Cisco Nexus 6000 シリーズ NX-OS SAN スイッチング コンフィギュレーション ガイド リリース 6.x

初版：2013 年 01 月 30 日

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

Text Part Number: OL-27932-01-J

【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

ここでは、次の項について説明します。

対象読者

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

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角カッコで囲んで示しています。

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

例では、次の表記法を使用しています。

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

このマニュアルでは、次の表記法を使用しています。

（注） 「注釈」です。 役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

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

Cisco Nexus 6000 シリーズ NX-OS ソフトウェアの関連資料

完全な Cisco NX-OS 6000 シリーズ マニュアル セットは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps12806/tsd_products_support_series_home.html

リリース ノート

リリース ノートは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps12806/prod_release_notes_list.html

コンフィギュレーション ガイド

これらのマニュアルは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps12806/products_installation_and_configuration_guides_list.html

このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 6000 Series NX-OS Adapter-FEX Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS FabricPath Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS FCoE Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Fundamentals Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Interfaces Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Layer 2 Switching Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Multicast Routing Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Quality of Service Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS SAN Switching Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Security Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS System Management Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Unicast Routing Configuration Guide*』

インストレーション ガイドおよびアップグレード ガイド

これらのマニュアルは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps12806/prod_installation_guides_list.html

このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 6000 Series NX-OS Software Upgrade and Downgrade Guides*』

ライセンス ガイド

『*License and Copyright Information for Cisco NX-OS Software*』は、http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/license_agreement/nx-ossw_lisns.html から入手できます。

コマンド リファレンス

これらのマニュアルは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps12806/prod_command_reference_list.html

このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 6000 Series NX-OS Fabric Extender Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS FabricPath Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Fundamentals Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Interfaces Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Layer 2 Interfaces Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Multicast Routing Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Quality of Service Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Security Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS System Management Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS TrustSec Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Unicast Routing Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Virtual Port Channel Command Reference*』

テクニカル リファレンス

『*Cisco Nexus 6000 Series NX-OS MIB Reference*』は http://www.cisco.com/en/US/docs/switches/datacenter/nexus6000/sw/mib/reference/NX6000_MIBRef.html から入手できます。

エラー メッセージおよびシステム メッセージ

『*Cisco Nexus 6000 Series NX-OS System Message Guide*』は、http://www.cisco.com/en/US/docs/switches/datacenter/nexus6000/sw/system_messages/reference/sl_nxos_book.html から入手できます。

トラブルシューティング ガイド

『*Cisco Nexus 6000 Series NX-OS Troubleshooting Guide*』は http://www.cisco.com/en/US/docs/switches/datacenter/nexus6000/sw/troubleshooting/guide/N5K_Troubleshooting_Guide.html から入手できます。

マニュアルに関するフィードバック

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

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。 RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

第 1 章

概要

この章の内容は、次のとおりです。

SAN スイッチングの概要

この章では、Cisco NX-OS デバイスの SAN スイッチングの概要について説明します。 この章の内容は、次のとおりです。

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 バーチャライゼーション

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。

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 チャネルと FICON トラフィックの両方について、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、特定のマスター 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 の拡張性、可用性、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。

FICON の場合、VSAN により、FICON およびオープン システムのハードウェアベースの分離が容易になります。

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ことができます。 VSAN は、可用性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、コストを削減できます。

ユーザは、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、論理ユニット番号（LUN）ゾーン分割と組み合わせて、特定のホストのみが 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制御のシングル ポイントを提供します。
- 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 チャレンジ ハンドシェイク認証プロトコル（DHCHAP）は、Cisco SAN 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 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用して、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。

Fabric Configuration Server

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コンフィギュレーション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。

第 2 章

ファイバチャネル ドメインパラメータの設定

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。

注意 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

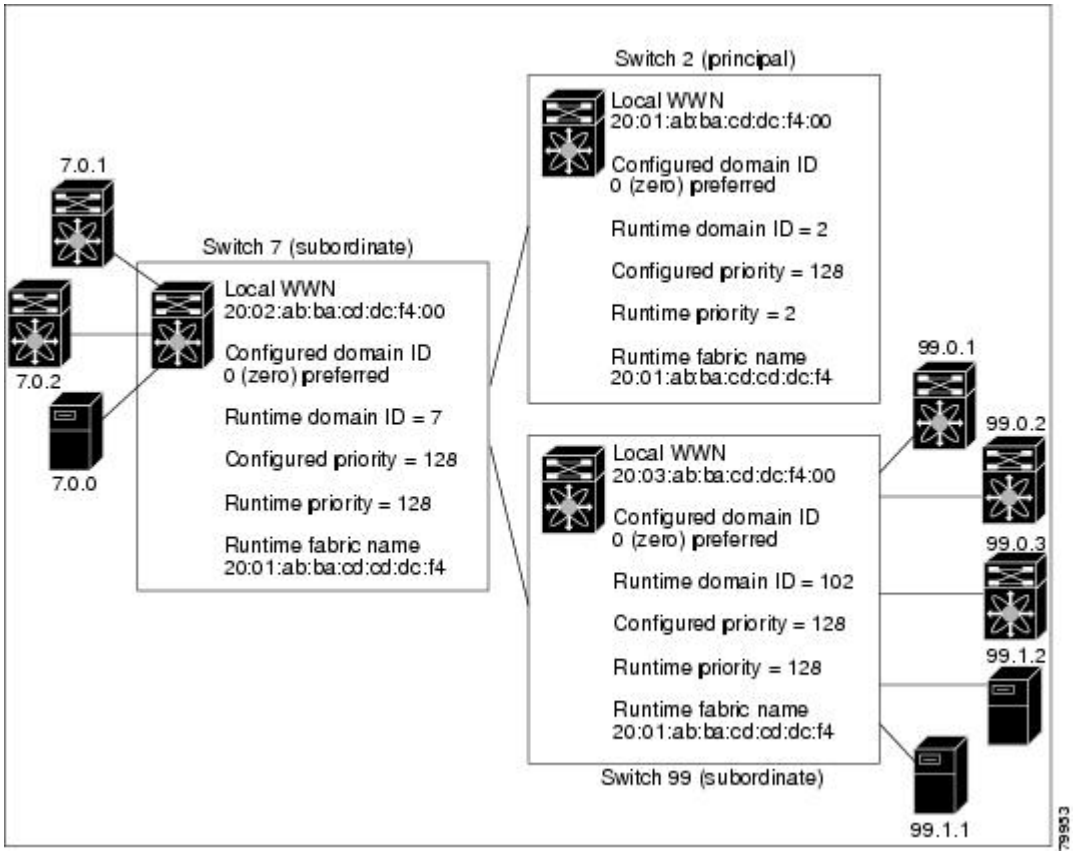
fcdomain は、4 つのフェーズで構成されます。

- 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 の設定例を示します。

図 *1*： *fcdomain* の設定例



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。 中断を伴う再起動を実行すると、Reconfigure Fabric（RCF）フレームがファブリックのその他のスイッチに送信され、VSAN のすべてのスイッチでデータ トラフィックが中断されます（リモートでセグメント化されている ISL を含む）。 中断を伴わない再起動を実行すると、Build Fabric（BF）フレームがファブリックのその他のスイッチに送信され、そのスイッチだけでデータ トラフィックが中断されます。

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。

（注） 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、次回の中断または非中断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。

VSAN が interop モードの場合は、この VSAN に対して fcdomain の中断再起動を実行できません。

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 オプションを使用すると、優先ドメイン ID などほとんどの設定は、対応する実行時の値に適用されます。

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。

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	**fcdomain restart vsan** *vsan-id* 例： `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* 例： `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イネーブル化

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。

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	**fcdomain optimize fast-restart vsan** *vsan-id* 例： `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* 例： `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。

Switch Priority

デフォルトでプライオリティ 128 が設定されています。 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 の再起動時にランタイムに適用されます。 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 プライオリティの設定

主要スイッチにプライオリティを設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**fcdomain priority** *number* **vsan** *vsan-id* 例： `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* 例： `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 の初期化の概要

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 のディセーブル化または再イネーブル化

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。

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 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。

ファブリック名の設定

ディセーブルにされた fcdomain にファブリック名の値を設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan** *vsan-id* 例： `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* 例： `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。 デフォルトでは、rcf-reject オプションはディセーブルです（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。

（注） 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。

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	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 3	**fcdomain rcf-reject vsan** *vsan-id* 例： `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 4	**no fcdomain rcf-reject vsan** *vsan-id* 例： `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。

自動再設定のイネーブル化

特定の VSAN（または VSAN 範囲）で自動再設定をイネーブルに設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**fcdomain auto-reconfigure vsan** *vsan-id* 例： `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。
ステップ 3	**no fcdomain auto-reconfigure vsan** *vsan-id* 例： `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

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。

設定済みドメイン ID のタイプは preferred または static 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 preferred です。

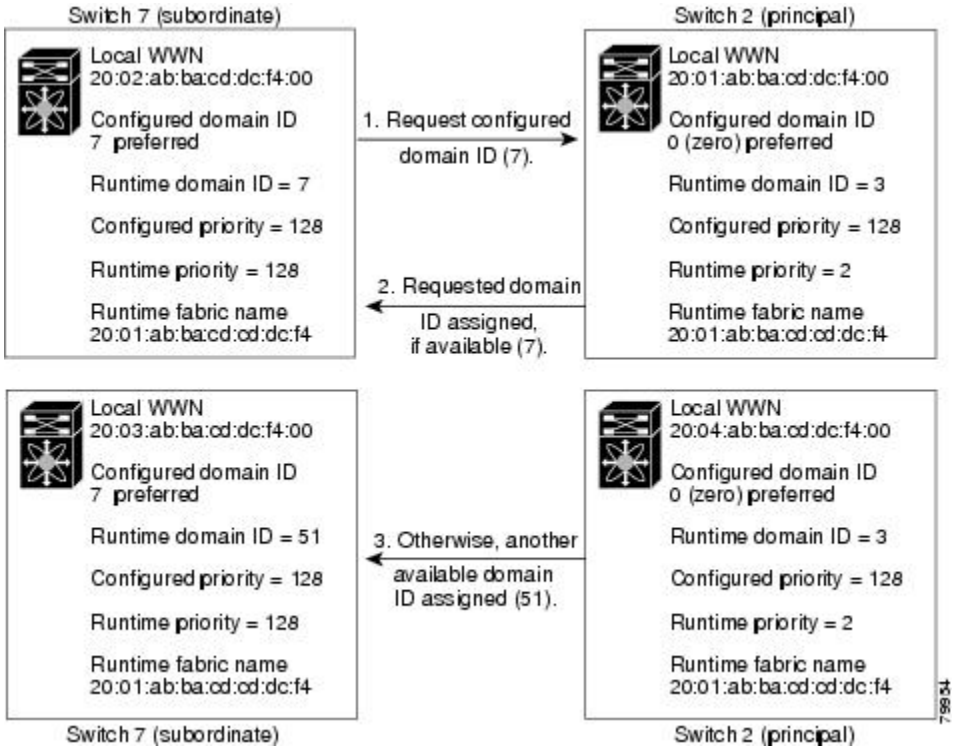
（注） 値 0（ゼロ）を設定できるのは、preferre オプションを使用した場合だけです。

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。 static 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。

図 *2*： *preferred* 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、preferred および static 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）。
  - 設定されているタイプが 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 を受け入れて、割り当てられたドメイン ID がランタイム 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 zero-preferred に設定することもできます。

注意 設定済みドメインの変更を実行時ドメインに適用する場合は、fcdomain restart コマンドを入力する必要があります。

（注） 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。

関連トピック

許可ドメイン ID リスト，（17 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。

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	**fcdomain domain** *domain-id* **static vsan** *vsan-id* 例： `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* 例： `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。
ステップ 4	**fcdomain domain** *domain-id* **preferred vsan** *vsan-id* 例： `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* 例： `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 リストの設定

許可ドメイン ID リストを設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**fcdomain allowed** *domain-id range* **vsan** *vsan-id* 例： `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* 例： `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できます。

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。

（注） 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。

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	**fcdomain distribute** 例： `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** 例： `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。

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	**fcdomain commit vsan** *vsan-id* 例： `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。

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	**fcdomain abort vsan** *vsan-id* 例： `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

保留中の設定変更は **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: Distribution Enable
Result: Success
```

連続ドメイン ID 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 割り当てのイネーブル化

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。

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	**fcdomain contiguous-allocation vsan** *vsan-id* **-** *vsan-id* 例： `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。 （注） **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* 例： `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、永続的 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。

（注） 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 で永続的 FC ID 機能をイネーブルにする必要があります。

（注） 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永続的 FC ID は、インターフェイス間を移動させることができ、同じ永続的 FC ID をそのまま維持することができます。

永続的 FC ID 機能のイネーブル化

永続的 FC ID 機能をイネーブルに設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**fcdomain fcid persistent vsan** *vsan-id* 例： `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。

	コマンドまたはアクション	目的
ステップ 3	**no fcdomain fcid persistent vsan** *vsan-id* 例： `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

永続的 FC ID 機能をイネーブルにすると、永続的 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。 永続的 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 内で永続的 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 の設定

永続的 FC ID を設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**fcdomain fcid database** 例： `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。

	コマンドまたはアクション	目的
ステップ 3	**vsan** *vsan-id* **wwn 33:e8:00:05:30:00:16:df fcid** *fcid* 例： `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。 （注） 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** 例： `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** 例： `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。 （注） 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

（注） ここに記載された説明が適用されるのは、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だけです。

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 以外の値を設定できます。 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設定する必要があります。

Cisco SAN スイッチでは、FC ID の永続性機能により、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 の固有エリア 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。

手順

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
```

