Cisco Nexus 9000 シリーズ NX-OS SAN スイッチング構成ガイド、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

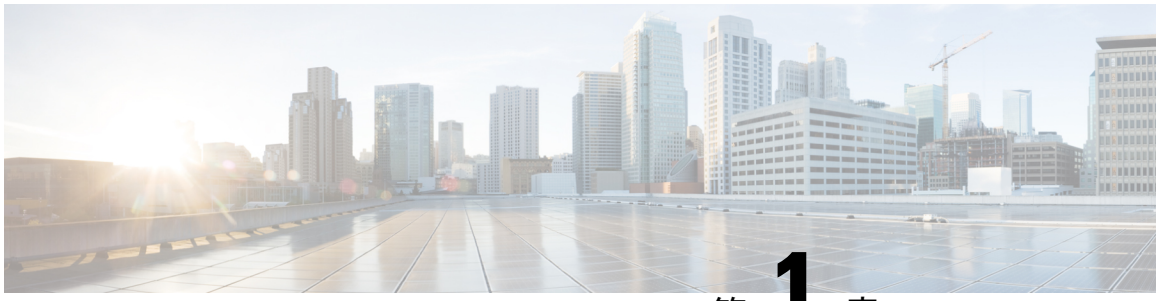
- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet [英語] にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press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

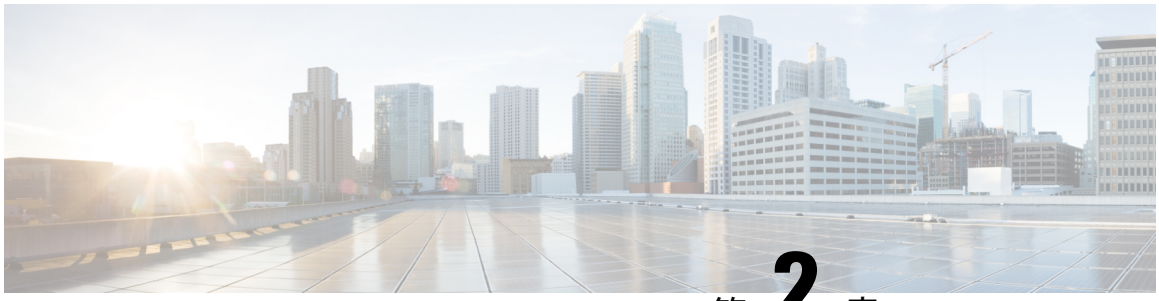
新機能と更新情報

新機能と更新情報

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
NA	このリリースで追加された新機能はありません。	10.6(1)F	該当なし

新機能と更新情報



第 2 章

SAN スイッチングのハードウェア サポート

SAN スイッチングのハードウェア サポート

次の表に、SAN スイッチングをサポートする Cisco Nexus 9000 シリーズ ハードウェアを示します。

表 *2 : Cisco Nexus 9300* シリーズ スイッチ：サポートするハードウェア

モデル（PID）	FC E ポート	FCoE E ポート	FC エッジ ポート	FCoE エッジ ポート	FEX サポート
N9K-C9336C-FX2-E	○	はい	○	○	非対応
N9K-C93180YC-FX	○	はい	○	○	非対応
N9K-C93360YC-FX2	○	はい	○	○	非対応

（注） Cisco NX-OS リリース 10.2(3)F 以降、FCoE E ポートがサポートされています。

次の FC SFP がサポートされています。

- DS-SFP-4X32G-SW は N9K-C9336C-FX2-E でのみサポートされます
- DS-SFP-FC8G-SW は N9K-C93180YC-FX および N9K-C93360YC-FX2 でのみサポートされます
- DS-SFP-FC16G-SW は N9K-C93180YC-FX および N9K-C93360YC-FX2 でのみサポートされます

- DS-SFP-FC32G-SW は N9K-C93180YC-FX および N9K-C93360YC-FX2 でのみサポートされます
- DS-SFP-FC32G LW は長距離 ISL でのみサポートされます（N9K-C93180YC-FX でサポート）

FCoE 長距離 ISL では、次の SFP がサポートされています。

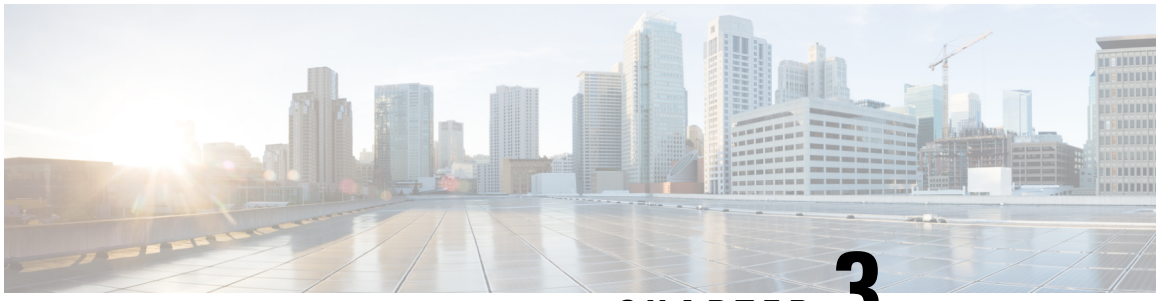
- SFP-10G-LR、SFP-10/25G-LR-I、および QSFP-40G-LR4/QSFP-40G-LR4-S は FCoE 長距離 ISL でのみサポートされます

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。



CHAPTER 3

概要

この章は、次の内容で構成されています。

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。

SAN スイッチングの概要

この章では、Cisco Nexus 9000 デバイスの SAN スイッチングの概要について説明します。この章は、次の項で構成されています。

拡張モジュールを使用した場合、使用可能なファイバ チャネル ポートは、Cisco Nexus 5010 スイッチで最大 8 個、Cisco Nexus 5020 スイッチで最大 16 個です。

ドメイン パラメータ

ファイバ チャネル ドメイン（fcdomain）機能では、FC-SW-2 標準で記述されているように、主要スイッチ選択、ドメイン ID 配信、FC ID 割り当て、ファブリック再設定機能が実行されます。ドメインは VSAN 単位で設定されます。ドメイン ID を設定しない場合、ローカル スイッチはランダムな ID を使用します。

N ポート仮想化

Cisco NX-OS ソフトウェアは業界標準の N ポート ID バーチャライゼーション（NPIV）をサポートします。NPIV を使用すると、単一の物理ファイバ チャネル リンクで複数の N ポート ファブリックが同時にログインできます。NPIV をサポートする HBA では、ホスト上の各仮想マシン（OS パーティション）についてゾーン分割とポート セキュリティを個別に設定できるようにすることで、SAN セキュリティを改善できます。NPIV はサーバ接続に有効なだけでなく、コアおよびエッジの SAN スイッチ間の接続にも有効です。

N ポート バーチャライザ（NPV）は、コアエッジ SAN のファイバ チャネル ドメイン ID 数を減らすことができる補完的な機能です。NPV モードで動作する Cisco MDS 9000 ファミリ ファブリック スイッチはファブリックに参加せず、コア スイッチ リンクとエンド デバイス間でトラフィックを通過させるだけです。このため、スイッチのドメイン ID は不要です。NPIV は、NPV コア スイッチへのリンクを共有する複数のエンド デバイスにログインするために、NPV モードのエッジ スイッチで使用されます。この機能を使用できるのは、Cisco MDS ブレード スイッチ シリーズ、Cisco MDS 9124 マルチレイヤ ファブリック スイッチ、および Cisco MDS 9134 マルチレイヤ ファブリック スイッチだけです。

N ポート バーチャライザ（NPV）は、コアエッジ SAN のファイバ チャネル ドメイン ID 数を減らすことができる補完的な機能です。NPV モードで動作する Cisco Nexus 9000 シリーズ ファブリック スイッチはファブリックに参加せず、コア スイッチ リンクとエンド デバイス間でトラフィックを通過させるだけです。このため、スイッチのドメイン ID は不要です。NPIV は、NPV コア スイッチへのリンクを共有する複数のエンド デバイスにログインするために、NPV モードのエッジ スイッチで使用されます。

VSAN トランキング

トランキングは、VSAN トランキングとも呼ばれ、複数の VSAN 内で、同一の物理リンクを介して、ポートが相互接続してフレームを送受信することを可能にします。トランキングは E ポートおよび F ポートでサポートされます

SAN ポート チャネル

ポートチャネルは、ファイバチャネル トラフィックについて、複数の物理 ISL を帯域幅が大きく、またポートの耐障害性が高い 1 つの論理リンクに集約します。この機能を使用すると、最大 16 の拡張ポート（E ポート）またはトランキング E ポート（TE ポート）をポートチャネルにバンドルできます。ISL ポートは任意のスイッチング モジュールに配置できるため、特定のプライマリ ポートは必要ありません。ポートまたはスイッチング モジュールに障害が発生した場合、ファブリックを再設定しなくても、ポートチャネルは引き続き正常に機能します。

Cisco NX-OS ソフトウェアでは、隣接するスイッチ間でポートチャネル設定情報を交換するときにプロトコルを使用するので、ポートチャネル管理が簡易化されます。たとえば、誤設定の検出や、互換性のある ISL でのポートチャネルの自動作成などの管理機能です。自動設定モー

ドでは、互換性のあるパラメータを使用するISLによって、チャネル グループが自動的に構成されます。手動操作は必要ありません。

ポートチャネルでは、発信元 FC-ID と宛先 FC-ID のハッシュ、さらにオプションで交換 ID を使用して、ファイバ チャネル トラフィックのロード バランスが実行されます。ポートチャネルを使用するロード バランシングは、ファイバ チャネル リンクと FCIP リンクの両方で実行されます。また、Cisco NX-OS ソフトウェアを設定して、コストが同じ複数の FSPF ルート間でロード バランスを実行することもできます。

仮想 SAN

仮想SAN（VSAN）は、単一の物理SANを複数のVSANに分割します。VSANを使用すると、Cisco NX-OS ソフトウェアで、大規模な物理ファブリックを個々の分離された環境に論理的に分割して、ファイバ チャネル SAN のスケーラビリティ、アベイラビリティ、管理性、およびネットワーク セキュリティを高めることができます。

それぞれの VSAN は、独自の一連のファイバ チャネル ファブリック サービスを持つ論理的および機能的に別個の SAN です。ファブリック サービスのこの分割は、個々の VSAN 内にファブリックの再設定およびエラー条件を含めることにより、ネットワークの不安定さを大幅に軽減します。VSAN が実現する厳密なトラフィック分離は、特定の VSAN の制御およびデータ トラフィックを VSAN 独自のドメイン内に限定することにより、SAN セキュリティを高めるために役立ちます。VSAN は、アベイラビリティを低下させることなく、分離された SAN アイランドを共通のインフラストラクチャに容易に統合できるようにすることで、コスト削減に貢献します。

ユーザーは、特定のVSANの範囲内に限定される管理者ロールを作成できます。たとえば、すべてのプラットフォーム固有の機能を設定できるネットワーク管理者ロールを設定する一方で、特定のVSAN内のみで設定および管理ができるその他のロールを設定できます。この手法は、スイッチ ポートまたは接続されたデバイスのWWN（World Wide Name）に基づいてメンバーシップを割り当てることができる、特定のVSANに対するユーザー操作の効果を分離することにより、SAN の管理性を高め、人為的エラーを原因とする中断を減らします。

VSANは、離れた場所にあるデバイスを含めるためにVSANを拡張する、SAN間のFibre Channel over IP（FCIP）リンク全体にわたりサポートされます。Cisco SAN スイッチは、VSAN のトランキングも実装します。トランキングでは、ISL（スイッチ間リンク）によって、同じ物理リンク上で複数の VSAN のトラフィックを伝送できます。

ゾーン分割

ゾーン分割は、SAN 内のデバイスのアクセス コントロールを提供します。Cisco NX-OS ソフトウェアは、次の種類のゾーン分割をサポートしています。

- Nポート ゾーン分割：エンドデバイス（ホストおよびストレージ）ポートに基づいてゾーン メンバーを定義します。
  - WWN
  - ファイバ チャネル ID（FC-ID）
- Fx ポート ゾーン分割：スイッチ ポートに基づいてゾーン メンバーを定義します。
  - WWN

- WWNおよびインターフェイスインデックス、またはドメインIDおよびインターフェイス インデックス

- ドメイン ID およびポート番号（Brocade の相互運用性用）。
- iSCSI ゾーン分割：ホスト ゾーンに基づいてゾーン メンバーを定義します。
  - iSCSI 名
  - IP アドレス
- LUN ゾーン分割：N ポート ゾーン分割と組み合わせて使用すると、論理ユニット番号（LUN）ゾーン分割は、特定のホストだけが LUN にアクセスできるようにし、異種ストレージサブシステム アクセスを管理するための単一制御点を提供します。
- 読み取り専用ゾーン：属性を設定して、任意のゾーン タイプでの I/O 操作を SCSI 読み取り専用コマンドに制限できます。この機能は、バックアップ、データ ウェアハウジングなど、サーバー間でボリュームを共有する場合に役立ちます。
- ブロードキャスト ゾーン：任意のゾーン タイプ用の属性を設定して、ブロードキャスト フレームを特定のゾーンのメンバーに制限できます。

厳密なネットワーク セキュリティを実現するため、入力スイッチで適用されるアクセス コントロール リスト（ACL）を使用して、ゾーン分割はフレームごとに常に適用されます。すべてのゾーン分割ポリシーはハードウェアで適用され、パフォーマンスの低下を引き起こすことはありません。拡張ゾーン分割セッション管理機能では、一度に1人のユーザーだけがゾーンを変更できるようにすることで、セキュリティがさらに高まります。

デバイス エイリアス サービス

ソフトウェアでは、VSAN 単位およびファブリック全体のデバイス エイリアス サービス（デバイス エイリアス）がサポートされます。デバイス エイリアス配信により、エイリアス名を手動で再度入力することなく、VSAN 間で HBA（ホスト バス アダプタ）を移動できます。

ファイバ チャネル ルーティング

Fabric Shortest Path First（FSPF）は、ファイバ チャネル ファブリックで使用されるプロトコルです。FSPF は、どのファイバ チャネル スイッチでも、デフォルトでイネーブルになっています。特に考慮が必要な設定を除いて、FSPF サービスを設定する必要はありません。FSPF はファブリック内の任意の 2 つのスイッチ間の最適パスを自動的に計算します。特に、FSPF は次の機能を実行するために使用されます。

- 任意の2つのスイッチ間の最短かつ最速のパスを確立して、ファブリック内のルートを動的に計算します。
- 特定のパスで障害が発生した場合は、代替パスを選択します。FSPFは複数のパスをサポートし、障害リンクを迂回する代替パスを自動的に計算します。2 つの同等パスを使用できる場合は、推奨ルートを設定します。

SCSI ターゲット

SCSI ターゲットにはディスク、テープ、およびその他のストレージ デバイスが含まれます。これらのターゲットは、ネーム サーバーに論理ユニット番号（LUN）を登録しません。SCSI LUN検出機能は、CLI（コマンドラインインターフェイス）またはSNMP（簡易ネットワーク管理プロトコル）を通して、オンデマンドで開始されます。近接スイッチが Cisco Nexus デバイスに属する場合、この情報は近接スイッチとも同期されます。

拡張ファイバ チャネル機能

分散サービス、エラー検出、およびリソース割り当てのためにファイバ チャネル プロトコル関連タイマーの値を設定できます。

単一のスイッチにWWNを一意に関連付ける必要があります。主要スイッチを選択するとき、およびドメイン ID を割り当てるときは、WWN を使用します。Cisco Nexus デバイスは、3 つの Network Address Authority（NAA）アドレス フォーマットをサポートします。

ファイバ チャネル標準では、任意のスイッチの F ポートに接続された N ポートに、一意の FC ID を割り当てる必要があります。使用する FC ID 番号を節約するために、 Cisco Nexus デバイスでは特殊な割り当て方式を使用しています。

FC-SP および DHCHAP

Fibre Channel Security Protocol（FC-SP）は、スイッチ間およびホストとスイッチ間で認証を実行して、企業全体のファブリックに関するセキュリティ問題を解決します。Diffie-Hellman Challenge Handshake Authentication Protocol（DHCHAP）は、 スイッチとその他のデバイス間で認証を行う FC-SP プロトコルです。DHCHAP は、CHAP プロトコルと Diffie-Hellman 交換を組み合わせて構成されています。

FC-SPの使用により、スイッチ、ストレージデバイス、およびホストは信頼性の高い管理可能な認証メカニズムを使ってそれぞれのアイデンティティを証明できます。FC-SP の使用により、ファイバ チャネル トラフィックをフレーム単位で保護することで、信頼できないリンクであってもスヌーピングやハイジャックを防止できます。ポリシーと管理アクションの一貫した組み合わせがファブリックを介して伝播されて、ファブリック全体での均一なレベルのセキュリティが実現します。

ポート セキュリティ

ポート セキュリティ機能は、1 つ以上の所定のスイッチ ポートへのアクセス権を持つ特定の World-Wide Name（WWN）をバインドすることによって、スイッチ ポートへの不正なアクセスを防止します。

スイッチ ポートでポート セキュリティをイネーブルにしている場合は、そのポートに接続するすべてのデバイスがポート セキュリティ データベースになければならず、所定のポートにバインドされているものとしてデータベースに記されている必要があります。これらの両方の基準を満たしていないと、ポートは動作上アクティブな状態にならず、ポートに接続しているデバイスは SAN へのアクセスを拒否されます。

ファブリック バインディング

ファブリック バインディングは、ファブリック バインディング設定で指定されたスイッチ間のみでスイッチ間リンク（ISL）がイネーブルにされるようにします。これによって、無許可のスイッチが、ファブリックに参加したり、現在のファブリック処理が中断したりできないようにします。この機能では、Exchange Fabric Membership Data（EEMD）プロトコルを使用する

ことによって、許可されたスイッチのリストがファブリック内の全スイッチで同一になります。

ファブリック構成サーバー

Fabric Configuration Server（FCS）を使用すると、トポロジ属性を検出したり、ファブリック要素の設定情報リポジトリを維持したりすることができます。通常、管理アプリケーションはNポートを通してスイッチの FCS に接続されます。複数の VSAN がファブリックを構成し、VSAN ごとに 1 つの FCS インスタンスが存在します。

SAN スイッチングの一般的な注意事項と制限事項

次に、SAN スイッチングの一般的な注意事項と制限事項を示します。

- SAN スイッチングは、Cisco Nexus C93180YC-FX および C93360YC-FX2 スイッチでのみサポートされます。Cisco NX-OS リリース 10.2(2)F 以降、SAN スイッチングはCisco N9K-C9336C-FX2-E プラットフォーム スイッチでもサポートされています。
- VE ポートまたは仮想拡張ポート（ISL）は、Cisco NX-OS リリース 10.2(3)F からサポートされています。
- ダイナミック ポート VLAN メンバーシップ（*DPVM*）はサポートされていません。
- スイッチ モードのファブリック エクステンダ（*FEX*）はサポートされていません
- IP over Fibre Channel（*IPFC*）機能はサポートされていません。
- Inter VSAN Routing（*IVR*）はサポートされていません
- CLI の XML および DME はサポートされていません。
- OBFL（show logging onboard）機能のサポートは、エラー統計に限定されています。

（注） OBFL の詳細については、*Cisco Nexus 9000* シリーズ *NX-OS* トラブルシューティング ガイド、リリース *9.3(x)* を参照してください。

- Nexus 9000 は、8 Gbps ファイバ チャネル インターフェイスで IDLE フィル パターンのみをサポートします。Nexus 9000 FC インターフェイスを 8 Gbps で動作させるには、一致する IDLE フィル パターンを使用するようにピア デバイスを設定する必要があります。ほとんどのサーバーおよびターゲット FC インターフェイスはこれをサポートしていないため、8 Gbps では Nexus 9000 に接続できません。8 Gbps で他のファイバ チャネル スイッチと相互運用するには、ピア スイッチ FC インターフェイスでも一致する IDLE フィル パターンが使用されていることを確認します。Cisco MDS スイッチの場合は、**switchportfill-pattern** インターフェイス構成コマンドを使用して設定します。8 Gbps でピア Nexus 9000 に接続するには、フィルパターン設定を使用しないでください。デフォルトでは、両方のデバイスが一致する IDLE フィル パターンを使用するからです。

- Cisco NX-OS リリース 10.2(2) 以降、Cisco Nexus N9K-C9336C-FX2-E プラットフォーム スイッチの動作速度と san-poへのメンバーの追加には、次の制限が課されています。
  - **fc-bo の速度変更**：
    - デフォルトの速度は 32G です。
    - 速度変更は、単一の fc-bo インターフェイス レベルでは実行できません。
    - fc-bo の速度変更は、fc-bo インターフェイス レベルの範囲で行われます。
      - 範囲には、フロント パネルのポートに対応する fc-bo のフル セットが含まれている必要があります。

（注） 範囲の一部を指定すると、速度設定で **ERR_01** エラーが表示されます。

      - san-po の一部である fc-bo を範囲に含めないでください。

（注） 範囲に san-po メンバーが含まれている場合、速度設定は **ERR_02** エラーを表示します。

      - 範囲には、複数の前面パネル ポートに対応する fc-bo ポートを設定できます。

  - **san-po の速度変更**：
    - san-po のデフォルトの速度は 32G です。
    - san-po の速度変更は、そのメンバーにフロント パネルのポートに対応するすべての fc-bo ポートが含まれている場合にのみ許可されます。

（注） san-po がフロント パネル ポートに対応する fc-bo ポートを部分的に設定している場合、速度変更により **ERR_03** エラーが表示されます。

    - san-po の速度を変更するには、san-po インターフェイスの範囲を指定します。

  - **実行中の構成の速度設定**：
    - 速度設定（デフォルトではない）は、fc-bo インターフェイスの範囲レベルで表示されます。 **sh runn** コマンドの個々の fc-breakout インターフェイスの下には表示されません。

- 速度設定（デフォルトではない）は、**show interface fc**<int no> コマンドで表示されます。

- **san-poへのメンバーの追加（channel-group x）**：
  - インターフェイスの範囲には、フロント パネルのポートに対応する fc-bo のフルセットが含まれている必要があります。

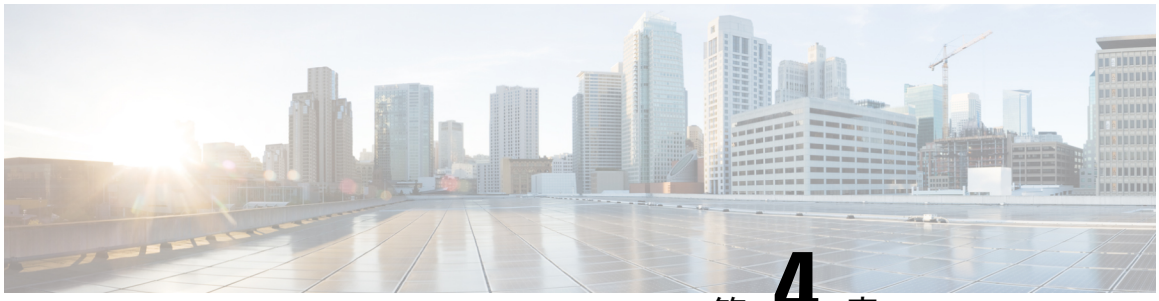
（注） チャネルの追加は成功しますが、一部の範囲に対して **WARN_01** 警告メッセージが表示されます。

  - 範囲には、複数の前面パネル ポートに対応する fc-bo ポートを設定できます。

```
ERR_01 : if-range contains partial set of fc1/18/1-4 fc-bo ports
ERR_02 : if-range contains fc1/21/1-4 ports; some are part sanpo
ERR_03 : san-port-channel21 does not contain full set of fc1/22/1-4 fc-bo ports
WARN_01 : Warning: if-range contains partial set of fc1/22/1-4 fc-bo ports
```

- Cisco NX-OS リリース 10.2(3)F 以降、ファイバ チャネル フォワーダ（FCF）間の仮想 E ポート（VE ポート）接続は、Cisco N9K-C93180YC-FX、N9K-C9336C-FX2-E、および N9K-C93360YC-FX2 プラットフォーム スイッチでサポートされます。

- 同じスイッチ上に FC または FCOE が設定されている場合、トンネルはサポートされません。



第 4 章

FC/FCoE スイッチ モードの有効化

この章は、次の内容で構成されています。

Cisco Nexus 9000 シリーズ スイッチで FC/FCoE スイッチ モードを有効にするには、**feature-set fcoe** を設定する必要があります。

（注） Cisco Nexus 9000 シリーズスイッチで NPV モードを有効にする方法の詳細については、cisco.com の *Cisco Nexus 9000 Series NX-OS FC-NPV and FCoE-NPV Configuration Guide* を参照してください。

FCoE 機能を有効にする

FC スイッチング モードに関する注意事項と制限事項

- リリース 10.1(1) 以降、FC スイッチモードは Cisco Nexus 93360YC-FX2 でサポートされます。
- リリース 10.2(2) 以降、FC スイッチモードは Cisco Nexus C9336C-FX2-E でサポートされます。

- FC/FCoE 構成はロールバックをサポートしていません。FC/FCoE 構成が存在する場合は、ベストエフォート オプションを使用します。他のすべての構成は成功しますが、FC/FCoE 構成ではエラー メッセージが表示されます。

FC/FCoE の有効化

スイッチで FC/FCoE をイネーブルにできますが、VLAN 1 で FCoE をイネーブルにすることはできません。

Note または、**Cisco NX-OS セットアップ ユーティリティ**に含まれている **FC セットアップ スクリプト**を使用して、FC/FCoE を有効にすることもできます。詳細については、対応するバージョンの*Cisco Nexus 9000* シリーズ *NX-OS* 基本設定ガイドを参照してください。cisco.com に掲載されています。

Note Cisco Nexus デバイスのファイバ チャネル機能はすべて、FC プラグインにパッケージ化されています。FC/FCoE を有効にすると、スイッチ ソフトウェアにより SAN_ENTERPRISE_PKG FC_FEATURES_PKG ライセンスのチェックが行われます。ライセンスが検出されると、ソフトウェアによりプラグインがロードされます。FC ポート ライセンスを有効にするには、パッケージ FC_PORT_ACTIVATION_PKG が必要です。

FC プラグインのロード後は、次の 2 つが使用可能となります。

- ファイバ チャネルおよび FCoE に関するすべての CLI
- インストールされている拡張モジュールのファイバチャネル インターフェイス。

180 日が経過すると、有効なライセンスが消失し、FC プラグインは無効となります。スイッチの次回リブート時に、すべての FC/FCoE コマンドが CLI から削除され、FC/FCoE 設定が消去されます。

Before you begin

FC_FEATURES_PKG（N5010SS または N5020SS）ライセンスがインストールされていることが必要です。次の表に、SAN スイッチングのライセンス要件に関する詳細情報を示します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **install feature-set fcoe**
3. switch(config)# **feature-set fcoe**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **install feature-set fcoe**	機能セット FCoE をインストールします。
ステップ 3	switch(config)# **feature-set fcoe**	FC/FCoE 機能を有効にします。

Example

次の例は、スイッチで FC/FCoE を有効にする方法を示しています。

```
switch# configure terminal
switch(config)# install feature-set fcoe
switch(config)# feature-set fcoe
```

FC/FCoE の無効化

FC/FCoE を無効にすると、すべての FC/FCoE コマンドが CLI から削除され、FC/FCoE 構成が削除されます。

Note スイッチに FC ポートがある場合、コマンド **no feature-set fcoe** は許可されません。スイッチに FC ポートがある場合は、このコマンドを発行する前に、それらをイーサネット ポートに変換する必要があります。Cisco Nexus C93180YC-FX、C9336C-FX2-E、および C93360YC-FX2 スイッチでは、機能セット fcoe を無効にした後にスイッチをリロードする必要があります。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no feature-set fcoe**
3. switch(config)# **no install feature-set fcoe**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no feature-set fcoe**	FC/FCoE 機能を無効にします。
ステップ 3	switch(config)# **no install feature-set fcoe**	機能セット FCoE をアンインストールします。

Example

次の例は、スイッチの FCoE を無効にする方法を示したものです。

```
switch# configure terminal
switch(config)# no feature-set fcoe
switch(config)# no install feature-set fcoe
```

FCoE リンクの LAN トラフィックの無効化

FCoE リンクの LAN トラフィックを無効にできます。

DCBX を使用すると、スイッチから、直接接続された CNA へ LAN 論理リンク ステータス（LLS）メッセージを送信できます。CNA へ LLS ダウン メッセージを送信する場合は、**shutdown lan** コマンドを入力します。このコマンドにより、インターフェイスの VLAN のうち、FCoE に対応していないすべての VLAN をダウンできます。インターフェイスの VLAN のうち FCoE に対応している VLAN では、中断されることなくそのまま SAN トラフィックを伝送できます。

手順の概要

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

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。 （注） これが 10G ブレイクアウト ポートの場合、*slot*/*port* 構文は *QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **shutdown lan**	インターフェイス上のイーサネット トラフィックをシャットダウンします。インターフェイスが FCoE VLAN の一部である場合は、シャットダウンを実行しても、その FCoE トラフィックに影響はありません。
ステップ 4	（任意） switch(config-if)# **no shutdown lan**	インターフェイス上のイーサネット トラフィックを再び有効にします。

FC-Map の設定

Note ファブリックの分離を維持し、FC-MAP のデフォルトを残すには、VLAN への VSAN のマッピング方式を使用することをお勧めします。

対象となる Cisco Nexus デバイスのファイバ チャネル ファブリックを識別するための FC-Map を設定することにより、ファブリック間の通信に伴うデータの破損を防ぐことができます。FC-Map が設定されると、現在のファブリックの一部ではない MAC アドレスがスイッチによって廃棄されます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **fcoe fcmap** *fabric-map*
3. (Optional) switch(config)# **no fcoe fcmap** *fabric-map*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **fcoe fcmap** *fabric-map*	グローバルFC-Mapを設定します。デフォルト値は、0E.FC.00 です。有効な範囲は、0E.FC.00 ～ 0E.FC.FF です。
ステップ 3	(Optional) switch(config)# **no fcoe fcmap** *fabric-map*	グローバル FC-Map をデフォルト値の 0E.FC.00 にリセットします。

Example

次に示すのは、グローバル FC-Map の設定例です。

```
switch# configure terminal
switch(config)# fcoe fcmap 0x0efc2a
```

ファブリック プライオリティの設定

Cisco Nexus デバイスはプライオリティをアドバタイズします。ファブリック内の CNA では、このプライオリティを基に、接続先として最適なスイッチが決定されます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **fcoe fcf-priority** *fabric-priority*
3. (Optional) switch(config)# **no fcoe fcf-priority** *fabric-priority*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **fcoe fcf-priority** *fabric-priority*	グローバル ファブリック プライオリティを設定します。デフォルト値は 128 です。有効な範囲は、0（高い）～ 255（低い）です。

	Command or Action	Purpose
ステップ 3	(Optional) switch(config)# **no fcoe fcf-priority** *fabric-priority*	グローバル ファブリック プライオリティをデフォルト値である 128 にリセットします。

Example

次に示すのは、グローバル ファブリック プライオリティの設定例です。

```
switch# configure terminal
switch(config)# fcoe fcf-priority 42
```

ジャンボ MTU の設定

次の例は、ジャンボ MTU をサポートするようにデフォルトのイーサネット システム クラスを設定する方法を示しています。

```
switch(config)# policy-map type network-qos jumbo
switch(config-pmap-nq)# class type network-qos class-fcoe
switch(config-pmap-c-nq)# pause no-drop
switch(config-pmap-c-nq)# mtu 2158
switch(config-pmap-nq)# class type network-qos class-default
switch(config-pmap-c-nq)# mtu 9216
switch(config-pmap-c-nq)# exit
switch(config-pmap-nq)# exit
switch(config)# system qos
switch(config-sys-qos)# service-policy type qos input fcoe-default-in-policy
switch(config-sys-qos)# service-policy type queuing input fcoe-default-in-policy
switch(config-sys-qos)# service-policy type queuing output fcoe-default-out-policy
switch(config-sys-qos)# service-policy type network-qos jumbo
```

アドバタイズメント間隔の設定

スイッチ上で、ファイバ チャネル ファブリックのアドバタイズメント間隔を設定できます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **fcoe fka-adv-period** *interval*
3. (Optional) switch(config)# **no fcoe fka-adv-period** *interval*

DETAILED STEPS

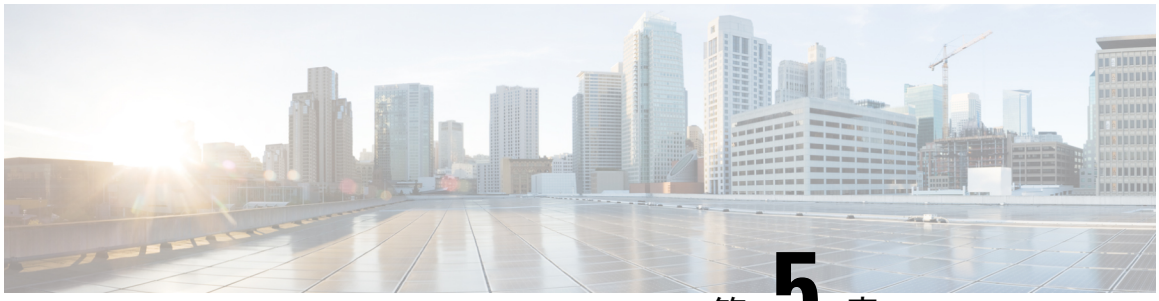
Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **fcoe fka-adv-period** *interval*	ファブリックのアドバタイズメント間隔を設定します。デフォルト値は 8 秒です。有効な範囲は 4 ～ 60 秒です。
ステップ 3	(Optional) switch(config)# **no fcoe fka-adv-period** *interval*	ファブリックのアドバタイズメント間隔を、デフォルト値の 8 秒にリセットします。

Example

次の例は、ファブリックのアドバタイズメント間隔を設定する方法を示したものです。

```
switch# configure terminal
switch(config)# fcoe fka-adv-period 42
```



第 5 章

FCoE の設定

この章は、次の内容で構成されています。

FCoE のトポロジ

直接接続された CNA のトポロジ

Cisco Nexus デバイスは、次の図のようにファイバ チャネル フォワーダ（FCF）として配置できます。

図 *1* : 直接接続された *FCF*

FCF が FCoE ノード（ENode）と他の FCF との間の中継に使用されないようにするため、FIP フレームは次のルールに従って処理されます。この処理により、異なるファブリック内の ENode と FCF との間のログイン セッションも回避されます。

- CNA から受信された FIP の送信要求フレームおよびログイン フレームは FCF により処理され、転送されません。
- FCF が他の FCF からインターフェイスを介して送信要求およびアドバタイズメントを受信すると、次のような処理が実行されます。
  - フレーム内の FC-MAP 値が FCF の FC-MAP 値と一致する（FCF が同一のファブリック内にある）場合、これらのフレームは無視され、廃棄されます。
  - FIP フレーム内の FC-MAP 値が FCF の FC-MAP 値と一致しない（FCF が異なるファブリック内にある）場合、インターフェイスが「FCoE 孤立」状態になります。

中継用の Cisco Nexus FCF を経由した場合に限って到達可能な FCF については、CNA から検出することもログインすることもできません。ハードウェアの制約上、Cisco Nexus デバイスでは、CNA と他の FCF との間の FCoE 中継機能は実行できません。

Cisco Nexus FCF では FCoE 中継機能が実行できないため、FCoE VLAN のアクティブな Spanning Tree Protocol（STP）パスが必ず CNA と FCF の間の直接接続されたリンクを経由するようにネットワーク トポロジを設計する必要があります。FCoE VLAN は、直接接続されたリンクに対してだけ設定するようにしてください。

リモート接続された CNA のトポロジ

Cisco Nexus デバイスは、次の図のようにリモート接続された CNA に対する FCF としては配置できますが、FIP スヌーピング ブリッジとしては配置できません。

図 *2:* リモート接続された *FCF*

FCF が ENode と他の FCF との間の中継に使用されないようにするため、FIP フレームは次のルールに従って処理されます。この処理により、異なるファブリック内の ENode と FCF との間のログイン セッションも回避されます。

- CNA から受信された FIP の送信要求フレームおよびログイン フレームは FCF により処理され、転送されません。
- FCF が他の FCF からインターフェイスを介して送信要求およびアドバタイズメントを受信すると、次のような処理が実行されます。
  - フレーム内の FC-MAP 値が FCF の FC-MAP 値と一致する（FCF が同一のファブリック内にある）場合、これらのフレームは無視され、廃棄されます。
  - FIP フレーム内の FC-MAP 値が FCF の FC-MAP 値と一致しない（FCF が異なるファブリック内にある）場合、インターフェイスが「FCoE 孤立」状態になります。

Cisco Nexus FCF では FCoE 中継機能が実行できないため、FCoE VLAN のアクティブな STP パスが必ず CNA と FCF の間の直接接続されたリンクを経由するようにネットワーク トポロジを設計する必要があります。FCoE VLAN は、直接接続されたリンクに対してだけ設定するようにしてください。

FCoE のベスト プラクティス

直接接続された CNA のベスト プラクティス

次の図は、直接接続された CNA と Cisco Nexus デバイスを使用したアクセス ネットワークのベスト プラクティス トポロジを示したものです。

図 *3 :* 直接接続された *CNA*

上図の配置トポロジに対する設定のベスト プラクティスは次のとおりです。

1. SAN 内の仮想ファブリック（VSAN）ごとにトラフィックを伝送できるよう、それぞれの統合アクセス スイッチに一意の専用 VLAN を設定する必要があります（VSAN 1 用に VLAN 1002、VSAN 2 用に VLAN 1003 など）。マルチ スパニングツリー（MST）を有効にした場合は、FCoE VLAN に対して別個の MST インスタンスを使用する必要があります。
2. ユニファイド ファブリック（UF）リンクをトランク ポートとして設定する必要があります。ネイティブ VLAN として FCoE VLAN を設定しないでください。仮想ファイバ チャネル インターフェイスの VF_Port トランキングおよび VSAN 管理を拡張できるよう、すべての FCoE VLAN を UF リンクのメンバとして設定する必要があります。

（注） イーサネット トラフィックおよび FCoE トラフィックはどちらも、統合ワイヤにより伝送されます。

3. UF リンクをスパニングツリー エッジ ポートとして設定する必要があります。
4. FCoE トラフィックの伝送用として指定されていないイーサネット リンクのメンバとして FCoE VLAN を設定しないでください。これは、FCoE VLAN に使用する STP のスコープを UF リンクに限定する必要があるためです。
5. LAN の代替パス用に（同一または別の SAN ファブリックにある）統合アクセス スイッチをイーサネット リンク経由で相互に接続する必要がある場合は、すべての FCoE VLAN をメンバーシップから除外することを、これらのリンクに対して明示的に設定する必要があります。この設定により、FCoE VLAN に使用する STP のスコープが UF リンクに限定されます。
6. SAN-A および SAN-B の FCoE に対してはそれぞれ別々の FCoE VLAN を使用する必要があります。

（注） 直接接続されたトポロジでは、すべての Gen-1（pre-FIP）CNA および Gen-2（FIP）CNA がサポートされています。

リモート接続された CNA のベスト プラクティス

次の図は、リモート接続された CNA と Cisco Nexus デバイスを使用したアクセス ネットワークのベスト プラクティス トポロジを示したものです。

図 *4:* リモート接続された *CNA*

上図の配置トポロジに対する設定のベスト プラクティスは次のとおりです。

1. SAN 内の仮想ファブリック（VSAN）ごとにトラフィックを伝送できるよう、それぞれの統合アクセス スイッチに一意の専用 VLAN を設定する必要があります（VSAN 1 用に VLAN 1002、VSAN 2 用に VLAN 1003 など）。MST を有効にした場合は、FCoE VLAN に対して別個の MST インスタンスを使用する必要があります。
2. ユニファイド ファブリック（UF）リンクをトランク ポートとして設定する必要があります。ネイティブ VLAN として FCoE VLAN を設定しないでください。仮想ファイバ チャネル インターフェイスの VF_Port トランキングおよび VSAN 管理を拡張できるよう、すべての FCoE VLAN を UF リンクのメンバとして設定する必要があります。

（注） イーサネット トラフィックおよび FCoE トラフィックはどちらも、ユニファイド ファブリック リンクにより伝送されます。

3. CNA およびブレード スイッチを、スパニングツリー エッジ ポートとして設定する必要があります。
4. 新しいリンクやブレード スイッチのプロビジョニングなど、さまざまなイベントに伴って実行される STP の再コンバージェンスの際に障害が発生しないよう、各ブレード スイッチは、（できれば EtherChannel を介して）ただ 1 つの Cisco Nexus 統合アクセス スイッチに接続される必要があります。
5. Cisco Nexus 統合アクセス スイッチには、それに接続されているブレード スイッチよりも高い STP プライオリティを設定する必要があります。そうすることで、統合アクセス スイッチがスパニングツリーのルートであり、かつそれに接続されているすべてのブレード スイッチがダウンストリーム ノードとなるような FCoE VLAN のアイランドを作成できます。
6. FCoE トラフィックの伝送用として指定されていないイーサネット リンクのメンバとして FCoE VLAN を設定しないでください。これは、FCoE VLAN に使用する STP のスコープを UF リンクに限定する必要があるためです。
7. LAN の代替パス用に、統合アクセス スイッチやブレード スイッチをイーサネット リンク経由で相互に接続する必要がある場合は、これらのリンクに対してすべての FCoE VLAN をメンバーシップから除外することを、明示的に設定する必要があります。この設定により、FCoE VLAN に使用する STP のスコープが UF リンクに限定されます。
8. SAN-A および SAN-B の FCoE に対してはそれぞれ別々の FCoE VLAN を使用する必要があります。

（注） リモート接続されたトポロジは、Gen-2、Gen-3、Gen-4（FIP）CNA に限ってサポートされます。

注意事項と制約事項

FC/FCoE には、次のガイドラインと制約事項があります。

- Cisco Nexus デバイスの FCoE は、Gen-1（pre-FIP）CNA および Gen-2（FIP）CNA 2 をサポートします。Cisco Nexus 2232PP ファブリック エクステンダ（FEX）の FCoE では、Gen-2 CNA に限りサポートされています。
- VLAN 1 では FCoE をイネーブルにできません。
- LLDP はデフォルトでは有効になっていないため、FCoE を有効にするには、**feature lldp** を使用して LLDP 機能を有効にする必要があります。
- 同一の FEX に対して、ストレート型とアクティブ-アクティブを組み合わせたトポロジはサポートされていません。
- FCOE は、銅線 SFP ではサポートされていません。
- FC/FCoE 構成はロールバックをサポートしていません。FC/FCoE 構成が存在する場合は、ベストエフォート オプションを使用します。他のすべての構成は成功しますが、FC/FCoE 構成ではエラー メッセージが表示されます。
- FCoE は 10 ギガビット、25 ギガビット、40 ギガビットおよび 100 ギガビット イーサネット インターフェイスでサポートされます。100G ブレイクアウト (4x25G) および 40G ブレイクアウト (4x10G) は、FCoE インターフェイスでサポートされています。
- Cisco Nexus デバイス インターフェイスのポート チャネルでは、複数のインターフェイスが設定されている場合、直接接続 FCoE（つまりバインドインターフェイスを介して CNA に直接接続された FCoE）はサポートされていません。単一リンクのポート チャネル上では、直接接続 FCoE がサポートされています。これにより、1 つの 10/25/40/100 GB リンクを持つ仮想ポート チャネル（vPC）を介して各アップストリーム スイッチに接続された CNA からの FCoE を実現できます。
- vFC に使用されるイーサネット インターフェイスでは、グローバルに定義されたデフォルトまたはカスタム ポリシーに関係なく、QOS ポリシーを手動で設定する必要があります。

（注） FC/FCoE のデフォルトの Quality of Service（QoS）ポリシーの説明については、ご使用のデバイスの Quality of Service についてのガイドを参照してください。ご使用の Nexus ソフトウェア リリース版を参照してください。このマニュアルの入手可能なバージョンは、次のサイトから取得できます：https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-installation-and-configuration-guides-list.html

FC/FCoE の構成

TCAM カービングの実行

ここでは、TCAM カービングの実行方法について説明します。

手順の概要

1. 機能 FCoE をインストールします。
2. fcoeが完全に機能するように、次のコマンドを設定します（まだ設定されていない場合）。
3. TCAM カービングを実行します。
4. 設定された TCAM リージョン サイズを確認するには、**show hardware access-list tcam region** コマンドを使用します。
5. 構成を保存し、コマンド **reload** を使用して、スイッチをリロードします。

手順の詳細

手順

ステップ 1 機能 FCoE をインストールします。

```
switch(config)# install feature-set fcoe
    switch(config)# switch(config)# feature-set fcoe
```

ステップ 2 fcoe が完全に機能するように、次のコマンドを設定します（まだ設定されていない場合）。

```
hardware access-list tcam region ing-ifacl 256
hardware access-list tcam region ing-redirect 256
```

256 は、FC/FCoE の ing-ifacl および ing-redirect リージョンに必要な最小 tcam スペースです。

（注）
現在の tcam の構成を確認するには、`show hardware access-list tcam region` コマンドを使用します。

必要な tcam スペースが使用できない場合は、`hardware access-list tcam region ing-racl 1536` コマンドを使用して ing-racl リージョンを縮小できます。

ステップ 3 TCAM カービングを実行します。

例：

```
Switch(config)# hardware access-list tcam region ing-racl 1536
Switch(config)# hardware access-list tcam region ing-ifacl 256
Switch(config)# hardware access-list tcam region ing-redirect 256
```

ステップ 4 設定された TCAM リージョン サイズを確認するには、**show hardware access-list tcam region** コマンドを使用します。

例：

```
Switch(config)# show hardware access-list tcam region
Switch(config)#
```

ステップ 5 構成を保存し、コマンド **reload** を使用して、スイッチをリロードします。

例：

```
Switch(config)# reload
Switch(config)#
```

次のタスク

TCAM のカービング後には、スイッチをリロードする必要があります。

LLDP の構成

ここでは、LLDP の設定方法について説明します。

手順の概要

1. **configure terminal**
2. [**no**] **feature lldp**

手順の詳細

手順

ステップ 1 **configure terminal**

グローバル設定モードを開始します。

ステップ 2 [**no**] **feature lldp**

デバイス上でLLDPをイネーブルまたはディセーブルにします。LLDPはデフォルトでディセーブルです。

デフォルトQoSの設定

FCoE のデフォルト ポリシーには、ネットワーク QoS、出力キューイング、入力キューイング、QoS の 4 種類があります。FCoE デフォルト ポリシーを有効にするには、**feature-set fcoe command** コマンドを使用して FCoE NPV 機能を有効にします。デフォルトの QoS 入力ポリシーである **default-fcoe-in-policy** は、すべてのFCおよびSAN ポート チャネル インターフェイ

スに暗黙的に付加され、FCからFCoEへのトラフィックを可能にします。これは、**show interface** {*fc slot/port* | *san-port-channel <no>*} **all** を使用して確認できます。デフォルトの QoS ポリシーは、すべての FC および FCoE トラフィックに CoS3 および Q1 を使用します。

ユーザー定義の QoS の構成

FCoE トラフィックに別のキューまたは CoS 値を使用するには、ユーザー定義のポリシーを作成します。トラフィックが異なるキューまたはCoSを使用できるようにするには、ユーザー定義の QoS 入力ポリシーを作成し、FC インターフェイスと FCoE インターフェイスの両方に明示的にアタッチする必要があります。ユーザー定義の QoS ポリシーを作成し、システム全体の QoS に対してアクティブにする必要があります。

（注） FCoE をサポートするには、イーサネットまたはポート チャネル インターフェイスを MTU 9216 (または使用可能な最大 MTU サイズ) で構成する必要があります。

次の例は、すべての FC および FCoE トラフィックに CoS3 および Q2 を使用するユーザー定義の QoS ポリシーを設定し、アクティブにする方法を示しています。

- ユーザー定義のネットワーク QoS ポリシーの設定：

```
switch(config)# policy-map type network-qos fcoe_nq
switch(config-pmap-nqos)# class type network-qos c-nq1
switch(config-pmap-nqos-c)# mtu 1500
switch(config-pmap-nqos-c)# class type network-qos c-nq2
switch(config-pmap-nqos-c)# mtu 9216
switch(config-pmap-nqos-c)# pause pfc-cos 3
switch(config-pmap-nqos-c)# class type network-qos c-nq3
switch(config-pmap-nqos-c)# mtu 1500
switch(config-pmap-nqos-c)# class type network-qos c-nq-default
switch(config-pmap-nqos-c)# mtu 1500
switch(config-pmap-nqos-c)# exit
switch(config-pmap-nqos)# exit
switch(config)#
```

- ユーザー定義の入力キューイング ポリシーの作成：

```
switch(config)# policy-map type queuing fcoe-in-policy
switch(config-pmap-que)# class type queuing c-in-q2
switch(config-pmap-c-que)# bandwidth percent 50
switch(config-pmap-c-que)# class type queuing c-in-q-default
switch(config-pmap-c-que)# bandwidth percent 50
switch(config-pmap-c-que)# exit
switch(config-pmap-que)# exit
switch(config)
```

- ユーザー定義の出力キューイング ポリシーの作成：

```
switch(config)# policy-map type queuing fcoe-out-policy
switch(config-pmap-que)# class type queuing c-out-q3
switch(config-pmap-c-que)# priority level 1
switch(config-pmap-c-que)# class type queuing c-out-q-default
switch(config-pmap-c-que)# bandwidth remaining percent 50
switch(config-pmap-c-que)# class type queuing c-out-q1
```

```
switch(config-pmap-c-que)# bandwidth remaining percent 0
switch(config-pmap-c-que)# class type queuing c-out-q2
switch(config-pmap-c-que)# bandwidth remaining percent 50
switch(config-pmap-c-que)# exit
switch(config-pmap-que)# exit
switch(config)#
```

- ユーザー定義の QoS 入力ポリシーの作成：

```
switch(config)# class-map type qos match-any fcoe
switch(config-cmap-qos)# match protocol fcoe
switch(config-cmap-qos)# match cos 3
switch(config-cmap-qos)# exit
switch(config)#
switch(config)# policy-map type qos fcoe_qos_policy
switch(config-pmap-qos)# class fcoe
switch(config-pmap-c-qos)# set cos 3
switch(config-pmap-c-qos)# set qos-group 2
switch(config-pmap-c-qos)# exit
switch(config-pmap-qos)# exit
switch(config)#
```

- ユーザー定義のシステム QoS ポリシーのアクティブ化：

```
switch(config)# system qos
switch(config-sys-qos)# service-policy type queuing input fcoe-in-policy
switch(config-sys-qos)# service-policy type queuing output fcoe-out-policy
switch(config-sys-qos)# service-policy type network-qos fcoe_nq
switch(config-sys-qos)# exit
switch(config)#
```

- FC または FCoE インターフェイスへの QoS 入力ポリシーの適用：

```
switch# conf
switch(config)# interface {fc <slot>/<port> | ethernet <slot>/<port> | san-port-channel
 <no> | port-channel <no>}
switch(config-if)# service-policy type qos input fcoe_qos_policy
```

- FC または FCoE インターフェイスからの QoS 入力ポリシーの削除：

```
switch# conf
switch(config)# interface {fc <slot>/<port> | ethernet <slot>/<port> | san-port-channel
 <no> | port-channel <no>}
switch(config-if)# no service-policy type qos input fcoe_qos_policy
```

- FC または FCoE インターフェイスに適用される QoS 入力ポリシーの確認：

```
switch# show running-config interface {fc <slot>/<port> | interface <slot>/<port> |
 san-port-channel <no> | port-channel <no>} all
```

（注）
- ユーザー定義の QoS ポリシーを使用する場合、同じ QoS 入力ポリシーをスイッチ内のすべての FC および FCoE インターフェイスに適用する必要があります。
- FCoE トラフィックは単一の CoS でのみサポートされるため、複数の QoS クラス マップで **match protocol fcoe** を設定しないでください。

トラフィック シェーピングの設定

トラフィック シェーピングにより、使用可能な帯域幅へのアクセスの制御、および送信されたトラフィックがリモートのターゲットインターフェイスのアクセス速度を超える場合に発生する輻輳を回避するために、トラフィックのフローを規制できます。トラフィック シェーピングはデータの伝送レートを制限するため、このコマンドは必要な場合にのみ使用できます。

次の例は、トラフィック シェーパーの構成方法を示しています。

- 次のコマンドは、すべての FC インターフェイスのデフォルトのシステム レベル設定を表示します。

```
switch(config)# show running-config all | i i rate
hardware qos fc rate-shaper
switch(config)#
```

- 次の例は、レートシェーパーの構成方法を示しています。このコマンドは、すべての FC インターフェイスに適用されます。

（注） まれに、4G、8G、16G、または 32G インターフェイスのいずれかで入力廃棄が発生することがあります。レートシェープを設定するには、*hardware qos fc rate-shaper [low]* コマンドを使用します。これはシステム レベルの設定であるため、すべての FC ポートに適用され、すべての FC ポートのレートが低下します。*hardware qos fc rate-shaper* コマンドのデフォルト オプションは、すべての FC インターフェイスに適用できます。

```
switch(config)# hardware qos fc rate-shaper low
switch(config)#
switch(config)#end
```

vPC を伴う FCoE の設定例

Cisco NX-OS リリース 9.3(5) 以降、Cisco Nexus N9K-93180YC-FX デバイスは vPC をサポートし、Cisco NX-OS リリース 10.1(1) 以降、Cisco Nexus N9K-C93360YC-FX2 デバイスも vPC をサポートします。Cisco Nexus N9K-93180YC-FX、N9K-C9336C-FX2-E、および N9K-C93360YC-FX2

デバイスはvPCをサポートします。vPCscanは、帯域幅を増やし、イーサネットファブリックへのロードバランシングを強化するように設定できます。次に、Cisco Nexus 9000 シリーズスイッチで vPC を使用するときに FCoE を設定する方法を説明する設定例を示します。

図 *5 :* ホスト *vPC* での *FCoE* トラフィック フロー

図 *6 : Nexus 9000 FCoE* および *vPC* ラボ トポロジ

（注） FCoE VLAN は、vPC ピア リンク間でトランキングしないでください。

（注） コア スイッチに接続する Cisco Nexus N9K-93180YC-FX スイッチ（スイッチモード）では、FC アップリンクのみがサポートされます。

設定例では、次のパラメータが含まれています。

```
switchname: tme-switch-1
switchname: tme-switch-2
mgmt ip: 172.25.182.66
mgmt ip: 172.25.182.67
```

設定例には、次のハードウェアが含まれています。

- Dell サーバ PE2950
- Emulex CNA または CISCO CNA
- Cisco NX-OS リリース 9.3(5)10.2(1)F 以降のリリースを実行している 2 つの Cisco Nexus 9000 スイッチ。

設定例は次の考慮事項と要件を含んでいます。

- DCBX をサポートする第 2 世代 CNA が必要です。
- 別のスイッチへの単一のホスト CNA ポート チャネル接続。単一スイッチのポート チャネルで、ポート チャネルまたは vPC に複数のメンバー ポートが含まれている場合、FCoE インターフェイスは機能しません。
- Cisco NX-OS リリース 9.3(5) 10.2(1)F 以降のリリース。
- FCoEを実行するには、FC機能パッケージが必要です。これがインストールされていない場合、90 日持続する一時ライセンスがあります。

Cisco Nexus 9000 シリーズ スイッチの vPC の設定例

この例では、基本設定（IP アドレス（mgmt0）、スイッチ名、管理者のパスワードなど）がスイッチで完了していると仮定します。

（注） 設定は、vPC トポロジの両方のピア スイッチで実行する必要があります。

手順の概要

1. **feature vpc**
2. **vPC domain**
3. **vpc peer-link**
4. **show vpc peer-keepalive**
5. **int po**
6. **vpc**
7. **show vpc statistics**

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	**feature vpc** 例： `tme-switch-1# conf t` `Enter configuration commands, one per line. End with CNTL/Z.` `tme-switch-1(config)# feature vpc` `tme-switch-1(config)#` `tme-switch-2# conf t` `Enter configuration commands, one per line. End with CNTL/Z.` `tme-switch-2(config)# feature vpc` `tme-switch-2(config)#`	両方のピア スイッチで vPC 機能をイネーブルにします。
ステップ 2	**vPC domain** 例： `tme-switch-1(config)# vpc domain 2` `tme-switch-1(config-vpc-domain)# peer-keepalive destination 192.165.200.230` `tme-switch-2(config)# vpc domain 2` `tme-switch-2(config-vpc-domain)# peer-keepalive destination 192.165.200.229`	vPC ドメインおよびピアのキープアライブの宛先を設定します。 （注） この設定では、スイッチ tme-switch-1 の管理 IP アドレスは 192.165.200.229、スイッチ tme-switch-2 の管理 IP アドレスは 192.165.200.230 です。

	コマンドまたはアクション	目的
ステップ 3	**vpc peer-link** 例： `tme-switch-1(config)# int port-channel 1` `tme-switch-1(config-if)# vpc peer-link` （注） vPC ピアリンクでは、スパニングツリー ポート タイプは、ネットワーク ポート タイプに変更されます。これにより、STPブリッジ保証（デフォルトでイネーブル）がディセーブルでなければ、vPC ピアリンクの STP ブリッジ保証がイネーブルになります。 `tme-switch-2(config)# int port-channel 1` `tme-switch-2(config-if)# vpc peer-link`	vPC ピアリンクとして使用するポート チャネル インターフェイスを設定します。
ステップ 4	**show vpc peer-keepalive** 例： `tme-switch-1(config)# show vpc peer-keepalive` `vPC keep-alive status : peer is alive` `--Destination : 172.25.182.167` `--Send status : Success` `--Receive status : Success` `--Last update from peer : (0) seconds, (975) msec` `tme-switch-1(config)#` `tme-switch-2(config)# show vpc peer-keepalive` `--PC keep-alive status : peer is alive` `--Destination : 172.25.182.166` `--Send status : Success` `--Receive status : Success` `--Last update from peer : (0) seconds, (10336) msec` `tme-switch-2(config)#`	ピア キープアライブに到達できることを確認します。
ステップ 5	**int po** 例： `tme-switch-1(config-if-range)# int po 1` `tme-switch-1(config-if)# switchport mode trunk` `tme-switch-1(config-if)# no shut` `tme-switch-1(config-if)# exit` `tme-switch-1(config)# int eth 1/39-40` `tme-switch-1(config-if-range)# switchport mode trunk` `tme-switch-1(config-if-range)# channel-group 1` `tme-switch-1(config-if-range)# no shut` `tme-switch-1(config-if-range)#` `tme-switch-2(config-if-range)# int po 1` `tme-switch-2(config-if)# switchport mode trunk`	vPC ピア リンク ポート チャネルにメンバー ポートを追加し、このポート チャネル インターフェイスを起動します。

	コマンドまたはアクション	目的
	tme-switch-2(config-if)# no shut tme-switch-2(config-if)# exit tme-switch-2(config)# int eth 1/39-40 tme-switch-2(config-if-range)# switchport mode trunk tme-switch-2(config-if-range)# channel-group 1 tme-switch-2(config-if-range)# no shut tme-switch-2(config-if-range)# tme-switch-1(config-if-range)# show int po1 port-channel 1 is up Hardware: Port-Channel, address: 000d.ecde.a92f (bia 000d.ecde.a92f) MTU 1500 bytes, BW 20000000 Kbit, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA Port mode is trunk full-duplex, 10 Gb/s Beacon is turned off Input flow-control is off, output flow-control is off Switchport monitor is off Members in this channel: Eth1/39, Eth1/40 Last clearing of "show interface" counters never 1 minute input rate 1848 bits/sec, 0 packets/sec 1 minute output rate 3488 bits/sec, 3 packets/sec tme-switch-1(config-if-range)# tme-switch-2(config-if-range)# show int po1 port-channel1 is up Hardware: Port-Channel, address: 000d.ecdf.5fae (bia 000d.ecdf.5fae) MTU 1500 bytes, BW 20000000 Kbit, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA Port mode is trunk full-duplex, 10 Gb/s Beacon is turned off Input flow-control is off, output flow-control is off Switchport monitor is off Members in this channel: Eth1/39, Eth1/40 Last clearing of "show interface" counters never minute input rate 1848 bits/sec, 0 packets/sec minute output rate 3488 bits/sec, 3 packets/sec tme-switch-2(config-if-range)#	
ステップ 6	**vpc** 例： tme-switch-1(config)# int po 11 tme-switch-1(config-if)# vpc 11 tme-switch-1(config-if)# switchport mode trunk tme-switch-1(config-if)# no shut tme-switch-1(config-if)# int eth 1/1 tme-switch-1(config-if)# switchport mode trunk tme-switch-1(config-if)# channel-group 11 tme-switch-1(config-if)# spanning-tree port type edge trunk tme-switch-1(config-if)#	vPC を作成し、メンバー インターフェイスを追加します。 （注） vPC トポロジを介した FCoE を実行するには、ポート チャネルは単一のメンバー インターフェイスだけを持っている必要があります。 （注） ポート チャネル インターフェイスの下に設定された vPC 番号は、両方の Nexus 9000 スイッチで一致

	コマンドまたはアクション	目的
	警告 エッジポートタイプ（PortFast）は、単一のホストに接続されているポートだけでイネーブルにする必要があります。エッジポートタイプ（PortFast）がイネーブルの場合、このインターフェイスにハブ、コンセントレータ、スイッチ、ブリッジなどの一部のデバイスを接続すると、一時的なブリッジングループが発生することがあります。このタイプの設定は、慎重に行う必要があります。 `tme-switch-2(config)# int po 11` `tme-switch-2(config-if)# vpc 11` `tme-switch-2(config-if)# switchport mode trunk` `tme-switch-2(config-if)# no shut` `tme-switch-2(config-if)# int eth 1/1` `tme-switch-2(config-if)# switchport mode trunk` `tme-switch-2(config-if)# channel-group 11` `tme-switch-2(config-if)# spanning-tree port type edge trunk` 警告 エッジポートタイプ（PortFast）は、単一のホストに接続されているポートだけでイネーブルにする必要があります。エッジポートタイプ（PortFast）がイネーブルの場合、このインターフェイスにハブ、コンセントレータ、スイッチ、ブリッジなどの一部のデバイスを接続すると、一時的なブリッジングループが発生することがあります。このタイプの設定は、慎重に行う必要があります。	する必要があります。ポートチャネルインターフェイス番号が両方のスイッチで一致している必要はありません。
ステップ 7	**show vpc statistics** 例： `tme-switch-1(config-if)# show vpc statistics vpc 11` `port-channel11 is up` `vPC Status: Up, vPC number: 11` `Hardware: Port-Channel, address: 000d.ecde.a908 (bia 000d.ecde.a908)` `MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,` `reliability 255/255, txload 1/255, rxload 1/255` `Encapsulation ARPA` `Port mode is trunk` `full-duplex, 10 Gb/s` `Beacon is turned off` `Input flow-control is off, output flow-control is off` `Switchport monitor is off` `Members in this channel: Eth1/1` `Last clearing of "show interface" counters never` `minute input rate 4968 bits/sec, 8 packets/sec` `minute output rate 792 bits/sec, 1 packets/sec` `tme-switch-1(config-if)#`	vPC インターフェイスが起動していて、動作していることを確認します。

	コマンドまたはアクション	目的
	tme-switch-2(config-if)# show vpc statistics vpc 11 port-channel11 is up vPC Status: Up, vPC number: 11 Hardware: Port-Channel, address: 000d.ecdf.5fae (bia 000d.ecdf.5fae) MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA Port mode is trunk full-duplex, 10 Gb/s Beacon is turned off Input flow-control is off, output flow-control is off Switchport monitor is off Members in this channel: Eth1/1 Last clearing of "show interface" counters never minute input rate 4968 bits/sec, 8 packets/sec minute output rate 792 bits/sec, 1 packets/sec tme-switch-1(config-if)#	

Cisco Nexus 9000 シリーズ スイッチの FCoE の設定例

2 つの Nexus 9000 スイッチ間に vPC をセットアップしたら、FCoE トポロジを設定できます。この手順では、IP アドレス（mgmt0）、スイッチ名、パスワード、管理者などを指定する基本設定が Nexus 9000 スイッチ上で実施済みであり、前のセクションに従って vPC 設定が完了していると想定しています。次の手順では、vPC トポロジとともに FCoE トポロジをセットアップするために必要な FCoE の基本設定を行います。

手順の概要

1. **install feature-set fcoe**
2. **feature-set fcoe**
3. **vsan database**
4. **interface port-channel**
5. **int vfc**
6. **show int brief**
7. **show flogi database**
8. **show vpc statistics**

