 9508 スイッチ：
  - 自動ネゴシエーションは、QSFP-100G および QSFP-40G（銅線）トランシーバではディセーブルになっています。
  - 2 m の銅線ケーブルのみがサポートされます。

Cisco Nexus 9348GC-FX3PH スイッチ

- Cisco NX-OS リリース 10.4(1)F 以降、Cisco Nexus C9348GC-FX3PH スイッチには以下の制限が適用されます。
  - フロント ポート 41 ～ 48 では、輻輳またはライン レート トラフィック中にコントロール プレーンが影響を受ける可能性があります。
  - ライン レート トラフィックの 99.98% でドロップはありません。
  - これらのインターフェイス カウンタは、前面ポート 41 ～ 48 でサポートされます。
    - インターフェイスパケット：入力パケット、Rx ユニキャストパケット、Rx マルチキャストパケット、Rx ブロードキャストパケット、Tx ユニキャストパケット、出力パケット、Tx マルチキャストパケット、および Tx ブロードキャストパケット。
    - インターフェイス エラー：入力ラント エラー、入力 FCS エラー、入力エラー、シンボル エラー、入力 CRC、および出力エラー。
    - インターフェイス コリジョン：コリジョン、シングル コリジョン、マルチ コリジョン、およびレイト コリジョン。
    - インターフェイス バイト：Rx バイト、および Tx バイト。
    - その他のサポートされているインターフェイス カウンタ：Tx Dropped、Short Frame、Jumbo Frames、Input Discard、Deferred、および Jabber。

Cisco Nexus N9K-9232E-B1 スイッチ

- Cisco NX-OS リリース 10.4(2)F 以降、Cisco Nexus N9K-C9232E-B1 スイッチはこれらの機能をサポートします。
  - 2 x 400G ポート、4 x 100G ポート、および 8 x 100G ポートのブレークアウトをサポートします。

- ブレークアウト 4x25G および 2x50G を 100G ファイバ リンクおよび 100G 光ファイバでサポートされています。
- ネイティブ 400G およびネイティブ 100G ポートをサポートされています。
- 800G 銅ケーブルは 9 ～ 24 ポートにのみ接続可能です。

自動ネゴシエーションはこのスイッチでサポートされません。

Cisco Nexus 9808 と Cisco Nexus 9804

Cisco NX-OS リリース 10.3(1)F 以降、Cisco Nexus 9800 プラットフォーム スイッチはこれらの機能を備えています。

- インターフェイス整合性チェッカーをサポートします。
- N9K-X9836DM-A ライン カードでは、ネイティブ (400G、100G、40G) およびブレイクアウト (4x100G) ポートのサポートが提供されます。
- N9K-X9836DM-A ラインカードには、CVR-QSFP-SFP10G アダプタを使用した10G光サポートが提供されています。
- N9K-X9836DM-A ライン カード用の 40G、100G 銅線ベースのリンクでは、自動ネゴシエーションはサポートされません。
- 物理インターフェイスの統計情報をサポートします。
- UDLD サポート。
- Cisco Nexus 9808/9804 プラットフォーム スイッチには、物理インターフェイスの統計に関して次の制限があります。
  - ポート チャネルはサポートされません。
  - ブロードキャスト カウンタまたは統計は、インターフェイス カウンタではサポートされません。
  - ローカルで生成または注入されたパケットは、ユニキャスト、マルチキャスト、またはブロードキャストに分類されません。ただし、これらは合計パケット数とバイト数に含めて計算されます。例：CDP パケットです。
  - フレームサイズは show interface ethernet 1/1 counters detailed snmp コマンドを使用して表示できます。

```
This platform counter Range
===============
TX Frame octet Range
TX legal frames with 1519-2500 bytes.
TX legal frames with 2501-9000 bytes.
Nexus existing platform
================
TX Length=1519-2047
TX Length=2048-4095
TX Length=4096-8191
TX Length=8192-9215
```

```
TX Length>=9216
Similar frame size support exists for Rx direction also.

show interface ethernet 1/1 counters detailed snmp
Ethernet1/1
Rx Packets: 4004
Rx Unicast Packets: 4000
Rx Jumbo Packets: 4000
Rx Bytes: 7031737
Rx Packets from 65 to 127 bytes: 1
Rx Packets from 128 to 255 bytes: 1
Rx Packets from 512 to 1023 bytes: 1
Rx Packets from 1024 to 1518 bytes: 1
Rx Packets from 1519 to 2500 bytes: 4000 >>>> New range supported
Tx Packets: 17
Tx Bytes: 4948
Tx Packets from 0 to 64 bytes: 2
Tx Packets from 65 to 127 bytes: 3
Tx Packets from 128 to 255 bytes: 10
Tx Packets from 512 to 1023 bytes: 1
Tx Packets from 1024 to 1518 bytes: 1
Tx Packets from 1519 to 2500 bytes: 2 >>>>> New range
```

- インターフェイス エラー カウンタでは、Align-Err、Runts、Giants、Input Discards、および Output Discards カウンタはサポートされておらず、0 として表示されます。

  次に例を示します。

```
show interface ethernet 1/1 counters errors

--------------------------------------------------------------------------------
Port Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize OutDiscards
--------------------------------------------------------------------------------
Eth1/1 0 0 0 0 0 0

--------------------------------------------------------------------------------
Port Single-Col Multi-Col Late-Col Exces-Col Carri-Sen Runts
--------------------------------------------------------------------------------
Eth1/1 0 0 0 0 0 0

--------------------------------------------------------------------------------
Port Giants SQETest-Err Deferred-Tx IntMacTx-Er IntMacRx-Er Symbol-Err
--------------------------------------------------------------------------------
Eth1/1 0 -- 0 0 0 0

--------------------------------------------------------------------------------
Port InDiscards
--------------------------------------------------------------------------------
Eth1/1 0

--------------------------------------------------------------------------------
Port Stomped-CRC
--------------------------------------------------------------------------------
Eth1/1 0
```

Cisco NX-OS リリース 10.4(1)F 以降、Cisco Nexus 9800 プラットフォーム スイッチで UDLD のサポートが提供されます。

- Cisco Nexus 9804 プラットフォーム スイッチおよび Cisco Nexus 9808 および 9804 スイッチを搭載した Cisco Nexus X98900CD-A および X9836DM-A ライン カードを UDLD がサポートします。

Cisco Nexus 9800 シリーズ スイッチの Cisco Nexus N9K-X9836DM-A ライン カードには、4 x 10G および 4 x 25G のブレイクアウト ポートが用意されています。

Cisco Nexus 93C64E-SG2-Q スイッチ 機能

Cisco NX-OS リリース 10.2（2）F以降、 Cisco Nexus 93C64E-SG2-Q スイッチ はこれらの機能をサポートしています。

- 100G ポート X 8、400G ポート X 2、および 100G ポート X 4 をサポート
- 800G、400G、200G、および 100G インターフェイスのネイティブ固定速度
- ブレークアウト 8 X 100G、2 X 400G と 4 X 100G ポートのブレークアウト モードをサポート
- 64 x QSFP-DD800 ポートをサポート
- 光モジュールのサポート
  - QDD-8X100G-FR
  - QDD-8x100G-LR
  - QDD-2X400G-FR4
  - QDD-2x400G-LR4

自動ネゴシエーションはサポートされません。

Cisco Nexus 9336C-SE1 スイッチの機能

Cisco NX-OS リリース 10.6(1)F 以降、 Cisco Nexus 9336C-SE1 スイッチはこれらの機能をサポートしています。

- ポート プロファイル
- UDLD

リタイマー ポート

リタイマー ポートは、特定のNexusスイッチおよびライン カードで使用できる特殊なハードウェアインターフェイスです。ポート：

- フォワーディング エンジンと前面パネル ポート間の信号完全性を向上させ、
- MACsecまたは SyncE 機能などの追加機能を提供する場合があり、
- の速度、光ファイバ、ケーブル、およびリンクパートナーの特性によっては、リンクアップ時間がやや長くなる場合があります。

リタイマーポートでは、ネゴシエート結果の速度、使用されている光ファイバ、トランシーバとケーブル、また接続されたリンク パートナーの特定の特性に応じて、リンク アップ時間が長くなる場合があります。

ほとんどの場合、リタイマーポートは数秒以内にリンクアップします。ネゴシエートされたパラメータと使用されているハードウェアによっては、リンクアップ時間が長くなる場合があります。

次の表に、リタイマーポートをサポートするNexusスイッチおよびラインカードを示し、各デバイスの特定のポートを示します。

表 *6:* サポートされるリタイマー ポート

スイッチ/ライン カード	リタイマー ポート
N9K-X9788TC-FX	49-52
N9K-C93240YC-FX2 N9K-C93240YC-FX2-Z	51-54
N9K-C9336C-FX2	1 ～ 6、33 ～ 36
N9K-X96136YC-R	49-52
N9K-X9736C-FX	29-36
N9K-C93180YC-FX3	1 ～ 54
N9K-C93216TC-FX2 N9K-C93360YC-FX2	97 ～ 108
N9K-X9716D-GX	1 ～ 16
N9K-C9336C-FX2-E	1 ～ 8
N9K-C9332D-GX2B	25～32
N9K-C9348D-GX2A	1-48
N9K-C9364D-GX2A	1-32
N9K-X9836DM-A	1-36
N9K-X9400-22L	1-22
N9K-X9400-16W	1 ～ 16
N9K-X9400-8D	1 ～ 8
N9K-C9364C-H1	1-64

N9K-C93400LD-H1	1～52
N9K-C9332D-H2R	1-32
N9K-X98900CD-A	1,4,7,10,13,16,19,22,25,28,31,34,37,40,43,46
N9K-C9348GC-FX3 N9K-C9348GC-FX3PH	49-54
N9K-C93108TC-FX3	49-54
N9K-C92348GC-FX3	49-54

インターフェイス パラメータのデフォルト設定

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	ディセーブル
帯域幅	インターフェイスのデータ レート
スループット遅延	100 マイクロ秒
管理ステータス	シャットダウン
MTU	1500 バイト
UDLD グローバル	グローバルにディセーブル
ポート別の UDLD イネーブル ステート（光ファイバ メディア用）	すべてのイーサネット光ファイバLANポートでイネーブル
銅線メディア用のポート別 UDLD イネーブル ステート	すべてのイーサネット 1G、10G、または 40G LAN ポートでディセーブル
UDLD メッセージの間隔	ディセーブル
UDLD アグレッシブ モード	ディセーブル
エラー ディセーブル	ディセーブル
エラー ディセーブル回復	ディセーブル
エラー ディセーブル回復間隔	300 秒

パラメータ	デフォルト
バッファ ブースト	イネーブル （注） この機能は、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です。

基本インターフェイス パラメータ

基本インターフェイス パラメータは、

- デバイス内でのネットワーク インターフェイスの動作を決定し、
- IP アドレス、デュプレックス モード、速度などの重要な設定を指定し、
- ネットワーク上の適切な接続とプロトコルの互換性を確保するのに役立つ構成要素です。

インターフェースのパラメータを設定する前にインターフェースを指定する必要があります

構成するインターフェイスを指定

153インターフェイス範囲設定モードでは、共有構成パラメータを使用して、同じタイプまたは異なるタイプの複数のインターフェイスを構成できます。インターフェイスを指定すると、インターフェイス構成モードを終了するまで、後続のすべてのコマンドは選択したインターフェイスに影響します。

構成するインターフェイスを指定するには、次の手順を活用します。

始める前に

インターフェイスタイプとそのID方法を確認します。

表 *7:* インターフェイスタイプとその識別方法

インターフェイス タイプ	ID
イーサネット	I/O モジュールのスロット番号およびモジュールのポート番号
管理	0（ポート 0）

手順

ステップ 1 グローバル構成モードを開始します。

例：

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

ステップ 2 **interface** *interface* コマンドを使用して構成する 1 つ以上のインターフェイスを指定します。

イーサネット インターフェイス：単一のイーサネットインターフェイスを指定します。

（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）との間にスペースは不要です。

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」のいずれかを指定できます。

例：

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

連続するイーサネットインターフェイスの範囲を指定するには（ダッシュ「-」を使用）、次のコマンドを実行します。

例：

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

不連続イーサネットインターフェイスを指定する場合（カンマを使用し、それぞれを完全に指定して）：

（注）
非隣接インターフェイスを指定する場合は、シンタックスの柔軟性を高くするために各エントリのインターフェイスタイプを入力します。タイプと ID の間のスペースを省略できます（「ethernet 4/5」または「ethernet4/5」）。

例：

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

ブレークアウトケーブルまたはマルチレベルスロットには、次のシンタックスを活用します。

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

管理インターフェイス

管理インターフェイスは「mgmt0」または「mgmt 0」となります。

例：

```
switch(config)# interface mgmt0
switch(config-if)#
```

VLAN インターフェイス

例：

```
switch(config)# interface vlan 10
      switch(config-if)#
```

ループバック インターフェイス

例：

```
switch(config)# interface loopback 1
      switch(config-if)#
```

サブインターフェイス

同じポート上のサブインターフェイスの範囲のみを指定できます（ダッシュ「-」を使用）。カンマを使用して複数のサブインターフェイスを別々に指定できます。

（注）
異なるポートにまたがる範囲を指定することはできません（たとえば、「2/29.2-2/30.2」は無効です）。

例：

```
switch(config)# interface ethernet 2/29.1-2
      switch(config-if-range)#
```

指定されたインターフェイスのインターフェイス構成モードになり、設定パラメータを適用できるようになりました。

インターフェイスに説明パラメータを追加

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追加します。

手順

ステップ 1 グローバル構成モードを開始します。

例：

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

ステップ 2 **interface** *interface* コマンドを使用してインターフェイスを指定します。

例：

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

例：

```
switch(config)# interface mgmt0
switch(config-if)#
```

- イーサネット ポートの場合は、 **ethernet** *slot/port* を使用します。たとえば、スロット 2、ポート 1 はイーサネット インターフェイス 2/1 を示します。

- 管理インターフェイスには、 **mgmt0** を使用します。たとえば、mgmt0 は管理インターフェイスを識別します。

ステップ 3 **description** *text* コマンドを使用して説明を追加します。

例：

```
switch(config-if)# description Ethernet port 3 on module 1
switch(config-if)#
```

ステップ 4 （任意） **show interface** *interface* コマンドを使用して説明を表示します。

例：

```
switch(config)# show interface ethernet 2/1
```

例：

```
switch(config)# show interface mgmt 0
```

Cisco NX-OSリリース 10.4(1)F 以降のバージョンでは、管理インターフェイスの説明を表示できます。

ステップ 5 設定を終了します。

例：

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

ステップ 6 （任意） 実行中の構成をスタートアップ構成に保存します。

例：

```
switch(config)# copy running-config startup-config
```

例

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
```

show interface mgmt の出力 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 interface mgmt 0mgmt0 is up
admin state is up,
  Hardware: GigabitEthernet, address: d009.c863.6660 (bia d009.c863.6660)
  Internet Address is 10.10.1.1
  MTU 1500 bytes, BW 1000000 Kbit , DLY 10 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, medium is broadcast
  full-duplex, 1000 Mb/s
  Auto-Negotiation is turned on
  Auto-mdix is turned off
  EtherType is 0x0000
  1 minute input rate 208920 bits/sec, 146 packets/sec
  1 minute output rate 514648 bits/sec, 144 packets/sec
  Rx
    11890676 input packets 11773213 unicast packets 97704 multicast packets
    19759 broadcast packets 2089190866 bytes
  Tx
    11776034 output packets 11774699 unicast packets 1323 multicast packets
    12 broadcast packets 5228573079 bytes
  Management transceiver: Present
  Active connector: SFP
```

RJ45 コネクタを取り外すと、**アクティブなコネクタ**に SFP が表示されます。

イーサネットポートに対してビーコン モードのイネーブル化

デバイスのステータス LED を点滅させて、特定のイーサネットポートを見つけます。

手順

ステップ 1 グローバル構成モードを開始します。 **configure terminal**

例：

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

ステップ 2 **interface ethernet** *slot/port* を使用してインターフェイスを指定します。 コマンドを使用します。

例：

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

ステップ 3 [**no**] **beacon** コマンドを使用してビーコン モードを有効にします。

例：

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

デフォルト モードはディセーブルです。**[no] beacon** コマンドを活用、ビーコン モードを無効にします。T

ステップ 4 （任意） **show interface ethernet** コマンドを使用してインターフェイスのステータスを表示します。

例：

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

ステップ 5 コンフィギュレーション モードを終了します。

例：

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

ステップ 6 （任意） 実行中の構成をスタートアップ構成に保存します。

例：

```
switch(config)# copy running-config startup-config
```

イーサネットポートの LED が点滅し、ポートの物理位置を目視で確認できます。

例

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 ステートの構成

error-disabled ステートとは、事前定義された障害または違反

- が検出されるとポートまたはインターフェイスを自動的に無効にし、シャットダウンの原因となった
- 特定のエラーを管理者に信号を送信するネットワーク インターフェイスの状態です。

インターフェイスが error-disabled ステートになる一般的な原因は次のとおりです。

- BPDU Guard 違反
- 単一方向リンク検出（UDLD）
- ポート セキュリティ違反（過剰なMAC アドレスの違反など）
- リンクフラッピングまたは物理層エラー

ネットワーク デバイスは、インターフェイスがディセーブルになった具体的な理由を示すログまたはステータスメッセージを提供することがよくあります。

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

リンクフラップやACL例外などの特定の障害が検出されたときに、インターフェイスがerrdisableステートになるように errdisable 検出を設定するには、次の作業を活用。

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。

始める前に

適切な管理権限（イネーブルおよび構成モードのアクセス）でデバイスにアクセスできる必要があります。

変更内容が失われないようにするため、実行コンフィギュレーションをパスワード を 変更。

。

手順

ステップ 1 グローバル構成モードを開始します。

例：

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

ステップ 2 **errdisable detect cause** {**acl-exception** | **all** | **link-flap** | **loopback**}を使用して、インターフェイスで error-disable をトリガーするための 1 つまたは複数の条件を指定します。

例：

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

Error-disable の検出は、サポートされる原因に対してデフォルトで有効になっています。

ステップ 3 リンクフラップ エラー無効化の数と間隔を設定、 **link-flap error-disable count** *number_of_link_flaps* **interval** *time_in_seconds* コマンドを使用して、特定の間隔で発生するフラップの数を指定します。

例：

```
switch(config-if)# link-flap error-disable count 10 interval 30
```

- **count** 許容されるリンク フラップの最大数（範囲：2 ～ 30）。
- **interval** はフラップがカウントされる秒数を指定します（範囲：30 ～ 420）。

ステップ 4 インターフェイスが error-disabled 状態になり、手動回復が必要な場合：

a) インターフェイスを管理上のシャットダウン状態にします。

例：

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

b) インターフェイスを管理上アップ状態にします。

例：

```
switch(config-if)# no shutdown
switch(config)#
```

（注）
これらのコマンドは errdisable ステートをクリアし、インターフェイス動作を復元します。

ステップ 5 （任意） **show interface status err-disabled** コマンドを使用して、error-disabled になったインターフェイスに関する情報を表示します。

例：

```
switch(config)# show interface status err-disabled
```

ステップ 6 （任意） **copy running-config startup-config** コマンドを使用して、実行中の構成を保存します。

例：

```
switch(config)# copy running-config startup-config
```

---

diserror-disabled 検出をイネーブルにすると、設定された原因がインターフェイスで検出された場合、そのインターフェイスは error-disabled ステートになります。

例

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)#
```

インターフェイスを error-disabled 状態から回復

インターフェイスは、いくつかの理由でエラーディセーブルになる場合があります。指定された間隔の後にインターフェイスが再び起動を試みることができるように、回復を構成します。

インターフェイスが error-disabled ステートから回復してアプリケーションを設定することができます。デフォルトで、 **errdisable recovery interval** コマンドを使用して、回復タイマーを構成しない限り、300 秒後にリトライします。

始める前に

スイッチCLIに管理アクセスできることを確認してください。

インターフェイスの error-disabled の原因を確認します。

手順

ステップ 1 グローバル構成モードを開始します。

例：

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

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**} を使用して、自動回復の条件を指定します コマンドを使用します。

例：

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

デバイスはインターフェイスの起動を試行し、300 秒待機してから、さらに試行します。自動回復は、デフォルトでは無効になっています。

ステップ 3 （任意） **show interface status err-disabled** コマンドを使用して error-disabled インターフェイスの情報を表示します。

例：

```
switch(config)# show interface status err-disabled
switch(config-if)#
```

ステップ 4 実行中の構成をスタートアップ構成に保存します。

例：

```
switch(config)# copy running-config startup-config
```

スイッチは、指定した条件に基づいて、回復間隔（デフォルトは300 秒）の経過後にインターフェイスのアップを試みます。

例

ここでは、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)#
```

インターフェイスの error-disabled 回復間隔の設定

スイッチ ポートが errdisable ステートになる場合、スイッチが回復を試みるまでポートがどのくらいの時間ディセーブルのままであるかを制御できます。

errdisableの回復間隔を設定すると、ポートの回復が自動化され、不要なダウンタイムが最小限に抑えられます。

error-disabled 回復タイマーの値を構成するために、以下の手順を使用できます。

始める前に

ポート回復に必要な間隔（秒単位）を決定します（有効な範囲：30 ～ 65535 秒）。

手順

ステップ 1 グローバル構成モードを開始します。

例：

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

ステップ 2 **errdisable recovery interval** *interval* を使用して、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。 コマンドを使用します。

例：

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

インターバル範囲の値に指定できる範囲は 30～ 65,535 秒です。デフォルト値は 300 秒です。

ステップ 3 （任意） **show interface status err-disabled** コマンドを使用して error-disabled インターフェイスに関する情報を表示します。

例：

```
switch(config)# show interface status err-disabled
switch(config-if)#
```

ステップ 4 （任意） 実行中の構成をスタートアップ構成に保存します。

例：

```
switch(config)# copy running-config startup-config
```

スイッチは自動的に、指定の間隔の経過後に error-disabled になったインターフェイスの回復を試みます。エラー状態によって以前に無効にされたポートは、構成済みのタイマーに基づいて回復プロセスを開始します。

例

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)#
```

MDIX パラメータの構成

異なるケーブル タイプまたは不明なケーブルタイプを使用する装置を接続する場合は、ポートに MDIX を設定します。ほとんどのデバイスでは、柔軟性を最大限に高めるために、デフォルトで MDIX が有効になっています。

他の銅線イーサネット ポートとの接続タイプを検出するには、ローカル ポートで MDIX をイネーブルにします。デフォルトでは、このパラメータはイネーブルです。

始める前に

インターフェイスとプラットフォームで手動 MDIX 構成がサポートされていることを確認します。リモート ポートの MDIX を有効にします。

手順

ステップ 1 グローバル構成モードを開始します。

例：

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

\

ステップ 2 **interface ethernet** *slot* / *port* コマンドを使用して、インターフェイスを指定します。

例：

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

ステップ 3 (**mdix auto**) コマンドを使用して、MDIX 検出を有効にします。

例：

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

```
switch(config)# no mdixswitch(config-if)#
```

no mdix コマンドは、MDIX 検出をディセーブルにします。

（注）
この **no mdix auto** コマンドは、X、N9K-C93108TC-FX、N9K-X9788TC-FX、および N9K-C9348GC-FXP デバイスでのみサポートされます。

ステップ 4 **show interface ethernet** *slot* / *port* コマンドを使用して、MDIX パラメータを確認します。

例：

```
switch(config)# show interface ethernet 3/1
                        switch(config-if)#
```

ステップ 5 設定を終了します。

例：

```
switch(config)# exit
```

ステップ 6 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保存します。

例：

```
switch(config)# copy running-config startup-config
```

これらの手順を完了した後、インターフェイスには MDIX モードが設定されたままになります。

例

次に、イーサネット ポート 3/1 の MDIX 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)# mdix auto
                switch(config-if)#
```

次に、イーサネット ポート 3/1 の MDIX 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)# no mdix
                switch(config-if)#
```

管理インターフェイスでのメディ アタイプの構成

Cisco NX-OS リリース 10.6(1)F以降では、デバイスの管理インターフェイスのメディアタイプを設定またはリセットできます。

これにより、使用中の物理ネットワーク メディアとの互換性が確保されます。管理インターフェイスは、RJ45、SFP、または自動モードをサポートしています。デフォルトでは、メディア タイプは自動に設定されています。

次の手順を使用して、 管理インターフェイスのメディア タイプを構成します。

始める前に

ネットワークに必要なメディア タイプを特定します（RJ45、 SFP、または自動）。

手順

ステップ 1 グローバル構成モードを開始します。

例：

```
Switch# configure terminal
```

ステップ 2 管理インターフェイスのインターフェイス構成モードを開始します。

例：

```
Switch (config)# interface mgmt 0
```

ステップ 3 **[no] media-type [rj45 | sfp | auto]** を使用して、インターフェイスのメディア タイプを設定します。

例：

```
Switch (Config)# media-type rj45
```

管理インターフェイスのメディアタイプの値を設定します。

- **media-type rj45** ：メディアタイプを RJ45 に設定します。
- **media-type sfp** ：メディアタイプを SFP に設定します。
- **media-type auto** ：メディアタイプを自動に設定します。

デフォルトの選択に戻すには、管理インターフェイスで **no media-type** を使用します。

（注）
デフォルトの構成は、**media-type auto** です。

管理インターフェイスは、指定されたメディア タイプを使用するように構成されます。デバイスは、ネットワーク接続に設定されたメディアオプションを使用します。

例

管理インターフェイスのメディアタイプ値を表示するには、 **show running-config interface mgmt0** コマンドを活用します。

```
switch# show running-config interface mgmt0
               !
               interface mgmt0
               vrf member management
               ip address 172.29.149.188/24

               mgmt0 is up
               admin state is up,
               Hardware: GigabitEthernet, address: 00a3.8e6d.800e (bia 00a3.8e6d.800e)

               MTU 1500 bytes, BW 1000000 Kbit , DLY 10 usec
               reliability 255/255, txload 1/255, rxload 1/255
               Encapsulation ARPA, medium is broadcast
               full-duplex, 1000 Mb/s
               Auto-Negotiation is turned on
               Auto-mdix is turned off
               EtherType is 0x0000
               1 minute input rate 3544 bits/sec, 5 packets/sec
               1 minute output rate 1472 bits/sec, 0 packets/sec
               Rx
               1263 input packets 0 unicast packets 654 multicast packets
               609 broadcast packets 112586 bytes
               Tx
               19 output packets 0 unicast packets 8 multicast packets
               11 broadcast packets 2641 bytes
               Management transceiver: Present
               Active connector: RJ45
               Configured Media-type: RJ45
```

SFP-10G-TX トランシーバのメディア タイプの構成

このタスクを使用して、デバイスインターフェイスにSFP-10G-TXメディア タイプを指定します。これを構成するには、インターフェイス コンフィギュレーション モードで **media-type 10g-tx** コマンドを入力します。デフォルトに復元するには、**no media-type 10g-tx** コマンドを入力します。

SFP-10G-TXトランシーバのメディア タイプを構成するには、次の手順を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	グローバル構成モードを開始します。 例： `Switch# configure terminal`	

	コマンドまたはアクション	目的
ステップ 2	SFP -10G-TX が取り付けられているインターフェイスのインターフェイス構成モードを開始します。 例： `Switch (config)# interface ethernet 1/5`	
ステップ 3	**media-type 10g-tx** コマンドを使用して、インターフェイスでメディア タイプを 10G-TX として構成します。 例： `Switch (Config)# [no] media-type 10g-tx`	（注） インターフェイスが管理「アップ」状態の間にメディア タイプ 10G-TX で設定されており、この設定をサポートしていない場合、インターフェイスは error-disabled ステートになります。回復するには、インターフェイスで次のコマンドを入力します。 • **shutdown** • **no shutdown**

インターフェイスは、SFP-10G-TX メディア タイプを使用するように設定されます。インターフェイスがこの構成をサポートしていない場合は、error-disabled ステートから回復するための追加の手順の実行が必要になる場合があります。

メディアタイプの確認

これらのコマンドを使用して、Cisco スイッチのメディアタイプ設定を確認します。メディアタイプは、物理インターフェイスの機能（銅線または光ファイバとサポートされる速度など）を定義します。

- **show running-config interface** *interface*：指定されたインターフェイスのメディアタイプセットを含む現在の設定を表示します。
- **show interface status**：すべてのアクティブインターフェイス、その動作ステータス、速度、および検出されたメディアタイプを一覧表示します。たとえば、SFP-10G-TX モジュールはさまざまなポートに存在する場合があります。
- **show module**：サポートされているポート タイプとスロットの詳細を含む、インストールされているハードウェアモジュールに関する詳細情報を表示します。

メディアタイプの設定を確認するために、この例を使用します。

（注） SFP-10G-TX モジュールをサポートするポートは、デバイスごとに異なる場合があります。この例では、Cisco Nexus N9K-C93240YC-FX2 スイッチの、SFP-10G-TX のポート番号を表示します。

```
switch# show running-config interface ethernet 1/2

            !Command: show running-config interface Ethernet1/2
            !Running configuration last done at: Mon Jun  1 10:16:46 2020
            !Time: Mon Jun  1 10:16:54 2020

            version 9.3(5) Bios:version 05.41

            interface Ethernet1/2
            switchport
            switchport access vlan 10
            mtu 9216
            media-type 10g-tx
            no shutdown

            Supported ports in Switch 01:


switch# show interface status | i i SFP-10
            Eth1/2        --                   connected 10        full    10G
SFP-10G-T-X
            Eth1/6        --                   connected 11        full    10G
SFP-10G-T-X
            Eth1/8        --                   connected 11        full    10G
SFP-10G-T-X
            Eth1/12       --                   connected 12        full    10G
SFP-10G-T-X
            Eth1/14       --                   connected 12        full    10G
SFP-10G-T-X
            Eth1/18       --                   connected 13        full    10G
SFP-10G-T-X
            Eth1/20       --                   connected 13        full    10G
SFP-10G-T-X
            Eth1/24       --                   connected 14        full    10G
SFP-10G-T-X
            Eth1/26       --                   connected 14        full    10G
SFP-10G-T-X
            Eth1/30       --                   connected 15        full    10G
SFP-10G-T-X
            Eth1/32       --                   connected 15        full    10G
SFP-10G-T-X
            Eth1/36       --                   connected 16        full    10G
SFP-10G-T-X
            Eth1/38       --                   connected 16        full    10G
SFP-10G-T-X
            Eth1/42       --                   connected 20        full    10G
SFP-10G-T-X
            Eth1/44       Connect_to_Sw_01     connected 202       full    10G
SFP-10G-T-X
            Eth1/48       Connect_to_Sw_02     connected 202       full    10G
SFP-10G-T-X
```

```
            switch# show module
            Mod Ports             Module-Type                        Model          Status

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

            1    60   48x10/25G + 12x40/100G Ethernet Modul N9K-C93240YC-FX2      active
 *
```

```
Mod  Sw                     Hw     Slot
---  ---------------------- ------ ----
1    9.3(4.104)             0.3020 NA


Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    b4-de-31-94-4e-c8 to b4-de-31-94-4f-0f  FDO2143306S

Mod  Online Diag Status
---  ------------------
1    Pass
```

MTU サイズの設定

最大伝送ユニット（MTU）サイズは、次のネットワーク インターフェイスのパラメータです。

- インターフェイスがフラグメンテーションなしで送信できる最大パケット サイズを定義します。
- インターフェイスがレイヤ 2 かレイヤ 3 かによって異なり、
- は、ネットワーク要件に合わせてデフォルト、ジャンボ、またはカスタム値に設定できます。

デフォルト値

- すべてのインターフェイスのデフォルトMTUは1500バイトで、これはシステムデフォルト MTU と呼ばれます。
- レイヤ 2 インターフェイスは、システム ジャンボ MTU のデフォルト値である 9216 バイトの値で設定できます。

MTU サイズの設定に関するガイドライン

MTU はインターフェイスごとに設定されます。インターフェイスはレイヤ 2 またはレイヤ 3 です。

- レイヤ 2 インターフェースでは、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（デフォルトで 9216 バイト）のいずれかを選択できます。

  1500 ～ 9216 バイトのレイヤ 2 MTUを設定するには、まずシステム ジャンボMTU を目的の値に調整します。次に、インターフェイス MTU を設定します。

（注） システムジャンボMTUサイズが変更されると、システムジャンボMTUを使用するすべてのレイヤ2インターフェイスは、新しい値に自動的に更新されます。

- レイヤ3インターフェイス（物理インターフェイス、スイッチ仮想インターフェイス[SVI]、またはサブインターフェイス）では、MTUサイズを576～9216バイトの範囲で設定できます。

例

システム ジャンボMTU を9000バイトに設定すると、ジャンボ値を使用するように設定されたすべてのレイヤ 2 インターフェイスが 9000 バイトに変更されます。

2000 バイトの MTU でレイヤ 3 SVIを設定するには、576 ～ 9216 バイトの範囲内の SVI 上で MTU を直接設定します。

インターフェイスの MTU サイズを構成します

MTUサイズを設定することで、特定のアプリケーションのネットワーク パフォーマンスを最適化し、アップストリームまたはダウンストリームのデバイスとの互換性を確保できます。MTU設定は、レイヤ 2 インターフェイスとレイヤ 3 インターフェイスで異なる場合があります。

始める前に

レイヤ 2、レイヤ 3、または管理インターフェイスのいずれを構成するのかを決定します。

適切な MTU 値が正しいことを確認してください。

- レイヤ 3 インターフェイス（物理、 SVI、またはサブインターフェイスを含む）の場合、576 ～ 9216 バイトの値を入力します。
- レイヤ2インターフェイスの場合、1500（システムデフォルト）またはシステムジャンボMTU値（デフォルトは 9216 バイト。この値は調整可能）を入力します。

  Cisco NX-OSリリース 9.3(1) 以降を実行しているCisco Nexus 9000 スイッチの管理インターフェイスでは、最大 9216 バイトがサポートされます。

（注） MTUサイズを変更すると、エンドデバイスが一時的にネットワーク接続を失う可能性があります。

手順

ステップ 1 グローバル構成モードを開始します。

例：

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

ステップ 2 **interface ethernet** *slot/port*、 vlan *vlan- id*mgmt *0* コマンドを使用して構成するイーサネット インターフェイスを指定します。

例：

```
switch(config)# interface ethernet 3/1
switch(config-if)#
switch(config)# interface vlan 100
switch(config-if)#
switch(config)# interface mgmt 0
switch(config-if)#
```

ステップ 3 **mtu** *size* コマンドを使用して、インターフェイスの MTU 値を構成します。

例：

```
switch(config-if)# mtu 9216
switch(config-if)#
```

size は、インターフェイスタイプでサポートされている範囲内の目的の MTU 値です。

- レイヤ 3 インターフェイスの場合、576 ～ 9216 バイトの値を入力します。
- レイヤ 2 インターフェイスの場合、1500 またはシステム ジャンボの MTU 値を入力します。

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」を参照してください。

ステップ 4 設定を終了します。

例：

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

選択したインターフェイスでは、パケット伝送用に設定した MTU 値が使用されます。

例

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)#
```

図は、show running-config interface コマンドの出力を示しています。

```
switch# show run int mgmt0
!Command: show running-config interface mgmt0
!Running configuration last done at: Fri May 31 11:32:28 2019
!Time: Fri May 31 11:32:33 2019
version 9.3(1) Bios:version 07.65
interface mgmt0
mtu 9216
vrf member management
```

```
ip address 168.51.170.73/82
```

システム ジャンボ MTU サイズの設定

ネットワーク環境が標準規格イーサネットフレームよりも大きいフレームに対するサポートを必要とする場合は、システム ジャンボMTUを設定。これにより、高性能アプリケーションのスループットを向上させることができます。システムジャンボMTUは、1500ー9216の偶数で指定する必要があります。デフォルトは9,216バイトです。

手順

ステップ1 グローバル構成モードを開始します。 **configure terminal**

例：

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

ステップ2 **system jumbomtu** *size* コマンドを使用して、システム ジャンボ MTU サイズを設定します。

例：

```
switch(config)# system jumbomtu 8000
                        switch(config)#
```

1500 ～ 9216 の偶数を使用します。

ステップ3 **interface** *type slot/port* コマンドを使用して、レイヤ 2 インターフェイスを指定します。

例：

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

ステップ4 **mtu** *size* コマンドを使用してMTU をインターフェイスに適用します。

例：

```
switch(config-if)# mtu 8000
                        switch(config-if)#
```

ステップ5 設定を終了します。

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 （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保存します。

例：

```
switch(config)# copy running-config startup-config
```

レイヤ 2 インターフェイスは新しいジャンボ MTU 値を使用して、指定により大きなフレームをサポートします。

例

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)# interface ethernet 2/2
               switch(config-if)# mtu 8000
```

イーサネット インターフェイスの帯域幅を構成します

Nexus スイッチでは、 帯域幅コマンドはレイヤ 3 プロトコルの情報値を設定します。イーサネット インターフェイスの物理帯域幅（1G、10G、40G など）は変更できません。

手順

ステップ 1 グローバル構成モードを開始します。

例：

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

ステップ 2 **interface ethernet** *slot/port* を使用してイーサネット インターフェイスを指定します。 コマンドを使用します。

例：

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

ステップ 3 **bandwidth** *kbps* コマンドを使用して、帯域幅を設定します。

例：

```
switch(config-if)# bandwidth 1000000
switch(config-if)#
```

帯域幅は情報専用の値です。範囲は、1 ～ 100,000,000 キロビット/秒です。

ステップ 4 （任意） **show interface ethernet** スロット/ポート を使用してインターフェイスのステータスを表示します。 コマンドを使用します。

例：

```
switch(config)# show interface ethernet 2/1
```

ステップ 5 コンフィギュレーション モードを終了します。

例：

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

ステップ 6 （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保存します。

例：

```
switch(config)# copy running-config startup-config
```

インターフェイスには、レイヤ3プロトコルの更新された情報で帯域幅の値が表示されます。物理インターフェイスの帯域幅は変更されません。

例

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 Kbs 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)#
```

スループット遅延間隔を設定

スループット遅延値は情報を提供し、イーサネット インターフェイスのプロトコル パスの設定に影響します。

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。

始める前に

feature eigrp コマンドを使用してインターフェイスを指定します。

手順

ステップ 1 グローバル構成モードを開始します。

例：

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

ステップ 2 **interface ethernet** *slot/port* コマンドを使用してインターフェイスを指定します。

例：

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

ステップ 3 **delay** *value*　コマンドを使用して遅延間隔を指定します。

例：

```
switch(config-if)# delay 10000
switch(config-if)#
```

1 ～ 16,777,215（10 マイクロ秒単位）の値を設定します。

ステップ 4 インターフェイスのステータスを表示して、遅延設定を確認します。

例：

```
switch(config)# show interface ethernet 3/1
switch(config-if)#
```

ステップ 5 （任意） 設定を終了します。

例：

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

ステップ 6 （任意） 実行中の構成をスタートアップ構成に保存します。

例：

```
switch(config)# copy running-config startup-config
```

例

この例では、イーサネット7/47 に高い遅延値を設定し、7/48 に低い（デフォルト）値を設定して、7/48 を優先インターフェイスにします。低い遅延値が高い値に優先します。

```
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)#
```

インターフェイスのシャットダウンとアクティブ化

メンテナンス、トラブルシューティング、または設定のために、インターフェイスを一時的に無効（シャットダウン）または有効（アクティブ）にする必要がある場合があります。

シャットダウンされたインターフェイスはディセーブルになります。モニタリングではダウンとして表示され、ルーティングプロトコルは更新から除外されます。インターフェイスは、い

つでも再アクティブ化することができます。インターフェイスを再アクティブ化するには、デバイスを再起動する必要があります。

インターフェイスをシャットダウンしてアクティブにするには、次の手順を活用。

手順

ステップ 1 グローバル構成モードを開始します。

例：

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

ステップ 2 **interface** *interface* コマンドを使用して、インターフェ ステータスを無効にします。

例：

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

switch(config)# interface mgmt0
switch(config-if)#
```

インターフェイス タイプと ID を指定できます。

（注）
イーサネットインターフェイスには *ethernet slot/port* を活用、管理インターフェイスには *mgmt0* を 使用します。

例

- イーサネット インターフェイス：1 番目の例は、スロット 2、ポート 1 イーサネット インターフェイスを指定する方法を示します。
- 管理インターフェイス：2 番目の例は、管理インターフェイスを指定する方法を示しています。

ステップ 3 **shutdown** コマンドを使用して、インターフェ ステータスを無効にします。

例：

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

ステップ 4 （任意） **show interface** *interface* コマンドを使用して、インターフェ ステータスを無効にします。

例：

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

ステップ 5 **no shutdown** コマンドを使用して、インターフェイスをイネーブルに（アクティブ化）します。

例：

```
switch(config-if)# no shutdown
switch(config-if)#
```

ステップ 6 （任意） インターフェイスのステータスを再度表示します。

例：

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

ステップ 7 インターフェイス モードを終了します。

例：

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

ステップ 8 （任意） **copy running-config startup-config** を使用して、実行中の構成をスタートアップ構成に保存します。

例：

```
switch(config)# copy running-config startup-config
```

ポートをイネーブルにすると、管理ステータスがディセーブル（ダウン）からイネーブル（アップ）に変わります。インターフェイスがアクティブになり、ルーティング アップデートに含まれます。

例

次に、イーサネット ポートの 3/1 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)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

インターフェイスでの UDLD モードのイネーブル化

UDLD は、光ファイバおよび銅線のイーサネット ポート上の単方向リンクを検出し、単方向通信によって引き起こされるネットワークの問題を防止します。UDLD をグローバルに、またはインターフェイスごとにイネーブルにします。信頼性のニーズに応じて通常モードまたはアグレッシブ モードを選択します。アグレッシブモードは、すべての光ファイバポートに対してグローバルに、または個々のインターフェイスに対してイネーブルにできます。

：

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コマンドのリストを示します。

表 *8*: 光ファイバ ポートおよび銅線ポートのデフォルト *UDLD* 設定

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	有効	無効
enable UDLD コマンド	**no udld disable**	**udld enable**
disable UDLD コマンド	**udld disable**	**no udld enable**

UDLD モードをイネーブルにするには、次の手順を使用します。

始める前に

UDLD をイネーブルにする前に、 **feature udld** コマンドを使用してグローバルにイネーブルになっていることを確認してください。銅線ポートでは、各インターフェイスの UDLD を明示的にイネーブルにします。光ファイバポートでは、UDLD はデフォルトでイネーブルです。 **no udld disable** コマンドでこれを確認します。

アグレッシブ UDLD モードは、UDLD をグローバルに設定し、指定した各インターフェイスでのみイネーブルにしてください。

手順

ステップ 1 グローバル構成モードを開始します。

例：

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

ステップ 2 **feature udld** コマンドを使用して、UDLD をグローバルにイネーブルにします。

例：

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

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

no feature udld コマンドを使用して、デフォルトで UDLD ファイバ ポートをディセーブルにします。

ステップ 3 （任意） UDLD メッセージを送信する間隔を **udld message-time** 秒単位 で指定します。 コマンドを使用します。

例：

```
switch(config)# udld message-time 30
switch(config)#
```

有効な範囲は 7 ～ 90 秒です。デフォルト値は 15 秒です。

ステップ 4 **udld aggressive** を使用したアグレッシブモードで UDLD をイネーブルにします。 コマンドを使用します。

例：

```
switch(config)# udld aggressive
switch(config)#
```

すべてのファイバポートでアグレッシブモードの UDLD をデフォルトでディセーブルにするには、 **no** 形式を使用します。

（注）
ポートを構成するために、**udld aggressive** コマンドを使用します。

- すべてのファイバポートについて、グローバル構成モードで `udld aggressive` コマンドを使用します。
- 特定の銅線インターフェイスの場合、インターフェイス構成モード **interface ethernet** *slot/port* を入力し、 **udld aggressive** コマンドをイネーブルにします。

ステップ 5 **udld** [**enable** | **disable**] を使用して、すべての光ファイバ インターフェイスにおいて、通常モードで UDLD をイネーブルにします。

例：

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

すべてのファイバポートで通常モードの UDLD をデフォルトでディセーブルにするには、 **no** コマンドを使用します。

ステップ 6 **show udld** [**ethernet** *slot/port* | **global** | **neighbors**] コマンドで UDLD ステータスを表示します。

例：

```
switch(config)# show udld
switch(config)#
```

ステップ 7 インターフェイス モードを終了します。

例：

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

ステップ 8 （任意） 実行中の構成をスタートアップ構成に保存します。

例：

```
switch(config)# copy running-config startup-config
```

UDLD は、構成に応じて双方向リンク検出機能を提供するために、選択されたモードで動作します。

例

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
```

次の例は、光ファイバインターフェイスのアグレッシブ UDLD モードをイネーブルにする方法を示しています。

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

次の例は、銅線イーサネット インターフェイス 3/1 のアグレッシブ UDLD モードをイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 3
switch(config-if)# udld aggressive
```

次の例は、アグレッシブ モードがイネーブルになっているかどうかを確認する方法を示しています。

```
switch# sh udld global

UDLD global configuration mode: enabled-aggressive
UDLD global message interval: 15
switch#
```

次に、udld アグレッシブ モードが特定のインターフェイスで動作可能かどうかを確認する例を示します。

```
switch# sh udld ethernet 8/2

Interface Ethernet8/2
--------------------------------
Port enable administrative configuration setting: device-default
Port enable operational state: enabled-aggressive
Current bidirectional state: bidirectional
Current operational state:  advertisement - Single neighbor detected
Message interval: 15
Timeout interval: 5
..!
```

イーサネット ポートにデバウンス タイマーを設定します。

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にします。

デバウンス タイマー値に 0 を指定して、タイマーをディセーブルにします。

ガイドライン

- サービス プロバイダー ネットワークに接続すると、10G および 100G ポートのリンク状態が繰り返し変化することがあります。リンク リセットまたはブレークリンク機能の一部として、リンク状態が変更された場合に、SFP の Tx 電源ライトが N/A 状態に変更されることが予想されます。リンク状態の変更中にこの動作を防ぐには、リンク デバウンス タイマーを 500 ミリ秒から開始し、リンクが安定するまで 500 ミリ秒間隔で増加します。
- DWDM、UVN、および WAN ネットワークでは、可能な場合は常に、自動リンク一時停止（ALS）を無効にします。デバイスがリンクをオフにすると、ALS は WAN 上のリンクを一時停止します。
- **link debounce time** および **link debounce link-up time** コマンドは、物理的なイーサネット インターフェイスにしか適用できません。
- 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。

デバウンス タイマーのサポート

- この **link debounce time** コマンドは、Cisco Nexus 9000 シリーズ スイッチの 1G、10G、40G、25G、および 100G SFP/QSFP ポートでサポートされます。
- **link debounce time** は、Cisco Nexus N9K-C9732C-FX、N9K-C9364C、N9K-X97160YC-EX、N9K-C9336C-FX2、および N9K-C93240YC-FX2 プラットフォーム スイッチで 1G、10G、25G、40G、100G ポートがサポートされます。
- この **link debounce time** コマンドは、Cisco Nexus 93300YC-FX および Cisco Nexus 9336C-FX スイッチの 10G および 40G ポートではサポートされません。

  link debounce time は、Cisco Nexus N9K-C9732C-FX、N9K-C9364C、N9K-X97160YC-EX、N9K-C9336C-FX2、および N9K-C93240YC-FX2 プラットフォーム スイッチで 1G、10G、25G、40G、100G ポートがサポートされます。
- **link debounce time** は、N9K-X97160TC-FX ライン カードを搭載した Cisco Nexus 9500 プラットフォーム スイッチの RJ-45 ポートではサポートされません。
- Cisco NX-OS リリース 10.2(3)F 以降、**link debounce time** コマンドは N9K-C93180YC-FX3S、N9K-C93180YC-FX3、N9K-C93108TC-FX3P、および N9K-X9716D-GX プラットフォーム スイッチでサポートされています。
- Cisco NX-OS リリース 10.2(3)F 以降、**link debounce time** コマンドは次のポートおよびプラットフォーム スイッチでサポートされています。

ポート	スイッチ
1G	Cisco Nexus C、N9K-C93300YC-FX2、N9K-C93240YC-FX2、N9K-C93240YC-FX2-Z、N9K-X97160YC-EX、N9K-C9316D-GX、N9K-CCD-C9360 N9K-C9232C、N9K-C9232C、N9K-C93180YC-FX3S、N9K-C93180YC-FX3、N9K-C93108TC-FX3P、および N9K-X9716D-GX
10G	Cisco Nexus 、N9K-C93300YC-FX2、N9K-C93240YC-FX2、N9K-C93240YC-FX2-Z、N9K-X97160YC-EX、N9K-C9316D-GX、N9K-CCD-C9360 N9K-C9232C、N9K-C9232C、N9K-C93180YC-FX3S、N9K-C93180YC-FX3、N9K-C93108TC-FX3P、および N9K-X9716D-GX
25 G	Cisco Nexus N9K-C93300YC-FX2、N9K-C93240YC-FX2、N9K-C93240YC-FX2-Z、N9K-X97160YC-EX、N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX、N9K-C9232C、 、N9K-C93180YC-FX3S、N9K-C93180YC-FX3、N9K-C93108TC-FX3P、および N9K-X9716D-GX
40G 100G 400G	Cisco Nexus 、N9K-X9732C-FX、N9K-C9336C-FX2、N9K-C93300YC-FX2、N9K-C93240YC-FX2、N9K-C93240YC-FX2-Z、N9K-EX-C9716-EX、N9K-C93600CD-GX、N9K-C9364C-GX、N9K-C9232C、N9K-C93180YC-FX3S、N9K-C93180YC-FX3、N9K-C93108TC-FX3P、および N9K-X9716D-GX

手順

ステップ 1 グローバル構成モードを開始します。

例：

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

ステップ 2 **interface ethernet** *slot/port* を使用してイーサネット インターフェイスを指定します。 コマンドを使用します。

例：

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

ステップ 3 **link debounce time** *time* コマンドを使用してデバウンス タイマーを設定します。

例：

```
switch(config-if)# link debounce time 1000
switch(config-if)#
```

time ：デバウンスタイマーの時間の範囲は 1 ～ 5000 ミリ秒です。

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。

ステップ 4 **link debounce link-up** *time* コマンドを使用してリンク アップ タイマーを設定。

例：

```
switch(config-if)# link debounce link-up 1000
switch(config-if)#
```

time ：リンクアップタイマーの時間の範囲は、1000 ～ 10000 ミリ秒です。このコマンドは、ポート速度が 10G、25G、40G、および 100G の場合にのみ適用されます。

デフォルトのタイマー値は 0 です。値を 0 に設定すると、インターフェイスは遅延なく起動します。

（注）
この **no link debounce link-up** コマンドもまた値を0にリセットします。

（注）
このコマンドは、Cisco Nexus N9K-X9732C-FX、N9K-C93300YC-FX、N9K-C9336C-FX2、、および N9K-X97160YC-EX スイッチでのみサポートされます。

例

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

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

- 次に、イーサネット インターフェイスのデバウンス リンクアップ タイマー 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 link-up time 1000
```

ポート プロファイルの設定

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

ポート プロファイルを作成します。

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、そのタイプと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以下の文字だけを使用します。

- 小文字の英字（a ～ z）
- 大文字の英字（A ～ Z）
- 数字（0 ～ 9）
- 次の特殊文字のみを使用してください。
  - 。
  - -
  - _

手順

	コマンドまたはアクション	目的
ステップ 1	グローバル構成モードを開始します。 例： `switch# configure terminal`	
ステップ 2	**port-profile** [**type** {**ethernet** | **interface-vlan** | **port-channel**}] *name* を使用して、目的のインターフェイス タイプのポート プロファイルを作成し、名前を付けます。 例： `switch(config)# port-profile type ethernet test`	
ステップ 3	ポート プロファイル構成モードを終了します。 例： `switch(config-ppm)# exit`	
ステップ 4	（任意） ポート プロファイル構成を検証します。 例： `switch# show port-profile`	

	コマンドまたはアクション	目的
ステップ 5	（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保存します。 例： `switch# copy running-config startup-config`	

例

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

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

ポート プロファイル構成モードを開始します

ポートプロファイルを追加、削除、変更、または作成するには、ポート プロファイル構成モードを開始します。

ポート プロファイル構成モードを開始するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	グローバル構成モードを開始します。 例： `switch# configure terminal`	
ステップ 2	**port-profile** [**type** {**ethernet** | **interface-vlan** | **port-channel**}] *name* コマンドを使用して、目的のインターフェイス タイプのポート プロファイルを作成し、名前を付けます。 例： `switch(config)# port-profile type ethernet test`	プロファイルの設定を追加または削除できます。
ステップ 3	ポート プロファイル構成モードを終了します。 例： `switch(config-ppm)# exit`	
ステップ 4	（任意） ポート プロファイル構成を表示します。 例：	

	コマンドまたはアクション	目的
	`switch# show port-profile`	
ステップ 5	（任意）実行中の構成をスタートアップ構成に保存します。 例： `switch# copy running-config startup-config`	

例

次に、指定されたポートプロファイルのポートプロファイル構成モードを開始し、すべてのインターフェイスを管理的に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

ポート プロファイルを複数のインターフェイスに一度に割り当てて、構成管理を簡素化します。

このタスクは、スイッチ上の同じタイプの複数のインターフェイスに同じポートプロファイルを適用する必要がある場合に活用。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。

一定範囲のインターフェイスへのポート プロファイルを割り当てるには

始める前に

すべてのターゲットインターフェイスが同じタイプであることを確認します（たとえば、すべてのイーサネット インターフェイス）。

手順

	コマンドまたはアクション	目的
ステップ 1	グローバル構成モードを開始します。 例： `switch# configure terminal`	
ステップ 2	**interface** [**ethernet** *slot/port* | **interface-vlan** *vlan-id* | **port-channel** *number*] コマンドを使用して、構成するインターフェイスを選択します。 例：	

	コマンドまたはアクション	目的
	`switch(config)# interface ethernet7/3-5, ethernet10/2, ethernet11/20-25`	
ステップ 3	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。 **例**： `switch(config-if)# inherit port-profile adam`	
ステップ 4	コンフィギュレーション モードを終了します。 **例**： `switch(config-if)# exit`	
ステップ 5	（任意） ポート プロファイル構成を表示します。 **例**： `switch# show port-profile`	
ステップ 6	（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することで、変更を保存します。 **例**： `switch# copy running-config startup-config`	

指定されたポート プロファイルは、選択したすべてのインターフェイスに適用されます。

例

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

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

特定のポート プロファイルのイネーブル化

ポート プロファイルをイネーブルにすることによって、ポート プロファイルで指定された設定を選択したインターフェイスに適用します。

ポートプロファイルをイネーブルにすると、対象のインターフェイスで設定の継承がアクティブになります。複数のポートプロファイルが継承される場合、最後の継承プロファイルのみを有効にする必要があります。これは、システムが下位プロファイルが有効であると想定するためです。

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。

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、次の手順を使用します。

始める前に

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 プロファイル構成モードを開始する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	グローバル構成モードを開始します。 **例**： `switch# configure terminal`	
ステップ 2	目的のインターフェイスのポートプロファイルを作成して名前を付け、 **port-profile** [**type** {**ethernet** | **interface-vlan** | **port-channel**}] *name* コマンドを使用してポートプロファイル構成モードを開始します。 **例**： `switch(config)# port-profile type ethernet test`	
ステップ 3	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。 **例**： `switch(config-ppm)# state enabled`	
ステップ 4	ポート プロファイル構成モードを終了します。 **例**： `switch(config-ppm)# exit`	
ステップ 5	（任意） ポート プロファイル構成を表示します。 **例**： `switch# show port-profile`	
ステップ 6	（任意） 実行中の構成をスタートアップ構成に保存します。 **例**： `switch# copy running-config startup-config`	

指定されたポートプロファイルを有効にすると、その構成が指定されたインターフェースに適用されます。

例

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

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

ポート プロファイルの継承

別のポート プロファイルから設定を自動的に継承するように、既存のポート プロファイルを設定します。

既存のポートプロファイルが別のプロファイルから設定を継承できるようにするには、次の作業を活用。システムは 4 つのレベルの継承をサポートしています。

始める前に

継承するプロファイルがすでに存在していることを確認してください

手順

	コマンドまたはアクション	目的
ステップ 1	グローバル構成モードを開始します。 **例**： `switch# configure terminal`	
ステップ 2	指定されたポート プロファイルに対して、**port-profile** *name*コマンドを使用して、ポート プロファイル構成モードを開始します。 **例**： `switch(config)# port-profile test`	
ステップ 3	別のプロファイルの設定を継承するには、 **inherit port-profile** *name* コマンドを活用します。 **例**： `switch(config-ppm)# inherit port-profile adam`	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	ポート プロファイル構成モードを終了します。	

	コマンドまたはアクション	目的
	例： `switch(config-ppm)# exit`	
ステップ 5	（任意） ポート プロファイル構成を確認します。 例： `switch# show port-profile`	
ステップ 6	（任意）実行中の構成をスタートアップ構成に保存します。 例： `switch# copy running-config startup-config`	

ポート プロファイルは、指定されたプロファイルからすべての設定を継承します。

例

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

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

一定範囲のインターフェイスからのポート プロファイルの削除

割り当てられたポートプロファイルを1つ以上のインターフェイスから削除します。この操作により、これらのインターフェイスがデフォルト設定に戻るか、または異なるプロファイルを割り当てることができます。

ポート プロファイルが適用されているインターフェイスからポート プロファイルを削除できます。この手順では、インターフェイス構成モードを使用します。

次の手順を実行して、インターフェイスの範囲からポート プロファイルを削除します。

始める前に

ポート プロファイルを削除する必要があるインターフェイスを特定します。

手順

	コマンドまたはアクション	目的
ステップ 1	グローバル構成モードを開始します。 例：	

	コマンドまたはアクション	目的
	`switch# configure terminal`	
ステップ 2	**interface** [**ethernet** *slot/port* | **interface-vlan***vlan-id* | **port-channel***number* コマンドを入力して、インターフェイスの範囲を選択します。 例： `switch(config)# interface ethernet 7/3-5, 10/2, 11/20-25`	
ステップ 3	**no inherit port-profile** *name* コマンドを使用して、選択したインターフェイスからポート プロファイルを削除します。 例： `switch(config-if)# no inherit port-profile adam`	
ステップ 4	コンフィギュレーション モードを終了します。 例： `switch(config-if)# exit`	
ステップ 5	（任意） ポート プロファイル構成を確認します。 例： `switch# show port-profile`	
ステップ 6	（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保存します。 例： `switch# copy running-config startup-config`	

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から割り当て解除します。

例

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

```
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

スイッチ構成内の特定のポート 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。

ポート プロファイルと他のポート プロファイルから構成を継承しないように関連付けを解除する必要がある場合は、次の作業を実行します。このアクションは、継承された構成パラメータを変更または制限するのに役立ちます。

手順

	コマンドまたはアクション	目的
ステップ 1	グローバル構成モードを開始します。 例： `switch# configure terminal`	
ステップ 2	指定されたポート プロファイルに対して、**port-profile** *name* コマンドを使用して、ポート プロファイル構成モードを開始します。 例： `switch(config)# port-profile test`	
ステップ 3	**no inherit port-profile** *name* コマンドを使用して、継承されたポート プロファイルを削除します。 例： `switch(config-ppm)# no inherit port-profile adam`	
ステップ 4	ポート プロファイル構成モードを終了します。 例： `switch(config-ppm)# exit`	
ステップ 5	（任意） ポート プロファイル構成を確認します。 例： `switch# show port-profile`	
ステップ 6	（任意） 実行中の構成をスタートアップ構成に保存します。 例： `switch# copy running-config startup-config`	

指定されたポートプロファイルは、指定ポートプロファイルから設定を継承しなくなります。

例

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

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

DWDM回線またはダーク光ファイバ回線でリンクMACアップタイマーを設定する

DWDM リンクとダーク光ファイバリンクでは、MACアップタイマーの調整が必要になる場合があります。この調整により、リンク イベントの信頼性の高い検出が保証されます。特定のタイマーを設定すると、誤ったリンクフラップを防ぐことができます。

この手順では、DWDM/ダーク ファイバ回線で MAC アップタイマーを設定する方法について説明します。

手順

ステップ 1 グローバル構成モードを開始します。

例：

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

ステップ 2 **interface** *type slot/port* を使用して、DWDM またはダーク光ファイバ回路のインターフェイスを選択します。

例：

```
switch(config)# interface ethernet1/2
switch(config-if)#
```

ステップ 3 **link mac-up timer** *seconds* を使用してリンク MAC アップ タイマーを設定します。

例：

```
switch(config-if)# link mac-up timer 10
```

リンク MAC アップ タイマーの範囲は 0 ～ 120 です。

（注）
この設定は、DWDM リンクまたはダーク光ファイバリンクでのみ設定してください。

リンク MAC アップ タイマーが、選択したインターフェイスに設定され、DWDM またはダーク光ファイバ回線のパフォーマンスが最適化され、信頼性が向上します。

25G 自動ネゴシエーションの設定

自動ネゴシエーションを使用すると、デバイスはリンク セグメントを介して所有する拡張動作モードをアドバタイズし、他のデバイスがアドバタイズする可能性がある対応する拡張動作モードを検出できます。自動ネゴシエーションは、リンク セグメントを共有する 2 つのデバイス間で情報を交換し、両方のデバイスの機能を最大限に活用するように自動的に設定する方法を提供します。

25G 自動ネゴシエーションの注意事項と制限事項

- Cisco NX-OS Release 9.2(1) 以降では、Cisco Nexus N9K-X97160YC-EX、N9K-C93180YC-FX、N9K-C93240YC-FX2、および N9K-C93240YC-FX2-Z で、銅ケーブルを使用したネイティブ25Gポートでの自動ネゴシエーションがサポートされています。
-
- 25Gインターフェイスの自動ネゴシエーションはデフォルトでディセーブルになっています
- 銅線ベースの 25G トランシーバには自動ネゴシエーションが必要です。銅線25Gインターフェイスで **command negotiate auto 25000** をイネーブルにします。リンクの両端間でこのパラメータが一致していない場合、インターフェイスはダウンしたままになることがあります。
- 自動ネゴシエーションは、25G ブレークアウトポートではサポートされていません。

25G 自動ネゴシエーションによる FEC 選択

表 *9 : 25G* 自動ネゴシエーションによる *FEC* 選択

ハードウェア	**CR** 長に基づく **FEC**			
	1 m	2m	3m	5m
N9K-C93240YC-FX2	FEC なし	FEC なし	FC-FEC	RS-IEEE
N9K-C93180YC-FX	FEC なし	FEC なし	FC-FEC	RS-IEEE
N9K-X97160YC-EX	FEC なし	FEC なし	FC-FEC	FC-FEC

インターフェイスの自動ネゴシエーションのイネーブル化

自動ネゴシエーションにより、インターフェイスは自動的に最適な速度とデュプレックスモードを選択できます。25G ネイティブ リンクの両端で自動ネゴシエーションを構成する必要があります。

negotiate auto コマンドを使用して、自動ネゴシエーションをイネーブルにすることができます。

自動ネゴシエーションをイネーブルにするには、次の手順を実行します。

手順

ステップ 1 グローバル構成モードを開始します。

例：

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

ステップ 2 **interface ethernet** *port number* コマンドを使用して、インターフェイスを選択します。

例：

```
switch# interface e1/7
  switch(config-if)#
```

ステップ 3 **negotiate auto** *port speed* コマンドを使用してインターフェイスで自動ネゴシエーションを有効にします

例：

```
switch(config-if)# negotiate auto 25000
 switch(config-if)#
```

（注）
このコマンドは、25G ネイティブ リンクの両側のインターフェイスに適用する必要があります。

選択したインターフェイスの自動ネゴシエーションをイネーブルにします。

例

次に、指定したイーサネットインターフェイスで自動ネゴシエーションを有効にする例を示します。

```
                switch# show interface e1/7 st

--------------------------------------------------------------------------------
                Port          Name               Status    Vlan      Duplex  Speed
Type

--------------------------------------------------------------------------------
                Eth1/7        --                 connected routed    full    25G
SFP-H25GB-CU1M
                switch# conf
                switch(config)# int e1/7
                switch(config-if)# negotiate auto 25000
```

インターフェイスの自動ネゴシエーションのディセーブル化

no negotiate auto コマンドを使用することにより、自動ネゴシエーションをディセーブルにすることができます。自動ネゴシエーションをディセーブルにするには、次の手順を実行します。

手順

ステップ 1 グローバル構成モードを開始します。

例：

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

ステップ 2 **interface ethernet** *port number* コマンドを使用してインターフェイスの自動ネゴシエーションをディセーブルにします。

例：

```
switch# int e1/7
switch(config-if)#
```

ステップ 3 **no negotiate auto** *port speed* コマンドを使用してインターフェイスの自動ネゴシエーションをディセーブルにします。

例：

```
switch(config-if)# no negotiate auto 25000
switch(config-if)#
```

（注）
適切に動作させるには、リンクの両端でこのコマンドを実行する必要があります。

設定したインターフェイスで自動ネゴシエーションが無効になっている。インターフェイスは、指定した速度で動作します。

例

ここではインターフェイスで自動ネゴシエーションをディセーブルにする例を示します。

```
                switch# sh int e1/7 st

--------------------------------------------------------------------------------
                Port          Name               Status    Vlan      Duplex  Speed
Type

--------------------------------------------------------------------------------
                Eth1/7        --                 connected routed    full    25G
SFP-H25GB-CU1M
                switch# conf
                switch(config)# int e1/7
```

```
switch(config-if)# no negotiate auto 25000
```

基本インターフェイスパラメータの表示のためのコマンド

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。

これらのコマンドは、基本インターフェイスのパラメータと状態に関する情報を表示します。

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

インターフェイスカウンタは、次のネットワーク モニタリング メトリックです。

- ネットワーク インターフェイス上のデータパケットとエラーに関する統計情報を記録する
- ネットワーク管理者がネットワークの問題を特定およびトラブルシューティングするのを支援する。
- パフォーマンスの追跡とキャパシティプランニングを可能にする

追加情報

インターフェイスカウンタは、インターフェイスごとに入出力パケット、エラー、廃棄、およびその他のイベントを追跡します。これらは、ネットワークの問題を診断し、経時的なトラフィックパターンを分析するために不可欠です。

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。

統計情報のサンプリング間隔の設定

サンプリング間隔では、スイッチがトラフィック モニタリングに関連する統計情報を収集する頻度をカスタマイズできます。

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。インターフェイス統計情報のサンプリング間隔を構成するには、次の手順を活用します。

手順

ステップ 1 グローバル構成モードを開始します。 **configure terminal**

例：

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

ステップ 2 **interface ethernet** *slot/port* コマンドを使用します。

例：

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

ステップ 3 **load-interval counters** [**1** | **2** | **3**] *seconds* コマンドを使用して、ビット レートとパケット レート統計の 1 つまたは複数のサンプリング間隔を構成します。

例：