（注） 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 1
...
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 機能をイネーブルにします。

```
switch# configure terminal
switch(config)# fcdomain fcid persistent vsan 1
switch(config)# end
```

ステップ 5 異なるエリアの新しい 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
```

（注） 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。

永続的 FC ID の選択消去

永続的 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。

表 *1*： 消去される *FC ID*

永続的 FC ID の状態	永続的 FC ID の使用状態	アクション
スタティック	使用中	削除されない
スタティック	使用中でない	削除されない
ダイナミック	使用中	削除されない
ダイナミック	使用中でない	削除される

永続的 FC ID の消去

永続的 FC ID を消去できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**purge fcdomain fcid vsan** *vsan-id* 例： `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* **-** *vsan-id* 例： `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 設定の確認

（注） 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: 5
        Number of times Local Switch was Principal: 0
        Number of 'Build Fabric's: 3
        Number of 'Fabric 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。

表 *2*： デフォルト *fcdomain* パラメータ

パラメータ	デフォルト
fcdomain 機能	イネーブル
設定済みドメイン ID	0（ゼロ）
設定済みドメイン	Preferred
auto-reconfigure オプション	ディセーブル
連続割り当てオプション	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

パラメータ	デフォルト
rcf-reject	ディセーブル
永続的 FC ID	イネーブル
許可ドメイン ID リスト設定の配信	ディセーブル

第 3 章

NPV の設定

この章の内容は、次のとおりです。

NPV の設定

NPV の概要

NPV の概要

デフォルトでは、Cisco Nexus デバイス スイッチは、ファブリック モードで動作します。 このモードでは、スイッチは標準のファイバ チャネル スイッチング機能を提供します。

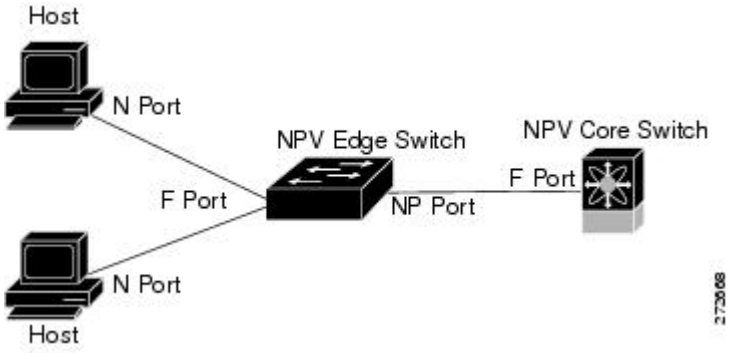
ファブリック モードでは、SAN に参加する各スイッチにドメイン ID が割り当てられます。 各 SAN（または VSAN）は、最大 239 個のドメイン ID 数をサポートするため、SAN におけるスイッチ数は 239 台に制限されます。 多数のエッジ スイッチが配置されている SAN トポロジでは、SAN はこの制限を超えて拡張する必要がある場合があります。 NPV は、コア スイッチのドメイン ID を複数のエッジ スイッチ間で共有することによって、このドメイン ID の制限を解消します。

NPV モードでエッジ スイッチは、すべてのトラフィックをサーバ側ポートからコア スイッチに中継します。 コア スイッチは、F ポート機能（ログインおよびポート セキュリティなど）およびすべてのファイバ チャネル スイッチング機能を提供します。

エッジ スイッチは、コア スイッチのファイバ チャネル ホスト、および接続装置の通常のファイバ チャネル スイッチのように見えます。

次の図に、インターフェイスレベルでの NPV 構成を示します。

図 3 : *NPV* のインターフェイスでの設定



NPV モード

NPV モードでは、エッジ スイッチは、ファイバ チャネル スイッチング機能を備えたコア スイッチにすべてのトラフィックを中継します。 エッジ スイッチはコア スイッチのドメイン ID を共有します。

スイッチを NPV モードに切り替えるには、NPV 機能をイネーブルに設定します。 このコンフィギュレーション コマンドにより、スイッチの再起動が自動的にトリガーされます。 NPV モードは、インターフェイスごとに設定できず、 スイッチ全体に適用されます。

NPV モードでは、ファブリック モードの CLI コマンドおよび機能のサブセットがサポートされます。 たとえば、ファブリック ログインおよびネーム サーバの登録に関連するコマンドはコア スイッチで提供されるため、エッジ スイッチにはこれらの機能は不要です。 ファブリック ログインおよびネーム サーバの登録データベースを表示するには、コア スイッチで **show flogi database** コマンドおよび **show fcns database** コマンドを入力する必要があります。

サーバ インターフェイス

サーバ インターフェイスは、サーバに接続するエッジ スイッチの F ポートです。 N port identifier virtualization（NPIV; N ポート識別子仮想化）機能をイネーブルにすると、サーバ インターフェイスは、複数のエンド デバイスをサポートできます。 NPIV は複数の FC ID を単一の N ポートに割り当てる手段を提供します。これにより、サーバはさまざまなアプリケーションに一意の FC ID を割り当てることができます。

（注） NPIV を使用するには、NPIV 機能をイネーブルにし、複数のデバイスをサポートするサーバ インターフェイスを再初期化します。

Cisco Nexus デバイスでは、サーバ インターフェイスは仮想ファイバ チャネル インターフェイスになります。

関連トピック

NPV の設定, （31 ページ）

NP アップリンク

エッジ スイッチからコア スイッチまでのすべてのインターフェイスは、プロキシ N ポート（NP ポート）として設定されます。

NP アップリンクは、エッジ スイッチの NP ポートからコア スイッチの F ポートまでの接続です。NP アップリンクが確立されると、エッジ スイッチは、コア スイッチに Fabric Login Message（FLOGI; ファブリック ログイン メッセージ）を送信し、FLOGI が正常に実行された場合は、エッジ スイッチ自身をコア スイッチのネーム サーバに登録します。 この NP アップリンクに接続されたエンド デバイスからの後続の FLOGI はコア スイッチにそのまま転送されます。

（注） スイッチの CLI コンフィギュレーション コマンドおよび出力表示では、NP アップリンクは外部インターフェイスと呼ばれます。

Cisco Nexus デバイスでは、NP アップリンク インターフェイスは仮想ファイバ チャネル インターフェイスです。

関連トピック

ファブリック ログイン, （127 ページ）

FLOGI 動作

NP ポートが動作可能になると、スイッチは最初に（NP ポートのポート WWN を使用して）FLOGI 要求を送信し、コア スイッチにログインします。

FLOGI 要求が完了した後、スイッチは自身を（NP ポートおよびエッジ スイッチの IP アドレスのシンボリック ポート名を使用して）コア スイッチのファブリック ネーム サーバに登録します。

次の表に、NPV モードで使用されるエッジ スイッチのポートおよびノード名を示します。

表 *3*： エッジ スイッチ *FLOGI* パラメータ

パラメータ	派生元
pWWN	エッジ スイッチの NP ポートの fWWN
nWWN	エッジ スイッチの VSAN ベースの sWWN

パラメータ	派生元
シンボリック ポート名	エッジ スイッチ名および NP ポート インターフェイスの文字列 （注） スイッチ名がない場合は、出力は「switch」と表示されます。たとえば、switch: fc 1/5 のようになります。
IP アドレス	エッジ スイッチの IP アドレス
シンボリック ノード名	エッジ スイッチ名

次のような理由により、エッジスイッチで fWWN ベースのゾーン分割を使用することは推奨しません。

- ゾーン分割はエッジ スイッチでは実施されない（コア スイッチ上で実施される）。
- エッジデバイスに接続された複数のデバイスがコア上の同じ F ポートを介してログインする（このため、異なるゾーンに分離できない）。
- 使用する NPV リンクによっては同じデバイスがコア スイッチの異なる fWWN を使用してログインする可能性があり、異なる fWWN でゾーン分割する必要がある。

関連トピック

ゾーンに関する情報, （85 ページ）

NPV トラフィック管理の注意事項

NPV トラフィック管理を導入する際には、次の注意事項に従ってください。

- NPV トラフィック管理は、自動トラフィック エンジニアリングがネットワーク要件を満たさない場合にだけ使用してください。
- すべてのサーバインターフェイスにトラフィック マップを設定する必要はありません。 NPV はデフォルトで自動トラフィック管理を使用します。

NPV の注意事項および制限事項

NPV を設定する場合、次の注意事項および制限事項に注意してください。

- NPV モードでは、2 つのエンド デバイス間のやり取りに、エッジ スイッチからコアへの同じアップリンクが使用されるため、順序どおりのデータ配信を行う必要はありません。 エッジ スイッチのアップストリームのコア スイッチが設定されている場合は、順序どおりの配信を実行します。

- コア スイッチ上で使用できるすべてのメンバ タイプを使用して、エッジ スイッチに接続されているエンドデバイスのゾーン分割を設定できます。 fWWN、sWWN、ドメイン、またはポートベースのゾーン分割では、コンフィギュレーションコマンドでコアスイッチのfWWN、sWWN、ドメイン、またはポートを使用してください。
- NPV モードでは、ポート トラッキングはサポートされません。
- NPV スイッチを介してログインするデバイスには、コア スイッチでポート セキュリティがサポートされます。 ポートセキュリティは、コアスイッチでインターフェイスごとにイネーブルにされます。 NPV スイッチを介してログインするデバイスのコア スイッチでセキュリティ ポートをイネーブルにするには、次の要件に従う必要があります。
  - 内部 FLOGI がポート セキュリティ データベースに存在している必要があります。これによりコア スイッチのポートで通信やリンクが許可されます。
  - すべてのエンド デバイスの pWWN もポート セキュリティ データベースに存在する必要があります。
- NPV モードでは、サーバをスイッチに接続できます。
- NPV モードでは、ターゲットをスイッチに接続できません。
- ファイバチャネル スイッチングは、エッジスイッチで実行されません。すべてのトラフィックはコア スイッチでスイッチングされます。
- NPV は NPIV 対応のモジュール サーバをサポートします。 この機能は階層型 NPIV と呼ばれます。
- NPV モードでは VF および VNP ポート タイプだけがサポートされます。

NPV の設定

NPV のイネーブル化

NPV をイネーブルにすると、システム設定が消去され、スイッチは再起動します。

（注） NPV をイネーブルにする前に、現在の設定をブート フラッシュ メモリまたは TFTP サーバに保存しておくことを推奨します。

NPV をイネーブルにする手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **npv enable**	NPV モードをイネーブルにします。 スイッチが再起動し、NPV モードで起動します。 （注） 再起動時に write-erase 操作が実行されます。
ステップ 3	switch(config-npv)# **no npv enable**	NPV モードをディセーブルにします。これによりスイッチがリロードされます。

NPV インターフェイスの設定

NPV をイネーブルにしたら、NP アップリンク インターフェイスおよびサーバ インターフェイスを設定する必要があります。

NP インターフェイスの設定

NPV をイネーブルにしたら、NP アップリンク インターフェイスおよびサーバ インターフェイスを設定する必要があります。 NP アップリンク インターフェイスを設定する手順は、次のとおりです。

サーバ インターフェイスを設定する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface vfc** *vfc-id*	コア NPV スイッチに接続するインターフェイスを選択します。
ステップ 3	switch(config-if)# **switchport mode NP**	このインターフェイスを NP ポートとして設定します。
ステップ 4	switch(config-if)# **no shutdown**	インターフェイスをアップにします。

サーバ インターフェイスの設定

サーバ インターフェイスを設定する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface vfc** *vfc-id*	コア NPV スイッチに接続するインターフェイスを選択します。
ステップ 3	switch(config-if)# **switchport mode F**	このインターフェイスを F ポートとして設定します。
ステップ 4	switch(config-if)# **no shutdown**	インターフェイスをアップにします。

NPV トラフィック管理の設定

NPV トラフィック マップの設定

NPV トラフィック マップにより、1 つ以上の NP アップリンク インターフェイスがサーバ インターフェイスに関連付けられます。 スイッチは、サーバ インターフェイスをこれらの NP アップリンクのいずれかに関連付けます。

（注） サーバインターフェイスがすでに NP アップリンクにマッピングされている場合は、このマッピングをトラフィック マップ設定に含める必要があります。

トラフィック マップを設定する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **npv traffic-map server-interface vfc** *vfc-id* **external-interface vfc** *vfc-id*	サーバ インターフェイス（またはサーバ インターフェイスの範囲）と NP アップリンク インターフェイス（または NP アップリンクインターフェイスの範囲）の間にマッピングを設定します。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **no npv traffic-map server-interface vfc** *vfc-id* **external-interface vfc** *vfc-id*	指定されたサーバインターフェイスと NP アップリンクインターフェイスの間のマッピングを削除します。

ディスラプティブ ロード バランシングのイネーブル化

追加の NP アップリンクを設定すると、ディスラプティブ ロード バランシング機能をイネーブルにして、サーバのトラフィック負荷をすべての NP アップリンクに均等に分散することができます。

ディスラプティブ ロード バランシングをイネーブルにする手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	NPV 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 2	switch(config)# **npv auto-load-balance disruptive**	スイッチのディスラプティブ ロードバランシングをイネーブルにします。
ステップ 3	switch (config)# **no npv auto-load-balance disruptive**	スイッチのディスラプティブ ロードバランシングをディセーブルにします。

NPV の確認

NPV に関する情報を表示する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show npv flogi-table** [**all**]	NPV 設定を表示します。

NPV の確認例

サーバ インターフェイスのデバイスおよび割り当てられた NP アップリンクのリストを表示するには、Cisco Nexus デバイスで **show npv flogi-table** コマンドを次のように入力します。