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	**install feature-set fcoe**	FCoE 機能をインストールします。
ステップ 2	**feature-set fcoe** 例：	Cisco Nexus 9000 スイッチで FCoE を有効にします。 （注）

	コマンドまたはアクション	目的
	tme-switch-1(config)# feature-set fcoe Please configure the following for fcoe to be fully functional: - hardware access-list tcam region ing-racl TCAM size - hardware access-list tcam region ing-ifacl TCAM size - hardware access-list tcam region ing-redirect TCAM size tme-switch-1(config)# tme-switch-2(config)# feature-set fcoe Please configure the following for fcoe to be fully functional: - hardware access-list tcam region ing-racl TCAM size - hardware access-list tcam region ing-ifacl TCAM size - hardware access-list tcam region ing-redirect TCAM size tme-switch-2(config)#	これが完了するまでに数分かかることがあります。この手順を実行する前に、TCAM カービングを完了する必要があります。TCAM カービングの完了後には、スイッチをリロードする必要があります。
ステップ 3	**vsan database** 例： tme-switch-1(config)# vsan database tme-switch-1(config-vsan-db)# vsan 100 tme-switch-1(config-vsan-db)# exit tme-switch-1(config)# vlan 100 tme-switch-1(config-vlan)# fcoe vsan 100 tme-switch-1(config-vlan)# show vlan fcoe VLAN VSAN Status -------- -------- -------- 100 100 Operational tme-switch-1(config-vlan)# tme-switch-2(config)# vsan database tme-switch-2(config-vsan-db)# vsan 101 tme-switch-2(config-vsan-db)# exit tme-switch-2(config)# vlan 101 tme-switch-2(config-vlan)# fcoe vsan 101 tme-switch-2(config-vlan)# show vlan fcoe VLAN VSAN Status -------- -------- -------- 101 101 Operational tme-switch-2(config)#	VSAN を構築して、FCoE トラフィックの伝送用として指定されている VLAN にマッピングします。 （注） VLAN 番号と VSAN 番号が同じである必要はありません。
ステップ 4	**interface port-channel** 例： tme-switch-1(config)# interface port-channel 11 tme-switch-1(config-if)# switchport trunk allowed vlan 1, 100 tme-switch-1(config-if)# mtu 9216 tme-switch-1(config-if)# service-policy type qos input default-fcoe-in-policy tme-switch-1(config-if)# show int trunk —————————————————————————— Port Native Status Port	vPC リンクの通過を許可される VLAN を設定します。

	コマンドまたはアクション	目的
	`` -- Eth1/1 1 trnk-bndl Po11 Eth1/39 1 trnk-bndl Po1 Eth1/40 1 trnk-bndl Po1 Po1 1 trunking -- Po11 1 trunking -- -- Port Vlans Allowed on Trunk -- Eth1/1 1,100 Eth1/39 1-3967,4048-4093 Eth1/40 1-3967,4048-4093 Po1 1-3967,4048-4093 Po11 1,100 -- Port Vlans Err-disabled on Trunk -- Eth1/1 none Eth1/39 100 Eth1/40 100 Po1 100 Po11 none -- Port STP Forwarding -- Eth1/1 none Eth1/39 none Eth1/40 none Po1 1 Po11 1,100 tme-switch-1(config-if)# tme-switch-2(config)# int po 11 tme-switch-2(config-if)# switchport trunk allowed vlan 1, 101 tme-switch-1(config-if)# mtu 9216 tme-switch-1(config-if)# service-policy type qos input default-fcoe-in-policy tme-switch-2(config-if)# show int trunk -- Port Native Status Port -- Eth1/1 1 trnk-bndl Po11 Eth1/39 1 trnk-bndl Po1 Eth1/40 1 trnk-bndl Po1 Po1 1 trunking -- Po11 1 trunking -- -- Port Vlans Allowed on Trunk -- Eth1/1 1,101 Eth1/39 1-3967,4048-4093 Eth1/40 1-3967,4048-4093 Po1 1-3967,4048-4093 Po11 1,101 -- Port Vlans Err-disabled on Trunk ```	

	コマンドまたはアクション	目的
	`` Eth1/1 none Eth1/39 101 Eth1/40 101 Po1 101 Po11 none Port STP Forwarding Eth1/1 none Eth1/39 none Eth1/40 none Po1 1 Po11 1,101 tme-switch-2(config-if)# ```	
ステップ 5	**int vfc** 例： ``` tme-switch-1(config)# int vfc 1 tme-switch-1(config-if)# bind interface po11 tme-switch-1(config-if)# no shut tme-switch-1(config-if)# tme-switch-2(config)# int vfc 1 tme-switch-2(config-if)# bind interface po11 tme-switch-2(config-if)# no shut tme-switch-2(config-if)# tme-switch-1(config)# vsan database tme-switch-1(config-vsan-db)# vsan 100 interface vfc 1 tme-switch-1(config)# show vsan membership vsan 1 interfaces: fc2/1 fc2/2 fc2/3 fc2/4 fc2/5 fc2/6 fc2/7 fc2/8 vsan 100 interfaces: vfc1 vsan 4079(evfp_isolated_vsan) interfaces: vsan 4094(isolated_vsan) interfaces: tme-switch-1(config)# tme-switch-2(config)# vsan database tme-switch-2(config-vsan-db)# vsan 101 interface vfc 1 tme-switch-2(config)# show vsan membership vsan 1 interfaces: fc2/1 fc2/2 fc2/3 fc2/4 fc2/5 fc2/6 fc2/7 fc2/8 vsan 101 interfaces: vfc1 vsan 4079(evfp_isolated_vsan) interfaces: ```	仮想ファイバ チャネル インターフェイス（vfc）を構築し、前のステップで構築したVSANに追加します。

	コマンドまたはアクション	目的
	vsan 4094(isolated_vsan) interfaces: tme-switch-2(config)#	
ステップ 6	**show int brief** 例： tme-switch-1(config-if)# show int brief —————————————————————————— Ethernet VLAN Type Mode Status Reason Speed —————————————————————————— Eth1/1 1 eth trunk up none 10G(D) Eth1/2 1 eth access up none 10G(D) Eth1/38 1 eth access down SFP not inserted 10G(D) Eth1/39 1 eth trunk up none 10G(D) Eth1/40 1 eth trunk up none 10G(D) —————————————————————————— Port-channel VLAN Type Mode Status Reason Speed —————————————————————————— Po1 1 eth trunk up none a-10G(D) none Po11 1 eth trunk up none a-10G(D) none —————————————————————————— Port VRF Status IP Address Speed MTU —————————————————————————— mgmt0 -- up 172.25.182.166 1000 1500 —————————————————————————— Interface Vsan Admin Admin Status SFP Oper Oper Port —————————————————————————— vfc1 100 F on up -- F auto -- tme-switch-1(config-if)# tme-switch-2(config-if)# show int brief —————————————————————————— Ethernet VLAN Type Mode Status Reason Speed Port —————————————————————————— Eth1/1 1 eth trunk up none 10G(D) 11 Eth1/2 1 eth access up none 10G(D) -- Eth1/38 1 eth access down SFP not inserted 10G(D) -- Eth1/39 1 eth trunk up none 10G(D) 1 Eth1/40 1 eth trunk up none 10G(D) 1 —————————————————————————— Port-channel VLAN Type Mode Status Reason Speed Protocol —————————————————————————— Po1 1 eth trunk up none a-10G(D) none Po11 1 eth trunk up none a-10G(D) none —————————————————————————— Port VRF Status IP Address Speed MTU —————————————————————————— mgmt0 -- up 172.25.182.167 1000 1500 —————————————————————————— Interface Vsan Admin Admin Status SFP Oper Oper ——————————————————————————	vfc が起動し、動作していることを確認します。

	コマンドまたはアクション	目的
	vfc1 101 F on up -- F auto -- tme-switch-2(config-if)#	
ステップ 7	**show flogi database** 例： tme-switch-1# show flogi database INTERFACE VSAN FCID PORT NAME NODE NAME vfc1 100 0x540000 21:00:00:c0:dd:11:2a:01 20:00:00:c0:dd:11:2a:01 Total number of flogi = 1. tme-switch-2# show flogi database INTERFACE VSAN FCID PORT NAME NODE NAME vfc1 101 0x540000 21:00:00:c0:dd:11:2a:01 20:00:00:c0:dd:11:2a:01 Total number of flogi = 1.	仮想ファイバ チャネル インターフェイスがファブリックにログインしたことを確認します。
ステップ 8	**show vpc statistics** 例： tme-switch-1(config-if)# show vpc statistics vpc 11 port-channel11 is up vPC Status: Up, vPC number: 11 Hardware: Port-Channel, address: 000d.ecde.a908 (bia 000d.ecde.a908) MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA Port mode is trunk full-duplex, 10 Gb/s Beacon is turned off Input flow-control is off, output flow-control is off Switchport monitor is off Members in this channel: Eth1/1 Last clearing of "show interface" counters never 1 minute input rate 4968 bits/sec, 8 packets/sec 1 minute output rate 792 bits/sec, 1 packets/sec tme-switch-2(config-if)# show vpc statistics vpc 11 port-channel11 is up vPC Status: Up, vPC number: 11 Hardware: Port-Channel, address: 000d.ecdf.5fae (bia 000d.ecdf.5fae) MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA Port mode is trunk full-duplex, 10 Gb/s Beacon is turned off Input flow-control is off, output flow-control is off	vPC が起動し、動作していることを確認します。

	コマンドまたはアクション	目的
	Switchport monitor is off Members in this channel: Eth1/1 Last clearing of "show interface" counters never 1 minute input rate 4968 bits/sec, 8 packets/sec 1 minute output rate 792 bits/sec, 1 packets/sec	

QoS の構成

QoS を設定するには、システム サービス ポリシーをアタッチする必要があります。**service-policy** コマンドは、システムのサービス ポリシーとしてシステム クラス ポリシー マップを指定します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **system qos**
3. switch(config-sys-qos)# **service-policy type** {**network-qos** | **qos** | **queuing**} [**input** | **output**] *fcoe default policy-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)# **system qos**	システム QoS 構成 モードを開始します。
ステップ 3	switch(config-sys-qos)# **service-policy type** {**network-qos** | **qos** | **queuing**} [**input** | **output**] *fcoe default policy-name*	デフォルトの FCoE ポリシー マップをシステムのサービス ポリシーとして使用するよう指定します。FCoE には次の 4 つの定義済みポリシー マップがあります。 • service-policy type queuing input fcoe-default-in-policy • service-policy type queuing output fcoe-default-out-policy • service-policy type qos input fcoe-default-in-policy • service-policy type network-qos fcoe-default-nq-policy （注）

	コマンドまたはアクション	目的
		Cisco Nexus デバイスで FCoE をイネーブルにする前に、事前定義された FCoE ポリシー マップをタイプ qos、タイプ network-qos、およびタイプ queuing の各ポリシー マップに追加する必要があります。

TCAM カービングに関する情報

3 値連想メモリ（TCAM）カービング機能では、TCAM のデフォルト リージョン サイズの変更を可能にするテンプレートベースの手段を使用します。スイッチが起動すると、他のどんなテンプレートも設定していなければ、このデフォルト テンプレートが表示されます。次の表に、テンプレート内のさまざまなリージョンの種類とサイズを示します。

表 *3:* 事前定義済み組み込みデフォルト テンプレート

[リージョン（**Region**）]	サイズ（エントリ数）	サイズ（ブロック数）	特長
Vacl	1024	16	入力 VLAN アクセス コントロール リスト（VACL）、出力 VACL
Ifacl	1152	18 日	入力インターフェイス ACL、入力レイヤ 3 物理ポート/サブインターフェイス RACL 、すべてのポートの出力 RACL、デフォルトのコントロール プレーン ポリシング（CoPP）
QoS	448	7	入力 vlan-qos、入力 system-qos、入力 interface-qos

[リージョン（Region）]	サイズ（エントリ数）	サイズ（ブロック数）	特長
Rbacl	1152	18 日	入力レイヤ 3 スイッチ仮想インターフェイス、入力レイヤ 3 ポート チャネル/ポート チャネル サブインターフェイス ルータ アクセス コントロール リスト（RACL）、出力 Cisco Trusted Security（CTS）
スパン	64	1	スパン
Sup	256	4	Sup-rdt
合計	**4096**	**64**	

ユーザー定義テンプレートに関する情報

デフォルト テンプレートに加えて最大 16 個のテンプレートを作成できます（つまり、同時に 17 個のテンプレートを保持できるということです）。希望の 3 値連想メモリ（TCAM）リージョンにどんなサイズでも設定できます。

各テンプレートで、次の操作を実行できます。

- 作成（Create）
- 変更
- 削除
- Commit

各テンプレートは、次のうちのいずれかのステータスになっています。

- 保存済み
- コミット型

作成（Create）

テンプレートを作成する場合、TCAM リージョンのサイズはデフォルト値に初期化されます。テンプレートを作成する場合、テンプレートはデフォルトでは保存済みステートになっています。テンプレートを作成すると、これを変更してどの TCAM リージョンのサイズも変更できます。各 TCAM ブロックのサイズは 64 エントリのため、リージョンのサイズは 64 の倍数で

設定する必要があります。入力した値が 64 の倍数でなかった場合、値を再入力するように求めるエラー メッセージが表示されます。

変更

すべての保存済みテンプレートを編集してどの TCAM リージョンのサイズでも変更できますが、どの TCAM のリージョンのサイズも 0 に設定することはできません。編集中、入力したサイズが 64 の境界線にあるかがソフトウェアによってチェックされます。テンプレートを変更する場合、すべての TCAM リージョンのサイズの合計が 4096 エントリより小さくなる必要があります。変更中は、4096 エントリ未満なのかはソフトウェアではチェックされません。

テンプレートは、保存済みステートのときにのみ変更できます。テンプレートをコミットした後は編集できません。

コミット済みのユーザー定義テンプレートは、別のユーザー定義テンプレートまたはデフォルト テンプレートを提供することによって作成済みステートに変更できます。

別のユーザー定義テンプレートを提供するには、次のコマンドを入力します。

hardware profile tcam resource service-template *user-defined-template*

デフォルト テンプレートを提供するには、次のコマンドを入力します。

no hardware profile tcam resource service-template *currently-committed- template*

削除

どの保存済みテンプレートも削除できます。テンプレートを削除した後では、そのテンプレートに関するすべての情報が失われます。コミットしたテンプレートは削除できません。

コミット済みのユーザー定義テンプレートは、別のユーザー定義テンプレートまたはデフォルト テンプレートを提供することによって作成済みステートに変更できます。

別のユーザー定義テンプレートを提供するには、次のコマンドを入力します。

hardware profile tcam resource service-template *user-defined-template*

デフォルト テンプレートを提供するには、次のコマンドを入力します。

no hardware profile tcam resource service-template *currently-committed- template*

Commit

自分のユーザ定義テンプレートまたはソフトウェアで提供されているデフォルトテンプレートはどれでもコミットできます。テンプレートをコミットするには、**commit** コマンドを入力し、スイッチの再起動を行います。**commit** コマンドを入力すると、ソフトェアによってテンプレートが検証されます。検証が成功すると、スイッチを再起動するか確認するメッセージが表示されます。テンプレート（ユーザー定義またはデフォルト）は、再起動後に適用されます。再起動を選択しなかった場合、TCAM リージョンへの変更は行われず、コミットされるテンプレートはありません。

Cisco NX-OS リリース 9.3(3) 以降では、テンプレートをコミットすると、実行コンフィギュレ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スイッチをリブートするかどうかを確認するプロンプトが表示されます。続行に同意すると、次のことが行われます。

- コミットしたテンプレートがスタートアップ コンフィギュレーションに保存されます。
- スイッチが再起動します。
- コミットしたテンプレートがソフトウェアによって使用されます。
- テンプレートが実行中ステートに移行します。

（注） Cisco NX-OS リリース 9.3(3) より前では、テンプレートをコミットした後、システムは自動では再起動せず **commit** コマンドの出力にメッセージが表示され、コミットしたテンプレートを有効にするためにスイッチを再起動するか尋ねられます。

コミットされていないTCAMプロファイルを含むバックアップ コンフィギュレーションから、書き込み消去、リロード、および実行コンフィギュレーションのコピーを実行すると、次のことが発生します。

1. TCAMプロファイルがコミットされると、スイッチはプロンプトなしで自動的にリロードします。
2. TCAM カービング CLI の後の設定は適用されません。
3. コミットされた TCAM プロファイルで設定を復元するには、バックアップ コンフィギュレーションを実行コンフィギュレーションに再度コピーする必要があります。ただし、TCAMカービングプロファイルはすでにコミットされているため、スイッチのリロードはありません。

新しいコミットされたTCAMプロファイルが原因でスイッチがリロードされると、**show system reset-reason** コマンドは、次に示すようにリロードの理由を表示します。

```
switch# show system reset-reason
----- reset reason for Supervisor-module 1 (from Supervisor in slot 1) ---
1) At 302777 usecs after Sun Jan 20 22:02:37 2019
    Reason: Reload due to change in TCAM service-template
    Service:
    Version: 9.3(3)

2) At 314447 usecs after Sun Jan 20 21:52:58 2019
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 9.3(3)

3) At 20142 usecs after Sun Jan 20 21:27:33 2019
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 9.3(3)
```

スイッチを再起動後、コミットされたテンプレートがCisco Nexusサーバー上のすべてのASICに適用されます。Cisco Nexusデバイス上の別のASICに別のテンプレートをコミットできません。各テンプレートの各リージョンのサイズを指定したすべての保存済みテンプレートおよびコミット済みテンプレートは実行コンフィギュレーションに表示されます。

テンプレートがコミットされたとき、以下がチェックされます。

1. TCAM 内のすべてのリージョンの合計サイズは 4096 エントリです。
2. 各リージョンのサイズは TCAM 内に収まります。どの時点でも、TCAM リージョンに対して常に実行サイズがあります。実行サイズ（ハードウェア TCAM 内の現在のサイズ）は、コミットされ実行テンプレートとして現在使用されているデフォルトまたはユーザ定義テンプレートのどちらかによって定義されます。現在コミットされているテンプレート内のリージョンのサイズを現在の実行サイズから増やす場合は、リージョンのサイズを増やすために使用可能な現在のリージョンの外部に未使用のエントリ（他のどのリージョンにも割り当てられていないエントリ）が十分にあるかチェックされます。現在コミットされているテンプレート内のリージョンのサイズを現在の実行サイズから減らす場合は、TCAM リージョンのサイズを減らすために開放できるエントリがリージョン内に十分にあるか判断するためにチェックされます。テンプレート内のリージョンのサイズを減らすすべての変更は、そのテンプレート内のリージョンのサイズを増やす変更の前に完了します。
3. sup-region のすべての機能をサポートするためにソフトウェアで 256 エントリを必要とするため、スーパーバイザ リージョンのサイズは 256 エントリより小さく変更できません。
4. 256 エントリが使用可能でも、スーパーバイザ リージョンのデフォルト サイズは 128 エントリです。TCAM カービングにより、128 エントリをさらに使用できます。sup-region の値を 128、192、または 256 に変更するには、CLI で **sup** キーワードを使用できます。
5. スーパーバイザ リージョンおよびスパン リージョンではハードウェアは 256 エントリより多くはサポートしません。このチェックは検査過程で実施されます。

これらすべてのチェックを通過した場合、そのテンプレートをコミットでき、再起動してテンプレートを適用するかを確認するプロンプトが表示されます。

これらのチェックが失敗した場合、コミットが失敗しテンプレートは保存済みステートに戻ります。コミットが失敗した場合、**commit** コマンドの出力に失敗の原因が表示されます。

デフォルトテンプレートは変更または削除できません。このテンプレートは、保存済みからコミット済み、コミット済みから保存済みへ移行のみが可能です。デフォルトテンプレートがコミットされた場合、実行コンフィギュレーションには表示されません。デフォルトテンプレートを適用するには、現在の実行テンプレートを使用して **no commit** コマンドを入力してください。このコマンドを入力すると、テンプレートをコミットするときに実行されるのと同じ検証チェックが実行されます。すべての検証が成功すると、スイッチを再起動するか確認するメッセージが表示されます。再起動に同意すると、テンプレートがスタートアップ コンフィギュレーションに保存されシステムが再起動します。再起動後、デフォルトテンプレートが適用されます。スタートアップ コンフィギュレーションには、再起動前にコミットしたコミット済みテンプレートがあります。再起動後に、スタートアップ コンフィギュレーションのテンプレートが使用されます。スタートアップ コンフィギュレーションにコミット済みテンプレートがない場合、デフォルト テンプレートが使用されます。

テンプレート管理コマンドを入力して、TCAM カービング テンプレートを作成および管理できます。このテンプレート ベース TCAM カービング CLI は config-sync でサポートされます。テンプレートの作成のみが config-sync 内部でサポートされます。テンプレート コミットは、config-sync コンテクストの外部でスイッチごとに別々に実施する必要があります。

ユーザー定義テンプレートの作成

手順の概要

1. switch# **configure terminal**
2. switch(config)# **hardware profile tcam resource template** *template-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)# **hardware profile tcam resource template** *template-name*	デフォルト リージョン サイズで新しいテンプレートを作成します。最大 16 個のテンプレート（加えてデフォルト テンプレート）を作成できます。*template-name* 引数には最大 64 文字を指定できます。

例

次に、qos-template という名前のユーザー定義テンプレートを作成する例を示します。

```
switch# configure terminal
switch(config)# hardware profile tcam resource template qos-template
```

ユーザー定義テンプレートに関する情報

デフォルト テンプレートに加えて最大 16 個のテンプレートを作成できます（つまり、同時に 17 個のテンプレートを保持できるということです）。希望の 3 値連想メモリ（TCAM）リージョンにどんなサイズでも設定できます。

各テンプレートで、次の操作を実行できます。

- 作成（Create）
- 変更
- 削除
- Commit

各テンプレートは、次のうちのいずれかのステータスになっています。

- 保存済み
- コミット型

作成（Create）

テンプレートを作成する場合、TCAM リージョンのサイズはデフォルト値に初期化されます。テンプレートを作成する場合、テンプレートはデフォルトでは保存済みステートになっています。テンプレートを作成すると、これを変更してどの TCAM リージョンのサイズも変更できます。各 TCAM ブロックのサイズは 64 エントリのため、リージョンのサイズは 64 の倍数で設定する必要があります。入力した値が 64 の倍数でなかった場合、値を再入力するように求めるエラー メッセージが表示されます。

変更

すべての保存済みテンプレートを編集してどの TCAM リージョンのサイズでも変更できますが、どの TCAM のリージョンのサイズも 0 に設定することはできません。編集中、入力したサイズが 64 の境界線にあるかがソフトウェアによってチェックされます。テンプレートを変更する場合、すべての TCAM リージョンのサイズの合計が 4096 エントリより小さくなる必要があります。変更中は、4096 エントリ未満なのかはソフトウェアではチェックされません。

テンプレートは、保存済みステートのときにのみ変更できます。テンプレートをコミットした後は編集できません。

コミット済みのユーザー定義テンプレートは、別のユーザー定義テンプレートまたはデフォルト テンプレートを提供することによって作成済みステートに変更できます。

別のユーザー定義テンプレートを提供するには、次のコマンドを入力します。

hardware profile tcam resource service-template *user-defined-template*

デフォルト テンプレートを提供するには、次のコマンドを入力します。

no hardware profile tcam resource service-template *currently-committed- template*

削除

どの保存済みテンプレートも削除できます。テンプレートを削除した後では、そのテンプレートに関するすべての情報が失われます。コミットしたテンプレートは削除できません。

コミット済みのユーザー定義テンプレートは、別のユーザー定義テンプレートまたはデフォルト テンプレートを提供することによって作成済みステートに変更できます。

別のユーザー定義テンプレートを提供するには、次のコマンドを入力します。

hardware profile tcam resource service-template *user-defined-template*

デフォルト テンプレートを提供するには、次のコマンドを入力します。

no hardware profile tcam resource service-template *currently-committed- template*

Commit

自分のユーザ定義テンプレートまたはソフトウェアで提供されているデフォルトテンプレートはどれでもコミットできます。テンプレートをコミットするには、**commit** コマンドを入力し、スイッチの再起動を行います。**commit** コマンドを入力すると、ソフトェアによってテンプレートが検証されます。検証が成功すると、スイッチを再起動するか確認するメッセージが表示されます。テンプレート（ユーザー定義またはデフォルト）は、再起動後に適用されます。再起

動を選択しなかった場合、TCAM リージョンへの変更は行われず、コミットされるテンプレートはありません。

Cisco NX-OS リリース 9.3(3) 以降では、テンプレートをコミットすると、実行コンフィギュレ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スイッチをリブートするかどうかを確認するプロンプトが表示されます。続行に同意すると、次のことが行われます。

- コミットしたテンプレートがスタートアップ コンフィギュレーションに保存されます。
- スイッチが再起動します。
- コミットしたテンプレートがソフトウェアによって使用されます。
- テンプレートが実行中ステートに移行します。

（注） Cisco NX-OS リリース 9.3(3) より前では、テンプレートをコミットした後、システムは自動では再起動せず **commit** コマンドの出力にメッセージが表示され、コミットしたテンプレートを有効にするためにスイッチを再起動するか尋ねられます。

コミットされていない TCAM プロファイルを含むバックアップ コンフィギュレーションから、書き込み消去、リロード、および実行コンフィギュレーションのコピーを実行すると、次のことが発生します。

1. TCAM プロファイルがコミットされると、スイッチはプロンプトなしで自動的にリロードします。
2. TCAM カービング CLI の後の設定は適用されません。
3. コミットされた TCAM プロファイルで設定を復元するには、バックアップ コンフィギュレーションを実行コンフィギュレーションに再度コピーする必要があります。ただし、TCAM カービング プロファイルはすでにコミットされているため、スイッチのリロードはありません。

新しいコミットされた TCAM プロファイルが原因でスイッチがリロードされると、**show system reset-reason** コマンドは、次に示すようにリロードの理由を表示します。

```
switch# show system reset-reason
----- reset reason for Supervisor-module 1 (from Supervisor in slot 1) ---
1) At 302777 usecs after Sun Jan 20 22:02:37 2019
    Reason: Reload due to change in TCAM service-template
    Service:
    Version: 9.3(3)

2) At 314447 usecs after Sun Jan 20 21:52:58 2019
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 9.3(3)

3) At 20142 usecs after Sun Jan 20 21:27:33 2019
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 9.3(3)
```

スイッチを再起動後、コミットされたテンプレートが Cisco Nexus サーバー上のすべての ASIC に適用されます。Cisco Nexus デバイス上の別の ASIC に別のテンプレートをコミットできません。各テンプレートの各リージョンのサイズを指定したすべての保存済みテンプレートおよびコミット済みテンプレートは実行コンフィギュレーションに表示されます。

テンプレートがコミットされたとき、以下がチェックされます。

1. TCAM 内のすべてのリージョンの合計サイズは 4096 エントリです。
2. 各リージョンのサイズは TCAM 内に収まります。どの時点でも、TCAM リージョンに対して常に実行サイズがあります。実行サイズ（ハードウェア TCAM 内の現在のサイズ）は、コミットされ実行テンプレートとして現在使用されているデフォルトまたはユーザ定義テンプレートのどちらかによって定義されます。現在コミットされているテンプレート内のリージョンのサイズを現在の実行サイズから増やす場合は、リージョンのサイズを増やすために使用可能な現在のリージョンの外部に未使用のエントリ（他のどのリージョンにも割り当てられていないエントリ）が十分にあるかチェックされます。現在コミットされているテンプレート内のリージョンのサイズを現在の実行サイズから減らす場合は、TCAM リージョンのサイズを減らすために開放できるエントリがリージョン内に十分にあるか判断するためにチェックされます。テンプレート内のリージョンのサイズを減らすすべての変更は、そのテンプレート内のリージョンのサイズを増やす変更の前に完了します。
3. sup-region のすべての機能をサポートするためにソフトウェアで 256 エントリを必要とするため、スーパーバイザ リージョンのサイズは 256 エントリより小さく変更できません。
4. 256 エントリが使用可能でも、スーパーバイザ リージョンのデフォルト サイズは 128 エントリです。TCAM カービングにより、128 エントリをさらに使用できます。sup-region の値を 128、192、または 256 に変更するには、CLI で **sup** キーワードを使用できます。
5. スーパーバイザ リージョンおよびスパン リージョンではハードウェアは 256 エントリより多くはサポートしません。このチェックは検査過程で実施されます。

これらすべてのチェックを通過した場合、そのテンプレートをコミットでき、再起動してテンプレートを適用するかを確認するプロンプトが表示されます。

これらのチェックが失敗した場合、コミットが失敗しテンプレートは保存済みステートに戻ります。コミットが失敗した場合、**commit** コマンドの出力に失敗の原因が表示されます。

デフォルトテンプレートは変更または削除できません。このテンプレートは、保存済みからコミット済み、コミット済みから保存済みへ移行のみが可能です。デフォルトテンプレートがコミットされた場合、実行コンフィギュレーションには表示されません。デフォルトテンプレートを適用するには、現在の実行テンプレートを使用して **no commit** コマンドを入力してください。このコマンドを入力すると、テンプレートをコミットするときに実行されるのと同じ検証チェックが実行されます。すべての検証が成功すると、スイッチを再起動するか確認するメッセージが表示されます。再起動に同意すると、テンプレートがスタートアップ コンフィギュレーションに保存されシステムが再起動します。再起動後、デフォルトテンプレートが適用されます。スタートアップ コンフィギュレーションには、再起動前にコミットしたコミット済みテンプレートがあります。再起動後に、スタートアップ コンフィギュレーションのテンプレー

トが使用されます。スタートアップ コンフィギュレーションにコミット済みテンプレートがない場合、デフォルト テンプレートが使用されます。

テンプレート管理コマンドを入力して、TCAM カービング テンプレートを作成および管理できます。このテンプレート ベース TCAM カービング CLI は config-sync でサポートされます。テンプレートの作成のみが config-sync 内部でサポートされます。テンプレート コミットは、config-sync コンテクストの外部でスイッチごとに別々に実施する必要があります。

ユーザー定義テンプレートの変更

手順の概要

1. switch# **configure terminal**
2. switch(config)# **hardware profile tcam resource template** *template-name*
3. switch(config-tmpl)# {**vacl** *vacl-region* | **ifacl** *ifacl-region* | **qos** *qos-region* | **rbacl** *rbacl-region* | **span** *span-region*}
4. switch(config-tmpl)# {**vacl** *vacl-region* | **ifacl** *ifacl-region* | **qos** *qos-region* | **rbacl** *rbacl-region* | **span** *span-region* **iracl** *iracl-region* **eracl** *eracl-region* **sup** *sup-region* **iracl** *iracl-region* **eracl** *eracl-region* **sup** *sup-region* }

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)# **hardware profile tcam resource template** *template-name*	デフォルト リージョン サイズで新しいテンプレートを作成します。最大 16 個のテンプレート（加えてデフォルトテンプレート）を作成できます。このコマンドは、テンプレート モードを開始するために使用します。
ステップ 3	switch(config-tmpl)# {**vacl** *vacl-region* | **ifacl** *ifacl-region* | **qos** *qos-region* | **rbacl** *rbacl-region* | **span** *span-region*}	リージョン ブロック サイズを設定します。 • *vacl-region*：このリージョンのブロックサイズは 64 ～ 3584 です。 • *ifacl-region*：このリージョンのブロックサイズは 320 ～ 3584 です。 • *qos-region*：このリージョンのブロックサイズは 64 ～ 3584 です。 • *rbacl-region*：このリージョンのブロックサイズは 64 ～ 3584 です。

	コマンドまたはアクション	目的
		• *span-region*：このリージョンのブロックサイズは 64 ～ 256 です。 （注） リージョンのサイズをゼロには設定できません。ブロック サイズは 64 の倍数にする必要があります。
ステップ 4	switch(config-tmpl)# {**vacl** *vacl-region* | **ifacl** *ifacl-region* | **qos** *qos-region* | **rbacl** *rbacl-region* | **span** *span-region* **iracl** *iracl-region* **eracl** *eracl-region* **sup** *sup-region* **iracl** *iracl-region* **eracl** *eracl-region* **sup** *sup-region* }	リージョン ブロック サイズを設定します。 • *vacl-region*：このリージョンのブロックサイズは 64 ～ 3584 です。 • *ifacl-region*：このリージョンのブロックサイズは 320 ～ 3584 です。 • *qos-region*：このリージョンのブロックサイズは 64 ～ 3584 です。 • *rbacl-region*：このリージョンのブロックサイズは 64 ～ 3584 です。 • *span-region*：このリージョンのブロックサイズは 64 ～ 256 です。 • *iracl-region*：このリージョンのブロックサイズは 64 ～ 3648 です。 • *eracl-region*：このリージョンのブロックサイズは 64 ～ 3648 です。 • *sup-region*：このリージョンのブロックサイズは 64 ～ 256 です。 （注） リージョンのサイズをゼロには設定できません。ブロック サイズは 64 の倍数にする必要があります。iracl と eracl のブロック サイズを合計すると 3712 になります。

例

次に、ユーザ定義 QoS テンプレートを変更する例を示します。

```
switch# configure terminal
switch(config)# hardware profile tcam resource template qos-template
switch(config-tmpl) qos 64
```

ユーザー定義テンプレートに関する情報

デフォルト テンプレートに加えて最大 16 個のテンプレートを作成できます（つまり、同時に 17 個のテンプレートを保持できるということです）。希望の 3 値連想メモリ（TCAM）リージョンにどんなサイズでも設定できます。

各テンプレートで、次の操作を実行できます。

- 作成（Create）
- 変更
- 削除
- Commit

各テンプレートは、次のうちのいずれかのステータスになっています。

- 保存済み
- コミット型

作成（Create）

テンプレートを作成する場合、TCAM リージョンのサイズはデフォルト値に初期化されます。テンプレートを作成する場合、テンプレートはデフォルトでは保存済みステートになっています。テンプレートを作成すると、これを変更してどの TCAM リージョンのサイズも変更できます。各 TCAM ブロックのサイズは 64 エントリのため、リージョンのサイズは 64 の倍数で設定する必要があります。入力した値が 64 の倍数でなかった場合、値を再入力するように求めるエラー メッセージが表示されます。

変更

すべての保存済みテンプレートを編集してどの TCAM リージョンのサイズでも変更できますが、どの TCAM のリージョンのサイズも 0 に設定することはできません。編集中、入力したサイズが 64 の境界線にあるかがソフトウェアによってチェックされます。テンプレートを変更する場合、すべての TCAM リージョンのサイズの合計が 4096 エントリより小さくなる必要があります。変更中は、4096 エントリ未満なのかはソフトウェアではチェックされません。

テンプレートは、保存済みステートのときにのみ変更できます。テンプレートをコミットした後は編集できません。

コミット済みのユーザー定義テンプレートは、別のユーザー定義テンプレートまたはデフォルト テンプレートを提供することによって作成済みステートに変更できます。

別のユーザー定義テンプレートを提供するには、次のコマンドを入力します。

hardware profile tcam resource service-template *user-defined-template*

デフォルト テンプレートを提供するには、次のコマンドを入力します。

no hardware profile tcam resource service-template *currently-committed- template*

削除

どの保存済みテンプレートも削除できます。テンプレートを削除した後では、そのテンプレートに関するすべての情報が失われます。コミットしたテンプレートは削除できません。

コミット済みのユーザー定義テンプレートは、別のユーザー定義テンプレートまたはデフォルト テンプレートを提供することによって作成済みステートに変更できます。

別のユーザー定義テンプレートを提供するには、次のコマンドを入力します。

hardware profile tcam resource service-template *user-defined-template*

デフォルト テンプレートを提供するには、次のコマンドを入力します。

no hardware profile tcam resource service-template *currently-committed- template*

Commit

自分のユーザ定義テンプレートまたはソフトウェアで提供されているデフォルトテンプレートはどれでもコミットできます。テンプレートをコミットするには、**commit** コマンドを入力し、スイッチの再起動を行います。**commit** コマンドを入力すると、ソフトェアによってテンプレートが検証されます。検証が成功すると、スイッチを再起動するか確認するメッセージが表示されます。テンプレート（ユーザー定義またはデフォルト）は、再起動後に適用されます。再起動を選択しなかった場合、TCAM リージョンへの変更は行われず、コミットされるテンプレートはありません。

Cisco NX-OS リリース 9.3(3) 以降では、テンプレートをコミットすると、実行コンフィギュレ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スイッチをリブートするかどうかを確認するプロンプトが表示されます。続行に同意すると、次のことが行われます。

- コミットしたテンプレートがスタートアップ コンフィギュレーションに保存されます。
- スイッチが再起動します。
- コミットしたテンプレートがソフトウェアによって使用されます。
- テンプレートが実行中ステートに移行します。

（注） Cisco NX-OS リリース 9.3(3) より前では、テンプレートをコミットした後、システムは自動では再起動せず **commit** コマンドの出力にメッセージが表示され、コミットしたテンプレートを有効にするためにスイッチを再起動するか尋ねられます。

コミットされていない TCAM プロファイルを含むバックアップ コンフィギュレーションから、書き込み消去、リロード、および実行コンフィギュレーションのコピーを実行すると、次のことが発生します。

1. TCAM プロファイルがコミットされると、スイッチはプロンプトなしで自動的にリロードします。
2. TCAM カービング CLI の後の設定は適用されません。

3. コミットされた TCAM プロファイルで設定を復元するには、バックアップ コンフィギュレーションを実行コンフィギュレーションに再度コピーする必要があります。ただし、TCAM カービング プロファイルはすでにコミットされているため、スイッチのリロードはありません。

新しいコミットされた TCAM プロファイルが原因でスイッチがリロードされると、**show system reset-reason** コマンドは、次に示すようにリロードの理由を表示します。

```
switch# show system reset-reason
----- reset reason for Supervisor-module 1 (from Supervisor in slot 1) ---
1) At 302777 usecs after Sun Jan 20 22:02:37 2019
    Reason: Reload due to change in TCAM service-template
    Service:
    Version: 9.3(3)

2) At 314447 usecs after Sun Jan 20 21:52:58 2019
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 9.3(3)

3) At 20142 usecs after Sun Jan 20 21:27:33 2019
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 9.3(3)
```

スイッチを再起動後、コミットされたテンプレートが Cisco Nexus サーバー上のすべての ASIC に適用されます。Cisco Nexus デバイス上の別の ASIC に別のテンプレートをコミットできません。各テンプレートの各リージョンのサイズを指定したすべての保存済みテンプレートおよびコミット済みテンプレートは実行コンフィギュレーションに表示されます。

テンプレートがコミットされたとき、以下がチェックされます。

1. TCAM 内のすべてのリージョンの合計サイズは 4096 エントリです。
2. 各リージョンのサイズは TCAM 内に収まります。どの時点でも、TCAM リージョンに対して常に実行サイズがあります。実行サイズ（ハードウェア TCAM 内の現在のサイズ）は、コミットされ実行テンプレートとして現在使用されているデフォルトまたはユーザ定義テンプレートのどちらかによって定義されます。現在コミットされているテンプレート内のリージョンのサイズを現在の実行サイズから増やす場合は、リージョンのサイズを増やすために使用可能な現在のリージョンの外部に未使用のエントリ（他のどのリージョンにも割り当てられていないエントリ）が十分にあるかチェックされます。現在コミットされているテンプレート内のリージョンのサイズを現在の実行サイズから減らす場合は、TCAM リージョンのサイズを減らすために開放できるエントリがリージョン内に十分にあるか判断するためにチェックされます。テンプレート内のリージョンのサイズを減らすすべての変更は、そのテンプレート内のリージョンのサイズを増やす変更の前に完了します。
3. sup-region のすべての機能をサポートするためにソフトウェアで 256 エントリを必要とするため、スーパーバイザ リージョンのサイズは 256 エントリより小さく変更できません。
4. 256 エントリが使用可能でも、スーパーバイザ リージョンのデフォルト サイズは 128 エントリです。TCAM カービングにより、128 エントリをさらに使用できます。sup-region の値を 128、192、または 256 に変更するには、CLI で **sup** キーワードを使用できます。

5. スーパーバイザ リージョンおよびスパン リージョンではハードウェアは 256 エントリより多くはサポートしません。このチェックは検査過程で実施されます。

これらすべてのチェックを通過した場合、そのテンプレートをコミットでき、再起動してテンプレートを適用するかを確認するプロンプトが表示されます。

これらのチェックが失敗した場合、コミットが失敗しテンプレートは保存済みステートに戻ります。コミットが失敗した場合、**commit** コマンドの出力に失敗の原因が表示されます。

デフォルトテンプレートは変更または削除できません。このテンプレートは、保存済みからコミット済み、コミット済みから保存済みへ移行のみが可能です。デフォルトテンプレートがコミットされた場合、実行コンフィギュレーションには表示されません。デフォルトテンプレートを適用するには、現在の実行テンプレートを使用して **no commit** コマンドを入力してください。このコマンドを入力すると、テンプレートをコミットするときに実行されるのと同じ検証チェックが実行されます。すべての検証が成功すると、スイッチを再起動するか確認するメッセージが表示されます。再起動に同意すると、テンプレートがスタートアップ コンフィギュレーションに保存されシステムが再起動します。再起動後、デフォルトテンプレートが適用されます。スタートアップ コンフィギュレーションには、再起動前にコミットしたコミット済みテンプレートがあります。再起動後に、スタートアップ コンフィギュレーションのテンプレートが使用されます。スタートアップ コンフィギュレーションにコミット済みテンプレートがない場合、デフォルト テンプレートが使用されます。

テンプレート管理コマンドを入力して、TCAM カービング テンプレートを作成および管理できます。このテンプレート ベース TCAM カービング CLI は config-sync でサポートされます。テンプレートの作成のみが config-sync 内部でサポートされます。テンプレート コミットは、config-sync コンテクストの外部でスイッチごとに別々に実施する必要があります。

ユーザー定義テンプレートのコミット

ユーザー定義テンプレートをコミットできます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **hardware profile tcam resource service-template** *template-name*
3. （任意） switch# **show hardware profile tcam resource template**

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	必須: 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)# **hardware profile tcam resource service-template** *template-name*	事前定義済みのテンプレートを実行イメージでコミットします。テンプレートをコミットすると、実行コンフィギュレ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スイッチをリブートするかどうかを確認するプロンプトが表示されます。続行に同意すると、指定したテンプレートが再起動後に適用されます。それ以外の場合、TCAM リージョンは変更されず、テンプレートもコミットされません。
ステップ 3	（任意） switch# **show hardware profile tcam resource template**	すべてのテンプレートを表示します。 （注） スイッチのリロード後、このコマンドを使用して、コミットされたテンプレートを表示します。

例

次の例では、ユーザー定義テンプレートをコミットする方法を示します。

```
switch# configure terminal
switch(config)# hardware profile tcam resource service-template temp1

Details of the temp1 template you are trying to commit are as follows:

-------------------------------------------------------------------------------
Template name: temp1
Current state: Created

Region  Features  Size-allocated    Current-size  Current-usage  Available/free
-------------------------------------------------------------------------------
Vacl    Vacl                1024            1024             15            1009
Ifacl   Ifacl               1152            1152            209             943
Rbacl   Rbacl               1152            1152              3            1149
Qos     Qos                  448             448             30             418
Span    Span                  64              64              2              62
Sup     Sup                  256             256             58             198
-------------------------------------------------------------------------------


To finish committing the template, the system will do the following:
    1> Save running config :  "copy running-config startup-config"
    2> Reboot the switch   :  "reload"


-------------------------------------------------------------------------------
Do you really want to continue with RELOAD ? (y/n) [no] yes
System is still initializing
Configuration mode is blocked until system is ready
switch(config)# [16152.925385] Shutdown Ports..
[16152.959744]  writing reset reason 9
[snip]
```

```
/AFTER SWITCH RELOADS/

switch# show hardware profile tcam resource template
    Template   Type     State   Vacl  Ifacl   Rbacl  Qos  Span   Sup      TOTAL
-------------------------------------------------------------------------------
     default system   Created   1024   1152  1152    448    64   256      4096
       temp1   user Committed   1024   1152  1152    448    64   256      4096
       temp2   user   Created   1024   1152  1152    448    64   256      4096
-------------------------------------------------------------------------------
```

次に、レイヤ3カード側UPCに対して、ユーザー定義のテンプレートをコミットし、適用する例を示します。

```
switch# configure terminal
switch(config)# hardware profile tcam resource service-template temp1

Details of the temp1 template you are trying to commit are as follows:

-------------------------------------------------------------------------------
Template name: temp1
Current state: Created

Region  Features  Size-allocated    Current-size  Current-usage  Available/free
-------------------------------------------------------------------------------
Vacl    Vacl               1984            2048             11            2037
Ifacl   Ifacl              1216            1152             26            1126
Rbacl   Rbacl               128             128              3             125
Qos     Qos                 448             448              9             439
Span    Span                 64              64              3              61
Sup     Sup                 256             128             81              47
ERacl   ERacl               1920               0              0               0
IRacl   IRacl               1792               0              0               0
-------------------------------------------------------------------------------


To finish committing the template, the system will do the following:
    1> Save running config :  "copy running-config startup-config"
    2> Reboot the switch   :  "reload"


-------------------------------------------------------------------------------
Do you really want to continue with RELOAD ? (y/n) [no] yes
System is still initializing
Configuration mode is blocked until system is ready
5548(config)# [166850.680711] Shutdown Ports..
[166850.716114]  writing reset reason 9,
[snip]

/AFTER SWITCH RELOADS/

switch# show hardware profile tcam resource template
    Template   Type     State   ERacl  Ifacl  IRacl   Qos  Span   Sup      TOTAL
-------------------------------------------------------------------------------
     default system   Created   2048     64   1664     64    64    64      4096
       temp1   user Committed   1920     64   1792     64    64    64      4096
       temp2   user   Created   2048     64   1664     64    64    64      4096
-------------------------------------------------------------------------------
```

ユーザー定義テンプレートに関する情報

デフォルト テンプレートに加えて最大 16 個のテンプレートを作成できます（つまり、同時に 17 個のテンプレートを保持できるということです）。希望の 3 値連想メモリ（TCAM）リージョンにどんなサイズでも設定できます。

各テンプレートで、次の操作を実行できます。

- 作成（Create）
- 変更
- 削除
- Commit

各テンプレートは、次のうちのいずれかのステータスになっています。

- 保存済み
- コミット型

作成（Create）

テンプレートを作成する場合、TCAM リージョンのサイズはデフォルト値に初期化されます。テンプレートを作成する場合、テンプレートはデフォルトでは保存済みステートになっています。テンプレートを作成すると、これを変更してどの TCAM リージョンのサイズも変更できます。各 TCAM ブロックのサイズは 64 エントリのため、リージョンのサイズは 64 の倍数で設定する必要があります。入力した値が 64 の倍数でなかった場合、値を再入力するように求めるエラー メッセージが表示されます。

変更

すべての保存済みテンプレートを編集してどの TCAM リージョンのサイズでも変更できますが、どの TCAM のリージョンのサイズも 0 に設定することはできません。編集中、入力したサイズが 64 の境界線にあるかがソフトウェアによってチェックされます。テンプレートを変更する場合、すべての TCAM リージョンのサイズの合計が 4096 エントリより小さくなる必要があります。変更中は、4096 エントリ未満なのかはソフトウェアではチェックされません。

テンプレートは、保存済みステートのときにのみ変更できます。テンプレートをコミットした後は編集できません。

コミット済みのユーザー定義テンプレートは、別のユーザー定義テンプレートまたはデフォルト テンプレートを提供することによって作成済みステートに変更できます。

別のユーザー定義テンプレートを提供するには、次のコマンドを入力します。

hardware profile tcam resource service-template *user-defined-template*

デフォルト テンプレートを提供するには、次のコマンドを入力します。

no hardware profile tcam resource service-template *currently-committed- template*

削除

どの保存済みテンプレートも削除できます。テンプレートを削除した後では、そのテンプレートに関するすべての情報が失われます。コミットしたテンプレートは削除できません。

コミット済みのユーザー定義テンプレートは、別のユーザー定義テンプレートまたはデフォルト テンプレートを提供することによって作成済みステートに変更できます。

別のユーザー定義テンプレートを提供するには、次のコマンドを入力します。

hardware profile tcam resource service-template *user-defined-template*

デフォルト テンプレートを提供するには、次のコマンドを入力します。

no hardware profile tcam resource service-template *currently-committed- template*

Commit

自分のユーザ定義テンプレートまたはソフトウェアで提供されているデフォルトテンプレートはどれでもコミットできます。テンプレートをコミットするには、**commit** コマンドを入力し、スイッチの再起動を行います。**commit** コマンドを入力すると、ソフトェアによってテンプレートが検証されます。検証が成功すると、スイッチを再起動するか確認するメッセージが表示されます。テンプレート（ユーザー定義またはデフォルト）は、再起動後に適用されます。再起動を選択しなかった場合、TCAM リージョンへの変更は行われず、コミットされるテンプレートはありません。

Cisco NX-OS リリース 9.3(3) 以降では、テンプレートをコミットすると、実行コンフィギュレ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スイッチをリブートするかどうかを確認するプロンプトが表示されます。続行に同意すると、次のことが行われます。

- コミットしたテンプレートがスタートアップ コンフィギュレーションに保存されます。
- スイッチが再起動します。
- コミットしたテンプレートがソフトウェアによって使用されます。
- テンプレートが実行中ステートに移行します。

（注） Cisco NX-OS リリース 9.3(3) より前では、テンプレートをコミットした後、システムは自動では再起動せず **commit** コマンドの出力にメッセージが表示され、コミットしたテンプレートを有効にするためにスイッチを再起動するか尋ねられます。

コミットされていない TCAM プロファイルを含むバックアップ コンフィギュレーションから、書き込み消去、リロード、および実行コンフィギュレーションのコピーを実行すると、次のことが発生します。

1. TCAM プロファイルがコミットされると、スイッチはプロンプトなしで自動的にリロードします。
2. TCAM カービング CLI の後の設定は適用されません。

3. コミットされた TCAM プロファイルで設定を復元するには、バックアップ コンフィギュレーションを実行コンフィギュレーションに再度コピーする必要があります。ただし、TCAM カービング プロファイルはすでにコミットされているため、スイッチのリロードはありません。

新しいコミットされた TCAM プロファイルが原因でスイッチがリロードされると、**show system reset-reason** コマンドは、次に示すようにリロードの理由を表示します。

```
switch# show system reset-reason
----- reset reason for Supervisor-module 1 (from Supervisor in slot 1) ---
1) At 302777 usecs after Sun Jan 20 22:02:37 2019
    Reason: Reload due to change in TCAM service-template
    Service:
    Version: 9.3(3)

2) At 314447 usecs after Sun Jan 20 21:52:58 2019
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 9.3(3)

3) At 20142 usecs after Sun Jan 20 21:27:33 2019
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 9.3(3)
```

スイッチを再起動後、コミットされたテンプレートが Cisco Nexus サーバー上のすべての ASIC に適用されます。Cisco Nexus デバイス上の別の ASIC に別のテンプレートをコミットできません。各テンプレートの各リージョンのサイズを指定したすべての保存済みテンプレートおよびコミット済みテンプレートは実行コンフィギュレーションに表示されます。

テンプレートがコミットされたとき、以下がチェックされます。

1. TCAM 内のすべてのリージョンの合計サイズは 4096 エントリです。
2. 各リージョンのサイズは TCAM 内に収まります。どの時点でも、TCAM リージョンに対して常に実行サイズがあります。実行サイズ（ハードウェア TCAM 内の現在のサイズ）は、コミットされ実行テンプレートとして現在使用されているデフォルトまたはユーザ定義テンプレートのどちらかによって定義されます。現在コミットされているテンプレート内のリージョンのサイズを現在の実行サイズから増やす場合は、リージョンのサイズを増やすために使用可能な現在のリージョンの外部に未使用のエントリ（他のどのリージョンにも割り当てられていないエントリ）が十分にあるかチェックされます。現在コミットされているテンプレート内のリージョンのサイズを現在の実行サイズから減らす場合は、TCAM リージョンのサイズを減らすために開放できるエントリがリージョン内に十分にあるか判断するためにチェックされます。テンプレート内のリージョンのサイズを減らすすべての変更は、そのテンプレート内のリージョンのサイズを増やす変更の前に完了します。
3. sup-region のすべての機能をサポートするためにソフトウェアで 256 エントリを必要とするため、スーパーバイザ リージョンのサイズは 256 エントリより小さく変更できません。
4. 256 エントリが使用可能でも、スーパーバイザ リージョンのデフォルト サイズは 128 エントリです。TCAM カービングにより、128 エントリをさらに使用できます。sup-region の値を 128、192、または 256 に変更するには、CLI で **sup** キーワードを使用できます。

5. スーパーバイザ リージョンおよびスパン リージョンではハードウェアは 256 エントリより多くはサポートしません。このチェックは検査過程で実施されます。

これらすべてのチェックを通過した場合、そのテンプレートをコミットでき、再起動してテンプレートを適用するかを確認するプロンプトが表示されます。

これらのチェックが失敗した場合、コミットが失敗しテンプレートは保存済みステートに戻ります。コミットが失敗した場合、**commit** コマンドの出力に失敗の原因が表示されます。

デフォルトテンプレートは変更または削除できません。このテンプレートは、保存済みからコミット済み、コミット済みから保存済みへ移行のみが可能です。デフォルトテンプレートがコミットされた場合、実行コンフィギュレーションには表示されません。デフォルトテンプレートを適用するには、現在の実行テンプレートを使用して **no commit** コマンドを入力してください。このコマンドを入力すると、テンプレートをコミットするときに実行されるのと同じ検証チェックが実行されます。すべての検証が成功すると、スイッチを再起動するか確認するメッセージが表示されます。再起動に同意すると、テンプレートがスタートアップ コンフィギュレーションに保存されシステムが再起動します。再起動後、デフォルトテンプレートが適用されます。スタートアップ コンフィギュレーションには、再起動前にコミットしたコミット済みテンプレートがあります。再起動後に、スタートアップ コンフィギュレーションのテンプレートが使用されます。スタートアップ コンフィギュレーションにコミット済みテンプレートがない場合、デフォルト テンプレートが使用されます。

テンプレート管理コマンドを入力して、TCAM カービング テンプレートを作成および管理できます。このテンプレート ベース TCAM カービング CLI は config-sync でサポートされます。テンプレートの作成のみが config-sync 内部でサポートされます。テンプレート コミットは、config-sync コンテクストの外部でスイッチごとに別々に実施する必要があります。

テンプレートの削除

テンプレートを作成後、そのテンプレートを削除できます。削除は、そのテンプレートに関するすべての情報をソフトウェアから取り除きます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **no hardware profile tcam resource template** *template-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)# **no hardware profile tcam resource template** *template-name*	ユーザー定義テンプレートを削除します。

	コマンドまたはアクション	目的
		保存済みのテンプレートだけが削除できます。コミット済み/実行中のテンプレートは削除できません。実行コンフィギュレーションに記述されているテンプレートは（スタートアップコンフィギュレーションも同様）削除できません。他のどんなユーザ定義テンプレートも保存済みのステータスにあれば削除できます。デフォルトテンプレートは削除できません。

例

次に、テンプレートを削除する例を示します

```
switch# configure terminal
switch(config)# no hardware profile tcam resource template qos-template
```

ユーザー定義テンプレートに関する情報

デフォルト テンプレートに加えて最大 16 個のテンプレートを作成できます（つまり、同時に 17 個のテンプレートを保持できるということです）。希望の 3 値連想メモリ（TCAM）リージョンにどんなサイズでも設定できます。

各テンプレートで、次の操作を実行できます。

- 作成（Create）
- 変更
- 削除
- Commit

各テンプレートは、次のうちのいずれかのステータスになっています。

- 保存済み
- コミット型

作成（Create）

テンプレートを作成する場合、TCAM リージョンのサイズはデフォルト値に初期化されます。テンプレートを作成する場合、テンプレートはデフォルトでは保存済みステートになっています。テンプレートを作成すると、これを変更してどの TCAM リージョンのサイズも変更できます。各 TCAM ブロックのサイズは 64 エントリのため、リージョンのサイズは 64 の倍数で設定する必要があります。入力した値が 64 の倍数でなかった場合、値を再入力するように求めるエラー メッセージが表示されます。

変更

すべての保存済みテンプレートを編集してどの TCAM リージョンのサイズでも変更できますが、どの TCAM のリージョンのサイズも 0 に設定することはできません。編集中、入力したサイズが 64 の境界線にあるかがソフトウェアによってチェックされます。テンプレートを変更する場合、すべての TCAM リージョンのサイズの合計が 4096 エントリより小さくなる必要があります。変更中は、4096 エントリ未満なのかはソフトウェアではチェックされません。

テンプレートは、保存済みステートのときにのみ変更できます。テンプレートをコミットした後は編集できません。

コミット済みのユーザー定義テンプレートは、別のユーザー定義テンプレートまたはデフォルト テンプレートを提供することによって作成済みステートに変更できます。

別のユーザー定義テンプレートを提供するには、次のコマンドを入力します。

hardware profile tcam resource service-template *user-defined-template*

デフォルト テンプレートを提供するには、次のコマンドを入力します。

no hardware profile tcam resource service-template *currently-committed- template*

削除

どの保存済みテンプレートも削除できます。テンプレートを削除した後では、そのテンプレートに関するすべての情報が失われます。コミットしたテンプレートは削除できません。

コミット済みのユーザー定義テンプレートは、別のユーザー定義テンプレートまたはデフォルト テンプレートを提供することによって作成済みステートに変更できます。

別のユーザー定義テンプレートを提供するには、次のコマンドを入力します。

hardware profile tcam resource service-template *user-defined-template*

デフォルト テンプレートを提供するには、次のコマンドを入力します。

no hardware profile tcam resource service-template *currently-committed- template*

Commit

自分のユーザ定義テンプレートまたはソフトウェアで提供されているデフォルトテンプレートはどれでもコミットできます。テンプレートをコミットするには、**commit** コマンドを入力し、スイッチの再起動を行います。**commit** コマンドを入力すると、ソフトェアによってテンプレートが検証されます。検証が成功すると、スイッチを再起動するか確認するメッセージが表示されます。テンプレート（ユーザー定義またはデフォルト）は、再起動後に適用されます。再起動を選択しなかった場合、TCAM リージョンへの変更は行われず、コミットされるテンプレートはありません。

Cisco NX-OS リリース 9.3(3) 以降では、テンプレートをコミットすると、実行コンフィギュレ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スイッチをリブートするかどうかを確認するプロンプトが表示されます。続行に同意すると、次のことが行われます。

- コミットしたテンプレートがスタートアップ コンフィギュレーションに保存されます。
- スイッチが再起動します。

- コミットしたテンプレートがソフトウェアによって使用されます。
- テンプレートが実行中ステートに移行します。

（注） Cisco NX-OS リリース 9.3(3) より前では、テンプレートをコミットした後、システムは自動では再起動せず **commit** コマンドの出力にメッセージが表示され、コミットしたテンプレートを有効にするためにスイッチを再起動するか尋ねられます。

コミットされていないTCAMプロファイルを含むバックアップ コンフィギュレーションから、書き込み消去、リロード、および実行コンフィギュレーションのコピーを実行すると、次のことが発生します。

1. TCAMプロファイルがコミットされると、スイッチはプロンプトなしで自動的にリロードします。
2. TCAM カービング CLI の後の設定は適用されません。
3. コミットされた TCAM プロファイルで設定を復元するには、バックアップ コンフィギュレーションを実行コンフィギュレーションに再度コピーする必要があります。ただし、TCAMカービングプロファイルはすでにコミットされているため、スイッチのリロードはありません。

新しいコミットされたTCAMプロファイルが原因でスイッチがリロードされると、**show system reset-reason** コマンドは、次に示すようにリロードの理由を表示します。

```
switch# show system reset-reason
----- reset reason for Supervisor-module 1 (from Supervisor in slot 1) ---
1) At 302777 usecs after Sun Jan 20 22:02:37 2019
    Reason: Reload due to change in TCAM service-template
    Service:
    Version: 9.3(3)

2) At 314447 usecs after Sun Jan 20 21:52:58 2019
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 9.3(3)

3) At 20142 usecs after Sun Jan 20 21:27:33 2019
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 9.3(3)
```

スイッチを再起動後、コミットされたテンプレートがCisco Nexusサーバー上のすべてのASICに適用されます。Cisco Nexusデバイス上の別のASICに別のテンプレートをコミットできません。各テンプレートの各リージョンのサイズを指定したすべての保存済みテンプレートおよびコミット済みテンプレートは実行コンフィギュレーションに表示されます。

テンプレートがコミットされたとき、以下がチェックされます。

1. TCAM 内のすべてのリージョンの合計サイズは 4096 エントリです。
2. 各リージョンのサイズは TCAM 内に収まります。どの時点でも、TCAM リージョンに対して常に実行サイズがあります。実行サイズ（ハードウェア TCAM 内の現在のサイズ）

は、コミットされ実行テンプレートとして現在使用されているデフォルトまたはユーザ定義テンプレートのどちらかによって定義されます。現在コミットされているテンプレート内のリージョンのサイズを現在の実行サイズから増やす場合は、リージョンのサイズを増やすために使用可能な現在のリージョンの外部に未使用のエントリ（他のどのリージョンにも割り当てられていないエントリ）が十分にあるかチェックされます。現在コミットされているテンプレート内のリージョンのサイズを現在の実行サイズから減らす場合は、TCAM リージョンのサイズを減らすために開放できるエントリがリージョン内に十分にあるか判断するためにチェックされます。テンプレート内のリージョンのサイズを減らすすべての変更は、そのテンプレート内のリージョンのサイズを増やす変更の前に完了します。

3. sup-region のすべての機能をサポートするためにソフトウェアで 256 エントリを必要とするため、スーパーバイザ リージョンのサイズは 256 エントリより小さく変更できません。
4. 256 エントリが使用可能でも、スーパーバイザ リージョンのデフォルト サイズは 128 エントリです。TCAM カービングにより、128 エントリをさらに使用できます。sup-region の値を 128、192、または 256 に変更するには、CLI で **sup** キーワードを使用できます。
5. スーパーバイザ リージョンおよびスパン リージョンではハードウェアは 256 エントリより多くはサポートしません。このチェックは検査過程で実施されます。

これらすべてのチェックを通過した場合、そのテンプレートをコミットでき、再起動してテンプレートを適用するかを確認するプロンプトが表示されます。

これらのチェックが失敗した場合、コミットが失敗しテンプレートは保存済みステートに戻ります。コミットが失敗した場合、**commit** コマンドの出力に失敗の原因が表示されます。

デフォルトテンプレートは変更または削除できません。このテンプレートは、保存済みからコミット済み、コミット済みから保存済みへ移行のみが可能です。デフォルトテンプレートがコミットされた場合、実行コンフィギュレーションには表示されません。デフォルトテンプレートを適用するには、現在の実行テンプレートを使用して **no commit** コマンドを入力してください。このコマンドを入力すると、テンプレートをコミットするときに実行されるのと同じ検証チェックが実行されます。すべての検証が成功すると、スイッチを再起動するか確認するメッセージが表示されます。再起動に同意すると、テンプレートがスタートアップ コンフィギュレーションに保存されシステムが再起動します。再起動後、デフォルトテンプレートが適用されます。スタートアップ コンフィギュレーションには、再起動前にコミットしたコミット済みテンプレートがあります。再起動後に、スタートアップ コンフィギュレーションのテンプレートが使用されます。スタートアップ コンフィギュレーションにコミット済みテンプレートがない場合、デフォルト テンプレートが使用されます。

テンプレート管理コマンドを入力して、TCAM カービング テンプレートを作成および管理できます。このテンプレート ベース TCAM カービング CLI は config-sync でサポートされます。テンプレートの作成のみが config-sync 内部でサポートされます。テンプレート コミットは、config-sync コンテクストの外部でスイッチごとに別々に実施する必要があります。

TCAM カービング設定の確認

TCAM カービングの設定情報を表示するには、次のいずれかのコマンドを入力します。

コマンド	目的
show hardware profile tcam resource template	すべてのテンプレートを表示します。
show hardware profile tcam resource template name *template-name*	ユーザー定義テンプレートを表示します。
show hardware profile tcam resource template default	デフォルト テンプレートを表示します。

FCoE 設定の確認

FCoE の設定情報を確認するには、次のうちいずれかの作業を行います。

コマンド	目的
switch# **show fcoe**	FCoE がスイッチでイネーブルになっているかどうかを表示します。
switch# **show fcoe database**	FCoE データベースの内容を表示します。
switch# **show interface** [*interface number*] **fcoe**	個々のインターフェイスまたはすべてのインターフェイスに関する FCoE 設定を表示します。
switch# **show queuing interface**[*interface slot/port*]	キューの設定および統計情報を表示します。
switch# **show policy-map interface**[*interface number*]	1 つまたはすべてのインターフェイスのポリシーマップ設定を表示します。