```
switch(config)# load-interval counters 1 100
switch(config)#
```

各カウンタでは、これらのデフォルト値が使用されます。

- 1：30 秒（VLAN の場合は 60 秒）
- 2：300 秒
- 3：未設定。

ステップ 4 （任意） **show interface** *interface* コマンドを使用してインターフェイス統計を表示します。

例：

```
switch(config)# show interface ethernet 2/2
switch#
```

ステップ 5 インターフェイス モードを終了します。

例：

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

ステップ 6 （任意） 実行中の構成をスタートアップ構成に保存します。

例：

```
switch(config)# copy running-config startup-config
```

指定されたインターフェイスが、設定されたサンプリング間隔を使用してトラフィック統計情報を収集するようになりました。

例

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 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。 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、構成モードまたはインターフェイス構成モードで実行できます。

手順

ステップ 1 **clear counters interface** [**all** | コマンドを使用して、インターフェイスでインターフェイス カウンタをクリアします。 ethernet スロット/ポート| **loopback** 番号 | **mgmt** 番号 | **port channel** *channel-number*] 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。

例：

```
switch# clear counters ethernet 2/1
switch#
```

ステップ 2 （任意） **show interface** *interface* コマンドを使用してインターフェイスのステータスを確認します。

例：

```
switch# show interface ethernet 2/1
switch#
```

ステップ 3 **show interface** [**ethernet** *slot/port* | **port channel** *channel-number*] **counters** コマンドを使用して、インターフェイス カウンタがリセットされることを確認します。

例：

```
switch# show interface ethernet 2/1 counterswitch#
```

指定されたインターフェイスのインターフェイス カウンタ統計情報がリセットされます。

例

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#
```

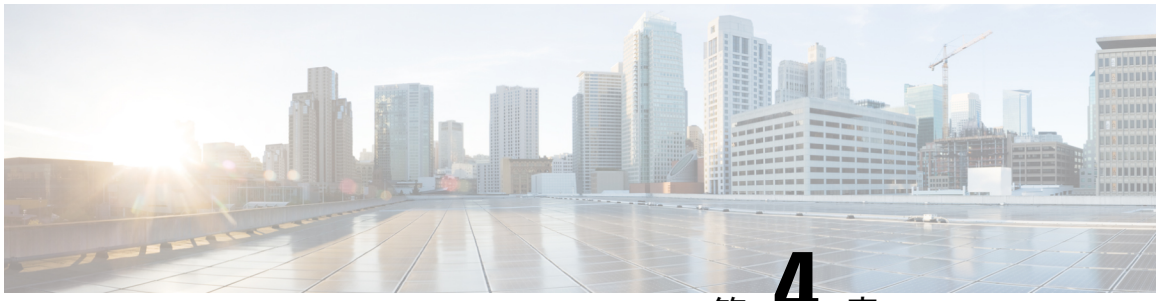
例： Cisco Nexus 9396PX スイッチでの QSA の構成

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

例： **Cisco Nexus 9396PX** スイッチでの **QSA** の構成



第 4 章

レイヤ 2 インターフェイスの設定

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 インターフェイスの概要

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。

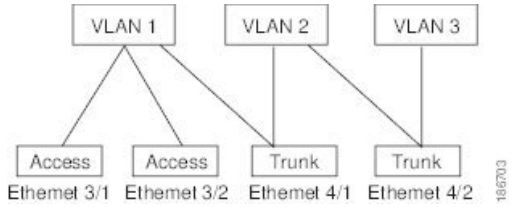
デフォルトでは、Cisco Nexus 9300-EX スイッチのすべてのポートはレイヤ 3 ポートであり、Cisco Nexus 9300 スイッチのすべてのポートはレイヤ 2 ポートです。

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。

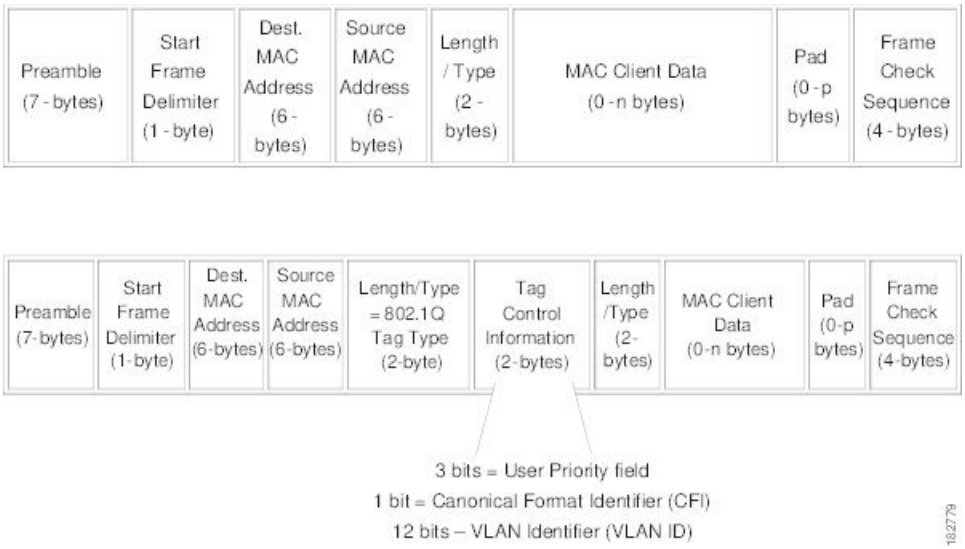
IEEE 802.1Q カプセル化

（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



ドロップ適性インジケータ

Nexus 9000 スイッチは DEI ビットが 1 に設定されたフレームを受信すると、そのまま次のホップに転送されます。たとえば、ネクスト ホップが Nexus 6000 の場合、dot1q ヘッダーで DEI ビットが 1 に設定されたパケットを受信すると、フレームがドロップされます。

Cisco Nexus NX-OS リリース 10.2(3)F 以降、DEI ビットが 1 に設定されたフレームが受信されるたびに、DEI ビットがクリアされます。

以下は DEI ビットをリセットするための構成です。

```
switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# system default reset-dei
switch(config)
```

以下は DEI ビットを設定するための構成です。

```
switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# no system default reset-dei
switch(config)
```

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。

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。

高可用性

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。

カウンタ値

設定、パケットサイズ、増分カウンタ値、およびトラフィックについては、次の情報を参照してください。

設定	パケット サイズ	増分カウンタ	トラフィック
L2 ポート：MTU 設定なし	6400 および 10000	ジャンボ、ジャイアント、および入力エラー	Dropped

設定	パケット サイズ	増分カウンタ	トラフィック
L2 ポート：ネットワーク QoS 設定のジャンボ MTU 9216	6400	Jumbo	Forwarded
L2 ポート：ネットワーク QoS 設定のジャンボ MTU 9216	10000	ジャンボ、ジャイアント、および入力エラー	Dropped
network-qos 設定のデフォルト レイヤ 3 MTU およびジャンボ MTU 9216 のレイヤ 3 ポート	6400	Jumbo	パケットは CPU にパントされ（CoP P設定の対象）、フラグメント化されてから、ソフトウェアによって転送されます。
network-qos 設定のデフォルト レイヤ 3 MTU およびジャンボ MTU 9216 のレイヤ 3 ポート	6400	Jumbo	パケットは CPU にパントされ（CoP P設定の対象）、フラグメント化されてから、ソフトウェアによって転送されます。
network-qos 設定のデフォルト レイヤ 3 MTU およびジャンボ MTU 9216 のレイヤ 3 ポート	10000	ジャンボ、ジャイアント、および入力エラー	Dropped
network-qos 設定のジャンボ レイヤ 3 MTU およびジャンボ MTU 9216 のレイヤ 3 ポート	6400	Jumbo	フラグメンテーションなしで転送されます。
network-qos 設定のジャンボ レイヤ 3 MTU およびジャンボ MTU 9216 のレイヤ 3 ポート	10000	ジャンボ、ジャイアント、および入力エラー	Dropped
ジャンボ レイヤ 3 MTU およびデフォルト L2 MTU 設定のレイヤ 3 ポート	6400 および 10000	ジャンボ、ジャイアント、および入力エラー	Dropped

（注）
- CRC 正常の 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。
- CRC 不良の 64バイト未満のパケット：runts カウンタが増加します。
- CRC 不良の 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 インターフェイスの前提条件

レイヤ 2 インターフェイスには次の前提条件があります。

- 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** コマンドを使用すれば、ポート モードを変更できます。
- **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ガイドラインおよび制約事項

VLAN トランキングには次の設定上のガイドラインと制限事項があります。

- Cisco Nexus 9000 シリーズ スイッチには、グローバルに設定できる **vlan dot1q tag native** コマンドがあります。これにより、設定されたトランク ポートのネイティブ VLAN がタグ付けされます。ただし、Catalyst 6500やサードパーティ製スイッチなどの接続されたスイッチでは、同様の設定が有効になっていない可能性があります。これにより、予期しない動作が発生する可能性があります。したがって、接続されたスイッチで設定されていない場合は、**vlan dot1q tag native** コマンドを無効にすることをお勧めします。
- ネイティブ VLAN を使用した SVI インターフェイスの BFD セッションは、Cisco Nexus 9300-X クラウド スケール スイッチでの **vlan dot1q tag native** コマンド構成ではサポートされていません。
- 自動ネゴシエーションは、N9K-X9636C-R、N9K-X9636C-RX、およびN9K-X9636Q-R ラインカードを搭載した Cisco Nexus 9508 プラットフォーム スイッチではサポートされません。
- 自動ネゴシエーションは、10/25/40/100直接接続銅ケーブルでのみサポートされます。
- BaseTポートでは自動ネゴシエーションを無効にできません。

- オートネゴシエーションは、光ファイバベースの光ファイバでは使用されません。
- Cisco NX-OS リリース9.2(1)以降では、N9K-X96136YC-R ライン カードを搭載した Cisco Nexus 9508 プラットフォーム スイッチは、48 ポートすべてで 1 ギガビットの速度をサポートします。ただし、自動ネゴシエーションはサポートされていないため、ケーブルを取り外しても 1000BASE-T SFP リンクが起動します。
- Cisco NX-OS リリース9.2(1)以降では、ネイティブ 25G ポートでの自動ネゴシエーションが、Cisco Nexus N9K-X97160YC-EX、N9K-C93180YC-FX、N9K-C93240YC-FX2、および N9K-C93240YC-FX2-Z スイッチでサポートされます。

（注） 自動ネゴシエーションは Cisco Nexus N9K-C92300YC スイッチではサポートされていません

- キーワードが付いている **show** コマンドはサポートされていません。 **internal**
- 自動ネゴシエーションは、Cisco Nexus 9200 および 9300-FX プラットフォーム スイッチ、および N9K-X9700-EX ラインカードを使用する Cisco Nexus 9500 プラットフォーム スイッチ上の 25-G イーサネット トランシーバ モジュールではサポートされません。
-
- QSA を使用した自動ネゴシエーション（40 G/100 G）および 1 GB は、次のポートではサポートされません。
  - Cisco Nexus 9336C-FX2 スイッチ：ポート 1 ー 6 および 33 ー 36
  - Cisco Nexus 9364C スイッチ
  - Cisco Nexus 93240YC-FX2 スイッチ：ポート 51 ー 54
  - Cisco Nexus 9788TC ライン カード：ポート 49 ー 52

（注） これらのポートで銅線ケーブルを使用する場合は、ピア速度を設定する必要があります。

- 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。
- 中継スイッチとして動作する ASE2 および ASE3 ベースの Cisco Nexus 9000 シリーズ スイッチは、二重タグ付きパケットの内部タグを保持しません。

  次の CLI は、LSE ベースの Cisco Nexus 9000 シリーズ スイッチでのみ必須です。Q-in-Q カプセル化またはカプセル化解除の要件を持たない、SP クラウド内の純粋な中継ボックス上ですべての VLAN タグをシームレスにパケット転送し、保持するには、CLIコマンド、 **system dot1q-tunnel transit** を設定します。CLI を削除するには、 **no system dot1q-tunnel transit** CLI コマンドを使用します。

スイッチで実行される CLI の注意事項は次のとおりです。

- トランク ポートから出力される L2 フレームは、ポート上のネイティブ VLAN でもタグ付けされます。
- 他のトンネリング メカニズム（VXLAN や MPLSなど）は、設定された CLI では機能しません。

- 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。
- clear mac address-table dynamic コマンドを使用して VLAN の MAC アドレスをクリアすると、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上にスタティックARPエントリが存在し、MACアドレスからポートへのマッピングが存在しない場合、スーパーバイザはARP要求を生成してMACアドレスを学習できます。MACアドレスを学習すると、隣接エントリは正しい物理ポートをポイントします。
- Cisco NX-OSは、SVIの1つがBIA MAC（バーンドインMACアドレス）を使用してCisco Nexus 9000上にある場合、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、BIA MACがSVI / VLAN間で共有される場合に発生します。BIA MACとは異なるMACを、トランスペアレントブリッジングが正しく動作するようにSVIで設定できます。

（注） この動作は、Cisco Nexus 9300 スイッチ（ネットワーク転送エンジン）および 95xx、96xx、94xx ライン カードを搭載した Cisco Nexus 9500 スイッチに適用されます。この動作は、Cisco Nexus 9200 スイッチ、Cisco Nexus 9300-EX および 9700-EX ライン カードを搭載した Cisco Nexus 9500 スイッチには適用されません。

- ポートローカルVLANは、ファブリックエクステンダ（FEX）をサポートしていません。
-
- インターフェイス モードをトランク VLAN とトランク VLAN に同時に設定しようとすると、エラー メッセージが表示されることがあります。Cisco NX-OS インターフェイスでは、インターフェイス モードのデフォルト値は access です。トランク関連の設定を実装するには、最初にインターフェイス モードを trunk に変更してから、トランク VLAN 範囲を設定する必要があります。
- vPC セットアップでは、VLAN が vPC VLAN の場合、VLAN およびシステムの MAC アドレス制限はサポートされません。
- インターフェイス、VLAN、システムで MAC アドレス テーブル制限が有効になっている場合は、既存のすべての MAC がフラッシュされ、再学習される可能性があります。
- vPC PO で有効になっている MAC アドレス テーブル制限は、両方のピアで一貫している必要があります。
- システム、ポート、および VLAN の MAC アドレス テーブル制限を一度に、または任意の組み合わせで設定すると、それぞれが設定されたとおりに MAC を制限します。プリファレンスは常に次の順序になります。
  - ポート
  - VLAN
  - システム
- MAC アドレス テーブルの制限は、vPC ピア リンクではサポートされていません。
- 設定可能な MAC アドレステーブルの最小値は 100 で、設定可能な最大値は 196000 です。
- インターフェイスまたは VLAN がセットアップから削除されると、関連する MAC アドレス テーブル制限の設定も削除されます。
- MAC アドレス テーブルの制限は、PVLAN インターフェイス タイプではサポートされません。
- MACアドレス テーブルの制限を超えると、デフォルトでトラフィックがフラッディングされます。
- Cisco Nexus N9K-C93180YC-FX3S スイッチまたは N9K-X9716D-GX ライン カードを搭載した Cisco Nexus 9500 スイッチのポートに FET-10G ファブリックエクステンダ トランシー

バを接続すると、 **switchport mode fex-fabric** コマンドを使用しても、ポートはファブリック ポートに変換されません。

- Cisco NX-OS リリース 10.2(1q)F 以降では、レイヤ2 (L2) インターフェイスは N9K-C9332D-GX2B プラットフォームスイッチでサポートされます。
- Cisco NX-OS リリース10.1(2) 以降、レイヤ 2 インターフェイスは、Cisco Nexus N9K-X9624D-R2 ライン カードでサポートされます。
- Cisco Nexus リリース 9.3(X) の場合、Cisco Nexus N9K-C93600CD-GX、N9K-C9364C-GX スイッチには次のガイドラインと制約事項があります。
  - Cisco Nexus NX-OS Release 10.1(2) 以降では、NX-OS N9K-C93600CD-GX、N9K-C9316D-GX、および N9K-C9364C-GX の速度 40G および 100G で自動ネゴシエーションがサポートされています。
  - Cisco Nexus 9300-GX プラットフォーム スイッチは、50Gx2 ブレークアウト ポートの 2 番目のレーンで FC-FEC をサポートしません。50Gx2 ブレークアウトが設定されている場合、2 番目のブレークアウト ポートはリンクアップしません。回避策：50Gx2 ブレークアウトで RS-FEC を設定します。
  - N9K-C9316D-GX の場合：ポート 1 ー 16 は QSA で 400G/100G/40G および 10G をサポートします。
  - N9K-C93600CD-GX の場合：ポート 1 ～ 24 の場合、4 個のポート（1-4、5-8、9-12 など「クアッド」と呼ばれます）はすべて、同じ速度で動作します。クワッド内のすべてのポートは、10G、または 40G または 100G で動作します。同じクワッド内では混合速度はサポートされません。QSAでは、クワッド内のすべてのポートが 10G の速度で動作できます。ポート 25 ー 26 は同じ速度で動作し、ポート 27 ー 28 は同じ速度で動作します。ポート 25 ー 26 または 27 ー 28 の速度の不一致はサポートされていません。

  N9K-C9364C-GXの ガイドラインと制約は次のとおりです。
  - ポート 1 ～ 64 の場合、4 個のポート（1-4、5-8、9-12 など「クアッド」と呼ばれます）はすべて、同じ速度で動作します。クワッド内のすべてのポートは、10G、または 40G または 100G で動作します。
  - 同じクワッド内では混合速度はサポートされません。
  - QSAでは、クワッド内のすべてのポートが 10G の速度で動作できます。
- Cisco NX-OS リリース 10.4（1）F 以降、L2 転送は Cisco Nexus 9332D-H2R プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.4（2）F 以降、L2 転送は Cisco Nexus 93400LD-H1 プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.4（3）F 以降、L2 転送は Cisco Nexus N9KC9364C-H1 プラットフォームスイッチでサポートされます。

- Cisco NX-OS リリース 10.4（1）F 以降、L2 インフラは Cisco Nexus 9332D-H2R プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.4（2）F 以降、L2 インフラは Cisco Nexus 93400LD-H1 プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.4（3）F 以降、L2 インフラは Cisco Nexus N9KC9364C-H1 プラットフォームスイッチでサポートされます。
- Cisco NX-OS リリース 10.4（2）F 以降、SFP-25G-ER-I トランシーバ モジュールは Cisco Nexus C93180YC-FX3 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4（3）F 以降で、ブレークアウト（4x10G、4x25G、 および 4x100G）ポート サポートは、X98900CD-A スイッチで提供されます。

  4x25 ブレークアウトは、以下のポートでのみサポートされます。サポートされるポートは、2、3、5、6、8、9、11、12、14、15、17、18、20、21、23、24、26、27、29、30、32、33、35、36 、38、39、41、42、44、45、47 および 48 です
- Cisco NX-OS リリース 10.4（3）F 以降、X98900CD-A および X9836DM-A のすべてのポートは、400EG ポートを備えた 2x200GE ブレークアウトをサポートします。
- Cisco NX-OS リリース 10.4（3）F 以降、X98900CD-A は 3、6、9、12、15、18、21、27、30、33、36、39、42、および 45 ポートでサポートされます。

（注） Cisco NX-OS リリース 10.2(2)F では、N9K-C93180YC-FX3S、N9K-C93180YC-FX3 スイッチの SFP-10G-TX モジュールのリンク アップ時間は 13 秒です。

に関する注意事項と制限事項 Cisco Nexus 93C64E-SG2-Q スイッチ

Cisco NX-OS リリース 10.2（2）F以降、Cisco Nexus 93C64E-SG2-Q スイッチ は以下のレイヤ 2 機能をサポートしています：

- 100G、400G、800G のポート速度
- レイヤ 2 アクセス ポートとトランク ポート、およびポート チャネル
- SVI および VLAN 論理インターフェイス
- 診断およびスパース レイヤ 2 モード用の VLAN
- デフォルトのポートチャネル ロードバランシング
- VLAN、SVI、およびレイヤ 2 とレイヤ 3 の両方の仮想ネットワーク インターフェイスの統計情報
- ブロードキャスト、ユニキャスト、およびマルチキャスト パケットのレイヤ 2 フラッディングをサポート

具体的な統計とスケールの情報については、『検証済みスケーラビリティ ガイド』を参照してください。

Cisco N9336C-SE1 スイッチ上の注意事項と制限事項

Cisco NX-OS リリース 10.6(1)F以降、Cisco Nexus 9336C-SE1 は以下のレイヤ 2 機能をサポートしています。

- 単一方向リンク検出（UDLD）
- レイヤ 2 アクセス ポートとトランク ポート
- ポート プロファイル
- スイッチ仮想インターフェイス（SVI）およびVLAN論理的なインターフェイス
- LACP およびポート チャネル
- 仮想ポート チャネル（vPC）
- ネイティブ VLAN トラフィックのタギング
- 予約済み VLAN
- Q-in-Q VLANトンネル

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。

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。

始める前に

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface 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

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

例

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。

始める前に

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface ethernet** *type slot/port* 例：	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
	switch(config)# **interface ethernet 3/1** switch(config-if)#	
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。
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。

例

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。

始める前に

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** {*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

	コマンドまたはアクション	目的
		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。

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。

例

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)#
```

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、指定されたポートの現在のVLANリストを新しいリストに置き換えます。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ため、**terminal dont-ask** を使用してプロンプトを無効にできます。 コマンドを入力してから、設定を貼り付けます。

始める前に

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** {**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

	コマンドまたはアクション	目的
		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。

例

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)#
```

ポートでの MAC アドレス制限の設定

Cisco NX-OS リリース 9.2(3) 以降、N9K-X9636C-RX、N3K-C3636C-R、およびN3K-C36180YC-R ライン カードを搭載した Cisco Nexus 9500 シリーズスイッチでは、各ポートが学習する MAC

アドレス数の上限を設定できます。たとえば、指定された VLAN での制限が 2000 の MAC である場合、レイヤ 2 フォワーディング マネージャ（L2FM）は、受信した最初の 2000 の MAC を受け入れ、残りの MAC を拒否します。インターフェイスの MAC アドレスの制限を設定するには、次の手順を実行します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **mac address-table limit interface port-channel** *value*
3. switch(config)# **show mac address-table limit interf**
4. switch(config)# **exit**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **mac address-table limit interface port-channel** *value*	ポート レベルで MAC 学習の上限を指定します。
ステップ 3	switch(config)# **show mac address-table limit interf**	MAC 制限が設定されているインターフェイスのリストを表示します。
ステップ 4	switch(config)# **exit**	コンフィグレーション モードを終了します。

例

次に、ポートレベルでの MAC 学習の上限を設定する例を示します。

```
switch# configure terminal
switch(config)# mac address-table limit interface port-channel 2 1000
Configuring Mac address limit will result in flushing existing Macs in the specified
VLAN/System.Proceed(yes/no)? [no]  yes
switch(config)# exit
```

次に、MAC アドレスの制限を表示する例を示します。

```
switch# configure terminal
switch(config)# show mac address-table limit interf
Interface    Conf Limit     Curr Count    Cfg Action    Currently
-----------    ------------   ---------     ---------    --------
Vlan1              196000             0           Flood         Flooding Unknown SA
Vlan341            196000             0           Flood         Flooding Unknown SA
Vlan342            196000             0           Flood         Flooding Unknown SA
Vlan343            196000             0           Flood         Flooding Unknown SA
Vlan344            196000             0           Flood         Flooding Unknown SA
Vlan345            196000             0           Flood         Flooding Unknown SA
```

```
Vlan346             196000              0           Flood         Flooding Unknown SA
Vlan347             196000              0           Flood         Flooding Unknown SA
Vlan348             196000              0           Flood         Flooding Unknown SA
Vlan349             196000              0           Flood         Flooding Unknown SA
Vlan350             196000              0           Flood         Flooding Unknown SA
port-channel1       196000              0           Flood         Flooding Unknown SA
port-channel2       1000                0           Flood         Flooding Unknown SA
port-channel11      196000              0           Flood         Flooding Unknown SA
port-channel12      196000              0           Flood         Flooding Unknown SA
port-channel13      196000              0           Flood         Flooding Unknown SA
port-channel601     196000              0           Flood         Flooding Unknown SA
port-channel603     196000              0           Flood         Flooding Unknown SA
port-channel888     196000              0           Flood         Flooding Unknown SA
Ethernet1/6         196000              0           Flood         Flooding Unknown SA
Ethernet1/15        196000              0           Flood         Flooding Unknown SA
Ethernet1/35        196000              0           Flood         Flooding Unknown SA
BF2(config)#
switch(config)# exit
```

スイッチポート分離の設定

インターフェイス上で最大 3967 の VLAN に対応するように、インターフェイス上でスイッチポート分離を設定できます。分離されたスイッチポートで設定されたインターフェイスは、STP BPDU を送信しません。

（注） **スイッチポート独立**モードは、FEX、スイッチ、ルータ、またはその他のネットワーキングデバイスに接続されたインターフェイスではサポートされません。スイッチポート分離は、FEX HIF ポートではサポートされていません。

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

手順

	コマンドまたはアクション	目的

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

	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`
	`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。
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。

速度グループが設定されている場合、**default interface** コマンドは次のエラーを表示します。

```
Error: default interface is not supported as speed-group is configured
```

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**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** コマンドを使用し、キーワードを使用して、設定を消し去ってしまう前にインターフェイスの実行コンフィギュレーションを保存します。

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。

例

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)#
```

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） この項で説明している **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

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定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） **system default interface-vlan autostate** コマンドを使用し、 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。

	コマンドまたはアクション	目的
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。

例

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

手順

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的
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。

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。

例

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 global 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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**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

	コマンドまたはアクション	目的
		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。

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。

例

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#
```

16 スロット シャーシの 50 G インターフェイスのインターフェイス ブレークアウト プロファイルの設定

インターフェイス ブレークアウト プロファイルは、-EX ライン カード用の Cisco Nexus 9516 スイッチで、高帯域幅の 100-G ポートを 2 つの 50-G インターフェイスに分割するために必要です。

手順の概要

1. **configure terminal**

2. （任意） **interface breakout-profile 50g-2x-only**
3. **copy running-config startup-config**
4. **reload**
5. **interface breakout module** *module-number* **port** *port-range* **map [10g-4x | 25g-4x | 50g-2x]**

手順の詳細

手順

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

ステップ 2	（任意） **interface breakout-profile 50g-2x-only**
	例：
	`switch(config)# interface breakout-profile 50g-2x-only`
	`Warning: Please save config and reload the switch for breakout-profile config to take effect`
	`Please save config and reload the switch for the configuration to take effect`
		このコマンドは、スロット 8ー16 をブレークアウトするために必要です。スロット 1 ー 7 には必要ありません。

ステップ 3	**copy running-config startup-config**
	例：
	`switch(config-inf)# copy running-config startup-config`
	`[########################################] 100%`
	`Copy complete, now saving to disk (please wait)...`
	`Copy complete.`
		実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ステップ 4	**reload**
	例：
	`switch(config-inf)# reload`
	`This command will reboot the system. (y/n)? [n] y`
		スイッチをリブートします。
		（注）
		スイッチがリロードされ、モジュールが起動したら、ブレークアウトするモジュールまたはポートについて次の CLI を入力します。

ステップ 5	**interface breakout module** *module-number* **port** *port-range* **map [10g-4x | 25g-4x | 50g-2x]** 例： `switch(config)# interface breakout module 1 port 1-32 map 50g-2x`	100 Gb ポートを 2 つの 50 Gb ポートに分割します。*module-number* の範囲は 1 ー 30 です。*port-range* の範囲は 1 ～ 72 です。

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

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定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） クライアントが **system default switchport shutdown** コマンドが発行されます。 • **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。

例

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)#
```

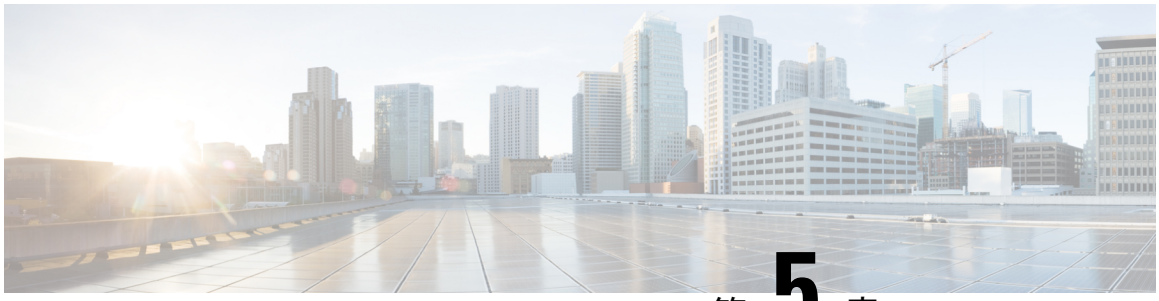
次に、レイヤ 2 トランク インターフェイスを設定してネイティブ VLAN および許容 VLAN を割り当て、デバイスにトランク インターフェイスのネイティブ VLAN トラフィックのタグを設定する例を示します。

```
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*』
高可用性	『*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 のデフォルト 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」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。

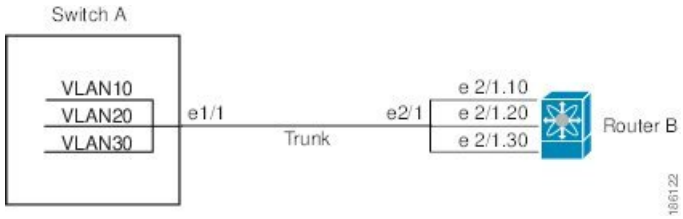
サブインターフェイスの名前は、親インターフェイスの名前（たとえば Ethernet 2/1）+ ピリオド（.）+そのインターフェイス独自の番号です。たとえば、イーサネット インターフェイス 2/1 に Ethernet 2/1.1 というサブインターフェイスを作成できます。この場合、.1 はそのサブインターフェイスを表します。

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。

VLAN インターフェイス

VLAN インターフェイス、またはスイッチ仮想インターフェイス（SVI）、は、デバイス上の VLAN を同じデバイス上のレイヤ 3 ルータ エンジンに接続する仮想ルーテッド インターフェイスです。VLAN に関連付けることができる VLAN インターフェイスは 1 つだけです。

ただし、VLAN に VLAN インターフェイスを構成する必要があるのは、VLAN 間でルーティングする場合か、または管理 VRF（仮想ルーティング/転送）以外の VRF インスタンスを経由してデバイスを IP ホスト接続する場合だけです。VLAN インターフェイスの作成を有効にすると、Cisco NX-OS によってデフォルト VLAN（VLAN 1）に VLAN インターフェイスが作成され、リモート スイッチ管理が許可されます。

VLAN ネットワーク インターフェイス機能を有効にしてから **feature interface-vlan** を構成します。システムはこの機能をディセーブルにする前のチェックポイントを自動的に取得するため、このチェックポイントにロールバックできます。ロールバックおよびチェックポイントについては、『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』を参照してください。

（注） **feature interface-vlan** 構成は、Nexus 9800スイッチでは使用できません。

レイヤ 3 VLAN 間ルーティング

VLAN インターフェイスでトラフィックをルーティングするには、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。

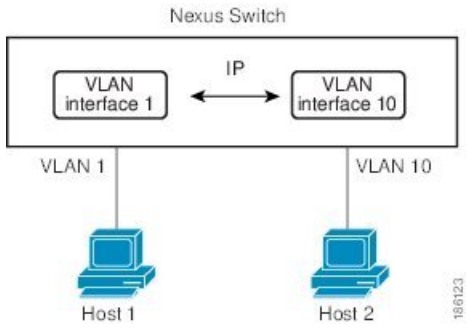
IP アドレスおよび IP ルーティングの詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

2 つの VLAN インターフェイスの接続

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。

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。

図 *5: VLAN* インターフェイスによる *2* つの *VLAN* の接続



（注） VLAN 1 の VLAN インターフェイスは削除できません。

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。

高可用性

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。

レイヤ 3 スタティック MAC アドレス

スタティック MAC アドレスは、次のレイヤ 3 インターフェイスに設定できます。

- レイヤ 3 インターフェイス
- レイヤ 3 サブインターフェイス
- レイヤ 3 ポート チャネル
- VLAN ネットワーク インターフェイス

（注） トンネル インターフェイスにはスタティック MAC アドレスを設定できません。

レイヤ 3 インターフェイスの前提条件

レイヤ 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。

レイヤ 3 インターフェイスの注意事項および制約事項

レイヤ 3 インターフェイスの構成には次の注意事項と制約事項があります：

- キーワードが付いている **show** コマンドはサポートされていません。 **internal**
- ポートチャネルのメンバーシップに構成されている物理インターフェイスで、サブインターフェイスを構成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自体の下にサブインターフェイスを構成する必要があります。
- 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構成する場合、Dynamic Host Configuration Protocol（DHCP）オプションはサポートされません。
- Cisco NX-OS リリース 10.5（2）F 以降、IP アンナンバード は Cisco Nexus 9808 と 9804 スイッチでサポートされます。
- Cisco NX-OS リリース 10.5（2）F 以降では、非 SVI インターフェイスでもに IP アンナンバード機能がサポートされます。

- X9700-EX および X9700-FX ライン カードを搭載した Cisco Nexus 9500 シリーズ スイッチの SVI およびサブインターフェイスの IPv6 カウンタはサポートされていません。
- SVI とサブインターフェイスの両方のマルチキャストおよびブロードキャスト カウンタはサポートされていません。
- SVI とサブインターフェイスの両方のカウンタのコントロールプレーン SVI/SI トラフィックはサポートされません。
- Cisco NX-OS リリース 9.3（6）以降では、Cisco Nexus N9K-C9336C-FX2 および N9K-C93240YC-FX2 スイッチでサブインターフェイス マルチキャストおよびブロードキャスト カウンタがサポートされています。
- サブインターフェイスのマルチキャストおよびブロードキャスト カウンタを有効にすると、SVI、レイヤ 2 VLAN、MPLS カウンタが機能しない場合があります。
- この統計情報では、最大 1000 個のサブインターフェイスがサポートされます。
- Cisco NX-OS リリース 10.2（2）F以降、 Cisco Nexus 93C64E-SG2-Q スイッチ はこれらのレイヤ 3 インターフェイスをサポートします。
  - レイヤ 3 物理インターフェイスおよび物理サブインターフェイス
  - レイヤ 3 ポート チャネルおよびポート チャネル サブインターフェイス
  - ルーテッド ポート
  - ブレークアウトポート
- Cisco NX-OS リリース 10.2（1q）F 以降では、レイヤ3（L3）インターフェイスは N9K-C9332D-GX2B プラットフォームスイッチでサポートされます。
- Cisco NX-OS リリース 10.1（2）以降、レイヤ 3 インターフェイスは Cisco Nexus N9K-X9624D-R2 ライン カードでサポートされます。
- Cisco NX-OS リリース 10.3(1)F 以降、Cisco Nexus 9808 プラットフォーム スイッチで L3、ループバック、サブインターフェイスのサポートが提供されます。
- Cisco NX-OS リリース 10.4（1）F 以降、Cisco Nexus 9804 プラットフォーム スイッチで L3、ループバック、サブインターフェイスのサポートが提供されます。
- Cisco NX-OS リリース 10.3(1)F 以降、Cisco Nexus 9808 プラットフォーム スイッチで L3 物理およびサブインターフェイスのサポートが提供されます。
- Cisco NX-OS リリース 10.4（1）F 以降、Cisco Nexus 9804 プラットフォーム スイッチで L3 物理およびサブインターフェイスのサポートが提供されます。
- Cisco NX-OS リリース 10.4（2）F 以降、Cisco Nexus C9232E-B1 プラットフォーム スイッチで以下の機能がサポートされます。
  - レイヤ 3、ループバック、およびサブインターフェイスのサポート

- 統計情報のサポートは、レイヤ3物理インターフェイスとサブインターフェイスで提供されます。

- Cisco Nexus 9800プラットフォームスイッチには、L3物理およびサブインターフェイスのサポートに関して次の制限があります。
  - ブロードキャストはサポートされていません。
  - **hardware profile sub-interface flex-stats** コマンドは適用されません。
  - サブインターフェイスの統計情報は、親インターフェイスに集約されません。
- Cisco NX-OSリリース10.4（1）F以降、L3転送はCisco Nexus 9332D-H2R プラットフォーム スイッチでサポートされます。
- Cisco NX-OSリリース10.4（2）F以降、L3転送はCisco Nexus 93400LD-H1プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.4（3）F以降、L3転送は Cisco Nexus N9KC9364C-H1 プラットフォームスイッチでサポートされます。
- Cisco NX-OS リリース 10.4（1）F以降では、Cisco Nexus 9808および9804スイッチを搭載したN9KX98900CD-AおよびN9KX9836DM-Aライン カードのL3物理およびサブインターフェイスに対して統計情報のサポートが提供されます。

（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 *10*: レイヤ *3*インターフェイスのデフォルト パラメータ

パラメータ	デフォルト
管理ステート	閉じる

レイヤ3インターフェイスの設定

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

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定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)#`
		インターフェイス設定モードを開始します。

ステップ 3	**no switchport** 例： `switch(config-if)# no switchport`	そのインターフェイスを、レイヤ 3 インターフェイスとして設定します。

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：	（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

	コマンドまたはアクション	目的
	switch# switch(config-if)# **int e2/1** switch(config-if)# **no shutdown**	き、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 7	**copy running-config startup-config** 例： switch(config)# **copy running-config startup-config**	（任意）この設定の変更を保存します。

例

- **medium** コマンドを使用し、 コマンドを使用します。

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

（注） デフォルト設定は、**broadcast** です。、およびこの設定は、 **show** のいずれにも表示されません コマンドにも表示されません。ただし、設定を **p2pshow running config** を入力すると、この設定が表示されます。 コマンドを使用する必要があります。

- **switchport** コマンドを使用し、 コマンドを使用します。

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

- 次に、ルーテッド インターフェイスを設定する例を示します。

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

インターフェイスのデフォルト設定がルーテッドされます。レイヤ 2 にインターフェイスを設定するには、**switchport** を入力します コマンドを使用します。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。

始める前に

親インターフェイスをルーテッド インターフェイスとして設定します。

「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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface 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。number の範囲は 1 ～ 4094 です。

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。

	コマンドまたはアクション	目的
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 ー 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）この設定の変更を保存します。

例

- 次に、サブインターフェイスを作成する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1.1
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** の出力 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
```

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

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**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。

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

	コマンドまたはアクション	目的
		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）この設定の変更を保存します。

例

次に、VLAN インターフェイスを作成する例を示します。

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

レイヤ 3 インターフェイス上のスタティック MAC アドレスの設定

レイヤ 3 インターフェイスのスタティック MAC アドレスを設定できます。ブロードキャストまたはマルチキャストのアドレスは、スタティック MAC アドレスとして設定できません。

Note トンネル インターフェイス上には、スタティック MAC アドレスを設定できません。

Note この設定は、16のVLANインターフェイスに制限されます。追加のVLANインターフェイスに設定を適用すると、ハードウェアプログラムが失敗したインターフェイスがダウン状態になります。ステータス。

SUMMARY STEPS

1. **config t**
2. **interface** [**ethernet** *slot/port* | **ethernet** *slot/port.number* | **port-channel** *number* | **vlan** *vlan-id*]
3. **mac-address** *mac-address*
4. **exit**
5. (Optional) **show interface** [**ethernet** *slot/port* | **ethernet** *slot/port.number* | **port-channel** *number* | **vlan** *vlan-id*]
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`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** [**ethernet** *slot/port* | **ethernet** *slot/port.number* | **port-channel** *number* | **vlan** *vlan-id*] **Example:** `switch(config)# interface ethernet 7/3`	レイヤ 3 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。 **Note** スタティック MAC アドレスを割り当てる前に、レイヤ 3 インターフェイスを作成する必要があります。

ステップ 3	**mac-address** *mac-address*
	Example:
	`switch(config-if)# mac-address 22ab.47dd.ff89`
	`switch(config-if)#`
		レイヤ 3 インターフェイスに追加するスタティック MAC アドレスを指定します。

ステップ 4	**exit**
	Example:
	`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	(Optional) **show interface** [**ethernet** *slot/port* | **ethernet** *slot/port.number* | **port-channel** *number* | **vlan** *vlan-id*] **Example:** `switch# show interface ethernet 7/3`	レイヤ 3 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	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、スロット 7、ポート 3 上のレイヤ 3 インターフェイスにスタティック MAC アドレスを設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 7/3
switch(config-if)# mac-address 22ab.47dd.ff89
switch(config-if)#
```

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。

始める前に

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

手順の概要

1. **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

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**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 ー 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`
	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 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。

	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(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

例

次に、ループバック インターフェイスを作成する例を示します。

```
switch# configure terminal
switch(config)# interface loopback 0
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# copy running-config startup-config
```

ゲートウェイの SVI での PBR の設定

この手順では、ゲートウェイのプライマリ SVI インターフェイスで PBR を設定します。

（注） アンナンバードプライマリ/セカンダリ VLAN インターフェイスに PBR ポリシーを設定する場合は、ステップ 2 ー 6 が必要です。これは、SVI 機能の IP アンナンバードでは必須ではありません。

手順の概要

1. **configure terminal**
2. **ip access-list** *list-name*
3. **permit tcp host** *ipaddr* **host** *ipaddr* **eq** *port-number*
4. **exit**
5. **route-map** *route-map-name*
6. **match ip address** *access-list-name*
7. **set ip next-hop** *addr1*
8. **exit**
9. **interface vlan** *vlan-id*
10. **ip address** *ip-addr*
11. **no ip redirects**
12. （任意） **ip policy route-map pbr-sample**
13. **exit**
14. **hsrp version 2**
15. **hsrp***group-num*
16. **name** *name-val*
17. **ip** *ip-addr*
18. **no shutdown**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コ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 access-list** *list-name* 例： `switch(config)# ip access-list pbr-sample`	アクセス リストを設定します。
ステップ 3	**permit tcp host** *ipaddr* **host** *ipaddr* **eq** *port-number* 例： `switch(config-acl)# permit tcp host 10.1.1.1 host 192.168.2.1 eq 80`	特定のポートで転送するパケットを指定します。
ステップ 4	**exit** 例： `switch(config-acl)# exit`	コンフィギュレーション モードを終了します。
ステップ 5	**route-map** *route-map-name* 例： `switch(config)# route-map pbr-sample`	ルートマップを作成するか、ルートマップ コマンド モードを開始します。
ステップ 6	**match ip address** *access-list-name* 例： `switch(config-route-map)# match ip address pbr-sample`	ルーティング テーブルから値を一致させます。
ステップ 7	**set ip next-hop** *addr1* 例： `switch(config-route-map)# set ip next-hop 192.168.1.1`	ネクストホップの IP アドレスを設定します。
ステップ 8	**exit** 例： `switch(config-route-map)# exit`	コマンド モードを終了します。
ステップ 9	**interface vlan** *vlan-id* 例： `switch(config)# interface vlan 2003`	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 ー 4094 です。これはプライマリ VLAN です。

	コマンドまたはアクション	目的
ステップ 10	**ip address** *ip-addr* 例： `switch(config-if)# ip address 10.0.0.1/8`	インターフェイスに IP アドレスを設定します。
ステップ 11	**no ip redirects** 例： `switch(config-if)# no ip redirects`	すべてのアンナンバード プライマリおよびセカンダリ VLAN インターフェイスで設定する必要があります。
ステップ 12	（任意） **ip policy route-map pbr-sample** 例： `switch(config-if)# ip policy route-map pbr-sample`	アンナンバードプライマリ/セカンダリ VLAN インターフェイスに PBR ポリシーを適用する場合は、このコマンドを入力します。
ステップ 13	**exit** 例： `switch(config-if)# exit`	コマンド モードを終了します。
ステップ 14	**hsrp version 2** 例： `switch(config-if)# hsrp version 2`	HSRP バージョンを設定します。
ステップ 15	**hsrp***group-num* 例： `switch(config-if)# hsrp 200`	HSRP グループ番号を設定します。
ステップ 16	**name** *name-val* 例： `switch(config-if-hsrp)# name primary`	冗長名の文字列を設定します。
ステップ 17	**ip** *ip-addr* 例： `switch(config-if-hsrp)# ip 10.0.0.100`	IP アドレスを設定します。
ステップ 18	**no shutdown** 例： `switch(config-if-hsrp)# no shutdown`	シャットダウンを無効にします。

ゲートウェイの SVI セカンダリ VLAN での IP アンナンバードの設定

この手順では、ゲートウェイのセカンダリ SVI で IP アンナンバードを設定します。Cisco NX-OS リリース9.3(6) 以降、この機能は Cisco Nexus N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX スイッチでサポートされます。

手順の概要

1. **configure terminal**
2. **interface vlan** *vlan-list*
3. **ip unnumbered vlan** *primary-vlan-id*
4. （任意） **ip policy route-map pbr-sample**
5. **no ip redirects**
6. **hsrp version 2**
7. **hsrp** *group-num*
8. **follow** *name*
9. **ip** *ip-addr*
10. **no shutdown**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	コンフィギュレーション モードを入力します。
ステップ 2	**interface vlan** *vlan-list* 例： `switch(config)# interface vlan 2001`	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。指定できる範囲は 1 ～ 4094 です。これはセカンダリ VLANです。
ステップ 3	**ip unnumbered vlan** *primary-vlan-id* 例： `switch(config-if)# ip unnumbered vlan 2003`	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。
ステップ 4	（任意） **ip policy route-map pbr-sample** 例： `switch(config-if)# ip policy route-map pbr-sample`	アンナンバードプライマリ/セカンダリ VLAN インターフェイスに PBR ポリシーを適用する場合は、このコマンドを入力します。
ステップ 5	**no ip redirects** 例： `switch(config-if)# no ip redirects`	すべてのアンナンバード プライマリおよびセカンダリ VLAN インターフェイスで設定する必要があります。
ステップ 6	**hsrp version 2** 例： `switch(config-if)# hsrp version 2`	HSRP バージョンを設定します。

	コマンドまたはアクション	目的
ステップ 7	**hsrp** *group-num* 例： `switch(config-if)# hsrp 200`	HSRP グループ番号を設定します。
ステップ 8	**follow** *name* 例： `switch(config-if-hsrp)# follow primary`	従うグループを設定します。
ステップ 9	**ip** *ip-addr* 例： `switch(config-if-hsrp)# ip 10.0.0.100`	HRSP IPv4 を入力し、仮想 IP アドレスを設定します。
ステップ 10	**no shutdown** 例： `switch(config-if-hsrp)# no shutdown`	シャットダウンを無効にします。

SVI TCAM リージョンの設定

Cisco NX-OS リリース 9.3(3) 以降では、Cisco Nexus 3100 シリーズ スイッチの SVI インターフェイスでレイヤ 3 統計情報を表示できます。ハードウェアの SVI Ternary Content Addressable Memory（TCAM）領域のサイズを変更して、SVI インターフェイスのレイヤ 3 着信ユニキャスト カウンタを表示できます。

手順の概要

1. **hardware profile tcam region** {**arpacl** | **e-racl**} | **ifacl** | **nat** | **qos**} |**qoslbl** | **racl**} | **vacl** | **svi** } *tcam_size*
2. **copy running-config startup-config**
3. switch(config)# **show hardware profile tcam region**
4. switch(config)# **reload**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**hardware profile tcam region** {**arpacl**	**e-racl**}	**ifacl**	**nat**	**qos**} |**qoslbl**	**racl**}	**vacl**	**svi** } *tcam_size*	ACL TCAM リージョン サイズを変更します。 • **arpacl**：アドレス解決プロトコル（ARP）の ACL（ARPACL）TCAM リージョン サイズを設定します。

	コマンドまたはアクション	目的
		• **e-racl**：出力ルータ ACL（ERACL）TCAM リージョン サイズを設定します。 • **e-vacl**：出力の VLAN ACL（EVACL）TCAM リージョン サイズを設定します。 • **ifacl**：インターフェイス ACL（ifacl）TCAM リージョンサイズを設定します。エントリの最大数は 1500 です。 • **nat**：NAT TCAM リージョンのサイズを設定します。 • **qos**：Quality of Service（QoS）TCAM リージョン サイズを設定します。 • **qoslbl**：QoS ラベル（qoslbl）TCAM リージョン サイズを設定します。 • **racl**：ルータの ACL（RACL）TCAM リージョン サイズを設定します。 • **vacl**：VLAN ACL（VACL）TCAM リージョン サイズを設定します。 • *svi*：SVI TCAM リージョン サイズを設定します。この SVI TCAM のデフォルト サイズは 0 です。 • *tcam_size*：TCAM サイズ。有効な範囲は 0 ～ 2,147,483,647 エントリです。 （注） **vacl** および **e-vacl** TCAM リージョンを同じサイズに設定する必要があります。
ステップ 2	**copy running-config startup-config** 例： `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。
ステップ 3	switch(config)# **show hardware profile tcam region** 例： `switch(config)# show hardware profile tcam region`	スイッチの次回のリロード時に適用される TCAM サイズを表示します。
ステップ 4	switch(config)# **reload** 例： `switch(config)# reload`	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）

	コマンドまたはアクション	目的
		copy running-config to startup-config を保存した後、次回のリロード時に新しいサイズ値が有効になります。

例

次に、SVI TCAM リージョンのサイズを変更する例を示します。

```
switch(config)# hardware profile tcam region svi 256
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'

switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

VRF へのインターフェイスの割り当て

VRF にレイヤ 3 インターフェイスを追加できます。

手順の概要

1. **configure terminal**
2. **interface** *interface-type number*
3. **vrf member** *vrf-name*
4. **ip address** *ip-prefix/length*
5. **show vrf** [*vrf-name*] **interface** *interface-type number*
6. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** *interface-type number*
	例：
	`switch(config)# interface loopback 0`
	`switch(config-if)#`
		インターフェイス設定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	**vrf member** *vrf-name* 例： `switch(config-if)# vrf member RemoteOfficeVRF`	このインターフェイスを VRF に追加します。
ステップ 4	**ip address** *ip-prefix/length* 例： `switch(config-if)# ip address 192.0.2.1/16`	このインターフェイスの IP アドレスを設定します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。
ステップ 5	**show vrf** [*vrf-name*] **interface** *interface-type number* 例： `switch(config-vrf)# show vrf Enterprise interface loopback 0`	（任意）VRF 情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

例

次に、VRF にレイヤ 3 インターフェイスを追加する例を示します。

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

インターフェイスでの 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)# **interface ethernet** *type slot/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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface ethernet** *type slot/port* | **mgmt** *mgmt-interface-number* | **vlan** *vlan id*	物理イーサネットインターフェイス、管理インターフェイス、またはVLANインターフェイスを作成します。 *vlan id* の範囲は 1 ～ 4094 です。
ステップ 3	switch(config-if)# [**no**] **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**	DHCP サーバに IPv4 または IPv6 アドレスを要求します。 取得されたいずれかのアドレスを削除するには、このコマンドの **no** 形式を使用します。
ステップ 5	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

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

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

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

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

SVI およびサブインターフェイスの入力/出力ユニキャスト カウンタの設定

Cisco NX-OS リリース 9.3（3）以降では、SVI およびサブインターフェイス ユニキャスト カウンタが Cisco Nexus 9300-EX、9300-FX/FX2 スイッチ、および X9700-EX および X9700-FX ラインカードを搭載した Cisco Nexus 9500 シリーズ スイッチでサポートされています。

Cisco NX-OS リリース 9.3（5）以降では、SVI およびサブインターフェイス ユニキャスト カウンタが Cisco Nexus N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX スイッチでサポートされています。

Cisco NX-OS リリース 10.5（2）F 以降、 **hardware profile svi-and-si flex stats enable flex-stats** コマンドが有効になっている場合、SVI 統計レートは Cisco Nexus 9300-FX、FX2、FX3、GX、GX2、H2R、H1 シリーズ ToR スイッチ、および 9500 シリーズ EoR でサポートされます。9700-EX、FX、FX3、および GX ラインカードを備えたスイッチ。

（注）
- この機能を有効にすると、VXLAN、MPLS、トンネル、マルチキャスト、および ERSPAN カウンターが無効になります。変更を有効にするために、スイッチをリロードしてください。
- vPC セットアップでは、両方の vPC ピアの **vpc ドメイン**で**ピアゲートウェイ**機能を有効にする必要があります。そうしないと、SVI カウンタが不整合になる可能性があります。
- マルチキャスト カウンタはサポートされていません。
- EOR スイッチでは、統計情報レートは最初の ASIC（ASIC 0）のポートでのみサポートされます。入力ポートまたは出力ポートが最初の ASIC 以外の別の ASIC にある場合、統計レートはサポートされません。

デバイスで SVI およびサブインターフェイスの入力/出力ユニキャスト カウンタを設定するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **[no] hardware profile svi-and-si flex-stats-enable**
3. **copy running-config startup-config**
4. **reload**

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**[no] hardware profile svi-and-si flex-stats-enable**
	例：
	`switch(config)# hardware profile svi-and-si flex-stats-enable`
	`switch(config-if)#`
		SVI およびサブインターフェイスの入力/出力ユニキャスト カウンタを設定します。
		（注）
		このコマンドを機能させるには、設定を保存し、スイッチをリロードする必要があります。

ステップ 3	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	この設定を保存します。
ステップ 4	**reload** 例： `switch(config-if)# reload`	スイッチをリロードします。

サブインターフェイスのマルチキャストおよびブロードキャストカウンタの設定

Cisco NX-OS リリース 9.3(6) 以降では、Cisco Nexus N9K-C9336C-FX2 および N9K-C93240YC-FX2 スイッチでサブインターフェイス マルチキャストおよびブロードキャスト カウンタがサポートされています。

デバイスでマルチキャストおよびブロードキャストカウンタを設定するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **[no] hardware profile sub-interface flex-stats**
3. **copy running-config startup-config**
4. **reload**

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**[no] hardware profile sub-interface flex-stats**
	例：
	`switch(config)# hardware profile sub-interface flex-stats`
	`switch(config-if)#`
		マルチキャストおよびブロードキャスト カウンタのサブインターフェイスのフレックス統計情報を有効にします。

ステップ 3	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	この設定を保存します。
ステップ 4	**reload** 例： `switch(config-if)# reload`	スイッチをリロードします。

例

次に、show interface counters コマンドの結果として、サブインターフェイスのマルチキャスト カウンタとブロードキャスト カウンタを表示する例を示します。

```
switch(config)# show int ethernet 1/31/4.1 counters
--------------------------------------------------------------------------------
Port                                    InOctets                      InUcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                    0                               0

--------------------------------------------------------------------------------
Port                                 InMcastPkts                      InBcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                    0                               0

--------------------------------------------------------------------------------
Port                                InIPv4Octets                  InIPv4UcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                    0                               0

--------------------------------------------------------------------------------
Port                              InIPv4McastPkts                  InIPv4BcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                    0                               0
```

```
--------------------------------------------------------------------------------
Port                                InInIPv6Octets                InInIPv6UcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                      0                               0

--------------------------------------------------------------------------------
Port                              InInIPv6McastPkts                InInIPv6BcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                      0                               0

--------------------------------------------------------------------------------
Port                                   OutOctets                     OutUcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                      0                               0

--------------------------------------------------------------------------------
Port                                 OutMcastPkts                     OutBcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                      0                               0

--------------------------------------------------------------------------------
Port                               OutIPv4Octets                OutIPv4UcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                      0                               0

--------------------------------------------------------------------------------
Port                             OutIPv4McastPkts                OutIPv4BcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                      0                               0

--------------------------------------------------------------------------------
Port                               OutIPv6Octets                OutIPv6UcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                      0                               0

--------------------------------------------------------------------------------
Port                             OutIPv6McastPkts                OutIPv6BcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                      0                               0
```

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 レートの、5分間指数減少移動平均を含む）を表示します。
show interface ethernet *slot/port* **brief**	レイヤ 3 インターフェイスの動作ステータスを表示します。

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

レイヤ 3 インターフェイスのモニタリング

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。
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。

コマンド	目的
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* **counters detailed** [**all**]	VLAN インターフェイスの統計情報を表示します。オプションとして、レイヤ 3 パケットおよびバイト カウンタをすべて含めることができます（ユニキャストおよびマルチキャスト）。
show interface vlan *number* **counters snmp**	SNMP MIB から報告された VLAN インターフェイス カウンタを表示します。

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
```

次に、 **hardware profile svi-and-si flex-stats-enable** コマンドが有効になっている場合の SVI カウンタと SVI 統計情報レートの詳細の出力例を示します。

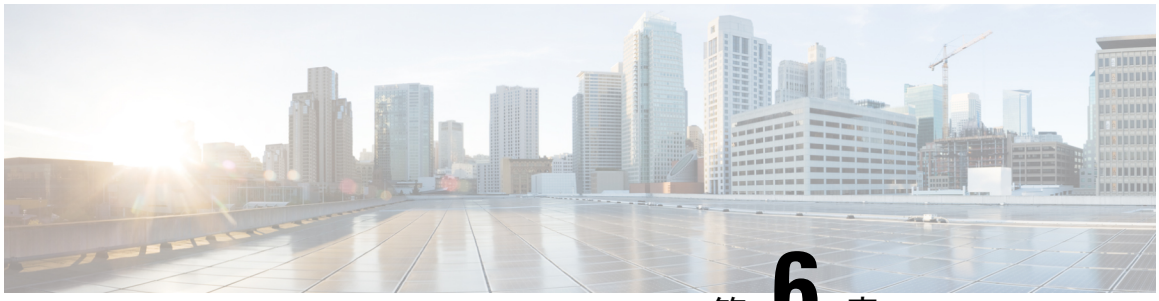
show interface コマンドでは、Cisco NX-OS リリース 10.5（2）F リリース以降、60 秒および 300 秒の統計レートまたはポーリング間隔が追加されています。

```
show interface  vlan 2406
Vlan2406 is up, line protocol is up, autostate enabled
  Hardware is EtherSVI, address is  3c13.ccc9.a397
  Internet Address is 20.0.0.2/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
   reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA
  Last clearing of "show interface" counters 00:11:03
```

```
Load-Interval #1: 1 minute (60 seconds)
60 seconds input rate 5492528 bits/sec, 10096 packets/sec
60 seconds output rate 0 bits/sec, 0 packets/sec
  input rate 5.49 Mbps, 10.10 Kpps; output rate 0 bps, 0 pps
Load-Interval #2: 5 minute (300 seconds)
300 seconds input rate 5448741 bits/sec, 10016 packets/sec
300 seconds output rate 0 bits/sec, 0 packets/sec
  input rate 5.45 Mbps, 10.02 Kpps; output rate 0 bps, 0 pps
L3 Switched:
  input: 0 pkts, 0 bytes - output: 0 pkts, 0 bytes
L3 in Switched:
  ucast: 6643884 pkts, 451784112 bytes
L3 out Switched:
  ucast: 0 pkts, 0 bytes
```

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

双方向フォワーディング検出

Bidirectional Forwarding Detection（BFD）は、2 台のデバイス間の転送パスで発生する障害を迅速に特定するために設計されたプロトコルです。BFDは、再コンバージェンス時間を予測できるようにすることで、ネットワークのプロファイリングとプランニングを簡素化します。

BFD は、さまざまなメディア タイプ、カプセル化、トポロジ、およびルーティング プロトコル全体で転送パス障害を検出します。2 つの隣接デバイス間のサブセカンド障害を検出し、サポートされているモジュールのデータプレーンに負荷を分散します。BFDは、プロトコルhelloメッセージよりも CPU の負荷を軽くすることができます。

非同期モード

BFD 非同期モードは、次のような BFD セッション モードです。

- 接続を監視するための定期的な制御パケットの交換が含まれ、
- BFD ネイバー セッションを確立して維持し、
- セッション パラメータをネゴシエートします。

BFD セッション パラメータ

次の表に、 BFD セッション パラメータとインターバルを示します。

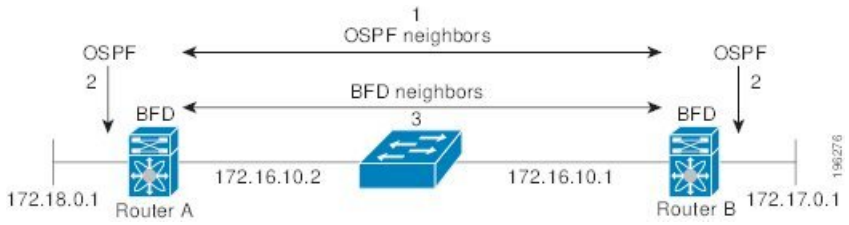
表 *11 : BFD* セッション パラメータ

セッションパラメータ	説明（Description）
目的の最小送信間隔	デバイスが BFD hello メッセージを送信するために構成された間隔。
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ために必要な欠落しているBFD hello メッセージの数。

BFD ネイバーのワークフロー

この図は、2 つのルータ間の BFD ネイバーセッション確立の詳細を示しています。

図 *6 : BFD* ネイバー関係の確立



BFD ネイバー セッションを確立する段階は、次のとおりです。

1. OSPFプロセスがBFDネイバーを探索します。
2. ローカル BFD プロセスは、 OSPF ネイバールータとのセッション BFD ネイバーセッションを開始する要求を受け取ります。
3. OSPF ネイバー ルータでの BFD ネイバー間でセッションが確立されます。

BFD の障害検出

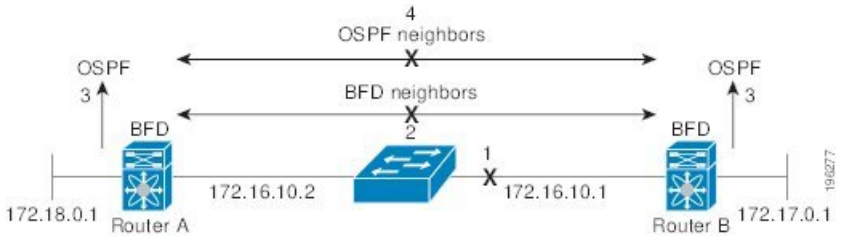
一度 BFD セッションが確立され、タイマー ネゴシエーションが終了すると、BFD ネイバーは、より速い速度の場合を除き IGP Hello プロトコルと同じ動作をする BFD 制御パケットを送信し、活性度を検出します。BFDは障害を検出しますが、プロトコルが障害の発生したピアをバイパスするための処置を行う必要があります。

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） 注意: 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速い必要があります。

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

エコー パケットは、送信側システムによってのみ定義および処理されます。IPv4 および IPv6 の場合、エコー パケットの宛先アドレスは送信側デバイスの宛先アドレスです。これは、リモート システムがパケットをローカル システムに転送するように選択されます。これにより、リモート システムでのルーティング ルックアップはバイパスされ、代わりに転送情報ベース（FIB）が利用されます。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。エコー機能は、リモート（ネイバー）システムにループ バックさせることにより、リモート システムの転送パスのみをテストします。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。

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。

高可用性

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 の前提条件

BFD を設定する前に、次の前提条件を満たしていることを確認します。

- BFD 機能をイネーブルにします。
- BFD 対応インターフェイスで ICMP のリダイレクト メッセージがディセーブルです。
- 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。
- 設定作業で詳細な前提条件を確認します。

注意事項と制約事項

BFD 設定時のガイドラインと制約事項は次のとおりです。

- QSFP 40/100-G BiDi は、ポートで使用可能な最高速度で起動します。たとえば、Cisco Nexus 93180LC-EX スイッチでは、最初の 28 ポートで 40 G、最後の 4 ポートで 100 G として起動します。40-G SR4 BiDi に接続する必要がある場合は、40/100-G BiDi の速度を 40 G に設定する必要があります。
- private-vlan 上のBFD はCisco Nexus 9000 スイッチではサポートされません。

- Cisco NX-OS リリース 10.2(1q)F 以降、PMN は N9K-C9332D-GX2B プラットフォーム スイッチでレイヤ 3 ユニキャスト BFD がサポートされます。
- 孤立ポートを介した vPC VLAN での BFD ネイバーの形成は、Cisco Nexus 9000 スイッチではサポートされていません。
- Cisco NX-OSリリース9.2（1）以降、QSFP-40 / 100-SRBD は 100-G の速度で起動し、N9K-X9636C-RX ライン カードを搭載した Cisco Nexus 9500 スイッチで 40-G または 100-G のいずれかの速度で他の QSFP-40 / 100-SRBD と相互運用します。QSFP-40 / 100-SRBD は、40G の速度で QSFP-40G-SR-BD と相互運用することもできます。ただし、40G の速度で動作するには、速度を 40G に設定する必要があります。
- キーワードが付いている **show** コマンドはサポートされていません。 **internal**
- メンバー単位の BFD リンクのサポートが Cisco Nexus 9000 シリーズ スイッチに追加されました。
- 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。
- IP アンナンバード インターフェイス上で BFD を設定する場合は、次の注意事項に従ってください。
  - インターフェイスがフラッピングないようにするため、 BFD エコー機能を無効にします。
  - IP アンナンバードインターフェイス上で BGP を設定する場合、 BFD マルチホップを有効にします。
- 多数の IPv6 隣接関係がある場合にBFDセッションがフラッピングしないように、レイヤ 3インターフェイス構成で **ipv6 nd ns-interval** コマンドの範囲を15 に設定。

  または、NS/NA パケットのControl Plane Policing （CoPP）ドロップが原因で発生する可能性のあるセッションの不安定性を回避するために、 BFD エコー間隔を増やします。
- BFD は BGPv6 をサポートします。
- BFD は EIGRPv6 をサポートします。
- BFD は、一意の（src_ip、dst_ip、interface/vrf）の組み合わせを持つセッションのみをサポートします。
- BFD は、シングルホップ BFD をサポートします。
  - シングルホップ静的 BFD のみがサポートされます。
  - 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、レイヤ 3 インターフェイスとして、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 インターフェイスをサポートします。
- BFD はレイヤ 3 隣接情報に応じて、レイヤ 2 のトポロジ変更を含むトポロジ変更を検出します。レイヤ 3 隣接情報が使用できない場合、VLAN インターフェイス（SVI）の BFD セッションはレイヤ 2 トポロジのコンバージェンス後に稼働しない可能性があります。
- 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。
- シングルホップとマルチホップの両方の BFD 機能は、特定の制限付きでサポートされます。マルチホップ BFD 機能の制限については、BFD マルチホップの注意事項と制約事項（214 ページ）のセクションを参照してください。
- 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 のリセットにより、他のポートのトラフィックが中断され、他のポートでの SVI セッションがフラップする可能性があります。たとえば、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ず、ASIC のトリガーをリセットする可能性があります。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。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。