```
switch# show npv flogi-table
--------------------------------------------------------------------------------
SERVER                                                                          EXTERNAL
INTERFACE VSAN FCID            PORT NAME               NODE NAME       INTERFACE
--------------------------------------------------------------------------------
vfc31    1    0xee0008 10:00:00:00:c9:60:e4:9a 20:00:00:00:c9:60:e4:9a  vfc21
vfc31    1    0xee0009 20:00:00:00:0a:00:00:01 20:00:00:00:c9:60:e4:9a  vfc22
vfc31    1    0xee000a 20:00:00:00:0a:00:00:02 20:00:00:00:c9:60:e4:9a  vfc23
vfc31    1    0xee000b 33:33:33:33:33:33:33:33 20:00:00:00:c9:60:e4:9a  vfc24

Total number of flogi = 4
```

（注） サーバインターフェイスごとに、外部インターフェイス値は割り当てられた NP アップリンクを表示します。

サーバ インターフェイスおよび NP アップリンク インターフェイスのステータスを表示するには、**show npv status** コマンドを次のように入力します。

```
switch# show npv status
npiv is enabled

External Interfaces:
====================
  Interface: vfc21, VSAN: 1, FCID: 0x1c0000, State: Up
  Interface: vfc22, VSAN: 1, FCID: 0x040000, State: Up
  Interface: vfc23, VSAN: 1, FCID: 0x260000, State: Up
  Interface: vfc24, VSAN: 1, FCID: 0x1a0000, State: Up

  Number of External Interfaces: 4

Server Interfaces:
==================
  Interface: vfc31, VSAN: 1, NPIV: No, State: Up

  Number of Server Interfaces: 1
```

（注） NPV エッジ スイッチの fcns データベース エントリを表示するには、コア スイッチで **show fcns database** コマンドを入力する必要があります。

すべての NPV エッジ スイッチを表示するには、コア スイッチで **show fcns database** コマンドを次のように入力します。

```
core-switch# show fcns database
```

show fcns database コマンド出力に表示される NPV エッジ スイッチについてさらに詳しい情報（IP アドレス、スイッチ名、インターフェイス名など）が必要な場合は、コア スイッチで **show fcns database detail** コマンドを次のように入力します。

```
core-switch# show fcns database detail
```

NPV トラフィック管理の確認

NPV トラフィック マップを表示するには、**show npv traffic-map** コマンドを入力します。

```
switch# show npv traffic-map
NPV Traffic Map Information:
----------------------------------------
Server-If       External-If(s)
----------------------------------------
vfc13           vfc110,vfc111
vfc15           vfc11,vfc12
----------------------------------------
```

NPV 内部トラフィックの詳細情報を表示するには、**show npv internal info traffic-map** コマンドを入力します。

ディスラプティブ ロード バランシングのステータスを表示するには、**show npv status** コマンドを次のように入力します。