次の例は、FCoE 機能が有効になっているかどうかを確認する方法を示したものです。

```
switch# show fcoe
Global FCF details
        FCF-MAC is 00:0d:ec:6d:95:00
        FC-MAP is 0e:fc:00
        FCF Priority is 128
        FKA Advertisement period for FCF is 8 seconds
```

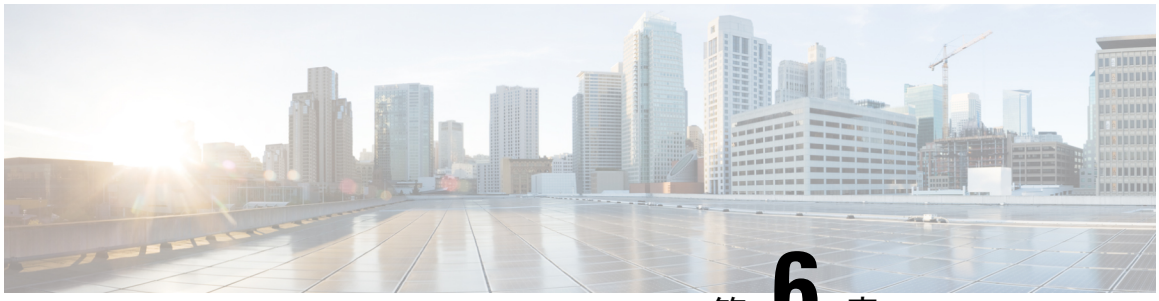
次に、FCoE データベースを表示する例を示します。

```
switch# show fcoe database
-------------------------------------------------------------------------------
INTERFACE       FCID            PORT NAME               MAC ADDRESS
-------------------------------------------------------------------------------
vfc3            0x490100        21:00:00:1b:32:0a:e7:b8 00:c0:dd:0e:5f:76
```

次の例は、あるインターフェイスの FCoE 設定を表示する方法を示したものです。

```
switch# show interface ethernet 1/37 fcoe
```

```
Ethernet1/37 is FCoE UP
    vfc3 is Up
        FCID is 0x490100
        PWWN is 21:00:00:1b:32:0a:e7:b8
        MAC addr is 00:c0:dd:0e:5f:76
```



第 6 章

長距離 over FCoE の構成

長距離 over FCoE の構成

N9K-C93180YC-FX は、FCoE ISL で長距離（最大 10 キロメートル）をサポートします。このサポートは、10G、25G、および40Gの速度に適用されます。ドロップのないライン レート トラフィックの場合、入力バッファ サイズと一時停止/再開しきい値を長距離 ISL で増やす必要があります。これは、ISL ポートにカスタム長距離 FCoE ポリシーを適用することで実現できます。デフォルト FCoE 関連のシステム レベルのネットワーク QoS およびキューイング ポリシーは、すべてのイーサネット ポートに固定の入力バッファ サイズとポーズ/再開しきい値を割り当てます。長距離 ISL の入力バッファ割り当ての増加を促進するには、カスタム短距離 FCoE ポリシーを使用していくつかのイーサネット ポートの入力バッファ割り当てを減らす必要がある場合があります。

（注） SAN トラフィックにはのみ FCoE 長距離 ISL を使用することを推奨します。

表 *4:* さまざまな速度での *FC* 長距離

スピード	ディスタンス
10G	10 km
25 G	10 km
40G	10 km

（注）

- VFC にバインドされていないイーサネット ポートまたは VFC にバインドされたイーサネットポート（短距離要件、100 メートル未満）の入力バッファ割り当ては、カスタム短距離 FCoE ポリシーを使用して減らすことができます。
- トラフィックを実行しているポートでポリシーが変更されると、トラフィックが一時的にドロップされます。
- イーサネット ポートの入力バッファの割り当てに失敗した場合は、イーサネット ポートを起動するために入力バッファを使用できるようになった後、ポートで shut/no shut を実行する必要があります。

異なるタイプのポリシーの構成

構成は、次のように、異なるタイプのポリシー、つまり、異なる速度のデフォルトのシステム レベル ポリシーとインターフェイス レベルのカスタム ポリシーによって異なります。

- **FCoE のデフォルトのシステム レベル ポリシー**

```
switch(config)# system qos
switch(config-sys-qos)# service-policy type network-qos default-fcoe-nq-policy
switch(config-sys-qos)# service-policy type queuing input default-fcoe-in-que-policy
switch(config-sys-qos)# service-policy type queuing output default-fcoe-out-policy
```

FCoE のシステム レベル ポリシーのデフォルト設定は次のとおりです。

- Buffer-size：104000
- Pause-threshold：20800
- Resume-threshold：19136

- **異なる速度でのインターフェイス レベルのカスタム ポリシー**

長距離をサポートする VFC/VFC-PO ISL にバインドされたイーサネット ポート/ポートチャネルに適用する必要がある長距離のカスタム ポリシーは次のとおりです。

- **10G ISL の長距離ポリシー**

```
switch(config)# policy-map type queuing ld_10G_fcoe_in_que_policy
switch(config-pmap-que)# class type queuing c-in-q1
switch(config-pmap-c-que)# bandwidth percent 90
switch(config-pmap-c-que)# pause buffer-size 166400 pause-threshold 20800
resume-threshold 19136
switch(config-pmap-c-que)# class type queuing c-in-q-default
switch(config-pmap-c-que)# bandwidth percent 10
switch(config-pmap-c-que)
```

```
switch(config)# policy-map type queuing ld_10G_fcoe_in_que_policy
switch(config-pmap-que)# class type queuing c-in-q1
switch(config-pmap-c-que)# bandwidth percent 90
switch(config-pmap-c-que)# pause buffer-size 291200 pause-threshold 145600
resume-threshold 143936
```

```
switch(config-pmap-c-que)# class type queuing c-in-q-default
switch(config-pmap-c-que)# bandwidth percent 10
```

- **25G ISL の長距離ポリシー**

```
switch(config)# policy-map type queuing ld_25G_fcoe_in_que_policy
switch(config-pmap-que)# class type queuing c-in-q1
switch(config-pmap-c-que)# bandwidth percent 90
switch(config-pmap-c-que)# pause buffer-size 384800 pause-threshold 20800
resume-threshold 19136
switch(config-pmap-c-que)# class type queuing c-in-q-default
switch(config-pmap-c-que)# bandwidth percent 10
switch(config-pmap-c-que)#
```

```
switch(config)# policy-map type queuing ld_25G_fcoe_in_que_policy
switch(config-pmap-que)# class type queuing c-in-q1
switch(config-pmap-c-que)# bandwidth percent 90
switch(config-pmap-c-que)#  pause buffer-size 728000 pause-threshold 364000
resume-threshold 362336
switch(config-pmap-c-que)# class type queuing c-in-q-default
switch(config-pmap-c-que)# bandwidth percent 10
switch(config-pmap-c-que)#
```

- **40G ISL の長距離ポリシー**

```
switch(config)# policy-map type queuing ld_40G_fcoe_in_que_policy
switch(config-pmap-que)# class type queuing c-in-q1
switch(config-pmap-c-que)# bandwidth percent 90
switch(config-pmap-c-que)# pause buffer-size 728000 pause-threshold 78208
resume-threshold 76544
switch(config-pmap-c-que)# class type queuing c-in-q-default
switch(config-pmap-c-que)# bandwidth percent 10
switch(config-pmap-c-que)#
```

```
switch(config)# policy-map type queuing ld_40G_fcoe_in_que_policy
switch(config-pmap-que)# class type queuing c-in-q1
switch(config-pmap-c-que)# bandwidth percent 90
switch(config-pmap-c-que)# pause buffer-size 1299584 pause-threshold 649792
resume-threshold 648128
switch(config-pmap-c-que)# class type queuing c-in-q-default
switch(config-pmap-c-que)# bandwidth percent 10
switch(config-pmap-c-que)#
```

入力バッファ サイズと一時停止/再開しきい値のカスタム ポリシー

長距離ポートを起動するのに十分なバッファがない場合は、デフォルト ポリシーを使用して10G/25Gイーサネット ポート（短距離要件、つまり 100 m 未満）に割り当てられたバッファを微調整する必要があります。長距離ポートを起動するのに十分なバッファが存在しない場合は、バッファ割り当て失敗のメッセージが表示されます。バッファ割り当て失敗メッセージの例は次のとおりです。

```
switch(config-if)# interface ethernet1/8
switch(config-if)# service-policy type queuing input ld_10G_fcoe_in_que_policy
switch(config-if)# no shutdown
2022 Oct 31 07:39:21 HW1 %$ VDC-1 %$ %ACLQOS-SLOT1-2-ACLQOS_FAILED: ACLQOS failure:
Ingress buffer allocation failed for interface Ethernet1/8
```

カスタムポリシーを作成して必要なバッファを解放し、既存のイーサネット ポートまたは短距離接続に使用される VFC にバインドされたイーサネット ポートに適用します。

```
switch(config)# policy-map type queuing 100m_fcoe_in_que_policy
switch(config-pmap-que)# class type queuing c-in-q1
switch(config-pmap-c-que)# bandwidth percent 50
```

```
switch(config-pmap-c-que)# pause buffer-size 41600 pause-threshold 20800 resume-threshold
 19136
switch(config-pmap-c-que)# class type queuing c-in-q-default
switch(config-pmap-c-que)# bandwidth percent 50
switch(config-pmap-c-que)#
```

長距離 FCoE ISL ごとに入力バッファを減らすために必要なイーサネット ポートの数

次の表に、特定の速度の単一の長距離 FCoE ISL に対応するために、入力バッファ サイズを縮小する必要があるイーサネット ポートの数を示します。

表 *5:* 入力バッファ サイズの削減に関する推奨事項

スピード	推奨
10G 長距離 ISL	1 つの 10G/25G ポートに 100m_fcoe_in_que_policy を適用
25G 長距離 ISL	5 つの 10G/25G ポートに 100m_fcoe_in_que_policy を適用
40G 長距離 ISL	9 つの 10G/25G ポートに 100m_fcoe_in_que_policy を適用

イーサネットインターフェイスに適用されるポリシーの構成例

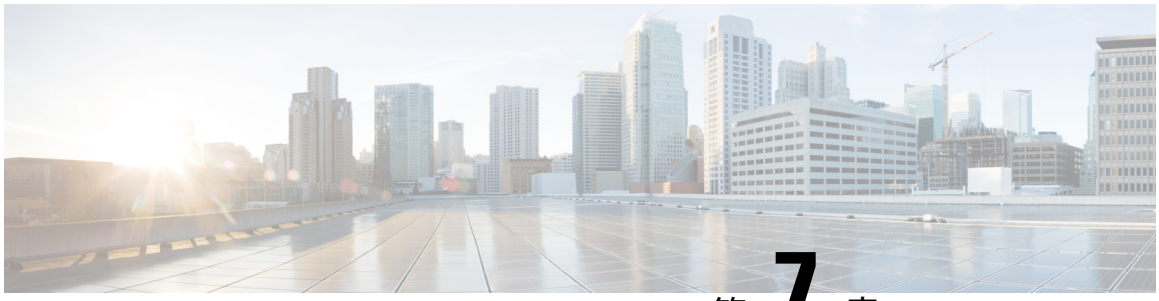
次のセクションでは、10G、25G、および40G FCoE長距離ISLを有効にするためにイーサネットインターフェイスに適用されるポリシーの設定例を示します。

```
switch(config)# interface ethernet 1/1
switch(config-if)# service-policy type queuing input ld_10G_fcoe_in_que_policy
switch(config-if)#

switch(config)# interface ethernet 1/2
switch(config-if)# service-policy type queuing input ld_25G_fcoe_in_que_policy
switch(config-if)#

switch(config)# interface ethernet 1/3
switch(config-if)# service-policy type queuing input ld_40G_fcoe_in_que_policy
switch(config-if)#

switch(config)# interface ethernet 1/4
switch(config-if)# service-policy type queuing input 100m_fcoe_in_que_policy
switch(config-if)#
```

Long-Distance Over FCoE の構成の確認

Long-Distance Over FCoE の構成情報を表示するには、次のいずれかのタスクを実行します。

コマンド	目的
show queuing interface eth *eth port*	割り当てられた入力バッファの可用性と一時停止/再開のしきい値を表示します。
show running-config interface ethernet *eth port*	構成の情報を表示します。



第 7 章

ファイバチャネル インターフェイスの構成0

この章は、次の内容で構成されています。

ファイバチャネル インターフェイスについて

ファイバチャネル インターフェイスについて

仮想ファイバ チャネル インターフェイス

Fibre Channel over Ethernet（FCoE）カプセル化により、物理イーサネット ケーブルでファイバ チャネルとイーサネット トラフィックを同時に伝送できます。Cisco Nexus デバイス では、FCoE 対応の物理イーサネット インターフェイスは、1 つの仮想のファイバ チャネル（vFC）インターフェイスのトラフィックを伝送できます。

vFC インターフェイスは、Cisco NX-OS の他のインターフェイスと同様に、設定やステータスなどのプロパティを持つ、操作可能なオブジェクトです。ネイティブ ファイバ チャネル インターフェイスと vFC インターフェイスは、同じ CLI コマンドを使用して設定します。

次の機能は、仮想ファイバ チャネル インターフェイスではサポートされません。

- SAN ポート チャネル

- SPAN 宛先を vFC インターフェイスにすることはできません。
- Buffer-to-Buffer credit（BB_credit）
- Exchange Link Parameter（ELP）
- 物理属性の設定（速度、レート、モード、トランスミッタ情報、MTU サイズ）
- ポート トラッキング

VF ポート

vFCインターフェイスは、常にトランク モードで実行されます。それ以外では、どのモードでも動作しません。vFCインターフェイスでは、**switchport trunk allowed vsan** コマンドを使用して vFC の許可 VSAN を設定できます（FC TF および TE ポートと類似）。ホストに接続されているvFCインターフェイスの場合、ログイン（FLOGI）をサポートするVSANはポートVSANだけです。VF ポートを設定する **switchport trunk allowed vsan** コマンドをインターフェイス モードで使用し、このような vFC インターフェイスの許可 VSAN をポート VSAN に制限することを推奨します。

160 vFC インターフェイスのサポートが含まれます。

Cisco Nexus デバイスは、vFC VSAN 割り当てとグローバルな VLAN-to-VSAN マッピング テーブルにより、VF ポートに対して適切な VLAN を選択できます。

10G-FEX インターフェイス経由の VF ポートのサポートは、各ファブリック エクステンダが Cisco Nexus デバイスに直接接続する、Cisco Nexus ファブリック エクステンダ ストレート型トポロジでのみサポートされます。

VE ポート

仮想 E ポート（VE ポート）は、非ファイバ チャネル リンク上の E ポートをエミュレートするポートです。Fibre Channel Forwarder（FCF）間の VE ポート接続は、ポイントツーポイント リンク上でサポートされます。このリンクは、個々のイーサネットインターフェイス、またはイーサネット ポートチャネル インターフェイスのメンバーです。FCF が接続された各イーサネットインターフェイスに、vFCインターフェイスを作成し、バインドする必要があります。インターフェイス モードで **switchport mode E** コマンドを使用して、vFC インターフェイスを VE ポートとして設定します。

VE ポートに関する注意事項は次のとおりです。

- vFC で auto モードはサポートされません。
- VE ポート トランキングは、FCoE 対応 VLAN 上でサポートされます。
- MACアドレスにバインドされているVEポートインターフェイスはサポートされません。
- デフォルトでは、VE ポートはトランク モードで有効になります。

  VE ポート上に複数の VSAN を構成できます。VE ポートの VSAN に対応する FCoE VLAN を、バインドしたイーサネット インターフェイスに構成する必要があります。

- スパニングツリー プロトコルは、vFC インターフェイスがバインドされたすべてのインターフェイスの FCoE VLAN 上で無効になります。これには、VE ポートがバインドされたインターフェイスが含まれます。

特定の FCF とピア FCF 間でサポートされる VE ポート ペアの数は、ピア FCF の FCF-MAC アドバタイジング機能に依存します。

- ピア FCF がそのすべてのインターフェイス上で同じ FCF-MAC アドレスをアドバタイズする場合、1 つの VE ポート上で FCF をピア FCF に接続できます。このようなトポロジでは、冗長性のために 1 つのポートチャネル インターフェイスを使用することを推奨します。
- ピア FCF が複数の FCF-MAC アドレスをアドバタイズする場合、VE ポート構成制限テーブルの制限が適用されます。

vPC トポロジの VE ポート

vPC トポロジの VE ポートに関する注意事項は次のとおりです。

- LAN トラフィック用の vPC 上で接続された FCF 間の FCoE VLAN には、専用リンクが必要です。
- FCoE VLAN はスイッチ間の vPC インターフェイス上に設定しないでください。
- FCoE ペイロード サイズが 2112 より大きい場合、VE ポートは輻輳中にフラップする可能性があります。

FSPF パラメータ

FSPF は、VSAN で起動されると、VE ポート上で VSAN 単位で動作します。vFC インターフェイスのデフォルトの FSPF コスト（メトリック）は、10 Gbps 単位の帯域幅です。イーサネット ポート チャネルにバインドされた VE ポートの場合、FSPF コストは動作可能なメンバー ポートの数に基づいて調整されます。

VE ポート設定の制限

インターフェイスタイプ	プラットフォーム			
	N9K-C9336C-FX2-E	N9K-C93360YC-FX2	N9K-C93180YC-FX	FEX
イーサネット ポート チャネル インターフェイスにバインドされている vFC（VE および VF）ポート	8（最大値）	8（最大値）	8（最大値）	サポート対象外

VNP ポート

FCoE NPV ブリッジから FCF への接続は、ポイントツーポイント リンク上でのみサポートされます。このリンクは、個々のイーサネット インターフェイス、またはイーサネット ポート チャネル インターフェイスのメンバーです。FCF が接続された各イーサネット インターフェイスに、vFC インターフェイスを作成し、バインドする必要があります。これらの vFC インターフェイスは、VNP ポートとして設定する必要があります。VNP ポートでは、FCoE NPV ブリッジが、それぞれ固有の eNode MAC アドレスが付いた複数の eNode を持つ FCoE 対応ホストをエミュレートします。MAC アドレスにバインドされる VNP ポート インターフェイスはサポートされません。デフォルトでは、VNP ポートはトランク モードでイネーブルになります。VNP ポートには、複数の VSAN を設定できます。VNP ポート VSAN に対応する FCoE VLAN を、バインドしたイーサネット インターフェイスに設定する必要があります。

スパニングツリープロトコル（STP）は、VNP ポートがバインドされたインターフェイス上の FCoE VLAN では自動的にディセーブルになります。

インターフェイス モード

スイッチ内の各物理ファイバチャネルインターフェイスは、複数のポートモード（Eモード、TE モード、F モード、および TF モードおよび TNP モード）のうちのいずれかで動作します。物理ファイバ チャネル インターフェイスを E ポートまたは F ポート、F ポート、または SD ポートとして設定できます。インターフェイスを auto モードに設定することもできます。ポート タイプは、インターフェイスの初期化中に判別されます。

NPV モードでは、ファイバ チャネル インターフェイスは F モード、または SD モードで動作します。NPモード、Fモード、SDモード で動作します。

仮想ファイバ チャネル インターフェイスは E モードまたは F モードで設定できます。

デフォルトでは、インターフェイスには VSAN 1 が自動的に割り当てられます。

各インターフェイスには、管理設定と動作ステータスが対応付けられています。

- 管理設定は、修正を加えない限り変更されません。この設定には、管理モードで設定できる各種の属性があります。
- 動作ステータスは、インターフェイス速度のような指定された属性の現在のステータスを表します。このステータスは変更できず、読み取り専用です。インターフェイスがダウンの状態のときは、値の一部（たとえば、動作速度）が有効にならない場合があります。

E ポート

拡張ポート（E ポート）モードでは、インターフェイスがファブリック拡張ポートとして機能します。このポートを別の E ポートに接続し、2 つのスイッチ間でスイッチ間リンク（ISL）を作成できます。E ポートはフレームをスイッチ間で伝送し、ファブリックを設定および管理できるようにします。リモート N ポート宛てフレームのスイッチ間コンジットとして機能します。E ポートは、クラス 3 およびクラス F サービスをサポートします。

別のスイッチに接続された E ポートも、SAN ポート チャネルを形成するように設定できます。

Related Topics

SAN ポート チャネルの設定 （141 ページ）

F ポート

ファブリック ポート（F ポート）モードでは、インターフェイスがファブリック ポートとして機能します。このポートは、ノードポート（N ポート）として動作する周辺装置（ホストまたはディスク）に接続できます。F ポートは、1 つの N ポートだけに接続できます。F ポートはクラス 3 サービスをサポートします。

NP ポート

スイッチが NPV モードで動作しているとき、スイッチをコア ネットワーク スイッチに接続するインターフェイスは NP ポートとして設定されます。NP ポートは N ポートと同様に動作しますが、複数の物理 N ポートに対するプロキシとして機能します。

Related Topics

N ポート バーチャライゼーションの構成

TE ポート

トランキング E ポート（TE ポート）モードでは、インターフェイスがトランキング拡張ポートとして機能します。別の TE ポートに接続し、2 つのスイッチ間で Extended ISL（EISL）を作成します。TE ポートは別の Cisco Nexus デバイス スイッチまたは Cisco MDS 9000 ファミリ スイッチに接続します。E ポートの機能を拡張して、次の内容をサポートします。

- VSAN トランキング
- ファイバ チャネル トレース（fctrace）機能

TE ポート モードでは、すべてのフレームが VSAN 情報を含む EISL フレーム フォーマットで送信されます。相互接続されたスイッチは VSAN ID を使用して、1 つまたは複数の VSAN からのトラフィックを同一の物理リンク上で多重化します。この機能は、Cisco Nexus デバイスでは VSAN トランキングと呼ばれます。TE ポートは、クラス 3 およびクラス F サービスをサポートします。

Related Topics

VSAN トランキングの設定

TF ポート

スイッチが NPV モードで動作しているとき、スイッチをコア ネットワーク スイッチに接続するインターフェイスは NP ポートとして設定されます。NP ポートは N ポートと同様に動作しますが、複数の物理 N ポートに対するプロキシとして機能します。

トランキング F ポート（TF ポート）モードでは、インターフェイスがトランキング拡張ポートとして機能します。トランキングした別の N ポート（TN ポート）または NP ポート（TNP ポート）に接続して、コア スイッチと NPV スイッチまたは HBA の間のリンクを作成し、タ

グ付きフレームを伝送できます。TFポートは、Fポートの機能を拡張して、VSANトランキングをサポートします。

TF ポート モードでは、すべてのフレームが、VSAN 情報を含む EISL フレーム フォーマットで送信されます。相互接続されたスイッチは VSAN ID を使用して、1 つまたは複数の VSAN からのトラフィックを同一の物理リンク上で多重化します。この機能は、Cisco Nexus デバイスでは VSAN トランキングと呼ばれます。TF ポートは、クラス 3 およびクラス F サービスをサポートします。

TNP ポート

トランキング NP ポート（TNP ポート）モードでは、インターフェイスがトランキング拡張ポートとして機能します。トランキングされた F ポート（TF ポート）に TNP ポートを接続して、NPV スイッチからコア NPIV スイッチへのリンクを作成することができます。

SD ポート

SPAN 宛先ポート（SD ポート）モードでは、インターフェイスがスイッチド ポート アナライザ（SPAN）として機能します。SPAN 機能は、ファイバ チャネル インターフェイスを通過するネットワーク トラフィックを監視します。このモニタリングは、SD ポートに接続された標準ファイバ チャネル アナライザ（または同様のスイッチ プローブ）を使用して行われます。SD ポートはフレームを受信しません。送信元トラフィックのコピーを送信するだけです。SPAN 機能は他の機能に割り込むことなく、SPAN 送信元ポートのネットワーク トラフィックのスイッチングに影響しません。

auto モード

auto モードに設定されたインターフェイスは、E ポート、F ポート、TE ポート、および TF ポート、NP ポートおよび TNP ポートのいずれかのモードで動作します。ポート モードは、インターフェイスの初期設定中に決定されます。たとえば、インターフェイスがノード（ホストまたはディスク）に接続されている場合、F ポート モードで動作します。インターフェイスがサードパーティ製のスイッチに接続されている場合、E ポート モードで動作します。インターフェイスが Cisco Nexus デバイス または Cisco MDS 9000 ファミリの別のスイッチに接続されている場合、TE ポート モードで動作できます。

Related Topics

VSAN トランキングの設定

インターフェイスの状態

インターフェイス ステートは、インターフェイスの管理設定および物理リンクのダイナミック ステートによって異なります。

管理ステート

管理のステートは、インターフェイスの管理設定を表します。次の表に、管理ステートを示します。

Table 6: 管理ステート

管理状態	説明
アップ	インターフェイスはイネーブルです。
下へ	インターフェイスはディセーブルです。インターフェイスをシャットダウンして管理上のディセーブル状態にした場合は、物理リンク層ステートの変更が無視されます。

動作ステート

動作ステートは、インターフェイスの現在の動作ステートを示します。次の表に、動作ステートを示します。

Table 7: 動作ステート

動作状態	説明
アップ	インターフェイスは、トラフィックを要求に応じて送受信しています。このステートにするためには、インターフェイスが管理上アップの状態、インターフェイス リンク層ステートがアップの状態で、インターフェイスの初期化が完了している必要があります。
下へ	インターフェイスが（データ）トラフィックを送信または受信できません。
トランキング	インターフェイスが TE または TF モードで正常に動作しています。

理由コード

理由コードは、インターフェイスの動作ステートによって異なります。次の表に、動作ステートの理由コードを示します。

Table 8: インターフェイス ステートの理由コード

管理設定	運用ステータス	理由コード
アップ	アップ	なし。
Down	Down	管理上ダウンされています。インターフェイスを管理上ダウンの状態に設定する場合、インターフェイスをディセーブルにします。トラフィックが受信または送信されません。
アップ	ダウン（Down）	次の表を参照してください。

管理ステートがupで、動作ステートがdownの場合、理由コードは、動作不能理由コードに基づいて異なります。次の表に、動作不能ステートの理由コードを示します。

Note 表に示されている理由コードは一部だけです。

Table 9: 動作不能ステートの理由コード

理由コード（長いバージョン）	説明	適用可能なモード
リンク障害または未接続	物理層リンクが正常に動作していません。	すべて（All）
SFP がありません	Small Form-Factor Pluggable（SFP）ハードウェアが接続されていません。	すべて（All）
初期化中	物理層リンクが正常に動作しており、プロトコル初期化が進行中です。	すべて（All）
Reconfigure fabric in progress	ファブリックが現在再設定されています。	
Offline	初期化を再試行する前に、スイッチソフトウェアが指定された R_A_TOV 時間待機します。	
非アクティブ	インターフェイスVSANが削除されているか、suspended ステートにあります。 インターフェイスを正常に動作させるには、設定されたアクティブなVSANにポートを割り当てます。	
ハードウェア障害（Hardware failure）	ハードウェア障害が検出されました。	
エラー ディセーブル化	エラー条件は、管理上の注意を必要とします。さまざまな理由でインターフェイスがエラーディセーブルになることがあります。次に例を示します。 • 設定障害。 • 互換性のない BB_credit 設定 インターフェイスを正常に動作させるには、まずこのステートの原因となるエラー条件を修正し、次にインターフェイスを管理上シャットダウンして、さらにまたは、インターフェイスをイネーブルにします。	

理由コード（長いバージョン）	説明	適用可能なモード
Isolation because limit of active port channels is exceeded.	スイッチにアクティブ SAN ポート チャネルの最大数がすでに設定されているので、インターフェイスは隔離されます。	
ELPが失敗したため、隔離されました	ポート ネゴシエーションが失敗しました。	E ポートと TE ポートのみ
ESCが失敗したため、隔離されました	ポート ネゴシエーションが失敗しました。	
ドメインの重複により隔離されました	Fibre Channel Domain（fcdomain）のオーバーラップ。	
Isolation due to domain ID assignment failure	割り当てられたドメイン ID が無効です。	
Isolation due to the other side of the link E port isolated	リンクのもう一方の端のEポートが分離しています。	
ファブリック再構成が無効なため、隔離されました	ファブリックの再設定によりポートが分離されました。	
ドメインマネージャがが無効なため、隔離されました	fcdomain 機能がディセーブルです。	
ゾーンのマージが失敗したため、隔離されました	ゾーン結合に失敗しました。	
Isolation due to VSAN mismatch	ISL の両端の VSAN が異なります。	
port channel administratively down	SAN ポート チャネルに所属するインターフェイスがダウンの状態です。	SAN ポート チャネル インターフェイスのみ
速度に互換性がないため、中断しました	SAN ポート チャネルに所属するインターフェイスに互換性のない速度が存在します。	
モードに互換性がないため、中断しました	SAN ポート チャネルに所属するインターフェイスに互換性のないモードが存在します。	
リモートスイッチWWNに互換性がないため、中断しました	不適切な接続が検出されました。SAN ポート チャネルのすべてのインターフェイスが同一のスイッチのスイッチ ペアに接続されている必要があります。	

理由コード（長いバージョン）	説明	適用可能なモード
Bound physical interface down	仮想ファイバ チャネル インターフェイスにバインドされたイーサネット インターフェイスが動作していません。	仮想ファイバ チャネル インターフェイスのみ
STP not forwarding in FCoE mapped VLAN	仮想ファイバ チャネル インターフェイスにバインドされたイーサネット インターフェイスが、仮想ファイバ チャネル インターフェイスに関連付けられたVLANに対してSTPフォワーディング ステートではありません。	仮想ファイバ チャネル インターフェイスのみ

バッファツーバッファ クレジット

BB_credit はフロー制御メカニズムで、ファイバ チャネル インターフェイスがフレームをドロップしないようにします。BB_creditは、ホップごとにネゴシエーションします。

BB_credit メカニズムは仮想ファイバチャネルインターフェイスではなく、ファイバチャネルインターフェイスで使用されます。受信 BB_credit では、ピアへの確認応答を必要とせずに、受信側の受信バッファの容量が決まります。これは、帯域幅遅延が大きいリンク（遅延が大きい長距離リンク）で、遅延時間が長い回線レート トラフィックを維持できるようにするうえで重要です。

受信 BB_credit（fcrxbbcredit）値を各ファイバ チャネル インターフェイスに設定できます。ほとんどの場合、デフォルト設定を変更する必要がありません。

仮想ファイバ チャネル インターフェイスの場合、BB_credit は使用されません。仮想ファイバー チャネル インターフェイスは、プライオリティ フロー制御と呼ばれるクラス ベースの一時停止メカニズムに基づいたフロー制御を提供します。 プライオリティ フロー制御

Note

- バッファ間（B2B）クレジットは構成できません。
- 8G リンクのフィル パターンは IDLE でなければなりません。両方のピアで、8G リンクのフィル パターンを IDLE に設定する必要があります。コマンド **switchport fill-pattern IDLE speed** *speed* を使用して、Cisco Nexus 9000 スイッチでフィル パターンを IDLE に設定します。

```
switch (config)# interface fc1/1
switch (config-if)# switchport fill-pattern IDLE speed 8000
```

Note 受信BB_credit値は、ポートモードによって異なります。物理ファイバチャネルインターフェイスの場合、Fモードおよび E モード インターフェイスのデフォルト値は 64 です。必要に応じて、この値を変更できます。最大値は 240 です。

受信 B2B クレジット値は、N9K-C93180YC-FX では64、N9K-C93360YC-FX2 および N9K-C9336C-FX2-E では 32 です。これは、両方のプラットフォームのすべてのポート モード (F、E) に適用され、変更できません。

ファイバチャネルのライセンス要件

ファイバ チャネル インターフェイスとその機能を使用する前に、正しいライセンスがインストールされていることを確認します。ライセンスの詳細については、このガイドの*FC/FCoE*の有効化の章を参照してください。

Note Storage Protocol Services ライセンスなしで仮想ファイバ チャネル インターフェイスを設定できますが、ライセンスがアクティブになるまでこれらのインターフェイスは動作状態になりません。

ファイバ チャネル ポート ライセンスの有効化

ここでは、SAN スイッチングのライセンスを有効にする方法について説明します。

始める前に

ポート ライセンスを有効にするには、ファイバ チャネル（FC）ポートをシャットダウンする必要があります。

（注） FC ポートへの変換については、ユニファイド ポートの設定を参照してください。

手順の概要

1. ポート ライセンスを有効にします。

手順の詳細

手順

ポート ライセンスを有効にします。

例：

```
Switch(config)# int fc1/1
Switch(config-if)# port-license acquire
```

ファイバ チャネルの QOS 要件

次のタイプのインターフェイスが使用されている場合は、FCoE QoS を設定する必要があります。

- ネイティブ FC - FC の場合
- FCoE - vFC の場合
- FC および FCoE - FC および vFC の場合

スイッチでイーサネットが設定されていない場合でも、FCoE QoS を追加する必要があります。

次のコマンドは、ネイティブ FC または FCoE、または FC と FCoE 用に構成する必要があるデフォルトの QoS 構成を有効にします。

```
switch(config)# system qos
switch(config-sys-qos)# service-policy type queuing input fcoe-default-in-policy
switch(config-sys-qos)# service-policy type queuing output fcoe-default-out-policy
switch(config-sys-qos)# service-policy type qos input fcoe-default-in-policy
switch(config-sys-qos)# service-policy type network-qos fcoe-default-nq-policy
```

QoS の構成による no-drop のサポート

ingress FC/FCoE フレームをマークするには、qos ingress ポリシーが使用されます。qos ingress ポリシーは、FC/FCoE トラフィックを処理するインターフェイスに適用する必要があります（vFC にバインドされるすべてのイーサネット/ポートチャネル インターフェイスなど）。

（注）

ポート qos 領域にハードウェア TCAM スペースが予約されていることを確認します。入力 PACL TCAM しきい値が syslog に表示される場合は常に、TCAM サイズを増やし、スイッチをリロードします。

この手順は、FCoE NPV が機能するために必須です。

- ポートの ACL 領域用に、TCAM スペースを予約します。

  他の領域用に予約された TCAM スペースを取得することが必要な場合があります。

- 設定を保存します。
- ライン カードまたはスイッチをリロードします。

  スイッチをリロードします。

- ACL 領域の TCAM スペースを確認します。
- N9K-C93180YC-FX、N9K-C93360YC-FX2、および N9K-C9336C-FX2-E での TCAM カービングの例：

```
hardware access-list tcam region ing-racl 1536
hardware access-list tcam region ing-ifacl 256
hardware access-list tcam region ing-redirect 256
```

- N9K-C92160YC-X、N9K-C9272Q、N9K-C93236C、N9K-C93180YC-EX、または N9K-C93180YC-FX での TCAM カービングの例

```
hardware access-list tcam region ing-racl 1536
hardware access-list tcam region ing-redirect 256
```

例：

```
switch# show hardware access-list tcam region |i i ifacl
Ingress PACL [ing-ifacl] size =  256
switch# config


switch(config)# hardware access-list tcam region ing-racl 1536
switch(config)# hardware access-list tcam region ing-ifacl 256
switch(config)# hardware access-list tcam region ing-redirect 256



switch# copy running-config startup-config
switch# reload

switch# show hardware access-list tcam region |i i ifacl
Ingress PACL [ing-ifacl] size =  256


switch# show hardware access-list tcam region | i "IPV4 Port QoS \[qos\] size"
Ingress PACL [ing-ifacl] size =  256
switch# config

switch(config)# hardware access-list tcam region ing-racl 1536
switch(config)# hardware access-list tcam region ing-ifacl 256
```

```
switch(config)# hardware access-list tcam region ing-redirect 256


switch# copy running-config startup-config

switch# reload

switch# show hardware access-list tcam region | i "IPV4 Port QoS \[qos\] size"
Ingress PACL [ing-ifacl] size =  256
```

FCoE QoS ポリシーの設定

- FCoE のデフォルト ポリシーには、network-qos、output queuing、input queuing の 4 種類があります。
- FCoE デフォルト ポリシーをアクティブにするには、**feature-set fcoe-npv** コマンドを使用して FCoE-NPV 機能を有効にし、**no feature-set fcoe-npv** コマンドを実行して FCoE デフォルト ポリシーを削除します。
- **no feature-set fcoe-npv** を入力する前に、インターフェイスおよびシステム レベルからすべての FCoE ポリシーを削除します。**no feature-set fcoe-npv** コマンドは、FC ポートが設定されていない場合にのみ使用できます。

（注） FCoE のデフォルト ポリシーを使用することを推奨します。適用されるすべてのポリシーは、同じタイプ（4q または 8q モード）である必要があり、システムおよびインターフェイス レベルで明示的に適用または削除する必要があります。

- FCoE に対して有効化された active-active FEX トポロジの QoS ポリシーを構成するとき、予期せぬ結果を避けるために、両方の VPC ピアの FEX HIF ポートで QoS ポリシーを構成しなければなりません。

（注） Active/Active FEXトポロジをサポートするのは、次のものだけです。

- N2K-C2232PP
- N2K-C2348UPQ
- NB22HP
- NB22IBM

- FCoE トラフィックに異なるキューまたは cos 値を使用するには、ユーザー定義のポリシーを作成します。

FC/FCoE の QoS ポリシーの構成

- FC/FCoE のデフォルト ポリシーには、network-qos、output queuing、input queuing、および qos の 4 種類があります。
- FC/FCoE トラフィックに別のキューまたは cos 値を使用するには、ユーザー定義のポリシーを作成します。
- これらの方法の 1 つに従って QoS ポリシーを構成できます。
  - 定義済みポリシー：要件に合わせて事前定義されたネットワーク QoS ポリシー（**default-fcoe-in-policy**）を適用できます。

（注）
- デフォルトでは、FCoEに適用されるポリシーはありません。
- **no-stats** を QoS ポリシーに適用することを推奨します。

  - ユーザー定義のポリシー：システム定義ポリシーの1つに準拠するQoSポリシーを作成できます。

システム全体の QoS ポリシーの設定

（注） FC/FCoE トラフィックを伝送するすべてのインターフェイスについて、ネットワーク QoS ポリシーと出力/入力キューイング ポリシーをシステム レベルで適用し、qos ポリシーをインターフェイス レベルで適用する必要があります。

```
switch(config)# system qos
switch(config-sys-qos)# service-policy type queuing input default-fcoe-in-que-policy
switch(config-sys-qos)# service-policy type queuing output { default-fcoe-8q-out-policy
 | default-fcoe-out-policy }
switch(config-sys-qos)# service-policy type network-qos { default-fcoe-8q-nq-policy |
default-fcoe-nq-policy }
```

ユーザー定義ポリシーの設定例

```
switch(config)# policy-map type network-qos fcoe_nq
switch(config-pmap-nqos)# class type network-qos c-nq1
switch(config-pmap-nqos-c)# pause pfc-cos 3
switch(config-pmap-nqos-c)# mtu 9216
switch(config-pmap-nqos-c)# class type network-qos c-nq2
switch(config-pmap-nqos-c)# mtu 1500
switch(config-pmap-nqos-c)# class type network-qos c-nq3
switch(config-pmap-nqos-c)# mtu 1500
switch(config-pmap-nqos-c)# class type network-qos c-nq-default
switch(config-pmap-nqos-c)# mtu 1500
switch(config-pmap-nqos-c)# exit
switch(config-pmap-nqos)# exit
switch(config)#
switch(config)# policy-map type queuing fcoe-in-policy
```

```
switch(config-pmap-que)# class type queuing c-in-q1
switch(config-pmap-c-que)# bandwidth percent 50
switch(config-pmap-c-que)# class type queuing c-in-q-default
switch(config-pmap-c-que)# bandwidth percent 50
switch(config-pmap-c-que)# exit
switch(config)
switch(config)# policy-map type queuing fcoe-out-policy
switch(config-pmap-que)# class type queuing c-out-q3
switch(config-pmap-c-que)# priority level 1
switch(config-pmap-c-que)# class type queuing c-out-q-default
switch(config-pmap-c-que)# bandwidth remaining percent 50
switch(config-pmap-c-que)# class type queuing c-out-q1
switch(config-pmap-c-que)# bandwidth remaining percent 50
switch(config-pmap-c-que)# class type queuing c-out-q2
switch(config-pmap-c-que)# bandwidth remaining percent 0
switch(config-pmap-c-que)# exit
switch(config)#
switch(config)# class-map type qos match-any fcoe
switch(config-cmap-qos)# match protocol fcoe
switch(config-cmap-qos)# match cos 3
switch(config-cmap-qos)# exit
switch(config)#
switch(config)# policy-map type qos fcoe_qos_policy
switch(config-pmap-qos)# class fcoe
switch(config-pmap-c-qos)# set cos 3
switch(config-pmap-c-qos)# set qos-group 1
switch(config-pmap-c-qos)# exit
switch(config-pmap-qos)# exit
switch(config)#
switch(config)# system qos
switch(config-sys-qos)# service-policy type queuing input fcoe-in-policy
switch(config-sys-qos)# service-policy type queuing output fcoe-out-policy
switch(config-sys-qos)# service-policy type network-qos fcoe_nq
```

（注） QOS ポリシーでの **set cos 3** コマンドは、ネイティブファイバチャネルポートがある場合にのみ必須で、N9K-C93180YC-FX プラットフォーム、N9K-C93360YC-FX2 プラットフォーム、および N9K-C9336C-FX2-E にのみ適用されます。他のすべての Cisco Nexus 9000 プラットフォームスイッチでは、この手順はオプションです。

（注） FEX が接続されている場合：

- システム レベルおよび HIF ポートに QoS ポリシーを適用して、FCoE トラフィックのポーズ フレームを受け入れます。
- FEX がオンラインの場合、8q ポリシーはサポートされません。

```
switch(config)# system qos
switch(config-sys-qos)# service-policy type queuing input policy-name
switch(config-sys-qos)# service-policy type queuing output policy-name
switch(config-sys-qos)# service-policy type network-qos policy-name
switch(config-sys-qos)# service-policy type qos input policy-name
```

FC/FCoE の VFC インターフェイスにバインドされている個々のイーサネット/ポートチャネル インターフェイスに対し、ingress QoS ポリシーを適用します。

```
switch(config)# interface ethernet 2/1
switch(config-if)# switchport mode trunk
switch(config-if)# mtu 9216 /* Or maximum allowed value */
switch(config-if)# service-policy type qos input { default-fcoe-in-policy | fcoe_qos_policy
 )  no-stats
switch(config-if)# exit
switch(config)#
```

（注） QoS ポリシーは、HIF インターフェイスまたは HIF インターフェイスのポート チャネルにアタッチする必要があります。

- HIF インターフェイス

```
interface "HIF port"
service-policy type qos input policy-name
```

- HIF インターフェイスのポート チャネル

```
interface port-channel
service-policy type qos input policy-name
```

（注） 次のプラットフォームは 8q ポリシーをサポートしていません。

- Cisco Nexus 9332PQ スイッチ
- Cisco Nexus C9372PX スイッチ
- Cisco Nexus C9396PX switch
- Cisco Nexus C9372PX-E スイッチ
- Cisco Nexus X9536C-S ライン カード
- Cisco Nexus X9564PX ライン カード

- FC/FCoE QoS ポリシーの設定
  - FC/FCoE のデフォルト ポリシーには、ネットワーク QoS、出力キューイング、入力キューイング、QoS の 4 種類があります。
  - FCoE デフォルト ポリシーをアクティブにするには、**feature-set fcoe-npv** コマンドを使用して FCoE-NPV 機能を有効にし、**no feature-set fcoe-npv** コマンドを実行して FCoE デフォルト ポリシーを削除します。

- **no feature-set fcoe-npv** を入力する前に、インターフェイスおよびシステム レベルからすべての FCoE ポリシーを削除します。

（注） FCoE のデフォルト ポリシーを使用することを推奨します。適用されるすべてのポリシーは、同じタイプ（4q または 8q モード）である必要があり、システムおよびインターフェイス レベルで明示的に適用または削除する必要があります。

- FC/FCoE トラフィックに別のキューまたは cos 値を使用するには、ユーザー定義のポリシーを作成します。

- FC/FCoE のネットワーク QoS ポリシーの構成
  - これらの方法の 1 つに従ってネットワーク QoS ポリシーを設定できます。
    - 定義済みポリシー：要件に合わせて事前定義されたネットワーク QoS ポリシーを適用できます。**default-fcoe-8q-nq-policy** または **default-fcoe-nq-policy** を選択するオプションがあります。

（注） デフォルトでは、FC/FCoE に適用されるポリシーはありません。

    - ユーザ定義のポリシー：システム定義ポリシーの 1 つに準拠するネットワークの QoS ポリシーを作成できます。

- FC/FCoE の出力キューイング ポリシーの構成
  - これらの方法の 1 つに従って、出力キューイング ポリシーを構成できます。
    - 定義済みポリシー：要件に合わせて事前定義された出力キューイング ポリシーを適用できます。**default-fcoe-8q-out-policy** または **default-fcoe-out-policy** を選択するオプションがあります。

（注） デフォルトでは、FC/FCoE に適用されるポリシーはありません。

    - ユーザー定義のポリシー：システム定義ポリシーの 1 つに準拠する出力キューイング ポリシーを作成できます。

- FC/FCoE の入力キューイング ポリシーの構成
  - これらの方法の 1 つに従って、入力キューイング ポリシーを構成できます。
    - 定義済みポリシー：定義済み入力キューイングポリシーを適用できます。**default-fcoe-in-que-policy**

（注） デフォルトでは、FCoE に適用されるポリシーはありません。

- ユーザー定義のポリシー：システム定義ポリシーの 1 つに準拠する入力キューイング ポリシーを作成できます。

- FCoE の QoS ポリシーの構成
  - これらの方法の 1 つに従って QoS ポリシーを構成できます。
    - 定義済みポリシー：要件に合わせて事前定義されたネットワーク QoS ポリシー（**default-fcoe-in-policy**）を適用できます。

（注）
- デフォルトでは、FCoEに適用されるポリシーはありません。
- **no-stats** を QoS ポリシーに適用することを推奨します。

    - ユーザー定義のポリシー：システム定義ポリシーの1つに準拠するQoSポリシーを作成できます。

- システム全体の QoS ポリシーの設定

（注） FCoE トラフィックを伝送するすべてのインターフェイスについて、ネットワークQoSポリシーと出力/入力キューイングポリシーをシステム レベルで適用し、qosポリシーをインターフェイス レベルで適用する必要があります。

```
switch(config)# system qos
switch(config-sys-qos)# service-policy type queuing input default-fcoe-in-que-policy
switch(config-sys-qos)# service-policy type queuing output { default-fcoe-8q-out-policy
 | default-fcoe-out-policy }
switch(config-sys-qos)# service-policy type network-qos { default-fcoe-8q-nq-policy
 | default-fcoe-nq-policy }
```

- ユーザー定義ポリシーの設定例

```
switch(config)# policy-map type network-qos fcoe_nq
switch(config-pmap-nqos)# class type network-qos c-nq1
switch(config-pmap-nqos-c)# pause pfc-cos 3
switch(config-pmap-nqos-c)# mtu 9216
switch(config-pmap-nqos-c)# class type network-qos c-nq2
switch(config-pmap-nqos-c)# mtu 1500
switch(config-pmap-nqos-c)# class type network-qos c-nq3
switch(config-pmap-nqos-c)# mtu 1500
switch(config-pmap-nqos-c)# class type network-qos c-nq-default
switch(config-pmap-nqos-c)# mtu 1500
```

```
switch(config-pmap-nqos-c)# exit
switch(config-pmap-nqos)# exit
switch(config)#
switch(config)# policy-map type queuing fcoe-in-policy
switch(config-pmap-que)# class type queuing c-in-q1
switch(config-pmap-c-que)# bandwidth percent 50
switch(config-pmap-c-que)# class type queuing c-in-q-default
switch(config-pmap-c-que)# bandwidth percent 50
switch(config-pmap-c-que)# exit
switch(config)
switch(config)# policy-map type queuing fcoe-out-policy
switch(config-pmap-que)# class type queuing c-out-q3
switch(config-pmap-c-que)# priority level 1
switch(config-pmap-c-que)# class type queuing c-out-q-default
switch(config-pmap-c-que)# bandwidth remaining percent 50
switch(config-pmap-c-que)# class type queuing c-out-q1
switch(config-pmap-c-que)# bandwidth remaining percent 50
switch(config-pmap-c-que)# class type queuing c-out-q2
switch(config-pmap-c-que)# bandwidth remaining percent 0
switch(config-pmap-c-que)# exit
switch(config)#
switch(config)# class-map type qos match-any fcoe
switch(config-cmap-qos)# match protocol fcoe
switch(config-cmap-qos)# match cos 3
switch(config-cmap-qos)# exit
switch(config)#
switch(config)# policy-map type qos fcoe_qos_policy
switch(config-pmap-qos)# class fcoe
switch(config-pmap-c-qos)# set cos 3
switch(config-pmap-c-qos)# set qos-group 1
switch(config-pmap-c-qos)# exit
switch(config-pmap-qos)# exit
switch(config)#
switch(config)# system qos
switch(config-sys-qos)# service-policy type queuing input fcoe-in-policy
switch(config-sys-qos)# service-policy type queuing output fcoe-out-policy
switch(config-sys-qos)# service-policy type network-qos fcoe_nq
```

（注） QOS ポリシーでの **set cos 3** コマンドは、ネイティブファイバチャネルポートがある場合にのみ必須で、N9K-C93180YC-FX プラットフォームにのみ適用されます。他のすべての Cisco Nexus 9000 プラットフォーム スイッチでは、この手順はオプションです。

（注） FEX が接続されている場合：

- システム レベルおよび HIF ポートに QoS ポリシーを適用して、FCoE トラフィックのポーズ フレームを受け入れます。
- FEX がオンラインの場合、8q ポリシーはサポートされません。

```
switch(config)# system qos
switch(config-sys-qos)# service-policy type queuing input
 policy-name
switch(config-sys-qos)# service-policy type queuing output
 policy-name
switch(config-sys-qos)# service-policy type network-qos
policy-name
switch(config-sys-qos)# service-policy type qos input
policy-name
```

FCoE の VFC インターフェイスにバインドされている個々のイーサネット/ポートチャネル インターフェイスに対し、ingress QoS ポリシーを適用します。

```
switch(config)# interface ethernet 2/1
switch(config-if)# switchport mode trunk
switch(config-if)# mtu 9216 /* Or maximum allowed value */
switch(config-if)# service-policy type qos input { default-fcoe-in-policy |
fcoe_qos_policy }
switch(config-if)# exit
switch(config)#
```

（注） QoS ポリシーは、HIF インターフェイスまたは HIF インターフェイスのポート チャネルにアタッチする必要があります。

- HIF インターフェイス

```
interface "HIF port"
service-policy type qos input policy-name
```

- HIF インターフェイスのポート チャネル

```
interface port-channel
service-policy type qos input policy-name
```

（注） 次のプラットフォームは 8q ポリシーをサポートしていません。

- Cisco Nexus 9332PQ スイッチ
- Cisco Nexus C9372PX スイッチ
- Cisco Nexus C9396PX switch
- Cisco Nexus C9372PX-E スイッチ
- Cisco Nexus X9536C-S ライン カード
- Cisco Nexus X9564PX ライン カード

（注） Syslog にラベル割り当ての失敗が表示される場合は常に、FC/FCoE ACL がインターフェイスに適用されていない可能性があります。次に、QoS ポリシーがインターフェイスに no-stats で適用されているかどうかを確認する必要があります。

物理ファイバチャネル インターフェイス

Cisco Nexus C93180YC-FX および C93360YC-FX2 スイッチは、SAN ネットワークに接続されたアップリンクまたは（サーバーまたはターゲットに接続された）ダウンリンクとして、それぞれ最大 48 および 96 の物理ファイバチャネル（FC）インターフェイスをサポートします。Cisco Nexus N9K-C9336C-FX2-E スイッチには、SAN ネットワークに接続されたアップリンクまたはダウンリンク (サーバまたはターゲットに接続された) として、最大 112 個の物理ファイバチャネル（FC）ブレークアウトインターフェイスを含めることができます。FC ブレークアウトで変換できるのは、9 ～ 36 のポートのみです。

各ファイバ チャネル ポートをダウンリンク（サーバに接続）、またはアップリンク（データセンター SAN ネットワークに接続）として使用できます。ファイバ チャネル インターフェイスは、E、F、NP、SD、TE、および TF および TNP のモードをサポートします。

Note NP および TNP は、機能 fcoe-npv でのみサポートされます。

長距離 ISL

Cisco NX-OS リリース 10.2(1)F 以降、Cisco Nexus N9K-C93180YC-FX および N9K-C93360YC-FX2 スイッチは、32 Gbps ファイバ チャネル スイッチ間リンク（ISL）での長距離をサポートします。

ファイバチャネル インターフェイスの構成0

長距離 ISL BB_credit を計算するための公式は、2 KB の一般的なファイバー チャネル フレームとインターフェイス速度を想定しています。新しいスイッチの固定（64）バッファ間クレジットは、最大 3 キロメートルの距離にわたって 32 Gbps ファイバチャネル ISL をサポートするようになりました。

表 *10* : さまざまな速度での *FC* 長距離

スピード	ディスタンス
32G	3 km
16G	5 km
8G	10 km

表 *11* : さまざまな速度での *FC* 長距離

スピード	ディスタンス	**Throughput**
32G	3 km	25.45G
16G	5 km	13.35G
8G	10 km	6.67G

ファイバチャネル インターフェイスの構成0

ファイバチャネル インターフェイスの構成

ファイバ チャネル インターフェイスを設定する手順は、次のとおりです。

Note FC ポートの作成またはポート変換については、ユニファイド ポートの設定セクションを参照してください。

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **interface** {**fc** *slot*/*port*}|{**vfc** *vfc-id*}

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configuration terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface** {**fc** *slot*/*port*}|{**vfc** *vfc-id*}	ファイバ チャネル インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。 **Note** ファイバ チャネル インターフェイスが設定された場合、自動的に一意の World Wide Name（WWN）が割り当てられます。インターフェイスの動作状態がアップの場合、ファイバチャネル ID（FC ID）も割り当てられます。 **Note** これが 10G ブレイクアウト ポートの場合、*slot*/*port* 構文は *QSFP-module*/*port* になります。 **Note** これが QSFP+ GEM またはブレイクアウト ポートの場合、*port* 構文は *QSFP-module*/*port* になります。

ファイバ チャネル インターフェイスの範囲の構成

ファイバ チャネル インターフェイスの範囲を設定する手順は、次のとおりです。

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **interface** { **fc** *slot*/*port - port* [, **fc** *slot*/*port - port*] | **vfc** *vfc-id - vfc-id* [, **vfc** *vfc-id - vfc-id*] }

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configuration terminal**	構成モードに入ります。

	Command or Action	Purpose
ステップ 2	switch(config)# **interface** { **fc** *slot*/*port* - *port* [, **fc** *slot*/*port* - *port*] | **vfc** *vfc-id* - *vfc-id* [, **vfc** *vfc-id* - *vfc-id*] }	ファイバ チャネル インターフェイスの範囲を選択し、インターフェイス コンフィギュレーション モードを開始します。 **Note** これが QSFP+ GEM またはブレイクアウト ポートの場合、*port* 構文は *QSFP-module*/*port* になります。

インターフェイスの管理状態の設定

インターフェイスを正常にシャットダウンする手順は、次のとおりです。

トラフィック フローを有効に無効にする手順は、次のとおりです。

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **interface** {**fc** *slot*/*port*}|{**vfc** *vfc-id*}
3. switch(config-if)# **shutdown**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configuration terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface** {**fc** *slot*/*port*}|{**vfc** *vfc-id*}	ファイバ チャネル インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。 **Note** これが 10G ブレイクアウト ポートの場合、*slot*/*port* 構文は *QSFP-module*/*port* になります。 **Note** これが QSFP+ GEM またはブレイクアウト ポートの場合、*port* 構文は *QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **shutdown**	インターフェイスを正常にシャットダウンし、トラフィック フローを管理上ディセーブルにします（デフォルト）。

インターフェイス モードの設定

SUMMARY STEPS

1. **configure terminal**
2. switch(config) # **interface vfc** *vfc-id*}
3. switch(config-if) # **switchport mode** {**F**}

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **interface vfc** *vfc-id*} **Example:** `switch(config) # interface vfc 20` `switch(config-if) #`	仮想ファイバチャネルインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if) # **switchport mode** {**F**} **Example:** `switch(config-if) # switchport mode F` `switch(config-if) #`	ポート モードを設定します。 vFC インターフェイスは F モードのみをサポートします。 **Note** SD ポートを自動では設定できません。このポートは管理上設定する必要があります。

Example

次に、VE ポート 20 を設定し、イーサネット スロット 1、ポート 3 にバインドする例を示します。

```
switch# config t
switch(config) # interface vfc 20
switch(config-if) # bind interface ethernet 1/3
switch(config-if) # switchport mode F
switch(config-if) # exit
switch#
```

次に、イーサネット slot1、ポート 3 インターフェイスにバインドされた vFC 20 の実行コンフィギュレーションの例を示します。

```
switch# show running-config
switch(config) # interface vfc20
```

```
switch(config-if) # bind interface Ethernet 1/3
switch(config-if) # switchport mode F
switch(config-if) # no shutdown
```

次に、VNP ポート 10 を設定し、イーサネット スロット 1、ポート 1 にバインドする例を示します。

```
switch # config t
switch(config) # interface vfc 10
switch(config-if) # bind interface ethernet 2/1
switch(config-if) # switchport mode NP
switch(config-if) # exit
switch#
```

インターフェイスの説明の構成

インターフェイスの説明は、トラフィックを識別したり、インターフェイスの使用状況を知る場合に役立ちます。インターフェイスの説明には、任意の英数字の文字列を使用できます。

インターフェイスの説明を設定する手順は、次のとおりです。

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **interface** {**fc** *slot*/*port*}|{**vfc** *vfc-id*}
3. switch(config-if)# **switchport description cisco-HBA2**
4. switch(config-if)# **no switchport description**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configuration terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface** {**fc** *slot*/*port*}|{**vfc** *vfc-id*}	ファイバ チャネル インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。 **Note** これが 10G ブレイクアウト ポートの場合、*slot*/*port* 構文は *QSFP-module*/*port* になります。 **Note** これが QSFP+ GEM またはブレイクアウト ポートの場合、*port* 構文は *QSFP-module*/*port* になります。

	Command or Action	Purpose
ステップ 3	switch(config-if)# **switchport description cisco-HBA2**	インターフェイスの説明を設定します。ストリングの長さは、最大 80 文字まで可能です。
ステップ 4	switch(config-if)# **no switchport description**	インターフェイスの説明をクリアします。

ユニファイド ポートの設定

始める前に

サポートされる Cisco Nexus スイッチが存在することを確認します。ユニファイド ポートは、Cisco Nexus C93180YC-FX スイッチ、N9K-C9336C-FX2-E、および C93360YC-FX2 スイッチで使用できます。

- Cisco Nexus 5672UP
- Cisco Nexus 5672UP-16G
- N56-M24UP2Q LEM を搭載した Cisco Nexus 56128P
- N5696-M20UP LEM を搭載した Cisco Nexus 5696Q

（注） C93180YC-FX、N9K-C9336C-FX2-E、または C93360YC-FX2 プラットフォームの詳細については、*Cisco Nexus 9000 Series Hardware Installation Guide* を参照してください。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **slot** *slot number*	スイッチ上のスロットを指定します。 （注） これが QSFP+ GEM またはブレイクアウト ポートの場合、*port* 構文は *QSFP-module*/*port* になります。
ステップ 3	switch(config-slot) # **port** *port number* **type** {**ethernet** | **fc**}	ユニファイド ポートをネイティブ ファイバ チャネル ポートおよびイーサネット ポートとして設定します。

	コマンドまたはアクション	目的
		• **type** ：シャーシのスロット上で設定するポートのタイプを指定します。 • **ethernet** ：イーサネット ポートを指定します。 • **fc** ：ファイバ チャネル（FC）ポートを指定します。 • **breakout** ：ポート タイプをイーサネット ポートから FC ポートに変更または分割します。ただし、このオプションはN9K-C9336C-FX2-E でのみサポートされます。 （注） • 拡張モジュール上のユニファイド ポートを変更するには、GEM カードの電源を再投入する必要があります。変更を有効にするためにスイッチ全体をリブートする必要はありません。 • ユニファイド ポートをファイバ チャネルとして設定する場合、ファイバ チャネル インターフェイスおよび VSAN メンバーシップの既存の設定は影響を受けません。 • N9K-C93180YC-FX スイッチでは、FC ポート範囲は4 の倍数にする必要があります。不連続にすることもできます。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。 • N9K-C93360YC-FX2 スイッチでは、カラム内の 4 つの前面パネルポートすべてをまとめて FC/イーサネットに変換する必要があります。このスイッチでは、4 つのポートがポート グループを形成します。たとえば、最初のポートグループは、1、2、49、50 です。 2 番目のポートグループは、3、4、51、52 になり、以下も同様です。 • N9K-C9336C-FX2-E スイッチでは、ポート タイプ (9 ～ 36 など) を FC ブレークアウト ポートとして変換できます。ポートは、連続した範囲 (たとえば、9 ～ 11)、非連続的な範囲 (たとえば、18、23、30)、または単一のポート (たとえば、36) の FC ブレークアウト ポートとして変換することもできます。 （注）

	コマンドまたはアクション	目的
		N5672-16G で FC ポートを構成する場合、16G をサポートするには、ファブリック モードを 40G モードにする必要があります。ポートがイーサネットから FC に変更されると、次回のリロード時にファブリック モードが 40G に変更されます。初めてポートを FC に変更すると、次のメッセージが表示されます：「ポートの種類が変更されました。ファブリックモードも変更されます。設定を保存して、スイッチをリロードしてください」。 現在のファブリック モード設定を確認するために使用します。 **show fabric-mode** FC ポート範囲は 4 の倍数にする必要があります。不連続にすることもできます。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。
ステップ 4	switch(config-slot) # **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
ステップ 5	switch(config-slot) # **reload**	スイッチをリブートします。
ステップ 6	switch(config) # **slot** *slot number*	スイッチ上のスロットを指定します。
ステップ 7	switch(config-slot) # **no port** *port number* **type fc**	copy r s を実行してスイッチをリロードした後、ポートをイーサネット ポートに戻します。 （注） すべての FC ポートが削除されると、ファブリック モードは 10-G モードに変わります。すべてのポートをイーサネットに変更すると、次のメッセージが表示されます。「ポートの種類が変更されました。ファブリックモードも変更されます。設定を保存して、スイッチをリロードしてください」。

例

次の例は、C93180YC-FX 拡張モジュールでユニファイド ポートを設定する方法を示したものです。

```
switch# configure terminal
switch(config)# slot 1
switch(config-slot)# port 1-16 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
switch(config-slot)#
```

（注） N9K-C93180YC-FX および N9K-C93360YC-FX2 スイッチでは、個々のポートを FC ポートに変換できません。 。N5672UP-16G では、スロット 2 のみに UP ポートがあります。

```
switch# configure terminal
switch(config)# slot 1
switch(config-slot)# port 1-24 type fc
Port type is changed. ACTION REQUIRED: Please save configurations and reload the switch
switch(config-slot)#
```

または

```
switch# configure terminal
switch(config)# slot 2
switch(config-slot)# port 13-24 type fc
Port type is changed. Please power-off and no power-off the module
switch(config-slot)#
```

次の例は、スロット 1、10 ポートを Cisco N6004X–M20UP モジュールの FC ポートとして設定する方法を示しています。

```
switch# configure terminal
switch(config)# slot 1
switch(config-slot)# port 1-10 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
```

ポート速度の設定

ポート速度は、仮想ファイバチャネル インターフェイスではなく、物理ファイバチャネル インターフェイスで設定できます。サポートされるすべてのプラットフォーム スイッチで、サポートされる最小速度は 4G で、最大速度は 32G です。 ただし、N9K-C9336C-FX2-E スイッチでサポートされる最小速度は 8G であり、サポートされる最大速度は同じく 32G です。デフォルトでは、インターフェイスのポート速度はスイッチによって自動計算されます。

Note 8G 速度はサーバーおよびターゲット インターフェイスに対してサポートされていません。

Caution ポート速度の変更は中断を伴う動作です。

インターフェイスのポート速度を設定する手順は、次のとおりです。

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **interface fc** *slot*/*port*