    Cisco Nexus シリーズ スイッチの SVI は、vPC を介して接続されたデバイスとの BFD ネイバー隣接関係を確立するように設定しないでください。これは、ネイバーからの BFD キープアライブが、vPC ピア スイッチに接続された vPC メンバー リンクを介して送信された場合、この SVI に到達せず、BFD 隣接関係が機能不全になるためです。
  - 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。
  - BEX over FEX HIF インターフェイスはサポートされていません。
  - BFD セッションが仮想ポート チャネル（vPC）ピア リンクを使用して SVI 経由で行われる場合（BCM または GEM いずれかのベースのポート）、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 機能を無効にし、変更後、BFD を再度有効にすることができます。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、BFD エコー セッションをフラップします。
- **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。
- no-bfd-echoモードでBFDv6を設定する場合は、乗数3のタイマー150 msで実行することを推奨します。
- BFDv6は、v6のVRRPv3およびHSRPではサポートされません。
- インターフェイスでIPv6 **eigrp bfd**を無効にすることはできません。
- IETF BFDは、N9K-X96136YC-R、N9K-X9636C-R、N9K-X9636C-RX、およびN9K-X9636Q-R ライン カードではサポートされません。
- 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エコー機能はサポートされません。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。 **bfd per-link**

- BFDリンクごとに設定する前に、BFDセッションがポートチャネルで実行されていないことを確認します。すでに実行中のBFDセッションがある場合は、それを削除してからbfdリンクごとの設定に進みます。
- リンクローカルでのリンクごとのBFDの設定はサポートされていません。
- サポートされているプラットフォームには、N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RX ライン カードを搭載した Cisco Nexus 9500 シリーズ スイッチがあります。

- Cisco NX-OS リリース 9.3(7) 以降では、アンナンバード インターフェイスで BFD がサポートされます。

（注） アンナンバード スイッチド仮想インターフェイス（SVI）を介した BFD はサポートされていません。

アンナンバード インターフェイス サポートでの BFD のダウングレードの互換性は、 **show incompatibility nxos bootflash:filename** コマンドを使用して確認することはできません。**install all** コマンドの実行中に互換性がチェックされます。

- Cisco NX-OS リリース 10.5(2)F 以降、BFD over IP アンナンバード は Cisco Nexus 9808 と 9804 スイッチでサポートされません。
- OSPF とともに番号付きインターフェイスで BFD を設定し、インターフェイスを番号なしインターフェイスに変換すると、OSPF および BFD コマンドは実行コンフィギュレーションに残りますが、BFD 機能が動作しない場合があります。
- 次の BFD コマンド設定は、設定の置換ではサポートされていません。
  - **port-channel bfd track-member-link**
  - **port-channel bfd destination** *destination-ip-address*
- Cisco Nexus 9800 プラットフォーム スイッチには、BFD IPv6 セッションに対して次の制限があります。
  - ライン カードのスーパーバイザ スイッチ モードの各 ASIC ユニットは、最大 256 の BFD IPv6 セッションをサポートします。より多くの BFD IPv6 セッションが必要な場合は、セッションを ASIC ユニットまたはラインカード全体に分散させる必要があります。
- Cisco NX-OS リリース 10.3(1)F 以降、BFD は Cisco Nexus 9808 プラットフォーム スイッチのルーテッドポート、ルーテッド サブインターフェイス、およびブレイクアウト ポートでシングルホップ BFD をサポートします。

- Cisco NX-OS リリース 10.4(1)F 以降、BFD は Cisco Nexus 9804 プラットフォーム スイッチのルーテッド ポート、ルーテッド サブインターフェイス、およびブレイクアウト ポートでシングルホップ BFD をサポートします。
- Cisco NX-OS リリース 10.4(2)F 以降では、Cisco Nexus C9232E-B1 スイッチに以下が適用されます。
  - ルーテッド ポート、ルーテッド サブ インターフェイス、およびブレークアウト ポートでのシングルホップ BFD がサポートされます。
  - BFD 認証はサポートされていません。
- Cisco NX-OS リリース 10.2（2）F以降、 Cisco Nexus 93C64E-SG2-Q スイッチ はこれらの機能をサポートしています。
  - レイヤ 3 物理インターフェイスおよび物理サブインターフェイスでのシングルホップ BFD
  - レイヤ 3 ポート チャネルおよびポート チャネル サブインターフェイスでのシングルホップ BFD
  - ルーテッド ポートおよびブレークアウト ポートでのシングルホップ BFD
  - IPv4 および IPv6 アドレスのシングルホップ BFD
  - 最小 BFD タイマー（50 ミリ秒）
  - BFD 非同期モード
  - BFD エコー機能
- **bfd authentication interop** コマンドを活用、 Nexusと Nexus 以外のプラットフォーム間の BFD認証の相互運用性を設定します。このコマンドを設定しない場合は、無効な認証シーケンス番号フィールドの形式が原因で、 BFD 認証が失敗します。
- BFD 認証は、Cisco Nexus 9800 プラットフォーム スイッチではのサポートされません。
- Cisco NX-OS リリース 10.4(1)F 以降、BFD は、Cisco Nexus 9808 および 9804 スイッチに搭載されている N9KX98900CD-A および N9KX9836DM-A ライン カードでシングルホップ BFD をサポートします。
- Cisco NX-OS リリース 10.4（3）F 以降、シングル ホップ BFD は、Cisco Nexus 9808 および 9804 L3 ポートチャネル インターフェイスおよびポートチャネル サブインターフェイスでサポートされますが、次の制限があります。
  - ポートチャネルインターフェイスごとに、128 セッションのみがサポートされます。
  - BFD 認証はサポートされていません。
- Cisco NX-OS リリース 10.4（3）F 以降、シングルホップ BFD は レイヤ 3 ポート チャンネルの Cisco Nexus 9800 スイッチでサポートされます。BFD サーバーは、使用可能なオンラ

インライン カードの中から、セッションのホスティング ライン カードを選択します。しかし、この機能には、次の制限があります：

- ホスティング ラインカードが変更されると、そのライン カードで進行中のセッションが削除され、使用可能な別のライン カードでホスティングが作成されます。
- BFD セッションの送信元 IP が変更されると、進行中のセッションが削除され、新しい送信元 IP で再作成されます。

- Cisco NX-OS リリース 10.6(1)F以降、シングルホップ BFD は Cisco Nexus 9336C-SE1 スイッチでサポートされます。

Nexus スイッチでの BFD サポート

BFD サポートは、これらのリリースの Nexus プラットフォームで利用できます。詳細については、「ISSU サポート マトリクス」を参照してください。

表 *12 : Nexus* スイッチでの *BFD* サポート

プラットフォーム	Cisco NX-OS のリリースで導入済み
N9336C-SE1	10.6.1F
N93-C64E-SG2-Q	10.5.3F
N9K-C9364C-H1	10.4.3F
N9K-C93400LD-H1 N9K-C9232E-B1	10.4.2F
Nexus 9804 N9K-C9332D-H2R	10.4.1F
Nexus 9808	10.3.1F
N9K-C9348D-GX2A N9K-C9364D-GX2A N9K-C9332D-GX2B Cisco Nexus 9300-EX、9300-FX、9300-FX2、9300-FX3、および 9300-GX。	10.2.3F
9364C-GX 9316D-GX 93600CD-GX N9K-X96136YC-R、N9K-X9636C-R、N9K-X9636C-RX および N9K-X9636Q-R	9.3.3F

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 *13* : デフォルトの *BFD* パラメータ

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

BFD の設定

BFD 設定階層と継承のベストプラクティス

次の場所で BFD を設定する場合は、次の点を考慮してください。

- インターフェイス レベルの構成とグローバル構成
- メンバ ポート、ポート チャネル

インターフェイス レベルの設定とグローバル構成

グローバル レベルおよびインターフェイス レベルで BFD を構成できます。

（注） インターフェイス レベルの構成はグローバル構成よりも優先されます。

メンバー ポートおよびポート チャネルの継承

プライマリ ポート チャネルの BFD 構成を継承するようにメンバ ポートを構成します。

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します。

手順

ステップ 1 **configure terminal** コマンドを使用して、構成モードを開始します。

例：

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

ステップ 2 **feature bfd** で BFD をイネーブルにします。 コマンドを使用します。

例：

```
switch(config)# feature bfd
```

ステップ 3 （任意） **show feature | include bfd** を使用して機能のステータスを表示します。 コマンドを使用します。

例：

```
switch(config)# show feature | include
bfd
```

ステップ 4 （任意） **copy running-config startup-config** コマンドを使用して構成を保存します。

例：

```
switch(config)# copy running-config startup-config
```

BFDのディスエーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	**no feature bfd** コマンドを使用して、BFD機能をディセーブルにし、関連する構成をすべて削除します。 例：	

	コマンドまたはアクション	目的
	`switch(config)# no feature bfd`	

グローバルな BFD パラメータの構成

デバイス上のすべての Bidirectional Forwarding Detection（BFD）セッションのデフォルトのセッション動作を設定します。

BFD グローバル パラメータは、すべての BFD セッションのタイマーおよび検出特性を設定します。これらのパラメータは、インターフェイスで上書きできます。

デバイスのすべての BFD セッションのこれらの設定を構成できます。両方の BFD ピアは、3 ウェイ ハンドシェイクでセッション パラメータをネゴシエートします。

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 の構成」の項を参照してください。

グローバル BFD パラメータを設定するには、次の手順を活用します。

始める前に

BFD 機能をイネーブルにします。 グローバルな BFD パラメータの構成 （181 ページ） を参照してください

手順

ステップ 1 **configure terminal** コマンドを使用して、構成モードを開始します。

例：

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

ステップ 2 **bfd interval** *mintx* **min_rx** *msec* **multiplier** *value* コマンドを使用して、すべての BFD セッションの BFD セッション パラメータを構成します。

例：

```
switch(config)# bfd interval 50 min_rx 50 multiplier 3
```

個々の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。

intervals *mintx* および *msec* の範囲は 50 ～ 999 ミリ秒で、デフォルトは 50 ミリ秒です。

乗数の範囲は 1 ～ 50 です。デフォルトは 3 です。

ステップ 3 **bfd slow-timer** [*interval*] コマンドを使用して、エコー機能で使用される slow timer を設定します。

例：

```
switch(config)# bfd slow-timer 2000
```

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ます。エコー機能がイネーブルの場合に、非同期セッションがBFD制御パケットを送信するレートを指定します。

slow-timer 値は、制御パケットの間隔を設定します。エコー パケットは、リンク障害検出のために設定された BFD 間隔を使用します。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 双方向フォワーディング検出（BFD）のエコー フレーム **bfd echo-interface loopback** *interface number*

例：

```
switch(config)# bfd echo-interface loopback 1 3
```

このコマンドは、指定されたループバック インターフェイスで設定されるアドレスに、エコーパケットの送信元アドレスを変更します。指定できるインターフェイス番号の範囲は 0 ～ 1023 です。

ステップ 5 （任意） **show running-config bfd** コマンドを使用して、BFD の実行中の構成を表示します。

例：

```
switch(config)# show running-config bfd
```

ステップ 6 （任意） **copy running-config startup-config** コマンドを使用して構成を保存します。

例：

```
switch(config)# copy running-config startup-config
```

インターフェイス上でこれらをオーバーライドした場合を除き、デバイスはすべてのBFDセッションに対して指定されたデフォルトBFDパラメータを使用します。

例

インターフェイス上での BFD の構成

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。

始める前に

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セクションを参照してください。

手順

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)#
```

インターフェイス設定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。

Cisco NX-OS Release 9.3(5) 以降では、 **bfd interval 50 min_rx 50 multiplier 3** コマンドを使用してデフォルトのタイマー値を使用して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は、**no bfd interval** コマンドと機能的に同等です。

インターフェイスの BFD セッション パラメータがデフォルト値に設定されると、そのインターフェイスで実行されているBFDセッションは、グローバルセッションパラメータを継承します（存在する場合）。

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 認証を無効にするには、コマンドの **no** 形式を使用します。

ステップ 5 **bfd authentication interop** コマンドを活用、 Nexus と Nexus 以外のプラットフォーム間の BFD 認証の相互運用性を設定します。

例：

```
switch(config-if)# bfd authentication interop
```

ステップ 6 **show running-config bfd**

例：

```
switch(config-if)# show running-config bfd
```

（任意）BFD 実行コンフィギュレーションを表示します。

ステップ 7 **copy running-config startup-config**

例：

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

（任意）この設定の変更を保存します。

例

次のタスク

-

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。

始める前に

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」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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *number*
	例：
	`switch(config)# interface port-channel 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。
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：	（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

	コマンドまたはアクション	目的
	`switch(config-if)# bfd authentication keyed-sha1 keyid 1 ascii_key cisco123`	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 認証を無効にするには、コマンドの **no** 形式を使用します。
ステップ 6	**show running-config bfd** 例： `switch(config-if)# show running-config bfd`	（任意）BFD 実行コンフィギュレーションを表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

BFD エコー機能の構成（タスク）

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。RFC 5880 に準拠するためにエコー機能を無効にすると、RequiredMinEchoRx BFDセッションパラメータはゼロ以外のままになります。エコー機能を有効にすると、slow timer 値は必要な最小受信間隔になります。

始める前に

BFD 機能をイネーブルにします。BFD 機能をイネーブルにします。

BFD セッション パラメータを設定します。グローバルな BFD パラメータの設定またはインターフェイスでの BFD の設定

no ip redirects コマンドを使用して、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。

手順

ステップ 1 **configure terminal** コマンドを使用して、構成モードを開始します。

例：

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

ステップ 2 slow timer をBFD が **bfd slow-timer** *echo-interval* コマンドを使用してエコー機能をイネーブルにします。

例：

```
switch(config)# bfd slow-timer 2000
```

BFDエコー機能をイネーブルにすると、この値により非同期セッションの速度も低下します。

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 ミリ秒です。

ステップ 3 **interface** *int-if* コマンドを使用してインターフェイス構成モードを開始します。

例：

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

? 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** コマンドを使用して、BFD の実行構成を表示します。

例：

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

デフォルトではイネーブルになっています。

ステップ 5 （任意） **show running-config bfd** コマンドを使用して、BFD の実行構成を表示します。

例：

```
switch(config-if)# show running-config bfd
```

ステップ 6 （任意） **copy running-config startup-config** コマンドを使用して構成を保存します。

例：

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

メンバー単位リンク BFD セッションの設定

メンバー単位の BFD リンクのサポートが Cisco Nexus 9000 シリーズ スイッチに追加されました。詳細については、次の項を参照してください。

リンク単位の効率化に対処するための BFD 拡張機能

IETF Micro BFD と呼ばれるリンク単位の効率化機能に対処するための双方向転送（BFD）拡張機能を使用すれば、すべてのリンク集約グループ（LAG）メンバー インターフェイス（RFC 7130 で規定されている）上で個別の BFD セッションを設定することができます。

この拡張機能により、BFDセッションはポートチャネルの各メンバーリンク上で動作します。BFDがリンク障害を検出すると、そのメンバーリンクが転送テーブルから削除されます。BFDセッションは個別のポート チャネル インターフェイス上で作成されるため、このメカニズムが迅速な障害検出を可能にします。

ポートチャネルのメンバー リンクで実行されている BFD セッションは、マイクロ BFD セッションと呼ばれます。ユーザは、メイン ポートチャネル インターフェイス経由で RFC 7130 BFD を設定できます。このインターフェイスでは、メンバーごとに 1 つずつのマイクロ BFD

セッションを使用することにより LAG 経由の帯域幅モニタリングが実行されます。メンバーポートのいずれかがダウンすると、そのポートが転送テーブルから削除されます。これにより、そのメンバー上のトラフィックの破損が回避されます。

マイクロ BFD セッションは、LACP ベースポート チャネルと非 LACP ベースポート チャネルの両方でサポートされます。マイクロ BFD セッションの設定方法の詳細については、「マイクロ *BFD* セッションの設定」のトピックを参照してください。

IETF 双方向フォワーディング検出の制限事項

IETF 双方向フォワーディング検出の次の制限事項を確認してください。

- BFDの制限事項
  - IETF Micro-BFD セッションは、シングルホップ BFD セッションのみをサポートします。異なるサブネットからの IP を構成してマイクロ BFD セッションを確立することは推奨できません 。
  - 論理ポートチャネルまたは独自の BFD メンバ単位リンクを介して BFD と共存することはできません。PCで BFD IETF IPv4 が 設定されている場合、BFD IPv6 の論理/独自リンク単位セッションもサポートされません。
  - いずれかのルーティングプロトコルで論理BFDセッションを設定する場合は、どのIETFポートチャネルにも適用されないようにしてください。同じポートチャネルに論理設定とIETF設定の両方を設定すると、ISSU /リロード時に未定義の動作が発生します。
  - IETF BFD IPv6 はサポートされていません。
  - エコー機能は、マイクロ BFD セッションではサポートされません。
  - ポート チャネル インターフェイスは、BFD セッションを実行している 2 台のスイッチ（ピアデバイス）間で直接接続されるべきです。中間のレイヤ2スイッチは想定されていません。

- EthPCM/LACP の制限事項
  - LACP ポート チャネルのメンバーがホット スタンバイ状態で、アクティブ リンクの 1 つで BFD 障害が発生した場合は、ホット スタンバイ リンクが直接起動しない可能性があります。BFD 障害が発生したアクティブ リンクがダウンすると、ホット スタンバイ メンバーがアクティブになります。ただし、ポートチャネルの最小リンク条件がヒットした場合、ホットスタンバイ リンクが起動する前にポートチャネルがダウンするのを防ぐことはできません。

- 一般的な制限事項
  - レイヤ 3 ポートチャネルでのみサポートされます。
  - 以下ではサポートされていません。
    - vPC

- レイヤ 3 サブインターフェイス
- レイヤ 2 ポートチャネル/レイヤ 2 ファブリックパス
- FPC/HIF PC
- レイヤ 3 サブインターフェイス
- ポートチャネル上の SVI

IETF メンバー単位セッションの移行/設定のガイドライン：

IETF メンバー単位セッションの移行/設定については、次のガイドラインを確認してください。

- ポートチャネル サブインターフェイス（RFC 7130 を実行できない）上でルーティング プロトコルを使用して作成された論理 BFD セッションは引き続きサポートされます。ただし、メイン ポートチャネル インターフェイスは、共存する論理セッションと RFC 7130 セッションの両方をサポートしません。いずれかのみをサポートできます。
- ユーザは、メイン ポートチャネル インターフェイス経由で RFC 7130 BFD を設定できます。このインターフェイスでは、メンバーごとに 1 つずつのマイクロ BFD セッションを使用することにより LAG 経由の帯域幅モニタリングが実行されます。いずれかのメンバーポートがダウンすると、BFD はポートチャネル マネージャにそのポートを通知し、ポートチャネル マネージャは LTL からポートを削除することで、そのメンバーのトラフィックのブラックホール化を防止します。
- ポートチャネルをアップにするために必要なリンクの最小数が満たされていない場合は、ポートチャネルマネージャがポートチャネルをダウンにします。これにより、ポートチャネル サブインターフェイスが設定されている場合にポートチャネル サブインターフェイスがダウンし、ルーティングプロトコルを通知する論理 BFD セッションもダウンします。
- メイン ポートチャネル インターフェイス上で設定された RFC 7130 を使用している場合、論理 BFD セッションは、アグレッシブ タイマーを RFC 7130 BFD セッションより弱くして実行する必要があります。ポートチャネル インターフェイスに RFC 7130 を設定することも、ポートチャネル サブインターフェイスの論理 BFD セッションと組み合わせて設定することもできます。
- 独自のリンク単位が設定されている場合、ポートチャネルで IETF Micro-BFD セッションを有効にすることはできません。その逆も同様です。独自のリンク単位の設定を削除する必要があります。独自のリンク単位の現在の実装では、アプリケーションによってブートストラップされる（リンクごとではない）BFD セッションがある場合、設定を変更できません。各アプリケーションの BFD トラッキングを削除し、リンクごとの設定を削除する必要があります。独自のリンク単位から IETF Micro-BFD への移行パスは次のとおりです。
  - アプリケーションの BFD 設定を削除します。
  - リンク単位の設定を削除します。
  - IETF Micro-BFD コマンドを有効にします。

- アプリケーションでBFDを有効にします。

メインのポートチャネル インターフェイスでは、独自の BFD から IETF Micro-BFD に移行するのに、同じパスをたどることができます。

ポート チャネル インターフェイスの設定

始める前に

BFD 機能が有効になっていることを確認します。

手順の概要

1. switch(config)# **interface port-channel** *port-number*
2. switch(config-if)# **no switchport**

手順の詳細

手順

ステップ 1 switch(config)# **interface port-channel** *port-number*

インターフェイスのポート チャネルを設定します。

ステップ 2 switch(config-if)# **no switchport**

インターフェイスをレイヤ 3 ポートチャネルとして設定します。

次のタスク

- BFD スタート タイマーの設定
- IETF リンク単位の BFD

（任意）BFD スタート タイマーの設定

BFD 開始タイマーを設定するには、次の手順を実行します。

手順の概要

1. switch(config-if)# **port-channel bfd start** *60*

手順の詳細

手順

switch(config-if)# **port-channel bfd start** *60*

ポート チャネルの BFD 開始タイマーを設定します。

（注）
デフォルト値は無限です（つまり、タイマーは動作していません）。ポートチャネルのBFD開始タイマー値の範囲は 60 ～ 3600 秒です。開始タイマーを動作させるためには、開始タイマーの値を、ポート チャネル BFD 設定を完了する前（つまり、port-channel bfd track-member-link と port-channel bfd destination をアクティブ メンバーとのレイヤ 3 ポート チャネル インターフェイス用に設定する前）に設定します。

次のタスク

- IETF リンク単位の BFD
- BFD 宛先 IP アドレスの設定

IETF リンク単位の BFD

手順の概要

1. switch(config-if)# **port-channel bfd track-member-link**

手順の詳細

手順

switch(config-if)# **port-channel bfd track-member-link**

ポート チャネル インターフェイス上で IETF BFD を有効にします。

次のタスク

- BFD 宛先 IP アドレスの設定
- マイクロ BFD セッションの設定の確認

BFD 宛先 IP アドレスの設定

次の手順を実行して、BFD 宛先 IP アドレスを設定します。

手順の概要

1. switch(config-if)# **port-channel bfd destination***ip-address*

手順の詳細

手順

switch(config-if)# **port-channel bfd destination***ip-address*

メンバー リンク上の BFD セッションに使用される IPv4 アドレスを設定します。

次のタスク

- マイクロ BFD セッションの設定の確認

マイクロ BFD セッションの設定の確認

マイクロ BFD セッション設定を確認するには、次のコマンドを使用します。

手順の概要

1. ポート チャネルとポート チャネル メンバーの動作状態を表示します。
2. switch# **show bfd neighbors**
3. switch# **show bfd neighbors details**
4. switch# **show tech-support bfd**
5. switch# **show tech-support lacp all**
6. switch# **show running-config interface port-channel** *port-channel-number*

手順の詳細

手順

ステップ 1 ポート チャネルとポート チャネル メンバーの動作状態を表示します。

switch# **show port-channel summary**

ステップ 2 switch# **show bfd neighbors**

ポート チャネル メンバー上のマイクロ BFD セッションを表示します。

ステップ 3 switch# **show bfd neighbors details**

ポート チャネル インターフェイスの BFD セッションと、メンバーの関連するマイクロ BFD セッションを表示します。

ステップ 4 switch# **show tech-support bfd**

BFD のテクニカル サポート情報を表示します。

ステップ 5 switch# **show tech-support lacp all**

イーサネット ポート マネージャ、イーサネット ポートチャネル マネージャ、および LACP のテクニカル サポート情報を表示します。

ステップ 6 switch# **show running-config interface port-channel** *port-channel-number*

ポート チャネル インターフェイスの実行コンフィギュレーション情報を表示します。

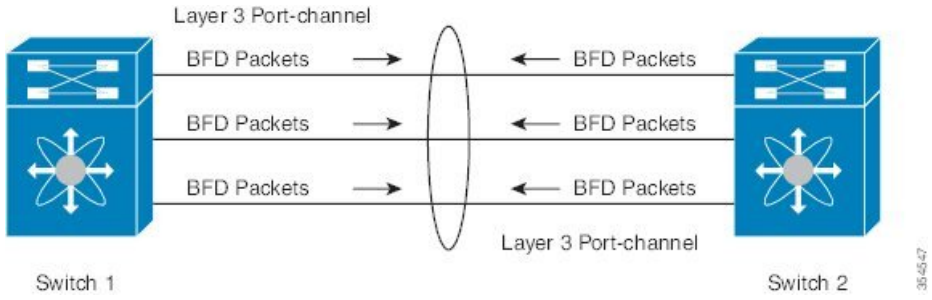
例：マイクロ BFD セッションの設定

マイクロ BFD セッションの設定については、次の例を参照してください。

マイクロ BFD セッションの設定

この例では、次のトポロジが使用されます。

図 *8:* マイクロ *BFD* セッションの設定



スイッチ 1 の設定例は次のとおりです。

```
feature bfd
configure terminal
    interface port-channel 10
       port-channel bfd track-member-link
       port-channel bfd destination 10.1.1.2
       port-channel bfd start 60
       ip address 10.1.1.1/24
```

スイッチ 2 の設定例は次のとおりです。

```
feature bfd
configure terminal
```

```
interface port-channel 10
      port-channel bfd track-member-link
      port-channel bfd destination 10.1.1.1
      port-channel bfd start 60
        ip address 10.1.1.2/24
```

マイクロBFDセッションの設定の確認

次に、**show running-config interface port-channel**<*port-channel*>、**show port-channel summary**, **show bfd neighbors vrf internet_routes**、および **show bfd neighbors interface port-channel** <*port-channel*> **vrf internet_routes details** コマンドの出力結果を示します。

```
switch# show running-config interface port-channel 1001

!Command: show running-config interface port-channel1001
!Time: Fri Oct 21 09:08:00 2016

version 7.0(3)I5(1)

interface port-channel1001
  no switchport
  vrf member internet_routes
  port-channel bfd track-member-link
  port-channel bfd destination 40.4.1.2
  ip address 40.4.1.1/24
  ipv6 address 2001:40:4:1::1/64

switch# show por
port-channel   port-profile
switch# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
1001  Po1001(RU)  Eth      LACP      Eth1/11/1(P)  Eth1/11/2(P)  Eth1/12/1(P)
                                     Eth1/12/2(P)
switch# show bfd neighbors vrf internet_routes

OurAddr         NeighAddr       LD/RD                 RH/RS           Holdown(mult)
 State       Int                  Vrf
40.4.1.1        40.4.1.2        1090519041/0          Up              N/A(3)
 Up          Po1001               internet_routes
40.4.1.1        40.4.1.2        1090519042/1090519051 Up              819(3)
 Up          Eth1/12/1            internet_routes
40.4.1.1        40.4.1.2        1090519043/1090519052 Up              819(3)
 Up          Eth1/12/2            internet_routes
40.4.1.1        40.4.1.2        1090519044/1090519053 Up              819(3)
 Up          Eth1/11/1            internet_routes
40.4.1.1        40.4.1.2        1090519045/1090519054 Up              819(3)
 Up          Eth1/11/2            internet_routes
switch#

switch# show bfd neighbors interface port-channel 1001 vrf internet_routes details
```

```
OurAddr         NeighAddr       LD/RD                 RH/RS           Holdown(mult)
 State       Int                   Vrf
40.4.1.1        40.4.1.2        1090519041/0          Up              N/A(3)
 Up          Po1001                internet_routes

Session state is Up
Local Diag: 0
Registered protocols:  eth_port_channel
Uptime: 1 days 11 hrs 4 mins 8 secs
Hosting LC: 0, Down reason: None, Reason not-hosted: None
Parent session, please check port channel config for member info
switch#

switch# show bfd neighbors interface ethernet 1/12/1 vrf internet_routes details

OurAddr         NeighAddr       LD/RD                 RH/RS           Holdown(mult)
 State       Int                   Vrf
40.4.1.1        40.4.1.2        1090519042/1090519051 Up              604(3)
 Up          Eth1/12/1             internet_routes

Session state is Up and not using echo function
Local Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: None
MinTxInt: 100000 us, MinRxInt: 100000 us, Multiplier: 3
Received MinRxInt: 300000 us, Received Multiplier: 3
Holdown (hits): 900 ms (0), Hello (hits): 300 ms (458317)
Rx Count: 427188, Rx Interval (ms) min/max/avg: 19/1801/295 last: 295 ms ago
Tx Count: 458317, Tx Interval (ms) min/max/avg: 275/275/275 last: 64 ms ago
Registered protocols:  eth_port_channel
Uptime: 1 days 11 hrs 4 mins 24 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.: 1090519051    - Your Discr.: 1090519042
             Min tx interval: 300000  - Min rx interval: 300000
             Min Echo interval: 300000 - Authentication bit: 0
Hosting LC: 1, Down reason: None, Reason not-hosted: None
Member session under parent interface Po1001


switch# show bfd neighbors interface ethernet 1/12/2 vrf internet_routes details

OurAddr         NeighAddr       LD/RD                 RH/RS           Holdown(mult)
 State       Int                   Vrf
40.4.1.1        40.4.1.2        1090519043/1090519052 Up              799(3)
 Up          Eth1/12/2             internet_routes

Session state is Up and not using echo function
Local Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: None
MinTxInt: 100000 us, MinRxInt: 100000 us, Multiplier: 3
Received MinRxInt: 300000 us, Received Multiplier: 3
Holdown (hits): 900 ms (0), Hello (hits): 300 ms (458336)
Rx Count: 427207, Rx Interval (ms) min/max/avg: 19/1668/295 last: 100 ms ago
Tx Count: 458336, Tx Interval (ms) min/max/avg: 275/275/275 last: 251 ms ago
Registered protocols:  eth_port_channel
Uptime: 1 days 11 hrs 4 mins 30 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.: 1090519052    - Your Discr.: 1090519043
             Min tx interval: 300000  - Min rx interval: 300000
             Min Echo interval: 300000 - Authentication bit: 0
```

```
Hosting LC: 1, Down reason: None, Reason not-hosted: None
Member session under parent interface Po1001
switch#
```

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

ボーダー ゲートウェイ プロトコル（BGP）の BFD を設定できます。

始める前に

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」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」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** [**multihop** | **singlehop**]
5. **update-source** *interface*
6. **show running-config bgp**
7. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**router bgp** *as-number*
	例：
	`switch(config)# router bgp 64496`
	`switch(config-router)#`
		BGP を有効にして、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。

	コマンドまたはアクション	目的

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。The *ip-address* 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** [**multihop** | **singlehop**] 例： `switch(config-router-neighbor)# bfd multiihop`	デバイスで BFD マルチ ホップまたはシングル ホップ セッションを設定します。デフォルトでは、キーワードは指定されていません。キーワードを指定せず、ピアが直接接続されている場合はシングル ホップ セッションが選択され、ピアが接続されていない場合はマルチ ホップ セッション タイプが選択されます。「multihop」または「singlehop」オプションを指定すると、セッション タイプは CLI オプションに従ってデバイスで強制されます。
ステップ 5	**update-source** *interface* 例： `switch(config-router-neighbor)# update-source ethernet 2/1`	ネイバーで BGP セッションを形成し、BFD とともにクライアントとして登録するために BGP を有効にするとき、特定のインターフェイスからのプライマリ IP アドレスをローカル アドレスとして BGP セッションで使用できます。
ステップ 6	**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 7	**copy running-config startup-config** 例： `switch(config-router-neighbor)# copy running-config startup-config`	（任意）この設定の変更を保存します。

EIGRP での BFD の設定

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

始める前に

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」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」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

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**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** を使用します 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)#`
		インターフェイス設定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）この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。

始める前に

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」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」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

手順

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

	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)#`
		インターフェイス設定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）この設定の変更を保存します。

OSPF での BFD の設定例

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
```

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。

始める前に

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」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」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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**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)#`
		インターフェイス設定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。

	コマンドまたはアクション	目的
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）この設定の変更を保存します。

IS-IS での BFD の設定例

IPv4およびIPv6アドレスファミリでBFDが有効になっているIS-ISの設定例。

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

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。

この項で説明している **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。

始める前に

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」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」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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**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)#`
		インターフェイス設定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。
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）この設定の変更を保存します。

VRRP での BFD の設定

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

この項で説明している **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。

始める前に

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」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」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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** *int-if*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス設定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。

	コマンドまたはアクション	目的
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）この設定の変更を保存します。

PIM（Protocol Independent Multicast） での BFD の設定

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

始める前に

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**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)#`
		インターフェイス設定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）この設定の変更を保存します。

スタティック ルートでの BFD の設定

インターフェイスのスタティック ルータの BFD を設定できます。Virtual Routing and Forwarding（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。

始める前に

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」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** *route interface* {*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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**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** *route interface* {*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。
ステップ 6	**copy running-config startup-config** 例： `switch(config-vrf)# copy running-config startup-config`	（任意）この設定の変更を保存します。

インターフェイスにおける BFD のディセーブル化

グローバルまたは VRF レベルでイネーブルにされた BFD のあるルーティング プロトコルに対するインターフェイス上の BFD を選択的にディセーブルにできます。

インターフェイス上の 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。

インターフェイスにおける BFD のディセーブル化

インターフェイスごとにBFDが無効になっている設定例。

```
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
```

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *int-if* 例： `switch(config-if)# interface ethernet 2/1`	インターフェイス設定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。
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** *vlan vlan-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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *vlan vlan-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。

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** *type number.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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *type number.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：	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。

	コマンドまたはアクション	目的
	`switch(config-if)# exit`	

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 BFD ネイバーに関する情報を表示します。
show bfd neighbors [**dest-ip** *ip-address*] [**src-ip** *ip-address*][**details**]	インターフェイスの指定された BFD ネイバー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 マルチ セッション（概念）

BFD マルチ セッションとは、次のようなネットワーク管理機能です。

- 単一のネットワークリンクを介して複数のBFDセッションを設定できる
- 迅速な異常検出を有効にすることでネットワークの信頼性を向上させる
- 単一のリンクを介した複数のパスの詳細なモニタリングを有効にする
- リソースの使用と拡張性を最適化する。

Cisco NX-OS リリース 10.5(3)F 以降、Cisco Nexus スイッチは BFD マルチセッションをサポートします。

BFD マルチホップ

IPv4 の BFD マルチホップおよび IPv6 の BFD マルチホップは、RFC5883 に準拠してサポートされます。BFD マルチホップ セッションは、固有のソースと宛先アドレス ペア間で設定されます。マルチホップ BFD セッションは、シングルホップ BFD セッションの場合のように、インターフェイスではなく、送信元と宛先の間のリンクに関連付けられます。

BFD マルチホップのホップ数

BFD マルチホップはTTLフィールドを最大制限に設定し、受信時に値をチェックしません。BFD コードは、BFDマルチホップ パケットが通過できるホップ数には影響しません。ただし、ほとんどのシステムでは、ホップ数が 255 に制限されています。

BFD マルチホップの注意事項と制約事項

BFD マルチホップ設定時の注意事項と制約事項は次のとおりです。

- Cisco NX-OS リリース 10.4 (1)F 以降、L3VNI インターフェイスを使用した VXLAN を介した BFD マルチホップがサポートされます。
- Cisco NX-OS リリース 9.3(6) から、BFD マルチホップは、BGP IPv4 でのみ Cisco Nexus 9200、9300-EX/FX/GX プラットフォーム スイッチおよびCisco Nexus 9500 プラットフォーム スイッチでサポートされています（N9K-X9700-EX ライン カード搭載のもの）。
- ダイナミック BGP コンフィギュレーションでは、シングル BGP ピアとマルチホップ BGP ピアの両方が BFD マルチホップ設定を受け入れます。
- BFD マルチホップは BGP でのみサポートされています。
- BFD マルチホップは、次のデバイスの BGP IPv6 マルチホップ ネイバーでサポートされます。
  - Cisco Nexus 9200YC-X、9300-EX、9300-FX および 9300-GX スイッチ
  - 、N9K-X97160YC-EX、、 または N9K-X9736C-FX ライン カードを搭載した Cisco Nexus 9500 プラットフォーム スイッチ

（注） -EX および -FX ライン カードを使用した Cisco Nexus 9500 プラットフォーム スイッチで BGP IPv6 の BFD マルチホップを使用するには、 **system routing template-mpls-heavy** コマンドを有効にする必要があります。

- マルチホップ BFD は、UDP 宛先ポート 4784 で識別されます。
- マルチホップ BFD のデフォルトのインターバル タイマーは、乗数 3 で 250 ms です。
- サポートされるマルチホップ BFD セッションの最大数は 100 です。
- 既存の BFD 認証サポートは、マルチホップ セッション用に拡張されています。
- エコー モードはマルチホップ BFD ではサポートされません。
- セグメント ルーティング アンダーレイによるマルチホップはサポートされていません。
- サポートされていないプラットフォームでは、BGPv6 マルチホップ ネイバーを設定するときに BFD コマンドが受け入れられます。ただし、セッションは作成またはインストールされません。
- マルチホップ BFD セッションがポート チャネルにインストールされている場合、次の点に注意する必要があります。
  - すべてのセッションが Cisco Nexus 9500 スイッチファミリの単一のラインカードでホストされている場合、ホストされたラインカードのリロード中に、すべてのセッションが別のラインカードでホストされます。この場合、BFD および BGP セッションがフラップすることがあります。
  - モジュール間ポートチャネルを介した BGP のマルチホップ BFD セッションは、完全な冗長性を提供しません。

BFD マルチホップ セッション グローバル インターバル 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。セッションごとに異なる BFD セッションパラメータを設定するには、セッション単位の設定コマンドを使用します。

始める前に

BFD 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **[no] bfd multihop interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*
3. **end**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーションモードに入ります。

ステップ 2	**[no] bfd multihop interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier* 例： `switch(config)# bfd multihop interval 250 min_rx 250 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。このコマンドは、デフォルトの動作を上書きします。*Required Minimum Receive Interval* と *Desired Minimum Transmit Interval* は 250 です。乗数のデフォルトは 3 です。
ステップ 3	**end** 例： `switch(config)# end`	設定の変更を保存し、設定セッションを終了します。

マルチホップ セッション単位の BFD パラメータの設定

マルチホップ セッション単位の BFD パラメータを設定できます。

始める前に

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」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. **update-source** *interface*
5. **bfd**
6. **bfd multihop interval** *mintx* **min_rx** *msec* **multiplier** *value*
7. **bfd multihop authentication keyed-sha1 keyid** *id* **key** *ascii_key*
8. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**router bgp** *as-number*
	例：
	`switch(config)# router bgp 64496`
	`switch(config-router)#`
		BGP を有効にして、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。The *ip-address* 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	**update-source** *interface*
	例：
	`switch(config-router-neighbor)# update-source Ethernet1/4`
	`switch(config-router-neighbor)#`
		インターフェイスから BFD セッションの送信元 IP アドレスを取得します。

ステップ 5	**bfd** 例： `switch(config-router-neighbor)# bfd multihop`	この BGP ピアの BFD をイネーブルにします。
ステップ 6	**bfd multihop interval** *mintx* **min_rx** *msec* **multiplier** *value* 例： `switch(config-router-neighbor)# bfd multihop interval 250 min_rx 250 multiplier 3`	このネイバーのマルチホップ BFD 間隔値を設定します。*mintx* および *msec* の範囲は 250 ～ 999 ミリ秒で、デフォルトは 250 です。乗数の範囲は 1 ～ 50 です。乗数のデフォルトは 3 です。
ステップ 7	**bfd multihop authentication keyed-sha1 keyid** *id* **key** *ascii_key* 例： `switch(config-router-neighbor)# bfd multihop authentication keyed-sha1 keyid 1 ascii_key cisco123`	（オプション）このネイバー上のマルチホップ BFD セッションで BFD 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 認証を無効にするには、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 8	**copy running-config startup-config** 例： `switch(config-router-neighbor)# copy running-config startup-config`	（任意）この設定の変更を保存します。

障害シナリオでのBFD vPC サブセカンド コンバージェンス

vPC（仮想ポート チャネル）コンバージェンスとは、vPC セットアップに関連する障害またはトポロジ変更からネットワークがどれくらい迅速に回復するかを意味します。電源障害が発生すると、vPC マルチキャスト トラフィックを処理するスイッチが 6 ～ 7 秒のコンバージェンス遅延に直面する可能性があります。

BFD vPC ウォッチ サブセカンド コンバージェンス機能を使用すると、ネットワーク内の単一リンクに障害が発生した場合、または電源障害のために単一スイッチがオフラインになった場合に、ペアの vPC スイッチが 250 ミリ秒以内でマルチキャスト トラフィックを収束できます。

Cisco NX-OS リリース 10.2（2）F以降、この機能は PIM プロトコルでのみサポートされ、BFD vPC ウォッチ通知を処理します。

（注） この機能は、他の IGP プロトコルには適用されません。

vPC サブセカンド コンバージェンスの利点

- **高速コンバージェンス**： 以下に示すトラフィック フローのネットワーク障害時に 250 ミリ秒以内のマルチキャスト トラフィック コンバージェンスを提供します。
  - vPC から vPC
  - vPC からレイヤ 3
  - レイヤ 3 から vPC
  - レイヤ 3 からレイヤ 3
- **効率的なマルチキャスト処理**：マルチキャスト トラフィック フェールオーバーの遅延に対処し、ネットワーク全体のパフォーマンスを向上させます。
- **強化されたネットワーク復元力**：予期しない障害時にネットワーク運用を維持するための堅牢なソリューションを提供します。単一リンクの障害やスイッチの電源オフなどのシナリオに対応し、最小限のトラフィック損失で迅速なフェールオーバーを実現します。

- **プラットフォーム サポート**： Cisco Nexus 9000 TOR プラットフォーム（FX2、FX3、および Cloudscale TOR）向けに最適化されています。

BFD vPC ウォッチ構成ワークフロー

1. スイッチでBFD機能構成を有効にし、高速検出のためにvPC ピア間に専用ポートチャネルを確立します。
2. ポート チャネルで **port-channel bfd track-member-link** コマンドを構成して、VPC ピアの障害を検出するために専用のポートチャネル上にマイクロ BFDセッションを作成します。

   マイクロ BFD セッションは、構成された乗数を使用して、最小 10 ミリ秒のアグレッシブな間隔で動作します。
3. vPC モニタリングを指定するには、ポートチャネル インターフェイスで **bfd vpc-watch** コマンドをイネーブルにします。

   vPC スイッチ トリガ イベントは、ポート チャネル インターフェイス上のすべてのサブスクライバにマイクロ BFDセッションの状態変更通知（SCN）をブロードキャストします。
4. プロトコル非依存マルチキャスト（Protocol Independent Multicast、PIM）がマイクロ BFD セッションの BFD 通知を受信し、セッションを維持します。

[Restrictions（機能制限）]

- BFD vPC ウォッチ機能は、これらの Cisco Nexus スイッチでのみサポートされます。
  - N9K-X9736C-FX、N9K-X9736Q-FX、N9K-X9788TC-FX、N9K-C93180YC-FXN9K-C93108TC-FX、N9K-C9348GC-F、N9K-C9348GC-FXP、N9K-C9358GY-FXP、N9K-X9732C-FX、
  - N9K-C9336C-FX2-E、N9K-C93216TC-FX2、N9K-C93360YC-FX2、N9K-C93240YC-FX2-Z、N9K-C93240YC-FX2、N9K-C9336C-FX2
  - N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX、N9K-X9716D-GX、
  - N9K-X9736C-FX3、N9K-C93180YC-FX3S、N9K-C93180YC-FX3、N9K-C93108TC-FX3P、N9K-C9348GC-FX3、N9K-C9348GC-FX3PH、N9K-C93108TC-FX3、N9K-C92348GC-FX3
  - N9K-C9364D-GX2A、N9K-C9332D-GX2B、N9K-C9348D-GX2A、N9K-C9408
  - N9K-C9332D-H2R、N9K-C9364C-H1、N9K-C93400LD-H1
- **bfd vpc-watch** コマンドは、**port-channel bfd track-member-link** 構成のポートチャネル インターフェイスに適用できます。

（注） **port-channel bfd track-member-link** の構成を削除する前に、必ず **bfd vpc-watch**の構成を解除してください。

- **bfd vpc-watch** がVPC ウォッチドッグ ポートチャネル インターフェイスで設定されている場合、このインターフェイスまたはそのメンバー リンクでマイクロ BFD セッションをダウンさせる管理操作を実行すると、トラフィックが重複する可能性があります。この問題を回避するには、VPC ウォッチドッグ インターフェイスで管理タスクを実行する前に、**bfd vpc-watch** 構成を削除します。
- 警告メッセージが **feature bfd** 構成に表示されます。

  `TX 間隔または RX 間隔またはエコー rx 間隔が 50 ミリ秒未満に設定されている場合、サポートされる BFD セッションのスケール制限は 10 です。`
- BFD 間隔乗数 1 は、Tx、Rx ro eho-rx 間隔のいずれかが 50 ミリ秒未満に設定されている場合はサポートされません 。
- Cisco NX-OS リリース 10.2（2）F リリースは、マイクロ BFD IPv6 セッションをサポートしていません 。
- Cisco NX-OS リリース 10.2（2）F以降、BFD IPv4 および IPv6 セッションの TX、RX 間隔は 10 ～ 999 ミリ秒の範囲です。

  Cisco NX-OS リリース 10.2（2）Fより前のリリースでは、BFD IPv4 および IPv6 セッションの TX および RX 間隔は 50 ～ 999 ミリ秒の範囲です。

  間隔は **bfd [ipv4 | ipv6] interval** 、 *msec* [**min_rx** *msec* **multiplier** *interval-multiplier*] コマンドを使用して設定できます。
- Cisco NX-OS リリース 10.2（2）F 以降、BFD IPv4 および IPv6 エコー セッションの BFD エコー受信間隔の範囲は 10 ～ 999 ミリ秒です。

  Cisco NX-OS リリース 10.2（2）Fより前のリリースでは、IPv4 および IPv6 セッションの BFD エコー間隔は 50 ～ 999 ミリ秒の範囲です。

  この間隔は、 **bfd [ipv4 | ipv6] echo-rx-interval** *msec* コマンドを使用して設定できます。

BFD vPC サブセカンド コンバージェンスの構成

スイッチで vPC コンバージェンスを有効にするには、次の手順を実行します。

始める前に

スイッチのBFD機能を構成します。

手順

ステップ 1 **configure terminal** コマンドを使用して、構成モードを開始します。

例：

```
switch# configure
```

ステップ 2 **feature bfd** コマンドを使用して、vPC スイッチで BFD 構成を有効にします。

例：

```
switch# feature bfd
switch(config)#
```

ステップ 3 **interface port-channel** *number* コマンドを使用して、ポート チャネル構成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。

例：

```
switch(config)# interface port-channel 2
switch(config-if)#
```

ステップ 4 **port-channel bfd track-member-link**コマンドを使用して、ポート チャネル インターフェイス上で IETF BFD を有効にします。

（注）
bfd vpc-watch コマンドは、**port-channel bfd track-member-link** コマンドがすでに構成されている場合にのみ、ポートチャネル インターフェイスで構成できます。

例：

```
switch(config-if)# port-channel bfd track-member-link
```

ステップ 5 **bfd vpc-watch** コマンドを使用して VPC ピア モニタリング インターフェイスを構成し、BFD SCN 通知を有効にします。

例：

```
switch(config-if)# bfd vpc-watch
switch(config-if)#
```

ステップ 6 **bfd interval** [*msec* **min_rx** *msec* **multiplier** *interval-multiplier*] コマンドを使用して、ポート チャネルですべての BFD セッションの BFD セッション パラメータを構成します。

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。

必要な最小の受信間隔は **min_rx** *msec* 、および指定できる最小送信間隔 **bfd interval** *msec* の範囲は、10～999 ms です。デフォルトの間隔は 50 ms です。

multiplier *msec* の乗数の範囲は 1 ～ 50 です。乗数のデフォルト値は 3 です。

（注）
Tx/Rx タイマーが 10 ミリ秒の場合は、1 に対する BFD 間隔乗数を使用します。

例：

```
switch(config-if)# bfd interval 10 min_rx 50 multiplier 3
```

ステップ 7 （任意）**show running-config bfd**と**show bfd neighbors interface port-channel details** コマンドを使用して、BFD 実行中の構成を表示します。

例：

```
switch(config)# show running-config bfd
interface port-channel45
  port-channel bfd track-member-link
```

```
  port-channel bfd destination 10.10.1.1
  bfd vpc-watch ---> VPC watchdog session configuration.

switch(config)# show bfd neighbors interface port-channel 45 details | no-more

Session state is AdminDown
Session type: Singlehop, Vpc-Watch: Enable
Local Diag: 7
Registered protocols:  eth_port_channe
AdminDown for 0 days 2 hrs 47 mins 16 secs
Hosting LC: 0, Down reason: None, Reason not-hosted: None
Parent session, please check port channel config for member info
```

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を設定する例を示します。

```
feature bfd
feature ospfv3
router ospfv3 Test1
interface Ethernet2/7
  ipv6 router ospfv3 Test1 area 0.0.0.0
  ospfv3 bfd
  no shutdown
```

BFDの例を表示

show bfd ipv6 neighbors details コマンドの実行結果の例を次に示します。

```
#show bfd ipv6 neighbors details
```

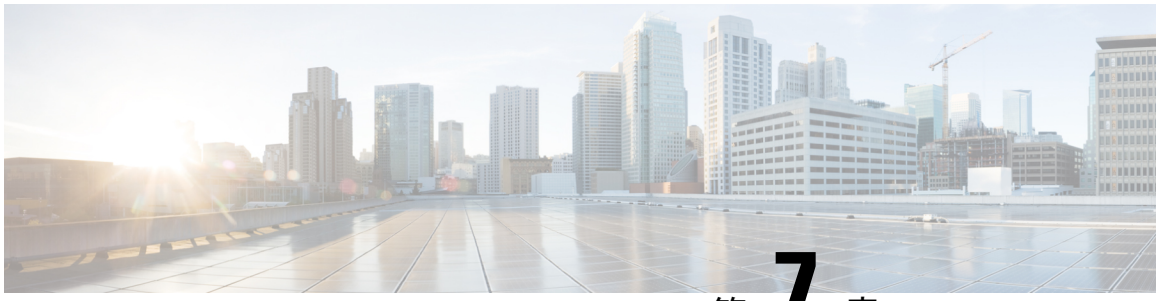
```
OurAddr                         NeighAddr
 LD/RD                 RH/RS           Holdown(mult)      State       Int
    Vrf
cc:10::2                        cc:10::1
 1090519335/1090519260 Up              5692(3)            Up          Po1
    default


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* シリーズ *NX-OS* ユニキャスト ルーティング設定ガイド』

RFC

RFC	タイトル
RFC 5880	*Bidirectional Forwarding Detection*（*BFD*）
RFC 5881	*BFD for IPv4 and IPv6 (Single Hop)*
RFC 7130	*Link Aggregation Group*（*LAG*）インターフェイスでの *Bidirectional Forwarding Detection*（*BFD*）



第 7 章

ポート チャネルの構成

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。

レイヤ 2 ポート チャネル インターフェイスとそのメンバー ポートは、異なる STP パラメータを持つことができます。ポート チャネルの STP パラメータを変更しても、メンバー ポートがバンドルされている場合はポートチャネルインターフェイスが優先されるため、メンバーポートの STP パラメータには影響しません。

（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。

Cisco NX-OSリリース 9.3(7) よりも前のリリースでは、個別（I）として動作するメンバー ポートのポート チャネル設定で、ポート チャネルではなくメンバー ポートで STP ポート タイプを定義できます。

Cisco NX-OS リリース 9.3(7) 以降、個別（I）として動作するメンバー ポートのポート チャネル設定では、メンバー ポートで STP ポート タイプを定義できなくなりました。これは STP によってブロックされたままになります。ポートチャネルでSTPポートタイプを設定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）。

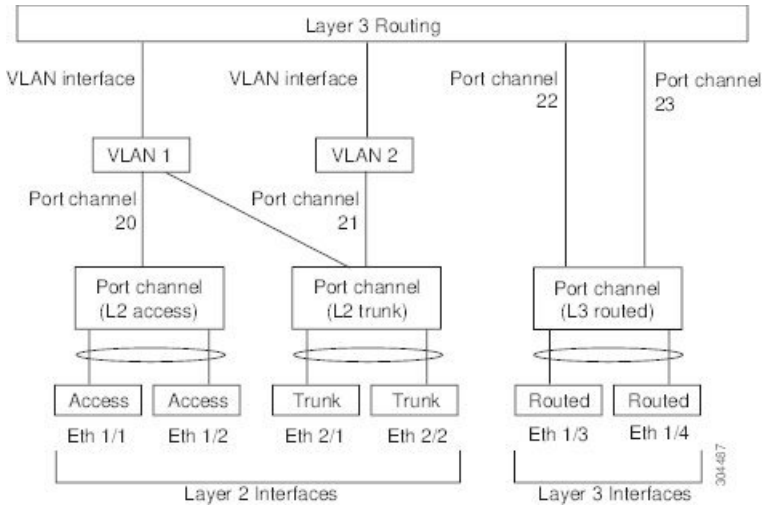
ポート チャネル インターフェイスを作成すると、ポート チャネルを直接作成できます。またはチャネル グループを作成して個別ポートをバンドルに集約させることができます。インターフェイスをチャネル グループに関連付けると、ポート チャネルがない場合は対応するポート チャネルが自動的に作成されます。この場合、ポート チャネルは最初のインターフェイスのレイヤ 2 またはレイヤ 3 設定を行います。最初にポート チャネルを作成することもできます。この場合は、Cisco NX-OS ソフトウェアがポート チャネルと同じチャネル番号の空のチャネル グループを作成してデフォルト レイヤ 2 またはレイヤ 3 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。メンバー ポートがすべてダウンしていれば、ポート チャネルはダウンしています。

ポートチャネル 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 *9*: 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 ポートでスタティック MAC アドレスを設定する情報については、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。

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。

基本設定

ポート チャネル インターフェイスには次の基本設定ができます。

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

互換性要件

チャネル グループにインターフェイスを追加する場合、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

show port-channel compatibility-parameters を使用します 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は、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 アドレス

- スパニングツリー プロトコル
- NAC
- サービス ポリシー
- アクセス コントロール リスト（ACL）

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

- ビーコン
- 説明
- CDP
- LACP ポート プライオリティ
- Debounce
- 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 L4 ポートです。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。**port-channel load-balance** コマンドを使用し、 して、チャネル グループ バンドルのインターフェイス間のロード バランシング方式を設定します。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の方式は src-dst ip-l4 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
- 送信元、宛先、および送信元と宛先の GRE 内部 IP ヘッダー

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。

ユニキャストおよびマルチキャスト トラフィックは、**show port-channel load-balancing**コマンド出力に表示される設定済みのロードバランシング アルゴリズムに基づいて、ポートチャネル リンク間でロードバランシングが行われます。

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。

シンメトリック ハッシング

ポートチャネル上のトラフィックを効果的にモニタできるようにするには、ポートチャネルに接続された各インターフェイスが、順方向と逆方向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、順方向および逆方向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は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は一連のフローに効果的にマッピングされます。

対称ハッシュを有効にすると、送信元および宛先IPアドレスなどのハッシュに使用されるパラメータは、ハッシュアルゴリズムに入力される前に正規化されます。このプロセスにより、パラメータが逆になった場合（順方向トラフィックの送信元が逆方向トラフィックの宛先になる）、ハッシュ出力は同じになります。したがって、同じインターフェイスが選択されます。

次のロードバランシング アルゴリズムがシンメトリック ハッシングをサポートします。

- src-dst ip
- src-dst ip-l4port

ECMP の注意事項と制限事項

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

- MAC ベースのみのハッシュの **port-channel load-balance [src | src-dst | dst] mac** コマンドを入力します。
- IP/レイヤ 4 ポートに基づくハッシュの場合は、**ip load-share** または **port-channel load-balance** コマンドを入力します。

- **port-channel load-balance** コマンドは **ip load-share** コマンドを上書きできます。IP パラメータと MAC パラメータの両方を設定するのに役立つ **port-channel load-balance** コマンドを入力することをお勧めします。
- IP/レイヤ 4 ポートに基づいてハッシュ アルゴリズムを強制するオプションはありません。デフォルトの MAC 設定は、常にポート チャネル設定の一部としてプログラムされます。
- トンネル上のトラフィック フローでは、ECMP の復元力のあるハッシュはサポートされません。
- Cisco NX-OS リリース 10.5(3)F 以降、 IP ロード シェアリング、レイヤ 3 ECMP ダイナミック ロード バランシング、および **opcode**、 **psn**、**queuepair** などの RDMA フィールドが Cisco Nexus 93C64E-SG2-Q、Cisco Nexus 9364E-SG2-O Silicon One スイッチでサポートされます。

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フローをロード バランシングするために使用されるスタティック 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。あるリンクで機能不全が発生すると、残った実行リンクでは、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、障害が発生したリンクにハッシュされなかったフローであっても、一部のパケットが順序どおりに配信されなくなります。

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。すべてのフローが新しいリンク数で再ハッシュされるため、一部のパケットは順序どおりに配信されません。

復元力のあるハッシュは、物理ポートにフローをマッピングし、ECMP グループとポートチャネルインターフェイスの両方でサポートされます。

物理的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、残りの動作中のリンク間で均等に再分配されます。動作中のリンクを流れる既存のフローは再ハッシュされないため、影響を受けません。

復元力のあるハッシュは、IPv4 および IPv6 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。

復元力のあるハッシュは、すべての Cisco Nexus 9000 シリーズ プラットフォーム でサポートされます。Cisco NX-OS リリース 9.3(3) 以降、復元力のあるハッシュは、Cisco Nexus 92160YC-X、92304QC、9272Q、9232C、9236C、92300YC スイッチでサポートされます。

GTP トンネル ロード バランシング

はじめに

GPRS トンネリング プロトコル（GTP）は、コア ルータとして Cisco Nexus 9000 シリーズ スイッチを介してワイヤレス ネットワーク上のモバイルデータを配信するために使用されます。GTP トラフィックを伝送する 2 つのルータがリンク バンドリングで接続されている場合、トラフィックはすべてのバンドル メンバー間で均等に分散される必要があります。

GTP ロード バランシングのさまざまなメカニズム

GTP ロード バランシングを実現するために、2 種類のメカニズムが使用されます。

- Cisco Nexus リリース 10.5（2）以降では、内部 IP ヘッダー フィールドの送信元、宛先 IP アドレス、および IP プロトコルを使用してロード バランシングを維持します。
- Cisco Nexus リリース 10.5（2）より前では、5 タプル ロード バランシング メカニズムが使用されます。ロードバランシング メカニズムでは、パケットの送信元 IP、宛先 IP、プロトコル、レイヤ 4 リソース、および宛先ポート（トラフィックが TCP または UDP の場合）フィールドが考慮されます。GTP トラフィックの場合は、これらのフィールドへの一意の値の数が限られていると、トンネルでのトラフィック ロードの均等分散が制限されます。

内部 IP ヘッダー GTP ロード バランシング メカニズム

内部 IP ヘッダー フィールド source-ip、dest-ip、および ip-protocol を使用して、ロード バランシングが実行されます。対称ロードバランシングは、同じフローの転送トラフィックとリバース トラフィックのスティッキ性を維持するためにサポートされます。

GTP 内部ヘッダー ベースのハッシュは、すべてのインターフェイスで IPv4 と IPv6 の両方で機能します。IPv4 と IPv6 の両方の内部 IP ヘッダーは、すべての cloudscale スイッチの 16 UDF をすべて使用します。内部 IP ヘッダーは、2 スイッチまたは 3 スイッチのバンドルに使用されます。

5 タプル GTP ロード バランシング メカニズム

ロード バランシングにおける GTP トラフィックの偏波を回避するために、GTP ヘッダーのトンネル エンドポイント ID（TEID）が UDP ポート番号の代わりに使用されます。TEID がトンネルごとに異なるため、トラフィックをバンドルの複数のリンク間で均等にロードバランシングすることができます。

この機能は、GTPU パケットに存在する 32 ビット TEID 値で送信元および宛先ポート情報を上書きします。

GTP トンネルのロード バランシング機能により、次のサポートが追加されます。

- 物理インターフェイスでの IPv4/IPv6 トランスポート ヘッダーによる GTP

- TE トンネルを介した GTP トラフィック
- UDP ポート 2152 を使用した GTPU

ip load-sharing address source-destination gtpu コマンドは、GTP トンネル ロード バランシングをイネーブルにします。

ロードバランシング後の GTP トラフィックの出力インターフェイスを確認するには、L4 プロトコルの送信元および宛先ポート番号の代わりに TEID を指定して **show cef {ipv4 | ipv6} exact-route** コマンドを使用します。送信元ポートで TEID の 16MSBist、宛先ポートで TEID の 16LSBits を使用します。

port-channel load-balance src-dst gtpu コマンドは、UDP 宛先ポート番号 2152 の GTP パケットをイネーブルにして、GTP TEID 値に基づいてロードバランシングを行います。このコマンドは、外側の 5 つのタプル（*src-ip*、*dst-ip*、 *ip proto*、*L4 sport*、*L4 dport*）が同じであっても、スイッチが GTP パケットのロードバランシングを行えるようにします。ハードウェア制御はポート チャネルと ECMP の両方で同じであるため、GTP オプションを使用して port-channel load-balance または ip load-sharing を有効にすると、GTP TEID ベースのロード バランシングが有効になります。

- **port-channel load-balance src-dst gtpu** コマンドは、VXLAN カプセル化の有無にかかわらず、両方の GTP パケットに適用できます。
- GTP ヘッダーが外部レイヤの一部である場合、 **port-channel load-balance src-dst gtpu** コマンドはハッシュのために外部レイヤから GTP TEID を取得します。
- GTP ヘッダーが内部レイヤの一部である場合、 **port-channel load-balance src-dst gtpu** コマンドはハッシュのために内部レイヤから GTP TEID を取得します。

show port-channel load-balance forwarding-path コマンドを使用する場合は、プロトコル フィールドを 17 に設定し、他のパラメータの値を設定する必要があります。次に例を示します。