```
switch# show npv status
npiv is enabled
disruptive load balancing is enabled
External Interfaces:
====================
  Interface: vfc21, VSAN: 2, FCID: 0x1c0000, State: Up
...
```

第 4 章

FCoE NPV の設定

この章の内容は、次のとおりです。

FCoE NPV について

Cisco Nexus デバイスでは、FCoE NPV がサポートされます。 FCoE NPV 機能は、FIP スヌーピングの拡張版であり、FCoE 対応ホストから FCoE 対応 FCoE フォワーダ（FCF）スイッチに安全に接続する方法を提供します。 FCoE NPV 機能には次の利点があります。

- FCoE NPV には、FCF でのホストのリモート管理に付随する管理上およびトラブルシューティング上の問題がありません。

- FCoE NPV は、トラフィックエンジニアリング、VSAN 管理、およびトラブルシューティングといった NPV の機能を維持しながら、NVP 機能の拡張として FIP スヌーピングを実装します。
- FCoE NPV および NPV の併用により、FC ポートと FCoE ポートを同時に使用した通信が可能になります。 これにより、FC から FCoE トポロジへの移行がスムースになります。

FCoE NPV をイネーブルにするには、次のいずれかの方法を選択します。

- **FCoE をイネーブルにしてから NPV をイネーブルにする**：この方法では、**feature fcoe** コマンドを使用して FCoE をイネーブルにしてから、**feature npv** コマンドを使用して NPV をイネーブルにする必要があります。 FCoE をイネーブルにすると、デフォルトでは動作モードが FC スイッチングとなり、NPV をイネーブルにすると NPV モードに変わります。 NPV モードへの切り替えにより、自動的に書き込み消去が行われ、システムがリロードされます。 リロードされると、システムは NPV モードで稼働します。 NPV モードを終了し、FC スイッチング モードに戻るには、**no feature npv** コマンドを入力します。 NPV モードを終了すると、書き込み消去とスイッチ リロードもトリガーされます。 この方法には、ストレージ プロトコル サービス パッケージ（FC_FEATURES_PKG）ライセンスが必要です。
- **FCoE NPV をイネーブルにする**：**feature fcoe-npv** コマンドを使用して FCoE NPV をイネーブルにすると、モードが NPV に変わります。 この方法を使用すると、書き込み消去とリロードは行われません。 この方法では、ライセンス パッケージ（N6K-FNPV-SSK9）が別途必要です。 このライセンスも、ストレージ プロトコル サービス ライセンスに含まれています。

方式	ライセンス	書き込み消去	リロード
FCoE をイネーブルにしてから NPV をイネーブルにする	ストレージプロトコル サービス パッケージ（FC_FEATURES_PKG）	Yes	Yes
FCoE NPV をイネーブルにする	（N6K-FNPV-SSK9）	No	No

FCoE 対応スイッチとの相互運用性

Cisco Nexus デバイスは、次の FCoE 対応スイッチと相互運用できます。

- FCF 機能（EthNPV および VE）を実行できるようにした Cisco MDS 9000 シリーズ マルチレイヤ スイッチ。
- FCF 機能（EthNPV および VE）を実行できるようにした Cisco Nexus 7000 シリーズ スイッチ。
- FIP スヌーピングがイネーブルな Cisco Nexus 4000 シリーズ スイッチ。

スイッチの相互運用性に関する詳細については、『Cisco Data Center Interoperability Support Matrix』を参照してください。

ライセンシング

次の表に、FCoE NPV のライセンス要件を示します。

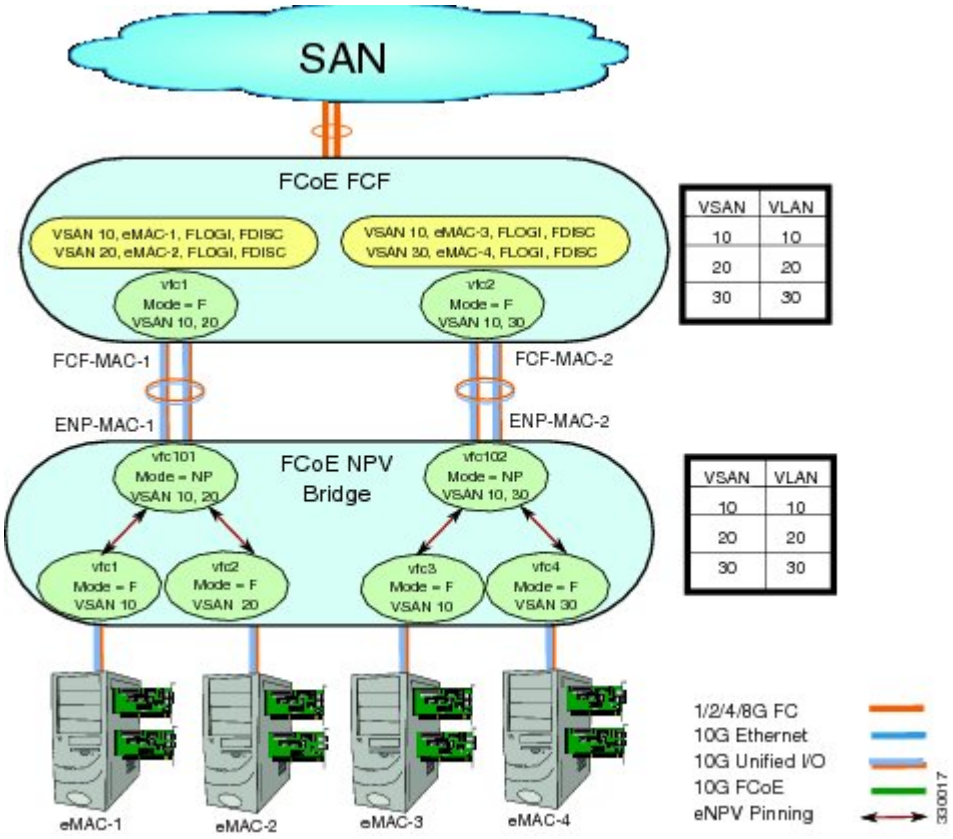
製品	ライセンス要件
NX-OS	FCoE NPV には、ライセンス（FCOE_NPV_PKG）が別途必要です。 ストレージ プロトコル サービス ライセンスには FCoE NPV のライセンスも含まれています。 FCoE および NPV にはストレージ プロトコル サービス パッケージ（FC_FEATURES_PKG）が必要です。 ライセンシングおよび Cisco NX-OS ライセンスのインストールが必要な機能の詳細については『Cisco NX-OS Licensing Guide』を参照してください。 トラブルシューティングのライセンスの問題については、ご使用のデバイスの『Troubleshooting Guide』を参照してください。

FCoE NPV モデル

次の図は、ホストと FCF を接続する FCoE NPV ブリッジを示しています。 コントロール プレーンの観点からいうと、FCoE NPV は、FCF およびホストの方向のプロキシ機能を実行します。これは、使用可能なすべての FCF アップリンク ポートにわたってホストへのログインを均等にロー

ド バランスすることを目的としています。 FCoE NPV ブリッジは VSAN 対応なので、ホストに VSAN を割り当てることができます。

図 *4*：*FCoE NPV* モデル



マッピングの要件

VSAN および VLAN-VSAN マッピング

ホストから接続する VSAN を作成し、さらにそれらの VSAN それぞれに専用の VLAN を作成して、マッピングする必要があります。 マッピングした VLAN を使用して、対応する VSAN の FIP および FCoE のトラフィックを伝送します。 VLAN-VSAN マッピングは、ファブリック全体で一貫した設定とする必要があります。 Cisco Nexus デバイスは 32 の VSAN をサポートします。

FC マッピング

FCoE NPV ブリッジについては、SAN ファブリックに関連付けた FC-MAP 値を設定する必要があります。これにより、他のファブリックにある FCF への誤接続を FCoE NPV ブリッジで分離できます。

ポート要件

VF ポート

FCoE NPV ブリッジのイーサネット インターフェイス上で直接接続したホストごとに、仮想ファイバ チャネル（vFC）インターフェイスを作成し、そのイーサネット インターフェイスにバインドする必要があります。 デフォルトでは、vFC インターフェイスは F モード（VF ポート）で設定されます。

この VF ポートは、次のパラメータで設定する必要があります。

- VLAN トランク イーサネット インターフェイスまたはポートチャネル インターフェイスに VF ポートをバインドする必要があります。 FCoE VLAN は、イーサネット インターフェイスのネイティブ VLAN として設定しないようにする必要があります。
- ポート VSAN は VF ポートに対して設定する必要があります。
- 管理ステートをアップ状態にする必要があります。

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 アドレスが設定された複数の 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。

（注） 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。

NPV 機能

次の NPV 機能は FCoE NPV 機能に適用されます。

- 自動トラフィック マッピング
- スタティック トラフィック マッピング
- ディスラプティブ ロード バランシング

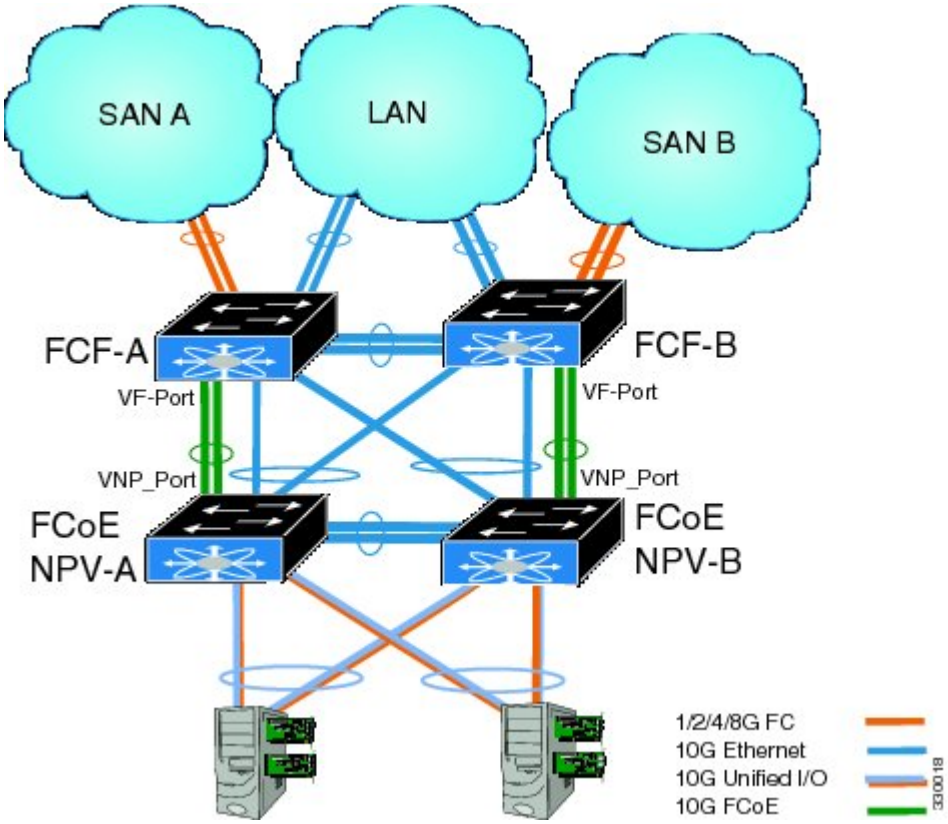
- FCoE NPV ブリッジでの FCoE フォワーディング
- VNP ポートを介して受信された FCoE フレームは、L2_DA が、VF ポートでホストに割り当てられている FCoE MAC アドレスのいずれかに一致する場合にのみ転送されます。それ以外の場合、FCoE フレームは破棄されます。

vPC トポロジ

FCoE NPV ブリッジと FCF 間の vPC トポロジで VNP ポートを設定している場合は、次の制限が適用されます。

- 同じ SAN ファブリックの中で複数の FCF にわたる vPC はサポートされません。
- LAN トラフィックについては、vPC 上で接続した FCF と FCoE NPV ブリッジ間の FCoE VLAN に専用リンクを使用する必要があります。
- 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。
- スイッチ間 vPC では、vPC メンバー ポートにバインドする VF ポートはサポートされません。

図 5：スイッチ間 *vPC* トポロジでの *VNP* ポート



サポートされるトポロジおよびサポートされないトポロジ

FCoE NPV は次のトポロジをサポートしています。

図 *6*：非 ***vPC*** ポート チャネルを介して ***Cisco Nexus*** デバイスに接続された ***FCoE NPV*** として機能する ***Cisco Nexus*** デバイス

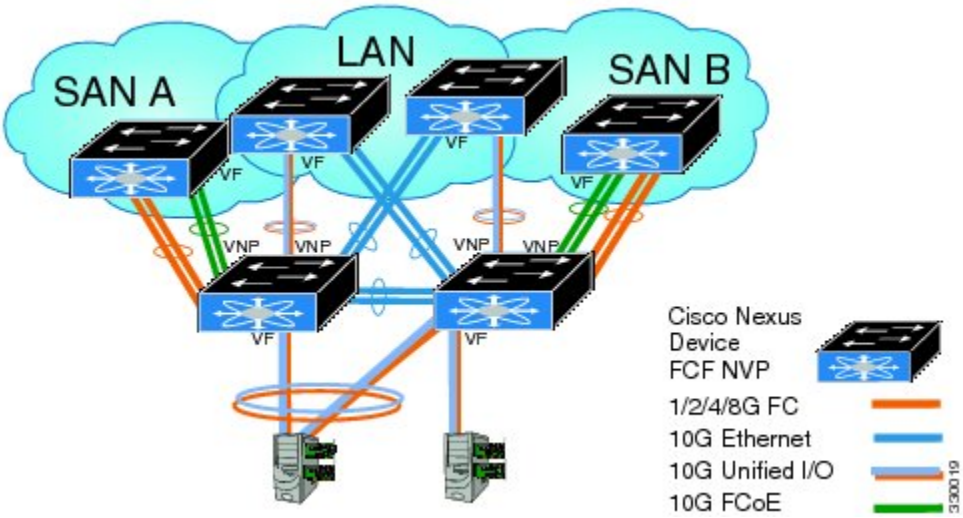


図 *7*：別の ***Cisco Nexus*** デバイスに ***vPC*** を介して接続された ***FCoE NPV*** として機能する ***Cisco Nexus*** デバイス

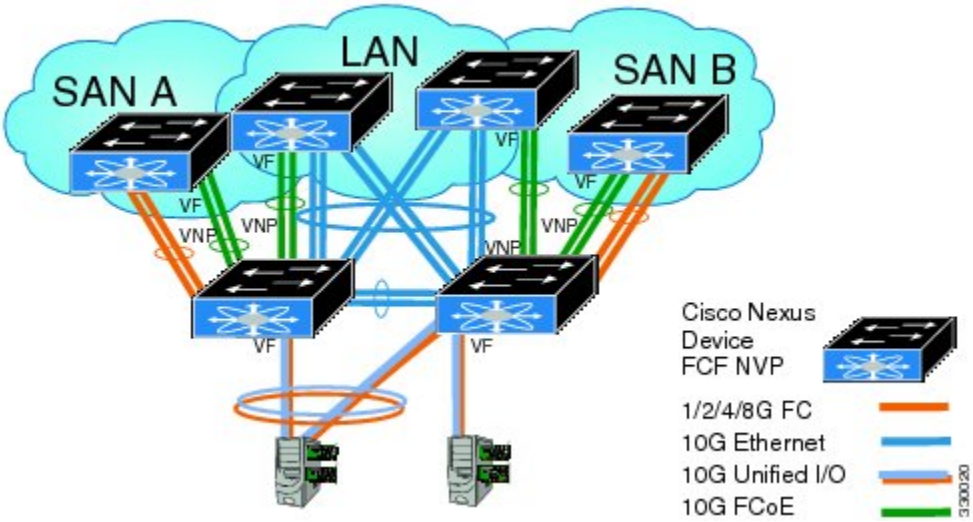


図 *8*：非 ***vPC*** ポート チャネルを介して ***Cisco Nexus*** デバイスに接続された ***FCoE NPV*** として機能する、***10GB*** ファブリック エクステンダを持つ ***Cisco Nexus*** デバイス

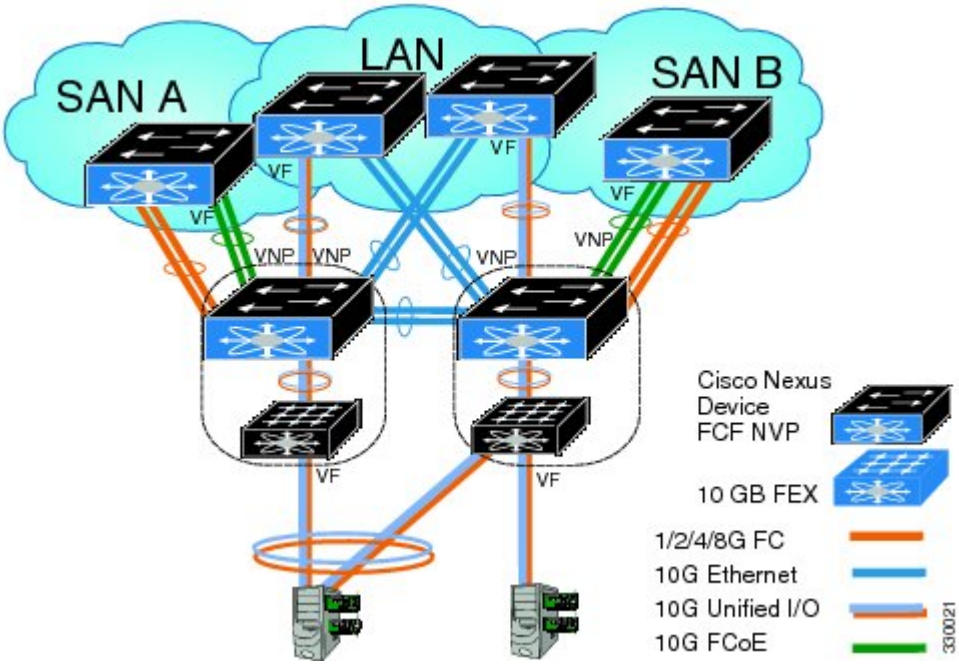
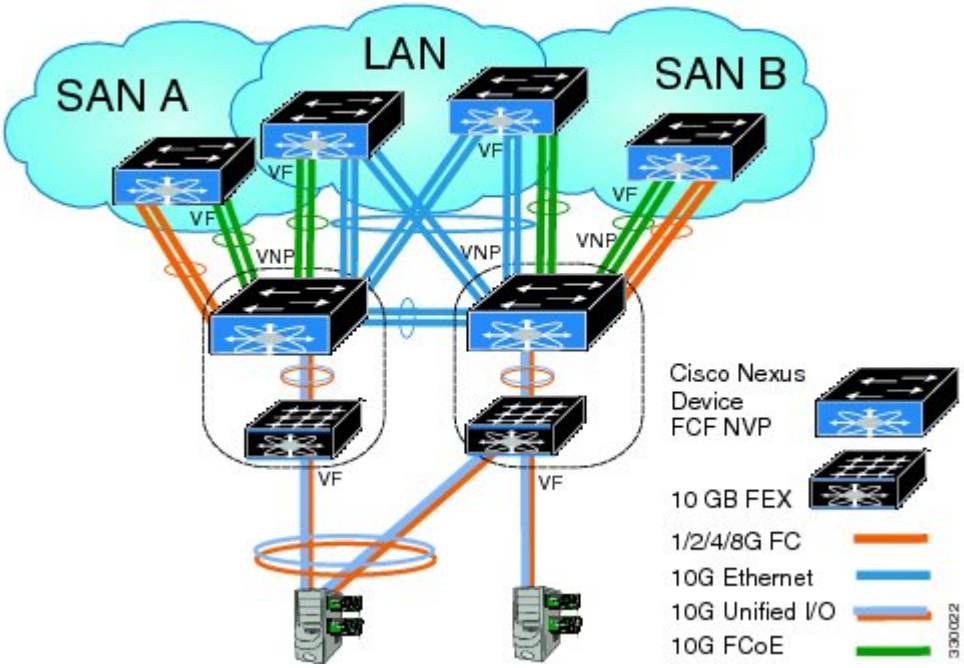


図 *9*：別の ***Cisco Nexus*** デバイスに ***vPC*** を介して接続された ***FCoE NPV*** として機能する、***10GB*** ファブリック エクステンダを持つ ***Cisco Nexus*** デバイス



サポートされていないトポロジ

FCoE NPV は次のトポロジをサポートしていません。

図 *10*：複数の *VF* ポート上で同一の *FCoE NPV* ブリッジに接続する *10GB* ファブリック エクステンダ

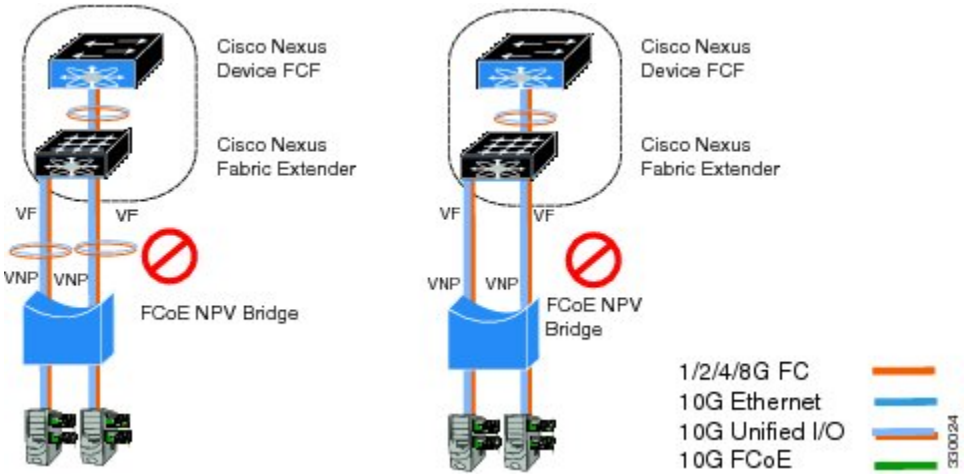


図 *11*：*FIP* スヌーピング ブリッジまたは別の *FCoE NPV* スイッチに接続する *FCoE NPV* ブリッジとして機能する *Cisco Nexus* デバイス

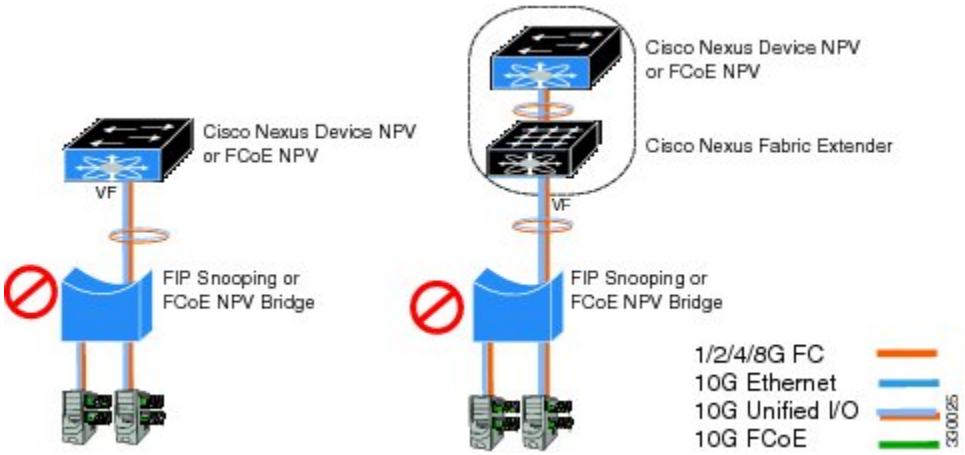
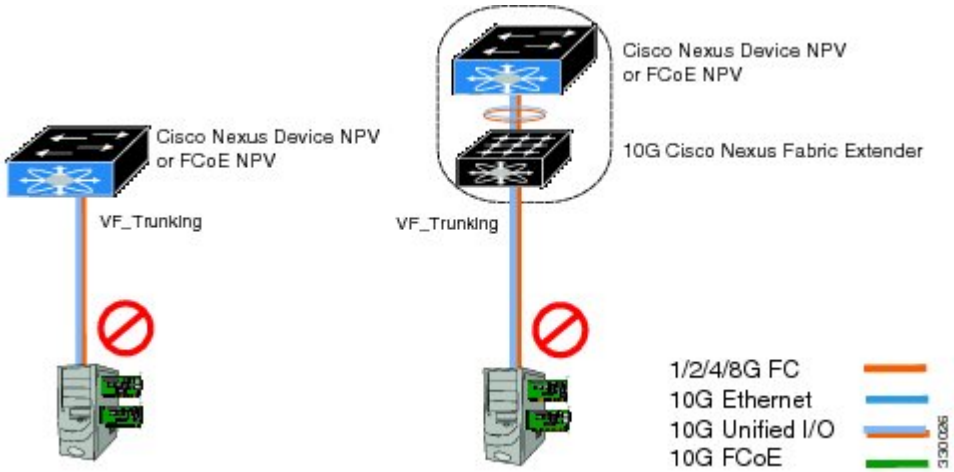


図 *12*：*FCoE NPV* モードでホストに接続する *VF* ポート トランク



注意事項および制約事項

FCoE NPV 機能の設定時の注意事項および制約事項は、次のとおりです。

- スイッチに FCoE NPV モードを設定すると、FCoE 機能をイネーブルにすることはできなくなります。 FCoE をイネーブルにするにはシステムのリロードが必要であることを示す警告が表示されます。

FCoE NPV 機能のアップグレードとダウングレードについては、次の注意事項および制約事項があります。

- FCoE NPV をイネーブルにして、VNP ポートを設定すると、Cisco NX-OS Release 5.0(3) N 1(1) またはそれ以前のリリースへのインサービス ソフトウェア ダウングレード（ISSD）はできません。
- FCoE NPV をイネーブルにしていても VNP ポートを設定していない場合は、Cisco NX-OS Release 5.0(3) N 1(1) またはそれ以前のリリースへの ISSD を実行しようとすると警告が表示されます。
- FCoE NPV ブリッジで ISSU を実行するには、**disable-fka** コマンドを使用して、コア スイッチでのタイムアウト値のチェック（FKA のチェック）をディセーブルにしておきます。

FCoE NPV 設定の制限

次の表に、イーサネット、イーサネット ポート チャネル、および仮想イーサネットの各インターフェイスで FCoE の設定に適用される制限を示します。

表 *4*：*VNP* ポート設定の制限

インターフェイス タイプ	Cisco Nexus 6000 シリーズ	Cisco Nexus 2000 シリーズ（10G インターフェイス）
イーサネット インターフェイスにバインドした VNP ポート	4 個の VNP ポート	未サポート
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した VNP ポート	2 個の VNP ポート	未サポート
仮想イーサネット（vEth）インターフェイスにバインドした VNP ポート	未サポート	未サポート

設定に対する制限のガイドラインは次のとおりです。

- 特定の FCF と FCoE NPV ブリッジの間でサポートできる VF ポート インターフェイスと VN ポート インターフェイスの数は、FCF から MAC に対する FCF のアドバタイジング能力によっても左右されます。
  - FCF がそのすべてのインターフェイス上で同じ FCF-MAC のアドレスをアドバタイズできる場合、FCoE NPV ブリッジは、1 つの VNP ポート上でその FCF に接続できます。このシナリオでは、1 つのポートチャネルインターフェイスを使用して冗長性を実現することを推奨します。
  - FCF が複数の FCF-MAC アドレスをアドバタイズする場合は、前表の制限が適用されます。 追加情報については、FCF スイッチのベスト プラクティスの推奨事項を参照してください。
- サポートされる VSAN の総数は 31 です（EVFP VSAN を除く）。
- サポートされる FCID の総数は 2048 です。

デフォルト設定

次の表に、各 FCoE NPV パラメータのデフォルト設定を示します。

表 *5*：デフォルトの *FCoE NPV* パラメータ

パラメータ	デフォルト
FCoE NPV	ディセーブル
FCoE	ディセーブル

パラメータ	デフォルト
NPV	ディセーブル
VNP ポート	ディセーブル
FIP Keep Alive（FKA）	ディセーブル

FCoE のイネーブル化および NPV のイネーブル化

まず FCoE をイネーブルにし、続いて NPV をイネーブルにできます。 この方法では、完全なストレージ サービス ライセンスが必要です。 この方法を使用すると、書き込み消去とリロードが実行されます。 この方法では、FCoE および FC の両方のアップストリームおよびホスト NPV の接続が可能です。 また、すべての QoS ポリシーのタイプで class-fcoe を設定する必要があります。

1 FCoE をイネーブルにします。
```
switch# configure terminal
switch(config)# feature fcoe
FC license checked out successfully
fc_plugin extracted successfully
FC plugin loaded successfully
FCoE manager enabled successfully
FC enabled on all modules successfully
Warning: Ensure class-fcoe is included in qos policy-maps of all types
```

2 NPV をイネーブルにします。
```
switch# configure terminal
switch(config)# feature npv
```

FCoE NPV のイネーブル化

feature fcoe-npv コマンドを使用して FCoE NPV をイネーブルにできます。 すべての FCoE 接続を扱うトポロジでは、この方法を推奨します。 この方法を使用すると書き込み消去とリロードが発生せず、ストレージ サービス ライセンスが不要です。 **feature fcoe-npv** コマンドを使用して FCoE NPV をイネーブルにするには、FCOE_NPV_PKG ライセンスをインストールしておく必要があります。

はじめる前に

FCoE NPV には次の前提条件があります。

- 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。
- VNP ポートを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	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	**feature fcoe-npv**	FCoE NPV をイネーブルにします。
ステップ 3	**exit**	フィギュレーション モードを終了します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次の例は、**feature fcoe-npv** コマンドを使用して FCoE NPV をイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# feature fcoe-npv
FCoE NPV license checked out successfully
fc_plugin extracted successfully
FC plugin loaded successfully
FCoE manager enabled successfully
FCoE NPV enabled on all modules successfully
```