3. switch(config-if)# **switchport speed 16000**
4. switch(config-if)# **no switchport speed**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configuration terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface fc** *slot*/*port*	指定されたインターフェイスを選択して、インターフェイス コンフィギュレーション モードを開始します。 **Note** 仮想ファイバ チャネル インターフェイスのポート速度は設定できません。 **Note** これが 10G ブレイクアウト ポートの場合、*slot*/*port* 構文は *QSFP-module*/*port* になります。 **Note** これが QSFP+ GEM またはブレイクアウト ポートの場合、*port* 構文は *QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **switchport speed 16000**	インターフェイスのポート速度を 16 Mbps に構成します。 数値は、Mbps 単位の速度を表します。4 Gbps インターフェイスには 4000 の速度、8 Gbps インターフェイスには 8000、16 Gbps インターフェイスには 16000、32 Gbps インターフェイスには 32000、または auto（デフォルト）を設定できます。 **Note** 16G ホスト アダプタを Cisco Nexus 9000 スイッチの 32G SFP ポートに接続するときに、速度が自動速度として設定されている場合、またはデフォルトが 8G 速度に設定されているときにリンクがアップしない場合は、**switchport speed 16000** コマンドを使用して、ポートを手動で設定する必要があります。
ステップ 4	switch(config-if)# **no switchport speed**	インターフェイスの出荷時のデフォルト（auto）管理速度に戻します。

トランク モードの構成

トランク モードを構成するには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **interface fc** *slot*/*port*
3. switch(config-if)# **switchport trunk mode on**
4. switch(config-if)# **switchport trunk mode off**
5. switch(config-if)# **switchport trunk mode auto**

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# **configuration terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface fc** *slot*/*port*	指定した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 3	switch(config-if)# **switchport trunk mode on**	指定されたインターフェイスのトランク モードをイネーブルにします（デフォルト）。
ステップ 4	switch(config-if)# **switchport trunk mode off**	指定されたインターフェイスのトランク モードをディセーブルにします。
ステップ 5	switch(config-if)# **switchport trunk mode auto**	インターフェイスの自動検知を提供するトランク モードを auto モードに設定します。

コメント

トランキング モードがオンの FC ポートと SAN-PO リンクが 2 つのスイッチ間で起動するには、両方のスイッチを互いの OUI で構成する必要があります。

OUI 値がデフォルトで登録されていない場合にのみ、スイッチでOUIを構成します。OUI は次のように検出および構成されます。

```
  N9K(config-if)# show wwn switch
    Switch WWN is 20:00:2c:d0:2d:50:ea:64
    N9K(config-if)#
```

スイッチでは、OUI (0x2cd02d) がすでに登録されている場合、次の出力が表示されます。

```
    MDS9710(config-if)# sh wwn oui | i 2cd02d
    0x2cd02d   Cisco                Default
    MDS9710(config-if) #
If the OUI is not registered, configure it manually.
 MDS9710(config-if)# wwn oui 0x2cd02d
```

Cisco NX-OS Release 7.3(0)D1(1) 以降では、Cisco MDS 9700 シリーズコアスイッチで OUI を構成できます。

自動検知

自動検知は、速度に関係なく、すべてのインターフェイスで有効になっています。8G Small Form-Factor Pluggable（SFP）が挿入されている場合、インターフェイスは 8G および 4G の速度で動作します。16G SFP が挿入されている場合、インターフェイスは 16G、8G、および 4G の速度でのみ動作し、32G SFP では、インターフェイスは 32G、16G、および 8G の速度で動作します。

Note Cisco Nexus C93180YC-FX スイッチは 10G SFP をサポートします。Cisco Nexus 2348UPQ では、16G は自動検知されません。16G 速度を明示的に設定するには、ファイバ チャネル インターフェイスを使用した *Cisco Unified FEX Nexus 2348UPQ* の設定を参照してください。

デフォルトではすべての 4 Gbps インターフェイスで 速度自動検知がイネーブルになっています。この設定を使用すると、4 Gbps ポートのインターフェイスは 1 Gbps、2 Gbps、または 4 Gbps の速度で動作します。専用レート モードで動作するインターフェイスに対して自動検知をイネーブルにすると、ポートが 1 Gbps または 2 Gbps の動作速度をネゴシエートした場合でも、4 Gbps 帯域幅が予約されます。

ブレークアウトによる FC ポートの変換

ファイバ チャネル（FC）ポートのブレーク アウト インターフェイスポート オプションは、Cisco Nexus N9K-C9336C-FX2-E プラットフォーム スイッチ上の FC のインターフェイスでのみサポートされています。LCM コンポーネントは、FC ポートのブレークアウトまたは変換をサポートします。

FCoE ポートを FC ポートに変換するには、次の手順を実行します。

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **slot1**
3. switch(config-slot)# **port 9 type fc breakout**
4. switch(config-slot)# **reload**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configuration terminal**	構成モードに入ります。

	Command or Action	Purpose
ステップ 2	switch(config)# **slot1**	シャーシのスロットで事前プロビジョニングを有効にします。
ステップ 3	switch(config-slot)# **port 9 type fc breakout**	ポート タイプを FCoE ポートからファイバー チャネル ポートに変更または分割します。 **Note** ポート タイプ、たとえば 9 ～ 36を、FC ブレークアウト ポートとして変換できます。ポートは、連続範囲 (たとえば、9 ～ 11)、非連続範囲 (たとえば、18、23、30)、または単一ポート (たとえば、36) の FC ブレークアウト ポートとして変換できます。
ステップ 4	switch(config-slot)# **reload**	スイッチをリロードします。

スイッチがリロードされると、スイッチは FC ブレークアウト ポート（fc1/9/1…fc1/9/4 など）でオンラインになります。

ブレイクアウト インターフェイスでの速度の変更

各ブレイクアウトインターフェイスで速度を変更できます。ただし、すべてのブレイクアウトポートの速度が変更されます。

コマンドの例：

```
switch(config)# int fc1/9/1-4
switch(config-if)# switchport speed 32000
!!!WARNING! This command affects all interfaces of a breakout port!!!
switch(config-if)#
```

（注） FC ブレークアウト ポートのデフォルトの速度は 32G です。

SD ポート フレーム カプセル化の設定

switchport encap eisl コマンドは、SD ポート インターフェイスにだけ適用されます。このコマンドは、SD ポート モードにあるインターフェイスによって送信されたすべてのフレームのフレーム フォーマットを判別します。カプセル化を EISL に設定すると、すべての SPAN 送信元について、すべての発信フレームが EISL フレーム フォーマットで送信されます。

switchport encap eisl コマンドは、デフォルトではディセーブルです。カプセル化を有効にすると、すべての発信フレームがカプセル化され、**show interface** *SD_port_interface* コマンドの出力には、カプセル化が EISL であることを示す新しい行が表示されます。

受信データ フィールド サイズの構成

仮想ファイバ チャネル インターフェイスではなく、ネイティブ ファイバ チャネル インターフェイスの受信データ フィールド サイズを設定できます。デフォルトのデータ フィールド サイズが 2112 バイトの場合、フレームの長さは 2148 バイトです。

受信データ フィールド サイズを設定する手順は、次のとおりです。

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **interface fc** *slot*/*port*
3. switch(config-if)# **switchport fcrxbufsize 2000**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configuration terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface fc** *slot*/*port*	ファイバ チャネル インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。 **Note** これが 10G ブレイクアウト ポートの場合、*slot*/*port* 構文は *QSFP-module*/*port* になります。 **Note** これが QSFP+ GEM またはブレイクアウト ポートの場合、*port* 構文は *QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **switchport fcrxbufsize 2000**	選択されたインターフェイスのデータ フィールド サイズを 2000 バイトに減らします。デフォルトは 2112 バイトで、範囲は 256 ～ 2112 バイトです。

ビット エラーしきい値を理解する

ビット エラー レートしきい値は、パフォーマンスの低下がトラフィックに重大な影響を与える前にエラー レートの増加を検出するために、スイッチにより使用されます。

ビット エラーは次のような理由のため発生します。

- ケーブル故障または不良。
- GBIC または SFP 故障または不良。

- GBIC または SFP は 1 Gbps で動作するように指定されているが、2 Gbps で使用されている。
- GBIC または SFP は 2 Gbps で動作するように指定されているが、4 Gbps で使用されている。
- 長距離に短距離ケーブルが使用されている、または短距離に長距離ケーブルが使用されている。
- 一時的な同期ロス
- ケーブルの片端または両端の接続のゆるみ。
- 片端または両端での不適切な GBIC 接続または SFP 接続。

5 分間に 15 のエラー バーストが発生すると、ビット エラー レートしきい値が検出されます。デフォルトでは、しきい値に達するとスイッチはインターフェイスを無効化します。

shutdown/**no shutdown** コマンドを順番に入力すると、インターフェイスを再度イネーブルにできます。

しきい値を超えてもインターフェイスが無効化されないようにスイッチを設定できます。

Note ビットエラーしきい値イベントによってインターフェイスがディセーブルにならないように設定されていても、ビット エラーしきい値イベントが検出されると、スイッチによって syslog メッセージが生成されます。

インターフェイスのビット エラーしきい値をディセーブルにする手順は、次のとおりです。

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **interface fc** *slot*/*port*
3. switch(config-if)# **switchport ignore bit-errors**
4. switch(config-if)# **no switchport ignore bit-errors**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configuration terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface fc** *slot*/*port*	ファイバ チャネル インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。 **Note** これが 10G ブレイクアウト ポートの場合、*slot*/*port* 構文は *QSFP-module*/*port* になります。

	Command or Action	Purpose
		Note これが QSFP+ GEM またはブレイクアウト ポートの場合、*port* 構文は *QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **switchport ignore bit-errors**	ビットエラーしきい値イベントを検出したとき、インターフェイスがディセーブルにならないようにします。
ステップ 4	switch(config-if)# **no switchport ignore bit-errors**	ビットエラーしきい値イベントを検出したとき、インターフェイスがイネーブルにならないようにします。

バッファ間クレジットの構成

⚠

Caution **switchport fcrxbbcredit** コマンドを使用してインターフェイスを設定すると、設定の変更がすぐに適用されるように、インターフェイスは自動的にフラップします。したがって、このような構成の計画は、スケジュールされたメンテナンス時間帯にのみ行い、運用環境へのそのような構成の影響を最小限に抑えることをお勧めします。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface fc** *slot*/*port*
3. switch(config-if)# **switchport fcrxbbcredit default**
4. switch(config-if)# **switchport fcrxbbcredit** *number* **mode** {**E** | **F** | **TE**}
5. switch(config-if)# **do show int fc** *slot*/*port*
6. (Optional) switch(config-if)# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface fc** *slot*/*port*	ファイバ チャネル インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。 **Note**

	Command or Action	Purpose
		これが 10G ブレイクアウト ポートの場合、*slot*/*port* 構文は *QSFP-module*/*port* になります。 **Note** これが QSFP+ GEM またはブレイクアウト ポートの場合、*port* 構文は *QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **switchport fcrxbbcredit default**	デフォルトの使用可能な値を選択されたインターフェイスに適用します。使用可能な値は、ポートモードによって異なります。 デフォルト値は、ポート機能に応じて割り当てられます。
ステップ 4	switch(config-if)# **switchport fcrxbbcredit** *number* **mode** {**E** | **F** | **TE**}	選択したインターフェイスにバッファ間クレジット番号を割り当て、必要に応じてポートが E、F、または TE のどのモードで動作するかを指定します。 **Note** **E**、**F**、または **TE** を **mode** 用に指定すると、バッファ間クレジットの値は、ポートがその特定のモードに設定されている場合にのみ、適用されます。 バッファ間クレジットの値の破には、1～240 です。 デフォルト値は 16 です。
ステップ 5	switch(config-if)# **do show int fc** *slot*/*port*	送受信のバッファ間クレジットを、このインターフェイスのその他の関連インターフェイス情報とともに表示します。 **Note** 正しいバッファ間クレジット値は、レジスタの読み取り時に得られます。データ トラフィックが遅いときに状況を確認するのに役立ちます。 **Note** これが 10G ブレイクアウト ポートの場合、*slot*/*port* 構文は *QSFP-module*/*port* になります。 **Note** これが QSFP+ GEM またはブレイクアウト ポートの場合、*port* 構文は *QSFP-module*/*port* になります。
ステップ 6	(Optional) switch(config-if)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

ファイバチャネルインターフェイスのグローバル属性の設定

スイッチ ポート属性のデフォルト値の構成

各種のスイッチポート属性の属性デフォルト値を設定できます。これらの属性は、この時点でそれぞれを指定しなくても、今後のすべてのスイッチ ポート設定にグローバルに適用されます。

スイッチ ポート属性を設定する手順は、次のとおりです。

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **no system default switchport shutdown san**
3. switch(config)# **system default switchport shutdown san**
4. switch(config)# **system default switchport trunk mode auto**

DETAILED STEPS

Procedure

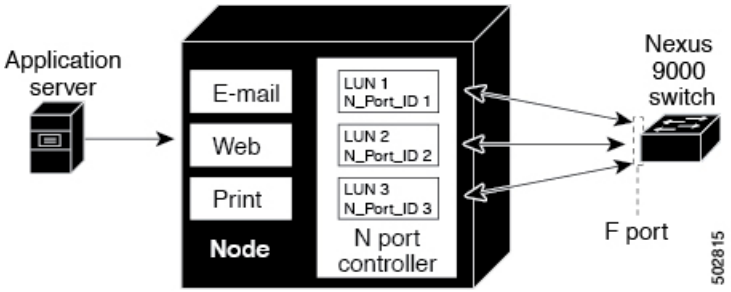
	Command or Action	Purpose
ステップ 1	switch# **configuration terminal**	構成モードに入ります。
ステップ 2	switch(config)# **no system default switchport shutdown san**	インターフェイス管理ステートのデフォルト設定を up に設定します（出荷時のデフォルト設定は down です）。 **Tip** このコマンドは、管理ステートに対してユーザ設定が存在しないインターフェイスにだけ適用されます。
ステップ 3	switch(config)# **system default switchport shutdown san**	インターフェイス管理ステートのデフォルト設定を down に設定します。これが出荷時のデフォルト設定です。 **Tip** このコマンドは、管理ステートに対してユーザ設定が存在しないインターフェイスにだけ適用されます。

	Command or Action	Purpose
ステップ 4	switch(config)# **system default switchport trunk mode auto**	インターフェイスの管理トランク モード ステートのデフォルト設定を auto に設定します。 **Note** デフォルト設定のトランク モードは on です。

N ポート識別子仮想化について

N ポート識別子仮想化（NPIV）は単一 N ポートに複数の FC ID を割り当てる手段を提供します。この機能を使用すると、N ポート上の複数のアプリケーションが異なる ID を使用したり、アクセス コントロール、ゾーニング、ポート セキュリティをアプリケーション レベルで実装したりできます。次の図に、NPIV を使用するアプリケーションの例を示します。

Figure 7: NPIV の例



N ポート識別子仮想化のイネーブル化

スイッチで NPIV をイネーブルまたはディセーブルにできます。**feature-set fcoe** が有効になっている場合、機能 NPIV はデフォルトで有効になります。

Before you begin

スイッチ上のすべての VSAN に対して NPIV をグローバルでイネーブルにし、NPIV 対応のアプリケーションが複数の N ポート ID を使用できるようにする必要があります。

Note すべての N ポート ID は同じ VSAN 内で割り当てられます。

SUMMARY STEPS

1. **configure terminal**
2. **feature npiv**
3. **no feature npiv**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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 npiv** **Example:** `switch(config)# feature npiv`	スイッチ上のすべての VSAN の NPIV をイネーブルにします。
ステップ 3	**no feature npiv** **Example:** `switch(config)# no feature npiv`	スイッチ上の NPIV をディセーブルにします（デフォルト）。

ポート チャネルの設定例

この項では、F ポート チャネルを共有モードで設定する方法、および NPIV コア スイッチの F ポートと NPV スイッチの NP ポート間のリンクを起動する方法の例を示します。F ポート チャネルを設定する前に、F ポート トランキング、F ポート チャネリング、および NPIV がイネーブルであることを確認します。

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(config)# interface san-po-channel 2
switch(config-if)# switchport mode F
switch(config-if)# channel mode active
switch(config-if)# exit
```

次に、コア スイッチで専用モードでポート チャネル メンバ インターフェイスを設定する例を示します。

```
switch(config)# interface fc1/4-6
switch(config-if)# shut
switch(config-if)# switchport mode F
switch(config-if)# switchport speed 32000
switch(config-if)# switchport trunk mode on
switch(config-if)# channel-group 2
switch(config-if)# no shut
switch(config-if)# exit
```

ファイバチャネル インターフェイスの確認

SFP トランスミッタ タイプの確認

SFP トランスミッタ タイプは、仮想ファイバ チャネルではなく、物理ファイバ チャネル インターフェイス用に表示できます。

Small Form-Factor Pluggable（SFP）ハードウェア トランスミッタは、**show interface brief** コマンドで表示される際に略語で示されます。関連するSFPがシスコによって割り当てられた拡張 ID を持つ場合、**show interface** コマンドと **show interface brief** コマンドは、トランスミッタ タイプではなく、ID を表示します。**show interface transceiver** コマンドと **show interface fc** *slot*/*port* transceiver コマンドは、シスコがサポートする SFP に関して両方の値を表示します。

インターフェイス情報の検証

show interface コマンドはインターフェイス構成を表示します。引数を入力しないと、このコマンドはスイッチ内に設定されたすべてのインターフェイスの情報を表示します。

インターフェイス情報を表示するのに引数（インターフェイスの範囲、または複数の指定されたインターフェイス）を指定することもできます。interface fc2/1 - 4 , fc3/2 - 3 という形式でコマンドを入力して、インターフェイスの範囲を指定できます。

次に、すべてのインターフェイスを表示する例を示します。

```
switch# show interface

fc3/1 is up
...
fc3/3 is up
...
Ethernet1/3 is up
...
mgmt0 is up
...
vethernet1/1 is up
...
vfc 1 is up
```

次に、指定された複数のインターフェイスを表示する例を示します。

```
switch# show interface fc3/1 , fc3/3
fc3/1 is up
...
fc3/3 is up
...
```

次に、特定の 1 つのインターフェイスを表示する例を示します。

```
switch# show interface vfc 1
```

```
vfc 1 is up

...
```

次に、インターフェイスの説明を表示する例を示します。

```
switch# show interface description
-------------------------------------------------
Interface          Description
-------------------------------------------------
fc3/1              test intest
Ethernet1/1              --
vfc 1              --
...
```

次に、すべてのインターフェイスを表示する例を示します（簡略）。

```
switch# show interface brief
```

次に、インターフェイス カウンタを表示する例を示します。

```
switch# show interface counters
```

次に、特定のインターフェイスのトランシーバ情報を表示する例を示します。

```
switch# show interface fc3/1 transceiver
```

Note SFP が存在する場合にだけ、**show interface transceiver** コマンドは有効です。

show running-configurationshow running-config コマンドを実行すると、すべてのインターフェイスの情報を含む実行コンフィギュレーション全体が表示されます。スイッチがリロードしたとき、インターフェイス コンフィギュレーション コマンドが正しい順序で実行するように、インターフェイスはコンフィギュレーションファイルに複数のエントリを持っています。特定の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する場合、そのインターフェイスのすべてのコンフィギュレーション コマンドはグループ化されます。

次の例では、すべての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する場合のインターフェイスの表示を示します。

```
switch# show running configurationshow running-config
...
interface fc3/5
  switchport speed 200016000
...
interface fc3/5
  switchport mode E
...
interface fc3/5
  channel-group 11 force
  no shutdown
```

次の例では、特定の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する場合のインターフェイスの表示を示します。

```
switch# show running configuration fc3/5show running-config fc3/5
interface fc3/5
  switchport speed 200016000
  switchport mode E
```

```
channel-group 11 force
no shutdown
```

BB_Credit 情報の確認

次に、すべてのファイバ チャネル インターフェイスの BB_credit 情報を表示する例を示します：

```
switch# show interface fc1/7
...
fc1/7 is up
Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
Port WWN is 20:07:2c:d0:2d:50:e5:24
Admin port mode is auto, trunk mode is off
snmp link state traps are enabled
Port mode is F, FCID is 0xe10280
Port vsan is 500
Operating Speed is 32 Gbps
Admin Speed is auto
Transmit B2B Credit is 12
Receive B2B Credit is 64
Receive data field Size is 2112
Beacon is turned off
fec state is enabled by default
5 minutes input rate 0 bits/sec,0 bytes/sec, 0 frames/sec
5 minutes output rate 0 bits/sec,0 bytes/sec, 0 frames/sec
16705 frames input,1225588 bytes
0 discards,0 errors
0 invalid CRC/FCS,0 unknown class
0 too long,0 too short
16714 frames output,1345676 bytes
0 discards,0 errors
0 input OLS,0 LRR,0 NOS,0 loop inits
7 output OLS,4 LRR, 0 NOS, 0 loop inits
Receive B2B Credit performance buffers is 0
12 transmit B2B credit remaining
0 low priority transmit B2B credit remaining
Interface last changed at Thu Nov 14 11:59:40 2019
```

ファイバチャネル インターフェイスのデフォルト設定

次の表に、ネイティブ ファイバチャネル 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。

Table 12: デフォルトのネイティブ ファイバチャネル インターフェイス パラメータ

パラメータ	デフォルト
インターフェイス モード	自動
インターフェイス速度	自動
管理状態	Shutdown（初期設定時に変更された場合を除く）

パラメータ	デフォルト
トランク モード	On（初期設定時に変更された場合を除く）
トランク許可 VSAN	1 ～ 4093
インターフェイス VSAN	デフォルト VSAN（1）
標識モード	Off（ディセーブル）
EISL カプセル化	ディセーブル
データ フィールドサイズ	2112 バイト

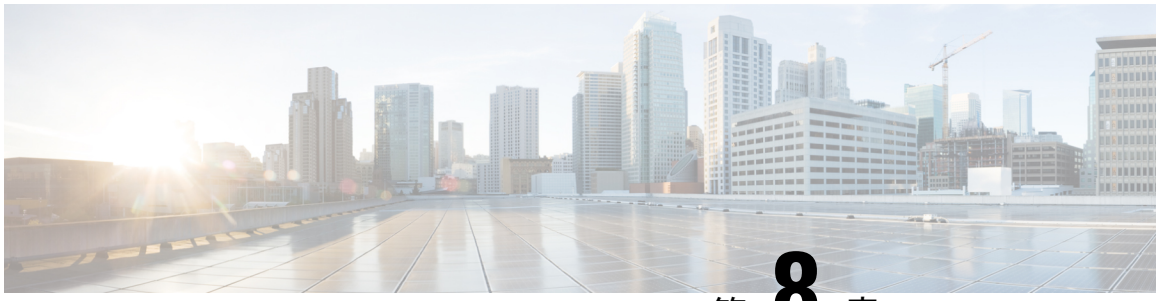
次の表に、ネイティブ ファイバチャネル インターフェイス パラメータのデフォルト設定を示します。

Table 13: デフォルトの仮想ファイバ チャネル インターフェイス パラメータ

パラメータ	デフォルト
インターフェイス モード	F モード
インターフェイス速度	該当なし
管理状態	Shutdown（初期設定時に変更された場合を除く）
トランク モード	[オン（On）]
トランク許可 VSAN	すべての VSAN
インターフェイス VSAN	デフォルト VSAN（1）
EISL カプセル化	該当なし
データ フィールドサイズ	適用対象外

ファイバチャネル インターフェイスの構成0

ファイバチャネル インターフェイスの構成0



第 8 章

VSAN の設定と管理

この章では、VSAN の設定と管理方法について説明します。

この章は、次の項で構成されています。

VSAN の設定と管理

VSAN（仮想 SAN）を使用することによって、ファイバ チャネル ファブリックでより高度なセキュリティと安定性を実現できます。VSANは同じファブリックに物理的に接続されたデバイスを分離します。VSAN では、一般の物理インフラストラクチャで複数の論理 SAN を作成できます。各 VSAN には最大 239 台のスイッチを組み込めます。それぞれの VSAN は、異なる VSAN で同じファイバ チャネル ID（FC ID）を同時に使用できる独立したアドレス領域を持ちます。

VSAN に関する情報

VSANは、仮想ストレージエリア ネットワーク（SAN）です。SANは、主にSCSIトラフィックを交換するためにホストとストレージ デバイス間を相互接続する専用ネットワークです。SAN では、この相互接続を行うために物理リンクを使用します。一連のプロトコルは SAN 上で実行され、ルーティング、ネーミングおよびゾーン分割を処理します。異なるトポロジで複数の SAN を設計できます。

各 VSAN には最大 239 台のスイッチを組み込めます。それぞれの VSAN は、異なる VSAN で同じファイバ チャネル ID（FC ID）を同時に使用できる独立したアドレス領域を持ちます。

VSAN トポロジ

VSAN には次の特徴もあります。

- 複数の VSAN で同じ物理トポロジを共有できます。
- 同じファイバ チャネル ID（FC ID）を別の VSAN 内のホストに割り当て、VSAN のスケーラビリティを高めることができます。
- VSAN の各インスタンスは、FSPF、ドメイン マネージャ、およびゾーン分割などの必要なすべてのプロトコルを実行します。
- VSAN 内のファブリック関連の設定は、別の VSAN 内の関連トラフィックに影響しません。
- ある VSAN 内のトラフィック中断を引き起こしたイベントはその VSAN 内にとどまり、他の VSAN に伝播されません。

次の図は、各フロアに 1 つずつ、3 つのスイッチがあるファブリックを示しています。スイッチと接続された装置の地理的な配置は、論理 VSAN の区分けには依存しません。VSAN 間では通信できません。各 VSAN 内では、すべてのメンバが相互に対話できます。

Figure 8: 論理 ***VSAN*** の区分け

アプリケーション サーバまたはストレージ アレイは、ファイバ チャネルまたは仮想ファイバ チャネル インターフェイスを使用してスイッチに接続できます。VSAN には、ファイバ チャネル インターフェイスと仮想ファイバ チャネル インターフェイスを組み合わせて含めることができます。

次の図に、VSAN 2（破線）と VSAN 7（実線）の 2 つの定義済み VSAN からなるファイバ チャネル スイッチングの物理インフラストラクチャを示します。VSAN 2 には、ホスト H1 と H2、アプリケーション サーバー AS2 と AS3、ストレージ アレイ SA1 と SA4 が含まれます。VSAN 7 は、H3、AS1、SA2、および SA3 と接続します。

Figure 9: 2 つの ***VSAN*** の例

このネットワーク内の 4 つのスイッチは、VSAN 2 と VSAN 7 の両方のトラフィックを伝送する VSAN トランク リンクによって相互接続されます。各 VSAN に異なるスイッチ間トポロジを設定できます。上の図では、VSAN 2 と VSAN 7 のスイッチ間トポロジは同じです。

VSAN がもしなければ、SAN ごとに別個のスイッチとリンクが必要です。VSAN をイネーブルにすることによって、同一のスイッチとリンクが複数の VSAN で共有されることがあります。VSAN では、スイッチ精度ではなく、ポート精度で SAN を作成できます。前の図では、VSAN が物理 SAN で定義された仮想トポロジを使用して相互に通信するホストまたはストレージデバイスのグループであることを表しています。

このようなグループを作成する基準は、VSAN トポロジによって異なります。

- VSAN は、次の条件に基づいてトラフィックを分離できます。
  - ストレージ プロバイダー データセンター内の異なるお客様
  - 企業ネットワークの業務またはテスト
  - ロー セキュリティおよびハイ セキュリティの要件
  - 別個の VSAN によるバックアップ トラフィック
  - ユーザー トラフィックからのデータの複製
- VSAN は、特定の部門またはアプリケーションのニーズを満たせます。

VSAN の利点

VSAN には、次のような利点があります。

- トラフィックの分離：必要に応じて、トラフィックを VSAN 境界内に含み、1 つの VSAN 内だけに装置を存在させることによって、ユーザー グループ間での絶対的な分離を確保します。
- スケーラビリティ：VSAN は、1 つの物理ファブリック上でオーバーレイされます。複数の論理 VSAN 層を作成することによって、SAN のスケーラビリティが向上します。
- VSAN 単位のファブリック サービス：VSAN 単位のファブリック サービスの複製は、拡張されたスケーラビリティとアベイラビリティを提供します。
- 冗長構成：同一の物理 SAN で作成された複数の VSAN は、冗長構成を保証します。1 つの VSAN に障害が発生した場合、ホストと装置の間にあるバックアップ パスによって、同一の物理 SAN にある別の VSAN に冗長保護が設定されます。
- 設定の容易さ：SANの物理構造を変更することなく、VSAN間でユーザーを追加、移動、または変更できます。ある VSAN から別の VSAN へ装置を移動する場合は、物理的な設定ではなく、ポート レベルの設定だけが必要となります。

最大 34 の VSAN を 1 つのスイッチに設定できます。これらの VSAN の 1 つがデフォルト VSAN（VSAN 1）、もう 1 つが独立 VSAN（VSAN 4094）と evfp isolated_vsan（vsan 4079）です。ユーザー指定の VSAN ID 範囲は 4078 と 4080～4093 です。

VSAN とゾーン

ゾーンは、VSAN 内に常に含まれます。VSAN に複数のゾーンを定義できます。

2 つの VSAN は未接続の 2 つの SAN に相当するので、VSAN 1 のゾーン A は、VSAN 2 のゾーン A とは異なる、別個のものです。次の表に、VSAN とゾーンの相違点を示します。

Table 14: VSAN とゾーンの比較

VSAN 特性	ゾーン特性
VSAN は、SAN とルーティング、ネーミング、およびゾーン分割プロトコルが同じです。	ルーティング、ネーミング、およびゾーニング プロトコルは、ゾーン単位で利用できません。
VSAN は、ユニキャスト、マルチキャスト、およびブロードキャスト トラフィックを制限します。	ゾーンは、ユニキャスト トラフィックを制限します。
メンバーシップは、一般的に VSAN ID を使用して F ポートに定義されます。	メンバーシップは、一般的に pWWN によって定義されます。
HBA またはストレージ デバイスは、1 つの VSAN（F ポートに対応付けられた VSAN）だけに所属できます。	HBA またはストレージ デバイスは、複数のゾーンに所属できます。
VSAN は、各 E ポート、送信元ポート、および宛先ポートでメンバーシップを実行します。	ゾーンは、送信元ポートおよび宛先ポートだけでメンバーシップを実行します。
VSAN は、規模が大きい環境（ストレージ サービス プロバイダー）で定義されます。	ゾーンは、ゾーンの外部に表示されないイニシエータおよびターゲットのセットで定義されます。
VSAN は、ファブリック全体を網羅します。	ゾーンは、ファブリック エッジで設定されます。

次の図は、VSAN とゾーン間の考えられる関係性を示します。VSAN 2 には、ゾーン A、ゾーン B、ゾーン C の 3 つのゾーンが定義されています。ゾーン C は、ファイバ チャネル標準に準拠してゾーン A とゾーン B にオーバーラップしています。VSAN 7 には、ゾーン A とゾーン D の 2 つのゾーンが定義されています。VSAN 境界を越えるゾーンはありません。VSAN 2 に定義されたゾーン A は、VSAN 7 に定義されたゾーン A とは別個のものです。

Figure 10: VSAN とゾーン分割

VSAN の注意事項と制限事項

VRF 設定時の注意事項と制限事項は次のとおりです。

- VSAN ID：VSAN ID は、デフォルト VSAN（VSAN 1）、ユーザー定義の VSAN（VSAN 2 ～ 4078 および 4080～4093）、evfp_isolated_vsan（VSAN 4079）および分離 VSAN（VSAN 4094）として、VSAN を識別します。

- ステート：VSANの管理ステートをactive（デフォルト）またはsuspendedステートに設定できます。VSAN が作成されると、VSAN はさまざまな状態またはステートに置かれます。
  - VSAN の active ステートは、VSAN が設定されイネーブルであることを示します。VSANをイネーブルにすることによって、VSANのサービスをアクティブにします。
  - VSAN の suspended ステートは、VSAN が設定されているがイネーブルではないことを示します。このVSANにポートが設定されている場合、ポートはディセーブルの状態です。このステートを使用して、VSANの設定を失うことなくVSANを非アクティブにします。suspended ステートの VSAN のすべてのポートは、ディセーブルの状態です。VSAN を suspended ステートにすることによって、ファブリック全体のすべての VSAN パラメータを事前設定し、VSAN をただちにアクティブにできます。
- VSAN 名：このテキスト ストリングは、管理目的で VSAN を識別します。名前は、1 ～ 32 文字で指定できます。また、すべての VSAN で一意である必要があります。デフォルトでは、VSAN 名は VSAN と VSAN ID を表す 4 桁のストリングを連結したものです。たとえば、VSAN 3 のデフォルト名は VSAN0003 です。

Note VSAN 名は一意である必要があります。

- ロード バランシング属性：これらの属性は、ロード バランシング パス選択に対する送信元/宛先 ID（src-dst-id）または Originator Exchange ID（OX ID）（デフォルトでは、src-dst-ox-id）の使用を示します。
- VSANがアクティブの状態で、最低1つのポートがアップの状態であれば、VSANは動作ステートにあります。このステートは、トラフィックがこのVSANを通過できることを示します。このステートは設定できません。
- Cisco Nexus 9300-FXおよび9700-FXプラットフォーム スイッチでは、デフォルトのVSAN 1を含む32のVSANのみを作成できます。
- トランキング F ポート チャネル機能を有効にするために f port-channel-trunk コマンドが実行される標準スイッチは、以下の予約済み VSAN と分離された VSAN の設定ガイドラインに従います。
  - いずれかのインターフェイスでトランク モードがオンであるか、NP ポート チャネルが稼働している場合、予約済み VSAN は 3040 ～ 4078 であり、ユーザー設定には使用できません。
  - 分離 VSAN の 4094、および拡張仮想ファブリック プロトコル（EVFP）分離 VSAN の 4079 は、ユーザー設定には使用できません。

VSAN の作成について

VSAN がアクティブの状態で、最低 1 つのポートがアップの状態であれば、VSAN は動作ステートにあります。このステートは、トラフィックがこの VSAN を通過できることを示します。このステートは設定できません。

VSAN の静的な作成

VSAN を作成する前には、VSAN に対してアプリケーション特有のパラメータを設定できません。

SUMMARY STEPS

1. **configure terminal**
2. **vsan database**
3. **vsan** *vsan-id*
4. **vsan** *vsan-id* **name** *name*
5. **vsan** *vsan-id* **suspend**
6. switch(config-vsan-db)# **no vsan** *vsan-id* **suspend**
7. switch(config-vsan-db)# **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**vsan database** **Example:** `switch(config)# vsan database`	VSAN に対するデータベースを設定します。アプリケーション特有の VSAN パラメータは、このプロンプトから設定できません。
ステップ 3	**vsan** *vsan-id* **Example:** `switch(config-vsan-db)# vsan 360`	VSAN が存在しない場合は、指定された ID で VSAN を作成します。
ステップ 4	**vsan** *vsan-id* **name** *name* **Example:** `switch(config-vsan-db)# vsan 360 name test`	割り当てられた名前で VSAN をアップデートします。
ステップ 5	**vsan** *vsan-id* **suspend** **Example:**	選択された VSAN を中断します。

	Command or Action	Purpose
	`switch(config-vsan-db)# vsan 470 suspend`	
ステップ 6	switch(config-vsan-db)# **no vsan** *vsan-id* **suspend** **Example:** `switch(config-vsan-db)# no vsan 470 suspend`	前のステップで入力した **suspend** コマンドを無効にします。
ステップ 7	switch(config-vsan-db)# **end** **Example:** `switch(config-vsan-db)# end`	EXEC モードに戻ります。

ポート VSAN メンバーシップ

スイッチのポート VSAN メンバーシップは、ポート単位で割り当てられます。デフォルトでは、各ポートはデフォルト VSAN に属します。ポートに VSAN メンバーシップを静的に（ポートに VSAN を割り当てて）割り当てることができます。

- スタティック：ポートに VSAN を割り当てます。
- ダイナミック：デバイス WWN に基づいて VSAN を割り当てます。この方式は、Dynamic Port VSAN Membership（DPVM）と呼ばれます。Cisco Nexus デバイス は DPVM をサポートしていません。

VSAN トランキング ポートは、許可リストの一部である VSAN の対応リストを持ちます。

スタティック ポート VSAN メンバーシップの概要

インターフェイス ポートの VSAN メンバーシップをスタティックに割り当てることができます。

SUMMARY STEPS

1. **configure terminal**
2. **vsan database**
3. **vsan** *vsan-id*
4. switch(config-vsan-db)# **vsan** *vsan-id* **interface vfc** *vfc-id*
5. **vsan** *vsan-id* **interface vfc** *vfc-id*
6. switch(config-vsan-db)# **vsan** *vsan-id* **vfc** *vfc-id*
7. **vsan** *vsan-id* **vfc** *vfc-id*}

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**vsan database** **Example:** `switch(config)# vsan database` `switch(config-vsan-db)#`	VSAN に対するデータベースを設定します。
ステップ 3	**vsan** *vsan-id* **Example:** `switch(config-vsan-db)# vsan 50`	VSAN が存在しない場合は、指定された ID で VSAN を作成します。
ステップ 4	switch(config-vsan-db)# **vsan** *vsan-id* **interface vfc** *vfc-id*	指定されたインターフェイスのメンバーシップを VSAN に割り当てます。
ステップ 5	**vsan** *vsan-id* **interface vfc** *vfc-id* **Example:** `switch(config-vsan-db)# vsan 34 interface vfc 5`	指定されたインターフェイスのメンバーシップを VSAN に割り当てます。
ステップ 6	switch(config-vsan-db)# **vsan** *vsan-id* **vfc** *vfc-id*	変更された VSAN を反映させるために、インターフェイスのメンバーシップ情報を更新します。 **Note** FC または vFC インターフェイスの VSAN メンバーシップを削除するには、別の VSAN にそのインターフェイスの VSAN メンバーシップを割り当てます。VSAN 1 に割り当てることを推奨します。
ステップ 7	**vsan** *vsan-id* **vfc** *vfc-id*} **Example:** `switch(config-vsan-db)# vsan 10 vfc 3`	変更された VSAN を反映させるために、インターフェイスのメンバーシップ情報を更新します。 **Note** vFC インターフェイスの VSAN メンバーシップを削除するには、別の VSAN にそのインターフェイスの VSAN メンバーシップを割り当てます。VSAN 1 に割り当てることを推奨します。

VSAN スタティック メンバーシップの表示

VSAN スタティック メンバーシップ情報を表示するには、**show vsan membership** コマンドを使用します。

次に、指定された VSAN のメンバーシップ情報を表示する例を示します。

```
switch # show vsan 1 membership
vsan 1 interfaces:
        vfc21   vfc22   vfc23   vfc24
        san-port-channel 3  vfc1/1
```

Note インターフェイスがこのVSANに設定されていない場合は、インターフェイス情報が表示されません。

次に、すべての VSAN のメンバーシップ情報を表示する例を示します。

```
switch # show vsan membership
vsan 1 interfaces:
        vfc21   vfc22   vfc23   vfc24
        san-port-channel 3  vfc31
vsan 2 interfaces:
        vfc23 vfc41
vsan 7 interfaces:
vsan 100 interfaces:
vsan 4094(isolated vsan) interfaces:
```

次に、指定されたインターフェイスのスタティック メンバーシップ情報を表示する例を示します。

```
switch # show vsan membership interface vfc21
vfc21
        vsan:1
        allowed list:1-4093
```

デフォルト VSAN

Cisco SAN スイッチの出荷時の設定では、デフォルトの VSAN 1 のみが有効です。VSAN 1 を実稼働環境の VSAN として使用しないことを推奨します。VSAN が設定されていない場合、ファブリック内のすべてのデバイスはデフォルト VSAN に含まれていると見なされます。デフォルトでは、デフォルト VSAN にすべてのポートが割り当てられています。

Note VSAN 1 は削除できませんが、中断できます。

最大 34 の VSAN を 1 つのスイッチに設定できます。これらの VSAN の 1 つがデフォルト VSAN（VSAN 1）、もう 1 つが独立 VSAN（VSAN 4094）と evfp isolated_vsan（vsan 4079）です。ユーザー指定の VSAN ID 範囲は 4078 と 4080～4093 です。

独立 VSAN

VSAN 4094 は独立 VSAN です。VSAN を削除すると、すべての非トランキング ポートが独立 VSAN に移動され、デフォルト VSAN または別の設定済み VSAN にポートが暗黙的に移動されるのを防ぎます。これにより、削除された VSAN のすべてのポートが分離されます（ディセーブルにされます）。

Note VSAN 4094 内にポートを設定するか、ポートを VSAN 4094 に移動すると、このポートがすぐに分離されます。

Caution 独立 VSAN を使用してポートを設定しないでください。

Note 最大 34 の VSAN を 1 つのスイッチに設定できます。これらの VSAN の 1 つがデフォルト VSAN（VSAN 1）、もう 1 つが独立 VSAN（VSAN 4094）と evfp isolated_vsan（vsan 4079）です。ユーザー指定の VSAN ID 範囲は 4078 と 4080～4093 です。

分離された VSAN メンバーシップの概要

show vsan 4094 membership コマンドを実行すると、独立 VSAN に関連するすべてのポートが表示されます。

VSAN の動作ステート

VSAN がアクティブの状態で、最低 1 つのポートがアップの状態であれば、VSAN は動作ステートにあります。このステートは、トラフィックがこの VSAN を通過できることを示します。このステートは設定できません。

スタティック VSAN の削除

アクティブな VSAN が削除されると、その属性が実行コンフィギュレーションからすべて削除されます。VSAN 関連情報は、次のようにシステム ソフトウェアによって保持されます。

- VSAN 属性およびポート メンバーシップの詳細は、VSAN マネージャによって保持されます。コンフィギュレーションから VSAN を削除すると、この機能が影響を受けます。VSAN が削除されると、VSAN 内のすべてのポートが非アクティブになり、ポートが独立 VSAN に移動されます。同一の VSAN が再作成されると、ポートはその VSAN に自動的に割り当てられることはありません。ポート VSAN メンバーシップを明示的に再設定する必要があります（次の図を参照してください）。

***Figure 11: VSAN* ポート メンバーシップの詳細**

- VSAN ベースのランタイム（ネーム サーバー）、ゾーン分割、および設定（スタティック ルート）情報は、VSAN が削除されると削除されます。
- 設定された VSAN インターフェイス情報は、VSAN が削除されると削除されます。

Note 許可 VSAN リストは、VSAN が削除されても影響を受けません。

設定されていない VSAN のコマンドは拒否されます。たとえば、VSAN 10 がシステムに設定されていない場合、ポートを VSAN 10 に移動するコマンド要求が拒否されます。

Related Topics

VSAN トランキングの設定

スタティック VSAN の削除

VSAN およびその各種属性を削除できます。

SUMMARY STEPS

1. **configure terminal**
2. **vsan database**
3. **vsan** *vsan-id*
4. switch(config-vsan-db)# **no vsan** *vsan-id*
5. switch(config-vsan-db)# **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**vsan database** **Example:** `switch(config)# vsan database` `switch(config-vsan-db)#`	VSAN データベースを設定します。
ステップ 3	**vsan** *vsan-id* **Example:** `switch(config-vsan-db)# vsan 2`	VSAN コンフィギュレーション モードを開始します。
ステップ 4	switch(config-vsan-db)# **no vsan** *vsan-id* **Example:** `switch(config-vsan-db)# no vsan 5`	データベースおよびスイッチから VSAN 5 を削除します。
ステップ 5	switch(config-vsan-db)# **end** **Example:** `switch(config-vsan-db)# end`	EXEC モードに戻ります。

ロード バランシングの概要

ロードバランシング属性は、ロードバランシング パス選択に対する送信元/宛先 ID（src-dst-id）または Originator Exchange ID（OX ID）（デフォルトでは、src-dst-ox-id）の使用を示します。

ロード バランシングの設定

既存の VSAN でロード バランシングを設定できます。

ロードバランシング属性は、ロードバランシング パス選択に対する送信元/宛先 ID（src-dst-id）または Originator Exchange ID（OX ID）（デフォルトでは、src-dst-ox-id）の使用を示します。

SUMMARY STEPS

1. **configure terminal**
2. **vsan database**
3. **vsan** *vsan-id*
4. **vsan** *vsan-id* **loadbalancing src-dst-id**

5. **no vsan** *vsan-id* **loadbalancing src-dst-id**
6. **vsan** *vsan-id* **loadbalancing src-dst-ox-id**
7. **vsan** *vsan-id* **suspend**
8. **no vsan** *vsan-id* **suspend**
9. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**vsan database** **Example:** `switch(config)# vsan database` `switch(config-vsan-db)#`	VSAN データベース コンフィギュレーション サブモードを開始します。
ステップ 3	**vsan** *vsan-id* **Example:** `switch(config-vsan-db)# vsan 15`	既存の VSAN を指定します。
ステップ 4	**vsan** *vsan-id* **loadbalancing src-dst-id** **Example:** `switch(config-vsan-db)# vsan 15 loadbalancing src-dst-id`	選択された VSAN に対してロード バランシングの保証をイネーブルにし、スイッチがパス選択プロセスで送信元/宛先 ID を使用するようにします。
ステップ 5	**no vsan** *vsan-id* **loadbalancing src-dst-id** **Example:** `switch(config-vsan-db)# no vsan 15 loadbalancing src-dst-id`	前のステップで入力したコマンドを無効にし、ロード バランシング パラメータのデフォルト値に戻します。
ステップ 6	**vsan** *vsan-id* **loadbalancing src-dst-ox-id** **Example:** `switch(config-vsan-db)# vsan 15 loadbalancing src-dst-ox-id`	送信元 ID、宛先 ID、OX ID（デフォルト）を使用するようにパス選択設定を変更します。
ステップ 7	**vsan** *vsan-id* **suspend** **Example:** `switch(config-vsan-db)# vsan 23 suspend`	選択された VSAN を中断します。
ステップ 8	**no vsan** *vsan-id* **suspend** **Example:** `switch(config-vsan-db)# no vsan 23 suspend`	前のステップで入力した **suspend** コマンドを無効にします。

	Command or Action	Purpose
ステップ 9	**end** **Example:** `switch(config-vsan-db)# end`	EXEC モードに戻ります。

interop モード

インターオペラビリティを使用すると、複数ベンダーによる製品の間で相互に接続できます。ファイバチャネル標準規格では、ベンダーに対して共通の外部ファイバチャネルインターフェイスを作成することを推奨しています。

Related Topics

スイッチの相互運用性 （295 ページ）

スタティック VSAN 設定の表示

次に、特定の VSAN に関する情報を表示する例を示します。

```
switch# show vsan 100
```

次に、VSAN 使用状況を表示する例を示します。

```
switch# show vsan usage
4 vsan configured
configured vsans:1-4
vsans available for configuration:5-4093
```

次に、すべての VSAN を表示する例を示します。

```
switch# show vsan
```

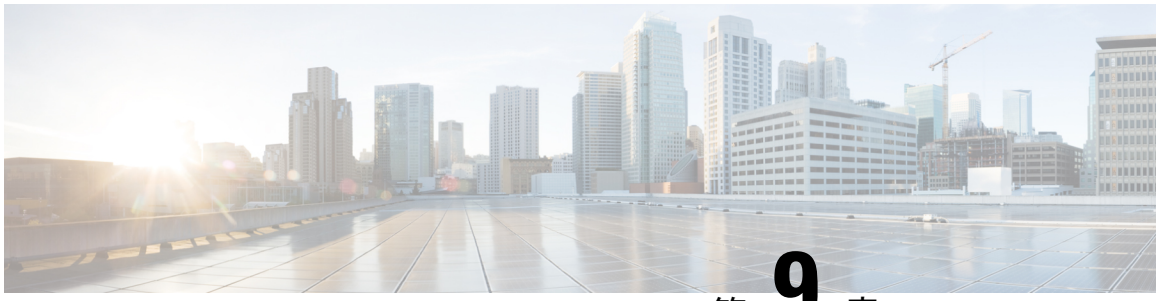
VSAN のデフォルト設定

次の表に、設定されたすべての VSAN のデフォルト設定を示します。

Table 15: デフォルト ***VSAN*** パラメータ

パラメータ	デフォルト
デフォルト VSAN	VSAN 1
状態	active ステート
名前	VSAN と VSAN ID を表す 4 桁のストリングを連結したものです。たとえば、VSAN 3 は VSAN0003 です。

パラメータ	デフォルト
ロード バランシング属性	OX ID（src-dst-ox-id）



第 9 章

SAN ポート チャネルの設定

この章は、次の内容で構成されています。

SAN ポート チャネルの設定

ストレージ エリア ネットワーク（SAN）ポート チャネルは、複数の物理インターフェイスを 1 つの論理インターフェイスに集約し、より精度の高い集約帯域幅、ロードバランシング、リンク冗長性を提供するものです。

Cisco Nexus 9000 スイッチでは、SAN ポート チャネルは物理ファイバ チャネル インターフェイスを含むことができます。ただし、仮想ファイバー チャネル インターフェイスはサポートされていません。SAN ポート チャネルは、最大 16 のファイバ チャネル インターフェイスを含むことができます。

SAN ポートチャネルに関する情報

E および TE ポートチャネルについて

E ポートチャネルは、複数の E ポートを 1 つの論理インターフェイスに集約し、より高度な集約帯域幅、ロードバランシング、およびリンク冗長性を提供する機能です。ポートチャネルはスイッチングモジュール間のインターフェイスに接続することができるため、スイッチングモジュールで障害が発生してもポートチャネルのリンクがダウンすることはありません。Cisco Nexus デバイスは FC スイッチモードで最大 4 つの ポートチャネルをサポートしています。これには E/TE ポートのポートチャネルが含まれます。

SAN ポート チャネルには、次の機能があります。

- ISL（スイッチ間リンク）（E ポート）または EISL（TE ポート）を介してポイントツーポイントで接続できます。複数のリンクを SAN ポート チャネルに結合できます。
- チャネル内で機能するすべてのリンクにトラフィックを分配して、ISL 上の集約帯域幅を増加させます。

- 複数のリンク間で負荷を分散し、最適な帯域利用率を維持します。ロード バランシングは、送信元 ID、宛先 ID、Originator Exchange ID（OX ID）に基づきます。
- ISL にハイ アベイラビリティを提供します。いずれか 1 つのリンクに障害が発生したら、それまでそのリンクで伝送されていたトラフィックが残りのリンクに切り替えられます。SAN ポート チャネルでリンクが 1 つダウンしても、上位層プロトコル（ULP）はそのことを認識しません。ULP から見れば、帯域幅は減っていても引き続きリンクが存在しています。リンク障害によるルーティング テーブルへの影響はありません。

Cisco Nexus デバイス は、最大 4 つの SAN ポート チャネル（ポート チャネルあたり 8 つのインターフェイス）をサポートします。ポート チャネル番号は、各チャネル グループに関連付けられた（スイッチごとに）一意の識別番号です。この番号の範囲は 1 ～ 256 です。

NPV ポート チャネルおよび NP ポート チャネルについて

Cisco Nexus デバイス NPV モードで最大 4 つの SAN ポート チャネル（ポート チャネルあたり 8 つのインターフェイス）をサポートします。つまり、NPV モードでは、Cisco Nexus デバイスで最大 4 x NP のポート チャネルをサポートします。ポート チャネル番号は、各チャネル グループに関連付けられた（スイッチごとに）一意の識別番号です。この番号の範囲は 1 ～ 256 です。

F および TF ポート チャネルについて

F ポートチャネルも、同じファイバ チャネル ノードに接続された F ポートのセットを組み合わせ、F ポートと NP ポート間で 1 つのリンクとして動作する論理インターフェイスです。F ポートチャネルでは、E ポートチャネルと同様の帯域利用率およびアベイラビリティをサポートします。F ポートチャネルは主に Nexus 9000 コアと NPV スイッチの接続に使用され、最適な帯域利用率および VSAN のアップリンク間での透過型フェールオーバーを実現します。F ポートチャネルのトランクでは、TF ポートと F ポートチャネルの機能性および利点が組み合わせられます。この論理リンクは、Cisco EPP (ELS) 上で Cisco PTP および PCP プロトコルを使用します。Cisco Nexus デバイス は F/TF ポート チャネルを含む FC スイッチ モードで最大 4 つの SAN ポート チャネルをサポートします。

Note ファイバチャネル トラフィックに対し、すべてのリンクがポート チャネルで使用できるように、 **port-channel load-balance ethernet***source-dest-port* コマンドを入力して、ポート チャネルのロードバランシングを「source-dest-port」に設定します。この設定では、「source-destination-oxid」ロード バランシングがファイバチャネル トラフィックに使用されます。

ポートチャネルと VSAN トランキングの理解

Cisco Nexus デバイスは、次のように VSAN トランキングとポート チャネルを実装します。

- SAN ポート チャネルでは、複数の物理リンクを 1 つの集約論理リンクに結合できます。

- 業界標準の E ポートは、他のベンダー スイッチにリンクできます。スイッチ間リンク（ISL）と呼ばれます（下の図の左側を参照）。
- VSAN トランキングを使用すると、複数の VSAN のトラフィックを伝送する EISL 形式でのフレーム伝送が可能になります。トランキングが E ポートで動作可能な場合、その E ポートは TE ポートになります。次の図の右側に示すように、EISL はシスコ スイッチ間のみで接続されます。

***Figure 12: VSAN* トランキングのみ**

- 下の図の左側に示すように、E ポートであるメンバで SAN ポート チャネルを作成できます。この設定では、ポート チャネルは論理 ISL（1 つの VSAN のトラフィックを伝送する）を実装します。
- 下の図の右側に示すように、TE ポートであるメンバで SAN ポート チャネルを作成できます。この設定では、ポート チャネルは論理 EISL（複数の VSAN のトラフィックを伝送する）を実装します。

***Figure 13:* ポート チャネルと *VSAN* トランキング**

- ポート チャネル インターフェイスは、次のポート セット間でチャネリングできます。
  - E ポートおよび TE ポート
  - F ポートおよび NP ポート
  - TF ポートおよび TNP ポート
- トランキングでは、スイッチ間で複数の VSAN のトラフィックが許可されます。
- ポート チャネルとトランキングは、TE ports over EISL 間で使用できます。

ロード バランシングを理解する

ロード バランシング機能は、次の方式を使用して提供できます。

- フローベース：送信元と宛先間のすべてのフレームが所定のフローで同一のリンクをたどります。つまり、フローの最初のエクスチェンジで選択されたリンクが、後続のすべてのエクスチェンジで使用されます。
- エクスチェンジベース：エクスチェンジの最初のフレームがリンクに割り当てられ、エクスチェンジの後続のフレームが同一のリンクをたどります。ただし、後続のエクスチェンジは、別のリンクを使用できます。この方式によって、より精度の高いロードバランシングが可能になり、さらに各エクスチェンジでのフレームの順序が維持されます。

次の図は、フロー ベースのロード バランシングがどのように機能するかを示しています。フローの最初のフレームが転送のためにインターフェイスで受信されると、リンク 1 が選択され

SAN ポート チャネルの設定

ます。そのフローの各後続のフレームが、同一のリンク上に送信されます。SID1 および DID1 のフレームは、リンク 2 を使用しません。

Figure 14: SID1、DID1、およびフロー ベースのロード バランシング

次の図は、エクスチェンジベースのロードバランシングがどのように機能するかを示しています。エクスチェンジで最初のフレームが転送用にインターフェイスで受信されると、リンク 1 がハッシュ アルゴリズムによって選択されます。その特定のエクスチェンジにある残りすべてのフレームが同一のリンクに送信されます。エクスチェンジ 1 では、リンク 2 を使用するフレームはありません。次のエクスチェンジでは、ハッシュ アルゴリズムによってリンク 2 が選択されます。ここではエクスチェンジ 2 のすべてのフレームが、リンク 2 を使用します。

Figure 15: SID1、DID1、およびエクスチェンジベースのロードバランシング

SAN ポート チャネルの設定

SAN ポート チャネルは、デフォルト値で作成されます。その他の物理インターフェイスと同様にデフォルト設定を変更できます。

次の図は、有効な SAN ポートチャネルの設定例を示しています。

***Figure 16:* 有効な *SAN* ポート チャネルの設定**

次の図は、無効な設定例を示しています。リンクが 1、2、3、4 の順番でアップした場合、ファブリックの設定が誤っているため、リンク 3 および 4 は動作上ダウンします。

***Figure 17:* 誤った設定**

SAN ポート チャネルの設定時の注意事項

SAN ポート チャネルを設定する前に、次の注意事項を守ってください。

- ポートチャネル モードはデフォルトでアクティブです。ポートチャネル **ON** モードはサポートされていません。
- 異なるポート グループのファイバチャネル ポートを使用して、SAN ポートチャネルを構成します。
- 1 つの SAN ポート チャネルが異なるスイッチ群に接続されないようにします。SAN ポート チャネルでは、同一のスイッチ群内でのポイントツーポイント接続が必要です。

- SANポートチャネルを誤って設定すると、誤設定メッセージを受け取る場合があります。このメッセージを受信した場合、エラーが検出されたため、ポートチャネルの物理リンクはディセーブルになります。
- 次の要件を満たしていない場合に、SAN ポート チャネルのエラーが検出されます。
  - SAN ポート チャネルの両側のスイッチが、同じ数のインターフェイスに接続されている必要があります。
  - 各インターフェイスは、反対側の対応するインターフェイスに接続されている必要があります。
  - ポートチャネルを設定したあとで、SANポートチャネルのリンクを変更できません。ポート チャネルを設定したあとにリンクを変更する場合は、必ずそのポート チャネル内でリンクをインターフェイスに再接続し、再度イネーブルにしてください。

    3 つすべての条件が満たされていない場合、そのリンクはディセーブルになっています。
- SAN ポートチャネルのメンバーの最大数は 16 です。
- Cisco Nexus N9K-C93180YC-FX スイッチは、実質的に暗黙の 1:1.6 オーバーサブスクリプション モデルに従います。したがって、24UP ポートのうち、すべてのポートが同時に 16-G FC ライン レートを取得できるわけではありません。
- Cisco Nexus 5672UP-16G スイッチを別の Cisco Nexus 5672UP-16G スイッチに接続する場合は、ポート グループ全体を同じポート タイプに接続します。ポート グループ内のポートは、次のいずれかのシナリオと同じタイプである必要があります。
  - 4 つの F ポートはすべて同じポート グループ内にある必要があります
  - 4 つの E ポートはすべて同じポート グループ内にある必要があります
  - 同じポート チャネルの 4 つのポートはすべて、同じポート グループ内にある必要があります。

  たとえば、Cisco Nexus 5672UP-16G スイッチのポート FC2/1 ～ 4 は、別の Cisco Nexus 5672UP-16G スイッチのポートタイプのポート 1 ～ 4、ポート 5 ～ 8、またはポート 9 ～ 12 に接続できます。

そのインターフェイスに **show interface** コマンドを入力して、ポートチャネルが設定どおりに機能していることを確認します。

F および TF ポート チャネルの注意事項

F および TF ポート チャネルの注意事項は次のとおりです。

- ポートを F モードとしておく必要があります。
- 自動作成はサポートされません。

- ON モードはサポートされません。サポートされるのは Active-Active モードだけです。デフォルトでは、NPV スイッチのモードは Active です。
- MDS スイッチの F ポートチャネル経由でログインしたデバイスは、IVR の非 NAT 設定でサポートされません。このデバイスをサポートするのは IVR NAT 設定だけです。
- ポート セキュリティ ルールは、物理 pWWN だけで単一リンク レベルで実行されます。
- F ポートチャネル経由でログインする N ポートのネーム サーバ登録では、ポートチャネル インターフェイスの fWWN を使用します。
- DPVM 設定はサポートされません。
- ダイナミック ポート VSAN メンバーシップ（DPVM）を使ってポート チャネルのポート VSAN を設定することはできません。
- F ポート チャネルを設定する前に、スイッチで fport-channel-trunk 機能が有効になっていることを確認してください。
- いずれかのインターフェイスでトランキングが設定されている NPV スイッチ、またはトランキング F ポート チャネル機能を有効にするために f port-channel-trunk コマンドが実行される標準スイッチは、以下の予約済み VSAN と分離された VSAN の設定ガイドラインに従います。
  - いずれかのインターフェイスでトランク モードがオンであるか、NP ポート チャネルが稼働している場合、予約済み VSAN は 3040 ～ 4078 であり、ユーザー設定には使用できません。
  - Exchange Virtual Fabric Protocol（EVFP）分離 VSAN は 4079 であり、ユーザー設定には使用できません。

SAN ポート チャネルの作成

SAN ポート チャネルを作成する手順は、次のとおりです。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	Command or Action	Purpose
ステップ 2	switch(config)# **interface san-port-channel** *channel-number*	デフォルトのモード（オン）を使用して、指定された SAN ポート チャネルを作成します。SAN ポート チャネル番号の範囲は、1 ～ 256 です。 **Note** 未使用のチャネル番号を入力して、新しいSANポート チャネルを作成します（ファイバチャネル ポート用）。使用済みと未使用のチャネル番号の範囲を表示するには、**show san-port-channel usage** コマンドを使用します。

ポートチャネル モードについて

チャネル グループ モード パラメータを使用して各 SAN ポート チャネルを設定し、このチャネル グループのすべてのメンバ ポートに対するポート チャネル プロトコルの動作を指定できます。チャネル グループ モードに指定できる値は、次のとおりです。

- オン（デフォルト）：メンバ ポートは SAN ポート チャネルの一部としてだけ動作するか、または非アクティブなままです。このモードでは、ポート チャネル プロトコルは起動されません。ただし、ポート チャネル プロトコル フレームがピア ポートから受信される場合は、ネゴシエーションが不可能な状態であることを示します。オンモードで設定されたポート チャネルでは、ポート チャネルの設定に対してポートの追加または削除を行う場合、各端のポート チャネル メンバ ポートを明示的にイネーブルおよびディセーブルに設定する必要があります。また、ローカル ポートおよびリモート ポートが相互に接続されていることを物理的に確認する必要があります。
- アクティブ：ピア ポートのチャネル グループ モードに関係なく、メンバ ポートはピア ポートとのポート チャネル プロトコル ネゴシエーションを開始します。チャネル グループで設定されているピア ポートがポート チャネル プロトコルをサポートしていない場合、またはネゴシエーション不可能なステータスを返す場合、デフォルトでオン モードの動作に設定されます。アクティブ ポート チャネル モードでは、各端でポート チャネル メンバ ポートを明示的にイネーブルおよびディセーブルに設定することなく自動回復が可能です。

Note F ポート チャネルはアクティブ モードのみでサポートされます。

次の表では、オン モードとアクティブ モードを比較します。

Table 16: チャネルグループ構成の相違点

オン モード	アクティブ モード
プロトコルは交換されません。	ピア ポートとのポート チャネル プロトコル ネゴシエーションが実行されます。

オン モード	アクティブ モード
動作値が SAN ポート チャネルと互換性がない場合、インターフェイスは中断ステートになります。	動作値が SAN ポート チャネルと互換性がない場合、インターフェイスは隔離ステートになります。
ポート チャネルのメンバ ポートの設定を追加または変更する場合、各端でポート チャネルのメンバ ポートを明示的にディセーブル（shut）およびイネーブル（no shut）にする必要があります。	ポート チャネル インターフェイスを追加または変更すると、SAN ポート チャネルは自動的に復旧します。
ポートの起動は同期化されません。	すべてのピア スイッチで、チャネル内のすべてのポートの起動が同時に行われます。
プロトコルが交換されないため、すべての誤構成が検出される訳ではありません。	ポート チャネル プロトコルを使用して常に誤構成が検出されます。
誤設定ポートを中断ステートに移行します。各端でメンバ ポートを明示的にディセーブル（shut）およびイネーブル（no shut）に設定する必要があります。	誤設定を修正するために、誤設定ポートを隔離ステートに移行します。誤設定を修正すれば、プロトコルによって自動的に復旧されます。
これは、デフォルトのモードです。	このモードは明示的に設定する必要があります。

アクティブ モードの SAN ポート チャネルの設定

アクティブ モードを設定する手順は、次のとおりです。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface san-port-channel** *channel-number*
3. switch(config-if)# **channel mode active**
4. switch(config-if)# **no channel mode active**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	Command or Action	Purpose
ステップ 2	switch(config)# **interface san-port-channel** *channel-number*	デフォルトのオン モードを使用して、指定されたポート チャネルを設定します。SAN ポート チャネル番号の範囲は、1 ～ 256 です。
ステップ 3	switch(config-if)# **channel mode active**	アクティブ モードを設定します。
ステップ 4	switch(config-if)# **no channel mode active**	デフォルトのオン モードに戻します。

アクティブ モードの設定例

アクティブ モードを設定する手順は、次のとおりです。