```
switch(config)# show port-channel load-balance forwarding-path interface port-channel 2
 src-ip 1.1.1.1 dst-ip 2.2.2.2 gtpteid
0x3 protocol 17
```

サポートされるプラットフォーム

Cisco Nexus リリース 9.3(3) GTP トンネル ロード バランシングの開始は、9700-EX および 9700-FX ライン カードを搭載した Cisco Nexus 9500 プラットフォーム スイッチでサポートされます。ただし、IPv6 フローの GTP トンネル ロード バランシングは、FM-E2 ファブリック モジュールを搭載した Cisco Nexus 9500 プラットフォーム スイッチでのみサポートされます。それは、FM-E ファブリック モジュールをもつ Cisco Nexus 9500 プラットフォーム スイッチではサポートされません。ハードウェア制御はポート チャネルと ECMP の両方で同じであるため、GTP オプションを使用して port-channel load-balance または ip load-sharing を有効にすると、両方のケースで GTP TEID ベースのロード バランシングが有効になります。マルチカプセル化パケットでは、GTP ヘッダーが外部ヘッダーの一部である場合、ハッシュのために外部レイヤから GTP TEIF を取得します。GTP ヘッダーが内部ヘッダーの一部である場合、内部レイヤから GTP TEIF を取得してハッシュします。

GTP トンネル ロード バランシングは、Cisco Nexus 9300-EX、9300-FX、9300-FX2、および 9300-GX プラットフォーム スイッチでサポートされます。

内部 IP ヘッダー GTP ロード バランシング メカニズムは、次でサポートされます。

- Cisco Nexus 9300-EX プラットフォーム スイッチ
- Cisco Nexus 9300-FX プラットフォーム スイッチ
- 9700-EX と 9700-FX ラインカードを搭載した Cisco Nexus 9500 プラットフォーム スイッチ
- Cisco Nexus 9300-EX、9300-FX、9300-FX2、および 9300-GX プラットフォーム スイッチ
- Cisco Nexus 9364C-H1 スイッチ

（注） Cisco Nexus 9364C-H1 スイッチは、サイズが 8 または 12 バイトの GTP ヘッダーを持つパケットの内部ヘッダー ベースのハッシュをネイティブにサポートできます。

LACP

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

LACP の概要

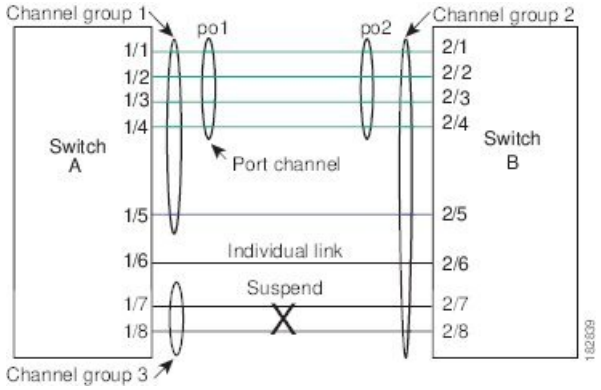
イーサネットのリンク アグリゲーション制御プロトコル（LACP）は、IEEE 802.1AX および IEEE 802.3ad で定義されています。このプロトコルは、物理ポートをまとめて 1 つの論理チャネルを形成する方法を制御します。

（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。ロールバックおよびチェックポイントについては、『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』を参照してください。

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 *10* : 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 グループにまとめることができます。

（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。

（注） LACP vPC コンバージェンス機能を使用するように設定され、Cisco NX-OS リリース 7.0(3)I7(5) を実行している Cisco Nexus 9500 シリーズ スイッチを、それより前のリリースにダウングレードすると、設定は削除されます。スイッチをアップグレードするときには、LACP vPC コンバージェンス機能を再度設定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。

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 *14 :* 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 はこのポート チャネルでイネーブルになっており、ポートはパッシブネゴシエーション状態になっています。ポートは受信した LACP パケットに応答しますが、LACP ネゴシエーションは開始しません。
active	LACP はこのポートチャネルでイネーブルになっており、ポートはアクティブ ネゴシエーション状態です。アクティブモードでは、ポートは LACP パケットを送信することによって他のポートとのネゴシエーションを開始します。
on	LACP はこのポート チャネルでディセーブルであり、ポートは非ネゴシエーション状態です。ポートチャネルが **on** 状態であることは、スタティック モードであることを表します。 ポートはポート チャネル メンバーシップの確認またはネゴシエートを行いません。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。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。**on** 状態が、デフォルト ポート チャネル モードです。

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、2 つのデバイスは LACP ポート チャネルを形成できます。

表 *15 :* チャネルモードの互換性

デバイス 1 > ポート-1	デバイス 2 > ポート-2	結果
アクティブ	アクティブ	ポート チャネルを形成できます。

デバイス 1 > ポート-1	デバイス 2 > ポート-2	結果
Active	Passive	ポート チャネルを形成できます。
パッシブ	パッシブ	ネゴシエーションを開始できるポートがないため、ポート チャネルを形成できません。
点灯	アクティブ	LACPが片側でのみ有効になっているため、ポート チャネルを形成できません。
点灯	パッシブ	LACP が有効になっていないため、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 ポート プライオリティ

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

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

LACP 管理キー

LACP は、LACP を使用するように設定されたポートごとに、チャ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 *16 : 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
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、無効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。これらの条件に対処するため、 **lacp graceful-convergence** コマンドが追加されました。

デフォルトで、ピアから LACP PDU を受信しない場合、ポートは一時停止状態に設定されます。 **lacp suspend-individual** は Cisco Nexus 9000 シリーズ スイッチではデフォルト設定です。このコマンドは、LACP PDU を受信しない場合、ポートを中断状態にします。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。**no 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。個々に設定されているポートは、ポート設定に基づいて個々のポートの属性を取得します。

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。

delayed 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。

ポートチャネルのどのポートが最初に起動するかは、ポートのポート プライオリティ値によって決まります。プライオリティ値が最も低いポート チャネルのメンバー リンクが、LACP 遅延ポートとして最初に起動します。リンクの動作ステータスに関係なく、LACP ポートに設定されたプライオリティが使用され、遅延 lacp ポートが選択されます。

注意事項と制約事項

この機能は、スパニングツリー ポート タイプ トランク モードで VPC が実行されているかどうかにはかかわらず、レイヤ 2 ポートチャネルをサポートします。次のガイドラインと制約事項が LACP に適用されます。

- 同じポートチャネルで **no lacp suspend-individuallacp mode delay** を使用することは、非 lacp 遅延ポートを個別の状態にする可能性があるため、推奨されません。ベスト プラクティスとして、これら 2 つの設定を組み合わせないようにする必要があります。
- レイヤ 3 ポートチャネルではサポートされません。
- Nexus 9000 スイッチでは、FEX NIF ファブリック ポートチャネルまたは FEX HIF ホスト ポートチャネルでサポートされません。

LACP ポートチャネルの最小リンクおよび LACP 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LACP 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 メンバー ポートが少数の場合、LACPポートチャネルが非アクティブになります。

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

LACP MaxBundle 機能では、次の処理が行われます。

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

（注） 最小リンクおよびMaxBundle機能は、LACPポートチャネルだけで動作します。スイッチは、この機能の構成だけなら非 LACP ポートチャネルでも行えますが、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 および非グレースフル スイッチオーバーは、LACP 高速タイマーではサポートされません。

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 チャネルを使用するロード バランシングを設定する必要があります。ロード バランシングの詳細については、「ポート チャネルを使用したロード バランシング」の項を参照してください。

高可用性

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 チャネル設定時のガイドラインおよび制約事項は、次のとおりです。

- Gen 1 ライン カードを備えた Cisco Nexus 9516 スイッチでの拡張ポートチャネルの導入では、コマンドの後にコマンドとコマンドを使用する必要があります。**port-channel scale-fanout copy run start reload**
- キーワードが付いている**show**コマンド**internal**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章の設定」を参照してください）。
- レイヤ 2 ポート チャネルでは、ポートに互換性が設定されていれば、STP ポート パス コストが異なる場合でもポート チャネルを形成できます。互換性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。
- L3 ポート チャネル インターフェイス間に L2 ePBR が構成されている場合、LACP パケットが ePBR デバイスでドロップされるため、ポート チャネルは起動しません。
- 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サポートされます。

- 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」）。
- 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。

- 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。
- Cisco Nexus 92300YC スイッチでは、同じクワドラントの一部である最初の 24 個のポート。同じクワドラントのすべてのポートは同じ速度である必要があります。クワドラント内のポートで異なる速度を使用することはサポートされていません。次に、同じクワドラントを共有するCisco Nexus 92300YCスイッチの最初の24個のポートを示します。
  - 1,4,7,10
  - 2,5,8,11
  - 3,6,9,12
  - 13,16,19,22
  - 14,17,20,23
  - 15,18,21,24
- X96136YC-R ライン カードを搭載した Cisco Nexus 9500 スイッチでは、ポート 17 ー 48 は同じクワドラントの一部です。同じクワドラントのポートは、すべてのポートで同じ速度（1/10G または 25G）である必要があります。クワドラント内のポートで異なる速度を使用することはサポートされていません。クワドラントのいずれかのポートに異なる速度を設定すると、ポートはエラーディセーブル状態になります。同じクワドラントのインターフェイスは次のとおりです。
  - 17 ～ 20
  - 21 ～ 24
  - 25 ～ 28
  - 29 ～ 32
  - 33 ～ 36
  - 37 ～ 40
  - 41 ～ 44
  - 45 ～ 48

- レジリエント ハッシュは、N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RX、および N9K-X96136YC-R ライン カードを搭載した Cisco Nexus 9500 Series スイッチでサポートされています。
- ポートチャネル対称ハッシュは、Cisco Nexus 9200、9300-EX、9300-FX/FX2、および 9300-GX プラットフォーム スイッチと、 、 、N9K-X9736C-FX、および N9K-X9732C-FX ライン カードを搭載した Cisco Nexus 9500プラットフォーム スイッチでサポートされています。
- ECMP 対称ハッシュは、Cisco Nexus 9200、9300-EX、および 9300-FX/FX2 プラットフォーム スイッチと、 、 、N9K-X9736C-FX、および N9K-X9732C-FX ライン カードを搭載した Cisco Nexus 9500 プラットフォーム スイッチでサポートされています。
- GRE内部ヘッダーは、次のスイッチでサポートされます。
  - Cisco Nexus 9364C プラットフォーム スイッチ
  - Cisco Nexus 9336C-FX2、9348GC-FXP、93108TC-FX、93180YC-FX、および 93240YC-FX2 プラットフォーム スイッチ
  - Cisco Nexus 9300-GX プラットフォーム スイッチ
  - N9K-X9736C-FX ライン カードを搭載した Cisco Nexus 9500 プラットフォーム スイッチ
- Cisco NX-OS リリース 9.3(6) 以降では、Cisco Nexus 9300-FX2 プラットフォーム スイッチは VXLAN および IP-in-IP トンネリングの共存をサポートします。制限事項を含む詳細については、「**VXLAN and IP-in-IP Tunneling** 」の項（『*Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x)*』）を参照してください。
- LACP を使用する FEX インターフェイスの場合、FEX インターフェイスのすべての DME 操作/ランタイム プロパティは更新されません。FEX ポートのすべてのランタイム アップデートは、FEX LACP プロセス コンテキストから発生し、親スイッチに通信されません。これは、1 日目の動作です。
- Cisco NX-OS リリース 10.3(1)F 以降、src/dst ip および src/dst L4 ポート番号に基づくハッシュは、Cisco Nexus 9808 プラットフォームスイッチでサポートされます。
- Cisco NX-OS リリース 10.4（1）以降、レイヤ 3 ポートチャネルは Cisco Nexus 9800 と 9332D-H2R スイッチでサポートされます。
- Cisco NX-OS リリース 10.4（2）F 以降、レイヤ 3 ポートチャネルは Cisco Nexus 9232E-B1 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4（1）F 以降、src/dst ip および src/dst L4 ポート番号に基づくハッシュは、次の Cisco Nexus スイッチでサポートされます：
  - Cisco Nexus 9804 プラットフォーム スイッチ
  - Cisco Nexus X98900CD-A および KX9836DM-A ラインカードと Cisco Nexus 9808 および 9804 スイッチです。

- Cisco NX-OS リリース 10.4(2)F 以降、src/dst ip および src/dst レイヤ 4 ポート番号に基づくハッシュは、Cisco Nexus C9232E-B1 スイッチでサポートされます。
- Cisco NX-OS リリース 10.2（2）F以降、 Cisco Nexus 93C64E-SG2-Q スイッチ はこれらの機能をサポートしています。
  - LACP
  - port-channel
- IPv6 フローの GTP トンネル ロード バランシングは、FM-E2 ファブリック モジュールを搭載した Cisco Nexus 9500 プラットフォーム スイッチでのみサポートされます。
- GTP トンネル ロード バランシングは、FM-E ファブリック モジュールをもつ Cisco Nexus 9500 プラットフォーム スイッチではサポートされません。
- GTP トンネル ロード バランシングの IPv4 または IPv6 GTP パケットのハッシュを構成しないでください。
- IPv4 または IPv6 GTP パケットのハッシュ（**hash-mode {gtp-inner-v4 | gtp-inner-v6}**）は、次のプラットフォームではサポートされていません。
  - N9K-C9332D-H2R
  - N9K-C93640CWD-HXB
  - N9K-C9364C-H1
  - N9K-C93400LD-H1

Cisco Nexus 9336C-SE1 のポート チャネルのサポート

- Cisco NX-OS リリース 10.6(1)F以降、 Cisco Nexus 9336C-SE1 はこれらの機能をサポートしています。
  - レイヤ 3 ポートチャネル
  - LACP

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 *17*: デフォルト ポート チャネル パラメータ

パラメータ	デフォルト
ポート チャネル	管理アップ

パラメータ	デフォルト
レイヤ 3 インターフェイスのロード バランシング方式	送信元および宛先 IP アドレス
レイヤ 2 インターフェイスのロード バランシング方式	送信元および宛先 MAC アドレス
モジュールごとのロード バランシング	ディセーブル
LACP	ディセーブル
チャンネル モード	on
LACP システム プライオリティ	32768
LACP ポート プライオリティ	32768
LACP 用最少リンク数	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 チャネルの構成

（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 vlan vlan-id* | *native vlan-id*} コマンドを使用して、 メンバーを設定します。

これは、チャネル 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。

始める前に

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *channel-number* 例：	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

	コマンドまたはアクション	目的
	`switch(config)# interface port-channel 1` `switch(config-if)`	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。

例

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については、「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。

始める前に

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

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** *type slot/port*
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		チャネル グループに追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**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** {**allowed vlan** *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。

	コマンドまたはアクション	目的
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** *type slot/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。

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。

例

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。

始める前に

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

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル 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
	`switch# configure terminal` `switch(config)#`	

ステップ 2	**interface** *type slot/port*
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		チャネル グループに追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**no switchport** 例： `switch(config-if)# no switchport`	インターフェイスをレイヤ 3 ポートとして設定します。
ステップ 4	**channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}] 例： • `switch(config-if)# channel-group 5` • `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** *type slot/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。

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。

例

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

手順

	コマンドまたはアクション	目的

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

ステップ2	**interface port-channel** *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。

	コマンドまたはアクション	目的

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。

例

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. **shutdown**
4. **exit**
5. **show interface port-channel** *channel-number*
6. **no shutdown**
7. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *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	**shutdown**
	例：
	`switch(config-if)# shutdown`
	`switch(config-if)#`
		インターフェイスをシャットダウンします。トラフィックは通過せず、インターフェイスは管理ダウン状態になります。デフォルトは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。

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。

	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。

例

次に、ポート チャネル 2 のインターフェイスをアップする例を示します。

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

ポート チャネルの説明の設定

ポート チャネルの説明を設定できます。

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *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	**description** 例：	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

	コマンドまたはアクション	目的
	`switch(config-if)# description engineering` `switch(config-if)#`	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。

例

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *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)# duplex 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。
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。

例

次に、ポート チャネル 2 に 100 Mb/s を設定する例を示します。

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

ポート チャネルを使ったロード バランシングの設定

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

（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。

始める前に

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-channel load-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*}] [**dst inner-header**] | **src inner-header** | **src-dst inner-header**] [**rotate** *rotate*]
3. **show port-channel load-balance**
4. **show port-channel load-balance** [**forwarding-path interface port-channel** *channel-number* |**src-ip** *src-ip* |**dst-ip** *dst-ip* |**protocol** *protocol* |**gtp-teid** *gtp-teid* |**module** *module_if*]
5. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的
ステップ 2	**port-channel load-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*}] [**dst inner-header**] | **src inner-header** | **src-dst inner-header**] [**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)#` • `switch(config)# port-channel load-balance dst inner-header` `switch(config)#` • `switch(config)# port-channel load-balance src inner-header` `switch(config)#` • `switch(config)# port-channel load-balance src-dst inner-header` `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-l4port** で、非 IP のデフォルトは **src-dst mac** です。 （注） GRE 内部 IP ヘッダーは、送信元、宛先、および送信元と宛先をサポートします。 （注） 次のロードバランシング アルゴリズムがシンメトリック ハッシングをサポートします。 • 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	**show port-channel load-balance** [**forwarding-path interface port-channel** *channel-number* |**src-ip** *src-ip* |**dst-ip** *dst-ip* |**protocol** *protocol* |**gtp-teid** *gtp-teid* |**module** *module_if*]
	例：
	`switch# show port-channel load-balance forwarding-path`
	`load-balance`
		（任意）パケットを転送する EtherChannel インターフェイスのポートを識別します。

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。

MPLS タグ付けトラフィック用にポート チャネルを使ったロード バランシングの構成

始める前に

- mpls の構成 port-channel load-balance と mpls load-sharing オプションは共存できません。
- MPLS タグ付き L2 トラフィックの場合は、mpls オプションを指定してポート チャネル ロード バランシング構成を使用できます。
- mpls オプションを使用した feature-set mpls および port-channel load-balance の構成は、相互に排他的です。
- mpls オプション機能を使用したポートチャネルのロードバランシング機能は、vxlan 機能と共存できません。
- 以下は、mpls label-ip が設定された `<non-mpls options>` を使用したポートチャネル ロード バランスの注意事項および制限事項です。
  - SRC と DST L2 アドレスフィールドの両方が、ASIC の MPLS の 4 つのラベルスタックすべてでオーバーロードされます。SRC-MAC は上位 3 つのラベルでオーバーロードされ、DST-MAC は残った 4 番目のラベルでオーバーロードされます。この機能をイネーブルにすると、ハッシュ用の MPLS IP パケットの SRC および DST L2 MAC フィールドが省略される可能性があります。
    - SRC または DST L2 アドレスフィールドに影響を与える非 mpls オプションの場合ラベル スタック ハッシュの計算に影響します。
- 以下は、mpls label-only が設定された `<non-mpls options>` を使用したポートチャネル ロードバランスの注意事項および制限事項です。
  - SRC と DST IP アドレスフィールドの両方が、ASIC の MPLS ラベルスタック（9 ラベル）でオーバーロードされます（SRC-IP は上位 5 つのラベルでオーバーロードされ、DST-IP は下位 4 つのラベルでオーバーロードされます）。したがって、このバリアントをオンにすると、一般に、ハッシュ用の MPLS パケットの SRC および DST IP フィールドが無視される可能性があります。
  - <non-mpls options> に「SRC IP」のみのバリアントが含まれている場合、上位 5 つの MPLS ラベルのみがハッシュの対象と見なされます（ラベル スタック サイズが 9 の場合）。
  - <non-mpls options> に DST IP のみのバリアントが含まれている場合、下位 4 つの MPLS ラベルのみがハッシュ用に考慮されます（スタック サイズ 9 の MPLS ラベルの場合）。たとえば、ラベルが 5 つしかない MPLS パケットの場合、これらのラベルはいずれもハッシュの対象とは見なされません。7 つのラベルを持つ MPLS パケットの場合、ハッシュの対象となるのは下位 2 ラベルだけです。
  - <non-mpls options> に SRC と DST IP フィールドの両方が含まれていない場合、いずれのラベルもハッシュの対象と見なされません。

• L4 SRC および DST ポートはハッシュの対象になりません。

手順の概要

1. **configure terminal**
2. **port-channel load-balance src-dst ip-l4port mpls** {**label-ip**|**label-only**}
3. （任意） **show port-channel load-balance**

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**port-channel load-balance src-dst ip-l4port mpls** {**label-ip**|**label-only**} 例： `switch(config)# port-channel load-balance src-dst ip-l4port mpls label-ip`	ポート チャネルを使用して MPLS のロード バランシングを指定します。 label-ip：MPLS ラベルと IP に基づいてロード シェアリングを指定します。 label-only：MPLS ラベルのみに基づいてロードシェアリングを指定します。
ステップ 3	（任意） **show port-channel load-balance** 例： `switch(config)# show port-channel load-balance`	ポート チャネル ロードバランシング アルゴリズムを表示します。

例

次の例は、mpls オプションを使用したロードバランス構成です。

```
switch# show port-channel load-balance
System config:
Non-IP: src-dst mac
IP: src-dst ip-l4port mpls label-ip rotate 0
Port Channel Load-Balancing Configura□□on for all modules:
Module 1:
Non-IP: src-dst mac
IP: src-dst ip-l4port mpls label-ip rotate 0
```

内部 IP ヘッダー GTP の構成

次の手順に従って、GTP 内部ヘッダー ハッシングを有効または無効にします：

手順の概要

1. **configure terminal**
2. **[no] port-channel load-balance src-dst inner-header gtp**
3. **[no] hash-mode {gtp-inner-v4 | gtp-inner-v6}**
4. **show port-channel load-balance**

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**[no] port-channel load-balance src-dst inner-header gtp**
	例：
	`switch(config)# port-channel load-balance src-dst inner-header gtp`
	`switch(config)#`	

ステップ 3	**[no] hash-mode {gtp-inner-v4 | gtp-inner-v6}**
	例：
	IPv4 向け
	`switch(config)# hash-mode gtp-inner-v4`
	`switch(config)#`
	IPv6 の場合
	`switch(config)# hash-mode gtp-inner-v6`
	`switch(config)#`
		IPv4 / IPv6 GTP パケットのハッシュを有効または無効にします。
		（注）
		• Cisco Nexus 9364C-H1 スイッチでは、IPv4 または IPv6 GTP パケットのハッシュ構成は必要ありません。
		• Cisco Nexus 9364C-H1 スイッチは、サイズが 8 または 12 バイトの GTP ヘッダーを持つパケットの内部ヘッダーベースのハッシュをネイティブにサポートできます。

ステップ 4	**show port-channel load-balance**
	例：
	`switch(config)# show port-channel load-balance`
	`switch(config)#`
		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。
		`switch# show port-channel load-balance`
		`System config:`
		`  Non-IP: src-dst mac`
		`  IP: src-dst inner-header rotate 0`

	コマンドまたはアクション	目的

		`Port Channel Load-Balancing Configuration for all modules:`
		`Module 1:`
		`  Non-IP: src-dst mac`
		`  IP: src-dst inner-header rotate 0`

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**feature lacp** 例： `switch(config)# feature lacp`	デバイスの LACP をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、LACP をイネーブルにする例を示します。

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

LACP ポート チャネル ポート モードの設定

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

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** *type slot/port*
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		チャネル グループに追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
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。

例

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） **no lacp min-links** コマンドを使用して、デフォルト ポートチャネル最小リンクの設定を復元します。

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。

始める前に

正しいポートチャネル 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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *number*
	例：
	`switch(config)# interface port-channel 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 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。

例

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。

始める前に

正しいポート チャネル インターフェイス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** *number*
3. **lacp max-bundle** *number*
4. **show running-config interface port-channel** *number*

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *number*
	例：
	`switch(config)# interface port-channel 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：	max-bundle を設定するポートチャネルインターフェイスを指定します。

	コマンドまたはアクション	目的
	`switch(config-if)# lacp max-bundle`	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。

例

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** コマンドを使用し、 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。

（注） vPC ピア リンクでの **lacp rate fast** の構成は推奨されません。**lacp rate fast** が vPC ピア リンク メンバー インターフェイスで設定されている場合、LACP ロギング レベルが 5 に設定されている場合にのみ、syslog メッセージにアラートが表示されます。

始める前に

LACP 機能がイネーブルになっていることを確認します。

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

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

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

ステップ 3	**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。

例

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

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

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

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

LACP 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。

始める前に

LACP をイネーブルにします。

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**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。
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。

例

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。

始める前に

LACP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface** *type slot/port*
3. **lacp port-priority** *priority*
4. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** *type slot/port*
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		チャネル グループに追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**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：	（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。

	コマンドまたはアクション	目的
	`switch(config-if)# copy running-config startup-config`	

例

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 システム MAC およびロールの設定

プロトコル交換用の LACP で使用される MAC アドレスとオプションのロールを設定できます。デフォルトでは、LACP は VDC MAC アドレスを使用します。デフォルトでは、ロールはプライマリです。

LACP でデフォルト（VDC）MAC アドレスとデフォルト ロールを使用するには、**no lacp system-mac** コマンドを使用します。

この手順は、Cisco Nexus 9336C-FX2、93300YC-FX2、および 93240YC-FX2-Z スイッチでサポートされています。

始める前に

LACP を有効にする必要があります。

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル 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	**lacp system-mac** *mac-address* **role** *role-value*
	例：
	`switch(config)# lacp system-mac 000a.000b.000c role primary`
	`switch(config)# lacp system-mac 000a.000b.000c role secondary`
		LACP プロトコル交換で使用する MAC アドレスを指定します。ロールはオプションです。プライマリがデフォルトです。

ステップ 3	（任意） **show lacp system-identifier** 例： `switch(config)# show lacp system-identifier`	設定されている MAC アドレスを表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします

例

次に、スイッチのロールをプライマリとして設定する例を示します。

```
Switch1# sh lacp system-identifier
32768,0-b-0-b-0-b
Switch1# sh run  | grep lacp
feature lacp
lacp system-mac 000b.000b.000b role primary
```

セカンダリとしてスイッチのロールを設定する例を示します。

```
Switch2# sh lacp system-identifier
32768,0-b-0-b-0-b
Switch2# sh run | grep lacp
feature lacp
lacp system-mac 000b.000b.000b role secondary
```

LACP グレースフル コンバージェンスのディセーブル化

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

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

始める前に

LACP をイネーブルにします。

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

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

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

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

例

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

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

LACP グレースフル コンバージェンスの再イネーブル化

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

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

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

ステップ 3	**shutdown** 例： `switch(config-if) shutdown`	ポート チャネルを管理シャットダウンします。
ステップ 4	**lacp graceful-convergence** 例：	ポート チャネルの LACP グレースフル コンバージェンスをイネーブルにします。

	コマンドまたはアクション	目的
	`switch(config-if)# lacp graceful-convergence`	
ステップ 5	**no shutdown** 例： `switch(config-if) no shutdown`	ポート チャネルを管理アップします。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

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

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

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。このプロセスは、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ときに、サーバの起動に失敗する原因になることがあります。

（注） **lacp suspend-individual** のみを入力する必要があります エッジ ポートのコマンド。このコマンドを使用する前に、ポート チャネルが管理上のダウン状態である必要があります。

始める前に

LACP をイネーブルにします。

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

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

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

ステップ 3	**shutdown** 例： `switch(config-if) shutdown`	ポート チャネルを管理シャットダウンします。
ステップ 4	**no lacp suspend-individual** 例： `switch(config-if)# no lacp suspend-individual`	ポート チャネルで LACP 個別ポートの一時停止動作をディセーブルにします。
ステップ 5	**no shutdown** 例： `switch(config-if) no shutdown`	ポート チャネルを管理アップします。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、ポート チャネルで LACP 個別ポートの一時停止をディセーブルにする方法を示します。

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

LACP の個別一時停止の再イネーブル化

デフォルトの LACP 個別ポートの一時停止を再度イネーブルにできます。

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

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

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

ステップ 3	**shutdown** 例： `switch(config-if) shutdown`	ポート チャネルを管理シャットダウンします。
ステップ 4	**lacp suspend-individual** 例： `switch(config-if)# lacp suspend-individual`	ポート チャネルで LACP 個別ポートの一時停止動作をイネーブルにします。
ステップ 5	**no shutdown** 例： `switch(config-if) no shutdown`	ポート チャネルを管理アップします。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、ポート チャネルで 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 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。遅延 LACP 機能を設定するには、ポートチャネルでコマンドを使用してから、ポートチャネルの 1 つのメンバーポートで LACP ポート プライオリティを設定します。**lacp mode delay**

（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） 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。

手順の概要

1. **configure terminal**
2. **interface port-channel** *number*
3. **lacp mode delay**

手順の詳細

手順

	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 を有効化します。 （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。

	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」を参照してください。 LACPポートのプライオリティによって、遅延LACPポートの選択が決まります。プライオリティの数値が最小のポートが選択されます。 複数のポートの優先順位が同じ場合、VDCシステムMACを使用して、使用するvPCが決定されます。次に、非vPCスイッチまたは選択されたvPCスイッチ内で、最も小さいイーサネットポート名が使用されます。 遅延LACP機能を設定し、ポートチャネルフラップで有効にすると、遅延LACPポートは通常のポートチャネルのメンバーとして動作し、サーバとスイッチ間でデータを交換できるようになります。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） 遅延LACPポートの選択は、ポートチャネルがスイッチまたはリモート サーバでフラップするまで完了または有効になりません。

例

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 をディセーブル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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**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。（`[まだ続けますか（はい / いいえ）？ [はい]（Do you still want to continue(y/n)? [yes]）]`）

ステップ 3	**copy running-config startup-config** 例：	（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。

	コマンドまたはアクション	目的
	`switch(config)# copy running-config startup-config`	

例

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** {*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。（`[まだ続けますか（はい / いいえ）？[はい]（Do you still want to continue(y/n)? [yes]）]`）

ステップ 4	**copy running-config startup-config** 例：	（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。

	コマンドまたはアクション	目的
	`switch(config)# copy running-config startup-config`	

例

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
```

ECMP の復元力のあるハッシュの有効化

復元力のあるECMPでは、ECMPグループからメンバーが削除されたときでも、既存のフローへの影響が最小限に抑えられます。これは、削除されたメンバーが以前占有していたインデックスにおいて、ラウンドロビン方式で既存のメンバーを複製することによって実現されます。

手順の概要

1. **configure terminal**
2. **hardware profile ecmp resilient**
3. **copy running-config startup-config**
4. **reload**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル設定モードを開始します。
ステップ 2	**hardware profile ecmp resilient** 例： `switch(config)# hardware profile ecmp resilient`	ECMP の復元力のあるハッシュを有効にすると、次のメッセージを表示されます。**警告：コマンドは次のリロード後に有効になります。** （注） このコマンドは、Cisco Nexus 9808/9804 プラットフォーム スイッチではサポートされていません。
ステップ 3	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

	コマンドまたはアクション	目的
ステップ 4	**reload** 例： `switch(config)# reload`	スイッチをリブートします。

ECMP の復元力のあるハッシュの無効化

始める前に

ECMP の復元力のあるハッシュが有効になっています。

手順の概要

1. **configure terminal**
2. **no hardware profile ecmp resilient**
3. **copy running-config startup-config**
4. **reload**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル設定モードを開始します。
ステップ 2	**no hardware profile ecmp resilient** 例： `switch(config)# no hardware profile ecmp resilient`	ECMP の復元力のあるハッシュを無効にし、次のメッセージを表示します。**警告：コマンドは次のリロード後に有効になります。**
ステップ 3	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
ステップ 4	**reload** 例： `switch(config)# reload`	スイッチをリブートします。

ECMP ロード バランシングの設定

ECMP ロード シェアリング アルゴリズムを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

始める前に

手順の概要

1. **ip load-sharing address** {**destination port destination** | **source-destination** [**port source-destination** | **gre** | **gtpu** | **ipv6-flowlabel** | **ttl** | **udf offset** *offset* **length** *length* | **symmetricinner** *allgreheader*]} [**universal-id** *seed*] [**rotate** *rotate*] [**concatenation**]
2. （任意） **ip load-sharing address** {**source** |**destination port destination** | **source-destination** [**port source-destination**[**rocev2**[**opcode** | **psn** | **queuepair**]]]} [**universal-id** *seed*]
3. （任意） **show ip load-sharing**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**ip load-sharing address** {**destination port destination** | **source-destination** [**port source-destination** | **gre** | **gtpu** | **ipv6-flowlabel** | **ttl** | **udf offset** *offset* **length** *length* | **symmetricinner** *allgreheader*]} [**universal-id** *seed*] [**rotate** *rotate*] [**concatenation**]
	例：
	`ip load-sharing address source-destination`
	例：
	`switch(config)# ip load-sharing address source-destination ipv6-flowlabel`
	例：
	`switch(config)# ip load-sharing address source-destination ttl`
	例：
	`switch(config)# ip load-sharing address source-destination udf offset 8 length 8`
	例：
	`switch(config)# [no] ip load-sharing address source-destination port source-destination symmetric`
	例：
	`switch(config)# ip load-sharing address source-destination port source-destination inner [all|greheader]`
		データ トラフィックに対する ECMP ロード シェアリング アルゴリズムを設定します。
		• **gre** オプションは、Generic Routing Encapsulation（GRE）キーの送信元と宛先の値を指定します。
		• **gtpu** オプションは、ポートの送信元/宛先の GPRS トンネリング プロトコル（GTP）トンネル エンドポイント識別子（TEID）値を指定します。
		• **ipv6-flowlabel** オプションには、ECMP ハッシュを計算するための IPv6 フロー ラベルが含まれます。これにより、異なるフローラベル値に基づいてすべてのリンクにトラフィック フローが分散されます。**port-channel load-balance** コマンドを使用してレイヤ 4 パラメータが有効になっている場合、このオプションを有効または無効にすると、ポートチャネルのロードバランシングも有効または無効になります。このオプションを使用できるのは、以下の デバイスのみです。
		• Cisco Nexus 9332C および 9364C プラットフォーム スイッチ

	コマンドまたはアクション	目的
		• X9700-EX/FX ライン カードおよび FM-E2 ファブリック モジュールを搭載して、Cisco Nexus 9500 プラットフォーム スイッチ（すべてのルーティング モードで） • X9700-EX / FX ライン カードおよび FM-E ファブリック モジュールを搭載した Cisco Nexus 9500 プラットフォーム スイッチ（ライン カードで IPv6 ルートがプログラムされている、非階層型ルーティング モードで） • Cisco NX-OS リリース 9.3(5) 以降では、Cisco Nexus N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX スイッチがこのオプションをサポートしています。 • **ttl** オプションには、ECMP ハッシュを計算するための存続可能時間情報が含まれています。これにより、異なる TTL 値に基づいてすべてのリンクにトラフィック フローが分散されます。IPv4フローの場合は、ttl 値に基づきます。IPv6 フローの場合は、ホップ制限に基づきます。**port-channel load-balance** コマンドを使用してレイヤ 4 パラメータが有効になっている場合、このオプションを有効または無効にすると、ポートチャネルのロードバランシングも有効または無効になります。Cisco Nexus 9364C および 9300-EX/FX/FX2 プラットフォームスイッチだけがこのオプションをサポートします。Cisco NX-OS リリース 9.3(5) 以降では、Cisco Nexus N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX スイッチがこのオプションをサポートしています。 • **udf** オプションには、ECMP ハッシュを計算するためのユーザ定義フィールドが含まれます。UDF フィールドのオフセット ベースと長さ（ビット単位）は設定できます。オフセット ベースの範囲は 0 ー 127 バイトです。UDF フィールドの長さの範囲は1ー32 ビットです。**port-channel load-balance** コマンドを使用してレイヤ 4 パラメータが有効になっている場合、このオプションを有効または無効にすると、ポー

	コマンドまたはアクション	目的
		トチャネルのロードバランシングも有効または無効になります。Cisco Nexus 9364C および 9300-EX/FX/FX2 プラットフォームスイッチだけがこのオプションをサポートします。Cisco NX-OS リリース 9.3(5) 以降では、Cisco Nexus N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX スイッチがこのオプションをサポートしています。 • **symmetric** オプションは、対称ハッシュをグローバルに有効にします。ECMP 対称ハッシュを無効にするには、コマンドで **no** キーワードを使用します。このコマンドは、グローバル コンフィギュレーション モードで実行する必要があります。 （注） 対称ハッシュが効果的に機能するために、構成された **universal-id** シード値が ECMP 対称ハッシュのパス内のノード間で一貫していることを確認します。 • **inner** オプションは、GREトラフィックの内部ヘッダーベースのハッシュをグローバルに有効にします。内部ヘッダーベースのハッシュを無効にするには、コマンドで **no** キーワードを使用します。このコマンドは、グローバル コンフィギュレーション モードで実行する必要があります。 • **all** ：GRE カプセル化パケットにこのオプションを設定すると、内部ヘッダーを使用する ECMP のパスのハッシュ化を開始します。これは、他のカプセル化タイプにも影響を与える可能性があります。これは、Cisco Nexus 9364C および 9300-EX/FX/FX2 プラットフォームスイッチ、および X9700-EX/FX ライン カードを搭載した Cisco Nexus 9500 プラットフォーム スイッチでサポートされています。 • **greheader** ：このオプションは、GRE カプセル化パケットに対してのみ設定できるもので、内部ヘッダーを使用する ECMP のパスのハッシュ化を開始します。これは、Cisco Nexus 9364C および 9300-FX/FX2 プ

	コマンドまたはアクション	目的
		ラットフォーム スイッチ、およびX9700-FX ライン カードを搭載した Cisco Nexus 9500 プラットフォーム スイッチでサポートされています。 次のオプションは、すべての IP ロード シェアリング設定で使用できます。 • **universal-id** オプションは、ハッシュ アルゴリズムのランダム シードを設定することにより、フローをあるリンクから別のリンクにシフトします。 汎用 ID を設定する必要はありません。ユーザが設定しなかった場合は、Cisco NX-OS が汎用 ID を選択します。*universal-id* の範囲は 1 ～ 4294967295 です。 • **rotate** オプションを使用すると、ハッシュ アルゴリズムは、リンク ピッキングの選択をローテーションさせます。これは、ネットワーク内のすべてのノードが同じリンクを継続的に選択しないようにするためです。これは、ハッシュ アルゴリズムのビットパターンに影響を与えることによって機能します。このオプションは、あるリンクから別のリンクにフローをシフトし、最初の ECMP レベルからすでにロード バランシング（極性化）されているトラフィックのロードバランシングを複数のリンク間で行います。 *rotate* 値を指定すると、64 ビットのストリームが、循環回転でのそのビット位置から解釈されます。*rotate* 値の範囲は 1 ～ 63 で、デフォルトは 32 です。 （注） 多層レイヤ3トポロジでは、極性が発生する可能性があります。極性を回避するには、トポロジの各層で異なる循環ビットを使用します。 （注） ポート チャネルの rotation 値を設定するには、**port-channel load-balance src-dst ip-l4port rotate** *rotate* コマンドを使用します。

	コマンドまたはアクション	目的
		• **concatenation** オプションを使用すると、ECMP のハッシュ タグ値とポート チャネルのハッシュ タグ値がひとつに結合され、より強力な 64 ビットのハッシュを使用できるようになります。このオプションを使用しない場合、ECMP のロード バランシングおよびポート チャネルのロードバランシングを個別に制御できます。デフォルトではディセーブルになっています。

ステップ 2	（任意） **ip load-sharing address** {**source** |**destination port destination** | **source-destination** [**port source-destination**[**rocev2**[**opcode** | **psn** | **queuepair**]]]} [**universal-id** *seed*]
	例：
	`switch(config)# ip load-sharing address source universal-id 2`
	`switch(config)# ip load-sharing address source-destination universal-id 2`
	`switch(config)# ip load-sharing address destination port destination universal-id 2`
	`switch(config)# ip load-sharing address source-destination universal-id 2`
	`switch(config)# ip load-sharing address source-destination port source-destination rocev2 opcode universal-id 2`
		Cisco Nexus 93C64E-SG2-Q、Cisco Nexus 9364E-SG2-O Silicon One スイッチでデータ トラフィックに対する ECMP および DLB ECMP ロード シェアリング アルゴリズムを構成します。
		5 タプル（送信元IP、接続先IP、宛て先ポート、送信元ポート、およびIPv4プロトコル）とは別に、**ip load-sharing** コマンドは次のオプションをサポートします。
		• **rocev2**：rocev2 パラメータは、ロード バランシングに使用されます。 **opcode**、 **psn**、 および **queuepair**のいずれかのパラメータまたはその組み合わせを使用します。
		（注）
		rocev2 psn をロード バランシングに使用すると、パケット リオーダーが発生する可能性があります。
		• **universal-id**：このオプションは、ハッシュ アルゴリズムのランダム シードを設定することにより、フローをあるリンクから別のリンクにシフトします。ユーザーが汎用 ID を構成しなかった場合は、Cisco NX-OS が汎用 ID を構成します。汎用 ID の範囲は 1 ～ 65535 です。
		（注）
		universal-id オプションは、DLB ECMPフロー署名には使用されません。
		ip load-sharing コマンドの構成時に、
		• ECMPの場合、5 つのタプル オプションのいずれかを選択すると、フロー署名はそのオプションのみを考慮します。

	コマンドまたはアクション	目的
		• ダイナミック ロード バランシング（DLB）ECMPの場合、フロー署名は、5 つのタプル オプションのうち 1 つ以上を選択した場合でも、常に 5 つのタプル オプションを使用します。 DLB ECMPの Silicon One スイッチでのIPロード シェアリングの詳細については、 Cisco.com の『 Cisco Nexus 9000 Series NX- OS Unicast Routing Configuration Guide 』の「 *Dynamic Load Balancing on Silicon One switches*」の項を参照してください。
ステップ 3	（任意） **show ip load-sharing** 例： `switch(config)# show ip load-sharing address source-destination`	データ トラフィックに対する ECMP のロード シェアリング アルゴリズムを表示します。 このコマンドは Cisco Nexus 93C64E-SG2-Q、Cisco Nexus 9364E-SG2-O Silicon One スイッチ上のデータトラフィックのみに対する DLB ECMPロードシェアリング アルゴリズムも表示します。

ECMP の復元力のあるハッシュ設定の確認

ECMP の復元力のあるハッシュ設定情報を表示するには、次の作業を行います。

コマンド	目的

`switch(config)# show running-config | grep "hardware profile ecmp resilient`
`hardware profile ecmp resilient`
`switch(config)#`
	機能が有効になったステータスを表示します。

`switch(config)# show running-config | grep "hardware profile ecmp resilient` `switch(config)#`	機能が無効になったステータスを表示します。

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。

コマンド	目的
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ー ポート間で同じにするパラメータを表示します。
show port-channel database [**interface port-channel** *channel-number*]	1 つ以上のポート チャネル インターフェイスの集約状態を表示します。
show port-channel 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。

コマンド	目的
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。

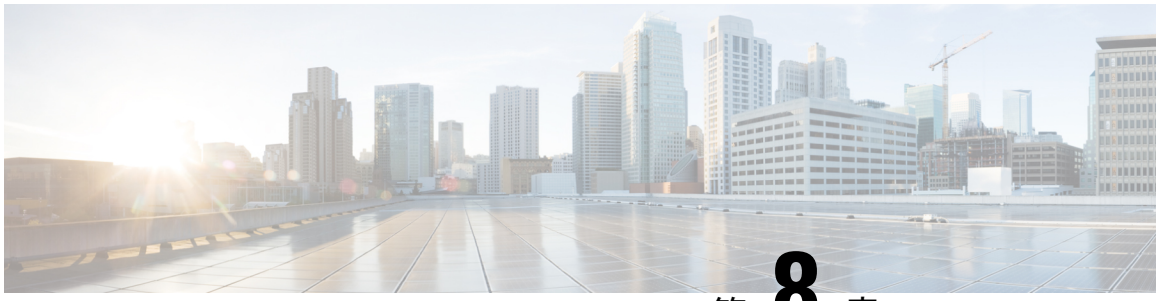
```
switch# configure terminal
switch (config)# feature lacp
switch (config)# interface port-channel 5
switch (config-if)# interface ethernet 1/4
switch(config-if)# switchport
switch(config-if)# channel-group 5 mode active
switch(config-if)# lacp port priority 40000
switch(config-if)# interface ethernet 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*』
高可用性	『*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

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 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。

- 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。

リモート対応ポートチャネル（vPC）は、単一のダウンストリームデバイスが2つのアップストリームデバイスに接続して、それらが1つの論理デバイスであるかのように使用できるようにするテクノロジーです。

- レイヤ 2 のポート チャネルのサポート
- オプションのリンク集約制御プロトコル（LACP）
- 冗長性とロードバランシングのイネーブル化

vPC はLACPの有無にかかわらずトランクモードポートチャネルをサポートし、ネットワークの安定性とコンバージェンスを向上させます。

vPC プロトコルの詳細と推奨事項

vPC で使用できるのは、レイヤ 2 ポート チャネルだけです。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を使用する場合、各デバイスには 32 個のアクティブ リンクと 8 個のスタンバイ リンクを設定できます。

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

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。

vPC を有効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。

（注） ポート チャネルを使用して vPC ドメインに接続されたデバイスは、両方の vPC ピアに接続する必要があります。

図 *11* : *vPC* のアーキテクチャ

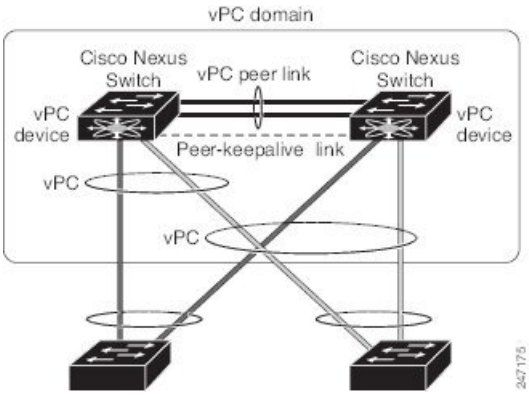
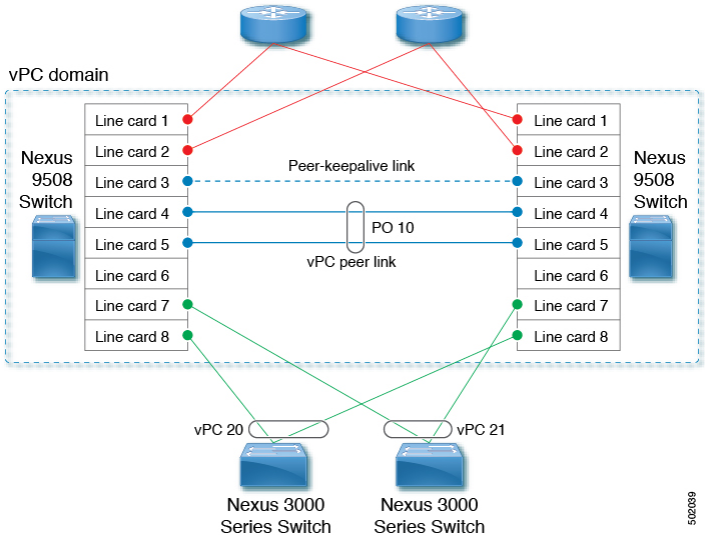


図 *12* : *vPC* インターフェイス



例：vPC ピア リンクの作成

1 ギガビット イーサネット以上の速度のイーサネット ポートを 2 つ以上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 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、再度専用ポート モードで 1 ギガビット以上の 速度の 2 つ以上のイーサネット ポートを使用して、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。

ハードウェアまたはモジュールの誤った使用法

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。

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。

オブジェクト推奨の追跡

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。

1 つのモジュール上ですべての vPC ピア リンクとコア側インターフェイスを設定しなければならない場合は、トラック オブジェクトを設定する必要があります。

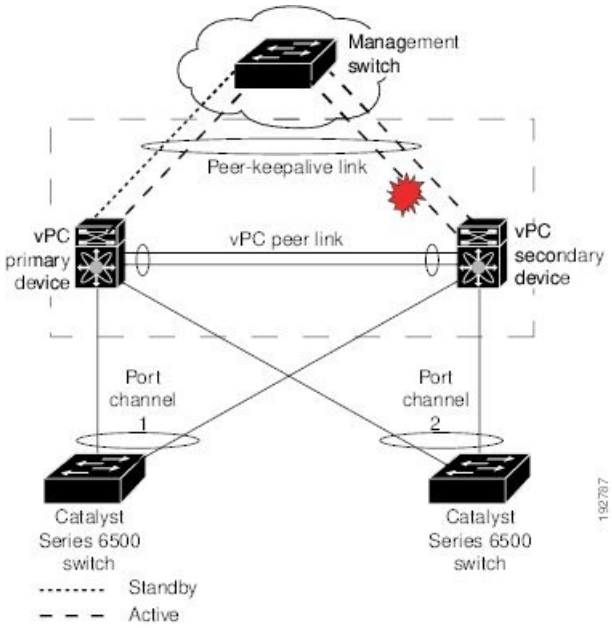
vPC の用語

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。このリンクは、少なくとも 10 ギガビット イーサネット インターフェイスを使用する必要があります。より広い帯域幅のインターフェイス（25 ギガビット イーサネット、40 ギガビット イーサネット、100 ギガビット イーサネットなど）も使用できます。
- 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 *13 : 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。

- 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 vPC 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 vPC 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。

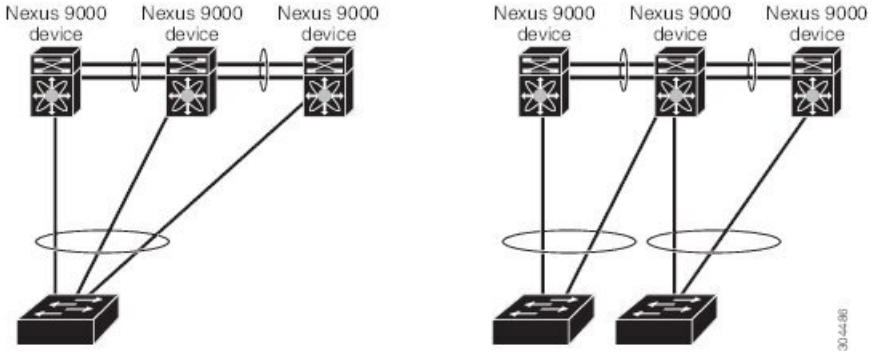
vPC ピア リンクの概要

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 ピア構成

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 *14* : 許可されていない *vPC* ピア設定



vPC ピア リンクと冗長性の構成

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 vPC 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 vPC 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。

互換性と構成の一貫性

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。

プライマリおよびセカンダリのデバイス ロール

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）。デフォルトの場合、Cisco NX-OS ソフトウェアでは、最小の MAC アドレスを基にプライマリ デバイスが選択されます。ただし、ロール プライオリティが設定されて

いる場合は、プライオリティが最も低いデバイスがプライマリ デバイスとして選択されます。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。

トラフィック ロードとロード バランシング

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）。

構成および MAC アドレスの同期

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、「CFSoE （324 ページ）」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、「CFSoE （324 ページ）」の項を参照）

vPC ピア リンク障害およびピア キープアライブ

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。

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、vPC 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 ルート構成

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 インターフェイスの構成

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 アクティブ構成

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）。

UDLD 構成に関する推奨事項

単方向リンク検出（UDLD）の構成では、次の留意点に注意してください。

- LACP がポート チャネル集約プロトコルとして使用されている場合は、vPC ドメイン内に UDLD は必要ありません。
- LACP がポート チャネル集約プロトコル（静的なポート チャネル）として使用されていない場合は、vPC メンバー ポートの通常モードで UDLD を使用します。
- STP が Bridge Assurance なしで使用されている場合と LACP が使用されていない場合は、vPC 孤立ポートの通常モードで UDLD を使用します。

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 vPC ピア リンク自体を使用することはしないでください。

障害検出タイマーとキープアライブ タイマー

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 リンクがダウンすると開始します。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とタイムアウトのパラメータ

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 キープアライブ リンクとメッセージの設定」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。

ピアキープアライブ IP アドレスは、グローバル ユニキャスト アドレスである必要があります。リンクローカル アドレスはサポートされていません。

ピアキープアライブの信頼できるポートの構成

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。

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構成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 ドメインの作成およびピア リンクの構成

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。vPC ピアごとにに設定できる vPC ドメイン ID は 1 つだけです。

各デバイス上で、vPC 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構成する必要があります。各デバイス上で vPC 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、静的にしか構成できません。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構成でき

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 システム MAC アドレスの割り当て

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 テーブルを表示する詳細については、「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 システム プライオリティ

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

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。

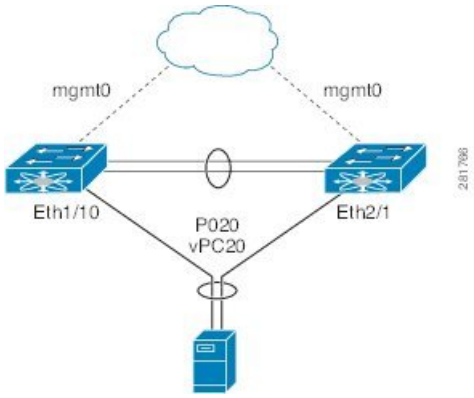
process_summary

このドキュメントでは、2 つの一般的な vPC トポロジについて説明します。つまり、 Cisco Nexus 9000 シリーズ デバイスを直接接続する基本設定と、ホスト vPC にファブリック エクステンダ（FEX）を含める構成です。

process_workflow

1. 最初のトポロジでは、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。

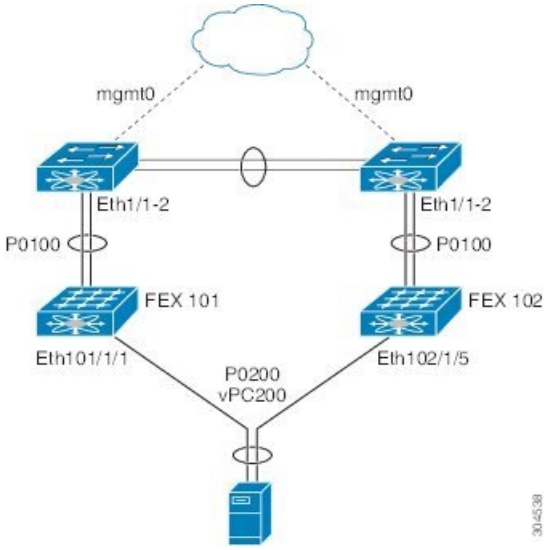
図 *15 : vPC* トポロジのスイッチ



この構成では、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。

2. 第 2 のトポロジは、ファブリック エクステンダ（FEX）を介してピア デバイスから vPC を設定する方法を示しています。

図 *16 : FEX Straight-Through* トポロジ（ホスト *vPC*）



この FEX ストレート スルー トポロジでは、各 FEX は Cisco Nexus 9000 シリーズ デバイスとシングルホーム接続されます。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。たとえば、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。

whats_next

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）。

vPC ピア リンクは vPC機能のコア コンポーネントであり、両方のピア デバイスに一貫した設定が必要です。

- vPC ピア リンクのレイヤ2ポートチャネルはトランクモードに設定する必要があります。
- 互換性パラメータは、vPC内のすべてのインターフェイスで同一である必要があります。

たとえば、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。

構成および注意事項

vPC 機能をイネーブルにし、vPC ピア リンクを設定した後、Cisco Fabric Services（CFS）は、ローカルとリモートの vPC ピア デバイス間の設定の一貫性を確保します。

（注） **show vpc consistency-parameters** を入力します。 vPC 内のすべてのインターフェイスで設定されている値を表示します。表示される構成は、vPC ピア リンクおよび vPC の稼働を制限する可能性のある構成だけです。

（注） 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。

正規のポート チャネルの詳細については、「ポート チャネルの構成」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） **show vpc consistency-parameters** を入力します。 vPC 内のすべてのインターフェイスで設定されている値を表示します。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** および **show vpc consistency-parameters** コマンドを実行し、syslog メッセージを確認します。

show vpc または **show vpc brief** コマンドの出力では、vPC ポートチャネルが 50 回構成されるたびに、次のメッセージが表示されます。

「show vpc consistency-parameters vpc <vpc-num>」を実行して、ダウンした vpc の整合性の理由および任意の vpc のタイプ 2 の整合性の理由を確認してください。

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。vPC ピア リンクの 1 個のデバイスだけで設定されている VLAN は、vPC または vPC ピア リンクを使用してトラフィックを通過させません。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 フィルタ
  - BPDU ガード
  - コスト
  - リンク タイプ
  - プライオリティ
  - VLAN（Rapid PVST+）
- 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。

整合性検査の動作

graceful consistency-check コマンドはデフォルトで設定されます。

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。

スイッチの vPC ポート チャネルを削除すると、vPC の役割に関わらず、ピア スイッチの対応する vPC ポート チャネルで許可される VLAN が一時停止されます。

vPC 番号

vPC ドメイン ID と vPC ピア リンクを作成し終えたら、ダウンストリーム 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。

ヒットレス vPC ロールの変更

仮想ポート チャネル（vPC）は、2 つの異なる Cisco Nexus 9000 シリーズ デバイスに物理的に接続されたリンクを、単一のポート チャネルとして扱えるようにします。vPC ロールの変更機能は、トラフィック フローに影響を与えることなく、vPC ピア間で vPC ロールを切り替えることができるようにします。vPC ロールの切り替えは、vPC ドメインに属しているデバイスのロール優先順位の値に基づいて行われます。vPC ロールの切り替え中にロール優先順位が低い vPC ピア デバイスがプライマリ vPC デバイスとして選択されます。vpc role preempt コマンドを使用して、ピア間で vPC ロールを切り替えることができます。

ヒットレス vPC ロール変更の設定方法については、ヒットレス vPC ロール変更の設定 （364 ページ） を参照してください。

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。

vPC オブジェクト トラッキング

（注） Cisco Nexus 9500 デバイスの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。これは、障害の可能性を減らすために推奨されます。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。

vPC オブジェクト トラッキングは、vPC ピア リンクとコアへのアップリンクの両方が存在するモジュールで障害が発生した場合、トラフィックのブラックホールになってしまうことを防止するために使用されます。トラッキング インターフェイス機能により、影響を受けるスイッチで vPC を一時停止し、トラフィックのブラックホールとなるのを防ぐことができます。

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 vPC ピア リンクがダウンしたときにスイッチオーバーをトリガーする場合は、次の追跡リストでブール AND を使用します。

単一モジュール上の関連するすべてのインターフェイスが故障したときに vPC をリモート ピアに切替えるように追跡リストを設定するには、次の手順に従います。

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 リンク上でブリッジ アシュアランスが自動的に有効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 拡張機能も有効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** を開始します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 フィルタ
- BPDU ガード
- コスト
- リンク タイプ
- プライオリティ
- VLAN（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。

show spanning-tree コマンドを使用すればコマンドで 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。この機能により、一対の Cisco Nexus 9000 シリーズ デバイスをレイヤ 2 トポロジ内に 1 つの STP ルートとして表示できます。この機能は、STP

ルートを vPC プライマリ スイッチに固定する必要性をなくし、vPC プライマリ スイッチに障害が発生した場合の vPC コンバージェンスを向上させます。

ループを回避するために、vPC ピア リンクは STP 計算からは除外されます。vPC ピア スイッチ モードでは、ダウンストリーム スイッチでの STP BPDU タイムアウトに関連した問題（この問題は、トラフィックの中断につながります）を避けるために、STP BPDU が両方の vPC ピア デバイスから送信されます。

この機能は、すべてのデバイス vPC に属する純粋なピア スイッチ トポロジで使用できます。

（注） ピア スイッチ機能は、vPC を使用するネットワークでサポートされ、STP ベースの冗長性はサポートされません。ハイブリッド ピア スイッチ設定で vPC ピア リンクに障害が発生すると、トラフィックが失われる場合があります。このシナリオでは、vPC ピアは同じ STP ルート ID や同じブリッジ ID を使用します。アクセス スイッチのトラフィックは 2 つに別れ、その半分が最初の vPC ピアに、残りの半分が 2 番目の vPC ピアに転送されます。vPC 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 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。

peer-gateway コマンドを使用し、 コマンドを使用します。

（注） この項で説明している **peer-gateway exclude-vlan** コマンド（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構成する際に使用）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、vPC 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 vPC 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 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** を有効にする必要があります 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、vPC 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 デバイス用の Cisco NX-OS ソフトウェアは、vPC で次をサポートします。

- PIM Any Source Multicast（ASM）。
- PIM Source-Specific Multicast（SSM）。

（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。

全体的なマルチキャスト コンバージェンス時間は、スケールと vPC ロールの変更 / PIM 再起動期間に依存します。

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）上のスイッチ仮想インターフェイス（SVI）とダウンストリーム デバイス間の PIM 隣接関係はサポートされません。この設定により、マルチキャストパケットがドロップされる可能性があります。ダウンストリームデバイスと PIM ネイバー関係が必要な場合は、vPC SVI ではなく、物理レイヤ 3 インターフェイスを Nexus スイッチで使用する必要があります。

vPC VLAN 上の SVI では、vPC ピアスイッチとの PIM 隣接関係が 1 つだけサポートされます。vPC-SVI の vPC ピアスイッチ以外のデバイスとの vPC ピアリンク上の PIM 隣接関係はサポートされていません。

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** を使用します コマンドを使用します。このコマンドにより、マルチキャスト ルートに 0 OIF があっても PIM はジョインを送信できます。vPC デバイスでは、非フォワーダは送信元へ PIM (S,G) ジョインをアップストリームに送信します。欠点は、非フォワーダからのリンク帯域幅のアップストリームが最終的にそれによってドロップされるトラフィックに使用されることです。コンバージェンスの向上によるメリットは、リンク使用帯域幅をはるかに上回っていることです。したがって、vPC を使用する場合は、このコマンドを使用することを推奨します。

vPC ピア リンクとルーティング

ファースト ホップ 冗長性プロトコル（FHRP）は、vPC と相互運用します。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 コマンドを使用すれば コマンドを使用して、ピアの隣接が形成され、VLAN インターフェイスがバックアップされるまで、vPC+ の回復を遅らせるようにリストア タイマーを設定します。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。**delay restore** コマンドを使用して、この機能を設定します。

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

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。

vPC ピア リンクのレイヤ 3 バックアップ ルートの構成

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。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。

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 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** または **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。

引数を使用せずに **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。

vPC 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、vPC 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

データセンターが停止すると、vPC ドメインの両方の vPC ピア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

vPC 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。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、そのピアがオンラインになるのに失敗した場合に、**auto-recovery** コマンドを使用して、 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、vPC 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 ロールのプライマリ デバイスとしても機能します。

自動回復リロード遅延

vPC ピアの自動回復は、**auto-recovery reload-delay** コマンドを使用して遅延させることができます。自動回復リロード遅延時間は、最初にアップしたピアで使用されます。**reload-delay time** コマンドは、両方のピアが回復するのを待機し、既存のロールを保持してから自動回復を開始するために使用します。デバイスは、回復したスイッチに対してプライマリ ロールを再開します。

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。

高可用性

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 アップグレードシナリオ

次の手順では、vPC ドメイン内の Cisco Nexus 9500 スイッチのペアを、同じタイプのライン カードを使用する、Cisco Nexus 9500 スイッチの別のペアに移行するためのシナリオについて説明します。このような移行の一般的な例としては、より多くのインターフェイスが必要な場合に、Cisco Nexus 9504 スイッチから Cisco Nexus 9508 スイッチに移行するケースがあります。次の移行シナリオはサポートされていません。

- 異なるライン カード セットを使用する Cisco Nexus 9500 スイッチへの移行。例えば、N9K-X94xx ラインカードを搭載した Cisco Nexus 9500 スイッチから、N9K-X97xx ラインカードを搭載した Cisco Nexus 9500 スイッチへの移行です。
- 異なる世代の Cisco Nexus 9300 スイッチ間の移行。例えば、Cisco Nexus N9K-C9372PX から Cisco Nexus N9K-93180YC-EX スイッチへの移行です。
- vPC ドメインでの、異なる世代の Cisco Nexus 9000 スイッチの使用はサポートされていません

vPCフォークリフトアップグレードの考慮事項：

- vPCロール選択とスティッキビット

  デフォルトの場合、Cisco NX-OS ソフトウェアでは、最小の MAC アドレスを基にプライマリ デバイスが選択されます。ただし、ロールプライオリティが設定されている場合は、プライオリティが最も低いデバイスがプライマリ デバイスとして選択されます。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（現在動作可能なプライマリ）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（不要な中断を回避するため）。この動作は、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ないスティッキビットで実現されます。この方法では、稼働中のデバイスがリロードされたデバイスに勝ちます。したがって、vPCプライマリはvPCの動作セカンダリになります。スティッキ ビットは、vPCノードが vPC ピア リンクおよびピア キープアライブ ダウンで起動し、自動回復期間後にプライマリになるときにも設定されます。

- vPC の遅延復元

  遅延復元タイマーは、ピア隣接が既に確立されている場合、リロードの後で復元済みの vPC ピア デバイスで起動する vPC の遅延のために使用されます。

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

- vPC 自動リカバリ

  両方のvPCピアスイッチがダウンしたデータセンターの停電中に、1つのスイッチのみが復元された場合、自動回復機能により、そのスイッチがプライマリスイッチの役割を引き継ぎ、自動回復期間後にvPCリンクが起動します。デフォルトの自動回復期間は240秒です。

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

	移行ステップ	予想される動作	Node1 Configured role（Ex：role priority 100）	Node1 動作のロール	Node2 Configured role（Ex：role priority 200）	Node2 動作のロール
1	初期状態です。	トラフィックはvPCピア（Node1とNode2）の両方によって転送されます。 Node1はプライマリで、Node2はセカンダリです。	プライマリ	プライマリ スティッキービット：False	セカンダリ	セカンダリ スティッキービット：False
2	Node2 の交換 – Node2 のすべての vPC とアップリンクをシャットダウンします。 vPC ピア リンクおよび vPC ピア キープアライブは、管理上のアップ状態です。	プライマリvPCピアNode1でトラフィックが収束しました。	プライマリ	プライマリ スティッキービット：False	セカンダリ	セカンダリ スティッキービット：False
3	Node2を削除します。	Node1は引き続きトラフィックを転送します。	プライマリ	プライマリ スティッキービット：False	適用対象外	適用対象外

	移行ステップ	予想される動作	Node1 Configured role（Ex：role priority 100）	Node1 動作のロール	Node2 Configured role（Ex：role priority 200）	Node2 動作のロール
4	New_Node2を設定します。構成を管理アップ状態のvPC ピア リンクおよびピア キープアライブでスタートアップ構成にコピーします。 New_Node2の電源をオフにします。 すべての接続を確立します。 New_Node2の電源をオンにします。	New_Node2がセカンダリとして起動します。Node1は引き続きプライマリです。 トラフィックはNode01で引き続き転送されます。	プライマリ	プライマリ スティッキービット：False	セカンダリ	セカンダリ スティッキービット：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、ノード1とNew_Node2の両方によって転送されます。	プライマリ	プライマリ スティッキービット：False	セカンダリ	セカンダリ スティッキービット：False
6	Node1の交換： Node1でvPCとアップリンクをシャットダウンします。	トラフィックはNew_Node2に収束します。	プライマリ	プライマリ スティッキービット：False	セカンダリ	セカンダリ スティッキービット：False
7	Node1を削除します。	New_Node2がセカンダリになり、プライマリが動作し、スティッキービットがTrueに設定されます。	適用対象外	適用対象外	セカンダリ	プライマリ スティッキービット：True

	移行ステップ	予想される動作	Node1 Configured role（Ex：role priority 100）	Node1 動作のロール	Node2 Configured role（Ex：role priority 200）	Node2 動作のロール
8	New_Node1を設定します。スタートアップ実行をコピーします。 新しいNode1の電源をオフにします。すべての接続を確立します。New_Node1の電源をオンにします。	New_Node1がプライマリ、運用セカンダリとして起動します。	プライマリ	セカンダリ スティッキービット：False	セカンダリ	プライマリ スティッキービット：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、新しいノード1と新しいノード2の両方によって転送されます。	プライマリ	セカンダリ スティッキービット：False	セカンダリ	プライマリ スティッキービット：True

（注） 設定済みのセカンダリノードを動作可能なセカンダリとして設定し、設定済みのプライマリを動作可能なプライマリとして使用する場合は、移行の最後にNode2をリロードできます。これオプションであり、機能上の影響はありません。

注意事項と制約事項

vPC 構成時の注意事項と制約事項は次のとおりです。

- 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。
- 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。
- vPC環境内のVLANに不整合がある場合は、セカンダリ スイッチのvPCレッグ全体を停止するのではなく、影響を受ける（一致しない）VLAN のみが一時停止されます。

- 既存のポート チャネルで 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。
- CFS リージョン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。
- 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。

  次の場合、レイヤ 3 リンクとバックツーバックvPCでマルチキャストストリームが重複する可能性があります。

  - SVIは、バックツーバックvPCの一部である4つすべてのスイッチで設定されます。
  - vPCの一部である4つのスイッチを接続する追加のL3リンクがあります。
  - PIMは、すべてのSVIおよびスイッチ間のL3リンクでイネーブルです。

  ストリームの重複を防ぐには、vPCスイッチペアの1つからSVIまたはPIM設定を削除します。
- このソフトウェアは、vPC 上での BIDR PIM および SSM はサポートされていません。
- vPC 環境での DHCP スヌーピング、DAI、IPSG はサポートされていません。DHCP リレーはサポートされています。
- ピアスイッチは、両方の VPC ピアが同じプライオリティを共有し、すべての VLAN または MST インスタンスのルートである場合にのみ構成できます。少なくとも 1 つの VLAN または MST インスタンスがルートでない場合、ピアスイッチを構成できません。
- では、FEX-AA（デュアルホーム FEX）および FEX-ST（FEX ストレートスルー）トポロジ（FEX-AA および FEX-ST）がサポートされています。次の親スイッチの組み合わせはサポートされていません。
  - Cisco Nexus 9300-EX および 9300 スイッチ。
  - Cisco Nexus 9300 および 9500 スイッチ。
  - Cisco Nexus 9300-EX および 9500 スイッチ。
- および Cisco NX-OSリリース 9.3(5) 以降、クラウド スケール ベースの TOR スイッチは、ハードウェア/データ プレーンの vPC ピア宛ての TTL = 1 パケットを転送できます。機能のシームレスな動作のために、これらのリリースまたはそれ以降のリリースのいずれかを使用することを推奨します。
- STP プライオリティの vPC ペアを設定する場合は、両方の vPC ピアを STP ルートとして機能させるために、両方の vPC ピア スイッチに同じプライオリティ レベルを設定する必要があります。
- **show** コマンド（**internal** キーワード付き ）はサポートされていません。
- Cisco Nexus 9000 シリーズ スイッチは、vPC トポロジでの NAT をサポートしていません。

- Cisco NX-OS リリース 9.2(1) 以降の Cisco Nexus 9000 スイッチでは、**show vpc consistency-checker** コマンドは使用できません。
- Cisco NX-OS リリース 9.2(1) 以降、**delay restore interface-bridge-domain** および **peer-gateway exclude-bridge-domain** コマンドは、Cisco Nexus 9500-R プラットフォーム スイッチでは利用できません。
- 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。
- この項で説明している **vpc orphan-ports suspend** コマンドは、非 vPC VLAN のポートおよびレイヤ 3 ポートにも適用可能です。ただし、VPC VLAN のポートで使用することをお勧めします。
- サポートされている vPC ドメインを形成するには、次の点に注意してください。
  - Cisco Nexus 9300 シリーズ スイッチの場合、両方のスイッチがまったく同じモデルである必要があります。
  - 2 つの Cisco Nexus 9500 シリーズ スイッチ間で vPC ドメインを形成する場合、両方のスイッチは、サポートされる vPC ドメインを形成するために、シャーシの同じスロットに挿入された同じモデルのライン カード、ファブリック モジュール、スーパーバイザ モジュール、およびシステム コントローラで構成されている必要があります。
- vPC ドメインを通じて接続されているすべてのデバイスは、デュアルホームである必要があります。
- **lacp suspend-individual** および **lacp mode delay** コマンドを実行して、PXE で vPC 経由で Cisco Nexus 9000 スイッチに接続しているサーバーを起動する必要があります。

での VPC のサポート Cisco Nexus 9336C-SE1

Cisco NX-OS リリース 10.6(1)F以降、 Cisco Nexus 9336C-SE1 では VPC がサポートされます。

vPC ピア リンクに関する注意事項

- ピアキープアライブ リンクを設定し、システムが vPC ピア リンクを確立する前に、ピア間の隣接関係を形成する必要があります。
- 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確認する必要があります。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 ピアリンクでは、デフォルトで MTU が 9216 に設定されています。
- vPC がダウンし、トラフィックが vPC 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はのベスト プラクティス、 vPC 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 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 の詳細については、「*Cisco Nexus 9000* シリーズ *NX-OS* ユニキャスト ルーティング設定ガイド」を参照してください。

- ジャンボ フレームは、vPC ピア リンクではデフォルトで有効に設定されます。
- vPC ポート チャネルの LACP 設定は、vPC ピア リンク上の両方の Cisco Nexus スイッチで一貫している必要があります。
- 2 つの Cisco Nexus 9000 シリーズ スイッチで **vpc domain** 構成モードの下にある **peer-switch** 機能を設定すると、vPC ピアリンクで有効になっていない VLAN に対してもスパニングツリー ルートが変更されます。両方のスイッチは、ブリッジ アドレスとして 1 つの MAC アドレスを持つ 1 つのシステムとして機能します。これは、non-vPC mst-instance または VLAN でも true です。したがって、2 つのスイッチ間の非 vPC ピア リンクはバックアップ リンクとしてブロックされます。これは予期された動作です。
- 第 1 世代の Broadcom ベースの Nexus 9300 シリーズ スイッチおよび Nexus 9500 シリーズ ライン カードは、vPCコンバージェンスに割り当てられた TCAM 領域の vPC ピアリンクとして、入力インターフェイスの **set ip next-hop** によるポリシーベース ルーティング（PBR）ルート マップをサポートしていません。

  この制限は、This limitation does not apply to cloud scale basedEX/FX/FX2 ラインカードを搭載した Nexus 9000 シリーズ デバイスや、9700-EX/FX ラインカードを搭載した Nexus 9500 プラットフォーム スイッチなど Nexus 9000 シリーズ デバイスに基づきクラウド スケールには適用されません。

vPC STP ヒットレス ロールの注意事項

- vPC ロール変更はいずれかのピア デバイスで実行できます。
- 元のセカンダリ デバイスに高プライオリティ値がある場合、元のプライオリティ デバイスはロール スワッピングは実行できません。vPC デバイスのいずれかでロール プライオリティを変更すると、元のセカンダリ デバイスの値は元のプライマリ デバイスの値よりも低くなります。デバイスの既存のロールを確認するには、ローカルおよびピア スイッチで show vpc role コマンドを使用します。
- vPC ドメインで vPC ヒットレス ロール変更機能を設定する前に、既存の設定済みロール プライオリティをチェックし、peer-switch コマンドを有効にします。これにより、両方の vPC ピアが同じ STP プライオリティになり、ロールの変更を発行する前にピアが稼働可能になることが保証されます。peer-switch コマンドを有効にできない場合、コンバージェンスの問題が発生する可能性があります。**show spanning-tree summary | grep peer** コマンドを使用して、ピア vPC スイッチが動作しているかどうかを確認します。

HSRP における vPC ピアの注意事項

- 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、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。
- 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。
- VRRP/HSRP の BFD は、vPC 環境で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ホット スタンバイ ルータ プロトコル（Hot Standby Router Protocol、HSRP）/仮想ルータ冗長プロトコル（Virtual Router Redundancy Protocol、VRRP）グループを持つことは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、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 Cisco Nexus 9000 vPC ピアでサポートされていません。

vPC 経由のレイヤ 3 に関する注意事項

- vPC を介したレイヤ 3 は、レイヤ 3 ユニキャスト通信の Cisco Nexus 9000 シリーズ スイッチでのみサポートされます。

  vPC 上のレイヤ 3 は、レイヤ 3 マルチキャスト トラフィックではサポートされません。詳細については、「レイヤ *3* および *vPC* 設定のベスト プラクティス」セクションを参照してください。

- デフォルトでは、レイヤ 3 vPC は、ピア vPC ノード宛てのすべてのパケット (TTL=1) を転送します。OSPF/BGP は、この転送が原因でフラップする可能性があります。スイッチ ハードウェアを前進させるには、ing-sup TCAM をサイズ 768 に切り分ける必要があります。TCAM カービング後にスイッチをリロードしてください。次に例を示します。