次の例は、**feature fcoe** コマンドおよび **feature npv** コマンドを使用して FCoE NPV をイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# feature fcoe
switch(config)# feature npv
```

FCoE NPV の NPV ポートの設定

FCoE NPV の NPV ポートを設定できます。

1. vFC ポートを作成します。

```
switch# config t
switch(config)# interface vfc 20
switch(config-if)#
```

2. その vFC をイーサネット ポートにバインドします。

```
switch(config-if)# bind interface ethernet 1/20
switch(config-if)#
```

3. ポート モードを NP に設定します。

```
switch(config-if)# switchport mode NP
switch(config-if)#
```

4 ポートをアップ状態にします。

```
switch(config-if)# interface vfc 20no shutdown
switch(config-if)#
```

FCoE NPV の設定の確認

FCoE NPV の設定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 fcoe database	FCoEデータベースに関する情報を表示します。
show interface Ethernet x/y fcoe	指定されたイーサネット インターフェイスの FCoE 情報を表示します。これには次のものがあります。 • FCF または関連する enode の MAC アドレス • ステータス • 関連する VFC 情報
show interface vfc x	指定された vFC インターフェイスに関する情報を表示します。これには属性やステータスなどがあります。
show npv status	NPV の設定のステータスを表示します。これには VNP ポートに関する情報などがあります。
show fcoe-npv issu-impact	ISSU に対する FCoE NPV の影響を表示します。
show running-config fcoe_mgr	FCoE に関する実行コンフィギュレーション情報を表示します。
show startup-config fcoe_mgr	FCoE に関するスタートアップ コンフィギュレーション情報を表示します。
show tech-support fcoe	FCoE のトラブルシューティング情報を表示します。
show npv flogi-table	N ポート バーチャライゼーション（NPV）のファブリック ログイン（FLOGI）セッションに関する情報を表示します。
show fcoe	Fibre Channel over Ethernet（FCoE）の設定のステータスを表示します。

これらのコマンドの出力フィールドの詳細については、ご使用のデバイスの『Command Reference』を参照してください。

FCoE NPV の設定例

次に、FCoE NPV、LACP、no-drop キューイングの QoS、および VLAN/VSAN マッピングをイネーブルにする例を示します。

```
switch# config t
switch(config)# feature fcoe-npv
FCoE NPV license checked out successfully
fc_plugin extracted successfully
FC plugin loaded successfully
FCoE manager enabled successfully
FCoE NPV enabled on all modules successfully

switch(config)# feature lacp

switch# config t
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 fcoe-default-nq-policy

switch(config)# vsan database
switch(config-vsan-db)# vsan 50-51
switch(config-vsan-db)# vlan 50
switch(config-vlan)# fcoe vsan 50
switch(config-vlan)# vlan 51
switch(config-vlan)# fcoe vsan 51

This example shows a summary of the interface configuration information for trunked NP
ports:
switch# show interface brief | grep TNP

vfc25      400    NP     on      trunking         swl    TNP     2    --
vfc26      400    NP     on      trunking         swl    TNP     2    --
vfc130     1      NP     on      trunking         --     TNP     auto --
switch#
```

次に、FCoE に関する実行コンフィギュレーション情報の例を示します。

```
switch# show running-config fcoe_mgr

!Command: show running-config fcoe_mgr
!Time: Wed Jan  20 21:59:39 2013

version 6.0(2)N1(1)

interface vfc1
  bind interface Ethernet1/19

interface vfc2
  bind interface Ethernet1/2

interface vfc90
  bind interface Ethernet1/9

interface vfc100
  bind interface Ethernet1/10

interface vfc110
  bind interface port-channel110
```

```
interface vfc111
  bind interface Ethernet1/11

interface vfc120
  bind interface port-channel120

interface vfc130
  bind interface port-channel130

interface vfc177
  bind interface Ethernet1/7
fcoe fka-adv-period 16
```

次に、FCoE VLAN から VSAN へのマッピングの例を示します。

```
switch# show vlan fcoe

Original VLAN ID        Translated VSAN ID      Association State
----------------        ------------------      -----------------

      400                       400              Operational
      20                        20               Operational
      100                       100              Operational
      500                       500              Operational
      200                       200              Operational
      300                       300              Operational
```

次に、vFC 130 インターフェイスに関する情報の例を示します。これには属性やステータスがあります。

```
switch# show interface vfc 130
vfc130 is trunking (Not all VSANs UP on the trunk)
    Bound interface is port-channel130
    Hardware is Virtual Fibre Channel
    Port WWN is 20:81:00:05:9b:74:bd:bf
    Admin port mode is NP, trunk mode is on
    snmp link state traps are enabled
    Port mode is TNP
    Port vsan is 1
    Trunk vsans (admin allowed and active) (1,20,100,200,300,400,500)
    Trunk vsans (up)                       (500)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             (1,20,100,200,300,400)
    1 minute input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    1 minute output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      15 frames input, 2276 bytes
        0 discards, 0 errors
      7 frames output, 1004 bytes
        0 discards, 0 errors
    last clearing of "show interface" counters Tue May 31 20:56:41 2011

    Interface last changed at Wed Jun  1 21:53:08 2011
```

次に、vFC 1 インターフェイスに関する情報の例を示します。これには属性やステータスがあります。

```
switch# show interface vfc 1
vfc1 is trunking (Not all VSANs UP on the trunk)
    Bound interface is Ethernet1/19
    Hardware is Virtual Fibre Channel
    Port WWN is 20:00:00:05:9b:74:bd:bf
    Admin port mode is F, trunk mode is on
    snmp link state traps are enabled
    Port mode is TF
    Port vsan is 20
    Trunk vsans (admin allowed and active) (1,20,100,200,300,400,500)
    Trunk vsans (up)                       (20)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             (1,100,200,300,400,500)
    1 minute input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
```

```
    1 minute output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      355278397 frames input, 573433988904 bytes
        0 discards, 0 errors
      391579316 frames output, 572319570200 bytes
        0 discards, 0 errors
    last clearing of "show interface" counters Tue May 31 20:56:41 2011

    Interface last changed at Wed Jun  1 20:25:36 2011
```

次に、NPV FLOGI セッションに関する情報の例を示します。

```
switch# show npv flogi-table
--------------------------------------------------------------------------------
SERVER                                                                  EXTERNAL
INTERFACE VSAN FCID            PORT NAME               NODE NAME       INTERFACE
--------------------------------------------------------------------------------
vfc1      20   0x670000 21:01:00:1b:32:2a:e5:b8 20:01:00:1b:32:2a:e5:b8 vfc26

Total number of flogi = 1.
```

次に、NPV の設定のステータスの例を示します。これには VNP ポートに関する情報などがあります。

```
switch# show npv status

npiv is enabled

disruptive load balancing is disabled

External Interfaces:
====================
  Interface:  vfc25, State: Trunking
        VSAN:    1, State: Up
        VSAN:  200, State: Up
        VSAN:  400, State: Up
        VSAN:   20, State: Up
        VSAN:  100, State: Up
        VSAN:  300, State: Up
        VSAN:  500, State: Up, FCID: 0xa10000
  Interface:  vfc26, State: Trunking
        VSAN:    1, State: Up
        VSAN:  200, State: Up
        VSAN:  400, State: Up
        VSAN:   20, State: Up
        VSAN:  100, State: Up
        VSAN:  300, State: Up
        VSAN:  500, State: Up, FCID: 0xa10001
  Interface: vfc90,  State: Down
  Interface: vfc100, State: Down
  Interface: vfc110, State: Down
  Interface: vfc111, State: Down
  Interface: vfc120, State: Down
  Interface: vfc130, State: Trunking
        VSAN:    1, State: Waiting For VSAN Up
        VSAN:  200, State: Up
        VSAN:  400, State: Up
        VSAN:  100, State: Up
        VSAN:  300, State: Up
        VSAN:  500, State: Up, FCID: 0xa10002