```
switch(config)# interface san-port-channel 1
switch(config-if)# channel mode active
```

SAN ポート チャネルの削除について

SAN ポート チャネルを削除すると、関連するチャネル メンバーシップも削除されます。削除された SAN ポート チャネルのすべてのインターフェイスは、個々の物理リンクに変換されます。SAN ポート チャネルを削除すると、使用されているモード（アクティブおよびオン）に関係なく、各端のポートが正常にシャットダウンされます。これは、インターフェイスのシャットダウン時にフレームが失われないことを意味します。

あるポートの SAN ポート チャネルを削除した場合、削除された SAN ポート チャネル内の各ポートは互換性パラメータの設定（速度、モード、ポート VSAN、許可 VSAN、およびポート セキュリティ）を維持します。これらの設定は、必要に応じて、明示的に変更できます。

- デフォルトのオンモードを使用すると、スイッチ全体の不整合な状態を防ぎ、整合性を保つために、ポートがシャットダウンします。これらのポートは再度明示的にイネーブルにする必要があります。
- アクティブ モードを使用すると、ポート チャネルのポートは削除から自動的に復旧します。

Related Topics

インターフェイスの管理状態の設定 （102 ページ）

SAN ポート チャネルの削除

SAN ポート チャネルを削除する手順は、次のとおりです。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no interface san-port-channel** *channel-number*	指定されたポート チャネル、関連するインターフェイス マッピング、およびこの SAN ポート チャネルのハードウェア アソシエーションを削除します。

SAN ポート チャネルのインターフェイス

物理ファイバ チャネル インターフェイス（またはインターフェイス範囲）を既存の SAN ポート チャネルに追加したり、そこから削除できます。互換性のあるコンフィギュレーション パラメータが、SAN ポート チャネルにマッピングされます。SAN ポート チャネルにインターフェイスを追加すると、SAN ポート チャネルのチャネル サイズと帯域幅が増加します。SAN ポート チャネルからインターフェイスを削除すると、SAN ポート チャネルのチャネル サイズと帯域幅が減少します。

Note 仮想ファイバ チャネル インターフェイスは、SAN ポート チャネルに追加できません。

SAN ポートチャネルへのインターフェイスの追加について

物理インターフェイス（またはインターフェイス範囲）を既存の SAN ポート チャネルに追加できます。互換性のあるコンフィギュレーション パラメータが、SAN ポート チャネルにマッピングされます。SAN ポート チャネルにインターフェイスを追加すると、SAN ポート チャネルのチャネル サイズと帯域幅が増加します。

メンバを追加すると、使用されているモード（アクティブおよびオン）に関係なく、各端のポートが正常にシャットダウンされます。これは、インターフェイスのシャットダウン時にフレームが失われないことを意味します。

Cisco Nexus N9K-C9336C-FX2-E プラットフォーム スイッチの SAN ポート チャネルにファイバ チャネル (FC) ブレイクアウト (BO) インターフェイスを追加するには、SAN スイッチングの一般的なガイドラインと制限事項を参照してください。

互換性チェック

互換性チェックでは、チャネルのすべての物理ポートで同一のパラメータ設定が確実に使用されるようにします。そうでない場合、ポートが SAN ポート チャネルに所属できません。互換性チェックは、ポートを SAN ポート チャネルに追加する前に実施します。

互換性チェックでは、SAN ポート チャネルの両側で次のパラメータと設定が一致することを確認します。

- 機能パラメータ（インターフェイスのタイプ、両側のファイバ チャネル）
- 管理上の互換性パラメータ（速度、モード、ポート VSAN、および許可 VSAN）
- 運用パラメータ（速度およびリモート スイッチの WWN）

リモート スイッチの機能パラメータと管理パラメータおよびローカル スイッチの機能パラメータと管理パラメータに互換性がない場合、ポートは追加できません。互換性チェックが正常であれば、インターフェイスは正常に動作し、対応する互換性パラメータ設定がこれらのインターフェイスに適用されます。

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

- インターフェイスがポート チャネルに追加されると、次のパラメータは削除され、代わってポート チャネルに関する値が指定されます。ただしこの変更は、インターフェイスに関する実行コンフィギュレーションには反映されません。
  - 帯域幅
  - 遅延
  - サービス ポリシー
  - ACL

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

中断および隔離ステート

動作パラメータに互換性がない場合、互換性チェックは失敗し、インターフェイスは設定されたモードに基づいて中断ステートまたは隔離ステートになります。

- インターフェイスがオンモードで設定されている場合、インターフェイスは中断ステートになります。
- インターフェイスがアクティブモードで設定されている場合、インターフェイスは隔離ステートになります。

SAN ポート チャネルへのインターフェイスの追加

SAN ポート チャネルにインターフェイスを追加する手順は、次のとおりです。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot*/port/*BO port*
3. switch(config-if)# **channel-group** *channel-number*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot*/port/*BO port*	指定されたインターフェイスのコンフィギュレーション モードを開始します。 **Note** これが 10G ブレイクアウト ポートの場合、*slot*/*port* 構文は *QSFP-module*/*port* になります。 **Note** これが QSFP+ GEM またはブレイクアウト ポートの場合、*port* 構文は *QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **channel-group** *channel-number*	ファイバ チャネル インターフェイスを指定されたチャネル グループに追加します。チャネル グループが存在しない場合は、作成されます。ポートがシャットダウンする

インターフェイスの強制追加

force オプションを指定して、SAN ポート チャネルがポート設定を上書きするように強制できます。この場合、インターフェイスは SAN ポート チャネルに追加されます。

- デフォルトのオンモードを使用すると、スイッチ全体の不整合な状態を防ぎ、整合性を保つために、ポートがシャットダウンします。これらのポートは再度明示的にイネーブルにする必要があります。
- アクティブ モードを使用すると、ポート チャネルのポートは追加から自動的に復旧します。

Note SAN ポート チャネルが 1 つのインターフェイス内で作成される場合、**force** オプションを使用できません。

ファイバ チャネル（FC）インターフェイスのブレーク アウト（BO）ポート オプションは、Cisco Nexus N9K-C9336C-FX2-E プラットフォーム スイッチにのみ必要です。

メンバーの強制追加後、使用するモード（Active および On）に関係なく、片側のポートは正常にダウンします。これは、インターフェイスがダウンしてもフレームが失われないことを示します。

SAN ポート チャネルへポートを強制的に追加する手順は、次のとおりです。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot*/*port /BO port*
3. switch(config-if)# **channel-group** *channel-number* **force**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot*/*port /BO port*	指定されたインターフェイスのコンフィギュレーション モードを開始します。 **Note** これが 10G ブレイクアウト ポートの場合、*slot*/*port* 構文は *QSFP-module*/*port* になります。 **Note** これが QSFP+ GEM またはブレイクアウト ポートの場合、*port* 構文は *QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **channel-group** *channel-number* **force**	指定されたチャネル グループにインターフェイスを強制的に追加します。E ポートがシャットダウンします。

SAN ポート チャネルからのインターフェイスの削除について

物理インターフェイスが SAN ポート チャネルから削除された場合は、チャネル メンバーシップが自動更新されます。削除されたインターフェイスが最後の動作可能なインターフェイスで

ある場合は、ポート チャネルのステータスは、down ステートに変更されます。SAN ポート チャネルからインターフェイスを削除すると、SAN ポート チャネルのチャネル サイズと帯域幅が減少します。

- デフォルトのオンモードを使用すると、スイッチ全体の不整合な状態を防ぎ、整合性を保つために、ポートがシャットダウンします。これらのポートは再度明示的にイネーブルにする必要があります。
- アクティブ モードを使用すると、ポート チャネルのポートは削除から自動的に復旧します。

メンバを削除すると、使用されているモード（アクティブおよびオン）に関係なく、各端のポートが正常にシャットダウンされます。これは、インターフェイスのシャットダウン時にフレームが失われないことを意味します。

SAN ポート チャネルからのインターフェイスの削除

SAN ポート チャネルから物理インターフェイス（または物理インターフェイス範囲）を削除する手順は、次のとおりです。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot*/*port*/*BO port*
3. switch(config-if)# **no channel-group** *channel-number*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot*/*port*/*BO port*	指定されたインターフェイスのコンフィギュレーション モードを開始します。 **Note** これが 10G ブレイクアウト ポートの場合、*slot*/*port* 構文は *QSFP-module*/*port* になります。 **Note** これが QSFP+ GEM またはブレイクアウト ポートの場合、*port* 構文は *QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **no channel-group** *channel-number*	物理ファイバ チャネル インターフェイスを指定されたチャネル グループから削除します。

SAN ポートチャネル プロトコル

スイッチ ソフトウェアでは、安定性のあるエラー検出および同期化機能を提供します。チャネルグループは手動で構成できます。チャネル グループは同じ機能と構成パラメータを持ちます。関連付けられた SAN ポート チャネル インターフェイスに適用される構成の変更は、チャネル グループ内のすべてのメンバーに伝播されます。

SAN ポート チャネルの設定を交換するプロトコルが Cisco SAN スイッチで使用できます。これにより、互換性のない ISL でのポート チャネル管理が簡素化されます。追加された自動作成モードでは、互換性のあるパラメータを持つ ISL でチャネル グループを自動的に作成でき、手動での作業は必要ありません。

デフォルトではポート チャネル プロトコルがイネーブルになっています。

ポート チャネル プロトコルは、Cisco SAN スイッチのポート チャネル機能モデルを拡張します。ポート チャネル プロトコルは、Exchange Peer Parameters（EPP）サービスを使用して、ISL のピア ポート間の通信を行います。各スイッチは、ローカル設定と動作値に加えて、ピア ポートから受信した情報を使用して、SAN ポート チャネルに属するべきかどうかを判断します。このプロトコルを使用すると、ポート一式が同一の SAN ポート チャネルに属するように設定できます。すべてのポートが互換性のあるパートナーを持つ場合だけ、ポート一式が同一のポート チャネルに属せます。

ポート チャネル プロトコルは、次の 2 つのサブプロトコルを使用します。

- 起動プロトコル：自動的に誤設定を検出するため、これらを修正できます。このプロトコルは両側で SAN ポート チャネルを同期化するため、特定のフロー（送信元 FC ID、宛先 FC ID、および OX_ID によって識別される）のフレームは両方向ともすべて同じ物理リンクを経由して伝送されます。これにより、FCIP リンク上の SAN ポート チャネルで書き込みアクセラレーションなどのアプリケーションを動作させることができます。
- 自動作成プロトコル：互換性のあるポートを SAN ポート チャネルに自動的に集約します。

チャネル グループの作成について

チャネル グループの自動作成がイネーブルの場合、ISL は手動介入なしにチャネル グループに自動的に設定できます。次の図に、チャネル グループの自動作成例を示します。

最初の ISL は個別リンクとしてアップします。次の図に示した例では、これはリンク A1～B1 です。次のリンク（たとえば A2-B2）がアップすると、ポート チャネル プロトコルは、このリンクがリンク A1-B1 と互換性があるかどうかを識別し、それぞれのスイッチでチャネル グループ 10 および 20 を自動的に作成します。それぞれのポートの設定に互換性がある場合、リンク A3-B3 はチャネル グループ（およびポート チャネル）に参加できます。リンク A4-B4 はチャネル グループ内の既存のメンバ ポートと互換性がないため、個別のリンクとして動作します。

Figure 18: チャネル グループの自動作成

チャネル グループ番号は動的に割り当てられます（チャネル グループが形成される場合）。

チャネル グループ番号は、ポートの初期化の順序により同一のポート チャネル群が再起動すると変化する場合があります。

次の表に、ユーザー設定のチャネルグループと自動設定のチャネルグループの相違点を示します。

Table 17: チャネルグループ設定の相違点

ユーザ設定のチャネル グループ	自動設定のチャネル グループ
ユーザが手動で設定します。	2 つの互換性のあるスイッチ間で互換性のあるリンクがアップしたときに自動的に作成されます（両端のすべてのポートでチャネル グループの自動作成がイネーブルになっている場合）。
メンバ ポートはチャネル グループの自動作成には参加できません。自動作成機能は設定できません。	これらのポートは、ユーザ設定のチャネル グループのメンバにはなりません。
チャネル グループのポートの一部を使用して SAN ポート チャネルを作成できます。オン モードまたはアクティブ モードの設定に応じて、互換性のないポートは中断ステートまたは隔離ステートのままになります。	チャネル グループに含まれるすべてのポートが SAN ポート チャネルに参加します。いずれのメンバ ポートも隔離ステートまたは中断ステートになりません。その代わりに、リンクに互換性がない場合、メンバ ポートはチャネル グループから削除されます。
SAN ポート チャネルに対する管理設定は、チャネル グループのすべてのポートに適用され、ポート チャネル インターフェイスの設定は保存できます。	SAN ポート チャネルに対する管理設定は、チャネル グループのすべてのポートに適用され、メンバ ポートの設定は保存されますが、ポート チャネル インターフェイスの設定は保存されません。このチャネル グループは、必要に応じて明示的に変更できます。
任意のチャネル グループの削除およびチャネル グループへのメンバの追加が可能です。	チャネル グループは削除できません。チャネル グループのメンバの追加および削除はできません。メンバ ポートが存在しない場合、チャネル グループは削除されます。

自動作成の注意事項

自動作成プロトコルを使用する場合、次の注意事項に従ってください。

- 自動作成機能がイネーブルの場合、ポートを SAN ポート チャネルの一部として設定できません。これらの 2 つの設定を同時に使用できません。
- 自動作成は、SAN ポート チャネルのネゴシエーションを行うローカル ポートとピア ポートの両方でイネーブルにする必要があります。
- 集約は、次の 2 通りの方法で実行されます。

- ポートを互換性のある自動作成 SAN ポート チャネルへ集約する。
- ポートを互換性のある別のポートと集約して新しいSANポートチャネルを構成する。

- 新しく作成される SAN ポート チャネルには、最大利用可能ポート チャネルからアベイラビリティに基づいて番号が降順に割り当てられます。すべてのポートチャネル番号を使い切ると、集約は許可されなくなります。
- メンバーシップの変更または自動作成された SAN ポート チャネルの削除はできません。
- 自動作成をディセーブルにすると、メンバ ポートはすべて自動作成された SAN ポート チャネルから削除されます。
- 自動作成された SAN ポート チャネルからすべてのメンバが削除されると、チャネルは自動的に削除され、チャネル番号は再利用できるように解放されます。
- 自動作成された SAN ポート チャネルは、再起動後は存在しません。自動作成された SAN ポート チャネルを手動で設定すると、再起動後も維持できます。SAN ポート チャネルを手動で設定すると、自動作成機能はすべてのメンバ ポートでディセーブルになります。
- 自動作成機能は、ポート単位またはスイッチ内のすべてのポートに対して、イネーブルまたはディセーブルに設定できます。この設定がイネーブルの場合、チャネル グループ モードはアクティブと見なされます。このタスクのデフォルトはディセーブルです。
- インターフェイスに対してチャネル グループの自動作成がイネーブルになっている場合、最初に自動作成をディセーブルにしてから、以前のソフトウェア バージョンにダウングレードするか、または手動設定されたチャネル グループでインターフェイスを設定する必要があります。

Tip Cisco Nexusデバイス で自動作成をイネーブルにする場合、自動作成設定を使用せずに、スイッチ間で少なくとも 1 つのポートを相互接続しておくことを推奨します。2 つのスイッチ間のすべてのポートを自動作成機能で同時に設定する場合、ポートは自動作成されたSANポートチャネルに追加される際に自動的にディセーブル化され、再度イネーブルになるため、2つのスイッチ間でトラフィックが中断される可能性があります。

自動作成の有効化および構成

自動チャネル グループを設定する手順は、次のとおりです。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface vfc** *vfc-id*
3. switch(config- if)# **channel-group auto**
4. switch(config- if)# **no channel-group auto**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface vfc** *vfc-id*	指定されたインターフェイスのコンフィギュレーション モードを開始します。
ステップ 3	switch(config- if)# **channel-group auto**	選択したインターフェイスでチャネル グループを自動作成します。
ステップ 4	switch(config- if)# **no channel-group auto**	現在のインターフェイスのチャネル グループの自動作成をディセーブルにします（システムのデフォルト設定で自動作成がイネーブルになっている場合も同様）。

自動作成の設定例

次に、自動チャネル グループを設定する例を示します。

```
switch(config)# interface vfc23
switch(config-if)# channel-group auto
```

手動設定チャネル グループについて

ユーザによって設定されたチャネル グループを自動作成チャネル グループに変更できません。ただし、自動作成されたチャネル グループから手動チャネル グループへの変更は可能です。このタスクは元に戻せません。チャネル グループ番号は変わりませんが、メンバ ポートは手動設定されたチャネル グループのプロパティに従って動作します。また、チャネル グループの自動作成はすべてのポートに対して暗黙的にディセーブルになります。

手動設定にする場合は、必ず SAN ポート チャネルの両側で実行してください。

手動構成チャネル グループへの変更

自動作成されたチャネル グループをユーザ設定チャネル グループに変更するには、**san-port-channel** *channel-group-number* persistent EXEC コマンドを使用します。SAN ポート チャネルが存在しない場合、このコマンドは実行されません。

ポート チャネルの設定例

この項では、F ポート チャネルを共有モードで設定する方法、および NPIV コア スイッチの F ポートと NPV スイッチの NP ポート間のリンクを起動する方法の例を示します。F ポート チャ

ネルを設定する前に、F ポート トランキング、F ポート チャネリング、および NPIV がイネーブルであることを確認します。

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(config)# interface san-po-channel 2
switch(config-if)# switchport mode F
switch(config-if)# channel mode active
switch(config-if)# exit
```

次に、コア スイッチで専用モードでポート チャネル メンバ インターフェイスを設定する例を示します。

```
switch(config)# interface fc1/4-6
switch(config-if)# shut
switch(config-if)# switchport mode F
switch(config-if)# switchport speed 32000
switch(config-if)# switchport trunk mode on
switch(config-if)# channel-group 2
switch(config-if)# no shut
switch(config-if)# exit
```

SAN ポート チャネル構成の確認

EXEC モードからいつでも既存の SAN ポート チャネルの特定の情報を表示できます。次の **show** コマンドを実行すると、既存の SAN ポート チャネルの詳細が表示されます。

show san-port-channel summary コマンドを実行すると、スイッチ内の SAN ポート チャネルの概要が表示されます。各 SAN ポート チャネルの 1 行ずつの概要には、管理ステート、動作可能ステート、接続されてアクティブな状態（アップ）のインターフェイスの数、コントロール プレーン トラフィック（ロードバランシングなし）を伝送するために SAN ポート チャネルで選択された主要な動作可能インターフェイスである First Operational Port（FOP）を表示します。FOP は SAN ポート チャネルで最初にアップするポートで、このポートがダウンした場合は変わることがあります。FOP は、show san-port-channel database cli のアスタリスク (*) でも識別されます。

VSAN の設定情報を表示するには、次のいずれかのタスクを実行します。

SUMMARY STEPS

1. switch# **show san-port-channel summary** | **database** | **consistency** [**details**] | **usage** | **compatibility-parameters**
2. switch# **show san-port-channel database interface san-port-channel** *channel-number*
3. switch# switch# **show interface vfc** *vfc*/*idt*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **show san-port-channel summary** | **database** | **consistency** [**details**] | **usage** | **compatibility-parameters**	SAN ポート チャネルの情報を表示します。
ステップ 2	switch# **show san-port-channel database interface san-port-channel** *channel-number*	指定された SAN ポート チャネルの情報を表示します。
ステップ 3	switch# switch# **show interface vfc** *vfc*/*idt*	指定されたファイバ チャネル インターフェイスの VSAN 設定情報を表示します。

確認コマンドの例

次に、SAN ポート チャネル情報の概要を表示する例を示します。

```
switch# show san-port-channel summary
--------------------------------------------------------------------------------
Interface                 Total Ports        Oper Ports        First Oper Port
--------------------------------------------------------------------------------
san-port-channel 7              2                 0                 --
san-port-channel 8              2                 0                 --
san-port-channel 9              2                 2
```

次に、SAN ポート チャネルの一貫性を表示する例を示します。

```
switch# show san-port-channel consistency
Database is consistent
```

次に、使用および未使用ポート チャネル番号の詳細を表示する例を示します。

```
switch# show san-port-channel usage
Totally 3 port-channel numbers used
===================================
Used  :   77 - 79
Unused:   1 - 76 , 80 - 256
```

自動作成された SAN ポート チャネルは、手動で作成された SAN ポート チャネルと区別できるように、明示的に示されます。次に、自動作成されたポート チャネルを表示する例を示します。

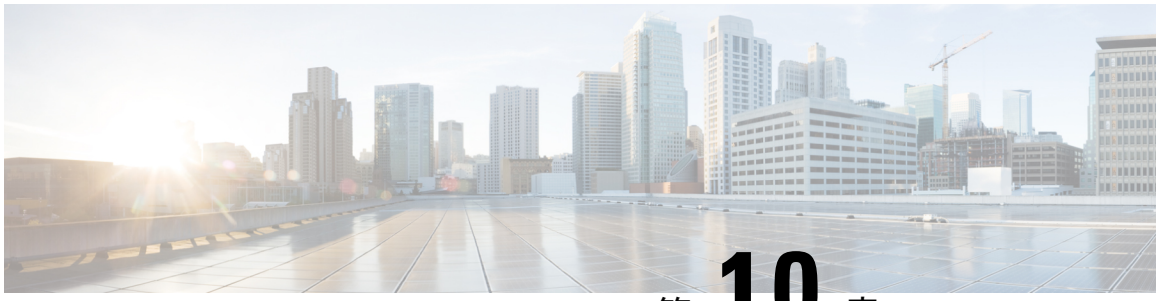
```
switch# show interface vfc21
vfc21 is trunking
    Hardware is Fibre Channel, FCOT is short wave laser
    Port WWN is 20:0a:00:0b:5f:3b:fe:80
    ...
    Receive data field Size is 2112
    Port-channel auto creation is enabled

Belongs to port-channel 123
...
```

SAN ポート チャネルのデフォルト設定

次の表に、SAN ポートチャネルのデフォルト設定を示します。

Table 18: デフォルト *SAN* 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	FSPF はデフォルトでイネーブルになっています。
ポート チャネル作成	管理上のアップ状態
デフォルト ポート チャネル モード	オン
自動作成	ディセーブル



第 10 章

ファイバチャネル ドメイン パラメータの構成

この章では、ファイバ チャネル ドメイン パラメータの設定方法について説明します。

この章は、次の項で構成されています。

ドメイン パラメータに関する情報

ファイバ チャネル ドメイン（fcdomain）機能では、FC-SW-2 標準で記述されているように、主要スイッチ選択、ドメイン ID 配信、FC ID 割り当て、ファブリック再設定機能が実行されます。ドメインは VSAN 単位で設定されます。ドメイン ID を設定しない場合、ローカル スイッチはランダムな ID を使用します。

Caution fcdomain パラメータは、通常変更しないでください。これらの変更は、管理者が行うか、スイッチ操作を熟知している人が行ってください。

設定を変更した場合は、必ず実行コンフィギュレーションを保存してください。次回にスイッチを再起動したときに、保存された設定が使用されます。設定を保存しない場合は、前回保存されたスタートアップ コンフィギュレーションが使用されます。

ファイバチャネル ドメイン

fcdomain は、4 つのフェーズで構成されます。

- 主要スイッチの選択：このフェーズでは、ファブリック内で一意の主要スイッチを選択できます。
- ドメイン ID の配信：このフェーズでは、ファブリック内のスイッチごとに、一意のドメイン ID を取得できます。

- FC ID の割り当て：このフェーズでは、ファブリック内の対応するスイッチに接続された各デバイスに、一意の FC ID を割り当てることができます。
- ファブリックの再設定：このフェーズでは、ファブリック内のすべてのスイッチを再同期化して、新しい主要スイッチ選択フェーズを同時に再開できるようにします。

次の図は、fcdomain の構成例を示します。

***Figure 19: fcdomain* の構成例**

ドメインの再起動

ファイバ チャネル ドメインは、中断を伴う方法または中断を伴わない方法で起動できます。中断再起動を実行した場合は、Reconfigure Fabric（RCF）フレームがファブリック内のその他のスイッチに送信され、VSAN（リモートでセグメント化された ISL を含む）内のすべてのスイッチでデータ トラフィックは中断されます。非中断再起動を実行した場合は、Build Fabric（BF）フレームがファブリック内のその他のスイッチに送信され、該当スイッチでだけデータ トラフィックは中断されます。

ドメイン ID の競合を解消するには、手動でドメイン ID を割り当てる必要があります。ドメイン ID を手動で割り当てるなど、ほとんどの設定変更では中断再起動が必要になります。ドメインの非中断再起動は、優先ドメイン ID をスタティック ドメイン ID（実ドメイン ID は変更なし）に変更する場合にかぎり実行できます。

Note スタティック ドメインはユーザによって固有に設定されるため、実行時のドメインと異なることがあります。ドメイン ID が異なる場合は、次回の再起動後にスタティック ドメイン ID を使用するように、実行時のドメイン ID が変更されます。

Note 中断を伴うファブリックの再起動再設定（RCF）は、Cisco Nexus C93180YC-FX スイッチではサポートされていません。

ほとんどの設定は、対応する実行時の値に適用できます。ここでは、実行時の値に fcdomain パラメータを適用する方法について詳細に説明します。

fcdomain restart コマンドを使用すると、変更が実行時の設定に適用されます。disruptive オプションはサポートされていません。

ドメインの再起動

ファブリックの中断再起動または非中断再起動を実行できます。

SUMMARY STEPS

1. **configure terminal**
2. **fcdomain restart vsan** *vsan-id*
3. switch(config)# **fcdomain restart disruptive vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**fcdomain restart vsan** *vsan-id* **Example:** `switch (config)# fcdomain restart vsan 100`	トラフィックを中断しないで再設定するようにVSANを設定します。VSAN IDの範囲は、1～4093です。
ステップ 3	switch(config)# **fcdomain restart disruptive vsan** *vsan-id* **Example:** `switch (config)# fcdomain restart disruptive vsan 101`	データ トラフィックを中断して再設定するようにVSAN を設定します。

ドメイン マネージャの高速再起動

主要リンクで障害が発生した場合、ドメインマネージャが新しい主要リンクを選択する必要があります。デフォルトでは、ドメイン マネージャはBuild Fabric（BF）フェーズを開始し、その後主要スイッチ選択フェーズが続きます。これらのフェーズは両方ともVSAN内のすべてのスイッチに影響を及ぼし、完了するまで合計15秒以上かかります。ドメイン マネージャが新しい主要リンクの選択に必要な時間を短縮するために、ドメインマネージャの高速再起動機能をイネーブルにできます。

高速再起動がイネーブルで、バックアップ リンクを利用できる場合、ドメイン マネージャはわずか数ミリ秒で新しい主要リンクを選択し、障害が発生したリンクを交換します。また、新しい主要リンクの選択に必要な再設定は、VSAN全体ではなく、障害が発生したリンクに直接接続した2つのスイッチにだけ影響します。バックアップ リンクが利用できない場合、ドメイン マネージャはデフォルトの動作に戻り、BF フェーズを開始します。その後、主要スイッチ選択フェーズが続きます。高速再起動機能はどのインターオペラビリティ モードでも使用できます。

ドメイン マネージャの高速再起動の有効化

ドメイン マネージャの高速再起動をイネーブルに設定できます。

SUMMARY STEPS

1. **configure terminal**
2. **fcdomain optimize fast-restart vsan** *vsan-id*
3. **no fcdomain optimize fast-restart vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**fcdomain optimize fast-restart vsan** *vsan-id* **Example:** `switch(config)# fcdomain optimize fast-restart vsan 1`	指定された VSAN でドメイン マネージャの高速再起動をイネーブルにします。VSAN ID の範囲は、1 ～ 4093 です。
ステップ 3	**no fcdomain optimize fast-restart vsan** *vsan-id* **Example:** `switch(config)# no fcdomain optimize fast-restart vsan 1`	指定された VSAN でドメイン マネージャの高速再起動をディセーブル（デフォルト）にします。VSAN ID の範囲は、1 ～ 4093 です。

スイッチの優先度

デフォルトでは、プライオリティは 128 に設定されます。プライオリティの有効設定範囲は 1 ～ 254 です。プライオリティ 1 が最高のプライオリティです。値 255 は、他のスイッチからは受け入れられますが、ローカルには設定できません。

安定したファブリックに追加された新しいスイッチが、主要スイッチになることはありません。主要スイッチ選択フェーズ中に、最高のプライオリティを持つスイッチが主要スイッチになります。2 つのスイッチに同じプライオリティが設定されている場合、小さい World Wide Name（WWN）のスイッチが主要スイッチになります。

プライオリティ設定は、fcdomain の再起動の実行時に適用されます。この設定は、中断再起動および非中断再起動のどちらにも適用できます。

スイッチ優先順位の構成

主要スイッチにプライオリティを設定できます。

SUMMARY STEPS

1. **configure terminal**
2. **fcdomain priority** *number* **vsan** *vsan-id*

3. **no fcdomain priority** *number* **vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**fcdomain priority** *number* **vsan** *vsan-id* **Example:** `switch(config)# fcdomain priority 12 vsan 1`	指定された VSAN 内のローカル スイッチに指定されたプライオリティを設定します。fcdomain プライオリティの範囲は、1 ～ 254 です。VSAN ID の範囲は、1 ～ 4093 です。
ステップ 3	**no fcdomain priority** *number* **vsan** *vsan-id* **Example:** `switch(config)# no fcdomain priority 12 vsan 1`	指定されたVSANのプライオリティを出荷時の設定（128）に戻します。fcdomain プライオリティの範囲は、1 ～ 254 です。VSAN ID の範囲は、1 ～ 4093 です。

fcdomain の開始について

デフォルトでは、fcdomain 機能は各スイッチ上でイネーブルになっています。スイッチ内で fcdomain機能をディセーブルにすると、そのスイッチはファブリック内のその他のスイッチと共存できなくなります。fcdomain 設定は中断再起動の実行時に適用されます。

fcdomain の無効化または再有効化

単一の VSAN または VSAN 範囲で fcdomain をディセーブルまたは再度イネーブルにする手順は、次のとおりです。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no fcdomain vsan** *vsan-id* **-** *vsan-id*
3. switch(config)# **fcdomain vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	Command or Action	Purpose
ステップ 2	switch(config)# **no fcdomain vsan** *vsan-id - vsan-id*	指定された VSAN 範囲で fcdomain 設定をディセーブルにします。
ステップ 3	switch(config)# **fcdomain vsan** *vsan-id*	指定された VSAN で fcdomain 設定をイネーブルにします。

ファブリック名の構成

無効化された fcdomain にファブリック名の値を構成できます。

SUMMARY STEPS

1. **configure terminal**
2. **fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan** *vsan-id*
3. **no fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan** *vsan-id* **Example:** `switch(config)# fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan 1`	指定されたVSANに設定済みファブリック名の値を割り当てます。VSAN IDの範囲は、1～4093です。
ステップ 3	**no fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan** *vsan-id* **Example:** `switch(config)# no fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan 1`	VSAN 3010のファブリック名の値を出荷時のデフォルト設定（20:01:00:05:30:00:28:df）に変更します。VSAN ID の範囲は、1 ～ 4093 です。

着信 RCF

rcf-reject オプションはインターフェイス単位、VSAN 単位で設定できます。rcf-reject オプションはデフォルトで無効になっています（つまり、RCF 要求フレームは自動的に拒否されません）。

rcf-reject オプションは即座に有効になります。

fcdomain の再起動は不要です。

Note 仮想ファイバ チャネル インターフェイスの RCF 拒否オプションを設定する必要はありません。

着信 RCF の拒否

着信 RCF 要求フレームを拒否できます。

SUMMARY STEPS

1. **configure terminal**
2. **interface vfc** *vfc-id*
3. switch(config)# **interface vfc** *vfc-id*
4. **fcdomain rcf-reject vsan** *vsan-id*
5. **no fcdomain rcf-reject vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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 vfc** *vfc-id* **Example:** `switch(config)# interface vfc 20`	指定されたインターフェイスを設定します。仮想インターフェイスの ID 範囲は、1 ～ 8192 です。
ステップ 3	switch(config)# **interface vfc** *vfc-id*	指定されたインターフェイスを設定します。
ステップ 4	**fcdomain rcf-reject vsan** *vsan-id* **Example:** `switch(config-if)# fcdomain rcf-reject vsan 10`	指定されたVSAN内の指定されたインターフェイス上でRCFフィルタをイネーブルにします。VSAN IDの範囲は、1 ～ 4093 です。
ステップ 5	**no fcdomain rcf-reject vsan** *vsan-id* **Example:** `switch(config-if)# no fcdomain rcf-reject vsan 10`	指定されたVSAN内の指定されたインターフェイス上でRCFフィルタをディセーブル（デフォルト）にします。VSAN ID の範囲は、1 ～ 4093 です。

マージされたファブリックの自動再構成

デフォルトでは、autoreconfigure オプションはディセーブルです。重複ドメインを含む、2 つの異なる安定したファブリックに属する 2 つのスイッチを結合した場合は、次のようになります。

- 両方のスイッチで autoreconfigure オプションがイネーブルの場合、中断再設定フェーズが開始します。
- いずれかまたは両方のスイッチで autoreconfigure オプションがディセーブルの場合は、2 つのスイッチ間のリンクが隔離されます。

autoreconfigure オプションは実行時に即座に有効になります。fcdomain を再起動する必要はありません。ドメインが重複によって現在隔離されており、後で両方のスイッチの autoreconfigure オプションをイネーブルにする場合は、ファブリックは隔離状態のままです。ファブリックを接続する前に両方のスイッチで autoreconfigure オプションをイネーブルにした場合、中断再設定（RCF）が発生します。中断再設定が発生すると、データ トラフィックが影響を受けることがあります。fcdomain に非中断再設定を行うには、重複リンク上の設定済みドメインを変更し、ドメインの重複を排除します。

自動再構成の有効化

特定の VSAN（または VSAN 範囲）で自動再構成を有効化できます。

SUMMARY STEPS

1. **configure terminal**
2. **fcdomain auto-reconfigure vsan** *vsan-id*
3. **no fcdomain auto-reconfigure vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**fcdomain auto-reconfigure vsan** *vsan-id* **Example:** `switch(config)# fcdomain auto-reconfigure vsan 1`	指定された VSAN で自動再設定オプションをイネーブルにします。VSAN ID の範囲は、1 ～ 4093 です。

	Command or Action	Purpose
ステップ 3	**no fcdomain auto-reconfigure vsan** *vsan-id* **Example:** `switch(config)# no fcdomain auto-reconfigure vsan 1`	指定された VSAN で自動再設定オプションをディセーブルにし、出荷時のデフォルト設定に戻します。VSAN ID の範囲は、1 ～ 4093 です。

ドメイン ID

ドメイン ID は VSAN 内のスイッチを一意に識別します。スイッチは異なる VSAN に異なるドメイン ID を持つことがあります。ドメイン ID は FC ID 全体の一部です。

ドメイン ID - 注意事項

設定済みドメイン ID のタイプは優先またはスタティックになります。デフォルトで、設定済みドメイン ID は 0（ゼロ）、設定タイプは優先です。

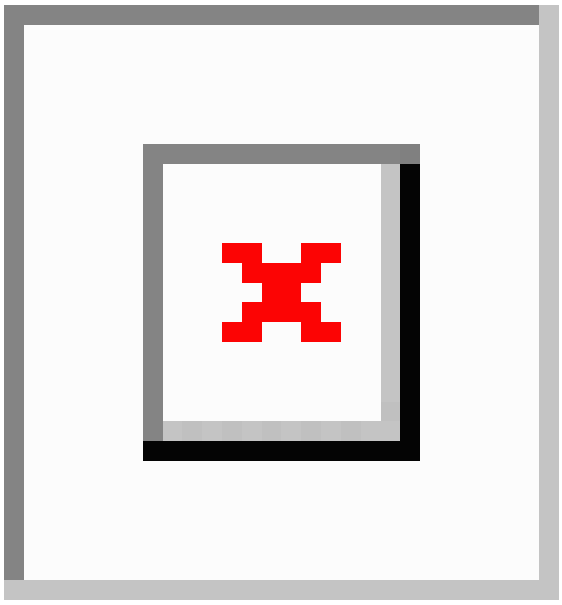
Note 値 0（ゼロ）を設定できるのは、優先オプションを使用した場合だけです。

ドメイン ID を設定しない場合、ローカル スイッチは要求内でランダムな ID を送信します。スタティック ドメイン ID を使用することを推奨します。

下位スイッチがドメインを要求する場合は、次のプロセスが実行されます（次の図を参照）。

- ローカル スイッチは主要スイッチに設定済みドメイン ID 要求を送信します。
- 要求されたドメイン ID が使用可能な場合、主要スイッチはこの ID を割り当てます。使用不可能な場合は、使用可能な別のドメイン ID を割り当てます。

Figure 20: 優先オプションを使用した設定プロセス



下位スイッチの動作は、次の 3 つの要素により異なります。

- 許可ドメイン ID リスト
- 設定済みドメイン ID
- 主要スイッチが要求元スイッチに割り当てたドメイン ID

状況に応じて、次のように変更されます。

- 受信されたドメイン ID が許可リストに含まれない場合は、要求されたドメイン ID が実行時ドメイン ID になり、該当する VSAN のすべてのインターフェイスが隔離されます。
- 割り当てられたドメイン ID と要求されたドメイン ID が同じである場合は、優先およびスタティック オプションは関係せず、割り当てられたドメイン ID が実行時ドメイン ID になります。
- 割り当てられたドメイン ID と要求されたドメイン ID が異なる場合は、次のようになります。
  - 設定タイプがスタティックの場合は、割り当てられたドメイン ID が廃棄され、すべてのローカル インターフェイスは隔離され、ローカル スイッチには設定済みのドメイン ID が自動的に割り当てられます（この ID が実行時ドメイン ID になります）。
  - 設定タイプが preferred の場合、ローカル スイッチは主要スイッチによって割り当てられたドメイン ID を受け入れ、割り当てられた ID が実行時ドメイン ID になります。

設定済みドメイン ID を変更したときに、変更が受け入れられるのは、新しいドメイン ID が、VSAN 内に現在設定されているすべての許可ドメイン ID リストに含まれている場合だけです。または、ドメイン ID を 0 の優先に設定することもできます。

Caution 設定したドメインの変更をランタイム ドメインに適用する場合は、fcdomain コマンドを入力する必要があります。

Note 許可ドメイン ID リストを設定した場合、追加するドメイン ID は VSAN のその範囲内にある必要があります。

Related Topics

許可ドメイン ID リスト （174 ページ）

スタティック ドメイン ID または優先ドメイン ID の設定

スタティック ドメイン ID または優先ドメイン ID を指定できます。

SUMMARY STEPS

1. **configure terminal**
2. **fcdomain domain** *domain-id* **static vsan** *vsan-id*
3. **no fcdomain domain** *domain-id* **static vsan** *vsan-id*
4. **fcdomain domain** *domain-id* **preferred vsan** *vsan-id*
5. **no fcdomain domain** *domain-id* **preferred vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**fcdomain domain** *domain-id* **static vsan** *vsan-id* **Example:** `switch(config)# fcdomain domain 1 static vsan 3`	特定の値だけを受け入れるように指定の VSAN 内のスイッチを設定し、要求されたドメイン ID が許可されない場合は、指定の VSAN 内のローカル インターフェイスを隔離ステートに移行します。ドメイン ID の範囲は 1 ～ 239 です。VSAN ID の範囲は、1 ～ 4093 です。
ステップ 3	**no fcdomain domain** *domain-id* **static vsan** *vsan-id* **Example:** `switch(config)# no fcdomain domain 1 static vsan 3`	設定済みドメイン ID を、指定 VSAN 内の出荷時のデフォルト設定にリセットします。設定済みドメイン ID は 0 preferred になります。

	Command or Action	Purpose
ステップ 4	**fcdomain domain** *domain-id* **preferred vsan** *vsan-id* **Example:** `switch(config)# fcdomain domain 1 preferred vsan 5`	preferred ドメイン ID 3 を要求するために指定の VSAN 内のスイッチを設定し、主要スイッチによって割り当てられた値をすべて受け入れます。ドメイン ID の範囲は 1 ～ 239 です。VSAN ID の範囲は、1 ～ 4093 です。
ステップ 5	**no fcdomain domain** *domain-id* **preferred vsan** *vsan-id* **Example:** `switch(config)# no fcdomain domain 1 preferred vsan 5`	指定の VSAN 内の設定済みドメイン ID を 0（デフォルト）にリセットします。設定済みドメイン ID は 0 preferred になります。

許可ドメイン ID リスト

デフォルトでは、割り当て済みのドメイン ID リストの有効範囲は 1 ～ 239 です。許可ドメイン ID リストに複数の範囲を指定し、各範囲をカンマで区切れます。主要スイッチは、ローカルに設定された許可ドメイン リストで使用可能なドメイン ID を割り当てます。

ドメイン ID が重複しないように、許可ドメイン ID リストを使用して VSAN を設計してください。このリストは将来 NAT 機能を使用しない IVR を実装する必要がある場合に役立ちます。

ファブリック内の 1 つのスイッチに許可リストを設定する場合は、整合性を保つために、ファブリック内のその他のすべてのスイッチに同じリストを設定するか、CFS を使用して設定を配信することを推奨します。

許可ドメイン ID リストの構成

許可ドメイン ID リストを設定できます。

SUMMARY STEPS

1. **configure terminal**
2. **fcdomain allowed** *domain-id range* **vsan** *vsan-id*
3. **no fcdomain allowed** *domain-id range* **vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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。

	Command or Action	Purpose
ステップ 2	**fcdomain allowed** *domain-id range* **vsan** *vsan-id* **Example:** `switch(config)# fcdomain allowed 3 vsan 10`	指定の VSAN でドメイン ID 範囲を持つスイッチを許可するようにリストを設定します。ドメイン ID の範囲は 1 ～ 239 です。VSAN ID の範囲は、1 ～ 4093 です。
ステップ 3	**no fcdomain allowed** *domain-id range* **vsan** *vsan-id* **Example:** `switch(config)# no fcdomain allowed 3 vsan 10`	指定の VSAN でドメイン ID 1 ～ 239 のスイッチを許可する出荷時のデフォルト設定に戻します。

許可ドメイン ID リストの CFS 配信

Cisco Fabric Services（CFS）インフラストラクチャを使用して、ファブリック内のすべての Cisco SAN スイッチへの許可ドメイン ID リスト設定情報の配信をイネーブルにできます。この機能を使用すると、1 つのスイッチのコンソールからファブリック全体の設定を同期化できます。VSAN 全体に同じ設定が配信されるので、誤設定や、同じ VSAN 内の 2 つのスイッチが互換性のない許可ドメインを設定してしまう可能性を防止します。

CFS を使用して許可ドメイン ID リストを配信し、VSAN 内のすべてのスイッチで許可ドメイン ID リストの整合性をとるようにします。

Note 許可ドメイン ID リストを設定してそれを主要スイッチにコミットするようお勧めします。

追加情報については、ご使用のデバイスの『System Management Configuration Guide』の「Using Cisco Fabric Services」を参照してください。

配信のイネーブル化

許可ドメイン ID リスト設定の配信をイネーブル（またはディセーブル）に設定できます。

許可ドメイン ID リストの CFS 配信はデフォルトではディセーブルになっています。許可ドメイン ID リストを配信するすべてのスイッチで配信をイネーブルにする必要があります。

Before you begin

CFS の前提条件は、次のとおりです。

CFS はデフォルトでイネーブルです。ファブリック内のすべてのデバイスで CFS をイネーブルに設定しないと配信は受信されません。アプリケーションに対して CFS がディセーブルになっていると、そのアプリケーションからコンフィギュレーションは配信されず、ファブリック内の他のデバイスからの配信も受け取ることができません。CFS を有効にするには、**cfs distribute** コマンドを使用します。

SUMMARY STEPS

1. **configure terminal**

2. **fcdomain distribute**
3. **no fcdomain distribute**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**fcdomain distribute** **Example:** `switch(config)# fcdomain distribute`	ドメイン設定の配信をイネーブルにします。
ステップ 3	**no fcdomain distribute** **Example:** `switch(config)# no fcdomain distribute`	ドメイン設定の配信をディセーブル（デフォルト）にします。

ファブリックのロック

既存の設定を変更するときの最初のアクションによって、保留中の設定が作成され、ファブリック内の機能がロックされます。ファブリックがロックされると、次のような状況になります。

- 他のユーザーがこの機能の設定に変更を加えることができなくなります。
- アクティブな設定をコピーすると保留中の設定が作成されます。以降の変更は保留中の設定に行われ、アクティブな設定（およびファブリック内の他のスイッチ）への変更をコミットまたは廃棄するまでそのままです。

変更のコミット

保留中のドメイン設定変更をコミットして、ロックを解除できます。

VSAN 内の他の SAN スイッチに保留中のドメイン設定の変更を適用するには、変更をコミットする必要があります。保留中の設定変更が配信され、コミットが正常に行われると、設定の変更が VSAN 全体の SAN スイッチのアクティブな設定に適用され、ファブリック ロックが解除されます。

SUMMARY STEPS

1. **configure terminal**
2. **fcdomain commit vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**fcdomain commit vsan** *vsan-id* **Example:** `switch(config)# fcdomain commit vsan 45`	保留中のドメイン設定変更をコミットします。

変更の破棄

保留中のドメイン設定変更を破棄して、ロックを解放できます。

いつでもドメイン設定への保留変更を廃棄して、ファブリックのロックを解除できます。保留中の変更を廃棄（中断）する場合、設定には影響せずに、ロックが解除されます。

SUMMARY STEPS

1. **configure terminal**
2. **fcdomain abort vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**fcdomain abort vsan** *vsan-id* **Example:** `switch(config)# fcdomain abort vsan 30`	保留中のドメイン設定変更を廃棄します。

ファブリックのロックのクリア

ドメイン設定作業を実行し、変更をコミットまたは廃棄してロックを解除していない場合、管理者はファブリック内の任意のスイッチからロックを解除できます。管理者がこのタスクを実行すると、保留中の変更は廃棄され、ファブリック ロックが解除されます。

保留中の変更はvolatileディレクトリだけで使用でき、スイッチを再起動すると廃棄されます。

ファブリック ロックを解除するには、管理者の権限を持つログイン ID を使用して EXEC モードで **clear fcdomain session vsan** コマンドを入力します。

```
switch# clear fcdomain session vsan 10
```

CFS 配信ステータスの表示

許可ドメイン ID リストの CFS 配信のステータスは **show fcdomain status** コマンドを使用して表示できます。

```
switch# show fcdomain status
CFS distribution is enabled
```

保留中の変更の表示

保留中の構成変更は **show fcdomain pending** コマンドを使用して表示できます。

```
switch# show fcdomain pending vsan 10
Pending Configured Allowed Domains
---------------------------------
VSAN 10
Assigned or unallowed domain IDs: 1-9,24,100,231-239.
[User] configured allowed domain IDs: 10-230.
```

保留中の設定と現在の設定の違いは、**show fcdomain pending-diff** コマンドを使用して表示できます。

```
switch# show fcdomain pending-diff vsan 10
Current Configured Allowed Domains
---------------------------------
VSAN 10
Assigned or unallowed domain IDs: 24,100.
[User] configured allowed domain IDs: 1-239.
Pending Configured Allowed Domains
---------------------------------
VSAN 10
Assigned or unallowed domain IDs: 1-9,24,100,231-239.
[User] configured allowed domain IDs: 10-230.
```

セッション ステータスの表示

配信セッションのステータスは **show fcdomain session-status vsan** コマンドを使用して表示できます。

```
switch# show fcdomain session-status vsan 1
```

```
Last Action Time Stamp : None
Last Action : None
Last Action Result : None
Last Action Failure Reason : none
```

連続ドメイン ID の割り当て

デフォルトでは、連続ドメイン割り当てはディセーブルです。下位スイッチが主要スイッチに複数の不連続ドメインを要求した場合は、次のようになります。

- 主要スイッチで連続ドメイン割り当てがイネーブルの場合、主要スイッチは連続ドメインを特定し、それらを下位スイッチに割り当てます。連続ドメインが使用できない場合、スイッチ ソフトウェアはこの要求を拒否します。
- 主要スイッチで連続ドメイン割り当てがディセーブルの場合、主要スイッチは使用可能なドメインを下位スイッチに割り当てます。

連続ドメイン ID 割り当ての有効化

特定の VSAN（または VSAN 範囲）で連続ドメインをイネーブルに設定できます。

SUMMARY STEPS

1. **configure terminal**
2. **fcdomain contiguous-allocation vsan** *vsan-id*
3. **no fcdomain contiguous-allocation vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**fcdomain contiguous-allocation vsan** *vsan-id* **Example:** `switch(config)# fcdomain contiguous-allocation vsan 22-30`	指定された VSAN 範囲で連続割り当てオプションをイネーブルにします。 **Note** **contiguous-allocation** オプションは実行時に即座に有効になります。fcdomain を再起動する必要はありません。
ステップ 3	**no fcdomain contiguous-allocation vsan** *vsan-id* **Example:** `switch(config)# no fcdomain contiguous-allocation vsan 7`	指定された VSAN で連続割り当てオプションをディセーブルにし、出荷時の設定に戻します。

FC ID

SAN スイッチにログインしたN ポートには、FC ID が割り当てられます。デフォルトでは、固定的FC ID機能はイネーブルです。この機能がディセーブルの場合は、次のようになります。

- N ポートは SAN スイッチにログインします。要求元 N ポートの WWN および割り当てられた FC ID が維持され、揮発性キャッシュに格納されます。この揮発性キャッシュの内容は、再起動時に保存されません。
- スイッチは、FC ID と WWN のバインディングをベストエフォート方式で保持するように設計されています。たとえば、スイッチから 1 つの N ポートを切断したあとに、別のデバイスから FC ID が要求されると、この要求が許可されて、WWN と初期 FC ID の関連付けが解除されます。
- 揮発性キャッシュには、WWN と FC ID のバインディングのエントリを 4000 まで格納できます。このキャッシュが満杯になると、新しい（より最近の）エントリによって、キャッシュ内の最も古いエントリが上書きされます。この場合、最も古いエントリの対応する WWN と FC ID の関連付けが失われます。
- N ポートを取り外し、同じスイッチの任意のポートに接続すると、（このポートが同じ VSAN に属するかぎり）この N ポートには同じ FC ID が割り当てられます。

永続的 FC ID

永続的 FC ID がイネーブルの場合は、次のようになります。

- fcdomain 内の現在使用中の FC ID は、再起動後も保存されます。
- fcdomain は、デバイス（ホストまたはディスク）をポートインターフェイスに接続したあとに学習されたダイナミック エントリを、自動的にデータベースに入力します。

Note AIX または HP-UX ホストからスイッチに接続する場合は、それらのホストに接続する VSAN で固定的 FC ID 機能をイネーブルにする必要があります。

Note 永続的 FC ID がイネーブルである場合、再起動後に FC ID を変更できません。FC ID はデフォルトではイネーブルですが、各 VSAN に対してディセーブルにできます。

F ポートに割り当てられた固定的 FC ID は、インターフェイス間を移動させることができ、同じ固定的 FC ID をそのまま維持することができます。

永続的 FC ID 機能の有効化

永続的 FC ID 機能をイネーブルに設定できます。

SUMMARY STEPS

1. **configure terminal**
2. **fcdomain fcid persistent vsan** *vsan-id*
3. **no fcdomain fcid persistent vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**fcdomain fcid persistent vsan** *vsan-id* **Example:** `switch(config)# fcdomain fcid persistent vsan 78`	指定された VSAN の FC ID 永続性をアクティブ（デフォルト）にします。
ステップ 3	**no fcdomain fcid persistent vsan** *vsan-id* **Example:** `switch(config)# no fcdomain fcid persistent vsan 33`	指定された VSAN の FC ID 永続性機能をディセーブルにします。

永続的 FC ID 設定時の注意事項

固定的 FC ID 機能をイネーブルにすると、固定的 FC ID サブモードを開始して、FC ID データベースにスタティックまたはダイナミック エントリを追加できるようになります。デフォルトでは、追加されたすべてのエントリはスタティックです。固定的 FC ID は VSAN 単位で設定します。

永続的 FC ID を手動で設定するための要件は、次のとおりです。

- 必要な VSAN 内で固定的 FC ID 機能がイネーブルになっていることを確認します。
- 目的の VSAN がアクティブ VSAN であることを確認します。永続的 FC ID は、アクティブ VSAN だけで設定できます。
- FC ID のドメイン部分が必要な VSAN 内の実行時ドメイン ID と同じであることを確認します。ソフトウェアがドメインの不一致を検出した場合、コマンドは拒否されます。
- エリアを設定するときに、FC ID のポート フィールドが 0（ゼロ）であることを確認します。

永続的 FC ID の構成

永続的 FC ID を構成設定できます。

SUMMARY STEPS

1. **configure terminal**
2. **fcdomain fcid database**
3. **vsan** *vsan-id* **wwn 33:e8:00:05:30:00:16:df fcid** *fcid*
4. **vsan** *vsan-id* **wwn 11:22:11:22:33:44:33:44 fcid** *fcid* **dynamic**
5. **vsan** *vsan-id* **wwn 11:22:11:22:33:44:33:44 fcid** *fcid* **area**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**fcdomain fcid database** **Example:** `switch(config)# fcdomain fcid database`	FC ID データベース コンフィギュレーション サブモードを開始します。
ステップ 3	**vsan** *vsan-id* **wwn 33:e8:00:05:30:00:16:df fcid** *fcid* **Example:** `switch(config-fcid-db)# vsan 26 wwn 33:e8:00:05:30:00:16:df fcid 4`	指定の VSAN のデバイス WWN（33:e8:00:05:30:00:16:df）に FC ID 0x070128 を設定します。 **Note** 重複 FC ID の割り当てを回避するには、**show fcdomain address-allocation vsan** コマンドを使用して、使用中の FC ID を表示します。
ステップ 4	**vsan** *vsan-id* **wwn 11:22:11:22:33:44:33:44 fcid** *fcid* **dynamic** **Example:** `switch(config-fcid-db)# vsan 13 wwn 11:22:11:22:33:44:33:44 fcid 6 dynamic`	ダイナミック モードで、指定の VSAN のデバイス WWN（11:22:11:22:33:44:33:44）に FC ID 0x070123 を設定します。
ステップ 5	**vsan** *vsan-id* **wwn 11:22:11:22:33:44:33:44 fcid** *fcid* **area** **Example:** `switch(config-fcid-db)# vsan 88 wwn 11:22:11:22:33:44:33:44 fcid 4 area`	指定の VSAN のデバイス WWN（11:22:11:22:33:44:33:44）に FC ID 0x070100 ～ 0x701FF を設定します。 **Note** この fcdomain のエリア全体を保護するには、FC ID の末尾 2 文字に 00 を割り当てます。

HBA に対する一意のエリア FC ID

Note ここに記載された説明は、ホスト バス アダプタ（HBA）ポートとストレージ ポートが同じスイッチに接続されている場合にのみお読みください。

HBA とストレージ ポートが同じスイッチに接続されている場合は、それぞれのポートに異なるエリア ID を設定しなければならないことがあります。たとえば、ストレージ ポート FC ID が 0x6f7704 の場合、このポートのエリアは 77 です。この場合、HBA ポートのエリアには 77 以外の値を構成できます。HBA ポートの FC ID は、ストレージ ポートの FC ID と異なる値に手動で構成する必要があります。

Cisco SAN スイッチでは、FC ID の永続性機能によってこの要件が満たされます。この機能を使用すると、ストレージ ポートまたは HBA ポートに異なるエリアを持つ FC ID を事前に割り当てることができます。

HBA に対する一意のエリア FC ID の設定

HBA ポートに異なるエリア ID を設定できます。

次のタスクでは、111（16 進値では 6f）のスイッチ ドメインの設定例を使用します。サーバは FCoE を介してスイッチに接続されます。HBA ポートはインターフェイス vfc20 に接続され、ストレージ ポートは同じスイッチのインターフェイス fc2/3 に接続されます。

Procedure

ステップ 1 **show flogi database** コマンドを使用して、HBA のポート WWN（Port Name フィールド）ID を取得します。

```
switch# show flogi database
--------------------------------------------------------------------
INTERFACE VSAN  FCID          PORT NAME               NODE NAME
--------------------------------------------------------------------
 vfc20     3   0x6f7703  50:05:08:b2:00:71:c8:c2   50:05:08:b2:00:71:c8:c0
 vfc23     3   0x6f7704  50:06:0e:80:03:29:61:0f   50:06:0e:80:03:29:61:0f
```

Note
この設定では、両方の FC ID に同じエリア 77 が割り当てられています。

ステップ 2 SAN スイッチの HBA インターフェイスをシャットダウンします。

```
switch# configure terminal
switch(config)# interface vfc 20
switch(config-if)# shutdown
switch(config-if)# end
```

ステップ 3 **show fcdomain vsan** コマンドを使用して、FC ID 機能がイネーブルであることを確認します。

```
switch# show fcdomain vsan 3
...
Local switch configuration information:
        State: Enabled
        FCID persistence: Disabled
```

この機能がディセーブルの場合は、次の手順に進み、永続的 FC ID をイネーブルにします。

この機能がすでにイネーブルの場合は、その後の手順にスキップします。

ステップ 4 SAN スイッチで永続的 FC ID をイネーブルにします。

```
switch# configure terminal
switch(config)# fcdomain fcid persistent vsan 3
switch(config)# end
```

ステップ 5 異なるエリア アロケーションの新しい FC ID を割り当てます。この例では、*77* を *ee* に置き換えます。

```
switch# configure terminal
switch(config)# fcdomain fcid database
switch(config-fcid-db)# vsan 3 wwn 50:05:08:b2:00:71:c8:c2
fcid 0x6fee00 area
```

ステップ 6 SAN スイッチの HBA インターフェイスをイネーブルにします。

```
switch# configure terminal
switch(config)# interface vfc 20
switch(config-if)# no shutdown
switch(config-if)# end
```

ステップ 7 **show flogi database** コマンドを使用して、HBA の pWWN ID を確認します。

```
switch# show flogi database
--------------------------------------------------------------------
INTERFACE VSAN  FCID      PORT NAME                NODE NAME
--------------------------------------------------------------------
 vfc20    3   0x6fee00    50:05:08:b2:00:71:c8:c2   50:05:08:b2:00:71:c8:c0
 vfc23    3   0x6f7704    50:06:0e:80:03:29:61:0f   50:06:0e:80:03:29:61:0f
```

Note
これで、両方の FC ID にそれぞれ異なるエリアが割り当てられました。

固定的 FC ID の選択消去

固定的 FC ID は、選択的に消去できます。現在使用中のスタティック エントリおよび FC ID は、削除できません。次の表に、永続的 FC ID が消去されると削除または保持される FC ID エントリを示します。

Table 19: 消去される *FC ID*

固定的 FC ID の状態	固定的 FC ID の使用状態	アクション
スタティック	利用中	削除されません
スタティック	使用しない	削除されません
ダイナミック	利用中	削除されません
ダイナミック	使用しない	Deleted

永続的 FC ID の消去

永続的 FC ID を消去できます。

SUMMARY STEPS

1. **purge fcdomain fcid vsan** *vsan-id*
2. **purge fcdomain fcid vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**purge fcdomain fcid vsan** *vsan-id* **Example:** `switch# purge fcdomain fcid vsan 667`	指定の VSAN の未使用のダイナミック FC ID をすべて消去します。
ステップ 2	**purge fcdomain fcid vsan** *vsan-id* **Example:** `switch# purge fcdomain fcid vsan 50-100`	指定の VSAN 範囲の未使用のダイナミック FC ID をすべて消去します。

fcdomain 構成の確認

Note fcdomain機能がディセーブルである場合、表示された実行時ファブリック名は設定済みファブリック名と同じです。

次に、fcdomain 設定に関する情報を表示する例を示します。

```
switch# show fcdomain vsan 2
```

指定された VSAN に属するすべてのスイッチのドメイン ID リストを表示するには、**show fcdomain domain-list** コマンドを使用します。このリストには、各ドメイン ID を所有するスイッチの WWN が記載されています。この例では次の値が使用されています。

- 20:01:00:05:30:00:47:df の WWN を持つスイッチが主要スイッチで、ドメインは 200 です。
- 20:01:00:0d:ec:08:60:c1 の WWN を持つスイッチはローカル スイッチ（CLI コマンドを入力してドメイン リストを表示したスイッチ）で、ドメインは 99 です。
- IVR マネージャは 20:01:00:05:30:00:47:df を仮想スイッチの WWN として使用して仮想ドメイン 97 を取得しました。

```
switch# show fcdomain domain-list vsan 76
Number of domains: 3
Domain ID              WWN
---------    -----------------------
0xc8(200)    20:01:00:05:30:00:47:df [Principal]
 0x63(99)    20:01:00:0d:ec:08:60:c1 [Local]
 0x61(97)    50:00:53:0f:ff:f0:10:06 [Virtual (IVR)]
```

このスイッチに設定された許可ドメイン ID のリストを表示するには、**show fcdomain allowed vsan** コマンドを使用します。

```
switch# show fcdomain allowed vsan 1
Assigned or unallowed domain IDs: 1-96,100,111-239.
[Interoperability Mode 1] allowed domain IDs: 97-127.
[User] configured allowed domain IDs: 50-110.
```

このスイッチに interop 1 モードが必要な場合は、要求されたドメイン ID がスイッチ ソフトウェア チェックに合格することを確認してください。

次に、指定の VSAN の既存の永続的 FC ID をすべて表示する例を示します。unused オプションを指定すると、未使用の永続的 FC ID だけを表示できます。

```
switch# show fcdomain fcid persistent vsan 1000
```

次に、指定の VSAN または SAN ポート チャネルのフレームおよびその他の fcdomain 統計情報を表示する例を示します。

```
switch# show fcdomain statistics vsan 1
VSAN Statistics
Number of Principal Switch Selections: 0
Number of times Local Switch was Principal: 0
Number of non disruptive reconfigurations: 0
Number of disruptive reconfigurations: 0
```

次に、割り当てられた FC ID および空いている FC ID のリストを含めて、FC ID 割り当てに関する統計情報を表示する例を示します。

```
switch# show fcdomain address-allocation vsan 1
```

次に、有効なアドレス割り当てキャッシュを表示する例を示します。ファブリックから取り除かれたデバイス（ディスクやホスト）を元のファブリックに戻す場合、主要スイッチはキャッシュを使用して FC ID を再度割り当てます。キャッシュ内では、VSAN はこのデバイスを含む VSAN を、WWN は FC ID を所有していたデバイスを、マスクは FC ID に対応する 1 つのエリアまたはエリア全体を表します。

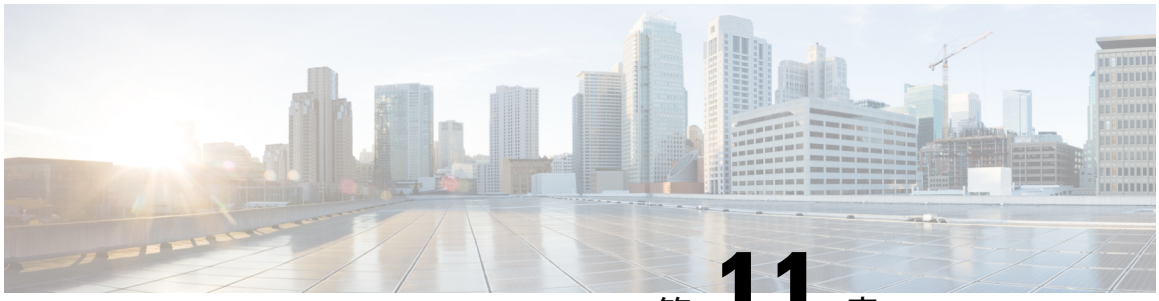
```
switch# show fcdomain address-allocation cache
```

ファイバチャネル ドメインのデフォルト設定

次の表は、すべての fcdomain パラメータのデフォルト設定を示します。

Table 20: デフォルト ***fcdomain*** パラメータ

パラメータ	デフォルト
fcdomain 機能	[有効（Enabled）]
設定済みドメイン ID	0（ゼロ）
設定済みドメイン	優先（Preferred）
auto-reconfigure オプション	ディセーブル
contiguous-allocation オプション	ディセーブル
プライオリティ	128
許可リスト	1 ～ 239
ファブリック名	20:01:00:05:30:00:28:df
rcf-reject	ディセーブル
固定的 FC ID	[有効（Enabled）]
許可ドメイン ID リスト設定の配信	無効化