```
show hardware access-list tcam region | gr ing-sup
     Ingress SUP [ing-sup] size = 768
```

  Cisco NX-OS リリース 9.3(4) にはこのデフォルトの動作がありますが、クラウド スケール ベースの TOR スイッチに対する vPC ピアへのパケットのハードウェア リダイレクトには TCAM 再分割オプションを使用できます。これには、ing-sup リージョンに少なくとも 768 スペースを割り当てる必要があり、リロードが必要であり、操作上のオーバーヘッドがあります。

- vPC ピアの IP を宛先としたレイヤ 3 ピアルータおよび TTL = 1 パケットのデフォルトの動作では、パケットを CPU にパントし、ソフトウェアを vPC ピアに転送します。これは、クラウド スケール ベースの EOR スイッチに適用されます。
- クラウド スケール ASIC ベースのスイッチでレイヤ 3 ピアルータを設定すると、ユニキャスト パケットで次の動作が発生することがあります。

- vPC ピア ノード宛ての TTL = 0 のユニキャスト パケットは、ピアに転送されます。
- TTL = 0 のユニキャスト パケットはピアによってドロップされず、代わりに SUP にパントされます。
- VPC ピア ノード宛ての TTL = 1 および TTL = 0 のユニキャスト パケットは、ソフトウェア転送およびハードウェア転送が可能です。そのため、ピア ノードで重複パケットが確認されます。

- Cisco NX-OS リリース 9.3(9) 以降、vPC ドメインの両方の vPC ピアでピア ゲートウェイおよびレイヤ 3 ピア ルータ コマンドが設定されていない場合、syslog が作成されます。

アップグレード中の vPC に関する注意事項

- vPC ピアは同じ Cisco NX-OS リリースを実行する必要があります。ソフトウェア アップグレード中は、最初にプライマリ vPC ピアをアップグレードする必要があります。
- 無停止アップグレードを実行する前に、vPC の両方のピアが同じモード（通常 ISSU モードまたは拡張 ISSU モード）であることを確認します。

（注） 拡張 ISSU モード（ブートモード lxc）が構成されたスイッチと非拡張 ISSU モードスイッチ間の vPC ピアリングはサポートされていません。

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デバイスがvPCを介してvPCドメインに接続されている場合、次のビューがあります。

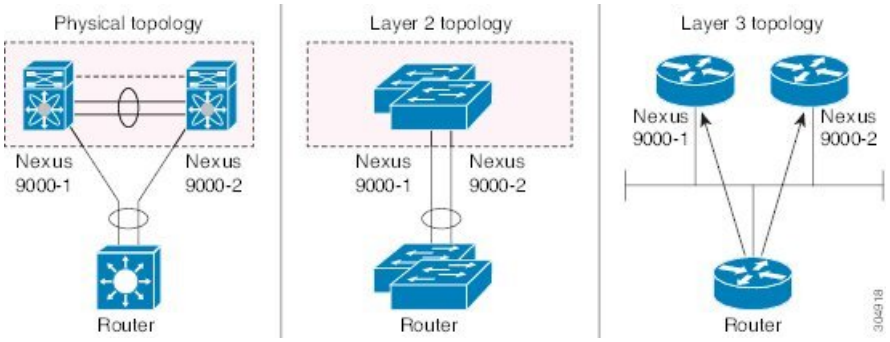
- レイヤ2では、レイヤ3デバイスはvPCピアデバイスによって提供される一意のレイヤ2スイッチを認識します。
- レイヤ 3 では、レイヤ 3 デバイスは 2 台の異なるレイヤ 3 デバイス（vPC ピア デバイスごとに 1 台）を認識します。

vPCはレイヤ2仮想化テクノロジーであるため、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固有の論理デバイスとして表示されます。

レイヤ3には仮想化テクノロジーがないため、各vPCピアデバイスは、ネットワークの他の部分では別個のレイヤ3デバイスと見なされます。

次の図は、vPCを使用した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 *17 : vPC*ピアデバイスのさまざまなビュー

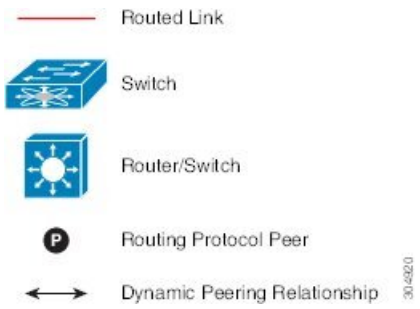


レイヤ 3 および vPC のサポートされるトポロジ

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。

レイヤ 3 と vPC のインタラクションには 2 つのアプローチがあります。1 つ目は、専用のレイヤ 3 リンクを使用してレイヤ 3 デバイスを各 vPC ピア デバイスに接続する方法です。2 つ目は、vPC 接続で伝送される専用 VLAN 上で、レイヤ 3 デバイスが各 vPC ピア デバイスで定義された SVI とピアリングできるようにすることです。次のセクションでは、次の図の凡例に記載されている要素を利用して、サポートされているすべてのトポロジについて説明します。

図 *18 :* 凡例

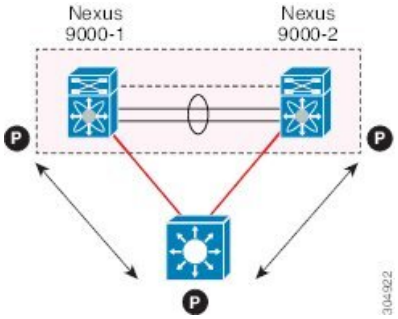


レイヤ 3 リンクを使用した外部ルータとのピアリング

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 ドメインの一部である Cisco Nexus 9000 スイッチ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と、レイヤ 3 ユニキャストおよびマルチキャスト通信をサポートできます。

図 *19 :* レイヤ *3* リンクを使用した外部ルータとのピアリング



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。

レイヤ 3 デバイスをレイヤ 3 リンクを使用している 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。

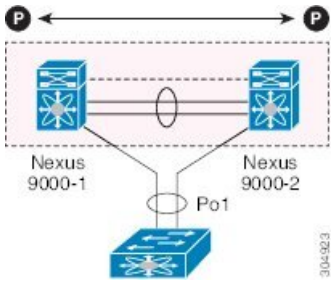
- レイヤ 3 デバイスを vPC ドメインに接続するには、独立したレイヤ 3 リンクを使用します。各リンクはポイントツーポイント レイヤ 3 接続を表し、小さな IP サブネット（/30 または /31）から取得された IP アドレスが割り当てられます。
- 複数の VRF にレイヤ 3 ピアリングが必要な場合は、それぞれが個別の VRF にマッピングされる複数のサブインターフェイスを定義することを推奨します。

バックアップ ルーティング パス用 vPC デバイス間のピアリング

この例では、レイヤ 3 バックアップ ルーテッド パスを持つ 2 つの vPC ピア デバイス間のピアリングを示します。vPC ピア デバイス 1 または vPC ピア デバイス 2 のレイヤ 3 アップリンクに障害が発生した場合、2 つのピア デバイス間のパスを使用して、レイヤ 3 アップリンクがアップ状態の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 リンク上で専用インターフェイス VLAN（SVI など）を使用するか、2 つの vPC ピア デバイス間で専用のレイヤ 2 またはレイヤ 3 リンクを使用して実装できます。

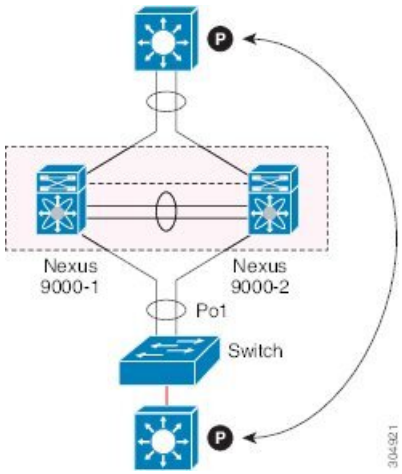
図 *20* : バックアップ ルーティング パス用 *vPC* デバイス間のピアリング



ルータ間の直接レイヤ 3 ピアリング

このシナリオでは、vPC ドメインの Nexus 9000 デバイスの部分が単にレイヤ 2 中継パスとして使用され、接続されたルータがレイヤ 3 ピアリングおよび通信を確立できるようにします。

図 *21* : ルータ間ピアリング



レイヤ 3 デバイスは、次の 2 つの方法で相互のピアとなることができます。また、ピアリングの方法は、このロールにどのようなデバイスが展開されるかによっても変わります。

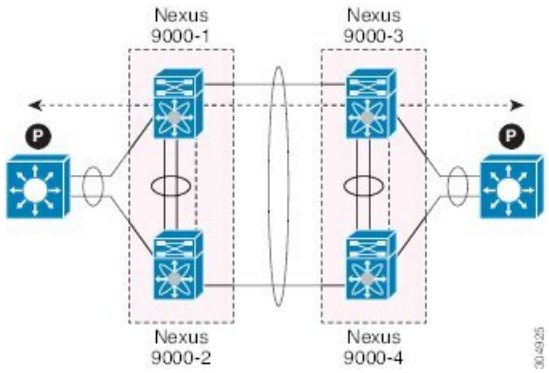
- 中間の Cisco Nexus 9000 vPC ピア スイッチを介してレイヤ 3 デバイス間で拡張される VLAN の VLAN ネットワーク インターフェイス（SVI）を定義します。
- 各レイヤ 3 デバイスでレイヤ 3 ポートチャネル インターフェイスを定義し、ポイントツーポイント レイヤ 3 ピアリングを確立します。

（注） 複数の VRF に対してレイヤ 3 ピアリングを確立する必要がある展開の場合、最初の方法では、VRF ごとに VLAN（および SVI）のレイヤ 3 デバイスで定義することが必要になります。2 番目の方法では、VRF ごとにレイヤ 3 ポートチャネル サブインターフェイスを作成できます。

トランジット 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。この場合も、同じvPCドメインの一部であるCisco Nexus 9000デバイスは、レイヤ2中継パスとしてのみ使用されます。ここでの違いは、Cisco Nexus 9000スイッチのペアが2つあることです。vPC接続を使用してレイヤ3デバイスに接続されている各スイッチは、それらの間のバックツーバックvPC接続も確立します。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:* トランジット 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



このトポロジは、直接リンク（ダーク ファイバまたはDWDM回線）で相互接続された個別のデータ センター間の接続を確立する場合によく使用されます。この場合、Cisco Nexus 9000スイッチの2つのペアはレイヤ2拡張サービスのみを提供し、レイヤ3デバイスがレイヤ3で相互にピアリングできるようにします。

パラレル相互接続ルーテッド ポート上の 外部ルーターとのピアリング

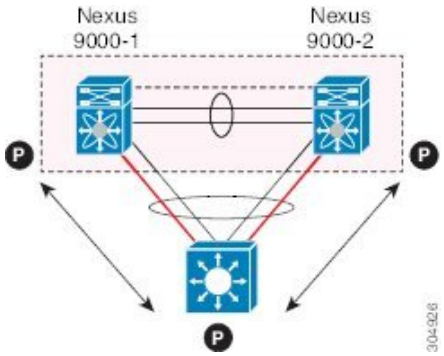
次の図に示すように、ルーテッド トラフィックとブリッジ トラフィックの両方が必要な場合は、ルーテッド トラフィックに個別のレイヤ3リンクを使用し、ブリッジ トラフィックに個別のレイヤ2ポート チャネルを使用します。

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特定のトラフィックを引き付けることです。レイヤ3リンクは、レイヤ3デバイスからvPCドメインにルーティングされたトラフィックを伝送するためにも使用されます。

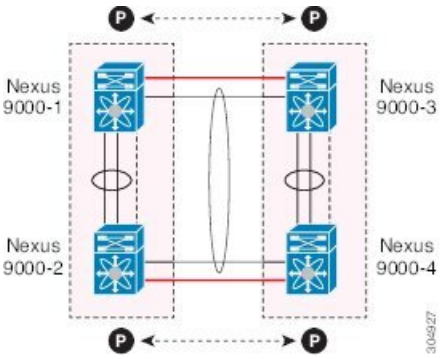
図 *23 :* パラレル相互接続ルーテッド ポート上の 外部ルーターとのピアリング



パラレル相互接続ルーテッド ポート上の vPC スイッチペア間のピアリング

前の項（中継スイッチとしてvPCデバイスを使用した2台のルータ間のピアリング）で示したものに代わる設計では、レイヤ2とレイヤ3の両方の拡張サービスを提供するために、各データセンターに導入された2ペアのCisco Nexus 9000スイッチを使用します。ルーティング プロトコル ピアリング隣接を2ペアのCisco Nexus 9000デバイス間で確立する必要がある場合、ベストプラクティスは、次の例に示すように2サイト間に専用のレイヤ3リンクを追加することです。

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



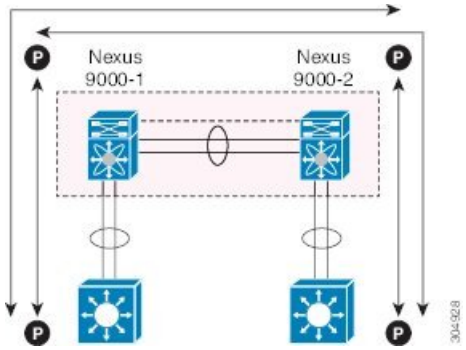
2 つのデータセンター間のバックツーバック vPC 接続は、ブリッジド トラフィックまたは VLAN 間トラフィックを伝送し、専用レイヤ 3 リンクは 2 サイト間でルーテッド トラフィックを伝送します。

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

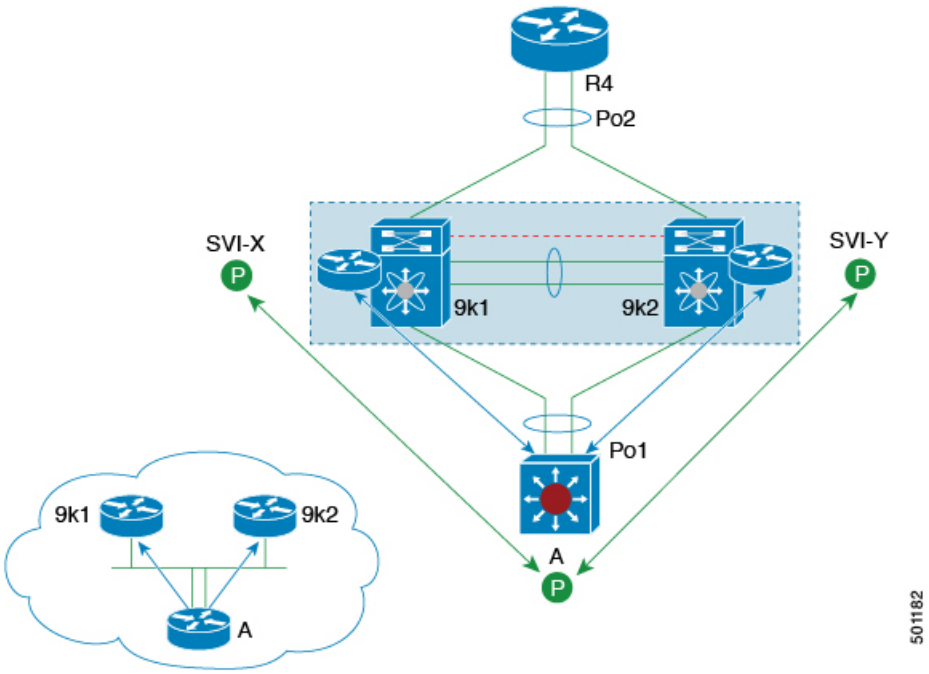


vPC 接続を介した直接ピアリング

Cisco NX-OS リリース 7.0(3)I5(1) 以降では、レイヤ 3 ルータと Cisco Nexus 9000 vPC スイッチのペア間にレイヤ 3 ピアリングを確立するための代替方法が導入されています。

（注） vPC 接続を介した直接ピアリングは、レイヤ 3 ユニキャスト通信でのみサポートされ、レイヤ 3 マルチキャスト トラフィックではサポートされません。レイヤ 3 マルチキャストが必要な場合は、専用のレイヤ 3 リンクでピアリングを確立する必要があります。

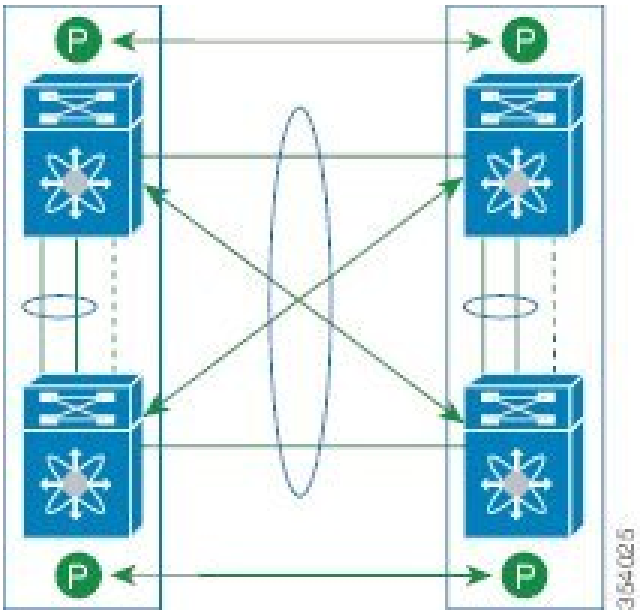
図 *26 :* サポート：ルータが両方の *vPC* ピアとピアリングする *vPC* 相互接続を介するピアリング。



このシナリオでは、同じ vPC ドメインの一部である外部ルータと Cisco Nexus 9000 スイッチ間のレイヤ 3 ピアリングは、vPC 接続で伝送される VLAN 上で直接確立されます。この場合の外部ルータは、各 vPC デバイスで定義された SVI インターフェイスとピアリングします。前の図 12 のシナリオでは、外部ルータは SVI またはレイヤ 3 ポートチャネルを使用して vPC デバイスとピアリングできます（複数の SVI またはポートチャネル サブインターフェイスをマルチ VRF 展開に使用できます）。

この展開モデルでは、vPC ドメインの一部として **layer3 peer-router** コマンドを設定する必要があります。vPC スイッチの 2 つの個別のペア間で確立された vPC バックツーバック接続でレイヤ 2 およびレイヤ 3 接続を確立するために、同じアプローチを採用できます。

図 *27* : サポート：各 *Nexus* デバイスが *2* つの *vPC* ピアとピアリングする *vPC* 相互接続を介したピアリング。



この展開モデルでは、4 つの Cisco Nexus 9000 スイッチすべてに同じ VLAN 内の SVI インターフェイスが設定され、これらの間でルーティング ピアリングと接続が確立されます。

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 *18* : デフォルト *vPC* パラメータ

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

vPC の設定

vPC の設定

（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場合は、事前に vPC 機能をイネーブルにしておく必要があります。

手順の概要

1. **configure terminal**
2. **feature vpc**
3. **exit**
4. **show feature**
5. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**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：	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。

	コマンドまたはアクション	目的
	`switch(config)# exit` `switch#`	
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。

例

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

手順

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的
ステップ 2	**no feature vpc** 例： `switch(config)# no feature vpc`	デバイスの vPC をディセーブルにします。

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

ステップ 4	**show feature** 例： `switch# show feature`	（任意）デバイス上でイネーブルになっている機能を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

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するこのドメイン 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*
3. **exit**
4. **show vpc brief**
5. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**vpc domain** *domain-id*
	例：
	`switch(config)# vpc domain 5`
	`switch(config-vpc-domain)#`
		デバイス上に vPC ドメインを作成し、設定目的で vpc-domain コンフィギュレーション モードを開始します。デフォルトはありません。指定できる範囲は 1 ～ 1000 です。

ステップ 3	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		vpc-domain 設定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。

例

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

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） 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。

（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。

始める前に

vPC 機能が有効なことを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain** *domain-id*
3. **peer-keepalive destination** *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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**vpc domain** *domain-id*
	例：
	`switch(config)# vpc domain 5`
	`switch(config-vpc-domain)#`
		デバイスで vPC ドメインを作成し、vpc-domain コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 3	**peer-keepalive destination** *ipaddress* [**hold-timeout** *secs* | **interval** *msecs* {**timeout** *secs*} | {**precedence** {*prec-value* | **network** | **internet** | **critical** | **flash-override** | **flash** | **immediate priority** | **routine**}} | **tos** {*tos-value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal**}} |**tos-byte** *tos-byte-value*} | **source** *ipaddress* | **vrf** {*name* | **management** **vpc-keepalive**}]
	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 および IPv6 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。
		（注）
		vPC ピアキープアライブ リンクのリモート エンドに IPv6 アドレスを設定するときに送信元 IP アドレスを指定しないと、次のエラー メッセージが表示されることがあります。
		`Cannot configure IPV6 peer-keepalive without source IPV6 address`
		管理ポートと VRF がデフォルトです。
		（注）
		独立した VRF を設定し、vPC ピアキープアライブ リンクのための VRF 内の各 vPC ピア デバイスからのレイヤ 3 ポートを使用することを推奨します。VRF の作成および設定の詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

ステップ 4	**exit**
	例：
	`switch(config)# 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。

例

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

指定した vPC ドメインの vPC ピア リンクとして設定するポート チャネルを各デバイス上で指定して、vPC ピア リンクを作成します。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。

始める前に

vPC 機能が有効なことを確認します。

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *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：	（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。

	コマンドまたはアクション	目的
	`switch(config-if)# switchport mode trunk`	
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 設定モードを終了します。

ステップ 7	**show vpc brief** 例： `switch# show vpc brief`	（任意）各 vPC に関する情報を表示します。vPC ピア リンクに関する情報も表示されます。
ステップ 8	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次の例は、vPC ピア リンクを設定する方法を示しています。

```
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)#
```

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。

始める前に

vPC 機能が有効なことを確認します。

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *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。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：	vpc-domain 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
	`switch(config)# exit` `switch#`	
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。

例

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 ピア リンクの構成の互換性チェック

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

手順

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的

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。

例

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

```
switch# 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。

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*
3. **graceful consistency-check**
4. **exit**
5. **show vpc brief**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル 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
	`switch# configure terminal` `switch(config)#`	

ステップ 2	**vpc domain** *domain-id*
	例：
	`switch(config-if)# vpc domain 5`
	`switch(config-vpc-domain)#`
		vPC ドメインがまだ存在していない場合はそれを作成し、vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**graceful consistency-check** 例： `switch(config-vpc-domain)# graceful consistency-check`	必須互換性パラメータで不一致が検出された場合に、セカンダリ ピア デバイスのリンクのみが一時停止するということを指定します。 この機能を無効にするには、このコマンドの **no** 形式を使用します。

ステップ 4	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		vpc-domain 設定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。

例

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。

始める前に

vPC 機能が有効なことを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain** *domain-id*

3. **peer-gateway**
4. **exit**
5. **show vpc brief**
6. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**vpc domain** *domain-id*
	例：
	`switch(config-if)# vpc domain 5`
	`switch(config-vpc-domain)#`
		vPC ドメインがまだ存在していない場合はそれを作成し、vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**peer-gateway** 例： `switch(config-vpc-domain)# peer-gateway` （注） 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 設定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。

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。

始める前に

vPC 機能が有効なことを確認します。

（注） VPC ピア間の非 VPC 専用トランク リンクを使用する場合は、STP が VLAN をブロックするのを防ぐために、非 VPC VLAN はピアによって異なるグローバル プライオリティが必要です。

手順の概要

1. **configure terminal**
2. **vpc domain** *domain-id*
3. **peer-switch**
4. **spanning-tree vlan** *vlan-range* **priority** *value*
5. **exit**
6. **show spanning-tree summary**
7. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**vpc domain** *domain-id*
	例：
	`switch(config)# vpc domain 5`
	`switch(config-vpc-domain)#`
		設定する vPC ドメインの番号を入力し、vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**peer-switch** 例：	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。

	コマンドまたはアクション	目的
	`switch(config-vpc-domain)# peer-switch`	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 設定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。

例

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)#
```

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。vPC 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、物理ポート、ポート チャネルでのみ設定できます。ただし、個々のポート チャネル メンバー ポートで同じ設定はできません。

vPC 孤立ポートの一時停止は、vPC メンバー ポートではサポートされません。

始める前に

vPC 機能が有効なことを確認します。

手順の概要

1. **configure terminal**
2. **show vpc orphan-ports**
3. **interface** *type slot/port*
4. **vpc orphan-port suspend**
5. **exit**
6. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**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-port 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：	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
	`switch(config-if)# exit` `switch#`	
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。

例

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)#
```

Cisco NX-OS リリース 9.2(1) 以降では、 **show vpc orphan-ports** コマンドの出力が以前のリリースの出力と若干異なります。次に、**show vpc orphan-ports** コマンドの出力例を示します。

```
switch# show vpc orphan-ports
--------::Going through port database. Please be patient.::--------
VLAN            Orphan Ports
-------         -------------------------
1               Eth1/18, Eth3/23

2               Eth3/23

3               Eth3/23

4               Eth3/23

5               Eth3/23
```

シングルモジュール vPC オブジェクト トラッキング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。

始める前に

vPC 機能が有効なことを確認します。

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*
3. **track** *track-object-id*
4. **exit**
5. **show vpc brief**
6. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**vpc domain** *domain-id*
	例：
	`switch(config)# vpc domain 5`
	`switch(config-vpc-domain)#`
		設定する vPC ドメインの番号を入力し、vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**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。

ステップ 4	**exit**
	例：
	`switch(config-vpc-domain)# exit`
	`switch#`
		vpc-domain 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	**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。

例

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。

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。

Cisco Nexus 9000 シリーズ デバイスは、**auto-recovery** コマンドを使用して、vPC プライマリ ピア が失敗し、ピア キープアライブと vPC ピア リンクを停止するとき、セカンダリ vPC ピアの vPC サービスを復元するように構成できます。ピア キープアライブと vPC ピア リンクの両方がダウンしているプライマリ スイッチに障害が発生すると、セカンダリ スイッチは vPC メンバーを一時停止します。ただし、キープアライブ ハートビートが 3 回失われると、セカンダリ スイッチはプライマリ スイッチの役割を再開し、vPCメンバーポートを起動します。
auto-recovery reload restore コマンドは、vPC プライマリ スイッチがリロードするシナリオで使用できます。この場合、セカンダリ スイッチは vPC プライマリの役割を再開し、IP VPC メンバー ポートを持ち込みます。

（注） Cisco Nexus 9000 スイッチでは、自動回復機能はデフォルトで有効になっていません。オブジェクト トラッキングがトリガーされると、vPC セカンダリ ピア デバイスはそのプライマリ デバイスへのロールを変更せず、vPC レッグを再初期化します。プライマリ ロールを引き継いで vPC レッグを再初期化できるように、vPC セカンダリ ピア デバイスで自動回復を手動で設定する必要があります。

始める前に

vPC 機能が有効なことを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain** *domain-id*
3. **auto-recovery** [**reload-delay** *time*]
4. **exit**
5. **show running-config vpc**
6. **show vpc consistency-parameters interface port-channel** *number*
7. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**vpc domain** *domain-id*
	例：
	`switch(config)# vpc domain 5`
	`switch(config-vpc-domain)#`
		設定する vPC ドメインの番号を入力し、vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**auto-recovery** [**reload-delay** *time*] 例： `switch(config-vpc-domain)# auto-recovery`	vPC がそのピアが機能しないことを前提として vPC を稼働させ始めるように設定し、vPC を復元するためのリロード後に待機する時間を指定します。デフォルト遅延値は 240 秒です。240 ~ 3600 秒の遅延を設定できます。 vPC をデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

	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 設定モードを終了します。

ステップ 5	**show running-config vpc** 例： `switch# show running-config vpc`	（任意）vPCに関する情報、特にリロードステータスを表示します。
ステップ 6	**show vpc consistency-parameters interface port-channel** *number* 例： `switch# show vpc consistency-parameters interface port-channel 1`	（任意）指定したインターフェイスのvPCの一貫性パラメータに関する情報を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。 （注） 自動リカバリ機能がイネーブルになっていることを確認するには、この手順を実行します。

例

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
switch(config-vpc-domain)# auto-recovery auto-recovery reload-delay 100

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
```

ヒットレス vPC ロール変更の設定

ヒットレス vPC ロールの変更を有効にするには、次の手順を実行します。

始める前に

- vPC 機能がイネーブルになっていることを確認します。
- vPC ピア リンクがアップしていることを確認します。
- デバイスのロール プライオリティを検証します。
- vPC ドメインで vPC ヒットレス ロール変更機能を設定する前に、既存の設定済みロール プライオリティをチェックし、 **peer-switch** コマンドを有効にします。これにより、両方の vPC ピアが同じ STP プライオリティになり、ロールの変更を発行する前にピアが稼働可能になることが保証されます。 **peer-switch** コマンドを有効にできない場合、コンバージェンスの問題が発生する可能性があります。

手順の概要

1. **vpc role preempt**
2. **show vpc role**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**vpc role preempt**
	例：
	`switch# vpc role preempt`
	`switch(config)#`
		ヒットレス vPC ロールの変更を有効にします。

ステップ 2	**show vpc role** 例： `switch(config)# show vpc role`	（任意）ヒットレスvPCロール変更機能を確認します。

例

次に、ヒットレス vPC ロールの変更を設定する例を示します。

```
switch# show vpc rolevPC Role status
----------------------------------------------------
vPC role                          : secondary
vPC system-mac                    : 00:23:04:ee:be:01
vPC system-priority               : 32667
vPC local system-mac              : 8c:60:4f:03:84:41
vPC local role-priority           : 32668
vPC peer system-mac               : 8c:60:4f:03:84:43
vPC peer role-priority            : 32667

! Configure vPC hitless role change on the device!

switch(config)# vpc role preempt
```

```
! The following is an output from the show vpc role command after the
vPC hitless feature is configured
switch(config)# show vpc role
vPC Role status
----------------------------------------------------
vPC role                        : primary
vPC system-mac                  : 00:00:00:00:00:00
vPC system-priority             : 32667
vPC local system-mac            : 8c:60:4f:03:84:41
vPC local role-priority         : 32666
vPC peer system-mac             : 8c:60:4f:03:84:43
vPC peer role-priority          : 32667

switch(config)#
```

vPC ロールの変更に関する使用ケース シナリオ

ヒットレス vPC ロール変更機能は、次のシナリオで使用できます。

- ロール変更要求：vPC ドメインのピアデバイスのロールを変更する場合。
- プライマリ スイッチのリロード：リロード後にロールが定義され、ロールが定義されると、ヒットレス vPC ロール変更機能を使用してロールを復元できます。たとえば、リロード後にプライマリデバイスが動作可能なセカンダリの役割を果たし、セカンダリ デバイスがプライマリの動作の役割を担う場合、**vpc role preempt** コマンドを使用して vPC ピアの役割を元の定義済みの役割に変更できます。

（注） vPC ロールを切り替える前に、必ず、既存のデバイス ロール プライオリティをチェックしてください。

- デュアル アクティブ リカバリ：デュアル アクティブ リカバリ シナリオでは、vPC プライマリ スイッチが引き続き（動作中）プライマリになりますが、vPC セカンダリ スイッチがターゲット プライマリ スイッチになり、vPC メンバー ポートがアップ状態になります。vPC ヒットレス機能を使用して、デバイス ロールを復元できます。デュアル アクティブ リカバリ後は、一方が稼働可能なプライマリで、もう一方が稼働可能なセカンダリの場合に、**vpc role preempt** コマンドを使用して、プライマリにするデバイス ロールとセカンダリにするデバイス ロールを復元できます。

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。

始める前に

vPC 機能が有効なことを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain** *domain-id*
3. **system-mac** *mac-address*
4. **exit**
5. **show vpc role**
6. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**vpc domain** *domain-id*
	例：
	`switch(config)# vpc domain 5`
	`switch(config-vpc-domain)#`
		設定する vPC ドメインの番号を入力します。システムは、vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**system-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 設定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。

例

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。

始める前に

vPC 機能が有効なことを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain** *domain-id*
3. **system-priority** *priority*
4. **exit**
5. **show vpc role**
6. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的

ステップ 2	**vpc domain** *domain-id*
	例：
	`switch(config)# vpc domain 5`
	`switch(config-vpc-domain)#`
		設定する vPC ドメインの番号を入力します。システムは、vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**system-priority** *priority*
	例：
	`switch(config-vpc-domain)# system-priority 4000`
	`switch(config-vpc-domain)#`
		指定した vPC ドメインに割り当てるシステム プライオリティを入力します。指定できる値の範囲は、1 ～ 65535 です。デフォルト値は 32667 です。

ステップ 4	**exit**
	例：
	`switch(config-vpc-domain)# exit`
	`switch#`
		vpc-domain 設定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。

例

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。

始める前に

vPC 機能が有効なことを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain** *domain-id*
3. **role priority** *priority*
4. **exit**
5. **show vpc role**
6. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**vpc domain** *domain-id*
	例：
	`switch(config)# vpc domain 5`
	`switch(config-vpc-domain)#`
		設定する vPC ドメインの番号を入力します。システムは、vpc-domain コンフィギュレーション モードを開始します。

ステップ 3	**role priority** *priority*
	例：
	`switch(config-vpc-domain)# role priority 4`
	`switch(config-vpc-domain)#`
		vPC システム プライオリティ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 設定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。

例

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)#
```

Cisco MAC アドレスを使用するための STP の有効化

この手順により、STP が Cisco MAC アドレス（00:26:0b:xx:xx:xx）を使用できるようになります。

始める前に

vPC 機能が有効なことを確認します。

手順

ステップ 1 **configure terminal**

例：

```
switch# configure terminal
```

グローバル構成モードを開始します。

ステップ 2 **vpc domain** *domain-id*

例：

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

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 構成モードを開始します。

ステップ 3 **[no] mac-address bpdu source version 2**

例：

```
switch(config-vpc-domain)# mac-address bpdu source version 2
```

STP がシスコの MAC アドレス（00:26:0b:xx:xx:xx）を、vPC ポートで生成される BDPU の発信元アドレスとして使用できるようになります。

ステップ 4 **exit**

例：

```
switch(config-vpc-domain)# exit
```

vpc-domain 構成モードを終了します。

ステップ 5 （任意） **copy running-config startup-config**

例：

```
switch(confg)# copy running-config startup-config
```

実行中の構成を、スタートアップ構成にコピーします。

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。

デュアル アクティブ検出ステータスの表示

vPC ピア リンクがダウンしたが、ピア キープアライブがアップのままの場合、vPC セカンダリ スイッチはその vPC メンバー ポートをすべてシャット ダウンします。このシナリオでは、動作中のセカンダリ デバイス上でデュアル アクティブ検出ステータスが 1 に設定され、その

メンバー ポートがシャットダウンされていることを示します。動作中のプライマリ デバイスでのデュアル アクティブ検出ステータスは 0 のままです。

次に、動作可能なセカンダリ デバイスのデュアル アクティブ検出ステータスを表示する例を示します。

```
switch# show vpc role
vPC Role status
----------------------------------------------------
vPC role                          :primary, operational secondary
Dual Active Detection Status      : 1
vPC system-mac                    : 00:23:04:ee:be:01
vPC system-priority               : 32667
vPC local system-mac              : 24:6c:84:34:c8:77
vPC local role-priority           : 200
vPC local config role-priority    : 200
vPC peer system-mac               : 24:6c:84:34:bf:df
vPC peer role-priority            : 300
vPC peer config role-priority     : 300
switch#
```

次に、動作可能なプライマリ デバイスのデュアル アクティブ検出ステータスを表示する例を示します。

```
switch# show vpc role
vPC Role status
----------------------------------------------------
vPC role                          :secondary, operational primary
Dual Active Detection Status      : 0
vPC system-mac                    : 00:23:04:ee:be:01
vPC system-priority               : 32667
vPC local system-mac              : 24:6c:84:34:bf:df
vPC local role-priority           : 300
vPC local config role-priority    : 300
vPC peer system-mac               : 24:6c:84:34:c8:77
vPC peer role-priority            : 200
vPC peer config role-priority     : 200
switch#
```

vPC のモニタリング

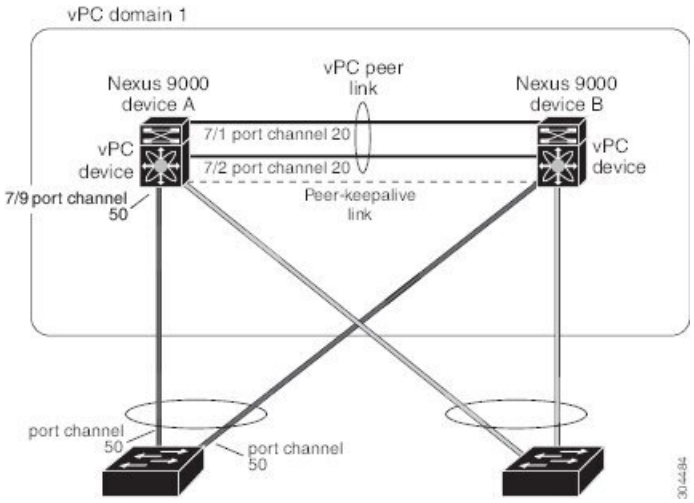
show vpc statistics コマンドを使用し、vPC統計情報を表示します。

（注） このコマンドは、現在作業している vPC ピア デバイスの vPC 統計情報しか表示しません。

vPC の設定例

次の例は、の図に示すように、デバイス A 上で vPC を設定する方法を示します。

図 *28 : vPC* の設定例



手順

ステップ 1 vPC および LACP をイネーブルにします。

例：

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

ステップ 2 （任意）vPC ピア リンクにするインターフェイスの 1 つを専用モードに構成します。

例：

```
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)# no shutdown
switch(config-if)# exit
switch(config)#
```

ステップ 3 （任意）vPC 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 モードに構成します。

例：

```
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)# no shutdown
switch(config-if)# exit
switch(config)#
```

ステップ 4 vPC 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 チャネルに構成します。

例：

```
switch(config)# interface ethernet 7/1-2
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1-50
switch(config-if)# switchport trunk native vlan 20
switch(config-if)# channel-group 20 mode active
switch(config-if)# exit
```

ステップ 5 VLAN を作成し、イネーブルにします。

例：

```
switch(config)# vlan 1-50
switch(config-vlan)# no shutdown
switch(config-vlan)# exit
```

ステップ 6 vPC ピアキープアライブ リンク用の独立した VEF を作成し、レイヤ 3 インターフェイスをその VRF に追加します。

例：

```
switch(config)# vrf context pkal
switch(config-vrf)# exit
switch(config)# interface ethernet 8/1
switch(config-if)# vrf member pkal
switch(config-if)# ip address 172.23.145.218/24
switch(config-if)# no shutdown
switch(config-if)# exit
```

ステップ 7 vPC ドメインを作成し、vPC ピアキープアライブ リンクを追加します。

例：

```
switch(config)# vpc domain 1
switch(config-vpc-domain)# peer-keepalive
destination 172.23.145.217 source 172.23.145.218 vrf pkal
switch(config-vpc-domain)# exit
```

ステップ 8 vPC vPC ピア リンクを構成します。

例：

```
switch(config)# interface port-channel 20
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1-50
switch(config-if)# vpc peer-link
switch(config-if)# exit
switch(config)#
```

ステップ 9 vPC のダウンストリーム デバイスへのポート チャネルのインターフェイスを設定します。

例：

```
switch(config)# interface ethernet 7/9
switch(config-if)# switchport mode trunk
switch(config-if)# allowed vlan 1-50
switch(config-if)# native vlan 20
switch(config-if)# channel-group 50 mode active
switch(config-if)# exit
```

```
switch(config)# interface port-channel 50
switch(config-if)# vpc 50
switch(config-if)# exit
switch(config)#
```

ステップ 10 設定を保存します。

例：

```
switch(config)# copy running-config startup-config
```

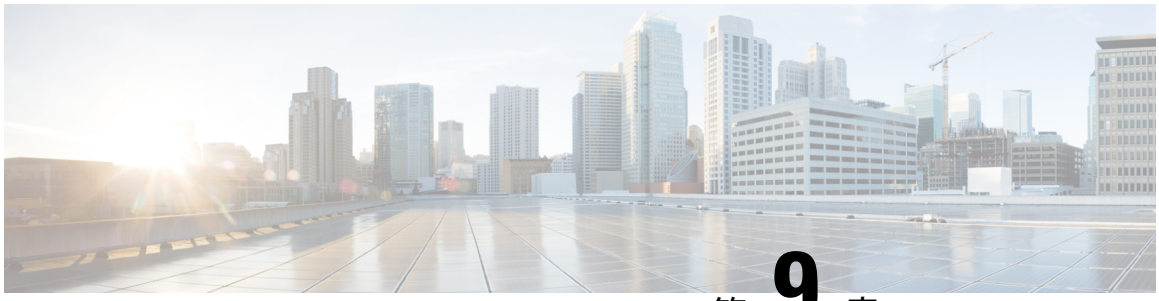
vPC の構成は、上記の手順に従って完了します。

例

（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
高可用性	高可用性
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

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。

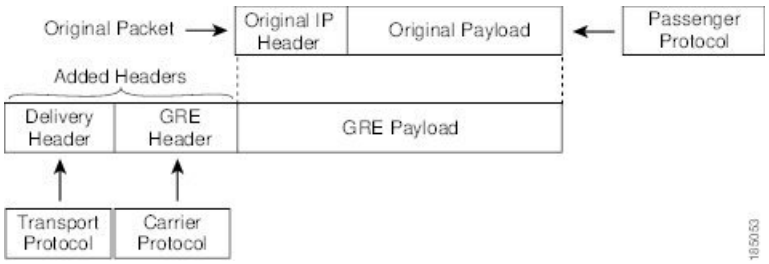
設定の前にトンネル機能をイネーブルにする必要があります。システムはこの機能をディセーブルにする前のチェックポイントを自動的に取得するため、このチェックポイントにロールバックできます。ロールバックおよびチェックポイントについては、『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』を参照してください。

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。

この次図は、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 *29 : 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

ポイントツーポイント IP-in-IP のカプセル化およびカプセル化解除は、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一種のトンネルです。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。

Cisco NX-OS リリース 10.4(1)F 以降、IPv4 トンネルは GRE でサポートされ、IPv6 トラフィックは GRE IPv4 内でカプセル化できます。

（注） Cisco NX-OS リリース 10.3(3)F 以降、PBR ポリシーに基づいて GRE または IP-in-IP トンネル宛先の選択がサポートされます。

（注） IP-in-IP トンネル カプセル化とカプセル化解除は、N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RX ライン カードを搭載した Cisco Nexus 9500 シリーズ スイッチではサポートされません。

（注） IP-in-IP トンネルのカプセル化とカプセル化解除は、Cisco Nexus 9300-EX、9300-FX、 9300-GX および Nexus 9500 プラットフォーム スイッチの vPC 設定で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

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。

パス MTU ディスカバリ

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。

高可用性

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。

- Cisco NX-OS リリース 9.3(3) 以降：
  - 合計 16 個の GRE/IPIP トンネルが、Cisco Nexus 9200、9300-EX/FX/FX2 スイッチ、および 9700-EX/FX ライン カードを搭載した 9500 スイッチでサポートされます。
  - 複数の、最大で 16 の IPIP Decap-any トンネルがサポートされています。VRF ごとに 1 つの decap-any トンネルです。これは、Cisco Nexus 9200 および 9300-EX/FX/FX2 プラットフォームでサポートされています。
  - IPIP/GRE カプセル化パケットが終端ノードで入力されるインターフェイスの VRF メンバーシップは、トンネルのパケットを正しく終端するために、トンネル転送 VRF と一致している必要があります。
  - パケットの外部ヘッダーがトンネルの送信元およびトンネルの宛先と一致する場合、デフォルト以外の VRF に着信する IPIP/GRE パケットは、デフォルトの VRF トンネルによって終端されることがあります。
- Cisco NX-OS リリース9.3(5) 以降では、次の機能が N9K-C9316D-GX、N9K-C93600CD-GX、および N9K-C9364C-GX スイッチでサポートされています。
  - 合計 16 の GRE/IPIP トンネル。
  - 複数の、最大で 16 の IPIP Decap-any トンネルがサポートされています。VRF ごとに 1 つの decap-any トンネルです。
- トンネルごとに、一意のトンネル宛先 IP を使用して同じ外部トランスポート VRF（**tunnel use-vrf**）を使用する複数の GRE トンネルまたは IP-in-IP トンネルを構成する必要があります。
  - N9K-X9736C-FX、N9K-X9736Q-FX、N9K-X9788TC-FX、N9K-C93180YC-FXN9K-C93108TC-FX、N9K-C9348GC-F、N9K-C9348GC-FXP、N9K-C9358GY-FXP、N9K-X9732C-FX、
  - N9K-C9336C-FX2-E、N9K-C93216TC-FX2、N9K-C93360YC-FX2、N9K-C93240YC-FX2-Z、N9K-C93240YC-FX2、N9K-C9336C-FX2
  - N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX、N9K-X9716D-GX、
  - N9K-X9736C-FX3、N9K-C93180YC-FX3S、N9K-C93180YC-FX3、N9K-C93108TC-FX3P、N9K-C9348GC-FX3、N9K-C9348GC-FX3PH、N9K-C93108TC-FX3、N9K-C92348GC-FX3
  - N9K-C9364D-GX2A、N9K-C9332D-GX2B、N9K-C9348D-GX2A、N9K-C9408

  - N9K-C9332D-H2R、N9K-C9364C-H1、N9K-C93400LD-H1

- Nexusプラットフォームでは、トンネルごとに、一意のトンネル送信元IPおよびトンネル宛先 IP を使用して同じ外部トランスポート VRF（**tunnel use-vrf**）を使用する複数の GRE トンネルまたは IP-in-IP トンネルを構成する必要があります。
- Nexus 9000 スイッチは、FC/FCOE トラフィックとの IP トンネルの共存をサポートしていません。FC/FCOE トラフィックを持つスイッチで IP トンネルを確立すると、そのトラフィックはドロップされます。
- Cisco NX-OS リリース 10.4(1)F 以降では、ループバック インターフェイスで tunnel source CLI コマンドを使用して、ループバック IP アドレスをトンネル送信元 IP アドレスとして構成できます。
- **internal** キーワードが付いているコ **show** マンド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 リリース9.3(3) 以降、サポートされる GRE および IP-in-IP の通常トンネルの最大数は 16 です。
- 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。
- Cisco NX-OS リリース 10.3(3)F 以降、PBR ポリシーに基づいて GRE または IP-in-IP トンネル宛先の選択がサポートされます。
- トンネル経由の BGP 隣接関係は、トンネル インターフェイスとトンネル入口が同じ VRF にあり（例：VRF-A）、トンネル出口が反対側からのルートリーク（例：VRF-B経由）で到達可能なシナリオでは、サポートされません。
- GRE トンネルは RACL をサポートしません。
- GREv6 トンネルまたはIP-in-IP トンネルを設定する場合、トンネル インターフェイスとトンネルの宛先に異なる VRF を使用することはできません。トンネルが正しく機能するには、両方が同じVRFを使用する必要があります。トンネルインターフェイスとトンネルの宛先に同じVRFを使用する必要があります。

GREv4 では、tunnel use-vrf とは異なるトンネル インターフェイス VRF の構成がサポートされています。

```
switch# interface tunnel X
vrf member INNER-VRF
tunnel use-vrf TRANSPORT-VRF
```

- GRE トンネルは、限定されたトラフィック（入力または出力）カウンタのみをサポートします。
- レイヤ 3 FEX インターフェイスは、トンネルの入口または出口として許可されません。
- GRE トンネルでは二重カプセル化は許可されません。
- BFD は GRE トンネルではサポートされていません。
- Cisco Nexus N9K-C9300-GX プラットフォームでは、GRE/IPinIP トンネル インターフェイスは、Dot1Q タグ付き L2 bcast または 1Q タグ付き L2/L3 mcast 中継トラフィックと共存できません。Cisco Nexus N9300-GX プラットフォームで**feature tunnel**を設定すると、次の警告が表示され、syslog メッセージにも警告が記録されます。デバイスに Dot1Q タグ付き L2 bcast または 1Q タグ付き L2/L3 mcast 中継トラフィックがある場合は、**feature tunnel** を設定しないでください。

```
N9300-GX(config)# feature tunnel
WARN:GRE/IPinIP cannot coexist with 1Q tagged L2 bcast or 1Q tagged L2/L3 mcast
transit packets on this
platform
N9300-GX(config)#
N9300-GX(config)# show logging logfile
2019 Dec 12 00:41:08 N9300-GX %TUNNEL-2-TRAFFIC_WARNING: GRE/IPinIP cannot coexist
with 1Q
tagged L2 bcast or 1Q tagged L2/L3 mcast transit packets on this platform
N9300-GX(config)#
```

- Cisco Nexus 9000 スイッチの**機能トンネル**機能は、VXLAN 機能である**機能 nv オーバーレイ**と共存できません。
- Cisco Nexus 9200、9300-EX、9300-FX、9300-FX2 シリーズ スイッチ、および 9700-EX/FX ライン カードを搭載した Cisco Nexus 9500 プラットフォーム スイッチでは、複数のトンネル インターフェイスを、同じ IP アドレスを送信元または宛先とする単一の VRFに含めることはできません。たとえば、デバイスは、トンネル 0 およびトンネル 1 のインターフェイスを、同じ IP アドレスまたはインターフェイスを送信元とするデフォルト VRF に含めることはできません。
- vPC の Cisco Nexus 9300-EX、9300-FX、9300-GX、および Nexus 9500 プラットフォーム スイッチは、それぞれのトンネルの GRE トンネル エンドポイントとして機能できます。ただし、トンネルの宛先を vPC 経由にすることはできません。
- Cisco NX-OS リリース 10.3(3)F 以降、トンネル インターフェイスの PBR ポリシーは、Cisco Nexus 9300-FX2/FX3/GX/GX2 プラットフォーム スイッチの **gre ip**、**ipip ip**、および **ipip decapsulate-any ip** モードでのみサポートされます。
- Cisco NX-OS リリース 10.4（1）F 以降、GRE トンネル は Cisco Nexus 9332D-H2R スイッチでサポートされています。

- Cisco NX-OS リリース 10.4（2）F 以降、GRE トンネル は Cisco Nexus 93400LD-H1 スイッチでサポートされます。
- FC または FCOE が構成されている場合、IP トンネルは Cisco Nexus 9300-FX または Cisco Nexus 9300-FX2 スイッチ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。

表 *19*：デフォルトの *IP* トンネル パラメータ

パラメータ	デフォルト
パス MTU ディスカバリ経過時間タイマー	10 分
パス MTU ディスカバリの最小 MTU	64
トンネル機能	無効化

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**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無効にするには、このコマンドの **no** 形式を使用します。
		（注）
		マルチキャストの重いテンプレートが適用されている場合、**feature tunnel** コマンドはマルチキャスト機能を中断する可能性があります。

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 GREv6 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。GREv4 では、トンネルの use-vrf とは異なるトンネルインターフェイス VRF の設定がサポートされています。

始める前に

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 | hostname}*
6. **tunnel use-vrf** *vrf-name*
7. **show interfaces tunnel** *number*
8. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface 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。 IP での GRE カプセル化の使用を指定するには、**gre** キーワードおよび **ip** キーワードを指定します。 **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、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、宛先として設定されたトンネルを使用できます。
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 | hostname}* 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。

例

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
```

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 カプセル化解除モードに設定できます。GRE モードはデフォルトのトンネル モードです。.

tunnel source direct および **tunnel mode ipv6ipv6 decapsulate-any** CLI コマンドは、Cisco Nexus 9000 シリーズ スイッチでサポートされています。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル 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
	`switch# configure terminal` `switch(config)#`	

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。 IP での GRE カプセル化の使用を指定するには、**gre** キーワードおよび **ip** キーワードを指定します。 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、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、宛先として設定されたトンネルを使用できます。
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 Maximum Transmission Unit（MTU; 最大伝送単位）を設定します。 有効な範囲は 64 ～ 9192 ユニットです。
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

例

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。

（注） Cisco NX-OSは、IPV4 over IPV4のGREプロトコルのみをサポートします。

始める前に

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**
4. **show interfaces tunnel** *number*
5. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface 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** 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。

Path MTU Discovery のイネーブル化

tunnel path-mtu discovery コマンドを使用し、トンネルのパスMTUディスカバリをイネーブルにします。

手順の概要

1. **tunnel path-mtu-discovery age-timer** *min*
2. **tunnel path-mtu-discovery min-mtu** *bytes*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**tunnel path-mtu-discovery age-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。指定できる範囲は 10 ～ 30 です。デフォルトは 10 です。
ステップ 2	**tunnel path-mtu-discovery min-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ー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。

始める前に

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface tunnel** *number*
	例：
	`switch(config)# interface tunnel 0`
	`switch(config-if)#`
		インターフェイス設定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：	（任意）この設定の変更を保存します。

	コマンドまたはアクション	目的
	`switch# copy running-config startup-config`	

例

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 カウントには、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
```