  Number of External Interfaces: 8

Server Interfaces:
==================
  Interface:   vfc1, VSAN:   20, State: Up
  Interface:   vfc2, VSAN: 4094, State: Down
  Interface:   vfc3, VSAN: 4094, State: Down
  Interface: vfc5000, VSAN: 4094, State: Down
  Interface: vfc6000, VSAN: 4094, State: Down
  Interface: vfc7000, VSAN: 4094, State: Down
  Interface: vfc8090, VSAN: 4094, State: Down
  Interface: vfc8191, VSAN: 4094, State: Down
```

```
  Number of Server Interfaces: 8
```

次に、ポート チャネル 130 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 interface port-channel 130

!Command: show running-config interface port-channel130
!Time: Wed Jan  30 22:01:05 2013

version 6.0(2)N1(1)

interface port-channel130
  switchport mode trunk
  switchport trunk native vlan 2
  no negotiate auto
```

次に、ISSU に対する FCoE NPV の影響の例を示します。

```
switch# show fcoe-npv issu-impact
show fcoe-npv issu-impact
-------------------------

Please make sure to enable "disable-fka" on all logged in VFCs
Please increase the FKA duration to 60 seconds on FCF


Active VNP ports with no disable-fka set
----------------------------------------

vfc90
vfc100
vfc110
vfc111
vfc120
vfc130

ISSU downgrade not supported as feature fcoe-npv is enabled
switch#
```

第 5 章

VSAN トランキングの設定

この章では、VSAN トランキング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。

VSAN トランキングの設定

VSAN トランキングの概要

VSAN トランキングにより、相互接続ポートは複数の VSAN でフレームを送受信できます。 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。

VSAN トランキングは、仮想ファイバ チャネル インターフェイスでサポートされます。

VSAN トランキング機能には、次の制限事項があります。

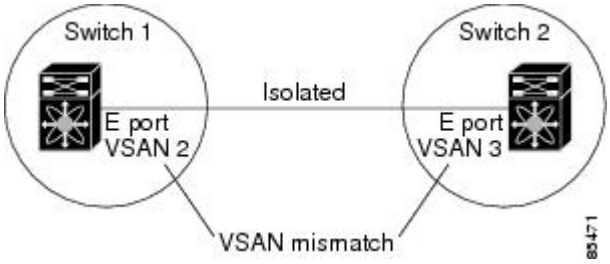
- トランキング設定は、E ポートにだけ適用されます。 トランク モードが E ポートでイネーブルにされており、そのポートがトランキング E ポートとして動作可能になると、TE ポートと見なされます。
- トランキング プロトコルは TE ポートに設定されたトランク許可 VSAN を使用して、フレームの送受信が可能な allowed-active VSAN を判別します。
- トランキングがイネーブルにされた E ポートがサードパーティ製のスイッチに接続されている場合、トランキング プロトコルは E ポートとしてシームレスな動作を保証します。

VSAN トランキングの不一致

E ポート間で VSAN が正しく設定されなかった場合、2 つの VSAN でトラフィックが結合される（その結果、2 つの VSAN が一致しなくなる）などの問題が発生します。 VSAN トランキング プ

ロトコルは、VSAN インターフェイスを ISL の両端で検証し、VSAN の結合を防ぎます（次の図を参照）。

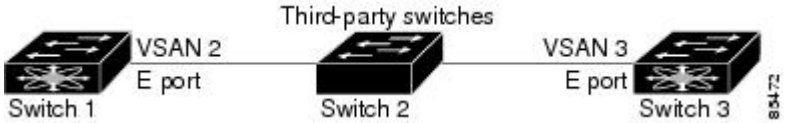
図 *13*： ***VSAN*** の不一致



この例では、トランキング プロトコルが潜在的な VSAN のマージを検出し、関連ポートを分離します。

2 つの Cisco SAN スイッチの間にサードパーティ製スイッチが配置されている場合、トランキング プロトコルは VSAN の結合を検出できません（次の図を参照）。

図 *14*： サードパーティ製スイッチによる ***VSAN*** の不一致



VSAN 2 と VSAN 3 は、ネーム サーバおよびゾーン アプリケーションにおいてオーバーラップするエントリによって事実上結合されます。 Cisco MDS 9000 Fabric Manager は、このようなトポロジの検出に役立ちます。

VSAN トランキング プロトコル

トランキング プロトコルは、E ポートおよび TE ポート動作にとって重要です。 トランキング プロトコルは、次の機能をサポートします。

- 動作可能なトランク モードのダイナミック ネゴシエーション
- トランク許可 VSAN の共通のセットの選択
- ISL（スイッチ間リンク）間の VSAN 不一致の検出

デフォルトでは、VSAN トランキング プロトコルはイネーブルです。 トランキング プロトコルがスイッチでディセーブルの場合、そのスイッチのポートは新規トランク コンフィギュレーションを適用できません。 既存のトランク設定は影響を受けません。TE ポートは引き続きトランク モードで機能しますが、トランキング プロトコルがイネーブルのときに事前にネゴシエートした VSAN のトラフィックだけをサポートします。 このスイッチに直接接続している他のスイッチも同様に接続インターフェイスで影響を受けます。 非トランキング ISL 間の異なるポート VSAN か

らのトラフィックを統合する必要がある場合、トランキング プロトコルをディセーブルにします。

VSAN トランキングの設定

注意事項と制約事項

VSAN トランキングを設定する場合、次の点に注意してください。

- VSAN トランキング ISL の両端が同じポート VSAN に属するよう設定することを推奨します。 ポート VSAN が異なるプラットフォームまたはファブリック スイッチでは、一端はエラーを返し、他端は接続されません。
- 不整合な設定を防ぐには、VSAN トランキング プロトコルをイネーブルまたはディセーブルにする前に **shutdown** コマンドを使用してすべての E ポートをディセーブルにします。

VSAN トランキング プロトコルのイネーブル化/ディセーブル化

VSAN トランキング プロトコルをイネーブルまたはディセーブルに設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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 trunk protocol enable** 例： `switch(config)# no trunk protocol enable`	トランキング プロトコルをディセーブルにします。
ステップ 3	**trunk protocol enable** 例： `switch(config)# trunk protocol enable`	トランキング プロトコルをイネーブルにします（デフォルト）。

Trunk Mode

デフォルトでは、すべてのファイバ チャネルでトランク モードはイネーブルです。 ただし、トランク モード設定は E ポート モードでしか有効になりません。 トランク モードを on（イネーブル）、off（ディセーブル）、または auto（自動）に設定できます。デフォルトのトランク モード

は on です。 リンクの両端のトランク モード設定によって、両端のリンクおよびポート モードのトランキング ステートが決まります（次の表を参照）。

表 *6*：スイッチ間のトランク モード ステータス

トランク モードの設定	最終的なステートとポート モード			
スイッチ 1	**スイッチ 2**	**トランキング ステート**	**ポート モード**	
on	auto または on	トランキング（EISL）	TE ポート	
off	auto、on、または off	トランキングなし（ISL）	E ポート	
auto	auto	トランキングなし（ISL）	E ポート	

Cisco SAN スイッチでの推奨設定は、トランクの一方が Auto、反対側が On 設定です。

（注） サードパーティ製のスイッチに接続されている場合、トランク モード設定は作用しません。スイッチ間リンク（ISL）は常にトランキング ディセーブルのステートです。

トランク モードの設定

トランク モードを設定できます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	switch(config)# **interface vfc** *vfc-id*	コア NPV スイッチに接続するインターフェイスを選択します。

	コマンドまたはアクション	目的
ステップ 3	**interface vfc** *vfc-id* 例： `switch(config)# interface vfc 15`	指定の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設定します。
ステップ 4	**switchport trunk mode on** 例： `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 5	**switchport trunk mode off** 例： `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。 （注） トランク モードは、仮想ファイバチャネル インターフェイスではオフにできません。
ステップ 6	**switchport trunk mode auto** 例： `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。

例

次に、トランク モードで vFC インターフェイスを設定する例を示します。

```
switch# configure terminal
switch#(config)# vfc 200
switch(config-if)# switchport trunk mode on
```

次に、トランク モードで vFC インターフェイス 200 の出力例を示します。

```
switch(config-if)# show interface vfc200
vfc200 is trunking (Not all VSANs UP on the trunk)
    Bound interface is Ethernet1/3
    Hardware is Virtual Fibre Channel
    Port WWN is 20:c7:00:0d:ec:f2:08:ff
    Peer port WWN is 00:00:00:00:00:00:00:00
    Admin port mode is E, trunk mode is on
    snmp link state traps are enabled
    Port mode is TE
    Port vsan is 1
    Trunk vsans (admin allowed and active) (1-6,10,22)
    Trunk vsans (up)                       ()
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             (1-6,10,22)
    5 minute input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minute output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      0 frames input, 0 bytes
        0 discards, 0 errors
      0 frames output, 0 bytes
        0 discards, 0 errors
    last clearing of "show interface" counters never
    Interface last changed at Mon Jan 18 10:01:27 2010
```

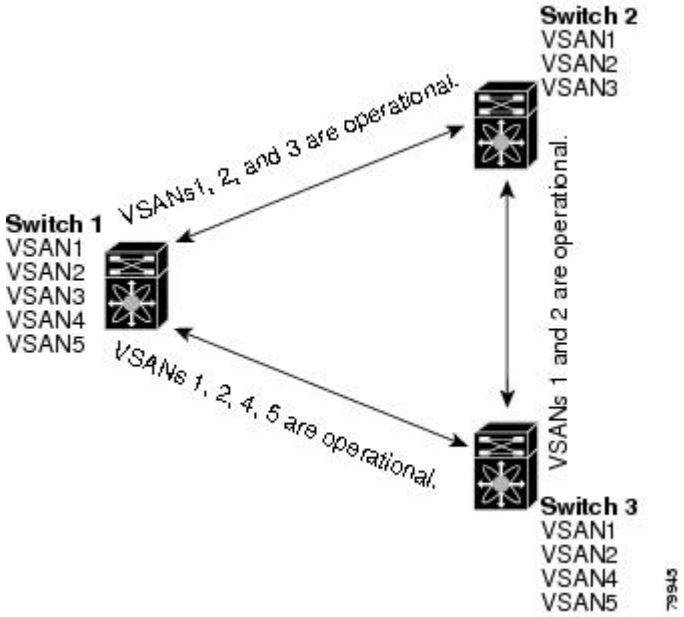
トランク許可 VSAN リスト

各ファイバ チャネル インターフェイスには、対応付けられたトランク許可 VSAN リストがあります。 TE ポート モードでは、フレームはこのリストに指定された 1 つまたは複数の VSAN で送受信されます。 デフォルトでは、完全な VSAN 範囲（1 ～ 4093）がトランク許可リストに含まれます。

スイッチに設定されたアクティブな状態の VSAN の共通のセットは、インターフェイスのトランク許可 VSAN リストに含まれ、*allowed-active VSAN* と呼ばれます。 トランキング プロトコルは、ISL の両端で allowed-active VSAN のリストを使用して、トラフィックが許可される通信可能な VSAN のリストを判別します。

次の図では、トランク許可 VSAN のデフォルト設定でスイッチ 1 は VSAN 1 ～ 5、スイッチ 2 は VSAN 1 ～ 3、スイッチ 3 は VSAN 1、2、4、および 5 が設定されています。 3 つすべてのスイッチに設定された VSAN はすべて、allowed-active です。 ただし、次に示すように、ISL の両端における allowed-active VSAN の共通のセットのみが通信可能になります。

図 *15*： *allowed-active VSAN* のデフォルト設定



allowed-active リストから選択した VSAN セットを設定して、トランキング ISL に指定された VSAN へのアクセスを制御できます。

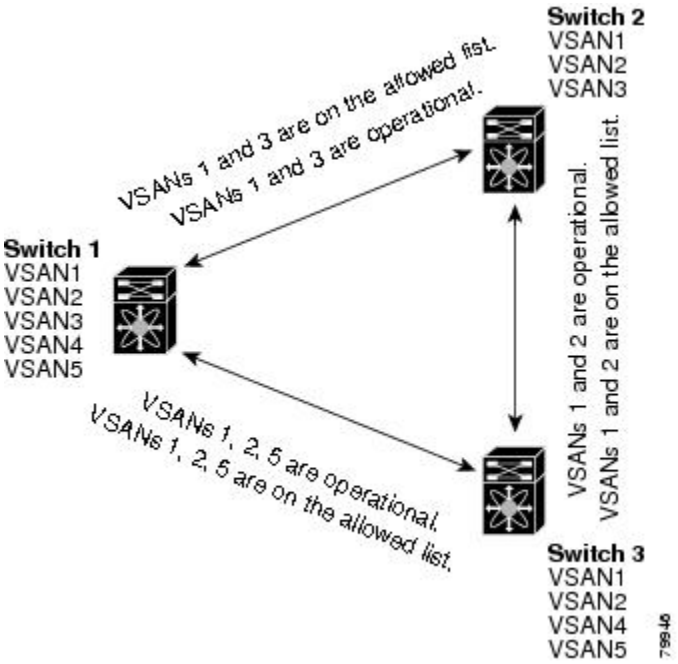
上の図を使用する例として、インターフェイスごとに許可 VSAN のリストを設定できます（次の図を参照）。 たとえば、スイッチ 1 に接続された ISL の許可 VSAN リストから VSAN 2 と VSAN 4 を削除する場合、各 ISL の通信可能な VSAN リストは次のようになります。

- スイッチ 1 とスイッチ 2 の間の ISL には、VSAN 1 と VSAN 3 が含まれます。
- スイッチ 2 とスイッチ 3 の間の ISL には、VSAN 1 と VSAN 2 が含まれます。