第 11 章

FCoE の VLAN および仮想インターフェイスの設定

この章は、次の内容で構成されています。

仮想インターフェイスの概要

Cisco Nexus デバイスでは、Fibre Channel over Ethernet（FCoE）がサポートされています。これにより、スイッチとサーバーの間の同じ物理イーサネット接続上でファイバ チャネルおよびイーサネット トラフィックを伝送できます。

FCoE のファイバ チャネル部分は、仮想ファイバ チャネル インターフェイスとして設定されます。論理ファイバ チャネル機能（インターフェイス モードなど）は、仮想ファイバ チャネル インターフェイスで設定できます。

仮想ファイバ チャネル インターフェイスは、いずれかのインターフェイスにバインドしたうえで使用する必要があります。バインド先は、コンバージド ネットワーク アダプタ（CNA）が Cisco Nexus デバイスに直接接続されている場合は物理イーサネット インターフェイス、CNA がレイヤ 2 ブリッジにリモート接続されている場合は MAC アドレス、CNA が 仮想ポートチャネル（vPC）を介してファイバ チャネル フォワーダ（FCF）に接続されている場合は EtherChannel となります。

VE ポート

仮想拡張（VE）ポートは、FCoEネットワークで拡張ポートとして機能します。VEポートは、ネットワーク内の複数のFCoEスイッチを接続できます。VEポートは、物理イーサネットポートまたはポート チャネルにバインドできます。

Cisco Nexus 9000 シリーズ スイッチでは、VE_Port がバインドされるポート チャネルのメンバ間のトラフィックは、SID、DID、および OXID に基づいてロード バランシングされます。

FCoEトラフィックに対し、すべてのリンクがポートチャネルで使用できるように、**port-channel load-balance ethernet** *source-dest-port* コマンドを入力して、ポート チャネルのロードバランシングを「source-dest-port」に設定します。この設定では、「source-destination-oxid」ロードバランシングが FCoE トラフィックに使用されます。

FCoE VLAN および仮想インターフェイスに関する注意事項および制約事項

FCoE VLAN と仮想ファイバ チャネル（vFC)インターフェイスには、以下の注意事項と制約事項があります。

- それぞれの vFC インターフェイスは、FCoE 対応イーサネット インターフェイス、EtherChannel インターフェイス、またはリモート接続されたアダプタの MAC アドレスにバインドする必要があります。FCoE は 10 ギガビット、25 ギガビット 40 ギガビット、および 100 ギガビット イーサネットインターフェイスでサポートされます。
- 仮想ファイバ チャネル インターフェイスは、いずれかのインターフェイスにバインドしたうえで使用する必要があります。バインド先は、物理イーサネット インターフェイス（コンバージド ネットワーク アダプタ（CNA）が Cisco Nexus デバイスに直接接続されている場合）、MACアドレス（CNA がレイヤ2ブリッジにリモート接続されている場合）、または EtherChannel です。
- vFC インターフェイスにバインドするイーサネット インターフェイスまたは EtherChannel インターフェイスを設定する際は、次の点に注意してください。
  - イーサネットまたは EthernetChannel インターフェイスは、トランク ポートにする必要があります（**switchport mode trunk** コマンドを使用します）。
  - vFC の VSAN に対応する FCoE VLAN は、許可 VLAN リストに含まれている必要があります。
  - インターフェイスに MTU 9216 および QoS ポリシーを設定します。デフォルト（サービス ポリシー タイプ qos input default-fcoe-in-policy）またはカスタム QoS ポリシーを使用できます。
  - FCoE VLAN をトランク ポートのネイティブ VLAN として設定しないでください。

Note トランク上のデフォルトの VLAN はネイティブ VLAN です。タグなしフレームはいずれも、ネイティブ VLAN トラフィックとしてトランクを通過します。

- FCoE には FCoE VLAN だけを使用する必要があります。
- デフォルト VLAN の VLAN1 を FCoE VLAN として使用しないでください。
- イーサネット インターフェイスは、PortFast として設定する必要があります（**spanning-tree port type edge trunk** コマンドを使用します）。

Note スイッチインターフェイスのトランキングが有効に設定されている場合でも、サーバインターフェイスにトランキングを設定する必要はありません。サーバから送信される FCoE 以外のトラフィックはすべて、ネイティブ VLAN 上を通過します。

- vFC インターフェイスは、FCoE Initialization Protocol（FIP）スヌーピング ブリッジに接続された複数のメンバ ポートを持つイーサネット ポートチャネルにバインドできます。
- 各 vFC インターフェイスは、ただ 1 つの VSAN に対応付けられます。
- vFC インターフェイスに関連付けられた VSAN は、専用の FCoE 対応 VLAN にマッピングする必要があります。
- プライベート VLAN では、FCoE はサポートされません。
- LAN の代替パス用に（同一または別の SAN ファブリックにある）統合アクセス スイッチをイーサネット リンク経由で相互に接続する必要がある場合は、すべての FCoE VLAN をメンバーシップから除外することを、これらのリンクに対して明示的に設定する必要があります。
- SAN-A および SAN-B ファブリックの FCoE に対してはそれぞれ別々の FCoE VLAN を使用する必要があります。
- vPC を介した pre-FIP CNA への FCoE 接続はサポートされていません。
- Nexus 9000 シリーズ スイッチは、vFC バインディングと vEthernet の組み合わせをサポートしていません。feature-set virtualization コマンドを使用して Cisco Adapter Fabric Extender（Adapter-FEX）を構成することはできません。
- ポートチャネルにバインド可能な vFCs の最大数は 48 です。
- ポートチャネルにバインド可能な vFC の最大数は 48（Nexus 6001 の場合は 24）です。

Note 仮想インターフェイスは、管理状態がダウンに設定された状態で作成されます。仮想インターフェイスを動作させるためには、管理状態を明示的に設定する必要があります。

仮想インターフェイスの設定

VSAN から VLAN へのマッピング

SAN 内の VSAN ごとにトラフィックを伝送できるよう、それぞれの統合アクセス スイッチには一意の専用 VLAN を設定する必要があります（VSAN 1 用に VLAN 1002、VSAN 2 用に VLAN 1003 など）。マルチ スパニング ツリーが有効に設定されている場合、FCoE VLAN には別個の MST インスタンスを使用する必要があります。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vlan** *vlan-id*
3. switch(config-vlan)# **fcoe** [**vsan** *vsan-id*]
4. switch(config-vlan)# **exit**
5. (Optional) switch(config)# **show vlan fcoe**
6. (Optional) switch(config-if)# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **vlan** *vlan-id*	VLAN コンフィギュレーション モードを開始します。VLAN 番号の有効範囲は 1 ～ 4,096 です。
ステップ 3	switch(config-vlan)# **fcoe** [**vsan** *vsan-id*]	指定された VLAN で FCoE をイネーブルにします。VSAN 番号を指定しない場合は、対象の VLAN から番号が同じ VSAN へマッピングが作成されます。 対象の VLAN から指定した VSAN へのマッピングを設定します。
ステップ 4	switch(config-vlan)# **exit**	VLAN コンフィギュレーション モードを終了します。Cisco Nexus デバイスで設定されたコマンドを実

	Command or Action	Purpose
		行するには、このモードを終了する必要があります。
ステップ 5	(Optional) switch(config)# **show vlan fcoe**	VLAN の FCoE 設定に関する情報を表示します。
ステップ 6	(Optional) switch(config-if)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

Example

次の例は、VLAN 200 を VSAN 2 にマッピングする方法を示したものです。

```
switch(config)# vlan 200
switch(config-vlan)# fcoe vsan 2
```

仮想ファイバ チャネル インターフェイスの作成

仮想ファイバ チャネル インターフェイスを作成できます。仮想ファイバ チャネル インターフェイスは、いずれかの物理インターフェイスにバインドしたうえで使用する必要があります。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface vfc** *vfc-id*
3. switch(config-if)# **bind** {**interface** {**ethernet** *slot*/*port* | **port-channel** *channel-number*} | **mac-address** *MAC-address*}
4. (Optional) switch(config-if)# **no bind** {**interface** {**ethernet** *slot*/*port* | **port-channel** *channel-number*} | **mac-address** *MAC-address*}
5. (Optional) switch(config)# **no interface vfc** *vfc-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface vfc** *vfc-id*	仮想ファイバ チャネル インターフェイスがまだ存在していない場合、それを作成し、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。

	Command or Action	Purpose
		仮想ファイバ チャネル インターフェイス ID の有効範囲は、1 ～ 8192 です。
ステップ 3	switch(config-if)# **bind** {**interface** {**ethernet** *slot*/*port* | **port-channel** *channel-number*} | **mac-address** *MAC-address*}	指定されたインターフェイスに仮想ファイバチャネル インターフェイスをバインドします。 **Note** これが 10G ブレイクアウト ポートの場合、*slot*/*port* 構文は *QSFP-module*/*port* になります。
ステップ 4	(Optional) switch(config-if)# **no bind** {**interface** {**ethernet** *slot*/*port* | **port-channel** *channel-number*} | **mac-address** *MAC-address*}	指定されたインターフェイスに対する仮想ファイバ チャネル インターフェイスのバインドを解除します。 **Note** これが 10G ブレイクアウト ポートの場合、*slot*/*port* 構文は *QSFP-module*/*port* になります。
ステップ 5	(Optional) switch(config)# **no interface vfc** *vfc-id*	仮想ファイバ チャネル インターフェイスを削除します。

Example

次の例は、イーサネット インターフェイスに仮想ファイバ チャネル インターフェイスをバインドする方法を示したものです。

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

次の例は、Cisco Nexus 2232PP ファブリック エクステンダ（FEX）イーサネット インターフェイスに仮想ファイバチャネルインターフェイスをバインドする方法を示したものです。

```
switch# configure terminal
switch(config)# interface vfc 1001
switch(config-if)# bind interface ethernet 100/1/1
```

次の例は、ポート チャネルに仮想ファイバ チャネル インターフェイスをバインドする方法を示したものです。

```
switch# configure terminal
switch(config)# interface vfc 3
switch(config-if)# bind interface port-channel 1
```

次の例は、Nexus デバイス 2232PP FEX 上の仮想ファイバ チャネル インターフェイスをバインドして vPC を作成する方法を示したものです。

```
switch# configure terminal
switch(config)# interface vfc 1001
switch(config-if)# bind interface ethernet 100/1/1
```

Note FCoE をサポートしていない Cisco Nexus FEX にインターフェイスをバインドしようとすると、エラー メッセージが表示されます。

次の例は、MAC アドレスに仮想ファイバ チャネル インターフェイスをバインドする方法を示したものです。

```
switch# configure terminal
switch(config)# interface vfc 2
switch(config-if)# bind mac-address 00:0a:00:00:00:36
```

次の例は、Cisco Nexus 2232PP FEX の MAC アドレスに仮想ファイバチャネル インターフェイスをバインドする方法を示したものです。

```
switch# configure terminal
switch(config)# interface vfc 1001
switch(config-if)# bind mac-address 00:01:0b:00:00:02
```

次の例は、仮想ファイバ チャネル インターフェイスを削除する方法を示したものです。

```
switch# configure terminal
switch(config)# no interface vfc 4
```

次の例は、イーサネット インターフェイスから仮想ファイバチャネル インターフェイスをバインド解除する方法を示したものです。

```
switch# configure terminal
switch(config)# int vfc17
switch(config-if)# no bind interface ethernet 1/17
switch(config-if)# exit
```

vFC インターフェイスの構成

次の手順は、マルチメンバー ポート チャネルのメンバー ポートへの vPC インターフェイスを設定する方法を示しています。

（注） 4 ポート vPC の設定を解除できるのは、ポート チャネルからメンバー ポートを削除した後だけです。単一のメンバー ポート チャネルでのみ設定を解除できます。

手順の概要

1. マルチメンバー ポート チャネルを作成します。
2. 個々のメンバー ポートをマルチメンバー ポート チャネルに追加します。

3. マルチメンバー ポート チャネルのメンバー ポートに vPC を関連付けます。

手順の詳細

手順

ステップ 1 マルチメンバー ポート チャネルを作成します。

```
switch(config-vlan)#  interface port-channel 500
switch(config-vlan)# [no]fcoe multi-vfc
```

ステップ 2 個々のメンバー ポートをマルチメンバー ポート チャネルに追加します。

```
switch(config-vlan)# interface ethernet 100/1/1
switch(config-vlan)# channel-group 500
switch (config)# interface ethernet 100/1/2
switch(config-if)# channel-group 500
```

ステップ 3 マルチメンバー ポート チャネルのメンバー ポートに vPC を関連付けます。

```
switch(config)#  interface vfc 10011
switch(config-vlan)# bind interface ethernet 100/1/1
switch(config-vlan)#  interface vfc 10012
switch (config)#  bind interface ethernet 100/1/2
```

仮想ファイバ チャネル インターフェイスと VSAN との関連付け

SAN 内の仮想ファブリック（VSAN）ごとにトラフィックを伝送できるよう、それぞれの統合アクセス スイッチには一意の専用 VLAN を設定する必要があります（VSAN 1 用に VLAN 1002、VSAN 2 用に VLAN 1003 など）。MST が有効に設定されている場合、FCoE VLAN には別個の MST インスタンスを使用する必要があります。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **vsan database**
3. switch(config-vsan)# **vsan** *vsan-id* **interface vfc** *vfc-id*
4. （任意） switch(config-vsan)# **no vsan** *vsan-id* **interface vfc** *vfc-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	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)# **vsan database**	VSAN 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-vsan)# **vsan** *vsan-id* **interface vfc** *vfc-id*	VSAN と仮想ファイバ チャネル インターフェイスの関連付けを設定します。 VSAN番号は、仮想ファイバチャネルインターフェイスにバインドされた物理イーサネット インターフェイスの上のVLANにマッピングする必要があります。
ステップ 4	（任意） switch(config-vsan)# **no vsan** *vsan-id* **interface vfc** *vfc-id*	VSAN と仮想ファイバ チャネル インターフェイスの関連付けを解除します。

例

次の例は、仮想ファイバ チャネル インターフェイスを VSAN に関連付ける方法を示したものです。

```
switch# configure terminal
switch(config)# vsan database
switch(config-vsan)# vsan 2 interface vfc 4
```

暗黙的仮想ファイバ チャネル ポート チャネル インターフェイスの作成

仮想ファイバー チャネル（vFC）を構築し、1 つのコマンドを使用してそれをイーサネット インターフェイスまたはポート チャネルに暗黙的にバインドすることができます。このためには、vFC 識別子がイーサネット インターフェイスまたはポート チャネル識別子とマッチする必要があります。イーサネットインターフェイスは、モジュール（スロットまたはポート）インターフェイス（スロット/QSFP-モジュール/ポート）にすることができます。

Note ブレイクアウト ポートに暗黙的な vFC を構築することはできません。

仮想ファイバ チャネル インターフェイスの設定

Before you begin

- FCoE の正しいライセンスがインストールされていることを確認します。
- FCoE がイネーブルになっていることを確認します。

Procedure

ステップ 1 グローバル構成モードを開始します。

switch# **configure terminal**

ステップ 2 vFC を構築します（まだ存在しない場合）。

さらに、*vfc slot/port* は、vFC をイーサネット スロット/ポート インターフェイスにバインドします。vFC スロット/*QSFP* モジュール/ポートは、vFC をブレークアウト インターフェイスにバインドします。

switch(config) # **interface vfc** {id | *slot/port* | *slot/QSFP-module/port* }

ステップ 3 vFC インターフェイスを起動します。

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

ステップ 4 Required: 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。

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

仮想ファイバ チャネル インターフェイスの設定

次の例は、イーサネット インターフェイスに仮想ファイバ チャネル インターフェイスを暗黙的にバインドする方法を示したものです。

```
switch# configure terminal
switch(config)# interface eth1/11
switch(config-if)# switchport mode trunk
switch(config-if)# mtu 9216
switch(config-if)# service-policy type qos input default-fcoe-in-policy
switch(config-if)# no shutdown

switch(config)# interface vfc1/11
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)#

switch(config)# vsan database
switch(config-vsan-db)# vsan 10
switch(config-vsan-db)# exit
switch(config)#

switch(config)# vlan 10
switch(config-vlan)# fcoe vsan 10
switch(config-vlan)# exit
switch(config)#
```

```
switch(config)# vsan database
switch(config-vsan-db)# vsan 10 interface vfc1/11
switch(config-vsan-db)# exit
switch(config)#
switch(config)# show interface vfc1/11
vfc1/11 is trunking (Not all VSANs UP on the trunk)
Bound interface is Ethernet1/11
Hardware is Ethernet
Port WWN is 20:0b:00:de:fb:9d:0e:a0
Admin port mode is F, trunk mode is on
snmp link state traps are enabled
Port mode is TF
Port vsan is 10
Operating Speed is 10 Gbps
Admin Speed is auto
Trunk vsans (admin allowed and active) (1,10)
Trunk vsans (up) (10)
Trunk vsans (isolated) ()
Trunk vsans (initializing) (1)
11 fcoe in packets
1692 fcoe in octets
0 fcoe out packets
0 fcoe out octets
Interface last changed at Mon Dec 16 09:03:33 2019

switch(config)#
```

仮想ファイバ チャネル の設定：ポート チャネル インターフェイス

Procedure

ステップ 1 グローバル構成モードを開始します。

switch# **configure terminal**

ステップ 2 番号に基づいてイーサネット ポート チャネルに暗黙的にバインドする vFC を構築します。

ポート番号の範囲は 1 ～ 4096 です。

switch(config) # **interface vfc-port-channel** *port number*

ステップ 3 vFC ポートを起動します。

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

ステップ 4 Required: 現在のインターフェイス コンフィギュレーション モードを終了します。

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

仮想ファイバ チャネル の設定：ポート チャネル インターフェイス

この例は、イーサネット ポート チャネルに暗黙的にバインドする vFC ポート チャネルを構築する方法を示しています。

```
switch# configure terminal
switch(config)# interface port-channel 10
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# mtu 9216
switch(config-if)# service-policy type qos input default-fcoe-in-policy
switch(config-if)# no shutdown
switch(config-if)# exit

switch(config)# interface eth1/49
switch(config-if)# channel-group 10 force
switch(config-if)# no shutdown
switch(config-if)# exit

switch# configure terminal
switch(config)# interface vfc-port-channel 10
switch(config-if)# no shutdown
switch(config-if)# exit

switch(config)# vlan 10
switch(config-vlan)# fcoe vsan 10
switch(config-vlan)# exit
switch(config)#

switch(config)# vsan database
switch(config-vsan-db)# vsan 10 interface vfc-port-channel 10
switch(config-vsan-db)# exit

switch(config)# show interface vfc-port-channel 10
vfc-po10 is trunking (Not all VSANs UP on the trunk)
Bound interface is port-channel10
Hardware is Ethernet
Port WWN is 25:1b:00:de:fb:9d:0e:a0
Admin port mode is F, trunk mode is on
snmp link state traps are enabled
Port mode is TF
Port vsan is 10
Operating Speed is 40 Gbps
Admin Speed is auto
Trunk vsans (admin allowed and active) (1,10)
Trunk vsans (up) (10)
Trunk vsans (isolated) ()
Trunk vsans (initializing) (1)
11 fcoe in packets
1236 fcoe in octets
0 fcoe out packets
0 fcoe out octets
Interface last changed at Mon Dec 16 08:56:13 2019
```

仮想インターフェイスの確認

仮想インターフェイスに関する設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
switch# **show interface vfc** *vfc-id*	指定されたファイバ チャネル インターフェイスの詳細な設定を表示します。

コマンド	目的
switch# **show interface brief**	すべてのインターフェイスのステータスが表示されます。
switch# **show vlan fcoe**	FCoE VLAN から VSAN へのマッピングを表示します。

次の例は、イーサネット インターフェイスにバインドされた仮想ファイバ チャネル インターフェイスを表示する方法を示したものです。

```
switch# show interface vfc 11

vfc11 is trunking (Not all VSANs UP on the trunk)


Bound interface is Ethernet1/11
Hardware is Ethernet
Port WWN is 20:0a:00:de:fb:9d:0e:df
Admin port mode is F, trunk mode is on
snmp link state traps are enabled
Port mode is TF
Port vsan is 10
Operating Speed is 10 Gbps
Admin Speed is auto
Trunk vsans (admin allowed and active) (1,10)
Trunk vsans (up) (10)
Trunk vsans (isolated) ()
Trunk vsans (initializing) (1)
2 fcoe in packets
152 fcoe in octets
0 fcoe out packets
0 fcoe out octets
Interface last changed at Wed Dec 18 10:36:58 2019
```

次の例は、MACアドレスにバインドされた仮想ファイバチャネル インターフェイスを表示する方法を示したものです。

```
switch# show interface vfc 11


vfc11 is trunking (Not all VSANs UP on the trunk)
Bound MAC is 0090.faf8.7513
Hardware is Ethernet
Port WWN is 20:0a:00:de:fb:9d:0e:df
Admin port mode is F, trunk mode is on
snmp link state traps are enabled
Port mode is TF
Port vsan is 10
Operating Speed is 10 Gbps
Admin Speed is auto
Trunk vsans (admin allowed and active) (1,10)
Trunk vsans (up) (10)
Trunk vsans (isolated) ()
Trunk vsans (initializing) (1)
3 fcoe in packets
228 fcoe in octets
0 fcoe out packets
0 fcoe out octets
Interface last changed at Mon Dec 16 09:09:02 2019
```

次の例は、スイッチ上のすべてのインターフェイスのステータスを表示する方法を示したものです（簡略化のため、出力の一部は省略）。

```
switch# show interface brief

--------------------------------------------------------------------------------
Port VRF Status IP Address Speed MTU
--------------------------------------------------------------------------------
mgmt0 -- up 9.9.9.9 1000 1500
--------------------------------------------------------------------------------
Ethernet VLAN Type Mode Status Reason Speed Port
Interface Ch #
--------------------------------------------------------------------------------
Eth1/1 1 eth trunk up none 100G(D) 1
Eth1/2 1 eth trunk up none 100G(D) 1
Eth1/3 -- eth routed down Administratively down auto(D) --
Eth1/4 -- eth routed down XCVR not inserted auto(D) --
Eth1/5 -- eth routed down Administratively down auto(D) --
Eth1/6 -- eth routed down Administratively down auto(D) --
Eth1/7 1 eth trunk up none 40G(D) 601
Eth1/8 -- eth routed down XCVR not inserted auto(D) --
Eth1/14 -- eth routed down XCVR not inserted auto(D) --
Eth1/16 -- eth routed down XCVR not inserted auto(D) --
Eth1/17 -- eth routed down XCVR not inserted auto(D) --
Eth1/18/1 1 eth trunk up none 10G(D) 181
Eth1/18/2 1 eth trunk up none 10G(D) 560
Eth1/18/3 1 eth trunk up none 10G(D) 560
Eth1/18/4 1 eth trunk up none 10G(D) 560
Eth1/19 -- eth routed down Administratively down auto(D) --
Eth1/20 -- eth routed down Administratively down auto(D) --
Eth1/21 -- eth routed down XCVR not inserted auto(D) --
Eth1/22 -- eth routed down XCVR not inserted auto(D) --
Eth1/23 -- eth routed down XCVR not inserted auto(D) --
Eth1/24 -- eth routed down XCVR not inserted auto(D) --
Eth1/25 1 eth trunk up none 100G(D) 2500
Eth1/26 1 eth trunk up none 40G(D) 26
Eth1/27 -- eth routed down XCVR not inserted auto(D) --
Eth1/28 -- eth routed down XCVR not inserted auto(D) --
Eth1/29 -- eth routed down XCVR not inserted auto(D) --
Eth1/31 1 eth trunk up none 40G(D) 559
Eth1/32 -- eth routed down XCVR not inserted auto(D) --
Eth1/33 -- eth routed down XCVR not inserted auto(D) --
Eth1/34 -- eth routed down XCVR not inserted auto(D) --
Eth1/35 -- eth routed down Administratively down auto(D) --
Eth1/36/1 -- eth routed down Administratively down auto(D) --
Eth1/36/2 -- eth routed down Administratively down auto(D) --
Eth1/36/3 -- eth routed down Administratively down auto(D) --
Eth1/36/4 -- eth routed down Administratively down auto(D) --

----------------------------------------------------------------------------------------
Port-channel VLAN Type Mode Status Reason Speed Protocol
Interface
----------------------------------------------------------------------------------------
Po1 1 eth trunk up none a-100G(D) lacp
Po26 1 eth trunk up none a-40G(D) none
Po181 1 eth trunk up none a-10G(D) none
Po559 1 eth trunk up none a-40G(D) none
Po560 1 eth trunk up none a-10G(D) none
Po601 1 eth trunk up none a-40G(D) none
Po2500 1 eth trunk up none a-100G(D) none

--------------------------------------------------------------------------------
Interface Vsan Admin Admin Status SFP Oper Oper Port
Mode Trunk Mode Speed Channel
Mode (Gbps)
--------------------------------------------------------------------------------
fc1/9/1 1 E on trunking swl TE 8 224
```

```
fc1/9/2 1 E on trunking swl TE 8 224
fc1/9/3 1 E on trunking swl TE 8 224
fc1/9/4 1 E on trunking swl TE 8 224
fc1/10/1 1 E on trunking swl TE 8 224
fc1/10/2 1 E on trunking swl TE 8 224
fc1/10/3 1 E on trunking swl TE 8 224
fc1/10/4 1 E on trunking swl TE 8 224
fc1/11/1 1 E on trunking swl TE 8 224
fc1/11/2 1 E on trunking swl TE 8 224
fc1/11/3 1 E on trunking swl TE 8 224
fc1/11/4 1 E on trunking swl TE 8 224
fc1/12/1 1 auto on down swl -- -- --
fc1/12/2 1 auto on down swl -- -- --
fc1/12/3 1 auto on down swl -- -- --
fc1/12/4 1 auto on down swl -- -- --
fc1/13/1 1 E on trunking swl TE 8 225
fc1/13/2 1 E on trunking swl TE 8 225
fc1/13/3 1 E on trunking swl TE 8 225
fc1/13/4 1 E on trunking swl TE 8 225
fc1/15/1 501 auto off up swl F 32 --
fc1/15/2 501 F on trunking swl TF 32 114
fc1/15/3 501 F off up swl F 32 --
fc1/15/4 1 F on trunking swl TF 32 118
fc1/30/1 1 E off notConnected swl -- -- --
fc1/30/2 1 E off notConnected swl -- -- --
fc1/30/3 1 E on trunking swl TE 32 --
fc1/30/4 1 E on notConnected swl -- -- --

--------------------------------------------------------------------------------
Interface Vsan Admin Status Oper Oper IP
Trunk Mode Speed Address
Mode (Gbps)
--------------------------------------------------------------------------------
san-port-channel114 501 on trunking TF 32 --
san-port-channel118 1 on trunking TF 32 --
san-port-channel224 1 on trunking TE 88 --
san-port-channel225 1 on trunking TE 32 --

--------------------------------------------------------------------------------
Interface Vsan Admin Admin Status Bind Oper Oper
Mode Trunk Info Mode Speed
Mode (Gbps)
--------------------------------------------------------------------------------
vfc1 501 F on trunking Ethernet1/26 TF 40
vfc2 501 F on trunking e02f.6d08.cda9 TF auto
vfc560 1 F on trunking port-channel560 TF 30
vfc1/25 501 F on trunking Ethernet1/25 TF 100

--------------------------------------------------------------------------------
Interface Vsan Admin Admin Status Bind Oper Oper
Mode Trunk Info Mode Speed
Mode (Gbps)
--------------------------------------------------------------------------------
vfc-po559 1 F on trunking port-channel559 TF 40
vfc-po601 501 F on trunking port-channel601 TF 40
```

次の例は、スイッチにおける VLAN と VSAN とのマッピングを表示する方法を示したものです。

```
switch# show vlan fcoe

VLAN      VSAN      Status

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

```
15        15        Operational
20        20        Operational
25        25        Operational
30        30        Non-operational
```

VSAN から VLAN へのマッピングの設定例

次に示すのは、FCoE VLAN および仮想ファイバ チャネル インターフェイスの設定例です。

手順の概要

1. 関連する VLAN を有効にし、その VLAN を VSAN へマッピングします。
2. 物理イーサネット インターフェイス上で VLAN を設定します。
3. 仮想ファイバチャネルインターフェイスを作成し、それを物理イーサネットインターフェイスにバインドします。
4. 仮想ファイバ チャネル インターフェイスを VSAN に関連付けます。
5. （任意）VSAN のメンバーシップ情報を表示します。
6. （任意）仮想ファイバ チャネル インターフェイスに関するインターフェイス情報を表示します。

手順の詳細

手順

ステップ 1 関連する VLAN を有効にし、その VLAN を VSAN へマッピングします。

```
switch(config)# vlan 200
switch(config-vlan)# fcoe vsan 2
switch(config-vlan)# exit
```

ステップ 2 物理イーサネット インターフェイス上で VLAN を設定します。

```
switch(config)# interface eth1/11
switch(config)# spanning-tree port type edge trunk
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1,200
switch(config-if)# mtu 9216
switch(config-if)# service-policy type qos input default-fcoe-in-policy
switch(config-if)# exit
```

ステップ 3 仮想ファイバ チャネル インターフェイスを作成し、それを物理イーサネット インターフェイスにバインドします。

```
switch(config)# interface vfc 11
switch(config-if)# bind interface ethernet 1/4
switch(config-if)# no shutdown
switch(config-if)# exit
```

（注）
デフォルトでは、仮想ファイバ チャネル インターフェイスはすべて VSAN 1 上に存在します。VLAN から VSAN へのマッピングを VSAN 1 以外の VSAN に対して行う場合は、ステップ 4 へ進みます。

ステップ 4 仮想ファイバ チャネル インターフェイスを VSAN に関連付けます。

```
switch(config)# vsan database
switch(config-vsan-db)# vsan 2
switch(config-vsan-db)# vsan 2 interface vfc 11
switch(config-vsan)# exit
```

ステップ 5 （任意）VSAN のメンバーシップ情報を表示します。

```
switch# show vsan 2 membership
vsan 2 interfaces
          vfc 11
```

ステップ 6 （任意）仮想ファイバ チャネル インターフェイスに関するインターフェイス情報を表示します。

```
switch# show interface vfc 11

vfc11 is trunking (Not all VSANs UP on the trunk)
Bound interface is Ethernet1/11
Hardware is Ethernet
Port WWN is 20:0a:00:de:fb:9d:0e:df
Admin port mode is F, trunk mode is on
snmp link state traps are enabled
Port mode is TF
Port vsan is 2
Operating Speed is 10 Gbps
Admin Speed is auto
Trunk vsans (admin allowed and active) (1-2,10)
Trunk vsans (up) (2)
Trunk vsans (isolated) ()
Trunk vsans (initializing) (1,10)
2 fcoe in packets
152 fcoe in octets
0 fcoe out packets
0 fcoe out octets
Interface last changed at Mon Dec 16 09:22:25 2019
```

FCoE over Enhanced vPC

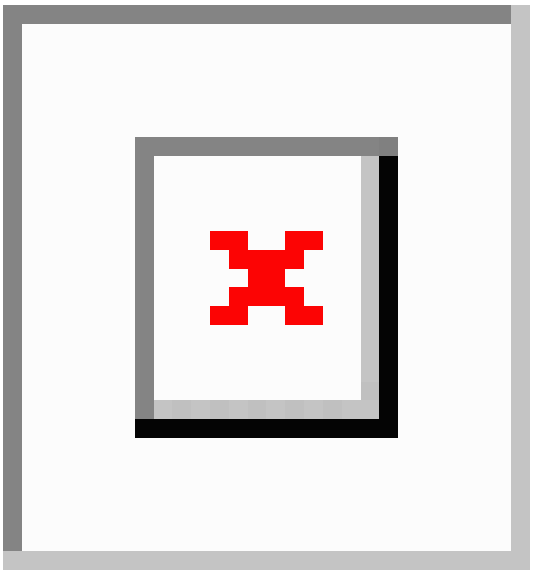
イーサネット トラフィックは、Enhanced vPC トポロジでは FEX とスイッチ ペア間でデュアル ホーム接続されますが、FCoE トラフィックは、SAN 分離を維持するためにシングル ホーム接続される必要があります。したがって、Enhanced vPC が FCoE をサポートする一方で、SAN 分離と高 FCoE 帯域幅が必要な場合は、シングル ホーム接続の FEX トポロジの方が望ましいこともあります。

シングル ホーム接続のトポロジに対する、Enhanced vPC のデメリットを考慮してください。

- 一般的な SAN ネットワークには、SAN A と SAN B という 2 つのファブリックがあり、その間のトラフィックは分離されています。Enhanced vPC トポロジでは、各スイッチは FEX によってペア化されており（シングル ホーム）、1 つの FEX からの FCoE トラフィックが 1 つのスイッチにしか送信されないようになっています。一方、イーサネット トラフィックは、各 FEX と両方のスイッチ間でデュアル ホーム接続されます。FEX からの FCoE トラフィックは 1 つのスイッチにしか送受信されず、イーサネット トラフィックは両方に送受信されるため、FEX アップリンクのトラフィック負荷は均等化されません。
- 8 つのアップリンク ポートを持つ FEX では、イーサネット トラフィックは 8 ポートをすべて使用しますが、シングル ホーム接続の FCoE トラフィックは、このトポロジでは 4 つのポートしか使用しないよう制限されているため、FCoE で使用可能な最大帯域幅も制限されます。さらに、共有リンクのデフォルトの QoS テンプレートは、FCoE トラフィックに対してリンク帯域幅の半分しか割り当てず、残りの半分はイーサネット トラフィックに割り当てられるという制限もあります。
- FEX を使用する Enhanced vPC トポロジでは、ホスト vPC は 2 ポートに制限されており、FEX あたり 1 ポートずつ使用します。

次の図は、それぞれ異なる Cisco Nexus デバイスに関連付けられた、2 つの Cisco Nexus 2000 FEX を使用するシステムの FCoE トラフィック フローを示します。

図 *21 : FCoE over Enhanced vPC*



FCoE over Enhanced vPC の設定

SAN 分離を維持するため、FCoE トラフィックはシングル ホーム接続される必要があります。まず、FEX を 1 つのスイッチと関連付けます。FEX とスイッチが関連付けられると、仮想ファイバ チャネル（vFC）インターフェイスを作成し、ポートにバインドします。

最初のピアで FEX とスイッチをペアリングすると、SAN トラフィックを分離できるよう別のポート番号を使用して 2 番目のピアでも同じ設定を繰り返します。設定が異なっても、整合性エラーが発生することはありません。これは、Enhanced vPC 設定の FCoE の部分は、vPC 整合性チェックの対象となっていないためです。

始める前に

FCoE over Enhanced vPC （206 ページ）の制限事項を確認してください。

手順の概要

1. switch# **configure terminal**
2. switch(config) # **fex** *fex-chassis_ID*
3. switch(config-fex) # **fcoe**
4. switch(config-fex) # **interface vfc** *vfc-id*
5. switch(config-if) # **bind interface ethernet** [*fex-chassis-ID*/]*slot*/*port*
6. switch(config-if) # **no shutdown**
7. （任意） switch(config-if) # **end**
8. （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) # **fex** *fex-chassis_ID*	指定された FEX のコンフィギュレーション モードを開始します。 *fex-chassis_ID* の範囲は 100 ～ 199 です。
ステップ 3	switch(config-fex) # **fcoe**	このスイッチにのみ FCoE トラフィックを送信するよう、FEX を設定します。
ステップ 4	switch(config-fex) # **interface vfc** *vfc-id*	仮想ファイバ チャネル インタフェースのコンフィギュレーション モードを開始します。インターフェイスが存在しない場合は、このコマンドにより、インターフェイスが作成されます。 *vfc-id* の範囲は、1 ～ 8192 です。
ステップ 5	switch(config-if) # **bind interface ethernet** [*fex-chassis-ID*/]*slot*/*port*	vFC インターフェイスを指定された物理イーサネット インターフェイスにバインドします。 *fex-chassis_ID* の範囲は 100 ～ 199 です。*slot* は 1 にする必要があります。FCoE では、*port* の範囲は 1 ～ 32 です。 （注） これが 10G ブレイクアウト ポートの場合、*slot*/*port* 構文は *QSFP-module*/*port* になります。
ステップ 6	switch(config-if) # **no shutdown**	インターフェイスを、デフォルトの操作状態に戻します。
ステップ 7	（任意） switch(config-if) # **end**	特権 EXEC モードに戻ります。
ステップ 8	（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

この例では、各 FEX を FCoE トラフィックのスイッチにペアリングする方法を示します。

```
nexus5000-sanA# configure terminal
nexus5000-sanA(config) # fex 101
nexus5000-sanA(config-fex) # fcoe
nexus5000-sanA(config-fex) # interface vfc 1
nexus5000-sanA(config-if) # bind interface ethernet 101/1/1
nexus5000-sanA(config-if) # no shutdown
nexus5000-sanA(config-if) # end
nexus5000-sanA# copy running-config startup-config
nexus5000-sanA#

nexus5000-sanB# configure terminal
nexus5000-sanB(config) # fex 102
nexus5000-sanB(config-fex) # fcoe
nexus5000-sanB(config-fex) # interface vfc 1
nexus5000-sanB(config-if) # bind interface ethernet 102/1/1
nexus5000-sanB(config-if) # no shutdown
nexus5000-sanB(config-if) # end
nexus5000-sanB# copy running-config startup-config
nexus5000-sanB#


nexus5500-sanA# configure terminal
nexus5500-sanA(config) # fex 101
nexus5500-sanA(config-fex) # fcoe
nexus5500-sanA(config-fex) # interface vfc 1
nexus5500-sanA(config-if) # bind interface ethernet 101/1/1
nexus5500-sanA(config-if) # no shutdown
nexus5500-sanA(config-if) # end
nexus5500-sanA# copy running-config startup-config
nexus5500-sanA#

nexus5500-sanB# configure terminal
nexus5500-sanB(config) # fex 102
nexus5500-sanB(config-fex) # fcoe
nexus5500-sanB(config-fex) # interface vfc 1
nexus5500-sanB(config-if) # bind interface ethernet 102/1/1
nexus5500-sanB(config-if) # no shutdown
nexus5500-sanB(config-if) # end
nexus5500-sanB# copy running-config startup-config
nexus5500-sanB#


nexus6000-sanA# configure terminal
nexus6000-sanA(config) # fex 101
nexus6000-sanA(config-fex) # fcoe
nexus6000-sanA(config-fex) # interface vfc 1
nexus6000-sanA(config-if) # bind interface ethernet 101/1/1
nexus6000-sanA(config-if) # no shutdown
nexus6000-sanA(config-if) # end
nexus6000-sanA# copy running-config startup-config
nexus6000-sanA#

nexus6000-sanB# configure terminal
nexus6000-sanB(config) # fex 102
nexus6000-sanB(config-fex) # fcoe
nexus6000-sanB(config-fex) # interface vfc 1
nexus6000-sanB(config-if) # bind interface ethernet 102/1/1
nexus6000-sanB(config-if) # no shutdown
nexus6000-sanB(config-if) # end
nexus6000-sanB# copy running-config startup-config
nexus6000-sanB#
```

vPC による SAN ブート

1 つの VFC インターフェイスが vPC メンバーにバインドされている場合、Cisco Nexus シリーズ スイッチは SAN ブートを使用できます。複数のインターフェイスを複数のメンバにバインドすることはできません。

- vPC に割り当てられたポートを含む FEX が Nexus スイッチに関連付けられていること。
- vPC メンバには、1 つの VFC インターフェイスしかバインドされていないこと。複数のインターフェイスを複数のメンバにバインドすることはできません。

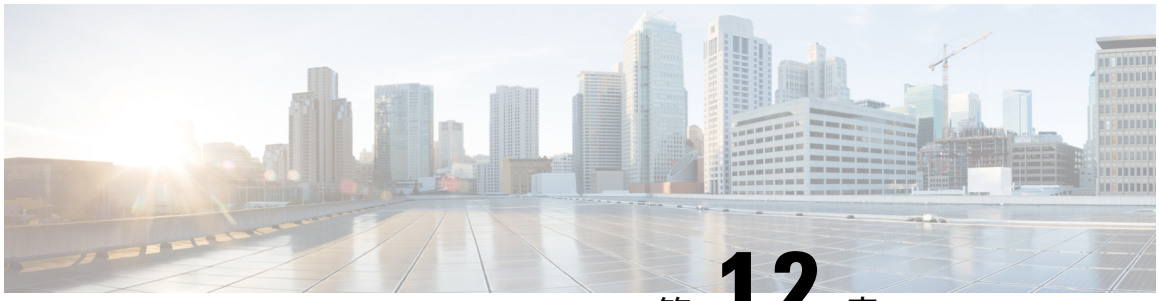
（注） 以前のすべての設定、および対応トポロジとの下位互換性を確保するには、Enhanced vPC を使用しないストレート-スルー FEX トポロジで FEX を設定する必要があります。

vPC による SAN ブートの設定例

この例では、仮想ファイバ チャネル インターフェイス 1 はファブリック A の物理イーサネット インターフェイス 101/1/1 、およびファブリック B のインターフェイス 102/1/1 にバインドされています。インターフェイスはまた、両方のファブリックの仮想ポート チャネル 1 にも関連付けられています。

```
nexus5000-sanA(config) # interface vfc 1
nexus5000-sanA(config-if) # bind interface eth 101/1/1
nexus5000-sanA(config) # interface eth 101/1/1
nexus5000-sanA(config-if) # channel-group 1 mode active
nexus5000-sanA(config-if) # interface port-channel 1
nexus5000-sanA(config-if) # vpc 1
nexus5000-sanA(config-if) #

nexus5000-sanB(config) # interface vfc 1
nexus5000-sanB(config-if) # bind interface eth 102/1/1
nexus5000-sanB(config) # interface eth 102/1/1
nexus5000-sanB(config-if) # channel-group 1 mode active
nexus5000-sanB(config-if) # interface port-channel 1
nexus5000-sanB(config-if) # vpc 1
nexus5000-sanB(config-if) #

nexus5500-sanA(config) # interface vfc 1
nexus5500-sanA(config-if) # bind interface eth 101/1/1
nexus5500-sanA(config) # interface eth 101/1/1
nexus5500-sanA(config-if) # channel-group 1 mode active
nexus5500-sanA(config-if) # interface port-channel 1
nexus5500-sanA(config-if) # vpc 1
nexus5500-sanA(config-if) #

nexus5500-sanB(config) # interface vfc 1
nexus5500-sanB(config-if) # bind interface eth 102/1/1
nexus5500-sanB(config) # interface eth 102/1/1
nexus5500-sanB(config-if) # channel-group 1 mode active
nexus5500-sanB(config-if) # interface port-channel 1
```

```
nexus5500-sanB(config-if) # vpc 1
nexus5500-sanB(config-if) #

nexus5600-sanA(config) # interface vfc 1
nexus5600-sanA(config-if) # bind interface eth 101/1/1
nexus5600-sanA(config) # interface eth 101/1/1
nexus5600-sanA(config-if) # channel-group 1 mode active
nexus5600-sanA(config-if) # interface port-channel 1
nexus5600-sanA(config-if) # vpc 1
nexus5600-sanA(config-if) #

nexus5600-sanB(config) # interface vfc 1
nexus5600-sanB(config-if) # bind interface eth 102/1/1
nexus5600-sanB(config) # interface eth 102/1/1
nexus5600-sanB(config-if) # channel-group 1 mode active
nexus5600-sanB(config-if) # interface port-channel 1
nexus5600-sanB(config-if) # vpc 1
nexus5600-sanB(config-if) #

nexus6000-sanA(config) # interface vfc 1
nexus6000-sanA(config-if) # bind interface eth 101/1/1
nexus6000-sanA(config) # interface eth 101/1/1
nexus6000-sanA(config-if) # channel-group 1 mode active
nexus6000-sanA(config-if) # interface port-channel 1
nexus6000-sanA(config-if) # vpc 1
nexus6000-sanA(config-if) #

nexus6000-sanB(config) # interface vfc 1
nexus6000-sanB(config-if) # bind interface eth 102/1/1
nexus6000-sanB(config) # interface eth 102/1/1
nexus6000-sanB(config-if) # channel-group 1 mode active
nexus6000-sanB(config-if) # interface port-channel 1
nexus6000-sanB(config-if) # vpc 1
nexus6000-sanB(config-if) #
```



第 12 章

FLOGI、ネームサーバー、およびRSCNデータベースの管理

この章では、FLOGI、ネーム サーバー、および RSCN データベースの設定と管理方法について説明します。

この章は、次の項で構成されています。

FLOGI、ネームサーバー、およびRSCNデータベースの管理

ファブリック ログイン

ファイバチャネルファブリックでは、ホストまたはディスクごとにFCIDが必要です。FLOGI テーブルにストレージ デバイスが表示されるどうかを確認するには、次の例のように **show flogi** コマンドを使用します。必要なデバイスが FLOGI テーブルに表示されていれば、FLOGI が正常に行われます。ホスト Host Bus Adapter（HBA）および接続ポートに直接接続されているスイッチ上の FLOGI データベースを検査します。ポートあたりの FLOGI または FDISC の最大数は 256 で、スイッチあたりの FLOGI または FDISC の最大数は 1000 です。

次に、FLOGI テーブルのストレージ デバイスを確認する例を示します。

```
switch# show flogi database
--------------------------------------------------------------------------------
INTERFACE  VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
vfc23      1     0xb200e2  21:00:00:04:cf:27:25:2c  20:00:00:04:cf:27:25:2c
vfc23      1     0xb200e1  21:00:00:04:cf:4c:18:61  20:00:00:04:cf:4c:18:61
vfc23      1     0xb200d1  21:00:00:04:cf:4c:18:64  20:00:00:04:cf:4c:18:64
vfc23      1     0xb200ce  21:00:00:04:cf:4c:16:fb  20:00:00:04:cf:4c:16:fb
vfc23      1     0xb200cd  21:00:00:04:cf:4c:18:f7  20:00:00:04:cf:4c:18:f7
vfc31     2     0xb30100  10:00:00:05:30:00:49:63  20:00:00:05:30:00:49:5e
Total number of flogi = 6.
```

次に、特定のインターフェイスに接続されたストレージ デバイスを確認する例を示します。

```
switch# show flogi database interface vfc1/1

INTERFACE  VSAN    FCID           PORT NAME               NODE NAME

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

vfc1/1     1     0x870000  20:00:00:1b:21:06:58:bc  10:00:00:1b:21:06:58:bc

Total number of flogi = 1.
```

次に、VSAN（仮想 SAN）1 に関連付けられたストレージ デバイスを確認する例を示します。

```
switch# show flogi database vsan 1

show flogi database vsan 1
--------------------------------------------------------------------------------
INTERFACE VSAN FCID PORT NAME NODE NAME
--------------------------------------------------------------------------------
fc1/17 1 0xee0000 21:00:00:24:ff:17:08:2e 20:00:00:24:ff:17:08:2e
fc1/18 1 0xee0020 10:00:00:90:fa:dc:0f:08 20:00:00:90:fa:dc:0f:08
fc1/37 1 0xee00ef 50:06:01:6a:08:60:7c:67 50:06:01:60:88:60:7c:67
Total number of flogi = 3.
```

ネーム サーバー プロキシ

ネーム サーバー機能は、各 VSAN 内のすべてのホストおよびストレージ デバイスの属性を含むデータベースを維持します。ネーム サーバーでは、情報を最初に登録したデバイスによるデータベース エントリの変更が認められます。

プロキシ機能は、別のデバイスによって登録されたデータベースエントリの内容を変更（更新または削除）する必要がある場合に役立ちます。

ネーム サーバ登録要求はすべて、パラメータが登録または変更されたポートと同じポートから発信されます。同一ポートから送られない場合、要求は拒否されます。

この許可を使用すると、WWN が他のノードに代わって特定のパラメータを登録できるようになります。

ネーム サーバ プロキシの登録について

ネーム サーバ登録要求はすべて、パラメータが登録または変更されたポートと同じポートから発信されます。同一ポートから送られない場合、要求は拒否されます。

この許可を使用すると、WWN が他のノードに代わって特定のパラメータを登録できるようになります。

ネーム サーバー プロキシの登録

ネーム サーバー プロキシを登録できます。

SUMMARY STEPS

1. **configure terminal**
2. **fcns proxy-port** *wwn-id* **vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**fcns proxy-port** *wwn-id* **vsan** *vsan-id* **Example:** `switch(config)# fcns proxy-port 11:22:11:22:33:44:33:44 vsan 300`	指定した VSAN のプロキシ ポートを設定します。

重複 pWWN の拒否

FC 標準では、NX-OS は同一スイッチ、同一 VSAN、および同一 FC ドメインですでにログインしている pWWN の任意のインターフェイスでのログインを受け入れます。同じ pWWN が、異なるインターフェイスで同じスイッチにログインしないようにするには、ポート セキュリティ機能を使用します。

デフォルトでは、同一 VSAN の異なるスイッチでの（重複する pWWN による）今後の FLOGI はすべて拒否され、以前の FLOGI が維持されます。これは FC 標準に準拠していません。

このオプションを無効にすると、以前の FCNS エントリを削除することで、同一 VSAN の異なるスイッチでの（重複する pWWN による）今後の FLOGI はすべて許可されます。

重複 pWWN の拒否

FC 標準では、NX-OS は同一スイッチ、同一 VSAN、および同一 FC ドメインですでにログインしている pWWN の任意のインターフェイスでのログインを受け入れます。同じ pWWN が、異なるインターフェイスで同じスイッチにログインしないようにするには、ポート セキュリティ機能を使用します。

デフォルトでは、同一 VSAN の異なるスイッチでの（重複する pWWN による）今後の FLOGI はすべて拒否され、以前の FLOGI が維持されます。これは FC 標準に準拠していません。

このオプションを無効にすると、以前の FCNS エントリを削除することで、同一 VSAN の異なるスイッチでの（重複する pWWN による）今後の FLOGI はすべて許可されます。

重複 pWWN を拒否するには、次の手順を実行します。

SUMMARY STEPS

1. **configure terminal**
2. **fcns reject-duplicate-pwwn vsan** *vsan-id*
3. **no fcns reject-duplicate-pwwn vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**fcns reject-duplicate-pwwn vsan** *vsan-id* **Example:** `switch(config)# fcns reject-duplicate-pwwn vsan 100`	異なるスイッチでの（重複する pWWN による）今後の FLOGI はすべて拒否され、以前の FLOGI が維持されます（デフォルト）。
ステップ 3	**no fcns reject-duplicate-pwwn vsan** *vsan-id* **Example:** `switch(config)# no fcns reject-duplicate-pwwn vsan 256`	以前の FLOGI エントリを削除することで、異なるスイッチでの（重複する pWWN による）今後の FLOGI はすべて許可されます。 ただし、他のスイッチの FLOGI データベースには以前のエントリがまだ含まれています。

ネーム サーバー データベース エントリ

ネーム サーバーはすべてのホストのネーム エントリを FCNS データベースに保管しています。ネーム サーバーは、Nx ポートが他のホストの属性を取得するために（ネーム サーバーへの）PLOGI を実行するときに、Nx ポートによる属性の登録を許可します。Nx ポートが明示的または暗黙的にログアウトする時点で、これらの属性は登録解除されます。

マルチスイッチ ファブリック構成では、各スイッチ上で稼働するネーム サーバー インスタンスが分散型データベースで情報を共有します。スイッチごとに 1 つのネーム サーバー プロセスのインスタンスが実行されます。

ネーム サーバーのデータベース エントリの表示

次に、すべての VSAN のネーム サーバー データベースを表示する例を示します。

```
switch# show fcns database

VSAN 1:
------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
------------------------------------------------------------------------
0xe90000    N     20:00:00:6b:f1:70:08:ec (Cisco)         scsi-fcp:init fc-gs
0xec0020    N     21:00:00:24:ff:7f:37:05 (Company A)     scsi-fcp:target
0xec0040    N     50:08:01:60:01:59:49:33                 scsi-fcp:init
0xec0060    N     20:12:00:11:0d:9d:06:00                 scsi-fcp:init
0xec0080    N     50:08:01:60:08:df:19:11                 scsi-fcp:init
0xec00a0    N     20:00:d8:b1:90:41:1d:d1 (Cisco)
0xec00ef    N     50:06:01:61:08:60:7a:ab (Company B)     scsi-fcp:both
0xee0000    N     50:08:01:60:08:df:19:10                 scsi-fcp
0xee0020    N     20:13:00:11:0d:9d:07:00                 scsi-fcp:target
```

```
0xee0040    N     10:00:00:90:fa:d1:ef:12 (Company C)     scsi-fcp:init
0xee0060    N     20:00:00:6b:f1:70:08:ed (Cisco)         scsi-fcp:init fc-gs
0xef0020    N     50:08:01:60:01:59:49:32                 scsi-fcp
0xef0040    N     20:11:00:11:0d:96:e7:00                 scsi-fcp:init

Total number of entries = 13

VSAN 2:
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x5e0020    N     25:6b:28:6f:7f:21:03:f6 (Cisco)         npv
0x5e0040    N     25:6b:e0:0e:da:49:c2:2a (Cisco)         npv
0x5e0080    N     21:ed:00:2a:10:7a:89:1d (Cisco)         npv
0x840000    N     20:0f:2c:d0:2d:50:d3:48 (Cisco)         npv
0x840040    N     25:52:2c:d0:2d:50:d3:48 (Cisco)         npv

Total number of entries = 5
```

次に、指定された VSAN のネーム サーバー データベースおよび統計情報を表示する例を示します。

```
switch# show fcns database vsan 1

VSAN 1:
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0xe90000    N     20:00:00:6b:f1:70:08:ec (Cisco)         scsi-fcp:init fc-gs
0xec0020    N     21:00:00:24:ff:7f:37:05 (Company A)     scsi-fcp:target
0xec0040    N     50:08:01:60:01:59:49:33                 scsi-fcp:init
0xec0060    N     20:12:00:11:0d:9d:06:00                 scsi-fcp:init
0xec0080    N     50:08:01:60:08:df:19:11                 scsi-fcp:init
0xec00a0    N     20:00:d8:b1:90:41:1d:d1 (Cisco)
0xec00ef    N     50:06:01:61:08:60:7a:ab (Company B)     scsi-fcp:both
0xee0000    N     50:08:01:60:08:df:19:10                 scsi-fcp
0xee0020    N     20:13:00:11:0d:9d:07:00                 scsi-fcp:target
0xee0040    N     10:00:00:90:fa:d1:ef:12 (Company C)     scsi-fcp:init
0xee0060    N     20:00:00:6b:f1:70:08:ed (Cisco)         scsi-fcp:init fc-gs
0xef0020    N     50:08:01:60:01:59:49:32                 scsi-fcp
0xef0040    N     20:11:00:11:0d:96:e7:00                 scsi-fcp:init

Total number of entries = 13
```

次に、すべての VSAN のネーム サーバー データベースを表示する例を示します。

```
switch# show fcns database detail

show fcns database detail
------------------------
VSAN:200 FCID:0xee0000
------------------------
port-wwn (vendor) :21:00:00:24:ff:17:08:2e (Qlogic)
node-wwn :20:00:00:24:ff:17:08:2e
class :3
node-ip-addr :0.0.0.0
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features :scsi-fcp:init
symbolic-port-name :
symbolic-node-name :QLE2742 FW:v8.05.44 DVR:v2.1.73.0
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :20:11:00:de:fb:53:a3:a0
hard-addr :0x000000
```

```
permanent-port-wwn (vendor) :21:00:00:24:ff:17:08:2e (Qlogic)
connected interface :fc1/17
switch name (IP address) :sw (192.168.1.1)
------------------------
VSAN:200 FCID:0xee0020
```

次に、すべての VSAN のネーム サーバー データベース統計を表示する例を示します。

```
switch# show fcns statistics
```

```
show fcns statistics
Name server statistics for vsan 1
==================================
registration requests received = 0
deregistration requests received = 0
queries received = 0
queries sent = 0
reject responses sent = 0
RSCNs received = 0
RSCNs sent = 0

Name server statistics for vsan 200
==================================
registration requests received = 18
deregistration requests received = 0
queries received = 78
queries sent = 0
reject responses sent = 0
RSCNs received = 0
RSCNs sent = 8

Name server statistics for vsan 201
==================================
registration requests received = 0
deregistration requests received = 0
queries received = 0
queries sent = 0
reject responses sent = 0
RSCNs received = 0
RSCNs sent = 0

Name server statistics for vsan 202
==================================
registration requests received = 0
deregistration requests received = 0
queries received = 0
queries sent = 0
reject responses sent = 0
RSCNs received = 0
RSCNs sent = 0
```

FDMI

Cisco Nexus N9K-C93180YC-FX、N9K-C93360YC-FX2、および N9K-C9336C-FX2-E スイッチは、FC-GS-4 規格で説明されているように、ファブリック デバイス管理インターフェイス (FDMI) 機能をサポートします。FDMI を使用すると、ファイバ チャネル HBA などのデバイスをインバンド通信によって管理できます。この機能を追加することにより、既存のファイバ チャネル ネーム サーバーおよび管理サーバーの機能を補完します。

FDMI機能を使用すると、独自のホストエージェントをインストールしなくても、スイッチ ソフトウェアによって接続先HBAおよびホスト オペレーティング システムに関する次のような管理情報を抽出できます。

- 製造元、モデル、およびシリアル番号
- ノード名およびノードのシンボリック名
- ハードウェア、ドライバ、およびファームウェアのバージョン
- ホスト オペレーティング システム（OS）の名前およびバージョン番号

FDMI エントリはすべて永続ストレージに保存され、FDMI プロセスを起動した時点で取り出されます。

FDMI の表示

次に、指定された VSAN のすべての HBA の詳細情報を表示する例を示します。

```
switch# show fdmi database detail vsan 1
```

この例では、すべての VSAN の HBA リストを表示します。

```
switch# sh fdmi database
Registered HBA List for VSAN 10
  10:00:00:90:fa:c7:e1:f6
Registered HBA List for VSAN 108
  20:04:00:11:0d:dd:00:00
  20:05:00:11:0d:dd:00:00
```

この例では、特定の VSAN の HBA リストを表示します。

```
switch# sh fdmi database vsan 10
Registered HBA List for VSAN 10
  10:00:00:90:fa:c7:e1:f6
```

この例では、HBA リストのすべての詳細を表示します。

```
switch# sh fdmi database detail
Registered HBA List for VSAN 10
-------------------------------
HBA-ID: 10:00:00:90:fa:c7:e1:f6
-------------------------------
Node Name         :20:00:00:90:fa:c7:e1:f6
Manufacturer      :Emulex Corporation
Serial Num        :FC61659139
Model             :LPe32002-M2
Model Description:Emulex LightPulse LPe32002-M2 2-Port 32Gb Fibre Channel Adapter
Hardware Ver      :0000000c
Driver Ver        :11.4.33.1
ROM Ver           :11.4.204.25
Firmware Ver      :11.4.204.25
OS Name/Ver       :VMware ESXi 6.7.0 Releasebuild-8169922
CT Payload Len    :245760
  Port-id: 10:00:00:90:fa:c7:e1:f6
    Supported FC4 types:1 scsi-fcp fc-gs
    Supported Speed    :8G 16G 32G
    Current Speed      :16G
    Maximum Frame Size :2048
    OS Device Name     :vmhba8
```

```
    Host Name          :localhost
Registered HBA List for VSAN 108
--------------------------------
HBA-ID: 20:04:00:11:0d:dd:00:00
--------------------------------
Node Name        :20:04:00:11:0d:23:b4:00
Manufacturer     :QLogic Corporation
Serial Num       :RFD1743U70327
Model            :QLE2742
Model Description:Cisco QLE2742 Dual Port 32Gb FC to PCIe Gen3 x8 Adapter
Hardware Ver     :BK3210407-43  B
Driver Ver       :8.07.00.34.Trunk-SCST.18-k
ROM Ver          :3.60
Firmware Ver     :8.08.204 (785ad0
  Port-id: 20:04:00:11:0d:dd:00:00
    Supported FC4 types:scsi-fcp 40 fc-av
    Supported Speed    :8G 16G 32G
    Current Speed      :32G
    Maximum Frame Size :2112
    OS Device Name     :qla2xxx:host7
    Host Name          :VirtuaLUN
--------------------------------
HBA-ID: 20:05:00:11:0d:dd:00:00
--------------------------------
Node Name        :20:05:00:11:0d:23:b5:00
Manufacturer     :QLogic Corporation
Serial Num       :RFD1743U70327
Model            :QLE2742
Model Description:Cisco QLE2742 Dual Port 32Gb FC to PCIe Gen3 x8 Adapter
Hardware Ver     :BK3210407-43  B
Driver Ver       :8.07.00.34.Trunk-SCST.18-k
ROM Ver          :3.60
Firmware Ver     :8.08.204 (785ad0
  Port-id: 20:05:00:11:0d:dd:00:00
    Supported FC4 types:scsi-fcp 40 fc-av
    Supported Speed    :8G 16G 32G
    Current Speed      :32G
    Maximum Frame Size :2112
    OS Device Name     :qla2xxx:host8
    Host Name          :VirtuaLUN
```

この例では、特定の VSAN の HBA リストのすべての詳細を表示します。

```
switch# sh fdmi database detail vsan 10
Registered HBA List for VSAN 10
--------------------------------
HBA-ID: 10:00:00:90:fa:c7:e1:f6
--------------------------------
Node Name        :20:00:00:90:fa:c7:e1:f6
Manufacturer     :Emulex Corporation
Serial Num       :FC61659139
Model            :LPe32002-M2
Model Description:Emulex LightPulse LPe32002-M2 2-Port 32Gb Fibre Channel Adapter
Hardware Ver     :0000000c
Driver Ver       :11.4.33.1
ROM Ver          :11.4.204.25
Firmware Ver     :11.4.204.25
OS Name/Ver      :VMware ESXi 6.7.0 Releasebuild-8169922
CT Payload Len   :245760
  Port-id: 10:00:00:90:fa:c7:e1:f6
    Supported FC4 types:1 scsi-fcp fc-gs
    Supported Speed    :8G 16G 32G
    Current Speed      :16G
    Maximum Frame Size :2048
```

```
OS Device Name      :vmhba8
Host Name           :localhost
```

RSCN

Registered State Change Notification（RSCN）は、ファブリック内で行われた変更について各ホストに通知するためのファイバ チャネル サービスです。ホストは、（State Change Registration（SCR）要求によって）ファブリック コントローラに登録することにより、この情報を受信できます。次のいずれかのイベントが発生した場合、適宜通知されます。

- ファブリックへのディスクの加入または脱退
- ネーム サーバの登録変更
- 新しいゾーンの実施
- IP アドレスの変更
- ホストの動作に影響する、その他の同様なイベント

スイッチ RSCN（SW-RSCN）は、登録されたホストおよびファブリック内の到達可能なすべてのスイッチに送信されます。

Note スイッチはRSCNを送信して、登録済みのノードに変更が発生したことを通知します。ネームサーバーに再度クエリーを発行して新しい情報を取得するのは、各ノードの責任範囲です。スイッチが各ノードに送信する RSCN には、変更に関する詳細情報は含まれていません。

RSCN 情報の概要

スイッチ RSCN（SW-RSCN）は、登録されたホストおよびファブリック内の到達可能なすべてのスイッチに送信されます。

Note スイッチはRSCNを送信して、登録済みのノードに変更が発生したことを通知します。ネームサーバーに再度クエリーを発行して新しい情報を取得するのは、各ノードの責任範囲です。スイッチが各ノードに送信する RSCN には、変更に関する詳細情報は含まれていません。

RSCN 情報の表示

次に、登録済みデバイス情報を表示する例を示します。

```
switch# show rscn scr-table vsan 1

show rscn scr-table vsan 1
SCR table for VSAN: 1
---------------------------------------------
FC-ID REGISTERED FOR
---------------------------------------------
0xee0000 fabric and nport detected rscns
```

```
0xee0020 fabric and nport detected rscns
0xee00ef fabric and nport detected rscns