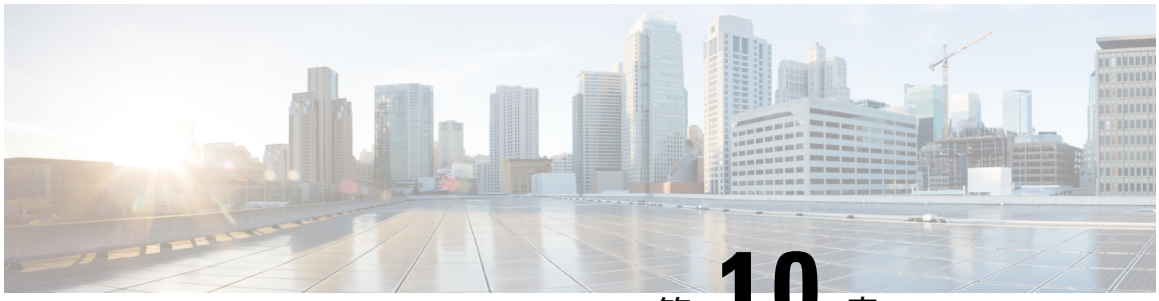
ルータ B：

```
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*』

関連資料



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。

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

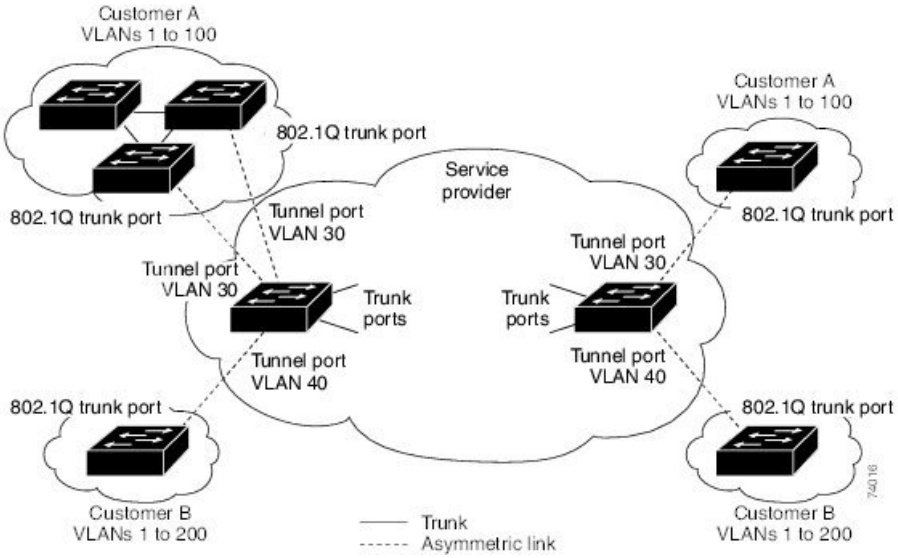
サービス プロバイダーのビジネス カスタマーには、多くの場合、サポートする VLAN ID および VLAN の数に固有の要件があります。同一サービスプロバイダ ネットワークのさまざまなカスタマーが必要とする VLAN 範囲は重複し、インフラストラクチャを通るカスタマーのトラフィックは混合してしまうことがあります。カスタマーごとに一意の VLAN ID 範囲を割り当てると、カスタマーの設定が制限され、802.1Q 仕様の VLAN に関する上限（4096 個）を容易に超えてしまいます。

（注） Q-in-Q は、ポート チャネルでサポートされています。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。サービスプロバイダーのインフラストラクチャ上でカスタマー VLAN ID が保持され、同じ VLAN 上に存在するように見えても、異なるカスタマーからのトラフィックが分離されます。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。

適切な VLAN ID で通常どおりにタグ付けされたカスタマーのトラフィックは、カスタマー デバイスの 802.1Q トランク ポートからサービス プロバイダー側のエッジ スイッチのトンネル ポートに発信されます。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。

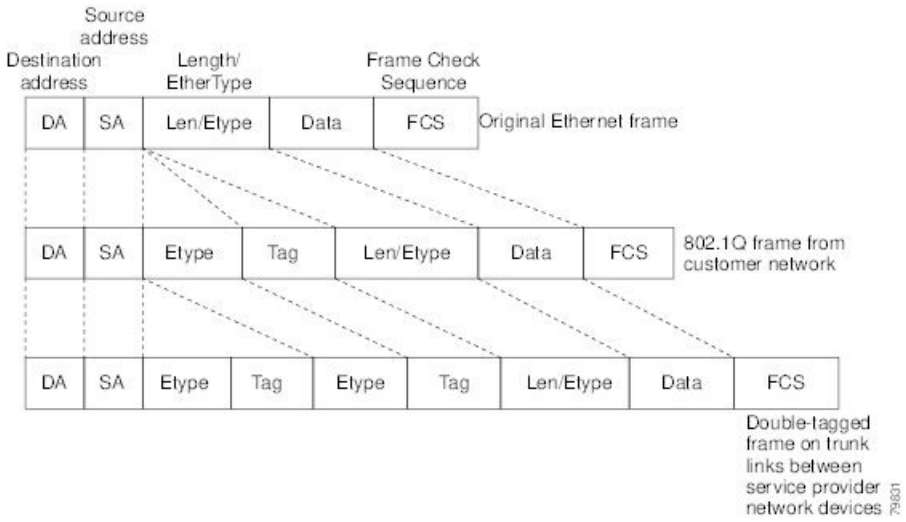
図 *30 : 802.1Q-in-Q* トンネル ポート



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 *31* : 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。

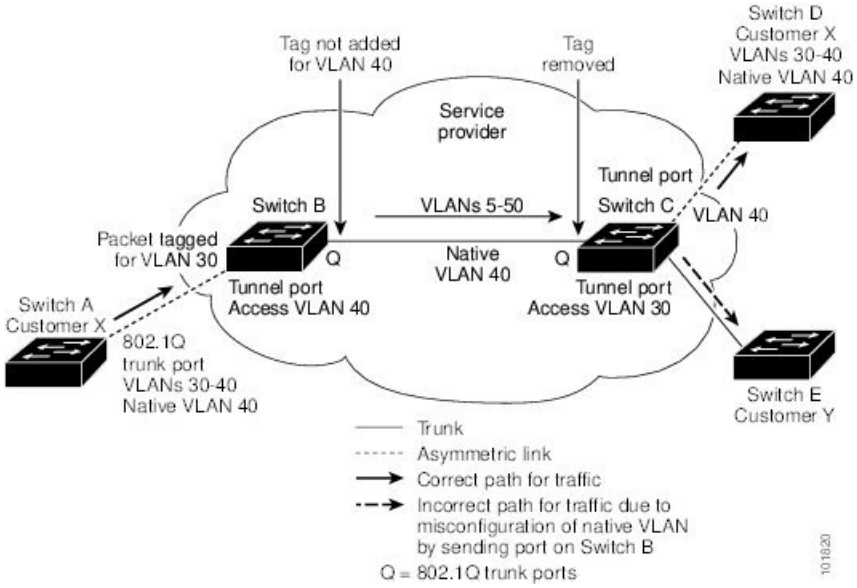
ネイティブ VLAN のリスク

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、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。

下の図の 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 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 *32 : 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。

トンネル ポートでマルチ タグ付き BPDU を許可するようにスイッチを設定できます。**l2protocol tunnel allow-double-tag** コマンドをイネーブルにすると、複数のタグが付けられたカスタマー BPDU がトンネル ポートに入ると、カスタマー トラフィックからの元の 802.1Q タグが保持され、外部 VLAN タグ（サービス プロバイダーによって割り当てられたカスタマー アクセス VLAN ID）が追加されます。カプセル化されたパケットに含まれています。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複数のタグが付けられます。BPDU がサービス プロバイダー ネットワークを離れると、外部タグが削除され、元の複数のタグが付けられた BPDU がカスタマー ネットワークに送信されます。

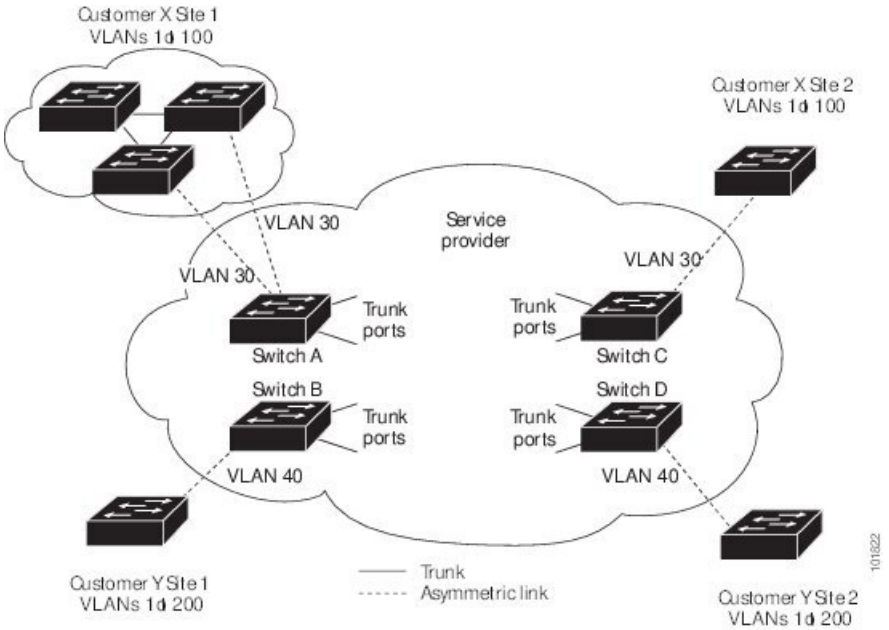
プロトコル トンネリングがイネーブルになると、サービスプロバイダーインフラストラクチャの受信側にあるエッジ スイッチが、レイヤ 2 プロトコルを特別の MAC アドレスでカプセル化し、サービス プロバイダー ネットワークの端まで送信します。ネットワークのコア スイッチでは、このパケットが処理されずに通常のパケットとして転送されます。CDP、STP、または VTP のブリッジ プロトコル データ ユニット（BPDU）は、サービスプロバイダー インフラストラクチャを通過し、サービスプロバイダー ネットワークの発信側にあるカスタマー スイッチまで配信されます。同一パケットは同じ VLAN のすべてのカスタマー 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、Software 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（415 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。

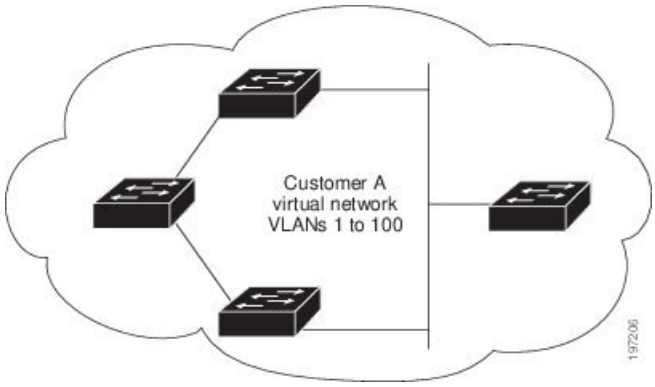
図 *33 :* レイヤ *2* プロトコル トンネリング



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 *34 : 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



複数プロバイダー VLAN を使用した選択的 Q-in-Q

複数プロバイダー VLAN を使用する選択的 Q-in-Q は、ポート上のユーザ固有の範囲のカスタマー VLAN を 1 つの特定のプロバイダー VLAN に関連付けることができるトンネリング機能であり、ポート上で複数のカスタマー VLAN をプロバイダー VLAN にマッピングできます。ポートに設定されたカスタマー VLAN のいずれかに一致する VLAN タグが付いたパケットは、

サービス プロバイダー VLAN のプロパティを使用して VLAN ファブリック全体でトンネリングされます。カプセル化パケットは、内部パケットのレイヤ 2 ヘッダーの一部としてカスタマー VLAN タグを伝送します。

VLAN のポート VLAN マッピングについて（着信 VLAN の変換）

サービス プロバイダーに、同じ VLAN カプセル化を使用して同じ物理スイッチに接続している複数の顧客があるものの、それらが同じ Layer 2 セグメント上に存在しない場合には、着信 VLAN を一意の VLAN/VNI に変換することが、セグメントを拡張する正しい方法です。

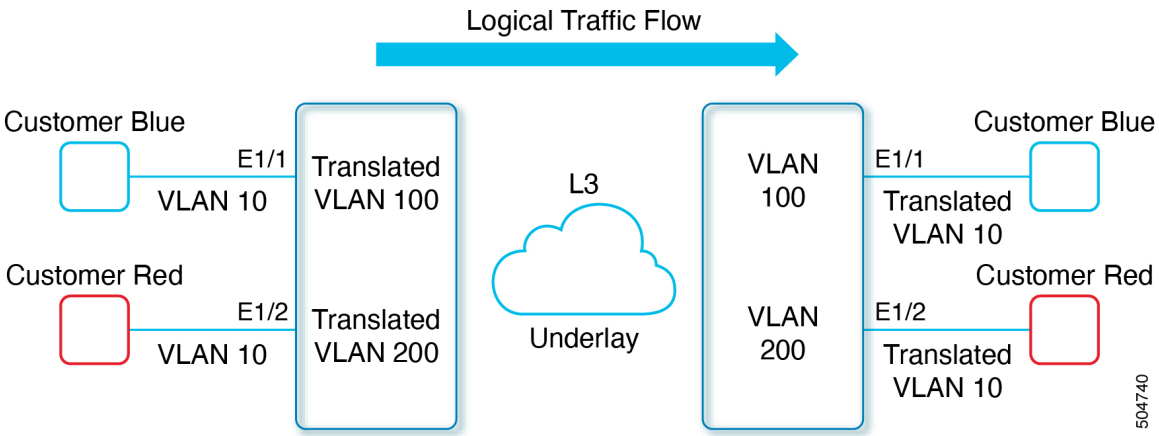
Cisco NX-OS リリース 10.3(3)F 以降、VXLAN VLAN 以外のポート VLAN マッピングは、Cisco Nexus 9300-EX/FX/FX2/FX3/GX/GX2、C9408 プラットフォーム スイッチ、および 9700-EX/FX/GX ライン カードを搭載した Cisco Nexus 9500 スイッチでサポートされます。

次の図では、Blue と Red がカプセル化として VLAN 10 を使用してリーフに接続しています。

この例では、Customer Blue の VLAN 10（インターフェイスE1/1）が VLAN 100 にマッピング/変換され、Customer Red の VLAN 10（インターフェイスE1/2）が VLAN 200 にマッピングされます。

もう一方のリーフでは、このマッピングが逆に適用されます。着信 VLAN 100 はインターフェイス E1/1 の VLAN 10 にマッピングされ、VLAN 200 はインターフェイス E1/2 の VLAN 10 にマッピングされます。

図 *35* : 論理的トラフィック フロー



入力（着信）VLAN とポートにあるローカル（変換先）VLAN との間での VLAN 変換を設定できます。VLAN 変換が有効にされたインターフェイスに到着するトラフィックにおいて、着信 VLAN は変換された VLAN にマッピングされます。

アンダーレイ上で、内部 dot1q が削除され、VXLAN ネットワーク以外に切り替えられます。VLAN 変換が設定された発信インターフェイスで、トラフィックは元の VLAN に変換されてから出力されます。トラフィック カウンタについては、入力 VLAN ではなく、変換先 VLAN にある VLAN カウンタを参照してください。

Q-in-Q トンネリングおよびレイヤ 2 プロトコル トンネリングの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、次の設定に関するガイドラインと制約事項があります。

- Q-in-Q は、サービス プロバイダーのエッジデバイスのカスタマー側インターフェイスで設定する必要があります。イーサネットフレームが Cisco Nexus 9000 シリーズ スイッチに入力されると、スイッチは 1 つの転送決定内で 2 つの 802.1Q ヘッダーを持つフレームをカプセル化できません。同様に、Q-in-Q カプセル化イーサネット フレームが 802.1Q ヘッダーのない Cisco Nexus 9000 シリーズ スイッチを出力する必要がある場合、スイッチは単一の転送決定内でイーサネット フレームから 2 つの 802.1Q ヘッダーをカプセル化解除できません。
- 複数の VLAN のマッピングがサポートされています。
- 複数の選択的 Q-in-Q タグはサポートされていません。つまり、Q-in-Q は単一のインターフェイスで複数の SP タグをサポートしません。
- 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。
- **system dot1q-tunnel transit** コマンドには次の制限があります。
  - このコマンドは、デバイスが Q-in-Q、選択的 Q-in-Q、または複数のプロバイダー VLAN 機能を備えた選択的 Q-in-Q で設定されている場合、Cisco Nexus 9300-EX/FX/FX2/FX3/GX スイッチおよび 9700-EX/FX/GX ライン カードを搭載した 9500 スイッチで必要です。
  - ToR またはモジュラ デバイスで **system dot1q-tunnel transit** コマンドを設定する必要があります。
  - vPC スイッチまたは非 vPC スイッチで **system dot1q-tunnel transit** コマンドを構成する必要があります。
  - これらのコマンドが構成されている場合、ポートのネイティブ VLAN であっても、トランク ポートを出るレイヤ 2 フレームは常にタグ付けされます。
  - このコマンドがスイッチで構成されている場合、MPLS、GRE、および IP-in-IP 機能は、Q-in-Q トンネリング機能との組み合わせでは実質的に機能しません。

- 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。
- 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、および 93120TX スイッチのアップリンク ポートと、N9K-M6PQ または N9K-M12PQ の汎用拡張モジュール（GEM）を搭載した Cisco Nexus 9396PX、9396TX、および 93128TX スイッチではサポートされていません。
- 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」）。
- Q-in-Q タギングはサポートされていません。
- Layer 2 プロトコル トンネリングは、N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RX ライン カードを搭載した Cisco Nexus 9500 シリーズ スイッチではサポートされません。
- N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RX ライン カードを搭載した Cisco Nexus 9500 シリーズ スイッチでは、Q-in-Q はポートまたはポートチャネルのレイヤ 2 アクセス VLAN エッジデバイスでのみサポートされます。
- FEX 設定は Q-in-Q ポートではサポートされません。
- コマンド **l2potocol tunnel stp** がトンネル インターフェイスで設定されている場合、サービス プロバイダーで設定する VLAN はカスタマーネットワークの VLAN とは異なる必要があります。
- LACP の L2PT トンネリングを使用するエッジ デバイスでフォールバック ISSU をトリガすると、エッジデバイスはソフトウェアでトンネリング（カプセル化および送信）を行います。ISSU 中のエッジデバイスのコントロール プレーンのダウンタイムが 90 秒を超える場合、エッジ デバイスのいずれかに接続されている LACP 対応ピアは、いずれかの LACP 対応ピアの LACP PDU タイムアウトが原因でフラップする可能性があります。90 秒の制限の期間は、次の理由によるものです。

- ISSU が原因でコントロール プレーンがダウンする直前に LACP PDU を送信するために、L2PT トンネリングを使用するエッジ デバイスで実行される特別なスクリプトはありません。
- エッジデバイスで確認された最後の LACP PDU は、ISSU がトリガされる前の最後の 90 秒間である可能性があります。これは、デフォルトの LACP PDU 送信レートが 30 秒で、タイムアウトが 90 秒であるためです。

Cisco N9336C-SE1 スイッチの注意事項と制約事項

Cisco NX-OS リリース 10.6(1)F以降では、 Cisco Nexus N9336C-SE1 スイッチで Q-in-Q を構成できます。

これらは、Cisco Nexus N9336C-SE1 スイッチの制限の一部です。

- **switchport trunk allowed vlan** *vlan_list* コマンドを使用して許可 VLAN の範囲を設定することはできません。

```
...!
interface Ethernet1/1  switchport mode trunk
switchport vlan mapping all dot1q-tunnel 30
switchport trunk allowed vlan 30-40
..!
```

この構成例では、トランクVLAN 30 がプロバイダーVLANです。VLAN 31 ～ 40 は、通常のトランクトラフィックをフィルタリングします。これらの VLAN はスパース モードで動作します。

- Q-in-Q で VLAN ACL は使用できません。
- マルチキャストはサポートされません。IGMP スヌーピングはサポートされていません。
- カスタム EtherType はサポートされません。
- QinQ のバリエーションはサポートされていません。
  - Q-in-VNI および選択的 Q-in-VNI
  - 選択的 Q-inQ はサポートされません。
- Cisco Nexus N9336C-SE1 スイッチが中継デバイスとして機能する場合、Q-in-Q トンネリングに **system dot1q-tunnel transit** コマンドを使用する必要はありません。

複数プロバイダー VLAN を使用した選択的 Q-in-Q の注意事項と制約事項

- 複数のプロバイダー VLAN を使用する選択的 Q-in-Q には、選択的 Q-in-Q に関する既存の制限事項とガイドラインがすべて適用されます。

- Cisco NX-OS リリース 9.3(5) 以降、複数プロバイダー VLAN を使用した選択的 Q-in-Q 機能は、Cisco Nexus N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX スイッチでサポートされます。
- 複数プロバイダー VLAN を使用した選択的 Q-in-Q 機能は、9300-EX、9300-FX、9300-FX2、9300-FX3、9332D-H2R および 93400LD-H1 スイッチでサポートされます。
- vPC ポート チャネルで複数のプロバイダー VLAN をイネーブルにする場合は、vPC ピア間で設定が一貫している必要があります。
- 通常のトランクではプロバイダー VLAN を許可しないことを推奨します。
- 選択的 QinQ トランク インターフェイスの許可された VLAN リストでは、ネイティブ VLAN とプロバイダー VLAN のみを許可します。
- 選択的 QinQ トランク VLAN は、同じ選択的 QinQ トランク インターフェイス上で通常の VLAN と混在させること はできません。
- ポートから VLAN へのマッピング（例：switchport vlan mapping 10 20）は、複数のプロバイダー VLAN で選択的 Q-in-Q 用に設定されたポートではサポートされません。
- プライベート VLAN は、複数のプロバイダー VLAN で選択的 Q-in-Q 用に設定されたポートではサポートされません。
- レイヤ 2 スイッチングのみがサポートされます。
- プロバイダー VLAN でのルーティングはサポートされていません。
- FEX は、複数のプロバイダー VLAN を使用する選択的 Q-in-Q ではサポートされません。
- DME 化されていない複数のプロバイダー VLAN コマンドを使用した選択的な Q-in-Q。
- VLAN1 が複数のプロバイダー タグを使用して選択的 Q-in-VNI を使用してネイティブ VLAN として設定されている場合、ネイティブ VLAN 上のトラフィックはドロップされます。ポートが選択的 Q-in-Q で設定されている場合は、VLAN1 をネイティブ VLAN として設定しないでください。 VLAN1 がカスタマー VLAN として設定されている場合、VLAN1 のトラフィックはドロップされます。

複合アクセス ポート機能セットに関する注意事項と制限事項

- Cisco NX-OS リリース 9.3(3) 以降では、IPv4 アンダーレイを搭載した Cisco Nexus C9348GC-FXPスイッチで複合アクセス ポート機能セットがサポートされています。
- 複合アクセス ポート機能セットは、次の機能で構成されます。
  - プライベート VLAN（セカンダリ隔離あり）
  - 選択的 Q-in-Q
  - ポートセキュリティ

- PVLANおよび選択的Q-in-Qに関するすべてのガイドラインと制限は、複合アクセス ポート機能セットにも適用されます。
- ポート モードの **private-vlan trunk secondary** は、複合アクセス ポート機能セットでサポートされます。
- vPC ポート チャネルで複合アクセス ポート機能セットを有効にする場合は、設定が vPC ピア全体で一貫していることを確認する必要があります。
- 複合アクセス ポート機能セットを実行する場合は、**system dot1q-tunnel transit** と入力することを推奨します。
- ポート VLAN マッピング（例：**switchport vlan mapping 10 20**）はサポートされていません。
- 選択的 Q-in-Q ではレイヤ 2 スイッチングのみがサポートされます。
- インターフェイスでdot1q-tunnelが構成されている場合、インターフェイスで **spanning-tree bpdufilter** を無効にすることはできません。
- 複合アクセス ポート機能のネイティブ VLAN では、ルーティングのみがサポートされます。

VLAN上のポートVLANマッピングに関する注意事項と制限事項

次に、ポート VLAN マッピングに関する注意事項と制限事項を示します。

- Cisco NX-OS リリース 10.3(3)F 以降、VLAN のポート VLAN マッピングは、Cisco Nexus 9300-EX/FX/FX2/FX3/GX/GX2、C9408 プラットフォーム スイッチ、および 9700-EX/FX/GX ライン カードを搭載した Cisco Nexus 9500 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4（1）F 以降、VLAN ののポート VLAN マッピングは Cisco Nexus 9332D-H2R スイッチでサポートされます。
- Cisco NX-OS リリース 10.4（2）F 以降、VLAN ののポート VLAN マッピングは Cisco Nexus 93400LD-H1 スイッチでサポートされます。
- 入力（着信）VLAN は、スイッチで VLAN として設定する必要はありません。変換された VLAN を構成する必要があります。
- すべてのレイヤ 2 送信元アドレスの学習およびレイヤ 2 MAC 宛先のルックアップは、変換先 VLAN で行われます。入力（着信）VLAN ではなく、変換先 VLAN にある VLAN カウンタを参照してください。
- ポート VLAN マッピング ルーティングは、変換された VLAN での SVI の設定をサポートします。
- 次に、ローカル VLAN 100 にマッピングされる着信 VLAN 10 の例を示します。

```
interface ethernet1/1
switchport vlan mapping 10 100
```

- 次に、PV 変換用のオーバーラップ VLAN の例を示します。最初のステートメントでは、VLAN-102 は変換された VLAN です。2 番目のステートメントでは、VLAN-102 は VLAN-103 に変換される VLAN です。

```
interface ethernet1/1
switchport vlan mapping 101 102
switchport vlan mapping 102 103
```

- force コマンドを使用して既存のポート チャネルにメンバーを追加する場合、「mapping enable」設定は一貫している必要があります。次に例を示します。

```
Int po 101
switchport vlan mapping enable
switchport vlan mapping 101 10
switchport trunk allowed vlan 10

int eth 1/8
/***No configuration***/
```

（注） switchport VLAN mapping enable コマンドは、ポート モードがトランクの場合にのみサポートされます。

- VLANマッピングは、ポートごとにVLANをスコーピングすることで、ポートへのVLANのローカリゼーションに役立ちます。一般的な使用例は、サービスプロバイダーのリーフスイッチに、重複する VLAN を持つ異なるカスタマーがあり、異なるポートに着信するサービス プロバイダー環境です。たとえば、顧客 A には Eth 1/1 に着信する VLAN 10 があり、顧客 B には Eth 2/2 に着信する VLAN 10があります。
- ポート VLAN マッピングは PVLAN と共存しません。
- **inherit port-profile** コマンドが PV インターフェイスで構成されている場合は、**no inherit port-profile** <*profile name*> コマンドを使用してデタッチしてから、**no switchport vlan mapping all** コマンドを実行します。
- **system dot1q-tunnel transit vlan provider_vlan_list** コマンドがスイッチ上でグローバルに構成されている場合は、プロバイダ VLAN をシステム上の他のトランクまたはアクセス ポートのネイティブまたはアクセス ポート VLAN として設定しないでください。システム上のネイティブ VLAN 以外のプロバイダ VLAN を選択する必要があります。

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

dot1qトンネルポートを作成するには、コマンドを使用します。**switchport mode**

（注） コマンドを使用して、802.1Qトンネルポートをエッジポートに設定する必要があります。**spanning-tree port type edge** ポートのプロバイダー 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します。

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。

Q-in-Q カプセル化またはカプセル化解除の要件を持たない SP クラウド内の純粋な中継ボックス上で、すべての VLAN タグのシームレスなパケット転送と保存を行うには、システム全体の **system dot1q-tunnel transit** コマンドを使用します。構成を削除するには、**no system dot1q-tunnel transit** コマンドを使用します。

system dot1q-tunnel transit または **system dot1q-tunnel transit vlan** *provider_vlan_list* コマンドのサポートされているプラットフォームと制限については、「Q-in-Q トンネリングおよびレイヤ 2 プロトコル トンネリングの注意事項と制約事項 （402 ページ）」セクションを参照してください。

始める前に

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. switch(config-if)# **spanning-tree port type edge**
6. switch(config-if)# **switchport access vlan** *vlan-id*
7. （任意） switch(config-if)# **no switchport mode dot1q-tunnel**
8. switch(config-if)# **exit**
9. （任意） switch(config)# **show dot1q-tunnel** [**interface** *if-range*]
10. （任意） switch(config)# **no shutdown**
11. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface ethernet** *slot/port*	設定する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)# **spanning-tree port type edge**	ポートをスパニングツリー エッジ ポートとして指定します。
ステップ 6	switch(config-if)# **switchport access vlan** *vlan-id*	プロバイダー アクセス VLAN 値を設定します。
ステップ 7	（任意） switch(config-if)# **no switchport mode dot1q-tunnel**	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 8	switch(config-if)# **exit**	コンフィグレーション モードを終了します。
ステップ 9	（任意） switch(config)# **show dot1q-tunnel** [**interface** *if-range*]	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 10	（任意） switch(config)# **no shutdown**	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	（任意） switch(config)# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

例

次に、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)# spanning-tree port type edge
switch(config-if)# switchport access vlan vlan 10
switch(config-if)# exit
switch(config)# exit
switch# show dot1q-tunnel
```

複数プロバイダー VLAN で選択的 Q-in-Q を設定する

始める前に

プロバイダー VLAN を設定する必要があります。

spanning-tree bpdufilter enable コマンドを使用して、トランクポートでスパニングツリーを無効にする必要があります。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** *interface-id*
3. switch(config if)# **switchport**
4. switch(config-if)# **switchport mode trunk**
5. switch(config-if)# **spanning-tree bpdufilter enable**
6. switch(config-if)# **switchport trunk native vlan** *vlan-id*
7. switch(config-if)# **switchport vlan mapping** *vlan-id-range* **dot1q-tunnel** *outer vlan-id*
8. switch(config-if)# **switchport trunk allowed vlan** *vlan_list*
9. switch(config-if)# **exit**
10. switch(config-if)# **show interfaces** *interface-id* **vlan mapping**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *interface-id*	サービス プロバイダ ネットワークに接続される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。物理インターフェイスまたは EtherChannel ポート チャネルを入力できます。

	コマンドまたはアクション	目的
ステップ 3	switch(config if)# **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 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。
ステップ 5	switch(config-if)# **spanning-tree bpdufilter enable**	このインターフェイスでのスパニングツリーBPDUの送信と処理を無効にします。
ステップ 6	switch(config-if)# **switchport trunk native vlan** *vlan-id*	802.1Q トランクのネイティブ VLAN を設定します。有効な値は 1 ～ 4094 です。デフォルト値は VLAN 1 です。
ステップ 7	switch(config-if)# **switchport vlan mapping** *vlan-id-range* **dot1q-tunnel** *outer vlan-id*	マッピングする VLAN ID を入力します。 • vlan-id-range1：カスタマー ネットワークからスイッチに入るカスタマー VLAN ID（C-VLAN）の範囲。指定できる範囲は 1 ～ 4094 です。VLAN-ID のストリングを入力できます。 • outer vlan-id：サービス プロバイダー ネットワークの外部 VLAN ID（S-VLAN）を入力します。指定できる範囲は 1 ～ 4094 です。
ステップ 8	switch(config-if)# **switchport trunk allowed vlan** *vlan_list*	トランク インターフェイスの許可 VLAN を設定します。
ステップ 9	switch(config-if)# **exit**	コンフィギュレーション モードを終了します。
ステップ 10	switch(config-if)# **show interfaces** *interface-id* **vlan mapping**	マッピングの設定の確認

次の例では、複数のプロバイダー VLAN で選択的 Q-in-Q を設定する方法を示します。

例

```
switch# sh run int e1/1

interface Ethernet1/1
  switchport
  switchport mode trunk
  switchport trunk native vlan 2
  switchport vlan mapping 3-400 dot1q-tunnel 400
  switchport vlan mapping 401-800 dot1q-tunnel 401
  switchport vlan mapping 801-1200 dot1q-tunnel 10
  switchport vlan mapping 1201-1600 dot1q-tunnel 1400
  switchport vlan mapping 1601-2000 dot1q-tunnel 9
  switchport vlan mapping 2001-2400 dot1q-tunnel 3000
  switchport vlan mapping 2401-2800 dot1q-tunnel 2099
```

```
  switchport vlan mapping 2801-3200 dot1q-tunnel 2800
  switchport vlan mapping 3201-3600 dot1q-tunnel 3967
  switchport vlan mapping 3601-4000 dot1q-tunnel 600
  spanning-tree bpdufilter enable
  switchport trunk allowed vlan 2,9-10,400-401,600,1400,2099,2800,3000,3967

switch# show interface e1/1 vlan mapping
Interface Eth1/1:
Original VLAN                     Translated VLAN
---------------                   -----------------
3                                        400
4                                        400
5                                        400
6                                        400
7                                        400
8                                        400
9                                        400
10                                       400
11                                       400
12                                       400
13                                       400
14                                       400
15                                       400
16                                       400
17                                       400
18                                       400
19                                       400
20                                       400

switch# show consistency-checker selective-qinq interface e1/1
Fetching ingressVlanXlate entries from slice:0 HW
Fetching ingressVlanXlate entries from slice:1 HW
Performing port specific checks for intf Eth1/1
Port specific selective QinQ checks for interface   Eth1/1 : PASS

Switch#
```

Q-in-Q 用の EtherType の変更

スイッチは、802.1Q および Q-in-Q カプセル化に 0x8100 のデフォルトの EtherTypeを使用します。EtherType は、スイッチポート インターフェイスで 0x9100、0x9200、および 0x88a8 に設定できません。

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** | **lacp** | **lldp** |**vtp**]

6. （任意） switch(config-if)# **no l2protocol tunnel** [**cdp** | **stp** | **lacp** | **lldp** |**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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface ethernet** *slot/port*	設定する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** | **lacp** | **lldp** |**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、LACP、LLDP または VTP トンネリングを有効にできます。
ステップ 6	（任意） switch(config-if)# **no l2protocol tunnel** [**cdp** | **stp** | **lacp** | **lldp** |**vtp**]	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**	コンフィグレーション モードを終了します。
ステップ 8	（任意） switch(config)# **no shutdown**	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	（任意） switch(config)# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

例

次に、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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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	（任意） switch(config)# **no l2protocol tunnel cos**	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**	コンフィグレーション モードを終了します。
ステップ 5	（任意） switch# **no shutdown**	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

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

例

次に、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)# **no 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

手順

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

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **interface 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	（任意） switch(config-if)# **no l2protocol tunnel drop-threshold** [**cdp** | **stp** | **vtp**]	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	（任意） switch(config-if)# **no l2protocol tunnel shutdown-threshold** [**cdp** | **stp** | **vtp**]	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**	コンフィグレーション モードを終了します。
ステップ 10	（任意） switch(config)# **no shutdown**	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	（任意） switch(config)# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

複合アクセス ポート機能セットの設定

混合アクセス ポートを設定するには、次の手順を実行します。

手順の概要

1. **interface** *interface* [**port** | **port-channel** | **vPC**]
2. **switchport mode private-vlan trunk** *secondary*

3. **switchport private-vlan trunk native vlan** *vlan_id*
4. **switchport private-vlan trunk allowed vlan** *vlan list*
5. **switchport private-vlan association trunk** *primary_vlan_ID secondary_vlan_ID*
6. **switchport vlan mapping** [*vlan-id-range* | *all*] *dot1q-tunnel outer vlan-id*
7. **storm-control broadcast level** [*high level*] [*lower level*]
8. **storm-control multicast level** [*high level*] [*lower level*]
9. **storm-control action** [**shutdown** | **trap**]
10. **load-interval counter** {*1* | *2* | *3* }
11. **switchport port-security maximum** [**max-addr**]
12. **switchport port-security** *action* [**restrict** | **shutdown** | **protect**]
13. **switchport port-security**
14. **service-policy** {**input** | **type** {**qos input** | **queuing** {**input** | **output**}}} *policy-map-name*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**interface** *interface* [**port**	**port-channel**	**vPC**] 例： `switch# interface port-channel 202`	指定されたポート チャネルをインターフェイス コンフィギュレーション モードにします。範囲は 1 ～ 4096 です。
ステップ 2	**switchport mode private-vlan trunk** *secondary* 例： `switch(config)# switchport mode private-vlan trunk secondary`	プライベート VLAN のセカンダリ トランク ポートとしてポートを設定します。
ステップ 3	**switchport private-vlan trunk native vlan** *vlan_id* 例： `switch(config)# switchport private-vlan trunk native vlan 4002`	PVLAN トランク ポートに割り当てるネイティブ VLAN を設定します。
ステップ 4	**switchport private-vlan trunk allowed vlan** *vlan list* 例： `switch(config)# switchport private-vlan trunk allowed vlan 1002,4002`	PVLAN トランク ポートで許容される通常の VLAN のリストを設定します。
ステップ 5	**switchport private-vlan association trunk** *primary_vlan_ID secondary_vlan_ID* 例： `switch(config)# switchport private-vlan association trunk 4050 4049`	PVLAN トランク ポートでプライマリ VLAN およびセカンダリ VKAN 間の関連付けを設定します。

	コマンドまたはアクション	目的
ステップ 6	**switchport vlan mapping** [*vlan-id-range* | *all*] *dot1q-tunnel outer vlan-id* 例： `switch(config-if)# switchport vlan mapping all dot1q-tunnel 1002`	すべての 4K VLAN を含むカスタマー範囲 VLAN またはキーワード all を入力します。
ステップ 7	**storm-control broadcast level** [*high level*] [*lower level*] 例： `switch(config-if)# storm-control broadcast level 1.00`	ブロードキャスト ストーム制御を設定します。ブロードキャスト トラフィックの上限しきい値レベルを指定します。
ステップ 8	**storm-control multicast level** [*high level*] [*lower level*] 例： `switch(config-if)# storm-control multicast level 1.00`	インターフェイス上のマルチキャスト トラフィック ストーム制御をイネーブルにし、トラフィック ストーム制御レベルを設定し、そのトラフィック ストーム制御レベルを、インターフェイス上でイネーブルにされているすべてのトラフィック ストーム制御モードに適用します。
ステップ 9	**storm-control action** [**shutdown** | **trap**] 例： `switch(config-if)# storm-control action shutdown`	トラフィック ストームの発生時にトラップを生成するか、ポートをエラー無効にするようにトラフィック ストーム制御を設定します。
ステップ 10	**load-interval counter** {*1* | *2* | *3* } 例： `switch(config-if)# load-interval counter 1 5`	インターフェイスで統計情報をサンプリングする間隔を指定します。
ステップ 11	**switchport port-security maximum** [**max-addr**] 例： `switch(config-if)# switchport port-security maximum 3`	ポートでセキュアMACアドレスの最大数を設定します。
ステップ 12	**switchport port-security** *action* [**restrict** | **shutdown** | **protect**] 例： `switch(config-if)# switchport port-security violation restrict`	インターフェイスのセキュリティ違反モードを制限します。
ステップ 13	**switchport port-security** 例： `switch(config-if)# switchport port-security`	ポート セキュリティのコンフィギュレーション情報を表示します。
ステップ 14	**service-policy** {**input** | **type** {**qos input** | **queuing** {**input** | **output**}}} *policy-map-name* 例：	ポリシーマップをインターフェイスに付加します。

	コマンドまたはアクション	目的
	`switch(config-if)# service-policy type qos input ovh_qos`	

Q-in-Q ダブル タギングの設定

STP および CDP BPDU のマルチタギングをイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface** *interface*
3. **switchport**
4. **switchport mode dot1q-tunnel**
5. **l2protocol tunnel [cdp | stp]**
6. （任意） **no l2protocol tunnel [cdp | stp]**
7. **l2protocol tunnel allow-double-tag**
8. （任意） **no l2protocol tunnel allow-double-tag**
9. **exit**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コ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 7/1`	設定するインターフェイスを指定します。
ステップ 3	**switchport** 例： `switch(config-if)# switchport`	インターフェイスをレイヤ 2 スイッチング ポートとして設定します。
ステップ 4	**switchport mode dot1q-tunnel** 例： `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。

	コマンドまたはアクション	目的
ステップ 5	**l2protocol tunnel [cdp | stp]** 例： `switch(config-if)# l2protocol tunnel cdp`	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 または STP トンネリングをイネーブルにできます。
ステップ 6	（任意） **no l2protocol tunnel [cdp | stp]** 例： `switch(config-if)# no l2protocol tunnel stp`	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	**l2protocol tunnel allow-double-tag** 例： `switch(config-if)# l2protocol tunnel allow-double-tag`	インターフェイスで STP および CDP BPDU のマルチタギングをイネーブルにします。
ステップ 8	（任意） **no l2protocol tunnel allow-double-tag** 例： `switch(config-if)# no l2protocol tunnel allow-double-tag`	インターフェイスで STP および CDP BPDU のマルチタギングをディセーブルにします。
ステップ 9	**exit** 例： `switch(config-if)# exit`	コンフィグレーション モードを終了します。

例

次に、STP および CDP BPDU のマルチタギ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 cdp
switch(config-if)#  l2protocol tunnel stp
switch(config-if)#  l2protocol tunnel allow-double-tag
switch(config-if)# exit
switch(config)# exit
switch#
```

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ているサービス 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#
```

VLAN 上のポート VLAN マッピングの構成

始める前に

- VLAN 変換を実装する物理またはポート チャネルがレイヤ 2 トランク ポートとして設定されていることを確認します。
- 変換先 VLAN がスイッチで作成されており、レイヤ 2 トランク ポートのトランク許可 VLAN の vlan-list にも追加されていることを確認します。

（注） ベスト プラクティスとして、入力 VLAN ID をインターフェイスのスイッチポート許可 vlan-list に追加しないでください。

手順

ステップ 1 **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。

ステップ 2 **interface** *type/port*

例：

```
switch(config)# interface Ethernet1/1
```

設定するインターフェイスを指定します。

ステップ 3 **[no] switchport vlan mapping enable**

例：

```
switch(config-if)# [no] switchport vlan mapping enable
```

スイッチ ポートでの VLAN 変換をイネーブルにします。VLAN 変換はデフォルトでディセーブルです。

（注）
VLAN 変換を無効にするには、このコマンドの **no** 形式を使用します。

ステップ 4 **[no] switchport vlan mapping** *vlan-id translated-vlan-id*

例：

```
switch(config-if)# switchport vlan mapping 10 100
```

VLAN を他の VLAN に変換します。

- *vlan-id* で指定できる範囲は 1 ～ 4094 です。*Translation-vlan-id*では、予約されていない VLAN ID だけが許可されます。
- 入力（着信）VLAN とポートにあるローカル（変換先）VLAN との間での VLAN 変換を設定できます。VLAN 変換が有効にされたインターフェイスに到着するトラフィックにおいて、着信 VLAN は変換された VLAN にマッピングされます。

トラフィックのルーティングは、変換された VLAN の SVI のコンテキストで行われます。VLAN 変換が設定された発信インターフェイスで、トラフィックは元の VLAN に変換されてから出力されます。

（注）
このコマンドの **no** 形式を使用すると、VLAN ペア間のマッピングがクリアされます。

ステップ 5 [no] switchport vlan mapping all

例：

```
switch(config-if)# no switchport vlan mapping all
```

インターフェイスに設定されたすべての VLAN のマッピングを削除します。

ステップ 6 copy running-config startup-config

例：

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

実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

（注）
VLAN 変換の設定は、スイッチ ポートが動作トランク ポートになるまで有効になりません。

ステップ 7 show interface [*if-identifier*] **vlan mapping**

例：

```
switch# show interface ethernet1/1 vlan mapping
```

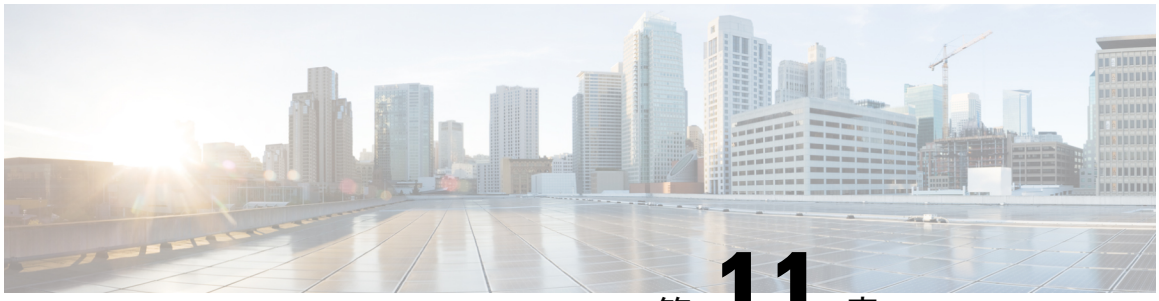
インターフェイスの範囲または特定のインターフェイスについて、VLAN マッピング情報を表示します。

例

次に、（入力）VLAN 10 と（ローカル）VLAN 100 間で VLAN 変換を設定する例を示します。show vlan counters コマンド出力は、カスタマー VLAN ではなく変換先 VLAN として統計情報カウンタを表示します。

```
switch#  configure terminal
switch(config)#  interface ethernet1/1
switch(config-if)#  switchport vlan mapping enable
switch(config-if)#  switchport vlan mapping 10 100
switch(config-if)#  switchport trunk allowed vlan 100
switch(config-if)#  show interface ethernet1/1 vlan mapping
Interface eth1/1:
```

```
Original VLAN           Translated VLAN
------------------      ---------------
10                           100

switch(config-if)#  show vlan counters
Vlan Id                              :100
Unicast Octets In                    :292442462
Unicast Packets In                   :1950525
Multicast Octets In                  :14619624
Multicast Packets In                 :91088
Broadcast Octets In                  :14619624
Broadcast Packets In                 :91088
Unicast Octets Out                   :304012656
Unicast Packets Out                  :2061976
L3 Unicast Octets In                 :0
L3 Unicast Packets In                :0
```



第 11 章

VLAN 上のポート VLAN マッピングの構成

この章で説明する内容は、次のとおりです。

VLAN のポート VLAN マッピングについて（着信 VLAN の変換）

サービス プロバイダーに、同じ VLAN カプセル化を使用して同じ物理スイッチに接続している複数の顧客があるものの、それらが同じ Layer 2 セグメント上に存在しない場合には、着信 VLAN を一意の VLAN/VNI に変換することが、セグメントを拡張する正しい方法です。

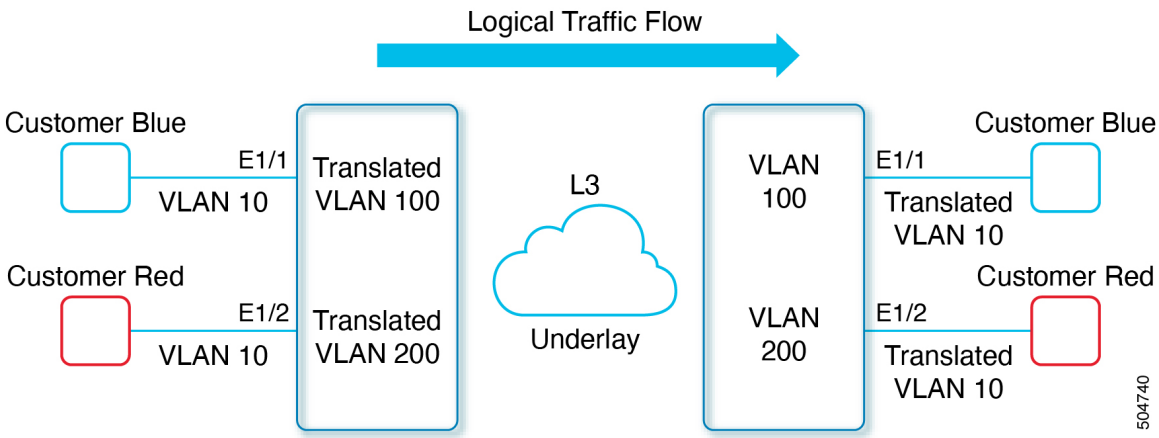
Cisco NX-OS リリース 10.3(3)F 以降、VXLAN VLAN 以外のポート VLAN マッピングは、Cisco Nexus 9300-EX/FX/FX2/FX3/GX/GX2、C9408 プラットフォーム スイッチ、および 9700-EX/FX/GX ライン カードを搭載した Cisco Nexus 9500 スイッチでサポートされます。

次の図では、Blue と Red がカプセル化として VLAN 10 を使用してリーフに接続しています。

この例では、Customer Blue の VLAN 10（インターフェイスE1/1）が VLAN 100 にマッピング/変換され、Customer Red の VLAN 10（インターフェイスE1/2）が VLAN 200 にマッピングされます。

もう一方のリーフでは、このマッピングが逆に適用されます。着信 VLAN 100 はインターフェイス E1/1 の VLAN 10 にマッピングされ、VLAN 200 はインターフェイス E1/2 の VLAN 10 にマッピングされます。

図 *36 :* 論理的トラフィック フロー



入力（着信）VLAN とポートにあるローカル（変換先）VLAN との間での VLAN 変換を設定できます。VLAN変換が有効にされたインターフェイスに到着するトラフィックにおいて、着信 VLAN は変換された VLAN にマッピングされます。

アンダーレイ上で、内部 dot1q が削除され、VXLAN ネットワーク以外に切り替えられます。VLAN 変換が設定された発信インターフェイスで、トラフィックは元の VLAN に変換されてから出力されます。トラフィック カウンタについては、入力 VLAN ではなく、変換先 VLAN にある VLAN カウンタを参照してください。

VLAN 上のポート VLAN マッピングに関する注意事項と制限事項

次に、ポート VLAN マッピングに関する注意事項と制限事項を示します。

- Cisco NX-OS リリース 10.3(3)F 以降、VLAN のポート VLAN マッピングは、Cisco Nexus 9300-EX/FX/FX2/FX3/GX/GX2、C9408 プラットフォーム スイッチ、および 9700-EX/FX/GX ライン カードを搭載した Cisco Nexus 9500 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4（1）F 以降、VLAN ののポート VLAN マッピングは Cisco Nexus 9332D-H2R スイッチでサポートされます。
- Cisco NX-OS リリース 10.4（2）F 以降、VLAN ののポート VLAN マッピングは Cisco Nexus 93400LD-H1 スイッチでサポートされます。
- 入力（着信）VLAN は、スイッチで VLAN として設定する必要はありません。変換された VLAN を構成する必要があります。
- すべてのレイヤ 2 送信元アドレスの学習およびレイヤ 2 MAC 宛先のルックアップは、変換先 VLAN で行われます。入力（着信）VLAN ではなく、変換先 VLAN にある VLAN カウンタを参照してください。

- ポート VLAN マッピング ルーティングは、変換された VLAN での SVI の設定をサポートします。
- 次に、ローカル VLAN 100 にマッピングされる着信 VLAN 10 の例を示します。

```
interface ethernet1/1
switchport vlan mapping 10 100
```

- 次に、PV 変換用のオーバーラップ VLAN の例を示します。最初のステートメントでは、VLAN-102 は変換された VLAN です。2 番目のステートメントでは、VLAN-102 は VLAN-103 に変換される VLAN です。

```
interface ethernet1/1
switchport vlan mapping 101 102
switchport vlan mapping 102 103
```

- force コマンドを使用して既存のポート チャネルにメンバーを追加する場合、「mapping enable」設定は一貫している必要があります。次に例を示します。

```
Int po 101
switchport vlan mapping enable
switchport vlan mapping 101 10
switchport trunk allowed vlan 10

int eth 1/8
/***No configuration***/
```

（注） switchport VLAN mapping enable コマンドは、ポート モードがトランクの場合にのみサポートされます。

- VLANマッピングは、ポートごとにVLANをスコーピングすることで、ポートへのVLANのローカリゼーションに役立ちます。一般的な使用例は、サービスプロバイダーのリーフスイッチに、重複する VLAN を持つ異なるカスタマーがあり、異なるポートに着信するサービス プロバイダー環境です。たとえば、顧客 A には Eth 1/1 に着信する VLAN 10 があり、顧客 B には Eth 2/2 に着信する VLAN 10があります。
- ポート VLAN マッピングは PVLAN と共存しません。
- **inherit port-profile** コマンドが PV インターフェイスで構成されている場合は、**no inherit port-profile** <*profile name*> コマンドを使用してデタッチしてから、**no switchport vlan mapping all** コマンドを実行します。
- **system dot1q-tunnel transit vlan provider_vlan_list** コマンドがスイッチ上でグローバルに構成されている場合は、プロバイダVLANをシステム上の他のトランクまたはアクセスポートのネイティブまたはアクセス ポート VLAN として設定しないでください。システム上のネイティブ VLAN 以外のプロバイダ VLAN を選択する必要があります。

VLAN 上のポート VLAN マッピングの構成

VLAN 上のポート VLAN マッピングの構成

始める前に

- VLAN 変換を実装する物理またはポート チャネルがレイヤ 2 トランク ポートとして設定されていることを確認します。
- 変換先 VLAN がスイッチで作成されており、レイヤ 2 トランク ポートのトランク許可 VLAN の vlan-list にも追加されていることを確認します。

（注） ベスト プラクティスとして、入力 VLAN ID をインターフェイスのスイッチポート許可 vlan-list に追加しないでください。

手順

ステップ 1 **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。

ステップ 2 **interface** *type/port*

例：

```
switch(config)# interface Ethernet1/1
```

設定するインターフェイスを指定します。

ステップ 3 **[no] switchport vlan mapping enable**

例：

```
switch(config-if)# [no] switchport vlan mapping enable
```

スイッチ ポートでの VLAN 変換をイネーブルにします。VLAN 変換はデフォルトでディセーブルです。

（注）
VLAN 変換を無効にするには、このコマンドの **no** 形式を使用します。

ステップ 4 **[no] switchport vlan mapping** *vlan-id translated-vlan-id*

例：

```
switch(config-if)# switchport vlan mapping 10 100
```

VLAN を他の VLAN に変換します。

VLAN 上のポート VLAN マッピングの構成

- *vlan-id* で指定できる範囲は 1 ～ 4094 です。*Translation-vlan-id*では、予約されていない VLAN ID だけが許可されます。
- 入力（着信）VLAN とポートにあるローカル（変換先）VLAN との間での VLAN 変換を設定できます。VLAN 変換が有効にされたインターフェイスに到着するトラフィックにおいて、着信 VLAN は変換された VLAN にマッピングされます。

トラフィックのルーティングは、変換された VLAN の SVI のコンテキストで行われます。VLAN 変換が設定された発信インターフェイスで、トラフィックは元の VLAN に変換されてから出力されます。

（注）
このコマンドの **no** 形式を使用すると、VLAN ペア間のマッピングがクリアされます。

ステップ 5 [no] switchport vlan mapping all

例：

```
switch(config-if)# no switchport vlan mapping all
```

インターフェイスに設定されたすべての VLAN のマッピングを削除します。

ステップ 6 copy running-config startup-config

例：

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

実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

（注）
VLAN 変換の設定は、スイッチ ポートが動作トランク ポートになるまで有効になりません。

ステップ 7 show interface [*if-identifier*] **vlan mapping**

例：

```
switch# show interface ethernet1/1 vlan mapping
```

インターフェイスの範囲または特定のインターフェイスについて、VLAN マッピング情報を表示します。

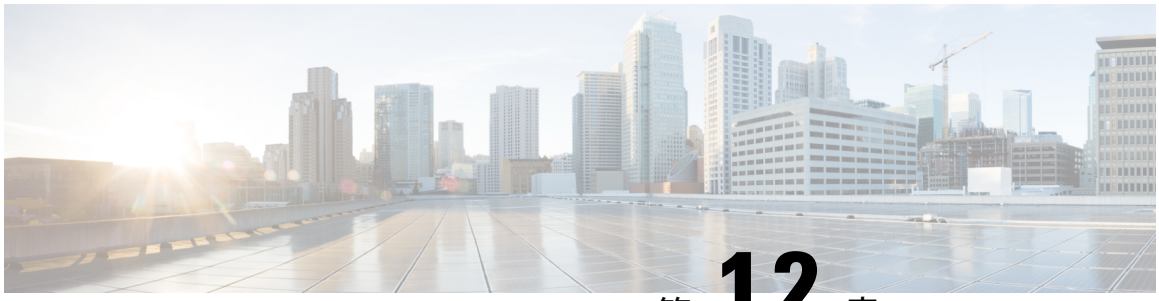
例

次に、（入力）VLAN 10 と（ローカル）VLAN 100 間で VLAN 変換を設定する例を示します。show vlan counters コマンド出力は、カスタマー VLAN ではなく変換先 VLAN として統計情報カウンタを表示します。

```
switch#  configure terminal
switch(config)#  interface ethernet1/1
switch(config-if)#  switchport vlan mapping enable
switch(config-if)#  switchport vlan mapping 10 100
switch(config-if)#  switchport trunk allowed vlan 100
switch(config-if)#  show interface ethernet1/1 vlan mapping
Interface eth1/1:
Original VLAN           Translated VLAN
------------------      ---------------
```

VLAN 上のポート VLAN マッピングの構成

```
10                          100

switch(config-if)#  show vlan counters
Vlan Id                               :100
Unicast Octets In                     :292442462
Unicast Packets In                    :1950525
Multicast Octets In                   :14619624
Multicast Packets In                  :91088
Broadcast Octets In                   :14619624
Broadcast Packets In                  :91088
Unicast Octets Out                    :304012656
Unicast Packets Out                   :2061976
L3 Unicast Octets In                  :0
L3 Unicast Packets In                 :0
```



第 12 章

スタティックおよびダイナミック NAT 変換の設定

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、内部ネットワークと外部ネットワークのそれぞれに接続するインターフェイスが少なくとも 1 つずつあります。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 アドレスをグローバルで一意の 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 はグローバルに一意な宛先アドレスをローカル アドレスに変換します。出口点が複数存在する場合、個々の NAT は同じ変換テーブルを持っている必要があります。

NAT は RFC 1631 に記述されています。

スタティック NAT に関する情報

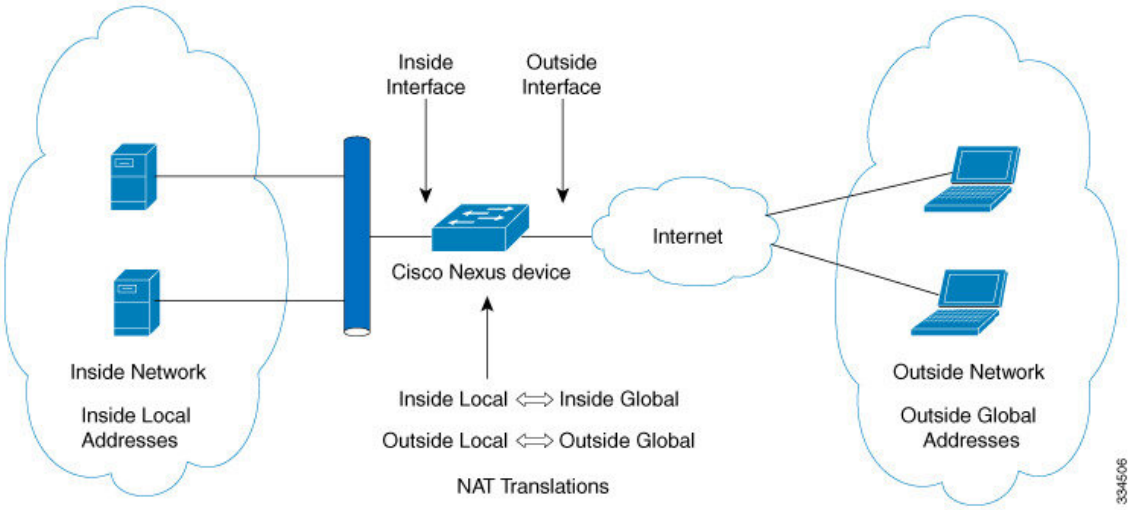
スタティック ネットワーク アドレス変換（NAT）を使用すると、ユーザは内部ローカル アドレスから外部グローバル アドレスへの 1 対 1 変換を設定することができます。これにより、内部から外部トラフィックおよび外部から内部トラフィックへの IP アドレスとポート番号の両方の変換が可能になります。Cisco Nexus デバイスはヒットレス NAT をサポートします。これは、既存の NAT トラフィック フローに影響を与えずに NAT 設定で NAT 変換を追加または削除できることを意味します。

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 *37*: 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る 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）では、実際のアドレスのグループは、宛先ネットワーク上でルーティング可能なマッピング アドレスのプールに変換されます。またダイナミック NAT では、未登録の IP アドレスと登録済み IP アドレス間で一対一のマッピング確立しますが、通信時にプール内で利用可能な登録済みアドレスによって、マッピングは変化します。

ダイナミック NAT を設定自動Aすると、使用している内部ネットワークと外部ネットワークまたはインターネット間に、ファイウォールが構築されます。ダイナミックNATは、スタブドメイン内で発信された接続のみを許可します。外部ネットワーク上のデバイスは、接続を開始していない限り、ネットワーク内のデバイスに接続できません。

ダイナミック NAT の場合、変換対象のトラフィックデバイスに受信するまでは、NAT 変換テーブルには変換エントリが存在しません。ダイナミック変換は、新しいエントリ用のスペースを確保するために使用されていない場合、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、Ternary Content Addressable Memory（TCAM）エントリが制限されるとクリアされます。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） この項で説明している **ip nat translation sampling-timeout** コマンドはサポートされていません。統計情報はインストール済みの NAT ポリシーに 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かまたはアクティブでないかを決定するために使用されます。

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。PAT（暗号化ともいう）、オーバーロードは未登録の複数の IP アドレスを、さまざまなポートを使うことによって、登録済みの単一の IP アドレスにマッピングするダイナミック NAT の 1 形態です。NAT設定には、同じまたは異なるACLを持つ複数のダイナミックNAT変換を含めることができます。ただし、特定のACLに対して指定できるインターフェイスは1つだけです。

タイムアウト メカニズム

タイムアウト メカニズムは、特定の NAT 変換タイムアウト エントリがクリアまたは期限切れになる前に維持される時間を制御する、設定可能なタイマーです。タイマーを設定する前に、別の TCP- NAT TCAM リージョンを切り分ける必要があります。

（注） TCP- NAT TCAM リージョンは、標準規格の NAT TCAM リージョンから分離されています。

スイッチでは、次のNAT変換タイムアウトタイマーがサポートされています。

- **syn-timeout**：TCPデータのパケットタイムアウト値。SYNリクエストを送信後、SYN-ACK応答を受信するまでの最大待ち時間です。

  タイムアウト値の範囲は、1 ～ 172800 秒です。TCP-NAT tcam リージョンが切り分けられる場合、デフォルト値は 60 秒です。[TCP- NAT TCAMリージョン（TCP - NAT TCAM region）] が切り分けられ ていない 場合、デフォルト値は never に設定されます。

（注） **syn-timeout** オプションは、Cisco Nexus 9200 および 9300-EX、-FX、-FX2、-FX3、-FXP、-GX プラットフォーム スイッチでサポートされています。

- **finrst-timeout**：RST または FIN パケットの受信によって接続が終了したときのフロー エントリのタイムアウト値。RSTパケットとFINパケットの両方の動作を設定するには、同じキーワードを使用します。

  タイムアウト値の範囲は、1 ～ 172800 秒です。TCP-NAT tcam リージョンが切り分けられる場合、デフォルト値は 60 秒です。[TCP- NAT TCAMリージョン（TCP - NAT TCAM region）] が切り分けられ ていない 場合、デフォルト値は never に設定されます。

  - 接続が確立された後にSYNパケット（SYN-> SYN-ACK-> FIN）が受信されると、finrstタイマーが開始されます。
  - 相手側からFIN-ACKを受信すると、変換エントリはすぐにクリアされます。それ以外の場合は、タイムアウト値の完了後にクリアされます。

    タイムアウト値の範囲は、1 ～ 172800 秒です。デフォルト値は 60 秒です。
  - 接続が確立された後にRSTパケットを受信した場合（SYN-->SYN-ACK-->RST）、変換エントリはすぐにクリアされます。

（注） ダイナミックプールベースの設定を使用し、FIN-ACKを受信した場合、変換エントリはクリアされません。

（注） **finrst-timeout** オプションは、Cisco Nexus 9200 および 9300-EX、-FX、-FX2、-FX3、-FXP、-GX プラットフォーム スイッチでサポートされています。

- **tcp-timeout**：TCP 変換のタイムアウト値。3 ウェイ ハンドシェイク（SYN、SYN-ACK、ACK）の後に確立した接続の最大待ち時間です。接続が確立された後にアクティブ フローが発生しない場合、変換は設定されたタイム アウト値に従って期限切れになります。

  タイムアウト値の範囲は、60 ～ 172800 秒です。デフォルト値は 3600 秒です。

- **udp-timeout**：すべての NAT UDP パケットのタイムアウト値。

タイムアウト値の範囲は、60 ～ 172800 秒です。デフォルト値は 3600 秒です。

- **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、60 ～ 172800 秒です。デフォルト値は 3600 秒です。

- **icmp-timeout** ：ICMP パケットのタイムアウト値。

  タイムアウト値の範囲は、60 ～ 172800 秒です。デフォルト値は 3600 秒です。

- **sampling-timeout** ：デバイスがダイナミック変換アクティビティをチェックするまでの時間。

  タイムアウト値の範囲は、900 ～ 172800 秒です。

タイマー値を設定するには、「FINRST および SYN タイマーの設定」を参照してください。

（注） 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：すべてのタイプのフロー（TCP および UDP 両方）に適用可能です。
- TCP TIME-OUT: TCP フローにのみ適用可能です。
- UDP TIME-OUT: UDP フローにのみ適用可能です。

udp-timeout and the **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。

ダイナミック NAT 変換を作成した後は、特に TCAM エントリの数が制限されている場合、新しい変換を作成できるように、使用していないものをクリアする必要があります

（注） 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 時間のデフォルトのタイムアウトが使用されます（60 秒後）。タイムアウトを設定した後、**clear ip nat translations 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、60 ～ 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 内部とは、変換を必要とす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 外部とは、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。通常、組織の管理下にはありません。外部ネットワーク内のホストを変換の対象にすることもできるため、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：ネットワークの内側部分に表示されるローカルな IP アドレスです。
- グローバル アドレス：ネットワークの外側部分に表示されるグローバルな IP アドレスです。
- 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、インターネット ネットワーク情報センター（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。必ずしも正規のアドレスでありません。内部でルート可能なアドレス空間から割り当てられたものです。
- 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たものです。

ダイナミック NAT のプール サポート

Cisco NX-OS は、ダイナミック NAT のプールをサポートします。ダイナミック NAT を使用すると、グローバル アドレスのプールを設定して、新しい変換ごとにプールからグローバル アドレスを動的に割り当てることができます。アドレスは、セッションが期限切れになるか、閉じられた後にプールに返されます。これにより、要件に基づいてアドレスをより効率的に使用できます。

PAT のサポートには、グローバル アドレス プールの使用が含まれます。これにより、IP アドレスの使用率がさらに最適化されます。PAT は、ポート番号を使用して、一度に 1 つの IP アドレスを使い果たします。ポートが該当グループで見つけられなかった場合や、複数の IP アドレスが設定されている場合、PAT は次の IP アドレスに移動して、ユーザー定義プールに基づいて、（ソース ポートを無視するか、それを保存しようと試みて）割り当てを取得します。

ダイナミック NAT および PAT では、各ホストは変換するたび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。

ダイナミック NAT が、ローカルで使用できない、またはローカルに設定されていない IP アドレスのプールを使用するように設定されている場合、アウトツーイン トラフィックは DEST MISS と見なされます。この動作により、**show system internal access-list dest-miss stats** コマンドの出力に DEST MISS カウンタの増分が表示されます。DEST MISS 統計情報は、Cisco NX-OS リリース 9.3(5) 以降でサポートされます。

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のパケットとして変換される場合、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 では、2 つの NAT 変換（1 つは内部、もう 1 つは変換）を変換グループの一部として設定できます。これらの変換は、NATデバイスを通過する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、個々の変換と結合された変換の両方が有効になります。

NAT 内部変換は、パケットが内部から外部に流れるときに送信元 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ときに、宛先 IP アドレスとポート番号を変更します。NAT 外部変換は、パケットが外部から内部に流れるときに送信元 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ときに宛先 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、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 1 つの変換ルールのみがパケットに適用されます。

同じグループに属するスタティック NAT 変換は、Twice NAT 設定の対象となります。スタティック設定にグループ ID が設定されていない場合、Twice NAT 設定は機能しません。グループ ID で識別される単一のグループに属するすべての内部および外部 NAT 変換は、ペアになって Twice NAT 変換を形成します。

ダイナミック Twice NAT 変換は、事前定義された **ip nat pool** または **インターフェイス過負荷** 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 の設定によって行われ、トラフィックはダイナミック NAT 変換ルールの方向から発信される必要があります。そのため、送信元変換はダイナミック NAT ルールを使用して行われます。

ダイナミック Twice NAT では、2 つの NAT 変換（内部と外部）を変換グループの一部として設定できます。1つの変換はダイナミックで、他の変換はスタティックである必要があります。これらの2つの変換が変換のグループの一部である場合、内部から外部または外部から内部のいずれかで NAT デバイスを通過するときに、両方の変換を 1 つのパケットに適用できます。

VRF 対応 NAT

VRF対応NAT機能により、スイッチはVRF（仮想ルーティングおよび転送インスタンス）のアドレス空間を認識し、パケットを変換できます。これにより、NAT機能は2つのVRF間で使用される重複アドレス空間のトラフィックを変換できます。

VRF対応NATに関する注意事項：

- VRF over NATは 9300-FX3 プラットフォーム スイッチでサポートされます。

- VRF対応のNAT機能は、N9K-9408PC-CFP2、N9K-X9564PX、N9K-C9272Q、N9K-C9272Q、N9K-X9464TX、N9K-X9464TX2、N9K-X9564TX、N9K-X9464PX、N9K-X9536PQ、N9K-X6963でサポートされています。 N9K-X9432PQ、N9K-C9332PQ、N9K-C9372PX、N9K-C9372PX-E、N9K-C9372TX、N9K-C9372TX-E、N9K-C93120TX
- Cisco NX-OS リリース 10.4(2)F 以降、VRF over NAT は、N9K-C93400LD-H1 でサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、VRF over NAT は、N9K-C9332D-H2R でサポートされます。
- VRF 対応 NAT 機能は Cisco Nexus 9300-EXプラットフォーム スイッチではサポートされていません。

（注） これは、Cisco Nexus 9300-EXFX プラットフォーム スイッチの NAT TCAM の制限です。NAT TCAM は VRF 対応ではありません。NAT は、Cisco Nexus 9300-EXプラットフォーム スイッチで重複する IP アドレスでは動作しません。

- Cisco NX-OS リリース 10.2(3)F 以降、VRF 対応 NAT は Cisco Nexus 9300-FX、FX2、GX と GX2 プラットフォーム スイッチでサポートされます。Cisco Nexus 9346C スイッチではサポートされません。
- 1つのnon-default-vrfから別のnon-default-vrfに流れるトラフィックは変換されません。（たとえば、vrfAからvrfB）。
- VRFからグローバルVRFに流れるトラフィックの場合、nat-outside設定はデフォルト以外のVRFインターフェイスではサポートされません。
- VRF対応NATは、スタティックおよびダイナミック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、 **match-in-vrf** オプション（ **ip nat** ）の コマンドは指定できません。
  - 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、 **match-in-vrf** オプション（ **ip nat** ）のコマンド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>} {pool <pool-name> [vrf
<vrf-name> [match-in-vrf]] [overload] | interface <globalAddrInterface> [vrf
<vrf-name> [match-in-vrf]] overload} [group <group-id> dynamic]