- スイッチ 3 とスイッチ 1 の間の ISL には、VSAN 1、VSAN 2、および VSAN 5 が含まれます。

したがって、VSAN 2 だけがスイッチ 1 からスイッチ 3、さらにスイッチ 2 にルーティングできます。

図 *16*： 通信可能な許可 *VSAN* の設定



VSAN の許可アクティブ リストの設定

インターフェイスに VSAN の許可アクティブ リストを設定できます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface vfc** *vfc-id* 例： `switch(config)# interface vfc 4`	指定されたインターフェイスを設定します。

	コマンドまたはアクション	目的
ステップ 3	**switchport trunk allowed vsan** *vsan-id* **-** *vsan-id* 例： `switch(config-if)# switchport trunk allowed vsan 35-55`	指定された VSAN 範囲の許可リストを変更します。
ステップ 4	**switchport trunk allowed vsan add** *vsan-id* 例： `switch(config-if)# switchport trunk allowed vsan add 40`	指定された VSAN を新しい許可リストに追加します。
ステップ 5	**no switchport trunk allowed vsan** *vsan-id* **-** *vsan-id* 例： `switch(config-if)# no switchport trunk allowed vsan 61-65`	指定された VSAN 範囲を削除します。
ステップ 6	**no switchport trunk allowed vsan add** *vsan-id* 例： `switch(config-if)# no switchport trunk allowed vsan add 40`	追加された許可リストを削除します。

VSAN トランキング情報の表示

show interface コマンドを EXEC モードから呼び出して、TE ポートの VSAN トランキング設定を表示します。 引数を入力せずに、このコマンドを実行すると、スイッチに設定されたすべてのインターフェイスの情報が表示されます。

次に、ファイバ チャネル インターフェイスのトランク モードを表示する例を示します。

```
switch# show interface vfc33
vfc33 is up
    Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:83:00:0d:ec:6d:78:40
    Peer port WWN is 20:0c:00:0d:ec:0d:d0:00
    Admin port mode is auto, trunk mode is on
...
```

次に、ファイバ チャネル インターフェイスのトランク プロトコルを表示する例を示します。

```
switch# show trunk protocol
Trunk protocol is enabled
```

次に、すべてのトランク インターフェイスの VSAN 情報を表示する例を示します。

```
switch# show interface trunk vsan 1-1000
vfc31 is not trunking
...
vfc311 is trunking
    Belongs to san-port-channel 6
    Vsan 1 is up, FCID is 0xef0000
    Vsan 2 is up, FCID is 0xef0000
...
san-port-channel 6 is trunking
    Vsan 1 is up, FCID is 0xef0000
    Vsan 2 is up, FCID is 0xef0000
```

VSAN トランクのデフォルト設定

次の表は、VSAN トランキング パラメータのデフォルト設定をリスト表示しています。

表 *7*：デフォルトの *VSAN* トランク設定パラメータ

パラメータ	デフォルト
スイッチ ポートのトランク モード	On
許可 VSAN リスト	1 ～ 4093 のユーザ定義の VSAN ID
トランキング プロトコル	イネーブル

第 6 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 Storage Area Network（SAN; ストレージ エリア ネットワーク）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。

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。

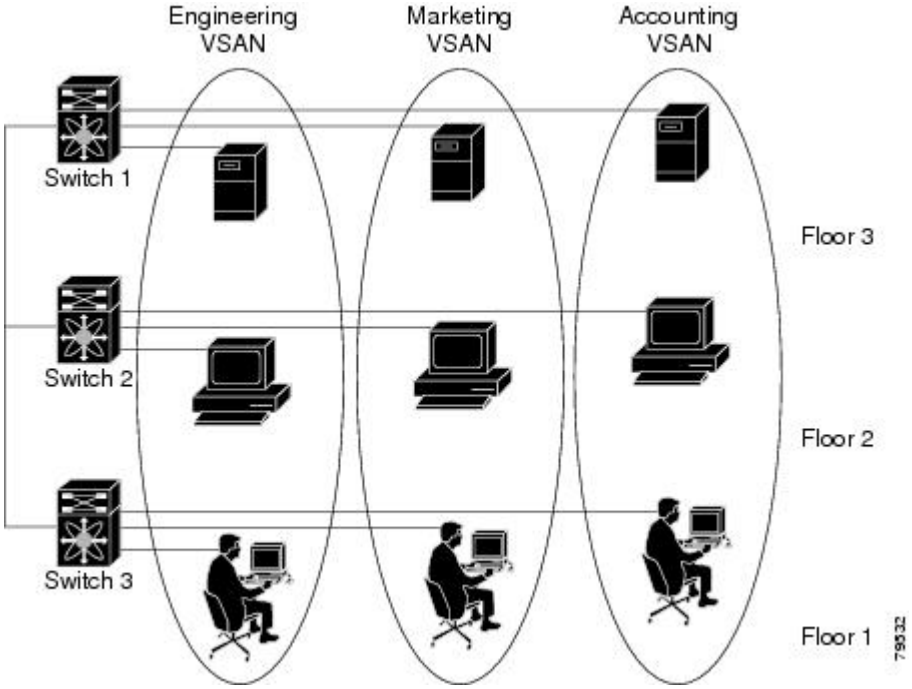
VSAN トポロジ

VSAN には次の特性もあります。

- 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。

次の図では、3 台のスイッチが各フロアに 1 台ずつあるファブリックを示します。 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。

図 *17*： 論理 *VSAN* の区分け

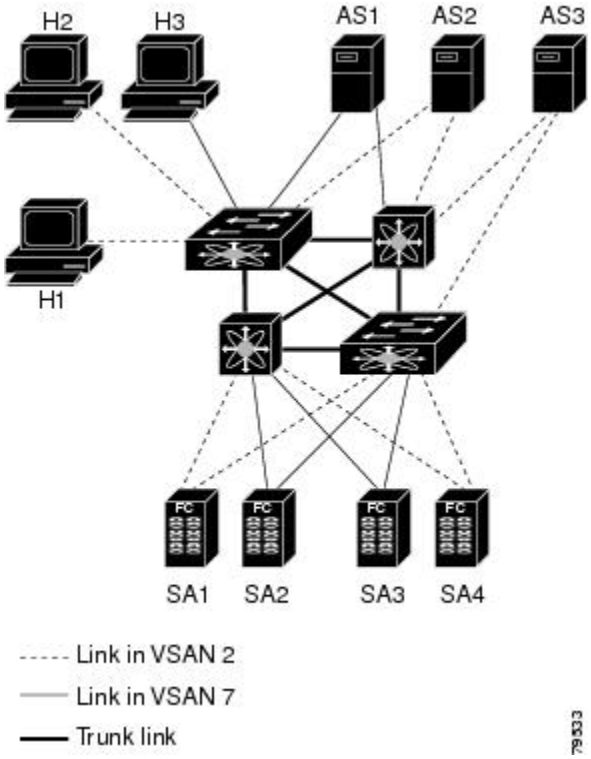


アプリケーション サーバまたはストレージアレイは、ファイバ チャネルまたは仮想ファイバ チャネル インターフェイスを使用してスイッチに接続できます。 VSAN には、ファイバ チャネル インターフェイスと仮想ファイバ チャネル インターフェイスを組み合わせて含めることができます。

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 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。

図 *18*： *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 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。 次の図は、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 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 256 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）です。 ユーザ指定の VSAN ID 範囲は 2 ～ 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。

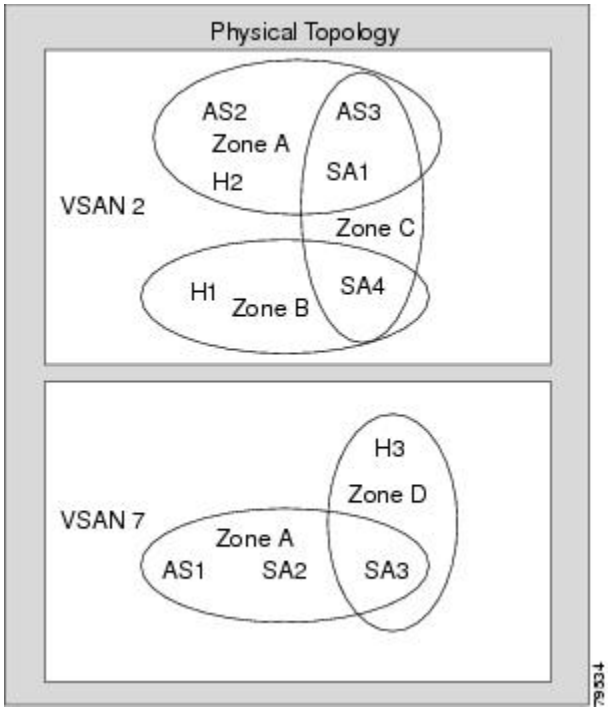
表 *8*： *VSAN* とゾーンの比較

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、通常 pWWN によって定義されます。

VSAN 特性	ゾーン特性
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。

図 *19*： ***VSAN*** とゾーン分割



VSAN の注意事項と制約事項

VSAN 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）、ユーザ定義の VSAN（VSAN 2 ～ 4093）、および独立 VSAN（VSAN 4094）で 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。

（注） 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。

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。

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	**vsan database** 例： `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* 例： `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* 例： `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** 例： `switch(config-vsan-db)# vsan 470 suspend`	選択された VSAN を中断します。
ステップ 6	switch(config-vsan-db)# **no vsan** *vsan-id* **suspend** 例： `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** 例： `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。 2 つの方式のいずれかを使用して、ポートに VSAN メンバーシップを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。 この方法は Dynamic Port VSAN Membership（DPVM）機能といいます。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。

関連トピック

スタティック ポート VSAN メンバーシップの概要, （76 ページ）
VSAN トランキングの設定, （59 ページ）

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。

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	**vsan database**
	
	例：
	`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* 例： `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	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。 （注） 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。