Total number of entries = 3
```

Note SCR テーブルは設定不可能です。ホストが RSCN 情報と一緒に SCR フレームを送信する場合にかぎり、入力されます。ホストが RSCN 情報を受信しない場合、**show rscn scr-table** コマンドはエントリを返しません。

multi-pid オプション

RSCN の multi-pid オプションがイネーブルな場合、登録済みの Nx ポートに対して生成された RSCN には、関連ポート ID を複数格納できます。この場合、ゾーン分割ルールを適用してから、影響を受けた複数のポート ID が 1 つの RSCN にまとめられます。このオプションをイネーブルにすることによって、RSCN の数を減らすことができます。たとえば、スイッチ 1 に 2 つのディスク（D1、D2）および 1 台のホスト（H）が接続されていると仮定します。ホスト H は、RSCN を受信するように登録済みです。D1、D2、および H は、同じゾーンに属しています。ディスク D1 および D2 が同時にオンラインである場合、次のどちらかの処理が適用されます。

- スイッチ 1 で multi-pid オプションがディセーブルになります。ホスト H に対して 2 つの RSCN が生成されます（1 つはディスク D1 用、もう 1 つはディスク D2 用）。
- スイッチ 1 で multi-pid オプションがイネーブルになります。ホスト H に対して RSCN が 1 つ生成され、RSCN ペイロードによって関連ポート ID がリストされます（この場合は D1 および D2）。

Note Nx ポートには、multi-pid RSCN ペイロードをサポートしないものがあります。その場合は、RSCN の multi-pid オプションをディセーブルにしてください。

Note PORT_OFFLINE イベントの場合、multi-pid オプションが有効か無効かに関係なく、複数の RSCN が生成され (ポートの数に応じて)、すぐに送信されます。

PORT_ONLINEイベントの場合、

- multi-pid オプションが有効になっていると、ポートの数に関係なく単一の RSCN が生成され、すぐに送信されます。この RSCN には、起動するすべてのポートに関する情報を含む複数のページが含まれています。
- multi-pid オプションが無効になっている場合、（ポートの数に応じて）複数の RSCN が生成され、すぐに送信されます。

multi-pid オプションの設定

multi-pid オプションを設定できます。

SUMMARY STEPS

1. **configure terminal**
2. **rscn multi-pid vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**rscn multi-pid vsan** *vsan-id* **Example:** `switch(config)# rscn multi-pid vsan 405`	指定された VSAN の RSCN を multi-pid フォーマットで送信します。

ドメイン フォーマット SW-RSCN の抑制

ドメイン フォーマット SW-RSCN は、ローカル スイッチ名またはローカル スイッチ管理 IP アドレスが変更されるとすぐに送信されます。この SW-RSCN は、ISL を介して、他のすべてのドメインおよびスイッチに送信されます。リモート スイッチから、ドメイン フォーマット SW-RSCN を開始したスイッチに対して GMAL コマンドおよび GIELN コマンドを発行すると、変更内容を判別できます。ドメイン フォーマット SW-RSCN によって、一部の他社製の SAN スイッチで問題が発生することがあります。

これらの SW-RSCN の ISL を介した送信を抑制できます。

SUMMARY STEPS

1. **configure terminal**
2. **rscn suppress domain-swrscn vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:**	グローバル コンフィギュレーション モードを開始します。

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	
ステップ 2	**rscn suppress domain-swrscn vsan** *vsan-id* **Example:** `switch(config)# rscn suppress domain-swrscn vsan 250`	指定された VSAN のドメイン フォーマット SW-RSCN の送信を抑制します。

結合 SW-RSCN

Cisco Nexus 9000 スイッチでのファイバ チャネル プロトコルのパフォーマンス向上のため、SW-RSCN は遅延され、収集され、1 つの結合 SW-RSCN として単一ファイバ チャネル交換でファブリック内のすべてのスイッチに送信されます。

結合 SW RSCN の有効化

結合 SW-RSCN を有効にするには、次の手順を実行します。

始める前に

- ファブリック内のすべてのスイッチが Cisco NX-OS 10.4(2)F 以降を実行している必要があります。
- この機能には、Cisco 以外のスイッチとの相互運用性はありません。

手順の概要

1. **configure terminal**
2. **rscn coalesce swrscn vsan** *vsan-id*
3. **rscn coalesce swrscn vsan** *vsan-id* **delay** *time*

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	**rscn coalesce swrscn vsan** *vsan-id* 例： `switch(config)# rscn coalesce swrscn vsan 1`	VSAN 1 の Switch Registered State Change Notification（SWRSCN）の結合を有効にします。デフォルト遅延は 500 ミリ秒です。

	コマンドまたはアクション	目的
ステップ 3	**rscn coalesce swrscn vsan** *vsan-id* **delay** *time* 例： `switch(config)# rscn coalesce swrscn vsan 1 delay 800`	VSAN 1 の Switch Registered State Change Notification（SWRSCN）の結合を有効にします。SW-RSCN を最大で 800 ミリ秒遅延します。 （注） Cisco NX-OS 10.4(2)F 以降が稼働しているすべてのスイッチでは、デフォルトで結合 SW-RSCN を処理できますが、結合 SW-RSCN の送信は CLI で有効にした後でのみ可能です。

結合 SW-RSCN の無効化

結合 SW-RSCN を無効にするには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **no rscn coalesce swrscn vsan** *vsan-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。
ステップ 2	**no rscn coalesce swrscn vsan** *vsan-id* 例： `switch(config)# no rscn coalesce swrscn vsan 1`	VSAN 1 の Switch Registered State Change Notification（SWRSCN）の結合を無効にします。

RSCN 統計情報のクリア

カウンタをクリアしたあとに、それらのカウンタを別のイベントに関して表示することができます。たとえば、特定のイベント（ONLINE または OFFLINE イベントなど）で生成された RSCN または SW-RSCN の個数を追跡できます。このような統計情報を利用して、VSAN 内で発生する各イベントへの応答を監視できます。

次に、指定された VSAN の RSCN 統計情報をクリアする例を示します。

```
switch# clear rscn statistics vsan 1
```

RSCN 統計情報をクリアした後、**show rscn statistics** コマンドを使用してクリアされたカウンタを表示できます。

```
switch# show rscn statistics vsan 1
```

RSCN タイマーの設定

RSCNは、VSAN単位のイベントリストキューを維持します。RSCNイベントは、生成されると、このキューに入れられます。最初のRSCNイベントがキューに入ると、VSAN単位のタイマーが始動します。タイムアウトになると、すべてのイベントがキューから出され、結合RSCNが登録済みユーザに送信されます。デフォルトのタイマー値の場合に、登録済みユーザーに送信される結合RSCNの数が最小になります。配置によっては、ファブリック内の変更を追跡するために、イベント タイマー値をさらに小さくする必要が生じることがあります。

Note RSCN タイマー値は、VSAN 内のすべてのスイッチで同一にする必要があります。

Note CFS はデフォルトでイネーブルです。ファブリック内のすべてのデバイスで CFS をイネーブルに設定しないと配信は受信されません。アプリケーションに対して CFS がディセーブルになっていると、そのアプリケーションからコンフィギュレーションは配信されず、ファブリック内の他のデバイスからの配信も受け取ることができません。CFS を有効にするには、**cfs distribute** コマンドを使用します。

Note ダウングレードを実行する場合は、事前に、ネットワーク内のRSCNタイマー値をデフォルト値に戻してください。デフォルト値に戻しておかないと、VSANおよびその他のデバイスを経由するリンクがディセーブルになります。

RSCN タイマーを設定できます。

SUMMARY STEPS

1. **configure terminal**
2. **rscn distribute**
3. **rscn event-tov** *timeout* **vsan** *vsan-id*
4. **no rscn event-tov** *timeout* **vsan** *vsan-id*
5. **rscn commit vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**rscn distribute** **Example:** `switch(config)# rscn distribute`	RSCN タイマーの設定の配布をイネーブルにします。
ステップ 3	**rscn event-tov** *timeout* **vsan** *vsan-id* **Example:** `switch(config)# rscn event-tov 1000 vsan 501`	指定した VSAN のイベント タイムアウト値（ミリ秒）を設定します。有効値は 0 ～ 2000 ミリ秒です。値をゼロ（0）に設定すると、タイマーはディセーブルになります。
ステップ 4	**no rscn event-tov** *timeout* **vsan** *vsan-id* **Example:** `switch(config)# no rscn event-tov 1100 vsan 245`	デフォルト値（ファイバ チャネル VSAN の場合、2000 ミリ秒）に戻します。
ステップ 5	**rscn commit vsan** *vsan-id* **Example:** `switch(config)# rscn commit vsan 25`	配布する RSCN タイマー設定を指定された VSAN 内のスイッチにコミットします。

RSCN タイマー設定の確認

RSCN タイマー設定を確認するには、**show rscn event-tov vsan** コマンドを使用します。次に、VSAN 10 の RSCN 統計情報をクリアする例を示します。

```
switch# show rscn event-tov vsan 10
Event TOV : 1000 ms
```

RSCN タイマー設定の配布

各スイッチのタイムアウト値は、手動で設定されるため、異なるスイッチが別々の時間にタイムアウトになると、誤設定が生じます。ネットワーク内の異なる N ポートが別々の時間に RSCN を受信してしまうことがあります。Cisco Fabric Service（CFS）インフラストラクチャでは、RSCN タイマー設定情報をファブリック内のすべてのスイッチに自動的に配布することで、この状況を解消します。また、SW-RSCN の数も削減します。

RSCN は、配布と非配布の 2 つのモードをサポートしています。配布モードでは、RSCN は CFS を使用して、ファブリック内のすべてのスイッチに設定を配布します。非配布モードでは、影響を受けるのはローカル スイッチに対するコンフィギュレーション コマンドだけです。

Note すべてのコンフィギュレーション コマンドが配布されるわけではありません。配布されるのは、**rscn event-tov tov vsan vsan** コマンドだけです。

Caution RSCN タイマー設定だけが配布されます。

RSCN タイマーは、初期化およびスイッチオーバーの実行時に CFS に登録されます。ハイ アベイラビリティを実現するため、RSCN タイマー配布がクラッシュし再起動する場合、またはスイッチオーバーが発生した場合には、クラッシュまたはスイッチオーバーが発生する前の状態から、通常の機能が再開されます。

追加情報については、ご使用のデバイスの『System Management Configuration Guide』の「Using Cisco Fabric Services」を参照してください。

RSCN タイマー設定の配布のイネーブル化

RSCN タイマー設定の配布をイネーブルに設定できます。

SUMMARY STEPS

1. **configure terminal**
2. **rscn distribute**
3. **no rscn distribute**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**rscn distribute** **Example:** `switch(config)# rscn distribute`	RSCN タイマーの設定の配布をイネーブルにします。
ステップ 3	**no rscn distribute** **Example:** `switch(config)# no rscn distribute`	RSCN タイマーの配布をディセーブル（デフォルト）にします。

ファブリックのロック

データベースを変更するときの最初のアクションによって、保留中のデータベースが作成され、VSAN内の機能がロックされます。ファブリックがロックされると、次のような状況になります。

- 他のユーザーがこの機能の設定に変更を加えることができなくなります。
- コンフィギュレーションデータベースのコピーが、最初のアクティブ変更と同時に保留中のデータベースになります。

RSCN タイマー設定の変更のコミット

アクティブデータベースに加えられた変更をコミットする場合、ファブリック内のすべてのスイッチに構成がコミットされます。コミットが正常に行われると、構成の変更がファブリック全体に適用され、ロックが解除されます。

RSCN タイマー設定の変更をコミットできます。

SUMMARY STEPS

1. **configure terminal**
2. **rscn commit vsan** *timeout*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**rscn commit vsan** *timeout* **Example:** `switch(config)# rscn commit vsan 500`	RSCN タイマーの変更をコミットします。

RSCN タイマー設定の変更の廃棄

保留中のデータベースに加えられた変更を廃棄（中断）する場合、コンフィギュレーションデータベースは影響を受けないまま、ロックが解除されます。

RSCN タイマー設定の変更を廃棄できます。

SUMMARY STEPS

1. **configure terminal**
2. **rscn abort vsan** *timeout*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**rscn abort vsan** *timeout* **Example:** `switch(config)# rscn abort vsan 800`	RSCN タイマーの変更を廃棄し、保留中のコンフィギュレーション データベースをクリアします。

ロック済みセッションのクリア

RSCN タイマー設定を変更したが、変更をコミットまたは廃棄してロックを解除するのを忘れた場合、管理者はファブリック内の任意のスイッチからロックを解除できます。管理者がこの操作を行うと、ユーザーによる保留データベースの変更は廃棄され、ファブリックのロックは解除されます。

保留中のデータベースは揮発性ディレクトリでだけ有効で、スイッチが再起動されると廃棄されます。

管理者の特権を使用して、ロックされた RSCN セッションを解除するには、EXECモードで **clear rscn session** コマンドを使用します。次に、VSAN 10 の RSCN セッションをクリアする例を示します。

```
switch# clear rscn session vsan 10
```

RSCN 設定の配布情報の表示

次に、RSCN 設定の配布の登録ステータスを表示する例を示します。

```
switch# show cfs application name rscn
 Enabled        : Yes
 Timeout        : 5s
 Merge Capable  : Yes
 Scope          : Logical
```

Note 結合対象のファブリックの RSCN タイマー値が異なる場合、結合は失敗します。

次に、設定のコミット時に有効な一連のコンフィギュレーション コマンドを表示する例を示します。

Note 保留中のデータベースには、既存設定と変更された設定の両方が含まれます。

```
switch# show rscn pending vsan 1
rscn event-tov 2000 ms vsan 1
rscn event-tov 2000 ms vsan 2
rscn event-tov 300 ms vsan 10
```

次に、保留中の設定とアクティブな設定の違いを表示する例を示します。

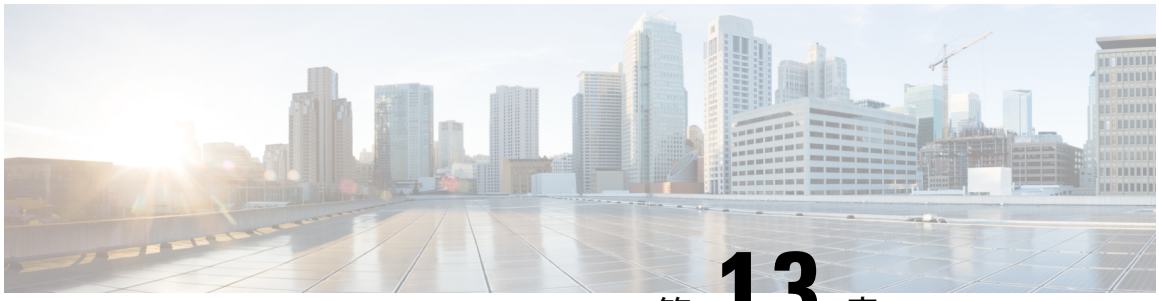
```
switch# show rscn pending-diff vsan 10
- rscn event-tov 2000
+ rscn event-tov 1001
```

RSCN のデフォルト設定

次の表に、RSCN のデフォルト設定を示します。

Table 21: デフォルトの ***RSCN*** 設定値

パラメータ	デフォルト
RSCN タイマー値	2000 ミリ秒（ファイバチャネル VSAN）
RSCN タイマー設定の配布	無効化



第 13 章

DDAS

この章では、デバイス エイリアス サービスの配信方法について説明します。

この章は、次の項で構成されています。

DDAS

Cisco SAN のスイッチは、ファブリック規模単位で配信デバイス エイリアス サービス（デバイス エイリアス）をサポートします。

デバイス エイリアスについての情報

Cisco SAN のスイッチは、ファブリック規模単位で配信デバイス エイリアス サービス（デバイス エイリアス）をサポートします。

Cisco SAN スイッチで（ゾーン分割など）異なる機能を設定するためにデバイスのポート WWN（pWWN）が指定されている必要がある場合、設定を行うたびに適切なデバイス名を割り当てなければなりません。不適切なデバイス名は、予想外の結果を招くことがあります。pWWN にわかりやすい名前を定義し、必要とされるすべてのコンフィギュレーション コマンドでこの名前を使用すれば、こうした問題を回避できます。このようなわかりやすい名前をデバイス エイリアスと呼びます。

デバイス エイリアスの機能

デバイス エイリアスには、次のような特徴があります。

- デバイス エイリアス情報は、VSAN 設定とは無関係です。
- デバイス エイリアス設定および配布は、ゾーン サーバおよびゾーン サーバ データベースとは無関係です。
- データを失うことなく、従来のゾーン エイリアス設定をインポートできます。

- デバイス エイリアス アプリケーションは Cisco Fabric Services（CFS）インフラストラクチャを使用して、効率的なデータベースの管理および配布を実現します。デバイスエイリアスは、協調型配布モードおよびファブリック規模の配布範囲を使用します。
- 基本および拡張および拡張モード。
- ゾーンを設定するために使用されたデバイス エイリアスは、それぞれの pWWN と一緒に、**show** コマンド出力に自動的に表示されます。

追加情報については、ご使用のデバイスの『System Management Configuration Guide』の「Using Cisco Fabric Services」を参照してください。

Related Topics

デバイス エイリアスのモード （236 ページ）

デバイス エイリアスの前提条件

デバイス エイリアスには、次の要件があります。

- デバイス エイリアスを割り当てることができるのは pWWN だけです。
- pWWN とマッピングされるデバイスエイリアスは、1 対 1 の関係である必要があります。
- デバイス エイリアス名には、最大 64 文字の英数字を使用でき、次の文字を 1 つまたは複数加えることができます。
  - a ～ z および A ～ Z
  - デバイス エイリアス名は、先頭の文字が英数字である必要があります（a ～ z または A ～ Z）。
  - 1 ～ 9
  - -（ハイフン）および _（下線）
  - $（ドル記号）および ^（キャレット）記号

ゾーン エイリアスとデバイス エイリアスの比較

次の表で、ゾーン ベースのエイリアス設定とデバイス エイリアス設定の違いを比較します。

Table 22: ゾーン エイリアスとデバイス エイリアスの比較

ゾーン ベースのエイリアス	デバイス エイリアス
エイリアスは指定した VSAN に限定されます。	VSAN 番号を指定せずにデバイス エイリアスを定義できます。また、同一の定義を何の制約もなく 1 つまたは複数の VSAN で使用できます。

ゾーン ベースのエイリアス	デバイス エイリアス
ゾーン エイリアスは、ゾーン分割設定の一部です。他の機能の設定にはエイリアス マッピングを使用できません。	pWWN を使用するすべての機能にデバイス エイリアスを使用できます。
エンド デバイスを指定するのにすべてのゾーン メンバ タイプを使用できます。	pWWN だけがサポートされます。
設定はゾーン サーバ データベース内に含まれ、他の機能では使用できません。	デバイス エイリアスは、ゾーン分割に限定されていません。デバイス エイリアス設定は FCNS、ゾーン、および fcping アプリケーションで使用することができます。

デバイス エイリアス データベース

デバイス エイリアス機能は 2 つのデータベースを使用して、デバイス エイリアス設定を受け入れ、実装します。

- 有効なデータベース：ファブリックが現在使用しているデータベース
- 保留中のデータベース：保留中のデバイス エイリアス設定の変更は保留中のデータベースに保存されます。

デバイス エイリアス設定を変更する場合、変更している間はファブリックがロックされたままの状態なので、変更をコミットまたは廃棄する必要があります。

デバイス エイリアス データベースの変更は、アプリケーションによって検証されます。いずれかのアプリケーションがデバイス エイリアス データベースの変更を受け入れることができない場合、これらの変更は拒否されます。これは、コミットまたは結合の操作によって行われたデバイス エイリアス データベースの変更に適用されます。

デバイス エイリアスの作成

保留データベースにデバイス エイリアスを作成できます。

SUMMARY STEPS

1. **configure terminal**
2. **device-alias database**
3. **device-alias name** *device-name* **pwwn** *pwwn-id*
4. **no device-alias name** *device-name*
5. **device-alias rename** *old-device-name new-device-name*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**device-alias database** **Example:** `switch(config)# device-alias database` `switch(config-device-alias-db)#`	保留データベース コンフィギュレーション サブモードを開始します。
ステップ 3	**device-alias name** *device-name* **pwwn** *pwwn-id* **Example:** `switch(config-device-alias-db)# device-alias name mydevice pwwn 21:01:00:e0:8b:2e:80:93`	pWWNによって識別されるデバイスのデバイス名を指定します。これが最初に入力されたデバイス エイリアス コンフィギュレーション コマンドであるため、保留データベースへの書き込みを開始し、同時にファブリックをロックします。
ステップ 4	**no device-alias name** *device-name* **Example:** `switch(config-device-alias-db)# no device-alias name mydevice`	pWWNによって識別されるデバイスのデバイス名を削除します。
ステップ 5	**device-alias rename** *old-device-name new-device-name* **Example:** `switch(config-device-alias-db)# device-alias rename mydevice mynewdevice`	既存のデバイス エイリアスを新しい名前に変更します。

例

次に、デバイス エイリアス設定を表示する例を示します。

```
switch# show device-alias name x
device-alias name x pwwn 21:01:00:e0:8b:2e:80:93
```

デバイス エイリアスのモード

基本モード（デフォルト モード）で動作する場合、デバイス エイリアスはすぐにpWWNに展開されます。基本モードで、デバイス エイリアスがたとえば新しい Host Bus Adapter（HBA）を指定するように変更された場合、その変更はゾーン サーバには反映されません。ユーザーは以前の HBA の pWWN を削除して新しい HBA の pWWN を追加し、ゾーンセットを再度アクティブ化する必要があります。

Note Cisco NX-OS Release 10 では、基本デバイス エイリアス モードと拡張デバイス エイリアス モードの両方がサポートされています。 1(1) 2(1)F。

拡張モードで動作する場合、アプリケーションはネイティブ形式でのデバイスエイリアス名を受け入れます。デバイスエイリアスをpWWNに展開する代わりに、デバイスエイリアス名が設定に保存され、ネイティブデバイスエイリアス形式で配布されます。このため、ゾーンサーバーなどのアプリケーションは、自動的にデバイス エイリアス メンバーシップの変更を追跡し、それに応じて変更を実行します。拡張モードでの動作の主な利点は、変更の実施を1カ所で行えるということです。

デバイス エイリアス モードを変更すると、デバイス エイリアスの配布がイネーブルまたはオンの場合にだけ、変更がネットワーク内のほかのスイッチに配布されます。イネーブルまたはオン以外の場合、モード変更はローカル スイッチでだけ行われます。

Note 拡張モードまたはネイティブ デバイス エイリアス ベースの設定は、interop モードの VSAN では受け入れられません。対応するゾーンにネイティブ デバイス エイリアス ベースのメンバがある場合、IVR ゾーンセットのアクティベーションは interop モードの VSAN で失敗します。

デバイス エイリアス サービスに対するデバイス エイリアスのモードの注意事項と制限事項

デバイス エイリアス サービス設定時の注意事項と制限事項は次のとおりです。

- 異なるデバイス エイリアス モードで稼働している 2 つのファブリックが結合されると、デバイス エイリアスの結合は失敗します。結合プロセス中、一方のモードまたは他方のモードに自動的に変換できません。このような状況では、どちらか一方のモードを選択する必要があります。
- 拡張モードから基本モードに変更する前に、最初にローカル スイッチとリモート スイッチの両方からすべてのネイティブ デバイス エイリアス ベースの設定を明示的に削除するか、またはすべてのデバイス エイリアス ベース設定のメンバを対応する pWWN に置き換える必要があります。
- デバイス エイリアス データベースからデバイス エイリアスを削除すると、すべてのアプリケーションは対応するデバイスエイリアスの実行を自動的に中止します。対応するデバイス エイリアスがアクティブなゾーンセットの一部である場合、その pWWN を出入りするすべてのトラフックが中断されます。
- デバイス エイリアス名を変更すると、デバイス エイリアス データベース内のデバイス エイリアス名が変更されるだけでなく、すべてのアプリケーションの対応するデバイスエイリアス設定も置き換えられます。
- デバイス エイリアス データベースに新しいデバイス エイリアスが追加され、そのデバイスエイリアスにアプリケーション設定が存在する場合、設定は自動的に有効になります。

たとえば、対応するデバイスエイリアスがアクティブなゾーンセットの一部で、デバイスがオンラインの場合、ゾーン分割が自動的に実行されます。ゾーンセットを再度アクティブ化する必要はありません。

- デバイス エイリアス名が新しい HBA の pWWN にマッピングされると、それに応じてアプリケーションの適用方法が変更されます。この場合、ゾーン サーバーは、新しい HBA の pWWN に基づいて自動的にゾーン分割を適用します。

デバイス エイリアス モードの設定

拡張モードで動作するデバイス エイリアスを設定できます。

SUMMARY STEPS

1. **configure terminal**
2. **device-alias mode enhanced**
3. **no device-alias mode enhance**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**device-alias mode enhanced** **Example:** `switch(config)# device-alias mode enhanced`	拡張モードで動作するデバイスエイリアスを割り当てます。
ステップ 3	**no device-alias mode enhance** **Example:** `switch(config)# no device-alias mode enhance`	基本モードで動作するデバイスエイリアスを割り当てます。

例

次に、現在のデバイス エイリアス モード設定を表示する例を示します。

```
switch# show device-alias status
Fabric Distribution: Enabled
Database:- Device Aliases 0 Mode: Basic
Locked By:- User "admin" SWWN 20:00:00:0d:ec:30:90:40
Pending Database:- Device Aliases 0 Mode: Basic
```

デバイス エイリアスの配布

デフォルトでは、デバイス エイリアスの配布はイネーブルになっています。デバイス エイリアス機能は CFS を使用して、ファブリック内のすべてのスイッチに変更内容を配布します。

デバイスエイリアスの配布がディセーブルの場合、データベースの変更内容はファブリック内のスイッチに配布されません。ファブリック内のすべてのスイッチで同じ変更を手動で行い、デバイスエイリアスデータベースを最新の状態に維持する必要があります。すぐにデータベースの変更が行われるので、保留中のデータベースおよびコミットまたは中断の操作もありません。変更をコミットしていない状態で配布をディセーブルにすると、コミット作業は失敗します。

Note CFS はデフォルトでイネーブルです。ファブリックのすべてのデバイスでは CFS が有効になっている必要があります。そうでない場合、デバイスは配信を受け入れません。アプリケーションで CFS 配信が無効にされている場合、そのアプリケーションは構成を配信せず、またファブリック内の他のデバイスからの配信も受け入れません。CFS を有効にするには、**cfs distribute** コマンドを使用します。

次に、失敗したデバイス エイリアスのステータスを表示する例を示します。

```
switch# show device-alias status
Fabric Distribution: Disabled
Database:- Device Aliases 25
Status of the last CFS operation issued from this switch:
==========================================================
Operation: Commit
Status: Failed (Reason: Operation is not permitted as the fabric distribution is
 currently disabled.)
```

ファブリックのロック

デバイス エイリアス設定作業を行うと（どのデバイス エイリアス作業かに関係なく）、ファブリックはデバイスエイリアス機能に対して自動的にロックされます。ファブリックがロックされると、次のような状況になります。

- 他のユーザーがこの機能の設定に変更を加えることができなくなります。
- 有効なデータベースのコピーが取得され、保留データベースとして使用されます。保留中のデータベースに対して、以降の変更が行われます。保留データベースへの変更をコミットするかまたは破棄（**abort**）するまで、保留データベースは使用されます。

変更のコミット

変更をコミットできます。

保留中のデータベースに行われた変更内容をコミットした場合、次のイベントが発生します。

- 有効なデータベースの内容が、保留中のデータベースの内容に上書きされます。
- 保留中のデータベースがファブリック内のスイッチに配布され、これらのスイッチの有効なデータベースが新しい変更内容に上書きされます。
- 保留中のデータベースの内容が空になります。
- ファブリック ロックがこの機能に対して解除されます。

SUMMARY STEPS

1. **configure terminal**
2. **device-alias commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**device-alias commit** **Example:** `switch(config)# device-alias commit`	現在アクティブなセッションに対する変更をコミットします。

変更の破棄

デバイス エイリアスのセッション変更を破棄できます。

保留中のデータベースで行われた変更内容を廃棄した場合、次のイベントが発生します。

- 有効なデータベースの内容は影響を受けません。
- 保留中のデータベースの内容が空になります。
- ファブリック ロックがこの機能に対して解除されます。

SUMMARY STEPS

1. **configure terminal**
2. **device-alias abort**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**device-alias abort** **Example:** `switch(config)# device-alias abort`	現在アクティブなセッションを廃棄します。

例

次に、破棄操作のステータスを表示する例を示します。

```
switch(config)# show device-alias status

Fabric Distribution: Enabled
Database:- Device Aliases 2 Mode: Basic
Checksum: 0x22a1d11a2762bdb3cae50f16a21a1e1
Locked By:- User "CLI/SNMPv3:admin" SWWN 20:00:00:de:fb:9d:0e:a0
Pending Database:- Device Aliases 3 Mode: Basic
```

次に、中断操作のステータスを表示する例を示します。

```
switch(config)# device-alias abort
switch(config)#

switch(config)#  show device-alias session status
Last Action Time Stamp : Mon Nov 4 09:10:11 2019
Last Action : Abort
Last Action Result : Success
Last Action Failure Reason : none
switch(config)#
```

ファブリック ロックの上書き

ロック操作（クリア、コミット、中断）は、デバイスエイリアスの配布がイネーブルの場合にだけ使用できます。ユーザーがデバイスエイリアス作業を行ったが、変更のコミットや廃棄を行ってロックを解除するのを忘れていた場合、管理者はファブリック内の任意のスイッチからロックを解除できます。管理者がこの操作を行うと、ユーザーによる保留データベースの変更は廃棄され、ファブリックのロックは解除されます。

スイッチを再起動した場合、変更は volatile ディレクトリでだけ使用でき、また廃棄される場合もあります。

管理者の権限を使用して、ロックされたデバイス エイリアス セッションを解除するには、EXEC モードで **clear device-alias session** コマンドを使用します。

```
switch# clear device-alias session
```

次に、クリア操作のステータスを表示する例を示します。

```
switch# show device-alias status
Fabric Distribution: Enabled
Database:- Device Aliases 24
Status of the last CFS operation issued from this switch:
==========================================================
Operation: Clear Session<--------------------Lock released by administrator
Status: Success<----------------------------Successful status of the operation
```

デバイス エイリアスの配布のディセーブル化とイネーブル化

デバイス エイリアスの配布をディセーブルまたはイネーブルに設定できます。

SUMMARY STEPS

1. **configure terminal**
2. **no device-alias distribute**
3. **device-alias distribute**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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 device-alias distribute** **Example:** `switch(config)# no device-alias distribute`	配布をディセーブルにします。
ステップ 3	**device-alias distribute** **Example:** `switch(config)# device-alias distribute`	配布をイネーブルにします（デフォルト）。

例

次に、デバイス エイリアスの配布のステータスを表示する例を示します。

```
switch# show device-alias status

Fabric Distribution: Disabled
Database:- Device Aliases 3 Mode: Basic
```

```
Checksum: 0x284031ab5aade498a7e89cef1b04d7f
switch(config)#
```

次に、配布がディセーブルな場合のデバイス エイリアスの表示例を示します。

```
switch# show device-alias status

Fabric Distribution: Disabled
Database:- Device Aliases 3 Mode: Basic
Checksum: 0x284031ab5aade498a7e89cef1b04d7f
switch(config)#
```

レガシー ゾーン エイリアスの構成

次の制約事項を満たす場合、レガシー ゾーン エイリアス設定をインポートし、データを失うことなくこの機能を使用できます。

- 各ゾーン エイリアスには、メンバが 1 つだけあります。
- メンバのタイプは pWWN です。

名前または定義の競合が存在する場合、ゾーン エイリアスはインポートされません。

設定に応じて、必要とされるゾーン エイリアスをデバイス エイリアス データベースにコピーしてください。

インポート操作が終了し、**commit** 操作を行うと、変更されたエイリアス データベースが物理ファブリック内のほかのすべてのスイッチに配布されます。ファブリック内の他のスイッチに設定を配信する必要がない場合は、**abort** 処理を実行して、マージ変更内容をすべて破棄できます。

ゾーン エイリアスのインポート

特定の VSAN のゾーン エイリアスをインポートできます。

SUMMARY STEPS

1. **configure terminal**
2. **device-alias import fcalias vsan** *vlan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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。

	Command or Action	Purpose
ステップ 2	**device-alias import fcalias vsan** *vlan-id* **Example:** `switch(config)# device-alias import fcalias vsan`	指定された VSAN の fcalias 情報をインポートします。

デバイス エイリアス データベースの結合の注意事項

2つのデバイスエイリアスデータベースを結合する場合は、次の注意事項に従ってください。

- 名前が異なる 2 つのデバイス エイリアスが同一の pWWN にマッピングされていないことを確認します。
- 2 つの同一の pWWN が 2 つの異なるデバイス エイリアスにマッピングされていないことを確認します。
- 両方のデータベースのデバイス エイリアスの合計数が、Cisco MDS SAN-OS Release 3.0（x）以前が稼働しているファブリックでは 8K（8191 個のデバイス エイリアス）、Cisco MDS SAN-OS Release 3.1（x）以降が稼働しているファブリックでは 20K を超えていないことを確認します。
- 両方のデータベースのデバイスエイリアスの総数が、20K を超えていないことを確認してください。

両方のデータベースのデバイスエントリの合計数がサポートされる設定制限値を超えた場合、結合は失敗します。たとえば、データベース *N* に 6000 個のデバイス エイリアス、データベース *M* に 2192 個のデバイス エイリアスがあり、SAN-OS Release 3.0(x) 以前が稼働している場合、この結合操作は失敗します。デバイス エイリアス モードが一致していない場合も、結合操作は失敗します。

追加情報については、ご使用のデバイスの『System Management Configuration Guide』の「CFS Merge Support」を参照してください。

デバイス エイリアス構成の確認

デバイス エイリアス情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show zoneset [**active**]	ゾーンセット情報のデバイスエイリアスを表示します。
show device-alias database [**pending** | **pending-diffs**]	デバイスエイリアスデータベースを表示します。
show device-alias {**pwwn** *pwwn-id* | **name** *device-name* } [**pending**]	指定された pWWN またはエイリアスのデバイス エイリアス情報を表示します。

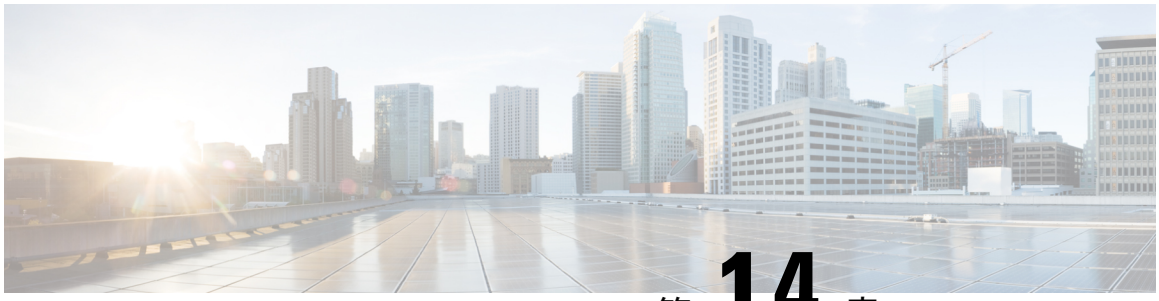
コマンド	目的
show flogi database [**pending**]	FLOGI データベースのデバイス エイリアス情報を表示します。
show fcns database [**pending**]	FCNS データベースのデバイス エイリアス情報を表示します。

デバイス エイリアス サービスのデフォルト設定

次の表に、デバイス エイリアス パラメータのデフォルト設定を示します。

Table 23: デフォルトのデバイス エイリアス パラメータ

パラメータ	デフォルト
デバイス エイリアスの配布	イネーブル
デバイス エイリアスのモード	基本（Basic）：
使用中のデータベース	有効なデータベース
変更を受け入れるデータベース	保留中のデータベース
デバイスエイリアス ファブリック ロックの状態	最初のデバイスエイリアス作業でロックされる



第 14 章

ゾーンの設定と管理

この章では、ゾーンの設定と管理方法について説明します。

この章は、次の項で構成されています。

ゾーンに関する情報

ゾーン分割により、ストレージ デバイス間またはユーザー グループ間でアクセス コントロールの設定ができます。ファブリックで管理者権限を持つユーザーは、ゾーンを作成してネットワーク セキュリティを強化し、データ損失またはデータ破壊を防止できます。ゾーン分割は、送信元/宛先 ID フィールドを検証することによって実行されます。

Note Cisco NX-OS リリース 10.2(1) は、基本、拡張、およびスマート ゾーニングをサポートします。FC-GS-4 および FC-SW-3 規格で指定されている高度なゾーン分割機能がサポートされます。既存の基本ゾーン分割機能または規格に準拠した高度なゾーン分割機能のどちらも使用できます。

Cisco NX-OS リリース 9.3(5) は、拡張ゾーニングとスマート ゾーニングをサポートします。FC-GS-4 および FC-SW-3 規格で指定されている高度なゾーン分割機能がサポートされます。既存の基本ゾーン分割機能または規格に準拠した高度なゾーン分割機能のどちらも使用できます。

ゾーン分割に関する情報

ゾーン分割の特徴

ゾーン分割には、次の特徴があります。

- ゾーンは、複数のゾーン メンバで構成されます。

- ゾーンのメンバ同士はアクセスできますが、異なるゾーンのメンバ同士はアクセスできません。
- ゾーン分割がアクティブでない場合、すべてのデバイスがデフォルト ゾーンのメンバとなります。
- ゾーン分割がアクティブの場合、アクティブ ゾーン（アクティブ ゾーン セットに含まれるゾーン）にないデバイスがデフォルト ゾーンのメンバとなります。
- ゾーンのサイズを変更できます。
- デバイスは複数のゾーンに所属できます。
- 物理ファブリックでは、最大16,000メンバを収容できます。これには、ファブリック内のすべての VSAN が含まれます。

- ゾーン セットは、1 つまたは複数のゾーンで構成されます。
  - ゾーン セットは、単一エンティティとしてファブリックのすべてのスイッチでアクティブまたは非アクティブにできます。
  - VSAN 内でアクティブにできるのは、常に 1 つのゾーン セットだけです。
  - 1 つのゾーンを 複数のゾーン セットのメンバにできます。
  - ゾーン スイッチあたりの最大ゾーン セット数は 1000 です。
- ゾーン分割は、ファブリックの任意のスイッチから管理できます。
  - 任意のスイッチからゾーンをアクティブにした場合、ファブリックのすべてのスイッチがアクティブ ゾーンセットを受信します。また、ファブリック内のすべてのスイッチにフル ゾーン セットが配布されます（送信元スイッチでこの機能が基本ゾーニング モードでイネーブルであり、拡張ゾーニング モードでデフォルトである場合）。
  - 既存のファブリックに新しいスイッチが追加されると、新しいスイッチによってゾーン セットが取得されます。
- ゾーンの変更を中断せずに設定できます。
  - 影響を受けないポートまたはデバイスのトラフィックを中断させることなく、新しいゾーンおよびゾーン セットをアクティブにできます。
- ゾーン メンバーシップは、次のデバイス エイリアス メンバーを使用して指定できます。
  - Port World Wide Name（pWWN）：スイッチに接続された N ポートの pWWN をゾーンのメンバとして指定します。
  - ファブリック pWWN：ファブリック ポートの WWN（スイッチ ポートの WWN）を指定します。このメンバーシップは、ポートベース ゾーン分割とも呼ばれます。
  - FC ID：スイッチに接続されたNポートのFC IDをゾーンのメンバとして指定します。

- インターフェイスおよびSwitch WWN（sWWN）：sWWNによって識別されたスイッチのインターフェイスを指定します。このメンバーシップは、インターフェイスゾーン分割とも呼ばれます。
- インターフェイスおよびドメインID：ドメインIDによって識別されたスイッチのインターフェイスを指定します。
- ドメインIDおよびポート番号：シスコ スイッチ ドメインのドメインIDを指定し、さらに他社製スイッチに所属するポートを指定します。
- デバイス エイリアス：デバイス エイリアス名を指定します。
- FC エイリアス：FC エイリアスの名前を指定します。

Note 仮想ファイバ チャネル インターフェイスのスイッチに接続されたNポートでは、ログイン デバイスのデバイス エイリアス、Nポートのp WWN、Nポートの FC ID、または仮想ファイバ チャネル インターフェイスのファブリックpWWNを使用して、ゾーン メンバーシップを指定できます。

- デフォルト ゾーン メンバーシップには、特定のメンバーシップとの関係を持たないすべてのポートまたはWWNが含まれます。デフォルトゾーンメンバ間のアクセスは、デフォルト ゾーン ポリシーによって制御されます。
- VSAN あたり最大 8000 ゾーン、スイッチ上の全 VSAN で最大 8000 ゾーンを設定できます。
- 最大 4000 のゾーン ACL エントリがサポートされています。
- ゾーン ACL エントリの数が 4000 を超えると、ゾーンはソフト ゾーニング モードに移行する可能性があります。

Note インターフェイスベース ゾーン分割は、Cisco SANスイッチでのみ機能します。インターフェイスベース ゾーン分割は、interop モードで設定された VSAN では機能しません。

ゾーン分割の例

次の図に、ファブリックの2つのゾーン（ゾーン1およびゾーン2）で構成されるゾーン セットを示します。ゾーン1は、3つすべてのホスト（H1、H2、H3）からストレージ システム S1 と S2 に存在するデータへのアクセスを提供します。ゾーン2では、S3のデータにH3からだけアクセスできます。H3は、両方のゾーンに存在します。

***Figure 22: 2*つのゾーンによるファブリック**

ほかの方法を使用して、このファブリックを複数のゾーンに分割することもできます。次の図は、別の方法を示します。新しいソフトウェアをテストするために、ストレージ システム S2 を分離する必要があると想定します。これを実行するために、ホスト H2 とストレージ S2 だけを含むゾーン 3 が設定されます。ゾーン 3 ではアクセスを H2 と S2 だけに限定し、ゾーン 1 ではアクセスを H1 と S1 だけに限定できます。

Figure 23: 3 つのゾーンによるファブリック

ゾーン実装

Cisco SAN スイッチは、自動的に次の基本的なゾーン機能をサポートします（設定を追加する必要はありません）。

- ゾーンが VSAN に含まれます。
- ハード ゾーン分割を手動でディセーブルにすることはできません。
- ネーム サーバー クエリーがソフト ゾーン分割されます。
- アクティブ ゾーン セットだけが配布されます。
- ゾーン分割されていないデバイスは、相互にアクセスできません。
- 各 VSAN に同一名のゾーンまたはゾーン セットを含めることができます。
- 各 VSAN には、フル データベースとアクティブ データベースがあります。
- アクティブ ゾーン セットを変更するには、フル ゾーン データベースをアクティブ化する必要があります。
- アクティブ ゾーン セットは、スイッチの再起動後も維持されます。
- フル データベースに加えた変更は、明示的に保存する必要があります。
- ゾーンの再アクティブ化（ゾーン セットがアクティブの状態で、別のゾーン セットをアクティブ化する場合）しても、既存のトラフィックは中断しません。

必要に応じて、さらに次のゾーン機能を設定できます。

- VSAN 単位ですべてのスイッチにフル ゾーン セットを伝播します。
- ゾーン分割されていないメンバのデフォルト ポリシーを変更します。
- VSAN を interop モードに設定することによって、他のベンダーと相互運用できます。相互に干渉することなく、同じスイッチ内で 1 つの VSAN を interop モードに、別の VSAN を基本モードに設定することもできます。
- E ポートを分離状態から復旧します。

アクティブおよびフル ゾーン セット

ゾーン セットを設定する前に、次の注意事項について検討してください。

- 各 VSAN は、複数のゾーン セットを持つことができますが、アクティブにできるのは常に 1 つのゾーン セットだけです。
- ゾーン セットを作成すると、そのゾーン セットは、フル ゾーン セットの一部となります。
- ゾーン セットがアクティブな場合は、フル ゾーン セットからのゾーン セットのコピーがゾーン分割の実行に使用されます。これは、アクティブ ゾーン セットと呼ばれます。アクティブ ゾーン セットは変更できません。アクティブ ゾーン セットに含まれるゾーンは、アクティブ ゾーンと呼ばれます。
- 管理者は、同一名のゾーン セットがアクティブであっても、フル ゾーン セットを変更できます。ただし、加えられた変更が有効になるのは、再アクティブ化したときです。
- アクティブ化が実行されると、永続的なコンフィギュレーションにアクティブ ゾーンセットが自動保存されます。これにより、スイッチのリセットにおいてもスイッチはアクティブ ゾーン セット情報を維持できます。
- ファブリックのその他すべてのスイッチは、アクティブ ゾーン セットを受信するので、それぞれのスイッチでゾーン分割を実行できます。
- ハードおよびソフト ゾーン分割は、アクティブ ゾーン セットを使用して実装されます。変更は、ゾーン セットのアクティブ化によって有効になります。
- アクティブ ゾーン セットに含まれない FC ID または Nx ポートは、デフォルト ゾーンに所属します。デフォルト ゾーン情報は、他のスイッチに配信されません。

Note 1 つのゾーンセットがアクティブな場合に、別のゾーンセットをアクティブにすると、現在アクティブなゾーンセットが自動的に非アクティブになります。新しいゾーンセットをアクティブにする前に、現在のアクティブ ゾーン セットを明示的に非アクティブにする必要はありません。

次の図は、アクティブなゾーン セットに追加されるゾーンを示します。

Figure 24: アクティブおよびフル ゾーン セット

ゾーンの設定

ゾーンを設定し、ゾーン名を割り当てることができます。

SUMMARY STEPS

1. **configure terminal**
2. **zone name** *zone-name* **vsan** *vsan-id*
3. **member** *type value*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**zone name** *zone-name* **vsan** *vsan-id* **Example:** `switch(config)# zone name test vsan 5`	指定された VSAN にゾーンを設定します。 **Note** すべての英数字か、または記号（$、-、^、_）のうち 1 つがサポートされます。
ステップ 3	**member** *type value* **Example:** `switch(config-zone)# member interface 4`	指定されたタイプ（pWWN、ファブリック pWWN、FC ID、FC エイリアス、デバイス エイリアス、ドメイン ID、またはインターフェイス）および値に基づいて、指定されたゾーンにメンバを設定します。 **Caution** 同じファブリック内に FabricWare を実行する Cisco MDS 9020 スイッチがある場合には、Cisco NX-OS を実行するすべての SAN スイッチには、pWWN タイプのゾーン分割だけを設定する必要があります。 **Tip** 該当する表示コマンド（たとえば、**show interface** または **show flogi database** コマンド）を使用して、必要な値を 16 進表記で取得します。

設定例

Tip **show wwn switch** コマンドを使用して sWWN を取得します。sWWN を指定しない場合、ソフトウェアは自動的にローカル sWWN を使用します。

次の例では、ゾーン メンバを設定します。

```
switch(config)# zone name MyZone vsan 2
```

pWWN の例：

```
switch(config-zone)# member pwwn 10:00:00:23:45:67:89:ab
```

ファブリック pWWN の例：

```
switch(config-zone)# member fwwn 10:01:10:01:10:ab:cd:ef
```

FC ID の例：

```
switch(config-zone)# member fcid 0xce00d1
```

FC エイリアスの例：

```
switch(config-zone)# member fcalias Payroll
```

デバイス エイリアスの例：

```
switch(config-zone)# member device-alias finance
```

ドメイン ID の例：

```
switch(config-zone)# member domain-id 2 portnumber 23
```

Show WWN の例:

```
switch# show wwn switch
```

ローカル sWWN インターフェイスの例：

```
switch(config-zone)# member interface vfc 21
```

リモート sWWN インターフェイスの例：

```
switch(config-zone)# member interface vfc 21 swwn 20:00:00:05:30:00:4a:de
```

ドメイン ID インターフェイスの例：

```
switch(config-zone)# member interface vfc 21 domain-id 25
```

Note **system default zone default-zone permit** および **system default zone distribute full** などのゾーンのデフォルト システム設定は、設定を手動で適用した後に、新しく作成された VSAN でのみ有効になります。これらの設定は、FC セットアップ スクリプトの一部として設定されている場合でも、VSAN 1 に適用されない場合があります。

次に、異なるタイプのメンバ エイリアスを設定する例を示します。

```
switch(config)# fcalias name AliasSample vsan 3
```

pWWN の例：

```
switch(config-fcalias)# member pwwn 10:00:00:23:45:67:89:ab
```

fWWN の例：

```
switch(config-fcalias)# member fwwn 10:01:10:01:10:ab:cd:ef
```

FC ID の例：

```
switch(config-fcalias)# member fcid 0x222222
```

ドメイン ID の例：

```
switch(config-fcalias)# member domain-id 2 portnumber 23
```

デバイス エイリアスの例：

```
switch(config-fcalias)# member device-alias devName
```

ゾーン セット

次の図では、それぞれ独自のメンバーシップ階層とゾーン メンバを持つセットが2つ作成されます。

Figure 25: ゾーン セット、ゾーン、ゾーン メンバーの階層

ゾーンは、アクセス コントロールを指定するための方式を提供します。ゾーンセットは、ファブリックでアクセス コントロールを実行するためのゾーンの分類です。ゾーン セット A またはゾーン セット B のいずれか（両方でなく）をアクティブにできます。

Tip ゾーン セットはメンバ ゾーンおよびVSAN名で設定します（設定されたVSANにゾーン セットが存在する場合）。

ゾーン セットのアクティブ化

既存のゾーン セットをアクティブまたは非アクティブにできます。

ゾーン セットに加えた変更は、それがアクティブ化されるまで、フル ゾーン セットには反映されません。

SUMMARY STEPS

1. **configure terminal**
2. **zoneset activate name** *zoneset-name* **vsan** *vsan-id*
3. **no zoneset activate name** *zoneset-name* **vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**zoneset activate name** *zoneset-name* **vsan** *vsan-id* **Example:**	指定されたゾーン セットをアクティブにします。

	Command or Action	Purpose
	`switch(config)# zoneset activate name test vsan 34`	
ステップ 3	**no zoneset activate name** *zoneset-name* **vsan** *vsan-id* **Example:** `switch(config)# no zoneset activate name test vsan 30`	指定されたゾーンセットを非アクティブにします。

デフォルト ゾーン

ファブリックの各メンバは（デバイスが Nx ポートに接続されている状態）、任意のゾーンに所属できます。どのアクティブ ゾーンにも所属しないメンバは、デフォルト ゾーンの一部と見なされます。したがって、ファブリックにアクティブなゾーンセットがない場合、すべてのデバイスがデフォルト ゾーンに所属するものと見なされます。メンバは複数のゾーンに所属できますが、デフォルト ゾーンに含まれるメンバは、その他のゾーンに所属できません。接続されたポートが起動すると、スイッチは、ポートがデフォルト ゾーンのメンバか判別します。

Note 設定されたゾーンとは異なり、デフォルト ゾーン情報は、ファブリックの他のスイッチに配信されません。

トラフィックをデフォルト ゾーンのメンバ間で許可または拒否できます。この情報は、すべてのスイッチには配信されません。各スイッチで設定する必要があります。

Note スイッチが初めて初期化されたとき、ゾーンは設定されておらず、すべてのメンバがデフォルト ゾーンに所属するものと見なされます。メンバは、相互に通信する許可を受けていません。

ファブリックの各スイッチにデフォルト ゾーン ポリシーを設定します。ファブリックの 1 つのスイッチでデフォルト ゾーン ポリシーを変更する場合、必ずファブリックの他のすべてのスイッチでも変更してください。

Note デフォルト ゾーン設定のデフォルト設定値は変更できます。

デフォルト ポリシーが permit として設定される場合、またはゾーン セットがアクティブのとき、デフォルト ゾーン メンバは明示的に表示されます。デフォルト ポリシーが deny として設定されている場合、アクティブ ゾーン セットを表示すると、このゾーンのメンバの一覧表示は明示されません。

デフォルト ゾーンのアクセス権限の設定

デフォルト ゾーン内のメンバに対してトラフィックを許可または拒否するには、次の作業を行います。

SUMMARY STEPS

1. **configure terminal**
2. **zone default-zone permit vsan** *vsan-id*
3. **no zone default-zone permit vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**zone default-zone permit vsan** *vsan-id* **Example:** `switch(config)# zone default-zone permit vsan 13`	デフォルト ゾーン メンバへのトラフィック フローを許可します。
ステップ 3	**no zone default-zone permit vsan** *vsan-id* **Example:** `switch(config)# no zone default-zone permit vsan 40`	デフォルト ゾーン メンバへのトラフィック フローを拒否（デフォルト）します。

FC エイリアスの作成

次の値を使用して、エイリアス名を割り当て、エイリアス メンバを設定できます。

- pWWN：N ポートの 16 進表記の WWN（10:00:00:23:45:67:89:ab など）
- fWWN：ファブリック ポートの 16 進表記の WWN（10:00:00:23:45:67:89:ab など）
- FC ID：0xhhhhhh 形式の N ポート ID（0xce00d1 など）
- ドメインID：ドメインID は 1 ～ 239 の整数です。このメンバーシップ設定を完了するには、他社製スイッチの必須ポート番号が必要です。
- インターフェイス：インターフェイスベース ゾーン分割は、スイッチ インターフェイスがゾーンを設定するのに使用される点でポートベース ゾーン分割と似ています。スイッチ インターフェイスをローカル スイッチとリモート スイッチの両方でゾーン メンバとして指定できます。リモート スイッチを指定するには、特定の VSAN 内のリモート Switch WWN（sWWN）またはドメイン ID を入力します。
- デバイス エイリアス：デバイス エイリアス名を指定します。

Tip スイッチは、VSAN あたり最大 2048 のエイリアスをサポートします。

FC エイリアスの作成

エイリアスを作成します。

SUMMARY STEPS

1. **configure terminal**
2. エイリアス名 vsan-id **fcalias name vsan**
3. **member** *type value*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	エイリアス名 vsan-id **fcalias name vsan** **Example:** `switch(config)# fcalias name testname vsan 50`	エイリアス名を設定します。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。
ステップ 3	**member** *type value* **Example:** `switch(config-fcalias)# member pwwn 20:00:20:94:00:00:00:01`	指定されたタイプ（pWWN、ファブリック pWWN、FC ID、ドメイン ID、またはインターフェイス）および値に基づいて、指定された FC エイリアスにメンバーを設定します。 **Note** 複数のメンバを複数の行で指定できます。

FC エイリアスの作成例

***Table 24: member* コマンドのタイプおよび値の構文**

デバイス エイリアス	**member device-alias** *device-alias*
ドメイン ID	ドメイン ID 番号 **member domain-id portnumber**
FC ID	**member fcid** *fcid*
ファブリック pWWN	**member fwwn** *fwwn-id*

ローカル sWWN インターフェイス	**member interface** *type slot*/*port* **Note** これが QSFP+ GEM またはブレイクアウト ポートの場合、*port* 構文は *QSFP-module*/*port* になります。 **Note** これが 10G ブレイクアウト ポートの場合、*slot*/*port* 構文は *QSFP-module*/*port* になります。
ドメイン ID インターフェイス	**member interface** *type slot*/*port* **domain-id** domain-id **Note** これが QSFP+ GEM またはブレイクアウト ポートの場合、*port* 構文は *QSFP-module*/*port* になります。 **Note** これが 10G ブレイクアウト ポートの場合、*slot*/*port* 構文は *QSFP-module*/*port* になります。
リモート sWWN インターフェイス	**member interface** *type slot*/*port* **swwn** *swwn-id* **Note** これが QSFP+ GEM またはブレイクアウト ポートの場合、*port* 構文は *QSFP-module*/*port* になります。 **Note** これが 10G ブレイクアウト ポートの場合、*slot*/*port* 構文は *QSFP-module*/*port* になります。
pWWN	**member pwwn** *pwwn-id*

次に、異なるタイプのメンバ エイリアスを設定する例を示します。

```
switch(config)# fcalias name AliasSample vsan 3
```

pWWN の例：

```
switch(config-fcalias)# member pwwn 10:00:00:23:45:67:89:ab
```

fWWN の例：

```
switch(config-fcalias)# member fwwn 10:01:10:01:10:ab:cd:ef
```

FC ID の例：

```
switch(config-fcalias)# member fcid 0x222222
```

ドメイン ID の例：

```
switch(config-fcalias)# member domain-id 2 portnumber 23
```

ローカル sWWN インターフェイスの例：

```
switch(config-fcalias)# member interface vfc 21
```

リモート sWWN インターフェイスの例：

```
switch(config-fcalias)# member interface vfc 21 swwn 20:00:00:05:30:00:4a:de
```

ドメイン ID インターフェイスの例：

```
switch(config-fcalias)# member interface vfc21 domain-id 25
```

デバイス エイリアスの例：

```
switch(config-fcalias)# member device-alias devName
```

ゾーン セットの作成とメンバ ゾーンの追加

ゾーン セットを作成して複数のメンバー ゾーンを追加できます。

SUMMARY STEPS

1. **configure terminal**
2. **zone set name** *zoneset-name* **vsan** *vsan-id*
3. **member** *name*
4. **zone name** *zone-name*
5. **member fcid** *fcid*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**zone set name** *zoneset-name* **vsan** *vsan-id* **Example:** `switch(config)# zone set name new vsan 23`	設定したゾーン セット名でゾーン セットを設定します。 **Tip** ゾーン セットをアクティブにするには、まずゾーンとゾーンセットを1つ作成する必要があります。
ステップ 3	**member** *name* **Example:** `switch(config-zoneset)# member new`	以前指定したゾーンセットのメンバーとしてゾーンを追加します。 **Tip** 指定されたゾーン名が事前に設定されていない場合、このコマンドを実行すると「Zone not present」エラー メッセージが返されます。

	Command or Action	Purpose
ステップ 4	**zone name** *zone-name* **Example:** `switch(config-zoneset)# zone name trial`	指定されたゾーン セットにゾーンを追加します。 **Tip** ゾーン セット プロンプトからゾーンを作成する必要がある場合は、このステップを実行します。
ステップ 5	**member fcid** *fcid* **Example:** `switch(config-zoneset-zone)# member fcid 0x222222`	新しいゾーンに新しいメンバを追加します。 **Tip** ゾーン セット プロンプトからゾーンにメンバを追加する必要がある場合は、このステップを実行します。

Tip アクティブ ゾーン セットを保存するために、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はありません。ただし、フル ゾーン セットを明示的に保存するには、実行コンフィギュレ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。

ゾーンの実行

ゾーン分割は、ソフトとハードの2つの方法で実行できます。各エンドデバイス（Nポート）は、ネーム サーバにクエリーを送信することでファブリック内の他のデバイスを検出します。デバイスがネーム サーバーにログインすると、ネーム サーバーはクエリー元デバイスがアクセスできる他のデバイスのリストを返します。Nポートがゾーンの外部にあるその他のデバイスの FCID を認識しない場合、そのデバイスにアクセスできません。

ソフト ゾーン分割では、ゾーン分割の制限がネーム サーバーとエンド デバイス間の対話時にだけ適用されます。エンドデバイスが何らかの方法でゾーン外部のデバイスのFCIDを認識できる場合、そのデバイスにアクセスできます。

ハードゾーン分割は、Nポートから送信される各フレームでハードウェアによって実行されます。スイッチにフレームが着信した時点で、送信元/宛先 ID と許可済みの組み合わせが照合されるため、ワイヤスピードでフレームを送信できます。ハードゾーン分割は、ゾーン分割のすべての形式に適用されます。

Note ハードゾーン分割は、すべてのフレームでゾーン分割制限を実行し、不正なアクセスを防ぎます。

Cisco SAN スイッチは、ハードとソフトの両方のゾーン分割をサポートします。

ゾーン セットの配信

フル ゾーン セットは、EXEC モード レベルで **zoneset distribute vsan** コマンドを使用する一時配信、またはコンフィギュレーション モード レベルで **zoneset distribute full vsan** コマンドを使用するフル ゾーン セット配信のどちらかの方式を使用して配信できます。次の表に、これらの方式の相違点を示します。

Table 25: ゾーン セット配信の相違点

一時配信 **zoneset distribute vsan** コマンド（**EXEC** モード）	フル ゾーン セット配信 **zoneset distribute full vsan** コマンド（コンフィギュレーション モード）
フル ゾーン セットはすぐに配信されます。	フル ゾーンセットはすぐには配信されません。
アクティブ化、非アクティブ化、または結合時には、アクティブ ゾーン セットと同時にフル ゾーン セット情報を伝播しません。	アクティブ化、非アクティブ化、または結合時には、アクティブ ゾーン セットと同時にフル ゾーン セット情報を伝播します。

フル ゾーン セットの配信のイネーブル化

すべての Cisco SAN スイッチは、新しい E ポート リンクが立ち上がったとき、または新しいゾーン セットが VSAN でアクティブにされたときに、アクティブ ゾーン セットを配信します。ゾーン セットの配信は、隣接スイッチへのマージ要求の送信時、またはゾーン セットのアクティブ化の際に行われます。

VSAN 単位で、VSAN 上のすべてのスイッチへのフル ゾーン セットおよびアクティブ ゾーン セットの配信をイネーブルに設定できます。

SUMMARY STEPS

1. **configure terminal**
2. **zoneset distribute full vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**zoneset distribute full vsan** *vsan-id* **Example:**	アクティブ ゾーン セットとともにフル ゾーン セットの送信をイネーブルにします。

	Command or Action	Purpose
	switch(config)# zoneset distribute full vsan 12	

ワンタイム配信のイネーブル化

ファブリック全体に、非アクティブで未変更のゾーン セットを一度だけ配信します。

この配信を実行するには、EXEC モードで **zoneset distribute vsan** *vsan-id* コマンドを使用します。

```
switch# zoneset distribute vsan 2
Zoneset distribution initiated. check zone status
```

このコマンドではフル ゾーン セット情報の配信だけを実行し、スタートアップ コンフィギュレーションへの情報の保存は行いません。フル ゾーン セット情報をスタートアップ コンフィギュレーションに保存する場合は、**copy running-config start-config** コマンドを明示的に入力する必要があります。

Note Cisco Nexus 9000 では、相互運用モード 3 のみがサポートされています。

ゾーン セット一時配信要求のステータスを確認するには、**show zone status vsan** *vsan-id* コマンドを使用します。