Switch(config)#ip nat outside source list <acl-name> pool <pool-name> [vrf
<vrf-name> [match-in-vrf]] [group <group-id> dynamic]}
```

- 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。

  したがって、レイヤ4およびその他の組み込みIPは変換されず、次のエラーが発生します。

  - FTP
  - ICMP障害
  - IPSec
  - HTTPS

- VRF対応NATは、インターフェイス上でNATまたはVACLをサポートします。（ただし、インターフェイスで両方の機能を同時にサポートすることはできません）。
- VRF対応NATは、NAT変換パケットではなく、元のパケットに適用される出力ACLをサポートします。
- VRF対応NATは、デフォルトのVRFのみをサポートします。
- VRF対応NATはMIBサポートを提供しません。
- VRF対応NATはDCNM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ません。
- サブネットが重複する VRF は、NAT なしで共通の宛先に移動できません。ただし、ダイナミック NAT ルール設定で VRF 間 NAT を使用すると、この機能を実現できます。スタティック NAT 設定は、重複アドレスではサポートされません。

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。

- Broadcom ベースの Cisco Nexus 9000 シリーズ スイッチでは、変換デバイス上の内部グローバルアドレスへのルートが外部インターフェイスを介して到達可能な場合、外部から内部へのネットワーク アドレス変換フローのパケットは、ネットワークでソフトウェアで転送、複製、およびループされます。この状況では、このフローの NAT 設定の最後に **add-route** CLI 引数を入力する必要があります。例えば、**`ip nat inside source static 192.168.1.1 172.16.1.1 add-route`** のようになります。
- キーワードが付いている **show** コマンドはサポートされていません。 **internal**
- 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 の変換をサポートします。
- 変換された IP が、外部インターフェイス サブネットの一部である場合、NAT の外部インターフェイスで **ip proxy-arp** コマンドを使用します。Cisco Nexus リリース 9.2(1) 以降で

は、NAT エイリアス機能がデフォルトで有効になっています。**ip proxy-arp** 構成を行う必要はありません。

- NAT と Flow は同じポートでは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で NAT をサポートします。
  - 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 とレイヤ 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。
  - 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TCAMエントリは割り当てられません。NAT機能にTCAMサイズを割り当てるには、他の機能のTCAMサイズを調整します。TCAM は **hardware access-list tcam region nat** *tcam-size* コマンドで割り当て可能です。
- HSRP および VRRP は NAT インターフェイスではサポートされません。
- 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。
- （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。
- NAT TCAM が切り分けられている場合、UDF ベースの機能が動作しないことがあります。
- ECMP NAT は Cisco Nexus 9000 スイッチではサポートされません。
- **[ip nat 内部（ip nat inside）]** または **[ip nat 外部（ip nat outside）]** などの NAT 構成は、ループバック インターフェイスではサポートされていません。

ダイナミック NAT の制約事項

ダイナミックネットワークアドレス変換（NAT）には、次の制約事項が適用されます。

- Broadcom ベースの Cisco Nexus 9000 シリーズ スイッチでは、変換デバイス上の内部グローバルアドレスへのルートが外部インターフェイスを介して到達可能な場合、外部から内部へのネットワーク アドレス変換フローのパケットは、ネットワークでソフトウェアで転送、複製、およびループされます。この状況では、このフローの NAT 設定の最後に **add-route** CLI 引数を入力する必要があります。例えば、**`ip nat inside source static 192.168.1.1 172.16.1.1 add-route`** のようになります。
- キーワードが付いている **show** コマンドはサポートされていません。 **internal**
- **interface overload option for inside policies** オプションは、外部および内部ポリシー両方の Cisco Nexus 9200、9300-EX、9300-FX、9300-FX2、9300-FX3、9300-FXP、および 9300-GX プラットフォーム スイッチではサポートされていません。
- VXLANルーティングはCisco Nexusデバイス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。
- アプリケーション層ゲートウェイ（ALG）変換はサポートされていません。ALG、またはアプリケーションレベル ゲートウェイは、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。
- デフォルト以外の仮想ルーティングおよび転送（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）はサポートされていません。
- Cisco Nexusデバイスでは、複数のグローバル仮想デバイスコンテキスト（VDC）はサポートされていません。
- ダイナミックNAT変換は、アクティブデバイス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はサポートされていません。ただし、NATとHot Standby Router Protocol（HSRP）は共存できます。
- のタイムアウト値は、設定されたタイムアウト+ 119秒までかかります。
- 通常、ICMP NATフローは、設定されたサンプリングタイムアウトおよび変換タイムアウトの満了後にタイムアウトします。ただし、スイッチに存在するICMP NATフローがアイドル状態になると、設定されたサンプリングタイムアウトの期限が切れた直後にタイムアウトします。

- Cisco Nexus 9300 プラットフォーム スイッチの ICMP にハードウェア プログラミングが導入されました。したがって、ICMP エントリはハードウェアの TCAM リソースを消費します。ICMP はハードウェア内にあるため、Cisco Nexus プラットフォーム シリーズ スイッチの NAT 変換の最大制限は 1024 に変更されます。リソースを最大限に活用するには、最大 100 ICMP エントリが許可されます。
- Cisco Nexus 9000シリーズスイッチで新しい変換を作成すると、変換がハードウェアでプログラムされるまでフローがソフトウェア転送されます。これには数秒かかることがあります。この期間中、内部グローバルアドレスの変換エントリはありません。したがって、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アドレスを割り当てます。
- ダイナミックNATでは、プールのオーバーロードとインターフェイスのオーバーロードは外部NATではサポートされません。
- NATオーバーロードは PBR（ポリシーベース ルーティング）を使用するため、PBR テーブル内の使用可能なネクストホップ エントリの最大数によって NAT の規模が決まります。NAT 内部インターフェイスの数が PBR テーブルで使用可能なネクストホップ エントリの範囲内にある場合、最大 NAT 変換スケールは変わりません。そうしないと、サポートされる変換の最大数が減少する可能性があります。PBR と NAT オーバーロードは相互に排他的ではありません。相互に制限されています。
- Cisco Nexus デバイスは、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）。
- **[ip nat 内部（ip nat inside）]** または **[ip nat 外部（ip nat outside）]** などの NAT 構成は、ループバック インターフェイスではサポートされていません。
- vPC を介したダイナミック NAT 機能はサポートされていません。
- トラフィックがPBR対応インターフェイスに入り、NATエントリがある場合、トラフィックは PBR 経由でルーティングされますが、IP アドレスは変換されません。

ダイナミック Twice NAT の注意事項および制約事項

Broadcom ベースの Cisco Nexus 9000 シリーズ スイッチでは、変換デバイス上の内部グローバル アドレスへのルートが外部インターフェイスを介して到達可能な場合、外部から内部へのネットワーク アドレス変換フローのパケットは、ネットワークでソフトウェアで転送、複製、およびループされます。この状況では、このフローの NAT 設定の最後に **add-route** CLI 引数を入力する必要があります。例えば、**`ip nat inside source static 192.168.1.1 172.16.1.1 add-route`** のようになります。

TCP/UDP/ICMP ヘッダーのない IP パケットは、ダイナミック NAT では変換されません。

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。

TCP 認識 NAT の注意事項および制約事項

TCP 対応 NAT には次の制限があります。

- TCP 対応 NAT 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。

  TCP 対応 NAT は、Cisco Nexus 9300-EX、FX、および FX2 シリーズ スイッチでサポートされます。

- Cisco NX-OS リリース 9.3(5) 以降、TCP 対応 NAT は Cisco Nexus N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX スイッチでサポートされます。
- 1 つの範囲のアドレス プールに関連付けることができる一致 ACL は 1 つだけです。プールを一致 ACL に関連付けると、インターフェイス IP を変更したり、プール範囲を変更したりできなくなります。
- ダイナミック NAT 設定で設定または使用する前に、プールを定義する必要があります。
- インターフェイスの過負荷の場合にプール範囲またはインターフェイスアドレスが変更されるたびに、ダイナミック NAT ルールを再設定する必要があります。

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

手順

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

	コマンドまたはアクション	目的
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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot*/*port*	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。 ループバック インターフェイスではこの構成がサポートされていません。
ステップ 4	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、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） 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、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Cisco Nexus デバイス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* [**vrf** *vrf-name*] [**match-in-vrf**] [**group** *group-id*]
3. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip nat inside source static** *local-ip-address global-ip-address* [**vrf** *vrf-name*] [**match-in-vrf**] [**group** *group-id*]	内部グローバル アドレスを内部ローカル アドレスに、またはその逆に（内部ローカル トラフィックを内部ローカル（local）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。 （注） Cisco Nexus 9000 シリーズ スイッチで Twice NAT 設定を実行している間は、異なる VRF 間で同じグループ ID を使用できません。一意の Twice NAT ルール

	コマンドまたはアクション	目的
		には、一意のグループ ID を使用する必要があります。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

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** *outsideGlobalIP outsideLocalIP* [**vrf** *vrf-name* [**match-in-vrf**] [**group** *group-id*] [**dynamic**] [**add-route**]]
3. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip nat outside source static** *outsideGlobalIP outsideLocalIP* [**vrf** *vrf-name* [**match-in-vrf**] [**group** *group-id*] [**dynamic**] [**add-route**]]	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

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

例

次に、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-address inside-global-address* | {**tcp**| **udp**} *inside-local-address* {*local-tcp-port* | *local-udp-port*} *inside-global-address* {*global-tcp-port* | *global-udp-port*}} {**vrf** *vrf-name* {**match-in-vrf**} {**group** *group-id*} }
3. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip nat inside source static** {*inside-local-address inside-global-address*	{**tcp**| **udp**} *inside-local-address* {*local-tcp-port*	*local-udp-port*} *inside-global-address* {*global-tcp-port*	*global-udp-port*}} {**vrf** *vrf-name* {**match-in-vrf**} {**group** *group-id*} }	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。

	コマンドまたはアクション	目的
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

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-address outside-local-address* | {**tcp** | **udp**} *outside-global-address* {*global-tcp-port* | *global-udp-port*} *outside-local-address* {*global-tcp-port* | *global-udp-port*}} {**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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip nat outside source static** {*outside-global-address outside-local-address* | {**tcp** | **udp**} *outside-global-address* {*global-tcp-port* | *global-udp-port*} *outside-local-address* {*global-tcp-port* | *global-udp-port*}} {**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。

	コマンドまたはアクション	目的
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

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 Network Address Translation（NAT）ルールを作成するために考慮されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat inside source static** *inside-local-ip-address inside-global-ip-address* [**group** *group-id*] [**add-route**]
4. **ip nat outside source static** *outside-global-ip-address outside-local-ip-address* [**group** *group-id*] [**add-route**]
5. **interface** *type number*
6. **ip address** *ip-address mask*
7. **ip nat inside**
8. **exit**
9. **interface** *type number*
10. **ip address** *ip-address mask*
11. **ip nat outside**
12. **end**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `switch> enable`	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。

	コマンドまたはアクション	目的
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	**ip nat inside source static** *inside-local-ip-address inside-global-ip-address* [**group** *group-id*] [**add-route**] 例： `switch(config)# ip nat inside source static 10.1.1.1 192.168.34.4 group 4`	内部ローカルIPアドレスを対応する内部グローバルIPアドレスに変換するようにスタティック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 4	**ip nat outside source static** *outside-global-ip-address outside-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`	スタティックTwice NATを設定して、外部グローバルIPアドレスを対応する外部ローカルIPアドレスに変換します。 • **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** *type number* 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	**ip address** *ip-address mask* 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	**ip nat inside** 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。 （注） ループバック インターフェイスでは構成がサポートされていません。
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** *type number* 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	**ip address** *ip-address mask* 例：	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。

	コマンドまたはアクション	目的
	`switch(config-if)# ip address 10.5.7.9 255.255.255.0`	
ステップ 11	**ip nat outside** 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。 （注） ループバック インターフェイスでは構成がサポートされていません。
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。

no-alias 設定の有効化と無効化

NAT デバイスは内部グローバル（IG）アドレスと外部ローカル（OL）アドレスを所有し、これらのアドレス宛ての ARP 要求に応答します。IG/OL アドレス サブネットがローカル インターフェイス サブネットと一致すると、NAT は IP エイリアスと ARP エントリをインストールします。この場合、デバイスは local-proxy-arp を使用して ARP 要求に応答します。

no-alias 機能は、アドレス範囲が外部インターフェイスの同じサブネットにある場合、特定の NAT プール アドレス範囲からのすべての変換された IP の ARP 要求に応答します。

NAT が設定されたインターフェイスで no-alias が有効になっている場合、外部インターフェイスはサブネット内の ARP 要求に応答しません。no-alias を無効にすると、外部インターフェイスと同じサブネット内の IP に対する ARP 要求が処理されます。

（注） この機能をサポートしていない古いリリースにダウングレードすると、*no-alias* オプションの設定が削除されることがあります。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature nat**
3. switch(config)# **show run nat**
4. switch(config)# **show ip nat-alias**
5. switch(config)# **clear ip nat-alias** *ip address*/*all*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **feature 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)# **show run nat**	NAT の設定を表示します。
ステップ 4	switch(config)# **show ip nat-alias**	エイリアスが作成されたかどうかの情報を表示します。 （注） デフォルトでは、エイリアスが作成されます。エイリアスを無効にするには、*no-alias* キーワードをコマンドに追加する必要があります。
ステップ 5	switch(config)# **clear ip nat-alias** *ip address*/*all*	エイリアスリストからエントリを削除します。特定のエントリを削除するには、削除する IP アドレスを指定する必要があります。すべてのエントリを削除するには、すべてのキーワードを使用します。

例

次に、すべてのインターフェイスの情報を表示する例を示します。

```
switch# configure terminal
switch(config)# show ip int b
IP Interface Status for VRF "default"(1)
Interface            IP Address      Interface Status
Lo0                  100.1.1.1       protocol-up/link-up/admin-up
Eth1/1               7.7.7.1         protocol-up/link-up/admin-up
Eth1/3               8.8.8.1         protocol-up/link-up/admin-up
```

次に、実行コンフィギュレーションの例を示します。

```
switch# configure terminal
switch(config)# show running-config nat
!Command: show running-config nat
!Running configuration last done at: Thu Aug 23 11:57:01 2018
!Time: Thu Aug 23 11:58:13 2018

version 9.2(2) Bios:version 07.64
feature nat
interface Ethernet1/1
  ip nat inside
interface Ethernet1/3
```

```
  ip nat outside
switch(config)#
```

この例は、エイリアスを設定する例を示します。

```
switch# configure terminal
switch(config)# ip nat pool p1 7.7.7.2 7.7.7.20 prefix-length 24
switch(config)# ip nat inside source static 1.1.1.2 8.8.8.3
switch(config)# ip nat outside source static 2.2.2.1 7.7.7.3
switch(config)# show ip nat-alias
Alias Information for Context: default
Address         Interface
7.7.7.2          Ethernet1/1
8.8.8.2          Ethernet1/3
switch(config)#
```

次に、*show ip nat-alias* の出力例を示します。デフォルトでは、エイリアスが作成されます。

```
switch# configure terminal
switch(config)# show ip nat-alias
Alias Information for Context: default
Address         Interface
7.7.7.2          Ethernet1/1
8.8.8.2          Ethernet1/3
switch(config)#
```

この例は、エイリアスを無効にする方法を示します。

```
switch# configure terminal
switch(config)# ip nat pool p1 7.7.7.2 7.7.7.20 prefix-length 24 no-alias
switch(config)# ip nat inside source static 1.1.1.2 8.8.8.3 no-alias
switch(config)# ip nat outside source static 2.2.2.1 7.7.7.3 no-alias
switch(config)# show ip nat-alias
Alias Information for Context: default
Address         Interface
7.7.7.2          Ethernet1/1
8.8.8.2          Ethernet1/3
switch(config)#

** None of the entry got appended as alias is disabled for above CLIs.
switch(config)#
```

この例は、エイリアスをクリアする方法を示します。エイリアス リストからエントリを削除するには、*clear ip nat-alias* を使用します。IP アドレスを指定して 1 つのエントリを削除することも、すべてのエイリアス エントリを削除することもできます。

```
switch# configure terminal
switch(config)# clear ip nat-alias address 7.7.7.2
switch(config)# show ip nat-alias
Alias Information for Context: default
Address         Interface
8.8.8.2          Ethernet1/3
switch(config)#
switch(config)# clear ip nat-alias all
switch(config)# show ip nat-alias
switch(config)#
```

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

次に、内部送信元および外部送信元のスタティック双方向NATを設定する例を示します。

```
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
```

静的 NAT の構成の確認

静的 NAT 構成がアクティブであり、予想どおりに動作していることを確認します。

トラブルシューティングまたは検証のために現在の静的 NAT マッピングを表示するには、次の手順を活用。

手順

	コマンドまたはアクション	目的
ステップ 1	IP NAT 変換を確認します。 例： `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 IP アドレスの変換を示します。

出力には、構成されているすべての NAT 変換が示されます。

例

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 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. **enable**
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. **ip nat inside source list** *access-list-name* **interface** *type number* [**vrf** *vrf-name* [**match-in-vrf**] [**add-route**] [**overload**]
8. **interface** *type number*

9. **ip address** *ip-address mask*
10. **ip nat inside**
11. **exit**
12. **interface** *type number*
13. **ip address** *ip-address mask*
14. **ip nat outside**
15. **exit**
16. **ip nat translation max-entries** *number-of-entries*
17. **ip nat translation timeout** *seconds*
18. **ip nat translation creation-delay** *seconds*
19. **ip nat translation icmp-timeout** *seconds*
20. **end**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
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。
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`	条件に一致するトラフィックを許可する条件をIPアクセスリストに設定します。
ステップ 5	**deny** *protocol source source-wildcard* **any** 例： `Switch(config-acl)# deny udp 10.111.11.100/32 any`	ネットワークに入る時に拒否されるパケットの条件を IP アクセス リストに設定します。
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。

	コマンドまたはアクション	目的
ステップ 7	**ip nat inside source list** *access-list-name* **interface** *type number* [**vrf** *vrf-name* [**match-in-vrf**] [**add-route**] [**overload**] 例： `Switch(config)# ip nat inside source list acl1 interface ethernet 1/1 overload`	ステップ 3 で定義したアクセス 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** *type number* 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	**ip address** *ip-address mask* 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	**ip nat inside** 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。 （注） ループバック インターフェイスでは構成がサポートされていません。
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** *type number* 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 13	**ip address** *ip-address mask* 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	**ip nat outside** 例： `Switch(config-if)# ip nat outside`	インターフェイスを外部ネットワークに接続します。 （注） ループバック インターフェイスでは構成がサポートされていません。

	コマンドまたはアクション	目的
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	**ip nat translation max-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ー1023です。
ステップ 17	**ip nat translation timeout** *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	**ip nat translation creation-delay** *seconds* 例： `switch(config)# ip nat translation creation-delay 250`	ダイナミック NAT 変換の ICMP タイムアウト値を指定します。 （注） ハードウェアでのNATエントリのプログラミング頻度を減らすために、NAT は変換を 1 秒間バッチ処理してプログラミングします。ハードウェアのプログラミングを頻繁に行うとCPUに負荷がかかりますが、プログラミングを遅らせるとセッションの確立が遅れます。このコマンドを使用して、バッチ処理を無効にしたり、作成遅延を短縮したりできます。作成遅延を 0 に設定することは推奨されません。
ステップ 19	**ip nat translation icmp-timeout** *seconds* 例： `switch(config)# ip nat translation icmp-timeout 100`	ダイナミック NAT 変換の ICMP タイムアウト値を指定します。
ステップ 20	**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、 コマンドを使用するか、 **ip nat pool** を使用します 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* [*startip endip*] {**prefix** *prefix-length* | **netmask** *network-mask*}
4. （任意） switch(config-ipnat-pool)# **address** *startip endip*
5. （任意） switch(config)# **no ip nat pool** *pool-name*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **feature nat**	デバイスの 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* [*startip endip*] {**prefix** *prefix-length* | **netmask** *network-mask*}	グローバル IP アドレスの範囲で NAT プールを作成します。IP アドレスは、プレフィッ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	（任意） switch(config-ipnat-pool)# **address** *startip endip*	グローバル IP アドレスの範囲を指定します（プールの作成時に指定していなかった場合）。
ステップ 5	（任意） switch(config)# **no ip nat pool** *pool-name*	指定した NAT プールを削除します。

例

次に、プレフィックス長を使用して NAT プールを作成する例を示します。

```
switch# configure terminal
switch(config)# ip nat pool pool1 30.1.1.1 30.1.1.2 prefix-length 24
switch(config)#
```

次に、ネットワークマスクを使用して NAT プールを作成する例を示します。

```
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、NAT プールを作成し、 **ip nat pool** を使用してグローバル IP アドレスの範囲を定義します。 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)#
```

次の例は、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。

始める前に

プールの送信元リストを設定する前に、必ずプールを設定してください。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	（任意） switch# **ip nat inside source list** *list-name* **pool** *pool-name* [**overload**]	オーバーロードの有無にかかわらず、プールを使用して NAT 内部送信元リストを作成します。
ステップ 3	（任意） switch# **ip nat outside source list** *list-name* **pool** *pool-name* [**add-route**]	オーバーロードなしでプールを使用して NAT 外部送信元リストを作成します。

例

次に、オーバーロードのないプールを使用してNAT内部送信元リストを作成する例を示します。

```
switch# configure terminal
switch(config)# ip nat inside source list list1 pool pool1
switch(config)#
```

次に、オーバーロードのあるプールを使用してNAT内部送信元リストを作成する例を示します。

```
switch# configure terminal
switch(config)# ip nat inside source list list2 pool pool2 overload
switch(config)#
```

次に、オーバーロードのないプールを使用してNAT外部送信元リストを作成する例を示します。

```
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にはダイナミック双方向 NAT を設定できます。

始める前に

スイッチで NAT 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)# **ip nat outside source static** *outside-global-ip-address outside-local-ip-address* | [**tcp** | **udp**] *outside-global-ip-address outside-global-port outside-local-ip-address outside-local-port* [**group** *group-id*] [**dynamic**] [**add-route**]
3. switch(config)# **ip nat inside source list** *access-list-name* [**interface** *type slot/port* **overload** | **pool** *pool-name* **overload**] [**group** *group-id*] [**dynamic**] [**add-route**]
4. switch(config)# **ip nat pool** *pool-name* [*startip endip*] {**prefix** *prefix-length* | **netmask** *network-mask*}
5. switch(config)# **interface** *type slot/port*
6. switch(config-if)# **ip nat outside**
7. switch(config-if)# **exit**
8. switch(config)# **interface** *type slot/port*
9. switch(config-if)# **ip nat inside**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip nat outside source static** *outside-global-ip-address outside-local-ip-address* | [**tcp** | **udp**] *outside-global-ip-address outside-global-port outside-local-ip-address outside-local-port* [**group** *group-id*] [**dynamic**] [**add-route**]	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か、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** *type slot/port* **overload** | **pool** *pool-name* **overload**] [**group** *group-id*] [**dynamic**] [**add-route**]	オーバーロードの有無にかかわらず、プールを使用して NAT 内部ソースリストを作成することによって、ダイナミック ソース変換を確立します。 **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* [*startip endip*] {**prefix** *prefix-length* | **netmask** *network-mask*}	グローバル IP アドレスの範囲で NAT プールを作成します。IP アドレスは、プレフィッ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** *type slot/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**	インターフェイスを外部ネットワークに接続します。
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** *type slot/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。

例

次に、内部送信元アドレスのダイナミック双方向 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

内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。外部送信元アドレスにダイナミック双方向 NATを設定できます。

始める前に

スイッチで NAT 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)# **ip nat inside source static** *inside-local-ip-address inside-global-ip-address* | [**tcp** | **udp**] *inside-local-ip-address local-port inside-global-ip-address global-port* [**group** *group-id*] [**dynamic**] [**add-route**]
3. switch(config)# **ip nat outside source list** *access-list-name* **pool** *pool-name* [**group** *group-id*] **dynamic** [**add-route**]
4. switch(config)# **ip nat pool** *pool-name* [*startip endip*] {**prefix** *prefix-length* | **netmask** *network-mask*}
5. switch(config)# **interface** *type slot/port*
6. switch(config-if)# **ip nat outside**
7. switch(config-if)# **exit**
8. switch(config)# **interface** *type slot/port*
9. switch(config-if)# **ip nat inside**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip nat inside source static** *inside-local-ip-address inside-global-ip-address*	[**tcp**	**udp**] *inside-local-ip-address local-port inside-global-ip-address global-port* [**group** *group-id*] [**dynamic**] [**add-route**]	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か、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。

	コマンドまたはアクション	目的
		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* **pool** *pool-name* [**group** *group-id*] **dynamic** [**add-route**]	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。
ステップ 4	switch(config)# **ip nat pool** *pool-name* [*startip endip*] {**prefix** *prefix-length* | **netmask** *network-mask*}	グローバル IP アドレスの範囲で NAT プールを作成します。IP アドレスは、プレフィッ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** *type slot/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**	インターフェイスを外部ネットワークに接続します。
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** *type slot/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。

例

次に、外部送信元アドレスにダイナミック双方向 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 outside source list acl_1 pool pool_1 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
```

FINRST および SYN タイマーの設定

ここでは、FINRST および SYN タイマー値の設定方法について説明します。

スイッチをリロードする場合、設定された FINRST や SYN タイマー値の復元または消去は、TCP TCAM が切り分けられるかどうかによって異なります。TCAM が切り分けられると、スイッチは現在設定されている値を復元します。

タイマー値が構成されていない場合、デフォルト値の 60 秒が設定されます。TCAM が切り分けられていない場合、スイッチは現在設定されている値をすべて削除し、デフォルト値を never に設定します。これは、TCP TCAM が切り分けられていない場合、TCP AWARE 機能がディセーブルになるためです。

手順の概要

1. switch# **configure terminal**
2. switch(config-if)# **ip nat translation syn-timeout** {**seconds** | **never**}
3. switch(config-if)# **ip nat translation finrst-timeout** {**seconds** | **never**}

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config-if)# **ip nat translation syn-timeout** {**seconds** | **never**}	SYN 要求を送信するが SYN-ACK 応答を受信しない TCP データのパケットタイムアウト値を指定します。タイムアウト値の範囲は、1 ～ 172800 秒です。TCP TCAM が切り分けられる場合、デフォルト値は 60 秒です。TCP TCAM が切り分けられていない場合、デフォルト値は *never* です。*never* キーワードは、SYN タイマーを非アクティブにします。 （注） TCP TCAM が切り分けられていない場合は、SYN タイマーを設定できません。
ステップ 3	switch(config-if)# **ip nat translation finrst-timeout** {**seconds** | **never**}	終了（FIN）パケットまたはリセット（RST）パケットを受信して接続が終了したときのフローエントリのタイムアウト値を指定します。RST と FIN の両方の動作を設定する必要があります。タイムアウト値の範囲は、1 ～ 172800 秒です。TCP TCAM が切り分けられる場合、デフォルト値は 60 秒です。TCP TCAM が切り分けられていない場合、デフォルト値は *never* です。*never* キーワードは、FIN または RST タイマーを非アクティブにします。 （注）

	コマンドまたはアクション	目的
		TCP TCAM が切り分けられていない場合は、FINRST タイマーを設定できません。

例

次の例は、TCP TCAM が切り分けられるタイミングを示しています。

```
switch(config)# ip nat translation syn-timeout 20
```

次の例は、TCP TCAM が切り分けられていない場合を示しています。

```
switch(config)# ip nat translation syn-timeout 20
Error: SYN TIMER CONFIG FAILED.TCP TCAM NOT CONFIGURED
```

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
clear ip nat translation [**all** | **inside** *global-ip-address local-ip-address* [**outside** *local-ip-address global-ip-address*] | **outside** *local-ip-address global-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。

例

次に、すべてのダイナミック変換をクリアする例を示します。

```
switch# clear ip nat translation all
```

次に、内部アドレスと外部アドレスのダイナミック変換をクリアする例を示します。

```
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。 エントリが作成および使用された日時など、各変換テーブル エントリの追加情報を表示します。

コマンド	目的
show run nat	NAT の設定を表示します。
show ip nat max	アクティブなネットワーク アドレス変換（NAT）の最大値を表示します。
show ip nat statistics	NAT 統計情報をモニタします。

例

次に、IP NAT 最大値を表示する例を示します。

```
switch# show ip nat max

IP NAT Max values
====================
Max Dyn Translations:80
Max all-host:0
No.Static:0
No.Dyn:1
No.Dyn-ICMP:1
====================
Switch(config)#
```

次に、NAT 統計情報を表示する例を示します。

```
switch# show ip nat statistics

IP NAT Statistics
==================================================
Stats Collected since: Mon Feb 24 18:27:34 2020
--------------------------------------------------
Total active translations: 1
No.Static: 0
No.Dyn:    1
No.Dyn-ICMP:   1
--------------------------------------------------
Total expired Translations: 0
SYN timer expired:          0
FIN-RST timer expired:      0
Inactive timer expired:     0
--------------------------------------------------
Total Hits:  2                  Total Misses:  2
In-Out Hits: 0                  In-Out Misses: 2
Out-In Hits: 2                  Out-In Misses: 0
--------------------------------------------------
Total SW Translated Packets: 2
In-Out SW Translated: 2
Out-In SW Translated: 0
--------------------------------------------------
Total SW Dropped Packets: 0
In-Out SW Dropped: 0
Out-In SW Dropped: 0

Address alloc. failure drop:      0
Port alloc.  failure drop:        0
Dyn. Translation max limit drop:  0
ICMP max limit drop:              0
```

```
Allhost max limit drop:           0
------------------------------------------------------
Total TCP session established: 0
Total TCP session closed:      0
------------------------------------------------------
NAT Inside Interfaces:  1
Ethernet1/34

NAT Outside Interfaces: 1
Ethernet1/32
------------------------------------------------------
Inside source list:
++++++++++++++++++++

Access list: T2
RefCount: 1
Pool: T2     Overload
Total addresses: 10
Allocated: 1    percentage: 10%
Missed: 0


Outside source list:
++++++++++++++++++++
------------------------------------------------------
======================================================
Switch(config)#
Switch(config)#


**No.Dyn-ICMP  field is to display the no of icmp dynamic translations , its a subset
of  "No.Dyn" field.
```

（注） Cisco NX-OS リリース 9.3(5) 以降では、**No.Dyn-ICMP** フィールドは **No.Dyn** フィールドのサブセットであり、ICMP ダイナミック変換の数が表示されます。

次に、NAT の実行コンフィギュレーションを表示する例を示します。

```
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
```

次に、アクティブな NAT 変換を表示する例を示します。

オーバーロードのある内部プール

```
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
```

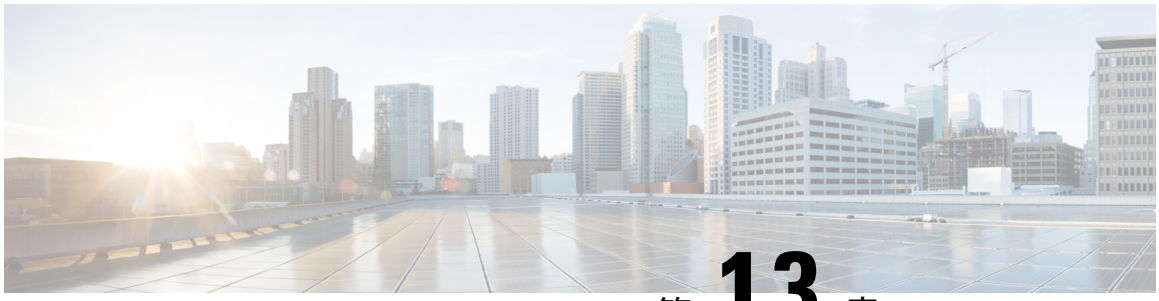
オーバーロードのない外部プール

```
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

次に、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）を設定する例を示します。

```
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
```



第 13 章

単一方向イーサネットの設定

この章では、Cisco Nexus 9000 シリーズ スイッチで双方向イーサネットを設定する方法を説明します。

単一方向イーサネット

単方向イーサネット（UDE）は、データの送受信に単一の光ファイバストランドを使用して通信できるネットワーク技術です。

単方向リンクを使用して、トラフィック ビデオ ストリーミング アプリケーションを送受信できます。これらのシナリオでは、ほとんどのトラフィックは確認応答されない一方向ストリームとして送信されます。

単方向リンクを作成するには、トラフィックを一方向に送受信するように、双方向トランシーバを使用して ポートを設定します。

適切な単一方向トランシーバが使用できない場合は、UDEを使用します。送信専用トランシーバがない場合は、ソフトウェアベース UDE で送信専用リンクを構成する必要があります。

ネットワークの停止を防ぐためにインターフェイスから離れるすべての制御トラフィックをブロックする必要がある場合は、QoSテンプレートを使用して特定のイーサネットポート上のすべての発信トラフィックをブロックします。

単方向イーサネット設定のベストプラクティス

Nexusスイッチで UDE を設定するには、次のベスト プラクティスと推奨事項を活用

- Nexusスイッチの送信専用モードでUDE を構成します。Cisco NX-OSリリース 10.1(2) より前のリリースでは、UDE 受信専用を使用 できません 。

- すべてのポートで同時に UDE をイネーブルにできます。
- Cisco NX-OSリリース 10.1(1) 以降から、UDE のブレークアウト サポートを使用できます。
- ポートで UDE を設定すると、ポート フラップが発生することがあります。UDE 設定の有無にかかわらず、物理インターフェイスをポート チャネルに追加できます。ただし、ポート チャネルに送信専用インターフェイスだけを追加してください。

  送信専用設定を他のインターフェイスと混在させると、UDE が動作しないことがあります。
- ポート チャネルのすべてのメンバーを UDE 送信専用として設定すると、ポート チャネルがパケットを受信できない場合があります。
- 特別なコントロール プレーン トラフィック プルーニングは、送信専用ポートでは設定されません。
- 単一方向ポートでは、次のようにリンクの反対側の終端にあるポートとのネゴシエーションが必要になる機能またはプロトコルがサポートされません。双方向通信を必要とするすべての機能をディセーブルにする必要があります。

UDE ポリサーの注意事項

Cisco NX-OS リリース 10.3(3) 以降、QoS テンプレート ベースの UDE を使用できます。UDE ポリシングの注意事項と制限事項を示します：

- レイヤ2インターフェイスでのみUDEテンプレートをイネーブルにします。ポートをタップアグリゲーション モードに設定します。
- ポリシーマップ **default-ndb-out-policy** は、システム QoS ではサポートされません。この機能をサポートするには、出力レイヤ 2 QoS TCAM リージョンをカービングします。

  リブート時に、スイッチは **default-ndb-out-policy** を構成されたインターフェイスに適用するのに時間がかかる場合があります。この期間中に、一部のパケットが転送される可能性があります。ポリシーが適用された後、スイッチはすべての出力制御トラフィックとフラッド トラフィックをドロップします。

  データ トラフィックがない場合でも、制御トラフィック プロトコル（ CPUからのCDP、LLDP、 ARP、 BPDUなど）がACLエントリと一致するためにドロップされます。これにより、違反数が増加します。この動作は **ndb-out-policy** を構成されている場合に予想されるものです。
- QoSテンプレートベースの UDE は、 Cisco Nexus 9300-FX、FX2、FX3、GX、GX2 シリーズ スイッチ、および 9700-FX または GX ライン カードを搭載したCisco Nexus 9500 シリーズ スイッチで使用できます。
- ポート チャネルでは QoS テンプレートを使用 できません 。

Nexus スイッチでの UDE サポート

- UDE サポートは、ネイティブ 10G-LR/10G-LRS トランシーバでのみ使用できます。UDE は、QSA またはブレークアウトケーブルでは使用 できません 。
- Cisco NX-OS リリース 10.1(2) 以降、UDE は Cisco Nexus スイッチでサポートされます。
  - N9K-X9624D-R2
  - N9K-X9636Q-R
  - N9K-X9636C-RX
  - N9K-X96136YC-R
  - N9K-X9624D-R2
  - N9K-X9636C-R
- ハードウェア レベルの UDE は、X97160YC-EX ライン カードを搭載した Cisco Nexus 9500 スイッチでのみサポートされます。
- Cisco NX-OS リリース 10.1(1) 以降、UDE は以下のポートでサポートされます。
  - Cisco Nexus 9000 FX、FX2、FX3 プラットフォーム スイッチ
  - N9K-C9336C-FX2
  - N9KC93240YC-FX2
  - N9K-C93180YC-FX
  - N9K-C93360YC-FX2 TOR スイッチ
  - N9K-X97160YC- EX ライン カード。
- Cisco NX-OS リリース 10.1(1) 以降、UDE は 10G-SR、10G-AOC、40G-SR、40G-LR、40G-AOC、100G-SR、100G-LR、および 100G-AOC の各トランシーバをサポートしています。 。

単一方向イーサネットの構成

スイッチ上で単方向通信のイーサネットインターフェイスを構成します。インターフェイスを送信専用モードまたは受信専用モードに設定。

手順

	コマンドまたはアクション	目的
ステップ 1	**interface ethernet** {**type slot /port**} コマンドを入力して、イーサネットインターフェイスの構成モードを終了します。	

	コマンドまたはアクション	目的
	例： `switch(config)# interface ethernet 3/1`	
ステップ 2	**unidirectional send-only** コマンドを使用して送信専用モードを構成します。 例： `switch(config-if)# unidirectional send-only`	
ステップ 3	**unidirectional receive-only** コマンドを使用して、受信専用モードを構成します。 例： `switch(config-if)# unidirectional receive-only`	
ステップ 4	**exit** コマンドを使用してインターフェイス モードを終了します。 例： `switch(config)# exit`	
ステップ 5	**show running-config interface** {**type slot /port**} コマンドを使用して、インターフェイスの実行中の構成を表示します。 例： `switch(config)# show running-config interface ethernet 3/1`	
ステップ 6	**copy running-config startup-config** コマンドを使用して構成を保存します。 例： `switch(config)# copy running-config startup-config`	

イーサネット インターフェイスは単方向に動作するように設定されています。

例

この例は、送信専用の単方向通信のイーサネットインターフェイスを設定する方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# unidirectional send-only
switch(config-if)# exit
switch(config)# exit
switch#
```

次に、インターフェイスの実行中の構成を表示し、単方向設定を確認して、構成を保存する例を示します。

```
switch# show running-config interface ethernet 3/1
!
interface ethernet 3/1
  unidirectional send-only
!
```

UDE ポリサーの構成

単方向イーサネット（UDE）QoSポリシーを使用して、イーサネットポートのすべての出力通信をブロックまたは制限します。

QoSテンプレートを使用して単一方向イーサネットを構成するには、次のステップを実行します。

手順

ステップ 1 **hardware access-list tcam region egr-l2-qos 256** コマンドを使用して、出力レイヤ 2 QoSのTCAM （Ternary Content Addressable Memory（CAM） ）リージョンを設定し、リソースを割り当てます。

このリージョンのサイズを 256 エントリに設定します。

ステップ 2 **copy run start** コマンドを使用して実行中の構成（ TCAMリージョンの変更を含む）をパスワード保存します。

変更を保存すると、リロード後も設定は保持されます。

ステップ 3 **reload** コマンドを使用してスイッチをリロードし、新しいTCAM構成の変更を適用します。

例：

```
switch(config)# hardware access-list tcam region egr-l2-qos 256
```

TCAM リージョンを変更した後、変更を有効にするには、スイッチを再起動する必要があります。

ステップ 4 **interface type slot/port** コマンドを入力して、イーサネット インターフェイスの構成モードを終了します。

例：

```
switch(config)# interface Ethernet 1/6
switch(config-if)#
```

ステップ 5 **service-policy type qos output default-ndb-out-policy** コマンドを使用して、UDE QoSサービス ポリシーをインターフェイスに適用します。

スイッチは、イーサネットインターフェイス上のすべての出力通信をポリシングします。スイッチは、設定されたパラメータを満たすトラフィックだけを転送し、違反するトラフィックをドロップします。

接続された QoS ポリシーは、イーサネットポート上のすべての出力通信を制限またはブロックします。設定されたポリシングパラメータに適合するトラフィックだけが転送されます。これらのパラメータに違反するすべてのトラフィックがドロップされます。

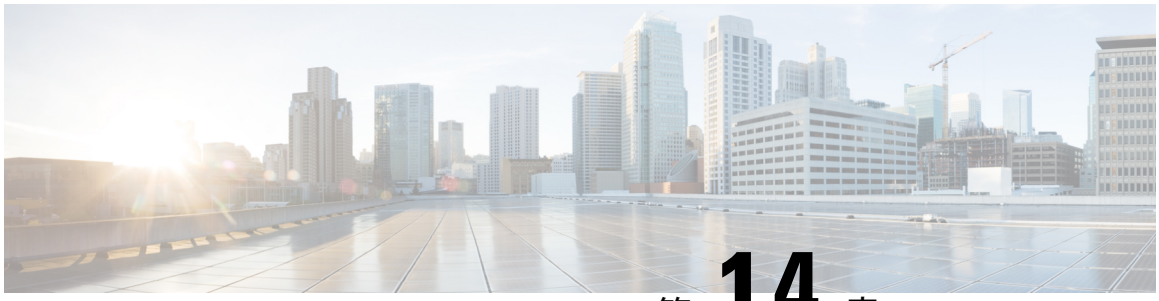
次のタスク

show policy-map type qos default-ndb-out-policy コマンドを使用してポリシーのステータスを確認します。

```
switch# show policy-map type qos default-ndb-out-policy

Type qos policy-maps
====================
policy-map type qos default-ndb-out-policy
class class-ndb-default
police cir 0 bps conform transmit violate drop
```

特定のインターフェイスの UDE ポリシーの統計情報を確認します。

```
switch# show policy-map interface Ethernet 1/6 output type qos

Global statistics status : enabled
Ethernet1/6
Service-policy (qos) output: default-ndb-out-policy
SNMP Policy Index: 285213501
Class-map (qos): class-ndb-default (match-any)
Slot 1
61211339 packets 15669992128 bytes
5 minute offered rate 17721223780 bps
Aggregate forwarded :
61211339 packets 110848 bytes
police cir 0 bps
conformed 0 bytes, n/a bps action: transmit
violated 15669881280 bytes, n/a bps action: drop
```



第 14 章

レイヤ 2 Data Center Interconnect の設定

このセクションでは、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）を設定する方法について説明します。

Data Center Interconnect（概念）

Data Center Interconnect（DCI）は、

- 2 つ以上の異なるデータセンター施設を任意の距離でリンクする
- 特定の VLAN を拡張し、サーバーおよびネットワーク接続ストレージ（NAS）デバイスにレイヤ 2 隣接関係を提供するネットワーキング技術と方法論のセットです。

Cisco Nexus 9000 シリーズスイッチは、FHRP 分離を使用した DCI をサポートします。ただし、N9K-X9636C-R および N9K-X9636Q-R ライン カードを搭載した Cisco Nexus 9500 スイッチでは、FHRP 分離を使用した DCI はサポートされていません。vPC を使用して複数のサイト間に単一の論理リンクを作成すると、DCI vPC ポート チャネル全体で BPDU フィルタリングを使用した STP 分離の利点を活用できます。この設定では、ブリッジ プロトコル データ ユニット（BPDU）はデータ センター間を通過せず、サイト間の STP 障害ドメインを効果的に分離します。

（注） 最大 2 つのデータ センターを相互接続するには、vPC を使用してください。

Nexus スイッチでの DCI サポート

（注） サポートされているプラットフォームには、N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RX ライン カードを搭載した Cisco Nexus 9500 シリーズ スイッチがあります。

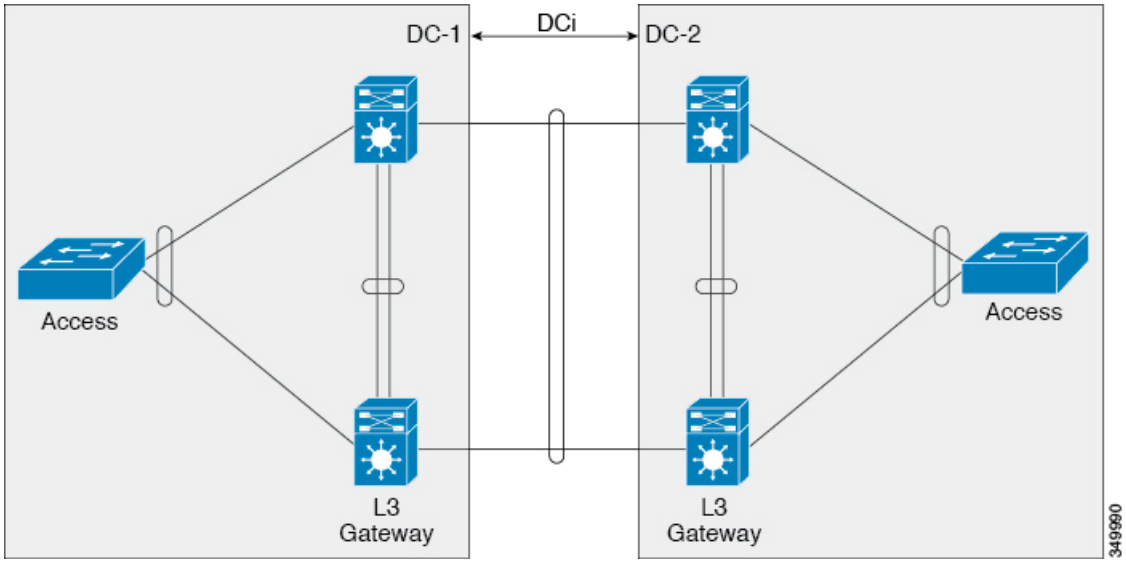
レイヤ 2 Data Center Interconnect の例

次に、vPCを使用したレイヤ2データセンターインターコネクト（DCI）の設定例を示します。次の例は、ファースト ホップ冗長性プロトコル（FHRP）分離を可能にします。

（注） vPCおよびホットスタンバイルーティングプロトコル（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 *38 :* デュアル レイヤ *2*/レイヤ *3* の *POD* 相互接続



この例では、同じ vPC のペアでレイヤ 3 （L3）ゲートウェイが設定され、DCI として機能します。Hot Standby Routing Protocol（HSRPHSRP を分離するには、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 を横断して移動する VLAN 用のスイッチ仮想インターフェイス（SVI）上で 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
```

第 15 章

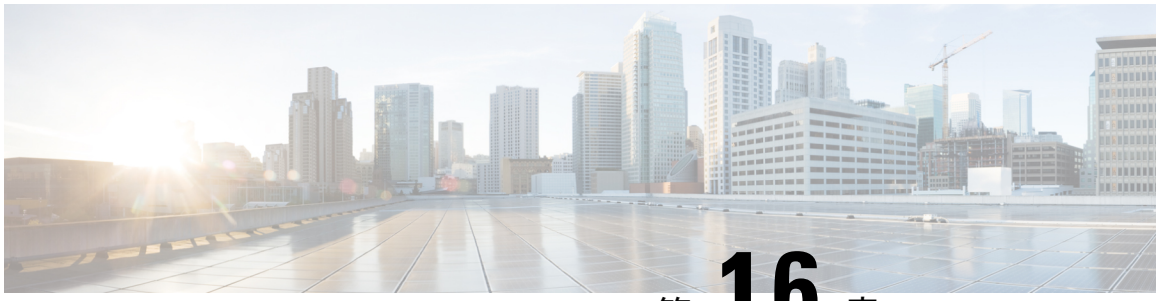
Cisco NX-OS インターフェイスがサポートする IETF RFC

ここでは、Cisco NX-OS でサポートされているインターフェイスの IETF RFC を示します。

IPv6 の RFC

RFC	タイトル
RFC 2373	『*IP Version 6 Addressing Architecture*』
RFC 2374	集約可能なグローバル ユニキャスト形式
RFC 2460	『*Internet Protocol, Version 6 (IPv6) Specification*』
RFC 2462	『*IPv6 Stateless Address Autoconfiguration*』
RFC 2464	イーサネット ネットワーク上での *IPv6* パケットの送信
RFC 2467	『*Transmission of IPv6 Packets over FDDI Networks*』
RFC 2472	『*IP Version 6 over PPP*』
RFC 2492	『*IPv6 over ATM Networks*』
RFC 2590	『*Transmission of IPv6 Packets over Frame Relay Networks Specification*』
RFC 3021	*IPv4 Point-to-Point* リンクでの *31* ビット プレフィックスの使用
RFC 3152	*IP6.ARPA* の委任
RFC 3162	*RADIUS* および *IPv6*

RFC	タイトル
RFC 3513	インターネット プロトコル バージョン 6（IPv6）アドレス 指定アーキテクチャ
RFC 3596	IP バージョン 6 への DNS 拡張
RFC 4193	固有ローカル IPv6 ユニキャスト アドレス



第 16 章

Cisco NX-OS インターフェイスの設定制限

設定制限は『*Cisco Nexus 9000* シリーズ *NX-OS* 検証済みスケーラビリティ ガイド』にまとめられています。

第 17 章

400G デジタル コヒーレント光ファイバの構成

この章では、400G デジタル コヒーレント QSFP-DD 光モジュールとサポートされる構成について説明します。

• OLS 構成の確認 （535 ページ）

400G デジタル コヒーレント光ファイバの概要

振幅のみを使用する PAM4 光ファイバ（パルス振幅変調）とは異なり、コヒーレント光ファイバは位相と振幅を使用してデータをエンコードします。これにより、コヒーレント光ファイバはノイズに対する耐性が向上しており、長距離伝送をサポートできます。

Cisco 400G デジタル コヒーレント光ファイバの詳細については、『Cisco 400G デジタル コヒーレント光ファイバ QSFP-DD 光ファイバ モジュール データ シート』を参照してください。

400G デジタル コヒーレント光ファイバには 2 つのバリエーションがあります。

- **ZR バリアント**：QSFP-DD ZR バリアントは OIF MSA に準拠しており、同じ MSA 標準に準拠した同等のコンポーネントとの互換性を提供します。ZR 標準の主な用途は、ポイントツーポイント トポロジで 400G 波長を最大 120 km の距離まで伝送できるようにすることです。
- **ZR Plus バリアント**：QSFP-DD OpenZR+ モジュールは、OpenZR+ MSA に準拠しています。ZR+プラグ可能コヒーレント光ファイバは、エンドポイント間で複数の波長を増幅できる複数のサイトを使用することにより、地域内から長距離伝送までをサポートします。ZR+は、変調方式、シェーピング、およびボーレートに関する複数の構成オプションをサポートしており、さまざまなネットワーク トポロジに対応し、他の方式よりも長い伝送距離（120 km 超）を可能にしています。

400G デジタル コヒーレント光ファイバ パラメータ

400G デジタル コヒーレント光ファイバは構成可能で、光ファイバに関する次のパラメータを構成できます。構成値の詳細については、表 20 : 400G デジタル コヒーレント QSFP-DD トラフィックの構成値 （488 ページ） を参照してください。

- **[トランスポンダ/マックスポンダ モード（Transponder/Muxponder mode）]**：このパラメータは、メディア回線を 400G で構成し、ホスト側に最大 4 つのクライアントを構成するために使用されます。
- **[DAC レート（DAC rate）]**：デジタル アナログ変換（DAC）パラメータは、オーバーサンプリング（パルス整形の有効化または無効化）とメディア回線モデムを標準（S）または拡張（E）に設定するために使用されます。
- **[FEC モード（FEC mode）]**：前方誤り訂正（FEC）は、メディア回線で cFEC または oFEC モードをサポートし、データ伝送中のエラーを制御するために使用されます。
- **[変調（Modulation）]**：このパラメータは、光波を制御して、搬送光波の情報をエンコードするために使用されます。サポートされる変調は、16 QAM、8 QAM、および QPSK です。

- **[CD 最小/最大（CD min/max）]**：波長分散（CD）は、光ファイバ通信において重要な要素となる現象です。光線が接続先に到達する時間がわずかに異なることで、その色(波長)に違いが生じることによって発生します。このパラメータは、デバイスが良好な光信号と周波数を取得する範囲を設定するために使用されます。

マックスポンダ-FEC-変調	CD デフォルト高（ps/nm）	CD デフォルト低（ps/nm）	最大プロビジョニング可能 CD 高（ps/nm）	最小プロビジョニング可能な CD 低（ps/nm）
400G-400GZR-cFEC-16QAM	2400	-2400	2400	-2400
400G-400GZR-oFEC-16QAM	13,000	-13000	52000	-52000
200G-200GZR-oFEC-QPSK	50000	-50000	100000	-100000
200G-200GZR-oFEC-8QAM	26000	-26000	100000	-100000
200G-200GZR-oFEC-16QAM	21000	-21000	85000	-85000
100G-100GZR-oFEC-QPSK	80000	-80000	160000	-160000

- **[Tx パワー（Tx power）]**：送信光ファイバ パワーは、光ファイバ モジュールの送信端にある光源の出力光ファイバ パワーを指し、受信光パワーは、光ファイバ モジュールの受信端にある光源の入力光ファイバ パワーを指します。

  各光モジュールには、独自の送信（TX）電力範囲があります。モジュールの機能に基づいて、送信（TX）電力値を変更できます。

光ファイバ モジュール	トランク速度[1、3]	光ファイバ送信パワー（Tx）シェイピング	インターバル（Interval	光ファイバ送信電力（Tx）値のサポートされる範囲（0.1 dBm 単位）[2]		
				最小値（Minimum Value）	最大標準値	最大最悪ケース値
QDD400GZRS	400G	いいえ	1	-150	-100	-100
QDD400GZRPS	400G	はい	1	-150	-110	-130
QDD400GZRPS	200G	はい	1	-150	-90	-105
QDD400GZRPS	100 G	はい	1	-150	-59	-75

- **[周波数（Frequency）]**：光ファイバ通信では、波長分割多重（WDM）は、異なる波長（つまり色）のレーザー光を使用して、複数の光キャリア信号を単一の光ファイバに多重化する技術です。この技術により、波長分割デュプレックスとも呼ばれる1本の光ファイバを介した双方向通信と、キャパシティの増加が可能になります。このパラメータは、ITU C-BANDテーブルの任意の周波数を設定するために使用されます。値の詳細については、「ITU C-BAND テーブル （545 ページ）」セクションを参照してください。

構成の詳細については、「ZR モジュールでの 400G デジタル コヒーレント光ファイバの構成 （494 ページ）」セクションを参照してください。

次の表に、トランスポンダ（TXP）およびマックスポンダ（MXP）モードでの 400G デジタル コヒーレント QSFP-DD 光ファイバ モジュールの可能なトラフィック構成値を示します。

表 *20 : 400G* デジタル コヒーレント *QSFP-DD* トラフィックの構成値

クライアント速度	トランク速度	周波数	FEC	変調	DAC レート
QDD-400G-ZR-S トランスポンダおよびマックスポンダの構成値					
1 クライアント、速度 400G	1 トランク、400G	C バンド、196.1 ～ 191.3 THz	cFEC	16 QAM	1 x 1
QDD-400G-ZRP-S トランスポンダおよびマックスポンダの構成値					
1X400GA UI-8	1 トランク、速度 400G	C バンド、196.1 ～ 191.3 THz	cFEC	16 QAM	1 x 1
4X100GA UI-2					
1X400GA UI-8	1 トランク、速度 400G	C バンド、196.1 ～ 191.3 THz	cFEC	16 QAM	1x1.5
4X100GA UI-2					
1X400GA UI-8	1 トランク、速度 400G	C バンド、196.1 ～ 191.3 THz	oFEC	16 QAM	1x1.25
4X100GA UI-2					
1X400GA UI-8	1 トランク、速度 400G	C バンド、196.1 ～ 191.3 THz	oFEC	16 QAM	1x2
4X100GA UI-2					
1X400GA UI-8	1 トランク、速度 400G	C バンド、196.1 ～ 191.3 THz	oFEC	16 QAM	1 x 1
4X100GA UI-2					

クライアント速度	トランク速度	周波数	FEC	変調	DAC レート
1X400GA UI-8	1 トランク、速度 400G	C バンド、196.1 ～ 191.3 THz	oFEC	16 QAM	1x1.5
4X100GA UI-2					
2X100GA UI-2	1 トランク、速度 200G	C バンド、196.1 ～ 191.3 THz	oFEC	QPSK	1x1.5
				QPSK	1
100 G	1 トランク、速度 100G	C バンド、196.1 ～ 191.3 THz	oFEC	QPSK	1x1.5

トラフィック構成パラメータ

次の表に、サポートされているさまざまなトラフィック構成を示します。

TXP/MXP	クライアント（Client）	トランク	変調	FEC	DAC レート
400G-TXP	1 クライアント、速度 400G	1 トランク、速度 400G	16 QAM	oFEC	1x1、1x1.25、1x1.5 および 1x2
400G-TXP	1 クライアント、速度 400G	1 トランク、速度 400G	16 QAM	cFEC	1x1、および 1x1.5
4x100G- MXP	4 クライアント、速度 100G	1 トランク、速度 400G	16 QAM	oFEC	1x1、1x1.25、1x1.5、および 1x2
4x100G- MXP	4 クライアント、速度 100G	1 トランク、速度 400G	16 QAM	cFEC	1x1、および 1x1.5
2x100G-MXP	2 クライアント、速度 100G	1 トランク、速度 200G	QPSK	oFEC	1x1、および 1x1.5
			8 QAM		1x1.25
			16 QAM		1x1.25
1x100G-MXP	1 クライアント、速度 100G	1 トランク、速度 100G	QPSK	oFEC	1x1.5

（注）

- ZR は 1x400G トランスポンダのみをサポートします。
- ZR は 1x1 DAC レートのみをサポートします。
- 4x100 および 2x100 マックスポンダを構成するには、ZRP を構成する前にインターフェイス ブレークアウトを実行する必要があります。詳細については、ブレークアウトの設定（499 ページ）の項を参照してください。

400G デジタル コヒーレント光ファイバの注意事項と制約事項

400G デジタル コヒーレント光ファイバには、次の注意事項と制約事項があります。

- Cisco NX-OS リリース 10.4(1)F 以降、400G デジタル コヒーレント光ファイバ（DCO）サポートは、Cisco Nexus 9300-GX2 および 9408 プラットフォーム スイッチで提供されます。
- Cisco NX-OS リリース 10.4(2)F 以降、QDD-400G-ZR-S および QDD-400G-ZRP-S 光ファイバ サポートは、次のスイッチおよびライン カードで提供されます。
  - Cisco Nexus 93600CD-GX、9316D-GX スイッチ、および X9716D-GX ライン カードを搭載した Cisco Nexus 9508/9504 スイッチ。
  - Cisco Nexus X98900CD-A and X9836DM-A ライン カードを搭載した Cisco Nexus 9804/9808 スイッチ。
- 1x100G トランスポンダおよび 2x100G マックスポンダ モードは、Cisco Nexus 93600CD-GX、9316D-GX スイッチ、および Cisco Nexus X98900CD-A および X9836DM-A ライン カードではサポートされません。
- QDD-400G-ZR-S 光ファイバは、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せん。
- QDD-400G-ZRP-S 光ファイバは、インターフェイスのブレークアウトをサポートします。ZRP 光ファイバでは、複数のブレークアウト マップがサポートされています。
- 2x100 ブレークアウト インターフェイスには、ブレークアウト マップ **100g-2x-pam4** オプションを使用します。
- システムの安定性と効率を向上させるために、DCO の頻繁な挿入と取り外しを避けることをお勧めします。OIR の場合、バックツーバック トランシーバの挿入と取り外しの間に少なくとも 1 分間待つ必要があります。
- ZR/ZRP モジュールの光ファイバの最大リンクアップ時間は最大 180 秒です。

- 電力制限のために影響を受けたコヒーレント光ファイバ ポートまたは MACsec ポートを回復するには、アクティブな ZR/ZRP ポートをディセーブルにするか、既存の MACsec セッションを構成解除して、影響を受けるポートをフラップする必要があります。

（注） N9K-C9332D-H2R スイッチには、MACSec セッションの数に制限はありません。

- 一部のプラットフォームでは、ハードウェアの電力制限があり、多数の 400Gig-ZR/ZRP トランシーバと MACsec 構成を同時に使用することが制限されています。
- Cisco NX-OS リリース 10.4(2)F 以降、2X100 マックスポンダは 8QAM および 16QAM 変調をサポートします。
- Cisco NX-OS リリース 10.4(3)F 以降では、Cisco Nexus C93400LD-H1 および N9K-C9332D-H2R スイッチで次のトランシーバがサポートされています。
  - QDD-400G-ZRP-S
  - QDD-400G-ZR-S

（注） N9K-C93400LD-H1、QDD-400G-ZRP-S、および QDD-400G-ZR-S トランシーバは、奇数番号または偶数番号のポートに挿入できます。ただし、N9K-C9332D-H2R スイッチでは、QDD-400G-ZRP-S および QDD-400G-ZR-S トランシーバは奇数番号のポートにのみ挿入する必要があります。これらのトランシーバを偶数番号のポートに挿入すると、ハードウェアの熱制限により、ポートがエラー状態になります。

- Cisco NX-OS リリース 10.4(3)F 以降、これらの追加のコマンドが導入されました。
  - **zr-Optics frequency** コマンドを使用すると、Cisco Nexus 9000 スイッチの ZR 光モジュールの周波数を設定して、DWDM システムで最適なパフォーマンスを実現できます。
  - **tunnel auto-squelch** コマンドは、光トランシーバのスケルチ機能を制御することで、信号整合性を自動的に管理するのに役立ちます。
  - **transceiver loopback** コマンドでは、Cisco デバイスの光トランシーバでループバック モードを構成できます。
  - **transceiver performance-monitoring** は、Cisco デバイスの光トランシーバのパフォーマンス モニタリングを可能にします。
  - **transceiver alarms** コマンドを使用すると、Cisco デバイスの光トランシーバでアラームを構成できます

- Cisco NX-OS リリース 10.2（2）F以降、**transceiver auto-squelch** コマンドは、光トランシーバのスケルチ機能を制御することで、信号整合性を自動的に管理するのに役立ちます。
- Cisco NX-OS リリース 10.2（2）F以降では、 **show interface** *interface* **transceiver details** コマンドの出力には、400G デジタルコヒーレント光ファイバのファームウェアのメジャーバージョンとマイナーバージョンに関する詳細も含まれます。
- Cisco NX-OS リリース 10.6(1)F 以降、パフォーマンス モニタリング データを使用した TPMON は、次の Cisco Nexus プラットフォームでサポートされています。
  - N9K-C9348D-GX2A
  - N9K-C9364D-GX2A
  - N9K-C9332D-GX2B
  - N9K-C9408
  - N9K-C93600CD-GX
  - N9K-C9316D-GX
  - N9K-C9804、N9K-C9808

  パフォーマンス モニタリング データは、次の光ファイバ/トランシーバ タイプでのみサポートされます。
  - QSFP-DD-400G-ZR-S
  - QSFP-DD-400G-ZRP-S
  - DP04QSDD-HE0

  - パフォーマンスモニタリングは任意のインターフェイスでイネーブルにできますが、履歴データは、上記の光ファイバ/トランシーバの場合にのみ収集されます。
  - パフォーマンス データでは、30 秒、15 分、および 24 時間の固定バケット間隔のみがサポートされます。ユーザー構成可能な間隔はサポートされていません。
  - TPMON は、33 の 30 秒間隔、33 の 15 分の間隔、2 つの 24 時間の間隔のパフォーマンス データを保持します。
  - すべてのパフォーマンスモニタリングデータは、TPMON プロセスの再起動時またはスイッチのリロード時に失われます。設定のみがこれらのイベント後に保持されます。
  - 間隔を指定せずに **clear counters interface transceiver performance-monitoring history** コマンドを使用して、30 秒、15 分、および 24 時間のバケットのすべての履歴データを同時にクリアできます。

- **DP04QSDD-HE0 の場合**

- リリース 10.4(3)F 以降、DP04QSDD-HE0 は、GX/GX2 プラットフォームおよび X98900CD-A および X9836DM-A ライン カードの 1x400 および 1x100 mux ポンダー モードでのみ、次の DAC レートでサポートされます。
  - dac_rate 1x1_50（CFEC あり）
  - dac_rates 1x1_25 および OFEC モードの 1x1_50
- 光学系の最大リンクアップ時間は最大 240 秒です。
- Cisco NX-OS リリース 10.5(1)F 以降、DP04QSDD-HE0(Bright-ZR) は、GX/GX2 プラットフォームおよび X98900CD-A および X9836DM-A ライン カード上の 4x100 および 2x100 mux ポンダー モードでサポートされます。

- 制約事項の概要は次のとおりです。
  - **Cisco Nexus 9364D-GX2A の場合**：
    - システムに 9 つ以上の MACsec セッションが構成されていて、ZR/ZRP トランシーバが存在しない場合、ZR/ZRP トランシーバを挿入すると対応するポートが無効になります。ZR/ZRP トランシーバが存在しない場合、許可される MACsec セッションの最大数は 16 です。
    - システムにアクティブ状態の ZR/ZRP トランシーバが 9 つ以上あり、MACsec セッションが存在しない場合、新しい MACsec セッションの起動は失敗します。MACsec セッションがシステムに存在しない場合、アクティブな ZR/ZRP トランシーバの最大数は 13 です。14 番目の ZR/ZRP トランシーバを挿入すると、対応するポートが無効になります。
    - MACsec セッションとアクティブな ZR/ZRP トランシーバの両方が共存する場合、合計の制限は MACsec セッションが最大 8 つ、ZR/ZRP トランシーバが最大 8 つです。9 番目の MACsec セッションを構成するか、9 番目のアクティブ ZR/ZRP を追加すると、対応するポートが無効になります。
    - ZR/ZRP トランシーバは、このプラットフォームの奇数番号の前面ポートでのみサポートされます。偶数番号の前面ポートに ZR/ZRP トランシーバを挿入すると、ポートはエラー状態になります。
  - **Cisco Nexus 9332D-GX2B の場合**：
    - システムに 5 つ以上の MACsec セッションが構成されていて、アクティブな ZR/ZRP トランシーバが存在しない場合、ZR/ZRP トランシーバを追加すると対応するポートが無効になります。アクティブな ZR/ZRP トランシーバが存在しない場合、許可される MACsec セッションの最大数は 8 です。9 番目の MACsec セッションを設定すると、対応するポートが無効になります。
    - システムに 5 つ以上のアクティブな ZR/ZRP トランシーバが挿入されていて、MACsec セッションが存在しない場合、新しい MACsec セッションの起動は失敗します。システムに MACsec セッションが存在しない場合、アクティブな ZR/ZRP

トランシーバの最大数は 8 です。9 番目の ZR/ZRP トランシーバを挿入すると、対応するポートが無効になります。

- MACsec セッションとアクティブな ZR/ZRP トランシーバの両方が共存する場合、組み合わせでの制限は最大 4 つの MACsec セッションと最大 4 つのアクティブな ZR/ZRP トランシーバです。5 番目の MACsec セッションを構成するか、5 番目の ZR/ZRP を挿入すると、対応するポートが無効になります。
- ZR/ZRP トランシーバは、このプラットフォームの前面ポートのいずれかでサポートされます。

- **Cisco Nexus 9348D-GX2A の場合**：
  - ZR/ZRP トランシーバは、このプラットフォームの次の 24 個の前面ポートでサポートされます。
    - 3、6、9、12、15、18、21、24、27、30、33、36、39、42、45、48、26、29、32、35、38、41、44、47

（注） 上記のリストにない他の前面ポートに ZR/ZRP トランシーバを挿入すると、ポートがエラー状態になります。

- **Cisco Nexus 9408 の場合**：
  - システムは、MACsec 構成が存在するかどうかに関係なく、最大 32 のアクティブな ZR/ZRP トランシーバをサポートできます。
  - ZR/ZRP トランシーバは、Cisco Nexus X9400-8D モジュールでのみサポートされます。

ZR モジュールでの 400G デジタル コヒーレント光ファイバの構成

DAC レート、マックスポンダ モード、変調、および FEC パラメータについて、ZR モジュールのコヒーレント光ファイバを構成できます。

始める前に

DCO の構成時に次の点に注意してください。

- ZR 光ファイバを挿入しないと、コヒーレント光ファイバ構成は機能しません。
- ZRP モジュールで特定の zr 光ファイバを構成すると、コヒーレント構成は機能しません。

- ZR モジュールで特定の zrp 光ファイバを構成すると、コヒーレント構成は機能しません。

手順の概要

1. **configure terminal**
2. **interface ethernet** {*type slot/port*}
3. [**no**] **zr-optics fec** *fec_val* **muxponder** *mxp_val* **modulation** *mod_val* **dac-rate** *dr_val*
4. （任意） **zr-optics cd-min** *cd_min* **cd-max** *cd_max*
5. （任意） **zr-optics transmit-power** *tx_pwr*
6. （任意） **zr-optics dwdm-carrier** [**100MHz-grid frequency** *freq_100mhz_val* | **100GHz-grid frequency** *freq_100ghz_val* | **50GHz-grid** { **frequency** *freq* | **itu-channel** *itu-chan* | **wavelength** *wavelen*}]
7. （任意） [**no**] **zr-optics frequency** *frequency-value*

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface ethernet** {*type slot/port*}
	例：
	`switch(config)# interface ethernet 1/3`
	`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	[**no**] **zr-optics fec** *fec_val* **muxponder** *mxp_val* **modulation** *mod_val* **dac-rate** *dr_val* 例： `switch(config-if)# zr-optics fec cFEC muxponder 1x400 modulation 16QAM dac-rate 1x1`	ZR 光ファイバで次のパラメータを構成します。詳細については、400G デジタル コヒーレント光ファイバパラメータ （486 ページ） セクションを参照してください。 • FEC • マックスポンダ • 変調 • DAC
ステップ 4	（任意） **zr-optics cd-min** *cd_min* **cd-max** *cd_max* 例： `switch(config-if)# zr-optics cd-min -2300 cd-max 2300`	設定された最小値と最大値を使用して、コヒーレント光ファイバの波長分散を構成します。詳細については、400G デジタル コヒーレント光ファイバ パラメータ （486 ページ） 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
		（注） 任意のデータ レートの CD の最大値と最小値を構成する場合は、構成された値の最小差が 1000 ps/nm 以上であることを確認します。
ステップ 5	（任意） **zr-optics transmit-power** *tx_pwr* 例： `switch(config-if)# zr-optics transmit-power -190`	光信号の送信電力を設定します。詳細については、400G デジタル コヒーレント光ファイバ パラメータ（486 ページ）の項を参照してください。 （注） Tx 電力パラメータは、ユーザー構成をハードウェアにプログラムするベスト エフォート構成です。しかし、ZR/ZRP トランシーバ ファームウェアはこれを参照としてのみ使用し、実行時に実際の最適な Tx 電力値を計算します。これはユーザー構成と同じである場合とそうでない場合があります。
ステップ 6	（任意） **zr-optics dwdm-carrier** [**100MHz-grid frequency** *freq_100mhz_val* | **100GHz-grid frequency** *freq_100ghz_val* | **50GHz-grid** { **frequency** *freq* | **itu-channel** *itu-chan* | **wavelength** *wavelen*}] 例： `switch(config-if)# zr-optics dwdm-carrier 100MHz-grid frequency 1913000`	構成された周波数（100MHz グリッド、100GHz グリッド、または 50GHz グリッド）に基づいて周波数を構成します。50GHz グリッドは、追加の ITU チャネルまたは波長パラメータを提供します。詳細については、400G デジタル コヒーレント光ファイバ パラメータ （486 ページ）の項を参照してください。 （注） 周波数が **[50Ghz グリッド波長（50Ghz-grid wavelength）]** または **[50 Ghz グリッド ITU チャネル（50Ghz-grid itu-channel）]** オプションを使用して構成されている場合、システムは特定の波長または ITU チャネルの周波数を計算し、それを使用してハードウェアをプログラムします。
ステップ 7	（任意） [**no**] **zr-optics frequency** *frequency-value* 例： `switch(config-if)# zr-optics frequency 193500.0`	DWDM グリッド要件に合わせて、ZR 光モジュールの動作周波数を GHz 単位で構成します。 頻度の構成を無効にするには、 **no** 形式を使用します。

ZRP モジュールでの 400G デジタル コヒーレント光ファイバ（DCO）の構成

DAC レート、マックスポンダ モード、変調、および FEC パラメータについて、ZRP モジュールのコヒーレント光ファイバを構成できます。

始める前に

DCO の構成時には、次の点に注意してください。

- ZRP 光ファイバを挿入しないと、コヒーレント光ファイバ構成は機能しません。
- ZRP モジュールで特定の zr 光ファイバを構成すると、コヒーレント構成は機能しません。
- ZR モジュールで特定の zrp 光ファイバを構成すると、コヒーレント構成は機能しません。

手順の概要

1. **configure terminal**
2. **interface ethernet** {*type slot/port*}
3. [**no**] **zrp-optics fec** *fec_val* **muxponder** *mxp_val* **modulation** *mod_val* **dac-rate** *dr_val*
4. （任意） **zrp-optics cd-min** *cd_min* **cd-max** *cd_max*
5. （任意） **zrp-optics transmit-power** *tx_pwr*
6. （任意） **zrp-optics dwdm-carrier** [**100MHz-grid frequency** *freq_100mhz_val* | **100GHz-grid frequency** *freq_100ghz_val* | **50GHz-grid** { **frequency** *freq* | **itu-channel** *itu-chan* | **wavelength** *wavelen*}]

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface ethernet** {*type slot/port*}
	例：
	`switch(config)# interface ethernet 1/3`
	`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	[**no**] **zrp-optics fec** *fec_val* **muxponder** *mxp_val* **modulation** *mod_val* **dac-rate** *dr_val* 例： `switch(config-if)# zrp-optics fec cFEC muxponder 1x400 modulation 16QAM dac-rate 1x1`	ZRP 光ファイバで次のパラメータを構成します。詳細については、400G デジタル コヒーレント光ファイバパラメータ （486ページ）セクションを参照してください。 • FEC • マックスポンダ • 変調 • DAC
ステップ 4	（任意） **zrp-optics cd-min** *cd_min* **cd-max** *cd_max* 例： `switch(config-if)# zrp-optics cd-min -2400 cd-max 2400`	設定された最小値と最大値を使用して、コヒーレント光ファイバの波長分散を構成します。詳細については、400G デジタル コヒーレント光ファイバ パラメータ （486 ページ）の項を参照してください。 （注） 任意のデータ レートの波長分散の最大値と最小値を構成する場合は、構成された値の最小差が 1000 ps/nm 以上であることを確認します。

ステップ 5	（任意） **zrp-optics transmit-power** *tx_pwr*
	例：
	`switch(config-if)# zrp-optics transmit-power -190`
	例：
	`switch(config-if)# zrp-optics transmit-power -13.5`
		光信号の送信電力を設定します。詳細については、400G デジタル コヒーレント光ファイバ パラメータ（486 ページ）の項を参照してください。
		（注）
		Tx 電力パラメータは、ユーザー設定をハードウェアにプログラムするベスト エフォート設定です。しかし、ZR/ZRP トランシーバファームウェアはこれを参照としてのみ使用し、実行時に実際の最適な Tx 電力値を計算します。これはユーザー構成と同じである場合とそうでない場合があります。
		（注）
		`zrp-optics transmit-power` コマンドは、10 進数形式と整数形式の両方の値を受け入れるようになりました。

ステップ 6	（任意） **zrp-optics dwdm-carrier** [**100MHz-grid frequency** *freq_100mhz_val* | **100GHz-grid frequency** *freq_100ghz_val* | **50GHz-grid** { **frequency** *freq* | **itu-channel** *itu-chan* | **wavelength** *wavelen*}] 例： `switch(config-if)# zrp-optics dwdm-carrier 100MHz-grid frequency 1913000`	構成された周波数（100MHz グリッド、100GHz グリッド、または 50GHz グリッド）に基づいて周波数を構成します。50GHz グリッドは、追加の ITU チャネルまたは波長パラメータを提供します。詳細については、400G デジタル コヒーレント光ファイバ パラメータ （486 ページ）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
		（注） 周波数が **[50Ghz グリッド波長（50Ghz-grid wavelength）]** または **[50 Ghz グリッド ITU チャネル（50Ghz-grid itu-channel）]** オプションを使用して構成されている場合、システムは特定の波長または ITU チャネルの周波数を計算し、それを使用してハードウェアをプログラムします。

ブレークアウトの設定

ZRP 光ファイバのインターフェイスでブレークアウトを構成できます。

手順の概要

1. **configure terminal**
2. **interface breakout module** {*slot*} **port** {*port_num*} **map** {*breakoutmap*}
3. **interface ethernet** {*type slot/port/sub-port*}
4. [**no**] **zrp-optics fec** *fec_val* **muxponder** *mxp_val* modulation *mod_val* **dac-rate** *dr_val*
5. （任意） **show running interface ethernet** {*type slot/port*}

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface breakout module** {*slot*} **port** {*port_num*} **map** {*breakoutmap*} 例： switch(config)# **interface breakout module 1 port 3 map 100g-2x-pam4**	インターフェイス ブレークアウトを構成します

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

	コマンドまたはアクション	目的
ステップ 4	[**no**] **zrp-optics fec** *fec_val* **muxponder** *mxp_val* modulation *mod_val* **dac-rate** *dr_val* 例： `switch(config-if)# zrp-optics fec oFEC muxponder 2x100 modulation QPSK dac-rate 1x1`	ブレークアウト インターフェイスで ZRP を構成します。
ステップ 5	（任意） **show running interface ethernet** {*type slot/port*} 例： `switch(config-if)# show running interface ethernet1/3/1`	ブレークアウトインターフェイスに設定されている構成情報を表示します。

トランシーバ自動スケルチの構成

光トランシーバのスケルチ機能を使用すると、信号の整合性を自動的に管理し、望ましくないノイズを防止し、クリーンな信号伝送を確保できます。

この機能は、信号の完全性が重要な高速光ネットワーク環境で使用します。

手順の概要

1. **configure terminal**
2. **interface ethernet** {*type slot/port/sub-port*}
3. [**no**] **transceiver auto-squelch**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**interface ethernet** {*type slot/port/sub-port*}
	例：
	`switch(config)# interface ethernet 1/3/1`
	`switch(config-if)#`
		構成するインターフェイスを指定し、インターフェイス構成モードを開始します。

ステップ 3	[**no**] **transceiver auto-squelch** 例： `switch(config-if)# transceiver auto-squelch`	望ましくないノイズを防ぐために、信号のスケルチングを有効にします。このコマンドは、デフォルトでイネーブルになっています。

	コマンドまたはアクション	目的
		自動スケルチングを無効にするには、 **no** 形式を使用します。

トランシーバー ループバックを構成

ループバック テストを使用して、信号を発信元に再ルーティングすることで、ネットワーク接続とトランシーバ機能を診断およびトラブルシューティングできます。

手順の概要

1. **configure terminal**
2. **interface ethernet** {*type slot/port/sub-port*}
3. [**no**] **transceiver loopback**{**internal** | **line**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**interface ethernet** {*type slot/port/sub-port*}
	例：
	`switch(config)# interface ethernet 1/3/1`
	`switch(config-if)#`
		構成するインターフェイスを指定して、インターフェイス構成モードを入力します。

ステップ 3	[**no**] **transceiver loopback**{**internal**	**line**
		例：
		`switch(config-if)# transceiver loopback internal`
		`switch(config-if)# transceiver loopback line`
		`switch(config-if)# no transceiver loopback`
			トランシーバループバックを有効にします。このコマンドは、デフォルトで無効になっています。
			• **[内部（Internal）]**：内部ループバックを構成して、外部信号なしでトランシーバの内部機能を検証します。
			• **[回線（Line）]**：送信された信号をレシーバにルーティングするように回線ループバックを構成します。このモードでは、伝送パス全体をテストし、信号または接続のエラーをチェックします。

	コマンドまたはアクション	目的
		トランシーバループバックを無効にするには、 **no** 形式を使用します。 （注） サービスを中断することなくループバック テストをサポートするようにネットワーク環境が構成されていることを確認します。

トランシーバ パフォーマンス モニタリングの構成

重要なメトリックを収集して分析することで、最適なパフォーマンスを確保し、潜在的な問題を迅速に検出できます。

手順の概要

1. **configure terminal**
2. **interface ethernet** {*type slot/port/sub-port*}
3. [**no**] **transceiver performance-monitoring**
4. （任意） **show interface ethernet** {*type slot/port*}**performance-monitoring**
5. （任意） **show interface ethernet** {*type slot/port*} **transceiver performance-monitoring history** *bucket_interval* {**fec** | **optics**} **interval** *interval_value*

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**interface ethernet** {*type slot/port/sub-port*}
	例：
	`switch(config)# interface ethernet 1/25`
	`switch(config-if)#`
		構成するインターフェイスを指定し、インターフェイス構成モードを開始します。

ステップ 3	[**no**] **transceiver performance-monitoring** 例： `switch(config-if)# transceiver performance-monitoring`	パフォーマンス モニタリングを構成して、パフォーマンスをモニターおよび最適化します。 • [リアルタイムモニタリング（Real-Time Monitoring）]：光パワーレベル、分散、ビット

	コマンドまたはアクション	目的
		エラー レートなどのトランシーバ メトリックを観察できます。 • 障害検出：トランシーバの問題をプロアクティブに特定して対処し、ネットワークの中断を防ぐことができます。 • [パフォーマンスの最適化（Performance Optimization）]：指定されたパラメータ内で動作するようにトランシーバをモニターして、ネットワークの効率を維持できます。 トランシーバ パフォーマンス モニタリングを無効にするには、 **no** 形式を使用します。

ステップ 4	（任意） **show interface ethernet** {*type slot/port*}**performance-monitoring**
	例：
	`switch(config-if)# show interface ethernet 1/25 transceiver performance-monitoring current 30-sec`
	`Interface Ethernet1/25`
		トランシーバ パフォーマンス モニタリング情報を表示します。

ステップ 5	（任意） **show interface ethernet** {*type slot/port*} **transceiver performance-monitoring history** *bucket_interval* {**fec** | **optics**} **interval** *interval_value* 例： `switch# show interface ethernet 1/25 transceiver performance-monitoring history 15-min fec interval 5`	指定したインターフェイスの履歴パフォーマンス モニターリング データ、バケット間隔、データ レイヤ、および間隔値を表示します。 • **eth_interface** はクエリされるイーサネット インターフェイスを指定します。 • **bucket_interval** はデータバケットの時間間隔（30 秒、15 分、または 24 時間）を示します。 • **fec** または **optics** は FEC データ レイヤと光データ レイヤを選択します。 • **interval_value** は表示する特定の履歴間隔を指定します。 （注） この CLI は、Cisco NX-OS リリース 10.6(1)F 以降でサポートされます。

例

トランシーバ パフォーマンス モニタリング情報の確認