```
switch# show zone status vsan 3
VSAN: 3 default-zone: permit distribute: active only Interop: 100
    mode:basic merge-control:allow
    session:none
    hard-zoning:enabled
Default zone:
    qos:none broadcast:disabled ronly:disabled
Full Zoning Database :
    Zonesets:0  Zones:0 Aliases: 0
Active Zoning Database :
    Name: nozoneset  Zonesets:1  Zones:2
Status: Zoneset distribution completed at 04:01:06 Aug 28 2010
```

リンクの分離からの回復

ファブリックの 2 つのスイッチが TE ポートまたは E ポートを使用して結合される場合、アクティブ ゾーン セットのデータベースが 2 つのスイッチまたはファブリック間で異なると、この TE ポートおよび E ポートが分離する可能性があります。TE ポートまたは E ポートが分離した場合、次の 3 つのオプションのいずれかを使用して分離状態からポートを回復できます。

- 近接スイッチのアクティブ ゾーンセットのデータベースをインポートし、現在のアクティブ ゾーン セットと交換します（次の図を参照）。

- 現在のデータベースを近接スイッチにエクスポートします。
- フル ゾーン セットを編集し、修正されたゾーン セットをアクティブにしてから、リンクを立ち上げることにより、手動で矛盾を解決します。

Figure 26: データベースのインポートとエクスポート

ゾーン セットのインポートおよびエクスポート

ゾーンセット情報を隣接スイッチにエクスポート、または隣接スイッチからインポートできます。

SUMMARY STEPS

1. switch# **zoneset import interface vfc** *vfc-id* **vsan** *vsan-id*
2. **zoneset import interface** {**vfc** | **vfc-port-channel**} *if-number* **vsan** *vsan-id*
3. **zoneset export vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **zoneset import interface vfc** *vfc-id* **vsan** *vsan-id*	VSAN または VSAN の範囲の指定されたインターフェイスを介して接続された隣接スイッチからゾーン セットをインポートします。
ステップ 2	**zoneset import interface** {**vfc** | **vfc-port-channel**} *if-number* **vsan** *vsan-id* **Example:** `switch# zoneset import interface 6 vsan 10`	VSAN または VSAN の範囲の指定されたインターフェイスを介して接続された隣接スイッチからゾーン セットをインポートします。
ステップ 3	**zoneset export vsan** *vsan-id* **Example:** `switch# zoneset export vsan 5`	指定された VSAN または VSAN の範囲を介して接続された隣接スイッチにゾーンセットをエクスポートします。

ゾーン セットの複製

コピーを作成し、既存のアクティブゾーンセットを変更することなく編集できます。アクティブ ゾーン セットを bootflash: ディレクトリ、volatile: ディレクトリ、または slot0 から次のいずれかのエリアにコピーできます。

- フル ゾーン セット

- リモート ロケーション（FTP、SCP、SFTP、または TFTP を使用）

アクティブ ゾーン セットは、フル ゾーン セットに含まれません。フル ゾーン セットが失われた場合または伝播されなかった場合に、既存のゾーンセットに変更を加えても、アクティブにできません。

Caution 同一名のゾーンがフル ゾーン データベースにすでに存在する場合、アクティブ ゾーン セットをフル ゾーン セットにコピーすると、その同一名のゾーンが上書きされることがあります。

ゾーン セットのコピー

Cisco SAN スイッチでは、アクティブ ゾーン セットは編集できません。ただし、アクティブ ゾーン セットをコピーして、編集可能な新しいゾーン セットを作成できます。

SUMMARY STEPS

1. **zone copy active-zoneset full-zoneset vsan** *vsan-id*
2. **zone copy vsan** *vsan-id* **active-zoneset scp://guest@myserver/tmp/active_zoneset.txt**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**zone copy active-zoneset full-zoneset vsan** *vsan-id* **Example:** `switch# zone copy active-zoneset full-zoneset vsan 301`	指定された VSAN のアクティブ ゾーン セットのコピーをフル ゾーン セットに作成します。
ステップ 2	**zone copy vsan** *vsan-id* **active-zoneset scp://guest@myserver/tmp/active_zoneset.txt** **Example:** `switch# zone copy vsan 55 active-zoneset scp://guest@myserver/tmp/active_zoneset.txt`	SCP を使用して、指定された VSAN のアクティブ ゾーンをリモート ロケーションにコピーします。

ゾーン、ゾーン セット、およびエイリアスの名前の変更

ゾーン、ゾーン セット、FC エイリアス、またはゾーン属性グループの名前を変更できます。

SUMMARY STEPS

1. **configure terminal**
2. **zoneset rename** *oldname newname* **vsan** *vsan-id*
3. **zone rename** *oldname newname* **vsan** *vsan-id*
4. **fcalias rename** *oldname newname* **vsan** *vsan-id*

5. **zone-attribute-group rename** *oldname newname* **vsan** *vsan-id*
6. **zoneset activate name** *newname* **vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**zoneset rename** *oldname newname* **vsan** *vsan-id* **Example:** `switch(config)# zoneset rename test myzoneset vsan 60`	指定されたVSANのゾーン セット名を変更します。
ステップ 3	**zone rename** *oldname newname* **vsan** *vsan-id* **Example:** `switch(config)# zone rename test myzone vsan 50`	指定された VSAN のゾーン名を変更します。
ステップ 4	**fcalias rename** *oldname newname* **vsan** *vsan-id* **Example:** `switch(config)# fcalias rename test myfc vsan 200`	指定された VSAN の fcalias 名を変更します。
ステップ 5	**zone-attribute-group rename** *oldname newname* **vsan** *vsan-id* **Example:** `switch(config)# zone-attribute-group rename test mygroup vsan 12`	指定されたVSANのゾーン属性グループ名を変更します。
ステップ 6	**zoneset activate name** *newname* **vsan** *vsan-id* **Example:** `switch(config)# zoneset activate name myzone vsan 50`	ゾーン セットをアクティブにし、アクティブ ゾーン セット内の新しいゾーン名に更新します。

ゾーンのクローニング、ゾーン セットと FC エイリアス

ゾーン、ゾーン セット、およびFC エイリアスを複製できます。

SUMMARY STEPS

1. **configure terminal**
2. **zoneset clone** *oldname newname* **vsan** *vsan-id*
3. **zone clone** *oldname newname* **vsan** *number*
4. **fcalias clone** *oldname newname* **vsan** *vsan-id*

5. **zone-attribute-group clone** *oldname newname* **vsan** *vsan-id*
6. **zoneset activate name** *newname* **vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**zoneset clone** *oldname newname* **vsan** *vsan-id* **Example:** `switch(config)# zoneset clone test myzoneset2 vsan 2`	指定されたVSANのゾーン セットをコピーします。
ステップ 3	**zone clone** *oldname newname* **vsan** *number* **Example:** `switch(config)# zone clone test myzone3 vsan 3`	指定された VSAN 内のゾーンをコピーします。
ステップ 4	**fcalias clone** *oldname newname* **vsan** *vsan-id* **Example:** `switch(config)# fcalias clone test myfcalias vsan 30`	指定された VSAN の FC エイリアス名をコピーします。
ステップ 5	**zone-attribute-group clone** *oldname newname* **vsan** *vsan-id* **Example:** `switch(config)# zone-attribute-group clone test mygroup2 vsan 10`	指定されたVSANのゾーン属性グループをコピーします。
ステップ 6	**zoneset activate name** *newname* **vsan** *vsan-id* **Example:** `switch(config)# zoneset activate name myzonetest1 vsan 3`	ゾーン セットをアクティブにし、アクティブ ゾーン セット内の新しいゾーン名に更新します。

ゾーン サーバー データベースのクリア

指定された VSAN のゾーン サーバー データベース内のすべての設定情報をクリアできます。

ゾーン サーバー データベースをクリアするには、次のコマンドを使用します。

```
switch# clear zone database vsan 2
```

Note **clear zone database** コマンドを入力したあとに、明示的に **copy running-config startup-config** を入力して、次にスイッチを起動するときに確実に実行構成が使用されるようにする必要があります。

Note ゾーン セットをクリアすると、フル ゾーン データベースだけが消去され、アクティブ ゾーン データベースは消去されません。

ゾーン設定の確認

ゾーン情報を表示するには、**show** コマンドを使用します。特定のオブジェクトの情報（たとえば、特定のゾーン、ゾーン セット、VSAN、エイリアス、または brief や active などのキーワード）を要求する場合、指定されたオブジェクトの情報だけが表示されます。

コマンド	目的
show zone	すべての VSAN のゾーン情報の表示
show zone vsan ***vsan-id***	特定の VSAN のゾーン情報の表示
show zoneset vsan ***vsan-id***	VSAN 範囲に設定されたゾーン セットの表示
show zone name ***zone-name***	特定のゾーンのメンバの表示
show fcalias vsan ***vsan-id***	fcalias 設定の表示
show zone member pwwn ***pwwn-id***	メンバが属しているすべてのゾーンの表示
show zone statistics	他のスイッチと交換された制御フレーム数の表示
show zoneset active	アクティブ ゾーン セットの表示
show zone active	アクティブ ゾーンの表示
show zone status	ゾーン ステータスの表示

拡張ゾーン分割

ゾーン分割機能は、FC-GS-4 および FC-SW-3 規格に準拠しています。どちらの規格も、前の項で説明した基本ゾーン分割機能と、この項で説明する拡張ゾーン分割機能をサポートしています。

拡張ゾーン分割

ゾーン分割機能は、FC-GS-4 および FC-SW-3 規格に準拠しています。どちらの規格も、前の項で説明した基本ゾーン分割機能と、この項で説明する拡張ゾーン分割機能をサポートしています。

Note 拡張ゾーン モードでスケール ゾーン構成が再生される場合は、保存されたスケール ゾーン構成を実行構成に適用する前に、ローカル ゾーン データベースを手動でクリアする必要があります。

次の表は、基本ゾーニングと拡張ゾーニングの違いを比較したものです。

Table 26: **拡張ゾーン分割の利点**

基本ゾーン分割	拡張ゾーン分割	拡張ゾーン分割の利点
複数の管理者が設定変更を同時に行うことができます。アクティブ化すると、ある管理者が別の管理者の設定変更を上書きできます。	単一のコンフィギュレーションセッションですべての設定を実行できます。セッションを開始すると、スイッチは変更を行うファブリック全体をロックします。	ファブリック全体を1つのコンフィギュレーションセッションで設定するため、ファブリック内での整合性が確保されます。
ゾーンが複数のゾーンセットに含まれる場合、各ゾーン セットにこのゾーンのインスタンスを作成します。	ゾーンが定義されると、必要に応じて、ゾーンセットがゾーンを参照します。	ゾーンが参照されるため、ペイロードサイズが縮小されています。データベースが大きくなるほど、そのサイズが重要になります。
デフォルトゾーンポリシーがスイッチごとに定義されます。ファブリックをスムーズに動作させるため、ファブリック内のスイッチはすべて同一のデフォルトゾーン設定を使用する必要があります。	ファブリック全体でデフォルトゾーン設定を実行および交換します。	ポリシーがファブリック全体に適用されるため、トラブルシューティングの時間が短縮されます。
スイッチ単位でのアクティブ化の結果を取得するため、管理スイッチはアクティブ化に関する複合ステータスを提供します。この場合、障害のあるスイッチは特定されません。	各リモートスイッチからアクティブ化の結果と問題の特性を取得します。	エラー通知機能が強化されているため、トラブルシューティングが容易です。

基本ゾーン分割	拡張ゾーン分割	拡張ゾーン分割の利点
ゾーン分割データベースを配信するには、同じゾーンセットを再度アクティブ化する必要があります。再度アクティブ化すると、ローカル スイッチおよびリモート スイッチのハードゾーン分割のハードウェア変更に影響することがあります。	ゾーン分割データベースに対して変更を行い、再度アクティブ化することなく変更を配信します。	アクティブ化せずにゾーンセットを配信すると、スイッチのハードゾーン分割のハードウェア変更が回避されます。
シスコ固有のゾーン メンバ タイプ（シンボリック ノード名およびその他のタイプ）は他社製スイッチによって使用されることがあります。結合時に、シスコ固有のタイプは他社製スイッチによって誤って解釈されることがあります。	メンバタイプを一意に識別するために、ベンダー固有のタイプ値とベンダーIDが提供されます。	ベンダー タイプが一意です。
fWWNベースのゾーン メンバーシップは、シスコのinteropモードでだけサポートされます。	標準の interop モード（interop モード 1）で fWWN ベースのメンバーシップがサポートされます。	fWWN ベースのメンバ タイプは標準化されています。

基本ゾーン分割から拡張ゾーン分割への変更

基本ゾーンモードから拡張ゾーンモードに変更できます。

Procedure

ステップ 1 ファブリック内のすべてのスイッチが拡張モードで動作可能であることを確認してください。

ステップ 2 1 つ以上のスイッチが拡張モードで動作できない場合、拡張モードへの変更要求は拒否されます。

ステップ 3 動作モードを拡張ゾーン分割モードに設定します。

拡張ゾーン分割から基本ゾーン分割への変更

Cisco SAN スイッチでは、ほかの Cisco NX-OS リリースへのダウングレードおよびアップグレードを可能にするために、拡張ゾーン分割から基本ゾーン分割に変更できます。

Procedure

ステップ 1 アクティブおよびフルゾーンセットに拡張ゾーン分割モード固有の設定が含まれていないことを確認します。

ステップ 2 このような設定が存在する場合は、次に進む前にこれらの設定を削除します。既存の設定を削除しないと、スイッチ ソフトウェアは自動的にこれらの設定を削除します。

ステップ 3 動作モードを基本ゾーン分割モードに設定します。

拡張ゾーン分割のイネーブル化

VSAN 内で拡張ゾーン分割をイネーブルに設定できます。

デフォルトでは、拡張ゾーン分割機能は Cisco MDS 9000 スイッチはディセーブルです。

SUMMARY STEPS

1. **configure terminal**
2. **zone mode enhanced vsan** *vsan-id*
3. **no zone mode enhanced vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**zone mode enhanced vsan** *vsan-id* **Example:** `switch(config)# zone mode enhanced vsan 22`	指定された VSAN で拡張ゾーン分割をイネーブルにします。
ステップ 3	**no zone mode enhanced vsan** *vsan-id* **Example:** `switch(config)# no zone mode enhanced vsan 30`	指定された VSAN で拡張ゾーン分割をディセーブルにします。

ゾーン データベースの変更

VSAN 内のゾーン分割データベースに対する変更をコミットまたは廃棄できます。

ゾーンデータベースに対する変更は、セッション内で実行されます。セッションは、コンフィギュレーションコマンドが初めて正常に実行されたときに作成されます。セッションが作成されると、ゾーン データベースのコピーが作成されます。セッションでの変更は、ゾーン分割データベースのコピー上で実行されます。ゾーン分割データベースのコピー上で行われる変更は、コミットするまで有効なゾーン分割データベースには適用されません。変更を適用すると、セッションはクローズします。

ファブリックが別のユーザーによってロックされ、何らかの理由でロックがクリアされない場合は、強制的に実行し、セッションをクローズします。このスイッチでロックをクリアする権限（ロール）が必要です。また、この操作は、セッションが作成されたスイッチから実行する必要があります。

SUMMARY STEPS

1. **configure terminal**
2. **zone commit vsan** *vsan-id*
3. switch(config)# **zone commit vsan** *vsan-id* **force**
4. switch(config)# **no zone commit vsan** *vsan-id*
5. **no zone commit vsan** *vsan-id* **force**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**zone commit vsan** *vsan-id* **Example:** `switch(config)# zone commit vsan 679`	拡張ゾーンデータベースに変更を適用し、セッションをクローズします。
ステップ 3	switch(config)# **zone commit vsan** *vsan-id* **force** **Example:** `switch(config)# zone commit vsan 34 force`	拡張ゾーンデータベースに変更を強制的に適用し、別のユーザーが作成したセッションをクローズします。
ステップ 4	switch(config)# **no zone commit vsan** *vsan-id* **Example:** `switch(config)# no zone commit vsan 22`	拡張ゾーン データベースへの変更を廃棄し、セッションをクローズします。
ステップ 5	**no zone commit vsan** *vsan-id* **force** **Example:** `switch(config)# no zone commit vsan 34 force`	拡張ゾーン データベースへの変更を強制的に廃棄し、別のユーザーが作成したセッションをクローズします。

ゾーン データベース ロックの解除

VSAN 内のスイッチのゾーン分割 データベースのセッション ロックを解除するには、最初にデータベースをロックしたスイッチから **no zone commit vsan** コマンドを使用します。

```
switch# configure terminal
switch(config)# no zone commit vsan 2
```

no zone commit vsan コマンドを実行したあとも、リモート スイッチ上でセッションがロックされたままの場合、リモート スイッチ上で **clear zone lock vsan** コマンドを使用できます。

```
switch# clear zone lock vsan 2
```

Note ファブリック内のセッション ロックを解除するには、最初に **no zone commit vsan** コマンドを使用することを推奨します。それが失敗した場合には、セッションがロックされたままのリモート スイッチで、**clear zone lock vsan** コマンドを使用してください。

拡張ゾーン情報の確認

次に、指定された VSAN のゾーン ステータスを表示する例を示します。

```
switch# show zone status vsan 2
```

データベースのマージ

結合方式は、ファブリック全体の結合制御設定によって異なります。

- 制限：2 つのデータベースが同一でない場合、スイッチ間の ISL は分離されます。
- 許可：2 つのデータベースは、次の表で指定された結合規則を使用して結合されます。

Table 27: データベースのゾーン結合ステータス

ローカル データベース	隣接データベース	結合ステータス	結合結果
データベースには同じ名前のゾーン セットが含まれます。拡張ゾーン分割モードでは、interop モード 3 のアクティブ ゾーン セットには名前がありません。ゾーン セット名はフル ゾーン セットにのみ存在しますが、異なるゾーン、エイリアス、属性グループになります。		成功	データベース mege が成功した場合、ISL は分離されません。
データベースには、同じ name1 を持つものの、異なるメンバーを持つゾーン、FC エイリアス、またはゾーン属性グループ オブジェクトが含まれます。		失敗	ローカル データベースには隣接データベースの情報が存在します。ISL は分離されます。

ローカル データベース	隣接データベース	結合ステータス	結合結果
データなし	データあり	成功	ローカル データベースおよび隣接データベースが結合されます。
データあり	データなし	成功	隣接データベースにはローカル データベースの情報が存在します。

結合プロセスは次のように動作します。

- ソフトウェアがプロトコル バージョンを比較します。プロトコル バージョンが異なる場合、ISL は分離されます。
- プロトコル バージョンが同じである場合、ゾーン ポリシーが比較されます。ゾーン ポリシー（**デフォルト ゾーニング**：許可/拒否、**スマート ゾーニング**：有効/無効、**マージ ポリシー** - 許可/制限を含む）が異なる場合、ISL は分離されます。
- ゾーン結合オプションが同じである場合、結合制御設定に基づいて比較が行われます。
  - 設定が「制限」の場合、アクティブ ゾーン セットとフル ゾーン セットが同じになる必要があります。これらが同じでない場合、リンクは分離されます。
  - 設定が「許可」の場合、結合規則を使用して結合が行われます。

ゾーン マージ制御ポリシーの設定

マージ制御ポリシーを設定できます。

SUMMARY STEPS

1. **configure terminal**
2. **zone merge-control restrict vsan** *vsan-id*
3. **no zone merge-control restrict vsan** *vsan-id*
4. **zone commit vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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。

	Command or Action	Purpose
ステップ 2	**zone merge-control restrict vsan** *vsan-id* **Example:** `switch(config)# zone merge-control restrict vsan 24`	現在のVSANの結合制御設定を「制限」に設定します。
ステップ 3	**no zone merge-control restrict vsan** *vsan-id* **Example:** `switch(config)# no zone merge-control restrict vsan 33`	現在の VSAN の結合制御設定をデフォルトの「許可」に設定します。
ステップ 4	**zone commit vsan** *vsan-id* **Example:** `switch(config)# zone commit vsan 20`	指定されたVSANに対する変更をコミットします。

デフォルトのゾーン ポリシー

デフォルト ゾーン内のトラフィックを許可または拒否できます。

SUMMARY STEPS

1. **configure terminal**
2. **zone default-zone permit vsan** *vsan-id*
3. **no zone default-zone permit vsan** *vsan-id*
4. **zone commit vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**zone default-zone permit vsan** *vsan-id* **Example:** `switch(config)# zone default-zone permit vsan 12`	デフォルト ゾーン メンバへのトラフィック フローを許可します。
ステップ 3	**no zone default-zone permit vsan** *vsan-id* **Example:** `switch(config)# no zone default-zone permit vsan 12`	デフォルト ゾーン メンバへのトラフィック フローを拒否し、出荷時の設定に戻します。

	Command or Action	Purpose
ステップ 4	**zone commit vsan** *vsan-id* **Example:** `switch(config)# zone commit vsan 340`	指定されたVSANに対する変更をコミットします。

システムのデフォルト ゾーン分割設定値の設定

スイッチ上の新しい VSAN のデフォルトのゾーン ポリシーおよびフル ゾーン配信のデフォルト設定値を設定できます。

Note system default zone default-zone permit および system default zone distribute full などのゾーンのデフォルト システム設定は、設定を手動で適用した後に、新しく作成された VSAN でのみ有効になります。これらの設定は、FC セットアップ スクリプトの一部として設定されている場合でも、VSAN 1 に適用されない場合があります。

FC スクリプトを使用してゾーン設定を構成することもできます。FC スクリプトを使用したデフォルトゾーン設定の構成の詳細については *Cisco Nexus 9000* シリーズ *NX-OS* 基本構成ガイドを参照してください。

SUMMARY STEPS

1. **configure terminal**
2. **system default zone default-zone permit**
3. **no system default zone default-zone permit**
4. **system default zone distribute full**
5. **no system default zone distribute full**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**system default zone default-zone permit** **Example:** `switch(config)# system default zone default-zone permit`	スイッチ上の新しい VSAN のデフォルト ゾーン分割ポリシーとして permit（許可）を設定します。

	Command or Action	Purpose
ステップ 3	**no system default zone default-zone permit** **Example:** `switch(config)# no system default zone default-zone permit`	スイッチ上の新しい VSAN のデフォルト ゾーン分割ポリシーとして deny（拒否）（デフォルト）を設定します。
ステップ 4	**system default zone distribute full** **Example:** `switch(config)# system default zone distribute full`	スイッチ上の新しいVSANのデフォルトとして、フルゾーンデータベース配信をイネーブルにします。
ステップ 5	**no system default zone distribute full** **Example:** `switch(config)# no system default zone distribute full`	スイッチ上の新しいVSANのデフォルトとして、フルゾーンデータベース配信をディセーブル（デフォルト）にします。アクティブ ゾーン データベースだけが配信されます。

スマート ゾーン分割の概要

スマートゾーン分割では、従来必要とされていたよりも少ないハードウェア リソースで、大きなゾーンのハードゾーン分割が行われます。従来のゾーン分割方式では、ゾーン内の各デバイスが相互に通信できます。管理者はゾーン設定ガイドラインに従って個々のゾーンを管理する必要があります。スマートゾーン分割では、1 つのターゲット ゾーンへの 1 つのイニシエータを作成する必要がありません。FCNS のデバイス タイプ情報を分析することで、Cisco NX-OS ソフトウェアによりハードウェア レベルで有用な組み合わせが実装されます。使用されていない組み合わせは無視されます。たとえば、イニシエータとイニシエータのペアではなく、イニシエータとターゲットのペアが設定されます。次の場合、デバイスは不明なものとして扱われます。

- デバイスに関して FC4 タイプが登録されいない。
- ゾーン変換時に、デバイスがファブリックにログインしていない。
- ゾーンは作成されているが、イニシエータとターゲットのいずれかまたは両方が指定されていない。

スマート ゾーン内の各デバイスのデバイス タイプ情報は、ファイバ チャネル ネーム サーバー（FCNS）データベースから host、target、または both として自動的に取り込まれます。この情報により、イニシエータ ターゲット ペアが指定され、ハードウェアではそれらのペアだけが設定されるため、スイッチ ハードウェアをより効率的に使用できるようになります。特殊な状況（別のディスク コントローラと通信する必要があるディスク コントローラなど）では、完全な制御を実現するため、スマート ゾーン分割のデフォルトが管理者により上書きされることがあります。

Note

- スマート ゾーン分割は VSAN レベルで有効にできますが、ゾーン レベルで無効にすることもできます。
- DMM、IOA、または SME アプリケーションが有効になっている VSAN では、スマート ゾーン分割はサポートされていません。

スマート ゾーン分割のメンバー設定

次の表に、サポートされているスマート ゾーン分割のメンバー設定を示します。

Table 28: スマート ゾーン分割の設定

機能	サポートあり
PWWN	はい
FCID	はい
FC エイリアス	はい
デバイスエイリアス	はい
インターフェイス	いいえ
IP アドレス	いいえ
シンボル ノード名	いいえ
FWWN	いいえ
ドメイン ID	×

VSAN でのスマート ゾーン分割の有効化

VSAN に対して **smart zoning** を設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **zone smart-zoning enable vsan 1**

VSAN でスマート ゾーン分割を有効にします。

ステップ 3 switch(config)# no **zone smart-zoning enable vsan 1**

VSAN でスマート ゾーン分割を無効にします。

スマート ゾーン分割のデフォルト値の設定

デフォルト値を設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# system default zone smart-zone enable

指定されたデフォルト値に基づいて作成された VSAN でスマート ゾーン分割を有効にします。

ステップ 3 switch(config)# no system default zone smart-zone enable

VSAN でスマート ゾーン分割を無効にします。

スマート ゾーン分割へのゾーンの自動変換

ネーム サーバーからデバイス タイプ情報を取得し、その情報をメンバーに追加するには、次の手順を実行します。これは、ゾーン、ゾーン セット、FC エイリアス、および VSAN のレベルで実行できます。ゾーン セットがスマート ゾーン分割に変換されたら、ゾーン セットをアクティブにする必要があります。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# zone convert smart-zoning fcalias name <alias-name> vsan <vsan no>

FC エイリアス メンバーのデバイス タイプ情報をネーム サーバーから取得します。

Note
zone convert コマンドを実行すると、FC4 タイプは SCSI-FCP になります。SCSI-FCP には、デバイスがイニシエータかターゲットかを決定するビットがあります。イニシエータとターゲットの両方が設定されている場合、デバイスは両方として扱われます。

ステップ 3 switch(config)# zone convert smart-zoning zone name <zone name> vsan <vsan no>

ゾーン メンバーのデバイス タイプ情報をネーム サーバーから取得します。

ステップ 4 switch(config)# zone convert smart-zoning zoneset name <zoneset name> vsan <vsan no>

指定されたゾーンセットで、すべてのゾーンと FC エイリアス メンバーのデバイス タイプ情報をネーム サーバーから取得します。

ステップ 5 switch(config)# zone convert smart-zoning vsan <vsan no>

VSAN 内に存在するすべてのゾーン セットのすべてのゾーンと FC エイリアス メンバーのデバイス タイプ情報をネーム サーバーから取得します。

ステップ 6 switch(config)# show zone smart-zoning auto-conv status vsan 1

VSAN の以前の自動変換ステータスが表示されます。

ステップ 7 switch(config)# show zone smart-zoning auto-conv log errors

スマート ゾーン分割自動変換のエラー ログが表示されます。

What to do next

デバイスがイニシエータ、ターゲット、またはその両方であるかどうかを確認するには、show fcns database コマンドを使用します。

```
switch# show fcns database
VSAN 1:
--------------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x9c0000 N 21:00:00:e0:8b:08:96:22 (Company 1) scsi-fcp:init
0x9c0100 N 10:00:00:05:30:00:59:1f (Company 2) ipfc
0x9c0200 N 21:00:00:e0:8b:07:91:36 (Company 3) scsi-fcp:init
0x9c03d6 NL 21:00:00:20:37:46:78:97 (Company 4) scsi-fcp:target
```

ゾーン メンバーのデバイス タイプの設定

ゾーン メンバーのデバイス タイプを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config-zoneset-zone)# **member device-alias** *name* **both**

デバイス エイリアス メンバーのデバイス タイプを both として設定します。サポートされる各メンバー タイプでは、init、target、および both がサポートされています。

ステップ 3 switch(config-zoneset-zone)# **member pwwn** *number* **target**

pwwn メンバーのデバイス タイプを target として設定します。サポートされる各メンバー タイプでは、init、target、および both がサポートされています。

ステップ 4 switch(config-zoneset-zone)# **member fcid** *number*

FCID メンバーのデバイス タイプを設定します。設定されている特定のデバイス タイプがありません。サポートされる各メンバー タイプでは、init、target、および both がサポートされています。

Note
ゾーン メンバーに対して特定のデバイス タイプが設定されていない場合は、バックエンドで、生成されたゾーン エントリがデバイス タイプ both として作成されます。

スマート ゾーン分割設定の削除

スマート ゾーン分割設定を削除するには、次の手順を実行します。

Procedure

ステップ 1 switch(config)# **clear zone smart-zoning fcalias name** *alias-name* **vsan** *number*

指定された FC エイリアスのすべてのメンバーのデバイス タイプ設定を削除します。

ステップ 2 switch(config)# **clear zone smart-zoning zone name** *zone name* **vsan** *number*

指定されたゾーンのすべてのメンバーのデバイス タイプ設定を削除します。

ステップ 3 switch(config)# **clear zone smart-zoning zoneset name** *zoneset name* **vsan** *number*

指定されたゾーン セットの FC エイリアスとゾーンのすべてのメンバーのデバイス タイプ設定を削除します。

ステップ 4 switch(config)# **clear zone smart-zoning vsan** *number*

VSAN の指定されたゾーン セットの FC エイリアスとゾーンのすべてメンバーのデバイス タイプ設定を削除します。

基本ゾーン分割モードにおけるゾーン レベルでのスマート ゾーン分割の無効化

基本ゾーン分割モードの VSAN に対してゾーン レベルでスマート ゾーン分割を無効にするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **zone name zone1 vsan 1**

ゾーン名を設定します。

ステップ 3 switch(config-zone)# **attribute disable-smart-zoning**

選択されたゾーンに対してスマート ゾーン分割を無効にします。

Note
このコマンドでは、選択されたゾーンのスマート ゾーン分割が無効になるだけです。デバイス タイプ設定は削除されません。

拡張ゾーン分割モードの VSAN に対するゾーン レベルでのスマート ゾーン分割の無効化

拡張ゾーン分割モードの VSAN に対してゾーン レベルでスマート ゾーン分割を無効にするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **zone-attribute-group name disable-sz vsan 1**

拡張ゾーン セッションを作成します。

ステップ 3 switch(config-attribute-group)#**disable-smart-zoning**

選択されたゾーンに対してスマート ゾーン分割を無効にします。

Note
このコマンドでは、選択されたゾーンのスマート ゾーン分割が無効になるだけです。デバイス タイプ設定は削除されません。

ステップ 4 switch(config-attribute-group)# **zone name prod vsan 1**

ゾーン名を設定します。

ステップ 5 switch(config-zone)# **attribute-group disable-sz**

選択されたゾーンのグループ属性名を割り当てるように設定します。

ステップ 6 switch(config-zone)# **zone commit vsan 1**

選択された VSAN に対するゾーン分割の変更を確定します。

ゾーン データベースの圧縮

過剰なゾーンを削除し、VSAN のゾーン データベースを圧縮できます。

Note スイッチが VSAN あたり 2000 を超えるゾーンをサポートしていても、ネイバーがサポートしていない場合、結合は失敗します。また、そのスイッチが VSAN あたり 2000 を超えるゾーンをサポートしていても、ファブリック内のすべてのスイッチが VSAN あたり 2000 を超えるゾーンをサポートしていない場合には、ゾーンセットのアクティブ化に失敗することがあります。

SUMMARY STEPS

1. **configure terminal**
2. **no zone name** *zone-name* **vsan** *vsan-id*
3. **zone compact vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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 zone name** *zone-name* **vsan** *vsan-id* **Example:** `switch(config)# no zone name myzone vsan 35`	ゾーンを削除し、ゾーン数を 2000 以下にします。
ステップ 3	**zone compact vsan** *vsan-id* **Example:** `switch(config)# zone compact vsan 42`	指定された VSAN のゾーン データベースを圧縮し、ゾーンが削除されたときに開放されたゾーン ID を回復します。

ゾーンおよびゾーン セットの分析

スイッチ上のゾーンおよびゾーン セットをより的確に管理するために、**show zone analysis** コマンドを使用して、ゾーン情報とゾーン セット情報を表示できます。

次に、フル ゾーン分割の分析を表示する例を示します。

```
switch# show zone analysis vsan 1
```

次に、アクティブ ゾーニングの分析を表示する例を示します。

```
switch# show zone analysis active vsan 1
```

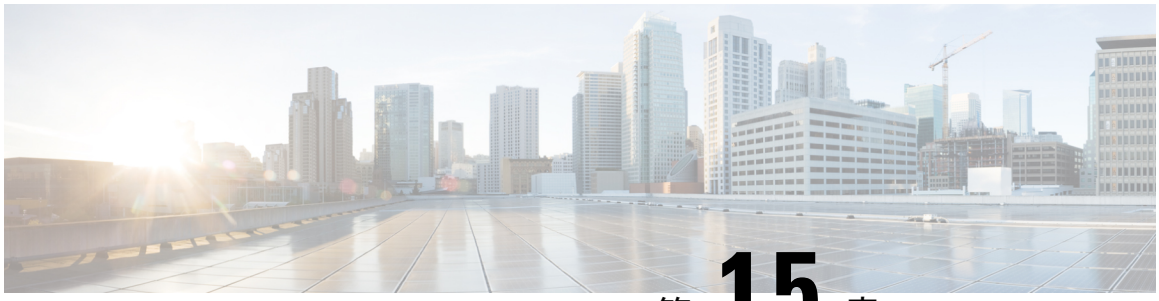
コマンド出力に表示される情報の詳細については、ご使用のデバイスの『Command Reference』を参照してください。

ゾーンのデフォルト設定

次の表に、基本ゾーン パラメータのデフォルト設定を示します。

Table 29: デフォルトの基本ゾーン パラメータ

パラメータ	デフォルト
デフォルト ゾーン ポリシー	すべてのメンバで拒否
フル ゾーン セット配信	フル ゾーン セットは配信されない
拡張ゾーン分割	ディセーブル



第 15 章

拡張ファイバ チャネル機能

この章では、拡張ファイバ チャネル機能を設定する方法について説明します。

この章は、次の項で構成されています。

拡張ファイバ チャネル機能および概念

ファイバ チャネル タイムアウト値

ファイバ チャネル プロトコルに関連するスイッチのタイマー値を変更するには、次のタイムアウト値（TOV）を設定します。

- Distributed Services TOV（D_S_TOV）：有効範囲は 5,000 ～ 10,000 ミリ秒です。
- Error Detect TOV（E_D_TOV）：有効範囲は 1,000 ～ 4,000 ミリ秒です。デフォルトは 2,000 ミリ秒です。この値は、ポート初期化中に他端と比較されます。
- Resource Allocation TOV（R_A_TOV）：有効範囲は 5,000 ～ 10,000 ミリ秒です。デフォルトは 10,000 ミリ秒です。この値は、ポート初期化中に他端と比較されます。

Note Fabric Stability TOV（F_S_TOV）定数は設定できません。

すべての VSAN のタイマー設定

ファイバ チャネル プロトコルに関連するスイッチのタイマー値を変更できます。

Caution D_S_TOV、E_D_TOV、および R_A_TOV 値をグローバルに変更するには、スイッチのすべての VSAN（仮想 SAN）を中断する必要があります。

Note タイマー値を変更するときにVSANを指定しない場合は、変更された値がスイッチ内のすべての VSAN に適用されます。

すべての VSAN にファイバ チャネル タイマーを設定できます。

SUMMARY STEPS

1. **configure terminal**
2. **fctimer R_A_TOV** *timeout*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**fctimer R_A_TOV** *timeout* **Example:** `switch(config)# fctimer R_A_TOV 8008000`	すべての VSAN の R_A_TOV タイムアウト値を設定します。単位はミリ秒です。 このタイプの設定は、すべてのVSANが一時停止されていないかぎり、許可されません。

VSAN ごとのタイマー設定

指定された VSAN に fctimer を発行して、ファイバ チャネルなどの特殊なリンクを含む VSAN に別の TOV 値を設定することもできます。VSAN ごとに異なる E_D_TOV、R_A_TOV、および D_S_TOV 値を設定できます。アクティブ VSAN のタイマー値を変更すると、VSAN は一時停止されてからアクティブになります。

Note この設定はファブリック内のすべてのスイッチに伝播させる必要があります。ファブリック内のすべてのスイッチに同じ値を設定してください。

VSAN ファイバチャネル タイマーごとに設定できます。

SUMMARY STEPS

1. **configure terminal**
2. **fctimer D_S_TOV** *timeout* **vsan** *vsan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**fctimer D_S_TOV** *timeout* **vsan** *vsan-id* **Example:** `switch(config#)# fctimer D_S_TOV 9009000 vsan 15`	指定された VSAN の D_S_TOV タイムアウト値（ミリ秒）を設定します。VSAN が一時的に停止します。必要に応じて、このコマンドを終了することもできます。

例

次に、VSAN 2 のタイマー値を設定する例を示します。

```
switch(config#)# fctimer D_S_TOV 6000 vsan 2
Warning: The vsan will be temporarily suspended when updating the timer value This
configuration would impact whole fabric. Do you want to continue? (y/n) y
Since this configuration is not propagated to other switches, please configure the same
value in all the switches
```

fctimer の配布

ファブリック内のすべての Cisco SAN スイッチに対して、VSAN 単位での fctimer のファブリック配布をイネーブルにできます。fctimer の設定を実行して、配布をイネーブルにすると、ファブリック内のすべてのスイッチにその設定が配布されます。

スイッチの配布をイネーブルにしたあとで最初のコンフィギュレーション コマンドを入力すると、ファブリック全体のロックを自動的に取得します。fctimer アプリケーションは、有効データベースと保留データベース モデルを使用し、使用中のコンフィギュレーションに基づいてコマンドを格納またはコミットします。

Note CFS はデフォルトでイネーブルです。ファブリックのすべてのデバイスでは CFS が有効になっている必要があります。そうでない場合、デバイスは配信を受け入れません。アプリケーションで CFS 配信が無効にされている場合、そのアプリケーションは構成を配信せず、またファブリック内の他のデバイスからの配信も受け入れません。CFS を有効にするには、**cfs distribute** コマンドを使用します。

追加情報については、ご使用のデバイスの『System Management Configuration Guide』の「Using Cisco Fabric Services」を参照してください。

fctimer の配布の有効化と無効化

fctimer のファブリック配布をイネーブルまたはディセーブルにできます。

SUMMARY STEPS

1. **configure terminal**
2. **fctimer distribute**
3. **no fctimer distribute**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**fctimer distribute** **Example:** `switch(config)# fctimer distribute`	ファブリック内のすべてのスイッチに対する fctimer 設定の配布をイネーブルにします。ファブリックのロックを取得して、その後の設定変更をすべて保留データベースに格納します。
ステップ 3	**no fctimer distribute** **Example:** `switch(config)# no fctimer distribute`	ファブリック内のすべてのスイッチに対する fctimer 設定の配布をディセーブル（デフォルト）にします。

fctimer 設定変更のコミット

fctimerの設定変更をコミットすると、有効データベースは保留データベースの設定変更によって上書きされ、ファブリック内のすべてのスイッチが同じ設定を受け取ります。セッション機能を実行せずに fctimer の設定変更をコミットすると、fctimer 設定は物理ファブリック内のすべてのスイッチに配布されます。

SUMMARY STEPS

1. **configure terminal**
2. **fctimer commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**fctimer commit** **Example:** `switch(config)# fctimer commit`	ファブリック内のすべてのスイッチに対して fctimer の設定変更を配布し、ロックを解除します。保留データベースに対する変更を有効データベースに上書きします。

fctimer 設定変更の廃棄

設定変更を加えたあと、変更内容をコミットする代わりに廃棄すると、この変更内容を廃棄できます。いずれの場合でも、ロックは解除されます。

SUMMARY STEPS

1. **configure terminal**
2. **fctimer abort**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**fctimer abort** **Example:** `switch(config)# fctimer abort`	保留データベースの fctimer の設定変更を廃棄して、ファブリックのロックを解除します。

ファブリック ロックの上書き

ユーザーが fctimer を設定して、変更のコミットや廃棄を行ってロックを解除するのを忘れていた場合、管理者はファブリック内の任意のスイッチからロックを解除できます。管理者がこの操作を行うと、ユーザーによる保留データベースの変更は廃棄され、ファブリックのロックは解除されます。

変更は volatile ディレクトリだけで使用でき、スイッチを再起動すると廃棄されます。

管理者特権を使用して、ロックされた fctimer セッションを解除するには、**clear fctimer session** コマンドを使用します。

```
switch# clear fctimer session
```

ファブリック データベースの結合の注意事項

2 つのファブリックを結合する場合は、次の注意事項に従ってください。

- 次の結合条件を確認します。
  - fctimer 値を配布する結合プロトコルが実行されない。ファブリックを結合する場合、fctimer 値を手動で結合する必要があります。
  - VSAN 単位の fctimer 設定は物理ファブリック内で配布される。
  - fctimer 設定は、変更された fctimer 値を持つ VSAN が含まれるスイッチだけに適用される。
  - グローバルな fctimer 値は配布されない。
- 配布がイネーブルになっている場合は、グローバル タイマーの値を設定しないでください。

Note 保留できる fctimer 設定操作の回数は 15 回以内です。15 回を超えて設定操作を行う場合には、保留設定をコミットするか、中止する必要があります。

追加情報については、ご使用のデバイスの『System Management Configuration Guide』の「CFS Merge Support」を参照してください。

構成された fctimer 値の確認

構成された fctimer 値を表示するには、**show fctimer** コマンドを使用します。次に、設定されているグローバル タイムアウト値（TOV）を表示する例を示します。

```
switch# show fctimer
F_S_TOV   D_S_TOV   E_D_TOV   R_A_TOV
----------------------------------------
5000 ms   5000 ms   2000 ms   10000 ms
```

Note **show fctimer** コマンドの出力には、（構成されていない場合でも）F_S_TOV 定数が表示されます。

次の例では、VSAN 10 の構成済み TOV が表示されています。

```
switch# show fctimer vsan 10
```

```
vsan no.  F_S_TOV   D_S_TOV   E_D_TOV   R_A_TOV
-------------------------------------------------
10        5000 ms   5000 ms   3000 ms   10000 ms
```

World Wide Names（WWN）

スイッチの World Wide Name（WWN）は、イーサネット MAC アドレスと同等です。MAC アドレスと同様に、デバイスごとにWWNを一意に対応付ける必要があります。主要スイッチを選択するとき、およびドメイン ID を割り当てるときは、WWN を使用します。

Cisco SAN スイッチは、3 つの Network Address Authority（NAA）アドレス フォーマットをサポートします（次の表を参照してください）。

Table 30: 標準化された ***NAA WWN*** フォーマット

NAA アドレス	**NAA タイプ**	**WWN フォーマット**	
IEEE 48 ビット アドレス	タイプ1 = 0001b	000 0000 0000b	48 ビット MAC アドレス
IEEE 拡張	タイプ2 = 0010b	ローカルに割り当て	48 ビット MAC アドレス
IEEE 登録	タイプ5 = 0101b	IEEE 企業 ID：24 ビット	VSID：36 ビット

Caution WWN の変更は、管理者または、スイッチの操作に精通した担当者が実行してください。

WWN 設定の確認

WWN 設定のステータスを表示するには、**show wwn** コマンドを使用します。次に、すべての WWN のステータスを表示する例を示します。

```
switch# show wwn status
Type    Configured     Available    Resvd.  Alarm State
----    ----------  --------------  ------  -----------
   1           64        48 ( 75%)      16    NONE
 2,5       524288    442368 ( 84%)   73728    NONE
```

次に、ブロック ID 51 の情報を表示する例を示します。

```
switch# show wwn status block-id 51
WWNs in this block: 21:00:ac:16:5e:52:00:03 to 21:ff:ac:16:5e:52:00:03
Num. of WWNs:: Configured: 256 Allocated:    0 Available: 256
Block Allocation Status: FREE
```

次に、特定のスイッチの WWN を表示する例を示します。

```
switch# show wwn switch
Switch WWN is 20:00:ac:16:5e:52:00:00
```

リンク初期化 WWN の使用方法

Exchange Link Protocol（ELP）および Exchange Fabric Protocol（EFP）は、リンク初期化の際に WWN を使用します。ELP と EFP はどちらも、デフォルトでは、リンク初期化時に VSAN WWN を使用します。ただし、ELP の使用方法はピア スイッチの使用方法に応じて変わります。

- ピア スイッチの ELP がスイッチの WWN を使用する場合、ローカル スイッチもスイッチの WWN を使用します。
- ピア スイッチの ELP が VSAN の WWN を使用する場合、ローカル スイッチも VSAN の WWN を使用します。

セカンダリ MAC アドレスの設定

セカンダリ MAC アドレスを割り当てることができます。

SUMMARY STEPS

1. **configure terminal**
2. **wwn secondary-mac** *wwn-id* **range** *value*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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	**wwn secondary-mac** *wwn-id* **range** *value* **Example:** `switch(config)# wwn secondary-mac 33:e8:00:05:30:00:16:df range 55`	セカンダリ MAC アドレスを設定します。このコマンドは元に戻せません。

例

次に、セカンダリ MAC アドレスを設定する例を示します。

```
switch(config)# wwn secondary-mac 00:99:55:77:55:55 range 64
This command CANNOT be undone.
Please enter the BASE MAC ADDRESS again: 00:99:55:77:55:55
Please enter the mac address RANGE again: 64
```

```
From now on WWN allocation would be based on new MACs. Are you sure? (yes/no) no
You entered: no. Secondary MAC NOT programmed
```

HBA の FC ID 割り当て

ファイバ チャネル標準では、任意のスイッチの F ポートに接続された N ポートに、一意の FC ID を割り当てる必要があります。使用する FC ID 番号を節約するために、Cisco SAN スイッチでは特殊な割り当て方式を使用しています。

一部の Host Bus Adapter（HBA）は、ドメインとエリアが同じ FC ID を持つターゲットを検出しません。スイッチ ソフトウェアは、この動作が発生しないテスト済みの企業 ID のリストを保持しています。これらの HBA には単一の FC ID が割り当てられます。HBA が同じドメインおよびエリア内のターゲットを検出できる場合、完全なエリアが割り当てられます。

多数のポートを持つスイッチのスケーラビリティを高めるため、スイッチ ソフトウェアは、同じドメインおよびエリア内のターゲットを検出できる HBA のリストを維持しています。各 HBA は、ファブリック ログイン時に pWWN で使用される会社 ID（組織固有識別子（OUI）とも呼ばれます）によって識別されます。リストされている会社 ID を持つ N ポートに完全な領域が割り当てられ、その他の場合は、単一の FC ID が割り当てられます。割り当てられる FC ID のタイプ（エリア全体または単一）に関係なく、FC ID エントリは永続的です。

デフォルトの企業 ID リスト

すべての Cisco SAN スイッチには、エリア割り当てが必要な企業 ID のデフォルト リストが含まれています。この企業 ID を使用すると、設定する永続的 FC ID エントリの数が少なくなります。これらのエントリは、CLI を使用して設定または変更できます。

⚠

Caution 永続的エントリは、企業 ID の設定よりも優先されます。HBA がターゲットを検出しない場合は、HBA とターゲットが同じスイッチに接続され、FC ID のエリアが同じであることを確認してから、次の手順を実行します。

1. HBA に接続されているポートをシャットダウンします。
2. 永続的 FC ID エントリをクリアします。
3. ポート WWN から企業 ID を取得します。
4. エリア割り当てを必要とするリストに企業 ID を追加します。
5. ポートをアップにします。

企業 ID のリストには、次の特性があります。

- 永続的 FC ID の設定は常に企業 ID リストよりも優先されます。エリアを受け取るように企業 ID が設定されている場合でも、永続的 FC ID の設定によって単一の FC ID が割り当てられます。
- 後続のリリースに追加される新規の企業 ID は、既存の企業 ID に自動的に追加されます。

- 企業IDのリストは、実行コンフィギュレーションおよび保存されたコンフィギュレーションの一部として保存されます。
- 企業 ID のリストが使用されるのは、fcinterop の FC ID 割り当て方式が auto モードの場合だけです。変更されないかぎり、interop の FC ID 割り当ては、デフォルトで auto に設定されています。

Tip fcinterop の FC ID 割り当て方式を auto に設定し、企業 ID リストと永続的 FC ID 設定を使用して、FC ID のデバイス割り当てを行うことをお勧めします。

FC ID の割り当てを変更するには、**fcinterop FCID allocation auto** コマンドを使用し、現在割り当てられているモードを表示するには、**show running-config** コマンドを使用します。

- **write erase** を入力すると、リストは該当するリリースに付属している企業 ID のデフォルト リストを継承します。

企業 ID の設定の確認

設定された企業 ID を表示するには、**show fcid-allocation area** コマンドを使用します。最初にデフォルトエントリが表示され、次にユーザーによって追加されたエントリが表示されます。エントリがデフォルト リストの一部で、あとで削除された場合でも、エントリは表示されます。

次に、デフォルトおよび設定された企業 ID のリストを表示する例を示します。

```
switch# show fcid-allocation area
FCID area allocation company id info:
00:50:2E <--------------- Default entry
00:50:8B
00:60:B0
00:A0:B8
00:E0:69
00:30:AE + <------------- User-added entry
00:32:23 +
00:E0:8B * <------------- Explicitly deleted entry (from the original default list)
Total company ids: 7
+ - Additional user configured company ids.
* - Explicitly deleted company ids from default list.
```

削除済みエントリの印が付いていない企業 ID のリストを組み合わせると、特定のリリースに付属するデフォルト エントリを暗黙的に導き出すことができます。

また、**show fcid-allocation company-id-from-wwn** コマンドを使用すると、特定の WWN の企業 ID を表示または取得することもできます。一部の WWN 形式では、企業 ID がサポートされていません。この場合、FC ID の永続的エントリを設定する必要があります。

次に、指定された WWN の企業 ID を表示する例を示します。

```
switch# show fcid-allocation company-id-from-wwn 20:00:00:05:30:00:21:60
Extracted oui: 0x000530
```

スイッチの相互運用性

相互運用性を使用すると、複数ベンダーによる製品の間で相互に通信することができます。ファイバチャネル標準規格では、ベンダーに対して共通の外部ファイバチャネルインターフェイスを使用することを推奨しています。

同じ方法で標準規格に準拠していないベンダーもあるため、相互運用モードが必要になります。ここでは、これらのモードの基本的な概念について簡単に説明します。

各ベンダーには標準モード、および同等の相互運用モードがあります。相互運用モードでは拡張機能または独自の機能が無効になり、標準に準拠した実装が可能になります。

Note Cisco Nexus デバイス スイッチでの相互運用性の設定方法に関する詳細は、*Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide* を参照してください。

Interop モードの概要

ソフトウェアは、1 つの相互運用モード（モード 3—Brocade ネイティブ モード （コア PID 1））のみをサポートします。相互運用モードのモード 3 では、ネイティブ モードを変更することなく、コア PID 1（Brocade ネイティブ モード）の Brocade スイッチをシームレスに追加できます。その他すべての機能は同じままです。

- モード 1：標準ベースの interop モード。ファブリック内の他のベンダー製品もすべて interop モードになっている必要があります。
- モード 2：Brocade ネイティブ モード（Core PID 0）
- モード 3：Brocade ネイティブ モード（Core PID 1）
- モード 4：McData ネイティブ モード

interop モード 2、3、および 4 の設定方法については、次の URL にある *Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide* を参照してください。http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/interoperability/guide/intopgd.html

次の表に、相互運用性モードを有効にした場合のスイッチ動作の変更点を示します。これらは、interop モードの Cisco Nexus デバイス スイッチに固有の変更点です。

Table 31: 相互運用モードが有効の場合のスイッチ動作の変更点

スイッチ機能	相互運用モードがイネーブルの場合の変更点
ドメイン ID	一部のベンダーは、ファブリック内の239のドメインを完全には使用できません。 ドメイン ID は 97 ～ 127 の範囲に制限されます。これは、McData の公称制限をこの同じ範囲内に収めるためです。ドメイン ID は Static または Preferred に設定できます。それぞれの動作は次のとおりです。 • Static：シスコ スイッチは 1 つのドメイン ID だけを受け入れ、そのドメイン ID を取得できない場合には、ファブリックから隔離します。 • Preferred：スイッチが要求したドメイン ID を取得できない場合、割り当てられた任意のドメインを受け入れます。
タイマー	ISL（スイッチ間リンク）を確立するときにファイバチャネル タイマー値が E ポートで交換されるので、すべてのスイッチでこれらのタイマーをすべて同じにする必要があります。タイマーには、F_S_TOV、D_S_TOV、E_D_TOV、および R_A_TOV があります。
F_S_TOV	Fabric Stability TOV タイマーが正確に一致するかどうかを確認してください。
D_S_TOV	Distributed Services TOV タイマーが正確に一致するかどうかを確認してください。
E_D_TOV	Error Detect TOV タイマーが正確に一致するかどうかを確認してください。
R_A_TOV	Resource Allocation TOV タイマーが正確に一致するかどうかを確認してください。
トランキング	2 つの異なるベンダー製のスイッチ間では、トランキングはサポートされません。この機能は、ポート単位またはスイッチ単位で無効にできます。
デフォルト ゾーン	ゾーンのデフォルトの許可動作（すべてのノードから他のすべてのノードを認識可能）または拒否動作（明示的にゾーンに配置されていないすべてのノードが隔離される）は変更できます。

スイッチ機能	相互運用モードがイネーブルの場合の変更点
ゾーン分割属性	ゾーンを pWWN に制限したり、その他の独自のゾーン分割方式（物理ポート番号）を除去することができます。 **Note** Brocade スイッチでは、**cfgsave**コマンドを使用して、ファブリック全体のゾーン分割設定を保存します。このコマンドは、同じファブリックに属する Cisco SAN スイッチには影響を及ぼしません。各 Cisco SAN スイッチで明示的に設定を保存する必要があります。
ゾーンの伝播	一部のベンダーは、他のスイッチに完全なゾーン設定を受け渡さないで、アクティブ ゾーン セットだけを受け渡します。 ファブリック内の他のスイッチにアクティブゾーンセットまたはゾーン設定が正しく伝播されたかどうかを確認してください。
VSAN	interop モードは、指定された VSAN にだけ有効です。
TE ポートおよび SAN ポート チャネル	シスコ スイッチと Cisco SAN 以外のスイッチを接続する場合は、TE ポートおよび SAN ポート チャネルを使用できません。Cisco SAN 以外のスイッチに接続できるのは、E ポートだけです。interop モードの場合でも、TE ポートおよび SAN ポート チャネルを使用すると、シスコ スイッチをほかの Cisco SAN スイッチに接続することができます。
FSPF	interop モードにしても、ファブリック内のフレームのルーティングは変更されません。スイッチは引き続き src-id、dst-id、および ox-id を使用して、複数の ISL リンク間でロード バランスします。
ドメインの中断再設定	これは、スイッチ全体に影響するイベントです。Brocade および McData では、ドメイン ID を変更するときにスイッチ全体をオフライン モードにしたり、再起動したりする必要があります。
ドメインの非中断再設定	これは、関連する VSAN に限定されるイベントです。Cisco SAN スイッチには、スイッチ全体ではなく、関連する VSAN のドメイン マネージャ プロセスだけを再起動する機能が組み込まれています。
ネーム サーバー	すべてのベンダーのネーム サーバー データベースに正しい値が格納されているかを確認してください。

interop モード 3 の設定

Cisco SAN スイッチの interop モード 3 を中断または非中断に構成できます。

Note Brocade スイッチから Cisco SAN スイッチまたは McData スイッチに接続する前に、Brocade の **msplmgmtdeactivate** コマンドを明示的に実行する必要があります。このコマンドは Brocade 独自のフレームを使用して、Cisco SAN スイッチまたは McData スイッチが認識しないプラットフォーム情報を交換します。これらのフレームを拒否すると、一般的な E ポートが隔離されます。

Procedure

	Command or Action	Purpose
ステップ 1	他ベンダー製スイッチに接続する E ポートの VSAN を相互運用モードにします。	`switch# configuration terminal` `switch(config)# vsan database` `switch(config-vsan-db)# vsan 10 interop 3` `switch(config-vsan-db)# exit`
ステップ 2	97（0x61）～ 127（0x7F）の範囲でドメイン ID を割り当てます。	**Note** これは、McData スイッチに適用される制限です。 Cisco SAN スイッチの場合、デフォルトでは、主要スイッチから ID が要求されます。Preferred オプションを使用した場合、Cisco SAN スイッチは固有の ID を要求しますが、主要スイッチから別の ID が割り当てられた場合もファブリックに参加します。Static オプションを使用した場合、要求された ID を主要スイッチが承認して、これを割り当てないかぎり、Cisco SAN スイッチはファブリックに参加しません。 **Note** ドメイン ID を変更すると、N ポートに割り当てられた FC ID も変更されます。
ステップ 3	FC タイマーを変更します（システム デフォルトから変更された場合）。	**Note** Cisco SAN スイッチ、Brocade、および McData の FC Error Detect（ED_TOV）と Resource Allocation（RA_TOV）のタイマーは、デフォルトで同一の値に設定されています。これらの値は、必要に応じて変更できます。RA_TOV のデフォルト値は 10 秒、ED_TOV のデフォルト値は 2 秒です。FC-SW2 標準に基づく場合、これらの値は、ファブリック内の各スイッチで一致している必要があります。 `switch(config)# fctimer e_d_tov ?` `<1000-100000> E_D_TOV in milliseconds(1000-100000)`

	Command or Action	Purpose
		switch(config)# **fctimer r_a_tov ?** <1000-4000> E_D_TOV in milliseconds(1000-4000)
ステップ 4	ドメインを変更するときに、変更されたVSANのドメインマネージャ機能の再起動が必要な場合と、不要な場合があります。	• **disruptive** オプションを使用して、ファブリックを強制的に再設定する場合は次のようになります。 switch(config)# **fcdomain restart disruptive vsan 1** または • ファブリックを強制的に再設定しない場合は次のようになります。 switch(config# **fcdomain restart vsan 10**

相互運用ステータスの確認

ここでは、ファブリックが起動していて、相互運用モードで稼働していることを確認するためのコマンドについて説明します。

任意の Cisco Nexus デバイス で相互運用性コマンドを入力した場合のステータスを確認する手順は、次のとおりです。

SUMMARY STEPS

1. ソフトウェア バージョンを確認します。
2. インターフェイスの状態が使用中の設定に必要な状態になっているかどうかを確認します。
3. 目的のコンフィギュレーションが稼働しているかどうかを確認します。
4. 相互運用性モードがアクティブであるかどうかを確認します。
5. ドメイン ID を確認します。
6. ローカル主要スイッチのステータスを確認します。
7. スイッチのネクスト ホップおよび宛先を確認します。
8. ネーム サーバ情報を確認します。

DETAILED STEPS

Procedure

ステップ 1 ソフトウェア バージョンを確認します。

Example:

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2008, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.
Software
  BIOS:      version 1.2.0
  loader:    version N/A
  kickstart: version 4.0(1a)N1(1)
  system:    version 4.0(1a)N1(1)
  BIOS compile time:       06/19/08
  kickstart image file is: bootflash:/n5000-uk9-kickstart.4.0.1a.N1.latest.bin
  kickstart compile time:  11/25/2008 6:00:00 [11/25/2008 14:17:12]
  system image file is:    bootflash:/n5000-uk9.4.0.1a.N1.latest.bin
  system compile time:     11/25/2008 6:00:00 [11/25/2008 14:59:49]
Hardware
  cisco Nexus5020 Chassis ("40x10GE/Supervisor")
  Intel(R) Celeron(R) M CPU with 2074308 kB of memory.
  Processor Board ID JAB120900PJ
  Device name: switch
  bootflash: 1003520 kB
Kernel uptime is 0 day(s), 1 hour(s), 29 minute(s), 55 second(s)
Last reset at 510130 usecs after Wed Nov 26 18:12:23 2008
  Reason: Reset Requested by CLI command reload
  System version: 4.0(1a)N1(1)
  Service:
plugin
  Core Plugin, Ethernet Plugin
```

ステップ2 インターフェイスの状態が使用中の設定に必要な状態になっているかどうかを確認します。

Example:

```
switch# show interface brief
--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                 Mode   Trunk                          Mode  Speed  Channel
                        Mode                                (Gbps)
```

```
--------------------------------------------------------------------------------
fc3/1      1      E      on      trunking         swl    TE      2    --
fc3/2      1      auto   on      sfpAbsent        --     --           --
fc3/3      1      E      on      trunking         swl    TE      2    --
fc3/4      1      auto   on      sfpAbsent        --     --           --
fc3/5      1      auto   auto    notConnected     swl    --           --
fc3/6      1      auto   on      sfpAbsent        --     --           --
fc3/7      1      auto   auto    sfpAbsent        --     --           --
fc3/8      1      auto   auto    sfpAbsent        --     --           --
```

ステップ 3 目的のコンフィギュレーションが稼働しているかどうかを確認します。

Example:

```
switch# show running-config
Building Configuration...
 interface fc2/1
no shutdown
 interface fc2/2
no shutdown
 interface fc2/3
 interface fc2/4
<snip>
interface mgmt0
ip address 6.1.1.96 255.255.255.0
switchport encap default
no shutdown
vsan database
vsan 1 interop
boot system bootflash:/nx5000-system-23e.bin
boot kickstart bootflash:/nx5000-kickstart-23e.bin
callhome
fcdomain domain 100 preferred vsan 1
ip route 6.1.1.0 255.255.255.0 6.1.1.1
ip routing
line console
  databits 5
  speed 110
logging linecard
ssh key rsa 512 force
ssh server enable
switchname switch
```

```
username admin password 5 $1$Li8/fBYX$SNc72.xt4nTXpSnR9OUFB/ role network-admin
```

ステップ 4 相互運用性モードがアクティブであるかどうかを確認します。

Example:

```
switch# show vsan 1
vsan 1 information
         name:VSAN0001  state:active
         interoperability mode:yes <-------------------- verify mode
         loadbalancing:src-id/dst-id/oxid
         operational state:up
```

ステップ 5 ドメイン ID を確認します。

Example:

```
switch# show fcdomain vsan 1
The local switch is a Subordinated Switch.
Local switch run time information:
        State: Stable
        Local switch WWN:    20:01:00:05:30:00:51:1f
        Running fabric name: 10:00:00:60:69:22:32:91
        Running priority: 128
        Current domain ID: 0x64(100) <---------------verify domain id
Local switch configuration information:
        State: Enabled
        Auto-reconfiguration: Disabled
        Contiguous-allocation: Disabled
        Configured fabric name: 41:6e:64:69:61:6d:6f:21
        Configured priority: 128
        Configured domain ID: 0x64(100) (preferred)
Principal switch run time information:
        Running priority: 2
Interface               Role          RCF-reject
----------------    -------------    ------------
fc2/1               Downstream       Disabled
fc2/2               Downstream       Disabled
fc2/4               Upstream         Disabled
----------------    -------------    ------------
```

ステップ 6 ローカル主要スイッチのステータスを確認します。

Example:

```
switch# show fcdomain domain-list vsan 1
Number of domains: 5
```

```
Domain ID              WWN
---------    -----------------------
 0x61(97)    10:00:00:60:69:50:0c:fe
 0x62(98)    20:01:00:05:30:00:47:9f
 0x63(99)    10:00:00:60:69:c0:0c:1d
0x64(100)    20:01:00:05:30:00:51:1f [Local]
0x65(101)    10:00:00:60:69:22:32:91 [Principal]
---------    -----------------------
```

ステップ 7 スイッチのネクスト ホップおよび宛先を確認します。

Example:

```
switch# show fspf internal route vsan 1
FSPF Unicast Routes
---------------------------
 VSAN Number  Dest Domain   Route Cost    Next hops
---------------------------------------------
           1     0x61(97)          500      fc2/2
           1     0x62(98)         1000      fc2/1
                                           fc2/2
           1     0x63(99)          500      fc2/1
           1    0x65(101)         1000      fc2/4
```

ステップ 8 ネーム サーバ情報を確認します。

Example:

```
switch# show fcns data vsan 1
VSAN 1:
-----------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR) FC4-TYPE:FEATURE
-----------------------------------------------------------------
0x610400    N     10:00:00:00:c9:24:3d:90 (Emulex)     scsi-fcp
0x6105dc    NL    21:00:00:20:37:28:31:6d (Seagate)    scsi-fcp
0x6105e0    NL    21:00:00:20:37:28:24:7b (Seagate)    scsi-fcp
0x6105e1    NL    21:00:00:20:37:28:22:ea (Seagate)    scsi-fcp
0x6105e2    NL    21:00:00:20:37:28:2e:65 (Seagate)    scsi-fcp
0x6105e4    NL    21:00:00:20:37:28:26:0d (Seagate)    scsi-fcp
0x630400    N     10:00:00:00:c9:24:3f:75 (Emulex)     scsi-fcp
0x630500    N     50:06:01:60:88:02:90:cb              scsi-fcp
0x6514e2    NL    21:00:00:20:37:a7:ca:b7 (Seagate)    scsi-fcp
0x6514e4    NL    21:00:00:20:37:a7:c7:e0 (Seagate)    scsi-fcp
0x6514e8    NL    21:00:00:20:37:a7:c7:df (Seagate)    scsi-fcp
0x651500    N     10:00:00:e0:69:f0:43:9f (JNI)
```

```
Total number of entries = 12
```

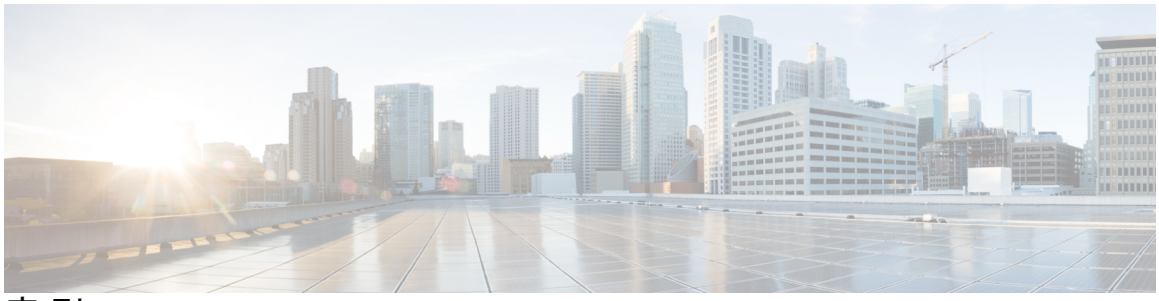
Note
シスコ スイッチ ネーム サーバにはローカル エントリおよびリモート エントリが表示され、エントリはタイムアウトしません。

高度なファイバチャネル機能のデフォルト設定

次の表に、この章で説明した機能のデフォルト設定を示します。

Table 32: **拡張機能のデフォルト設定値**

パラメータ	デフォルト
CIM サーバー	ディセーブル
CIM サーバー セキュリティ プロトコル	HTTP
D_S_TOV	5,000 ミリ秒
E_D_TOV	2,000 ミリ秒
R_A_TOV	10,000 ミリ秒
fctrace を呼び出すタイムアウト時間	5 秒
fcping 機能によって送信されるフレーム数	5 フレーム
リモート キャプチャ接続プロトコル	TCP
リモート キャプチャ接続モード	Passive
ローカル キャプチャ フレーム制限	10 フレーム
FC ID の割り当てモード	autoモード
ループ モニタリング	ディセーブル
interop モード	無効化



索 引

記号

A

B

E

F

H

I

M

N

P

R

S

T

V

W

Z

と

ね

の

は

ひ

ふ

ほ

ま

ゆ

れ

ろ

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。