```
switch(config-if)# show interface ethernet 1/25 transceiver performance-monitoring current
 30-sec
```

```
Interface Ethernet1/25
--------------------------

Optics in the current interval [21:32:49 Wed Nov 20 2024 - 21:33:00 Wed Nov 20 2024]

Parameter          MIN         AVG         MAX
-----------------------------------------------
CD(Short)[ps/nm]  0.00        0.00        0.00
DGD[ps]           0.47        0.55        0.63
RX PWR[dBm]       -9.56       -9.55       -9.54
TX PWR[dBm]       -10.00      -9.99       -9.99
OSNR[dB]          28.10       28.10       28.10
RX CHAN PWR[dBm]  -9.25       -9.24       -9.22
ESNR[dB]          16.60       16.60       16.60
LASER BIAS[mA]    201.00      201.00      201.00
FREQ OFF[Mhz]     -314.00     -303.00     -294.00
SOP RATE[krad/s]  4.00        4.00        4.00
PDL[dB]           0.50        0.50        0.50
SOPMD[ps^2]       1.60        1.79        2.17

FEC in the current interval [21:32:49 Wed Nov 20 2024 - 21:33:00 Wed Nov 20 2024]

EC BITS  : 0
UC WORDS : 0

Parameter          MIN        AVG        MAX
-------------------------------------------
PREFEC BER         9.32e-04   9.38e-04   9.43e-04
POSTFEC BER        0.00e+00   0.00e+00   0.00e+00
Q FACTOR[dB]       9.80       9.86       9.89
Q MARGIN[dB]       2.80       2.80       2.80
```

トランシーバ パフォーマンス モニタリング情報のクリア

インターフェイスの 30 秒間隔カウンタをクリアするには

```
clear counters interface ethernet <> transceiver performance-monitoring current 30-sec
```

インターフェイスの 15 分間隔カウンタをクリアするには

```
clear counters interface ethernet <> transceiver performance-monitoring current 15-min
```

インターフェイスの 24 時間間隔カウンタをクリアするには

```
clear counters interface ethernet <> transceiver performance-monitoring current 24-hour
```

すべてのインターフェイス上で 30 秒間隔カウンタをクリアするには

```
clear counters interface transceiver performance-monitoring current 30-sec
```

すべてのインターフェイス上の 15 分間隔カウンタをクリアするには

```
clear counters interface transceiver performance-monitoring current 15-min
```

すべてのインターフェイスで 24 時間間隔カウンタをクリアするには

```
clear counters interface transceiver performance-monitoring current 24-hour
```

履歴トランシーバ パフォーマンス モニタリング データのクリアするには

特定のインターフェイスのすべての履歴パフォーマンス モニターリング データ（30 秒、15 分、および 24 時間のバケット）をクリアするには：

```
clear counters interface ethernet <> transceiver performance-monitoring history
```

すべてのインターフェイス上でパフォーマンス モニターリング履歴データをすべてクリアするには、次の手順を実行します。

```
clear counters interface transceiver performance-monitoring history
```

オプションで、1 つのタイプのバケット（30 秒、15 分、または 24 時間）のみをクリアする場合は、特定の間隔を指定できます。

```
clear counters interface ethernet <> transceiver performance-monitoring history 30-sec
```

トランシーバ アラームの構成

キー パフォーマンス パラメータのしきい値を設定して、しきい値が事前定義されたしきい値を超えたときにアラームをトリガーします。

手順

ステップ 1 **configure terminal** コマンドを使用して、グローバル コンフィギュレーション モードを開始します。

例：

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

ステップ 2 インターフェイスを指定して、インターフェイス構成モードを開始する **interface ethernet***type slot/port/sub-port* を使用します。

例：

```
switch(config)# interface ethernet 1/21/1
switch(config-if)#
```

ステップ 3 [**no**] **transceiver alarms cd** | **dgd** | **lbc** | **osnr** | **prefec-ber** | **laser-temperature** | **temperature** | **voltage** | **rx-power** { **high-threshold** | **low-threshold***threshold-value* }を使用してトランシーバアラームのしきい値を設定します。

例：

```
switch(config)# interface ethernet 1/21
switch(config-if)# transceiver alarms cd high-threshld 300000
switch(config-if)# transceiver alarms dgd high-threshold 100
switch(config-if)# transceiver alarms esnr high-threshold 25
switch(config-if)# transceiver alarms laser-temperature low-threshold 51.67
switch(config-if)# transceiver alarms laser-temperature high-threshold 40.21
switch(config-if)# transceiver alarms temperature low-threshold 79.00
switch(config-if)# transceiver alarms temperature high-threshold 1.00
switch(config-if)# transceiver alarms voltage low-threshold 6.90
switch(config-if)# transceiver alarms voltage high-threshold 2.67
switch(config-if)# transceiver alarms rx-power low-threshold 46.00
switch(config-if)# transceiver alarms rx-power high-threshold -41.23
```

アラームをトリガーするために重要なメトリックをモニターするためのしきい値を設定します。

- **cd**：波長分散の上限しきい値と下限しきい値を設定します。

- **dgd**：グループ遅延差の高しきい値と低しきい値を設定します。
- **ensr**：電気信号対雑音比の高しきい値と低しきい値を設定します。
- **lbc**：レーザー バイアス電流のパラメータの上限しきい値と下限しきい値を設定します。
- **onsr**：光信号対雑音比の低しきい値を設定します。
- **prefec-ber**：前方誤り訂正ビット エラー レートの上限しきい値と下限しきい値を設定します。
- **laser-temperature**：レーザー温度の上限と下限のしきい値を設定します。
- **voltage**：上限と下限のしきい値の電圧を設定します。
- **rx-power**：順方向 rx 電力の上限と下限のしきい値を設定します。

トランシーバ アラームを無効にするには、 **no** 形式を使用します。

（注）
ネットワーク設計およびパフォーマンス要件のしきい値を決定します。しきい値を定期的に確認して調整し、ネットワークの状態と目的に合わせます。

ステップ 4 （任意） **show running-config interface ethernet** コマンドを使用してトランシーバ アラームを表示します。

例：

```
switch(config)# show running-config interface ethernet 1/21
!Command: show running-config interface Ethernet1/21
!No configuration change since last restart
!Time: Mon Mar 24 21:57:21 2025
.
.!
interface Ethernet1/1
  transceiver alarms laser-temperature low-threshold 51.67
  transceiver alarms laser-temperature high-threshold 40.21
  transceiver alarms temperature low-threshold 79.00
  transceiver alarms temperature high-threshold 1.00
  transceiver alarms voltage low-threshold 6.90
  transceiver alarms voltage high-threshold 2.67
  transceiver alarms rx-power low-threshold 46.00
  transceiver alarms rx-power high-threshold -41.23
  no shutdown
```

トランシーバ アラームの表示

```
switch# show interface ethernet 1/21 transceiver alarms
 Interface Ethernet1/21
Current System Time: 08:54:38 Wed Apr 23 2025
Current State       Occurrences         Last Trigger                 Last Reset
-------------       -----------         ------------                 ----------
DEFAULT TRANSCEIVER ALARMS:
---------------------------
.
.
.
CONFIGURATION ALARMS:
---------------------
```

```
FEC Alarms:
  Pre Fec BER low alarm        ok           0                      never
       never
  Pre Fec BER high alarm       ok           0                      never
       never

Optics Alarms:
  CD low alarm                 ok           0                      never
       never
  CD high alarm                ok           0                      never
       never
  DGD high alarm               ok           0                      never
       never
  LBC low alarm                ok           0                      never
       never
  LBC high alarm               ok           0                      never
       never
  OSNR low alarm               ok           0                      never
       never
  ESNR low alarm               ok           0                      never
       never
  ESNR high alarm           ok           0                      never
    never
  Temperature low alarm     ok           0                      never
    never
  Temperature high alarm   activated     1       01:09:27 Apr 21 2025
    never
  Voltage low alarm        activated     1       19:07:39 Apr 21 2025
    never
  Voltage high alarm         ok           0                      never
     never
  Rx Power low alarm         ok           0                      never
    never
  Rx Power high alarm        ok           0                      never
    never
  Laser temperature low alarm  ok           0                      never
       never
  Laser temperature high alarm ok           0                      never
       never
```

トランシーバ アラーム情報のクリア

インターフェイスのアラームをクリアするには、**clear counters interface ethernet transceiver alarms** コマンドを使用します。

```
clear counters interface ethernet 1/21 transceiver alarms
```

すべてのインターフェイスでアラームをクリアするには、 **clear counters interface transceiver alarms** コマンドを使用します。

```
clear counters interface transceiver alarms
```

400G デジタル コヒーレント光ファイバの確認

400G デジタル コヒーレント光ファイバ構成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 running interface ethernet {*type slot/port*}	コヒーレント ZR/ZRP 光ファイバを検証するように設定されたインターフェイスの実行コンフィギュレーション情報を表示します。
show interface ethernet {*type slot/port*} **transceiver details**	インターフェイスのコヒーレント ZR/ZRP 光ファイバ構成情報を表示します。

400G コヒーレント光ファイバの構成例

次に、ZR/ZRP 光ファイバを使用した実行構成の例を示します。

```
switch(config-if)# show running  interface ethernet1/3

!Command: show running-config interface Ethernet1/3
!Running configuration last done at: Mon Aug 28 12:16:40 2023
!Time: Mon Aug 17 12:17:40 2023

version 10.3(2) Bios:version 01.10

interface Ethernet1/3
  zr-optics fec cFEC muxponder 1x400 modulation 16QAM dac-rate 1x1
  zr-optics cd-min -2400 cd-max 2400
  zr-optics transmit-power -190
  zr-optics dwdm-carrier 100MHz-grid frequency 1931000
  no shutdown
```

次に、コヒーレント構成を確認する例を示します。

10.5(3)F から：

```
switch# show interface ethernet1/3 transceiver details
Ethernet1/3
    transceiver is present
    type is QSFP-DD-400G-ZR-S
    name is CISCO-ACACIA
    part number is DP04QSDD-E20-190
    revision is A
    serial number is ACA254700F0
    nominal bitrate is 425000 MBit/sec per channel
    cisco id is 0x18
    cisco extended id number is 21
    cisco part number is 10-3495-01
    cisco product id is QDD-400G-ZR-S
    cisco version id is V01
    firmware version is 61.10
    Link length SMF is 12 km
    Nominal transmitter wavelength is 1547.70 nm
    Wavelength tolerance is 166.550 nm
    host lane count is 8
    media lane count is 1
    max module temperature is 80 deg C
    min module temperature is 0 deg C
    min operational voltage is 3.12 V
    vendor OUI is 0x7cb25c
    date code is 211125
    clei code is INUIANYEAA
```

```
    power class is 8 (>14 W maximum)
    max power is 20.00 W
    near-end lanes used none
    far-end lane code for 8 lanes Undefined
    media interface is unknown value 0x10
    Advertising code is Optical Interfaces: SMF
    Host electrical interface code is 400GAUI-8 C2M (Annex 120E)

Optics Status:
 FEC State: cFEC
 DWDM carrier Info: Frequency: 0.0000 THz
 Wavelength: inf nm
 DAC Rate: 1x1
 Configured Tx Power: -7.00 dBm
 Modulation Type: 16QAM
 Muxponder Type: 1x400
 Configured CD-MIN: -2400 ps/nm CD-MAX: 2400 ps/nm
 Transceiver Squelch Status: Enable
 Laser Admin State: Off
 Laser Oper State: Off
 Loopback Mode: Disabled

Vendor Details:
 Optics Type: QSFP-DD-400G-ZR-S
 Firmware Version: Major.Minor.Build
     Active : 61.20.13
     Inactive: 61.20.13
Lane Number:1 Network Lane
  ------------------------------------------------------------------------------
                Current              Alarms                  Warnings
                Measurement     High        Low         High          Low
  ------------------------------------------------------------------------------
  Temperature   36.00 C        80.00 C     -5.00 C     75.00 C       15.00 C
  Voltage        3.36 V         3.46 V      3.13 V      3.43 V        3.16 V
  Current           N/A            N/A         N/A         N/A           N/A
  Tx Power          N/A         0.00 dBm  -18.23 dBm   -2.00 dBm    -16.02 dBm
  Rx Power          N/A         1.99 dBm  -23.01 dBm    0.00 dBm    -20.00 dBm
  Transmit Fault Count = 0
  ------------------------------------------------------------------------------
  Note: ++  high-alarm; +  high-warning; --  low-alarm; -  low-warning
```

10.5(2)F まで：

```
switch# show int e1/3 transceiver details
Ethernet1/3
    transceiver is present
    type is QSFP-DD-400G-ZR-S
    name is CISCO-ACACIA
    part number is DP04QSDD-E20-190
    revision is A
    serial number is ACA2524000V
    nominal bitrate is 425000 MBit/sec per channel
    cisco id is 24
    cisco extended id number is 21
    cisco part number is 10-3495-01
    cisco product id is QDD-400G-ZR-S
    cisco version id is V01
    firmware version is 61.22
    Link length SMF is 12 km
    Nominal transmitter wavelength is 1547.70 nm
    Wavelength tolerance is 166.550 nm
    host lane count is 8
    media lane count is 1
    max module temperature is 80 deg C
    min module temperature is 0 deg C
```

```
    min operational voltage is 3.12 V
    vendor OUI is 0x7cb25c
    date code is 210614
    clei code is INUIANYEAA
    power class is 8 (>14 W maximum)
    max power is 20.00 W
    near-end lanes used none
    far-end lane code for 8 lanes Undefined
    media interface is C-band tunable laser
    Advertising code is Optical Interfaces: SMF
    Host electrical interface code is 400GAUI-8 C2M (Annex 120E)

    Optics Status:
        FEC State: cFEC
        DWDM carrier Info: Frequency: 193.1000 THz
                           Wavelength: 1552.524 nm
        DAC Rate: 1x1
        Configured Tx Power: -10.00 dBm
        Modulation Type: 16QAM
        Muxponder Type: 1x400
        Configured CD-MIN: -2400 ps/nm     CD-MAX: 2400 ps/nm
        Transceiver Squelch Status: Enable
        Laser Admin State: On
        Laser Oper State: On
        Loopback Mode: Disabled

    Vendor Details:
        Optics Type: QSFP-DD-400G-ZR-S
        Firmware Version: Major.Minor.Build
                Active  : 61.22.21
                Inactive: 61.10.12
Lane Number:1 Network Lane
  ------------------------------------------------------------------------------------
                     Current                        Alarms                  Warnings
                     Measurement             High        Low         High          Low
  ------------------------------------------------------------------------------------
  Temperature          46.00 C             80.00 C      -5.00 C      75.00 C      15.00
 C
  Voltage               3.26 V              3.46 V       3.13 V       3.43 V       3.16
 V
  Current                N/A                N/A          N/A          N/A          N/A

  Tx Power            -10.00 dBm           0.00 dBm   -18.23 dBm    -2.00 dBm   -16.02
 dBm
  Rx Power             -9.70 dBm           7.99 dBm   -23.01 dBm     7.99 dBm   -21.54
 dBm
  Laser temperature    47.13 C              N/A          N/A          N/A          N/A

  RX Channel Power     -9.57 dbm           3.00 dbm   -23.50 dbm     0.00 dbm   -20.00
 dbm
  Pre-FEC BER        8.13e-04               N/A          N/A          N/A          N/A

  Post-FEC BER       0.00e+00               N/A          N/A          N/A          N/A

  CD (Short Link)       0.00 ps/nm          N/A          N/A          N/A          N/A

  CD (Long Link)        0.00 ps/nm          N/A          N/A          N/A          N/A

  Diff. group delay     3.00 ps             N/A          N/A          N/A          N/A

  SOPMD                33.00 ps^2           N/A          N/A          N/A          N/A

  PDL                   0.50 dB             N/A          N/A          N/A          N/A
```

```
  OSNR                  36.40 dB              N/A          N/A          N/A          N/A
  ESNR                  18.00 dB              N/A          N/A          N/A          N/A
  Carrier freq off    -391.00 MHz             N/A          N/A          N/A          N/A
  SOP Rate of Chg       0.00 krad/s           N/A          N/A          N/A          N/A
  Laser bias          210.00 mA               N/A          N/A          N/A          N/A
  RX Q factor           9.89 dB               N/A          N/A          N/A          N/A
  RX Q margin           2.70 dB               N/A          N/A          N/A          N/A
  SOPMD LO GR          33.00 ps^2             N/A          N/A          N/A          N/A
  Tx modulator bias    34.93 %                N/A          N/A          N/A          N/A
  Transmit Fault Count = 0
  ------------------------------------------------------------------------------
  Note: ++  high-alarm; +  high-warning; --  low-alarm; -  low-warning
```

次の例は、ブレークアウトインターフェイスでブレークアウト構成を構成する方法を示しています。

```
switch(config)# interface ethernet 1/3/1
switch(config-if)# zrp-optics fec ofec muxponder 2x100 modulation QPSK dac-rate 1x1

switch (config-if)# show running interface ethernet1/3/1


interface Ethernet1/3/1
  zrp-optics fec oFEC muxponder 2x100 modulation QPSK dac-rate 1x1
  zrp-optics cd-min -50000 cd-max 50000
  zrp-optics transmit-power -190
  zrp-optics dwdm-carrier 100MHz-grid frequency 1913000
  no shutdown
```

ZR 光ファイバのファームウェアのアップグレード

このタスクを活用、N9K-C9332D-H2R の ZR 光ファイバのファームウェアをアップグレードします。

始める前に

ファームウェア アップグレードのガイドラインをお読みください。

- 一度に 1 つのインターフェイスでファームウェアのダウンロードとアクティブ化を実行し、信頼性の高いの高い集中的なアップグレード プロセスを確保します。
- アップグレードプロセス中のインターフェイス構成の変更を一時停止して、スムーズなエクスペリエンスを確保します。

  リンクの安定性に影響を与える可能性のあるピア ポートでの操作は、慎重に行ってください。これにより、意図しない動作を防ぎ、アップグレード中の不要なポート再プログラミングを回避できます。

- の機能（DOM フェッチなど）に影響を与える可能性があるため、ファームウェアのダウングレードは避けてください。

  をダウングレード必要がある場合は、トランシーバを手動で再度装着するか、システムのリロードを実行して回復を支援してください。

手順

ステップ 1 **install transceiver interface ethernet***interface***download** コマンドを使用して、トランシーバにファームウェアをインストールします。

例：

```
Switch# install transceiver interface ethernet 1/31 download
bootflash:560-0101-37_Rev_71_110_25_gl2qsdd.ackit
Transceiver firmware download started
Switch#

2025 Apr 20 20:38:53 Switch %USER-SLOT1-2-SYSTEM_MSG: Firmware Download for transceiver on interface
 eth1/31 is completed, proceed with activation process.
```

show install transceiver コマンドを使用して、トランシーバのダウンロードステータスを確認します。

```
Switch# show install transceiver interface ethernet 1/1 status

Downloading is in progress [45/100 Completed]
```

ステップ 2 **install transceiver interface ethernet***interface***activate** | **disruptive** コマンドを使用して、トランシーバでファームウェアのインストールをアクティブ化します。

ファームウェアをスイッチにインストールします。

- **activate**：ファームウェアのインストールをアクティブ化。
- **disruptive**：中断を伴うファームウェアのインストールをアクティブ化。

例：

```
Switch# install transceiver interface ethernet 1/31 activate
Firmware activation is started
Switch#

2025 Apr 20 20:40:10 Switch %USER-SLOT1-2-SYSTEM_MSG: Firmware Activation for transceiver on interface
 eth1/31 is completed.
```

ステップ 3 **show install transceiver interface ethernet***interface***info** | **status** を使用して、トランシーバのファームウェアのバージョンとステータスを確認します。

例：

```
Switch# show install transceiver interface ethernet 1/31 info
Firmware Version:
Active : 71.110.25
Passive : 71.120.8
Switch#

Switch# show install transceiver interface ethernet 1/31 status
```

```
No transceiver firmware upgrade is in process.
Switch#
```

光回線システムの概要：QSFP-DD のプラガブル サポート

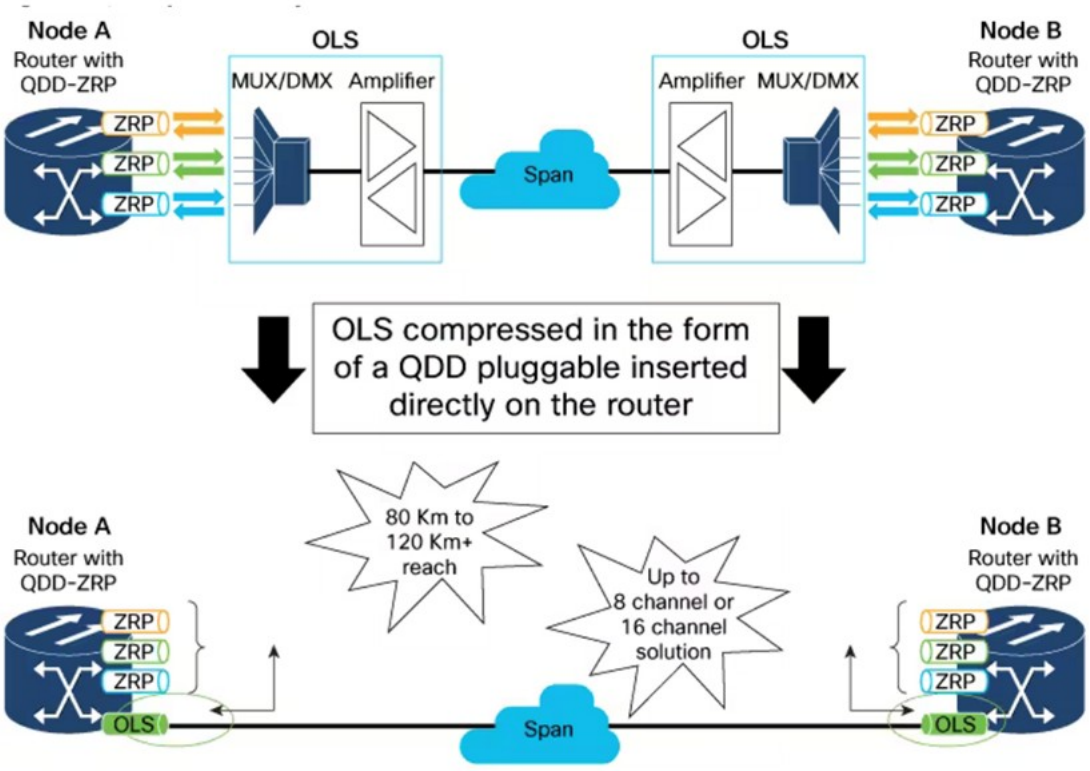
QDD 光回線システム（OLS）は、限られた数のコヒーレント光チャネルでトラフィックおよび

- シングル スパンのポイントツーポイント リンクとして送信する場合
- の2 台のルータまたはスイッチ間の接続を可能にするプラガブル光増幅器です。

OLS は、追加の光ハードウェアユニットなしで 8 または 16 の光チャネルを転送するのに役立ちます。

OLS トポロジは次のように表示されます：

図 *39 : OLS* トポロジ



メリット

ルータまたはスイッチのポートに接続されたQSFP-DDモジュールには、増幅機能があります。OLS を使用する利点は次のとおりです。

- 増幅用のコンパクトなソリューションを提供し、
- 拡張されたリーチを提供し、
- ファイバ帯域幅の増加、および
- 消費電力を低減します。

シスコが提供するコヒーレント オプティクスの ZR および ZR Plus バリアントの QSFP-DD OLS のプラガブル形式のソリューションは、

- 機器、ラックスペース、電力の削減、
- 外部アンプやマルチプレクサの使用を避け、
- 光ファイバ仕様、チャネル数、および信号のラインレートに応じて、400G QSFP-DD ZR または、ZR プラス リンクの到達距離を 40 km から 130 km 以上に拡張、および
- 光ファイバ仕様、チャネル数、および信号のラインレートに応じて、400G Bright QSFP-DD ZR または、ZR + リンクの到達距離を 80 km から 130 km 以上に拡張することに役立ちます。

サポートされるプラットフォーム

- Cisco Nexus 9300 シリーズ スイッチ
  - N9K-C9364D-GX2A
  - N9K-C9332D-GX2B
  - N9K-C9348D-GX2A
- Cisco Nexus 9400 シリーズ スイッチ（N9K-X9400-8D LEM 搭載 N9K-C9408）

注意事項と制約事項

OLS 動作モードの注意事項

次に、OLS 動作モードの設定に関するガイドラインを示します。

- OLS 構成をアクティブにして適用するには、インターフェイスで **no shutdown** コマンドを使用します。

- 自動電力制御モードでは、入力信号強度に関係なく、増幅器の出力電力が一定に保たれます。
- 手動制御モードでは、利得値はピア OLS の RX と送信 OLS の TX の間の損失に基づいて決まります。リンク損失を活用 COM および回線側で適切なゲインを構成し、重要なアプリケーションで高い信号対雑音比率を実現します。

  利得値は、ピア OLS の RX と送信 OLS の TX 間の損失に基づいて決まります。2 つの OLS（ols A と ols B）間のリンク損失は A -> B で、ols A の tx_power から ols B の rx_power を引いたものです。損失は、ols B の利得によって補正されます。

  たとえば、リンク損失が 10db で、ols-A の tx power が 0db の場合、ols B の rx_power は 0 -10 で、-10dbm になります。この 10dbm の利得を、COM（受信）側で補正するために ols B に適用します。

光安全リモート インターロック（OSRI）の注意事項

OSRI が有効になっている場合、最大出力電力は入力電力に基づいて -15dBm になります。

OLS 安全制御モード

- 安全制御モードは、回線側でのみ有効になります。
- 安全制御モードが有効で、回線 RX で LOS が検出された場合。回線 TX は、信号出力電力を 8 dBm に正規化し、回線増幅器を自動電力削減（APR）にします。これにより、オープン回線での高レベルの光パワーの放出が防止されます。
- APR（自動電力削減）は、安全制御が有効になっており、rx-los が検出された場合に、アンプを安全な状態に保ち、既知の電力レベル（8dbm）に固定する一時的な状態です。トラブルシューティングの場合には、APR を永続的に（リンク接続によって独立して）強制できます。
- リンク接続が確認されると、増幅器は最終的な動作状態（利得制御または電力制御）に移行します。

波長と周波数に関する推奨事項

（注） OLS でコヒーレント光学系を使用する場合は、固有の周波数があることを確認します。

チャネル間隔	総帯域幅	波長（nm）		周波数（THz）	
		開始	契約	開始	契約
8 チャネル（200 GHz 間隔）	19.2 nm	1539.1	1558.4	192.375	192.775
16 チャネル（100 GHz 間隔）	2.4 THz				

8 チャネル システムの推奨事項

ITU XR チャネル	周波数（THz）	波長（nm）
37	194.3	1542.94
41	194.1	1544.53
45	193.9	1546.12
49	193.7	1547.72
53	193.5	1549.32
57	193.3	1550.92
61	193.1	1552.52
65	192.9	1554.13

16 チャネル システムの推奨事項

ITU XR チャネル	周波数（THz）	波長（nm）
37	194.3	1542.94
39	194.2	1543.73
41	194.1	1544.53
43	194.0	1545.32
45	193.9	1546.12
47	193.8	1546.92
49	193.7	1547.72
51	193.6	1548.51
53	193.5	1549.32

ITU XR チャネル	周波数（THz）	波長（nm）
55	193.4	1550.12
57	193.3	1550.92
59	193.2	1551.72
61	193.1	1552.52
63	193.0	1553.33
65	192.9	1554.13
67	192.8	1554.94

QDD-ZR のリンク損失

Line Rate	トラフィック モードの設定	TX 電力設定	保証されたリンク損失範囲 (dB)
400G	400ZR-CFEC-16QAm-0-S	デフォルト	0～19

リンク損失	QDD-OLS 設定	
	EDFA-TX ゲイン（dB）	EDFA-RX ゲイン（dB）
0	22	3
1	23	

リンク損失	QDD-OLS 設定	
	EDFA-TX ゲイン（dB）	EDFA-RX ゲイン（dB）
2	24	4
3		5
4		6
5		7
6		8
7		9
8		10
9		11
10		12
11		13
12		14
13		15
14		16
15		17
16		18
17		19
18		20
19		21
20	24	22
21	24	23
22	N/A	該当なし
23	N/A	該当なし
24	N/A	該当なし
25	N/A	該当なし
26	N/A	該当なし
27	N/A	該当なし
28	N/A	該当なし
29	N/A	該当なし
30	N/A	該当なし
31	N/A	該当なし

リンク損失	QDD-OLS 設定	
	EDFA-TX ゲイン（dB）	EDFA-RX ゲイン（dB）
32	N/A	該当なし
33	N/A	該当なし

QDD-ZRP のリンク損失

Line Rate	トラフィック モードの設定	TX 電力設定	保証されたリンク損失範囲 (dB)
400G	400ZR-oFEC-16QAM-1-E	デフォルト	0～23
300 G	300ZR-oFEC-8QAM-1-E	デフォルト	0 ～ 26
200G	200ZR-oFEC-16QPSK-0-S	デフォルト	0 ～ 29

QDD-ZRP 400G のリンク損失

リンク損失	**QDD-OLS** 設定	
	EDFA-TX ゲイン（**dB**）	**EDFA-RX** ゲイン（**dB**）
0	22	3
1	23	
2	24	
3		4
4		5
5		6
6		7
7		8
8		9
9		10
10		11
11		12
12		13
13		14
14		15
15		16
16		17
17		18
18		19
19		20
20		21
21		22
22		23
23		24
24	24	24
25	24	24
26	N/A	該当なし
27	N/A	該当なし
28	N/A	該当なし
29	N/A	該当なし

リンク損失	QDD-OLS 設定	
	EDFA-TX ゲイン（dB）	EDFA-RX ゲイン（dB）
30	N/A	該当なし
31	N/A	該当なし
32	N/A	該当なし
33	N/A	該当なし

QDD-ZRP 300G のリンク損失

リンク損失	**QDD-OLS** 設定	
	EDFA-TX ゲイン（**dB**）	**EDFA-RX** ゲイン（**dB**）
0	22	3
1	23	
2	24	
3		4
4		5
5		6
6		7
7		8
8		9
9		10
10		11
11		12
12		13
13		14
14		15
15		16
16		17
17		18
18		19
19		20
20		21
21		22
22		23
23		24
24		
25		
26		
27	24	24
28	24	24
29	N/A	該当なし

リンク損失	QDD-OLS 設定	
	EDFA-TX ゲイン（dB）	EDFA-RX ゲイン（dB）
30	N/A	該当なし
31	N/A	該当なし
32	N/A	該当なし
33	N/A	該当なし

QDD-ZRP 200G のリンク損失

リンク損失	**QDD-OLS** 設定	
	EDFA-TX ゲイン（**dB**）	**EDFA-RX** ゲイン（**dB**）
0	21	3
1	22	
2	23	
3	24	
4		4
5		5
6		6
7		7
8		8
9		9
10		10
11		11
12		12
13		13
14		14
15		15
16		16
17		17
18		18
19		19
20		20
21		21
22		22
23		23
24		24
25		
26		
27		
28		
29		

リンク損失	QDD-OLS 設定	
	EDFA-TX ゲイン（dB）	EDFA-RX ゲイン（dB）
30	24	24
31	N/A	該当なし
32	N/A	該当なし
33	N/A	該当なし

Bright-ZRP のリンク損失

Line Rate	トラフィック モードの設定	TX 電力設定	保証されたリンク損失範囲 (dB)
400G	400ZR-oFEC-16QAM-1-E	デフォルト	0 ～ 28
300 G	300ZR-oFEC-8QAM-1-E	デフォルト	0 ～ 29
200G	300ZR-oFEC-8QAM-1-E	デフォルト	0 ～ 29

Bright-ZRP 400G のリンク損失

リンク損失	**QDD-OLS** 設定	
	EDFA-TX ゲイン（**dB**）	**EDFA-RX** ゲイン（**dB**）
0	13	3
1	14	
2	15	
3	16	
4		4
5		5
6		6
7		7
8		8
9		9
10		10
11		11
12		12
13		13
14		14
15		15
16		16
17		17
18		18
19		19
20		20
21		21
22		22
23		23
24		24
25		
26		
27		
28		
29	17	24

リンク損失	QDD-OLS 設定	
	EDFA-TX ゲイン（dB）	EDFA-RX ゲイン（dB）
30	17	24
31	N/A	該当なし
32	N/A	該当なし
33	N/A	該当なし

QDD-ZRP 300G のリンク損失

リンク損失	**QDD-OLS** 設定	
	EDFA-TX ゲイン（**dB**）	**EDFA-RX** ゲイン（**dB**）
0	13	3
1	14	
2	15	
3	16	
4		4
5		5
6		6
7		7
8		8
9		9
10		10
11		11
12		12
13		13
14		14
15		15
16		16
17		17
18		18
19		19
20		20
21		21
22		22
23		23
24		24
25		
26		
27		
28		
29		

リンク損失	QDD-OLS 設定	
	EDFA-TX ゲイン（dB）	EDFA-RX ゲイン（dB）
30	17	24
31	17	24
32	N/A	該当なし
33	N/A	該当なし

QDD-ZRP 200G のリンク損失

リンク損失	**QDD-OLS** 設定	
	EDFA-TX ゲイン（**dB**）	**EDFA-RX** ゲイン（**dB**）
0	13	3
1	14	
2	15	
3	16	
4		4
5		5
6		6
7		7
8		8
9		9
10		10
11		11
12		12
13		13
14		14
15		15
16		16
17		17
18		18
19		19
20		20
21		21
22		22
23		23
24		24
25		
26		
27		
28		
29		

リンク損失	QDD-OLS 設定	
	EDFA-TX ゲイン（dB）	EDFA-RX ゲイン（dB）
30	17	24
31	17	24
32	N/A	該当なし
33	N/A	該当なし

増幅器制御モードの構成

OLS には 2 つのアンプがあります。

- COM 増幅器は、

  伝送のためにファイバ ネットワークから接続されたコヒーレント オプティクスへの着信信号をブーストします。

- 回線増幅器は、

  コヒーレント オプティクスからの信号をブーストして、ファイバを介して送信します。

手順の概要

1. グローバル構成モードを開始します。
2. 回線および com の増幅器制御モードを有効または無効にします。
   - 出力制御の手動。
   - 出力制御の powermode

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	グローバル構成モードを開始します。 例： `switch# configure terminal`	**configure terminal**
ステップ 2	回線およびcomの増幅器制御モードを有効または無効にします。 • 出力制御の手動。	**[no] ols { com | line } egress control <mode>** デフォルトのモードは手動です。パラメータ設定は次の表で定義されています。

	コマンドまたはアクション	目的
	• 出力制御の powermode 例： `switch(config)# ols com egress control manual`	側面 / デフォルト / 最小 / 最大 com / 手動 / power / 手動 ライン / 手動 / power / 手動

ゲイン コントロール モードを構成

手順の概要

1. グローバル構成モードを開始します。
2. 回線と COM の OLS プラガブルの目的のゲイン値を構成します。

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	グローバル構成モードを開始します。 例： `switch# configure terminal`	**configure terminal**
ステップ 2	回線と COM の OLS プラガブルの目的のゲイン値を構成します。 例： `switch(config)# ols com egress gain 200`	**[no] { ols com egress <com_gain> | line egress gain <line_gain> }** ゲインの単位は 0.1 dBm です。パラメータ設定は次の表で定義されています。 側面 / デフォルト / 最小 / 最大 com / 200 / 30 / 250 ライン / 210 / 70 / 250

電力制御モードの構成

手順の概要

1. グローバル構成モードを開始します。
2. 回線と COM の OLS プラガブルの目的の出力電力（TX）を構成します。

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	グローバル構成モードを開始します。 例： `switch# configure terminal`	**configure terminal**
ステップ 2	回線と COM の OLS プラガブルの目的の出力電力（TX）を構成します。 例： `switch(config)# ols com egress power 20`	**[no] ols { com egress power <com_power> | line egress power <line_power> }** 電力の単位はdBmです。パラメータ設定は次の表で定義されています。 側面 / デフォルト / 最小 / 最大 com / 80 / 10 / 170 ライン / 80 / 0 / 170

電力削減モードを構成

手順の概要

1. グローバル構成モードを開始します。
2. 電力削減モードを有効または無効化にします。

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	グローバル構成モードを開始します。 例： `switch# configure terminal`	**configure terminal**
ステップ 2	電力削減モードを有効または無効化にします。 例： `switch(config)# ols com egress force power-reduction`	**[no] ols { com | line } egress force power-reduction** 側面 / デフォルト / 最小 / 最大 com / オフ / オン / オフ ライン / オフ / オン / オフ

光安全性リモートインターロック（OSRI）モードの構成

増幅器をシャットダウンするには、光安全性リモート インターロック（OSRI）構成を使用します。プラガブルのメンテナンスのため、および OLS プラガブルが動作していない場合は、構成を使用します。

手順の概要

1. グローバル構成モードを開始します。
2. 電力削減モードを有効または無効にします。

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	グローバル構成モードを開始します。 例： `switch# configure terminal`	**configure terminal**
ステップ 2	電力削減モードを有効または無効にします。 例： `switch(config)# ols com egress force power-reduction`	**[no] ols { com | line } egress force power-reduction** デフォルトモードは、オフです。パラメータ設定は次の表で定義されています。 側面 / デフォルト / 最小 / 最大 com / オフ / オン / オフ ライン / オフ / オン / オフ

安全制御モードを構成

手順の概要

1. グローバル構成モードを開始します。
2. 安全制御モードを有効または無効にします。
   - 自動または
   - 無効

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	グローバル構成モードを開始します。 例： `switch# configure terminal`	**configure terminal**
ステップ 2	安全制御モードを有効または無効にします。 • 自動または • 無効 例： `switch(config)# ols ols line egress safety-control`	**[no] ols line egress safety-control** デフォルト モードは、自動です。

OLS 構成の確認

OLS 詳細情報を表示します。

詳細な OLS 情報を確認するには、 **show interface ethernet traffic details** コマンドを使用します。

```
switch# show interface ethernet 1/2 transceiver details
Ethernet1/2
    transceiver is present
    type is ONS-QDD-OLS
    name is CISCO-ACCELINK
    part number is EDFA-211917-QDD
    revision is 27
    serial number is ACW2723Z007
    nominal bitrate is 425000 MBit/sec per channel
    cisco id is 24
    cisco extended id number is 237
    cisco part number is 1010045801
    cisco product id is ONS-QDD-OLS
    cisco version id is V01
    firmware version is 2.7
    host lane count is 0
    media lane count is 0
    max module temperature is 0 deg C
    min module temperature is 0 deg C
    min operational voltage is 0.00 V
    vendor OUI is 0x000000
    date code is 23070401
    clei code is WMOGAT2MAA
    power class is 2 (3.5 W maximum)
    max power is 3.50 W
    near-end lanes used none
    far-end lane code for 8 lanes Undefined
    media interface is others
```

```
Advertising code is Optical Interfaces: SMF
Host electrical interface code is Undefined
media interface advertising code is Undefined
Operational Parameters:
---------------------
   COM Side:
      Total Tx Power = -327.68 dBm
      Rx Signal Power = -327.68 dBm
      Tx Signal Power = -327.68 dBm
      Egress Ampli Gain = 0.0 dBm
      Egress Ampli OSRI = ON
      Egress Force APR = ON
   Line Side:
      Total Tx Power = -327.68 dBm
      Rx Signal Power = -327.68 dBm
      Tx Signal Power = -327.68 dBm
      Egress Ampli Gain = 0.0 dBm
      Egress Ampli Safety Control mode = disabled
      Egress Ampli OSRI = ON
      Egress Force APR = ON
Configured Parameters:
----------------------
   COM Side:
      Egress Ampli Gain = 20.0 dBm
      Egress Ampli Power = 17.0 dBm
      Egress Ampli OSRI = ON
      Ampli Control mode = Power
      Rx Low Threshold = -300.0 dBm
      Tx Low Threshold = -50.0 dBm
      Egress Force APR = ON
   Line Side:
      Egress Ampli Gain = 20.0 dBm
      Egress Ampli Power = 17.0 dBm
      Egress Ampli Safety Control mode = disabled
      Egress Ampli OSRI = ON
      Ampli Control mode = Power
      Rx Low Threshold = -300.0 dBm
      Tx Low Threshold = -50.0 dBm
      Egress Force APR = ON
  Temperature = 19.70 Celsius
  Voltage = 3.34 V
```

簡易 OLS 情報の表示

OLS 情報を簡単に確認するには、 **show interface ethernet brief** コマンドを使用します。

```
switch# show interface e1/2 brief

--------------------------------------------------------------------------------
Ethernet        VLAN    Type Mode   Status  Reason                 Speed     Port
Interface                                                                    Ch #
--------------------------------------------------------------------------------
Eth1/2          --      eth  routed down    olsInserted              auto(D) --
```

光ファイバのステータスを表示します。

show interface status コマンドを使用して、オプティクのステータスを確認します。

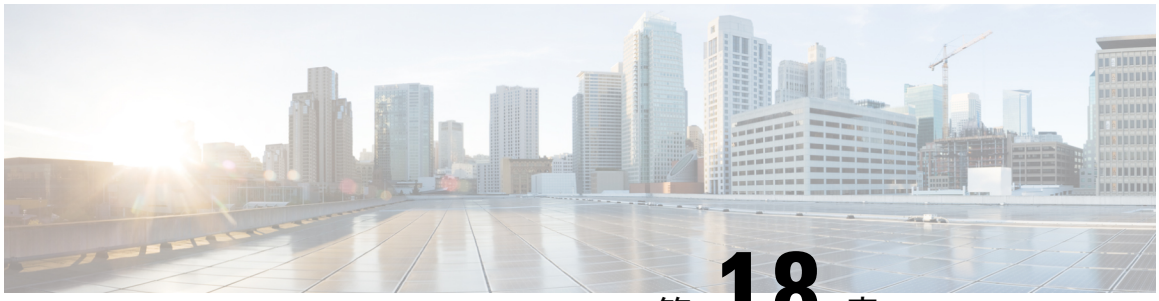
```
switch# show interface e1/2 status

--------------------------------------------------------------------------------
Port          Name               Status    Vlan      Duplex  Speed   Type
```

```
--------------------------------------------------------------------------------
Eth1/2        --                 olsInsert routed    auto    auto    ONS-QDD-OLS
```

実行構成を表示します

OLS の実行構成を表示するには、 **show running-config interface ethernet** コマンドを使用します。

```
switch# show running-config interface ethernet1/2
!Command: show running-config interface Ethernet1/2
!Running configuration last done at: Mon Feb 26 12:39:24 2024
!Time: Mon Feb 26 13:03:34 2024
version 10.4(3) Bios:version 01.07
interface Ethernet1/2
  ols com egress control power
  ols com egress osri
  ols com egress power 170
  ols line egress control power
  ols line egress osri
  ols line egress gain 200
  ols line egress power 170
  no ols line egress safety-control
  ols com egress force power-reduction
  ols line egress force power-reduction
  no shutdown
```



第 18 章

光ファイバの多用途診断モニタリング

Cisco NX-OS リリース 10.6(1)F以降では、多目的診断モニタリング（VDM）を使用して Cisco N9364E-SG2-Q スイッチの着脱可能な光モジュールをモニタできます。

Cisco NX-OS リリース 10.6(1)F は、対応する光モジュールでの VDM 機能のサポートが導入されます。ただし、機能はモジュールのベンダーとその特定のファームウェアバージョンによって異なります。

- この機能により、従来のデジタル オプティカル モニタリング（DOM）（DOM）を超える標準規格のパフォーマンスと診断モニタリング機能が拡張されます。
- VDM を使用すると、信号対雑音比率、Pre-FEC ビット エラー レート、レーザー エージングなどの高度なデータ パラメータにアクセスできます。
- より効果的な能動的なメンテナンスを実行し、複雑な問題をトラブルシュート、長期的な光モジュールの実行可能性を評価することができます。

VDMを活用、光リンクの状態とパフォーマンスをより詳細にインサイトします。詳細なパラメータを追跡することで、エスカレーションされる前に潜在的な問題を特定し、能動的なメンテナンスを改善できます。

主要パラメータ（VDM オブザーバブル）

モジュールに応じて、VDM で一連のオブザーバブル タイプをモニタできます。次の表に、主要なパラメータ、そのデータ型、および単位を示します。

表 *21* : 主要なパラメータ（*VDM* オブザーバブル）

観測可能型	インスタンス タイプ	ユニット（Units）
[Laser Age (Data Path)]：サポート開始（BOL）からサポート終了（EOL）までのパーセンテージ。数字が大きいほど、EOL に近いことを意味します。	基本	%

観測可能型	インスタンス タイプ	ユニット（Units）
[TEC 電流（モジュール）（TEC Current (Module)）]：冷却レーザーの熱電気冷却器（TEC）に流れる電流の量	基本	%
[Laser Frequency Error (Media Lane)]：ターゲット中心周波数と実際の現在の中心周波数の差。	基本	MHz
レーザー温度（メディア レーン）：冷却レーザーのターゲットレーザー温度と実際の温度の温度差。	基本	°C
eSNR メディア入力（メディア レーン）：入力光レーンの電気信号対雑音比。	基本	dB
eSNR ホスト入力（レーン）	基本	dB
PAM4 Level Transition Parameter Media Input（メディア レーン）：電気レベル スライサー ノイズを測定します。	基本	dB
PAM4 レベル遷移パラメータ ホスト 入力（レーン）	基本	dB
Pre-FEC BER 最小メディア入力（データ パス）：観察された最小の前方誤り訂正ビットエラー率	統計	—
Pre-FEC BER 最小ホスト入力（データ パス）	統計	—
Pre-FEC BER 最大メディア入力（データ パス）	統計	—
Pre-FEC BER 最大ホスト入力（データ パス）	統計	—
Pre-FEC BER 平均メディア入力（データ パス）	統計	—
Pre-FEC BER 平均ホスト入力（データ パス）	統計	—
Pre-FEC BER 現在の値メディア入力（データパス）	基本	—
Pre-FEC BER 現在値ホスト入力（データ パス）	基本	—
[FERC Minimum Media Input (Data Path)]：フレームエラー数。修正不可能な FEC フレームの数。	統計	—
FERC 最小ホスト入力（データ パス）	統計	—
FERC 最大メディア入力（データ パス）	統計	—
FERC 最大ホスト入力（データ パス）	統計	—
FERC平均メディア入力（データ パス）	統計	—

観測可能型	インスタンス タイプ	ユニット（Units）
FERC 平均ホスト入力（データ パス）	統計	—
FERC 現在値メディア入力（データ パス）	基本	—
FERC 現在値ホスト入力（データ パス）	基本	—

（注） 表示される正確な形式と特定の VDM パラメータは、モジュール タイプおよびシステム ソフトウェア バージョンによって異なる場合があります。

トランシーバの VDM 情報を表示します

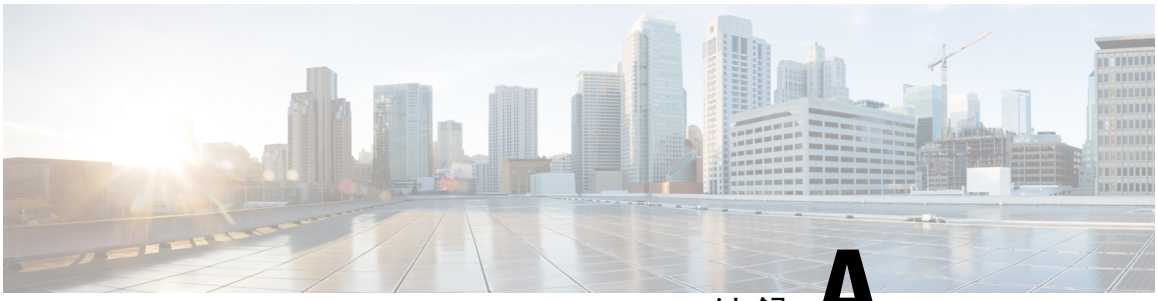
サポート対象のトランシーバの VDM 情報を表示するには、 **show interface ethernet** *interface_id* **transceiver vdm** コマンドを使用してトランシーバ診断を表示します。コマンド出力には、VDM パラメータが含まれます。

```
switch# show interface ethernet 1/4/1 transceiver vdm
Ethernet1/4/1
    transceiver is present
    type is OSFP-8x100G-DR
    name is FINISAR CORP.
    part number is FTCE4517E1PCM
    revision is A0
    serial number is XCNCGZ2
    nominal bitrate is 425000 MBit/sec per channel
    cisco id is 25
    cisco extended id number is 0
    firmware version is 3.5
    Link length SMF is 0.5 km
    Nominal transmitter wavelength is 1311.00 nm
    Wavelength tolerance is 6.500 nm
    host lane count is 4
    media lane count is 4
    max module temperature is 70 deg C
    min module temperature is 0 deg C
    min operational voltage is 3.14 V
    vendor OUI is 0x009065
    date code is 241226
    power class is 8 (>14 W maximum)
    max power is 16.00 W
    near-end lanes used none
    far-end lane code for 8 lanes Undefined
    media interface is 1310 nm EML
    Advertising code is Optical Interfaces: SMF
    media interface advertising code is 400GBASE-DR4 (Cl 124)
Lane Number:1 Network Lane
  Current temperature                    :   28.75 C
  Temperature high alarm                 :  Off
  Temperature low alarm                  :  Off
  Temperature high warning               :  Off
  Temperature low warning                :  Off
  Temperature high alarm threshold       :   75.00 C
  Temperature low alarm threshold        :   -5.00 C
  Temperature high warning threshold     :   72.00 C
```

```
Temperature low warning threshold      :   -2.00 C
Current voltage                  :    3.34 V
Voltage high alarm               :  Off
Voltage low alarm                :  Off
Voltage high warning             :  Off
Voltage low warning              :  Off
Voltage high alarm threshold         :    3.63 V
Voltage low alarm threshold           :    2.97 V
Voltage high warning threshold       :    3.46 V
Voltage low warning threshold        :    3.13 V
Current current                      :  N/A
Current high alarm                   :  Off
Current low alarm                    :  Off
Current high warning                 :  Off
Current low warning              :  Off
Current high alarm threshold         :  125.00 mA
Current low alarm threshold          :   25.00 mA
Current high warning threshold       :  120.00 mA
Current low warning threshold        :   30.00 mA
Current Tx Power                     :  N/A
Tx power high alarm                  :  Off
Tx power low alarm                   :  Off
Tx power high warning          :  Off
Tx power low warning           :  Off
Tx power high alarm threshold    :    7.39 dBm
Tx power low alarm threshold     :   -3.30 dBm
Tx power high warning threshold  :    5.39 dBm
Tx power low warning threshold   :   -1.30 dBm
Current Rx power                 :    0.66 dBm
Rx power high alarm              :  Off
Rx power low alarm               :  Off
Rx power high warning            :  Off
Rx power low warning             :  Off
Rx power high alarm threshold    :    6.19 dBm
Rx power low alarm threshold      :  -11.24 dBm
Rx power high warnings threshold :    4.19 dBm
Rx power low warnings threshold  :   -9.20 dBm
Transmit Fault Count                     :  0
Laser age                                :    0.00
TEC current                              :  9637.00
Laser frequency error                :  not valid
Laser temperature                        :   10.00
eSNR media input                         :    0.00
eSNR host input                          :  6110.00
PAM4 level transition parameter media input:    0.00
PAM4 level transition parameter host input:  65535.00
Pre-FEC BER minimum media input         :    0.00
Pre-FEC BER minimum host input          :    0.00
Pre-FEC BER maximum media input         :    0.00
Pre-FEC BER maximum host input          :    0.00
Pre-FEC BER average media input         :    0.00
Pre-FEC BER average host input          :    0.00
Pre-FEC BER current media input         :    0.00
Pre-FEC BER current host input          :    0.00
FERC minimum media input                :    0.00
FERC minimum host input                 :    0.00
FERC maximum media input                :    0.00
FERC maximum host input                 :    0.00
FERC average media input                :    0.00
FERC average host input                 :    0.00
FERC current value media input          :    0.00
FERC current value host input           :    0.00
```

VDM DME センサー

VDM は DME で利用できます。詳細については、[Cisco Nexus NX-API リファレンス（Cisco Nexus NX-API References）]を参照してください。



付録 A

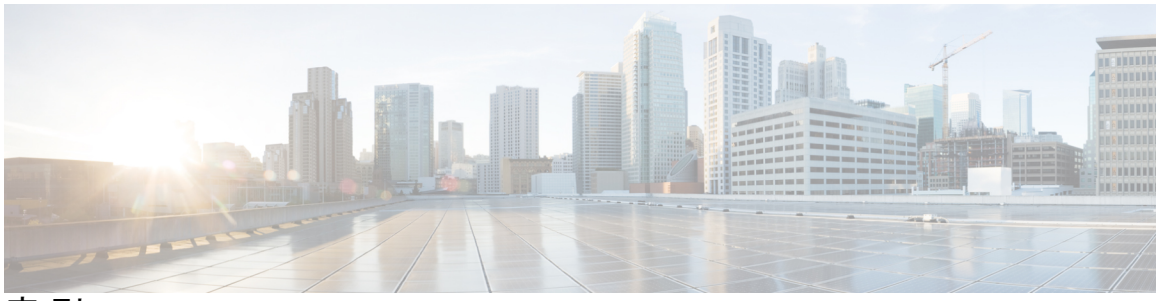
ITU C-BAND テーブル

ITU チャネル	周波数（GHz）	波長
1	19610	1528773
2	19605	1529163
3	19600	1529553
4	19595	1529944
5	19590	1530334
6	19585	1530725
7	19580	1531116
8	19575	1531507
9	19570	1531898
10	19565	1532290
11	19560	1532681
12	19555	1533073
13	19550	1533465
14	19545	1533858
15	19540	1534250
16	19535	1534643
17	19530	1535036
18	19525	1535429
19	19520	1535822
20	19515	1536216
21	19510	1536609
22	19505	1537003
23	19500	1537397

ITU チャネル	周波数（GHz）	波長
24	19495	1537792
25	19490	1538186
26	19485	1538581
27	19480	1538976
36	19475	1539371
29	19470	1539766
30	19465	1540162
31	19460	1540557
32	19455	1540953
33	19450	1541349
34	19445	1541746
35	19440	1542142
36	19435	1542539
37	19430	1542936
38	19425	1543333
39	19420	1543730
40	19415	1544128
41	19410	1544526
42	19405	1544924
43	19400	1545322
44	19395	1545720
45	19390	1546119
46	19385	1546518
47	19380	1546917
48	19375	1547316
49	19370	1547715
50	19365	1548115
51	19360	1548515
52	19355	1548915
53	19350	1549315
54	19345	1549715
55	19340	1550116

ITU チャネル	周波数（GHz）	波長
56	19335	1550517
57	19330	1550918
58	19325	1551319
59	19320	1551721
60	19315	1552122
61	19310	1552524
62	19305	1552926
63	19300	1553329
64	19295	1553731
65	19290	1554134
66	19285	1554537
67	19280	1554940
68	19275	1555343
69	19270	1555747
70	19265	1556151
71	19260	1556555
72	19255	1556959
73	19250	1557363
74	19245	1557768
75	19240	1558173
76	19235	1558578
77	19230	1558983
78	19225	1559389
79	19220	1559794
80	19215	1560200
81	19210	1560606
82	19205	1561013
83	19200	1561419
84	19195	1561826
85	19190	1562233
86	19185	1562640
87	19180	1563047

ITU チャネル	周波数（GHz）	波長
88	19175	1563455
89	19170	1563863
90	19165	1564271
91	19160	1564679
92	19155	1565087
93	19150	1565496
94	19145	1565905
95	19140	1566314
96	19135	1566723
97	19130	1567133



索引

I

L

M

N

P

R

S

T

U

V

い

さ

し

す

と

翻訳について
このドキュメントは、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。