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
```

（注） 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 VSAN 1 のみがイネーブルです。 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。

（注） VSAN 1 は削除できませんが、中断できます。

最大 256 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）です。 ユーザ指定の VSAN ID 範囲は 2 ～ 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）。

（注） 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。

注意 独立 VSAN を使用してポートを設定しないでください。

（注） 最大 256 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）です。 ユーザ指定の VSAN ID 範囲は 2 ～ 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。

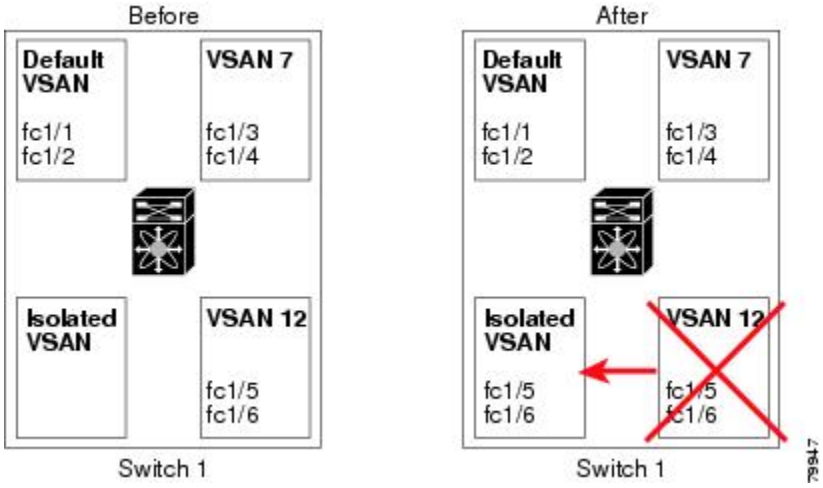
スタティック VSAN の削除

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）。

図 *20*： ***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）、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。

（注） 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。

関連トピック

VSAN トランキングの設定，（59 ページ）

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。

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	**vsan database**
	
	例：
	`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* 例： `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* 例： `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** 例： `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。

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	**vsan database**
	
	例：
	`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* 例： `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** 例： `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** 例： `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** 例： `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** 例： `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** 例： `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。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `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。

関連トピック

スイッチの相互運用性

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。

表 *9*：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
ステート	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 7 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。

この章の内容は、次のとおりです。

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 グループ間のアクセス コントロールの設定が可能になります。 ファブリックで管理者権限を持つユーザは、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。

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。

- 1 つのゾーンは、複数のゾーン メンバーから構成されます。
  - 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。
  - 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 500 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（この機能が送信元スイッチでイネーブルである場合）。
  - 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、次の識別情報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 をゾーンのメンバーとして指定します。
  - 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 をゾーンのメンバーとして指定します。
  - 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。

（注） 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、N ポートの pWWN、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。

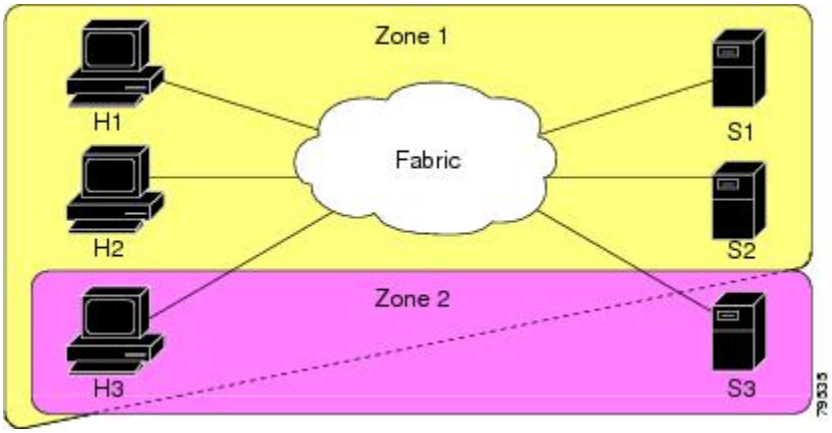
- デフォルト ゾーン メンバーシップには、特定のメンバーシップとの関係を持たないすべてのポートまたは WWN が含まれます。 デフォルト ゾーン メンバー間のアクセスは、デフォルト ゾーン ポリシーによって制御されます。
- VSAN あたり最大 8000 ゾーン、スイッチ上の全 VSAN で最大 8000 ゾーンを設定できます。

（注） インターフェイスベース ゾーン分割は、Cisco SAN スイッチだけで機能します。 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。

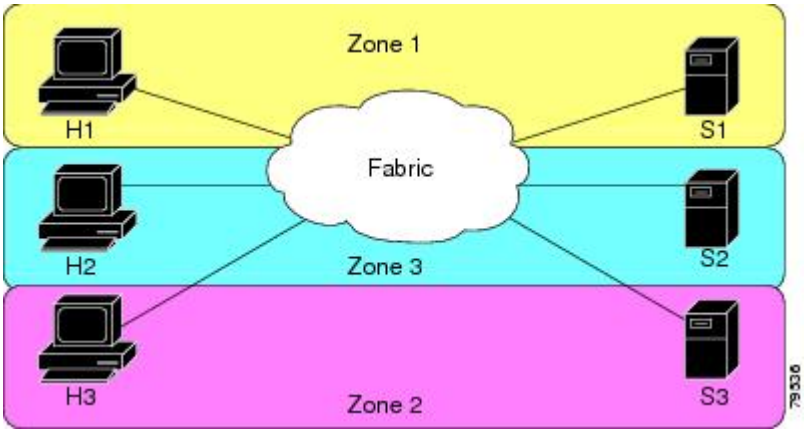
図 *21*： *2* つのゾーンによるファブリック



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。

図 *22*： *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 ゾーン分割をディセーブルにできません。
- ネーム サーバ 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。
- ゾーンを再アクティブ化（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

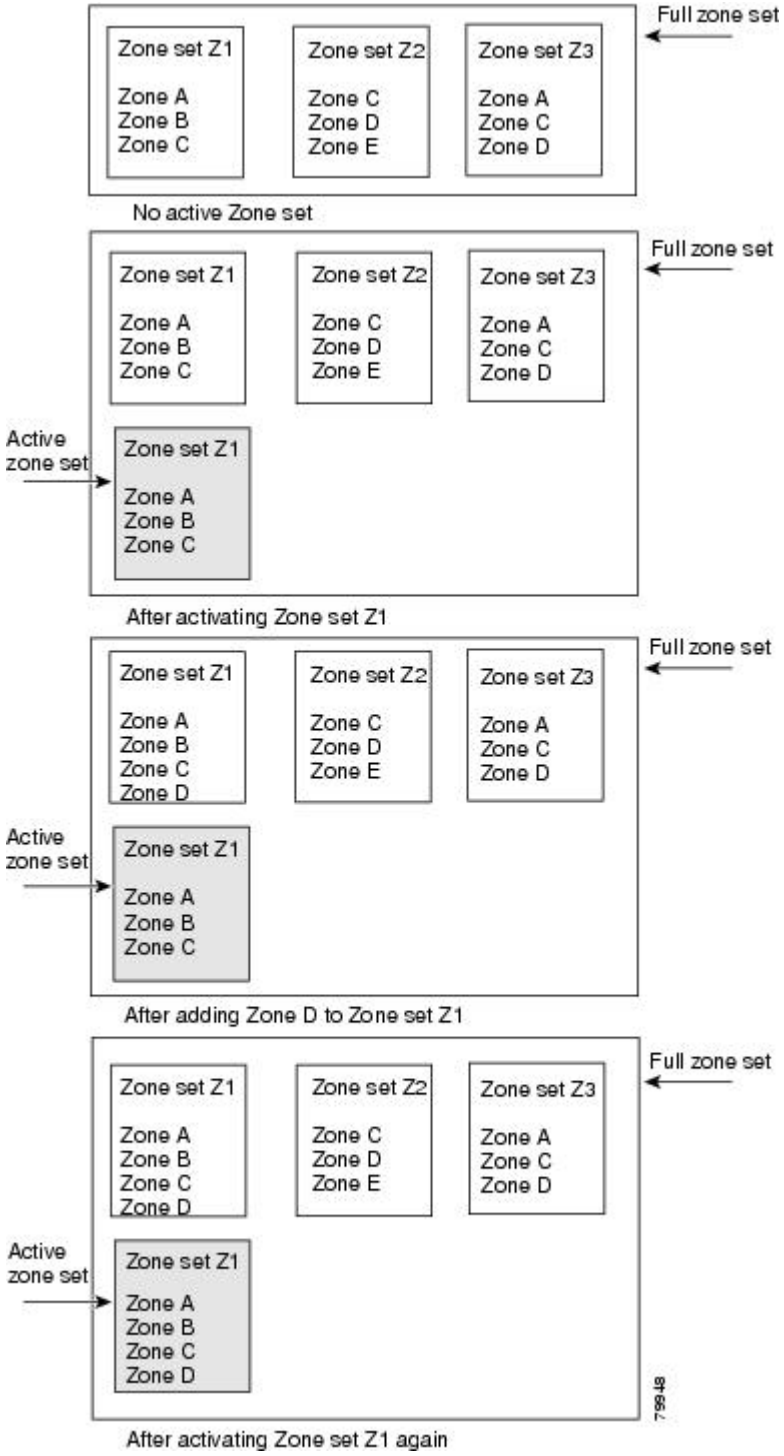
ゾーン セットを設定する前に、次の注意事項について検討してください。

- 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 セットのゾーン セットのコピーがゾーン分割に使用されます。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。

（注） 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。

図 *23*： 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。

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	**zone name** *zone-name* **vsan** *vsan-id* 例： `switch(config)# zone name test vsan 5`	指定された VSAN にゾーンを設定します。 （注） 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* 例： `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、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。 注意 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。 ヒント 該当する表示コマンド（たとえば、**show interface** または **show flogi database**）を使用して、必要な値を 16 進表記で取得します。

設定例

ヒント **show wwn switch** コマンドを使用して sWWN を取得します。 sWWN を指定しない場合は、自動的にローカル sWWN が使用されます。

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
```

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
```

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
```

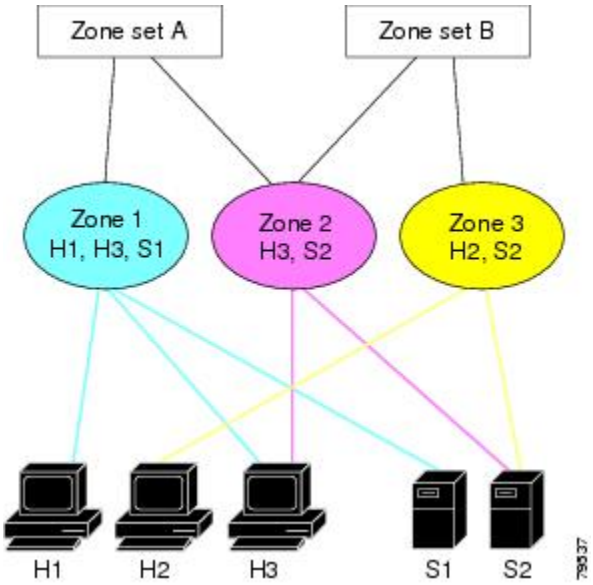
デバイス エイリアスの例：

```
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。

図 *24*： ゾーン セット、ゾーン、ゾーン メンバの階層



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。

ヒント　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。

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	**zoneset activate name** *zoneset-name* **vsan** *vsan-id* 例： `switch(config)# zoneset activate name test vsan 34`	指定されたゾーンセットをアクティブにします。
ステップ 3	**no zoneset activate name** *zoneset-name* **vsan** *vsan-id* 例： `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。

（注） 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。

（注） 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。

（注） 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 として設定されている場合、またはゾーン セットがアクティブの場合、デフォルト ゾーン メンバーが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は、アクティブなゾーン セットを表示しても、このゾーンのメンバーは明示的に一覧表示されません。

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。

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	**zone default-zone permit vsan** *vsan-id* 例： `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* 例： `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 ポート名の WWN は 16 進形式です（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。

ヒント　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

エイリアスを設定します。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**fcalias name** *alias-name* **vsan** *vsan-id* 例： `switch(config)# fcalias name testname vsan 50`	エイリアス名を設定します。 エイリアス名には最大 64 文字の英数字文字列を指定します。大文字と小文字は区別されます。
ステップ 3	**member** *type value* 例： `switch(config-fcalias)# member pwwn 4`	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を設定します。 （注）　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

表 *10*：***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	**member domain-id** *domain-id* **portnumber** *number*

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* （注） これが 10G ブレークアウト ポートの場合、*slot/port* 構文は *slot/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 （注） これが 10G ブレークアウト ポートの場合、*slot/port* 構文は *slot/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* （注） これが 10G ブレークアウト ポートの場合、*slot/port* 構文は *slot/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 ゾーンを追加できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コ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* 例： `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。 ヒント　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* 例： `switch(config-zoneset)# member new`	以前指定したゾーン セットのメンバとしてゾーンを追加します。 ヒント　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。
ステップ 4	**zone name** *zone-name* 例： `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。 ヒント　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* 例： `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。 ヒント　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。

ヒント　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アクティブ ゾーン セットを保存する必要はありません。 ただし、明示的にフル ゾーン セットを保存するには、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 サーバにログインすると、ネーム サーバ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、ゾーン分割制限がネームサーバ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。

（注） 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 のスイッチは、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。

表 *11*：ゾーン セット配信の相違

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 セット配信のイネーブル化

Cisco SAN のすべてのスイッチは、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。

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	**zoneset distribute full vsan** *vsan-id* 例： `switch(config)# zoneset distribute full vsan 12`	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。

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。

（注） フルゾーンセットの一時配信は interop 2 および interop 3 モードでサポートされており、interop 1 モードではサポートされていません。

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。

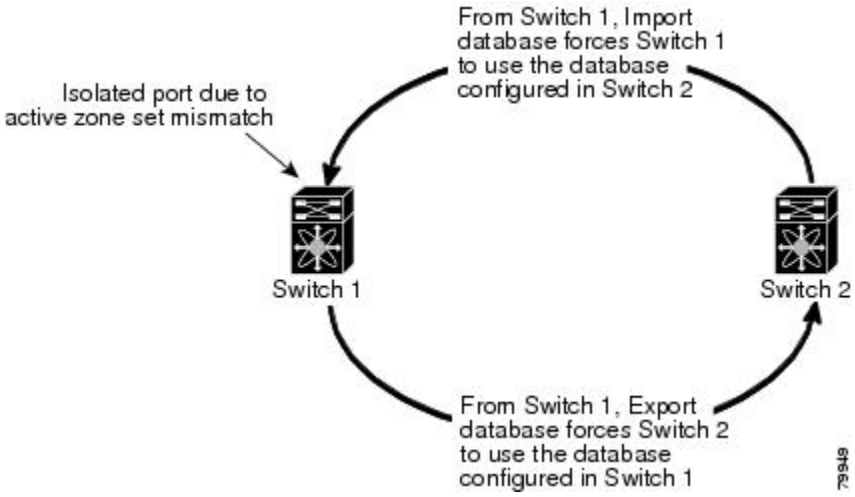
```
switch# show zone status vsan 3
VSAN: 3 default-zone: permit distribute: active only Interop: 100
    mode:basic merge-control:allow

    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 ポートが分離することがあります。 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。

- 近隣スイッチのアクティブ ゾーン セット 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（次の図を参照してください）。
- 現在のデータベースを隣接の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。

図 *25*： 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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **zoneset import interface vfc** *vfc-id* **vsan** *vsan-id*	VSAN または VSAN の範囲に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。

	コマンドまたはアクション	目的
ステップ 2	**zoneset export vsan** *vsan-id* 例： `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 セット配信

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。

注意 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。

手順

	コマンドまたはアクション	目的
ステップ 1	**zone copy active-zoneset full-zoneset vsan** *vsan-id* 例： `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。

	コマンドまたはアクション	目的
ステップ 2	**zone copy vsan** *vsan-id* **active-zoneset scp://guest@myserver/tmp/active_zoneset.txt** 例： `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。

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	**zoneset rename** *oldname newname* **vsan** *vsan-id* 例： `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* 例： `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* 例： `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* 例： `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。

	コマンドまたはアクション	目的
ステップ 6	**zoneset activate name** *newname* **vsan** *vsan-id* 例： `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、ゾーン セット、FC エイリアス、およびゾーン属性グループのコピー

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をコピーできます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コ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* 例： `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* 例： `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* 例： `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* 例： `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* 例： `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 データベースのクリア

指定された VSAN のゾーン サーバ 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 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
```

（注） **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コンフィギュレーションが使用されるようにする必要があります。

（注） 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-id*	VSAN 範囲に設定されたゾーン セットの表示
show zone nam*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。

次の表に、Cisco SAN スイッチのすべてのスイッチの拡張ゾーン分割機能の利点を示します。

表 *12*： 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、サイズも顕著になります。
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になります。

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。

手順

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。

手順

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すべての Cisco SAN スイッチでディセーブルです。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**zone mode enhanced vsan** *vsan-id* 例： `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* 例： `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。

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	**zone commit vsan** *vsan-id* 例： `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** 例： `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* 例： `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** 例： `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
```

（注） 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。

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。

表 *13*：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 1 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	ISL は分離されます。
データベースには、同じ名前 1 で、異なるメンバを持つゾーン、ゾーン 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。
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。

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	**zone merge-control restrict vsan** *vsan-id* 例： `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* 例： `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* 例： `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。

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	**zone default-zone permit vsan** *vsan-id* 例： `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* 例： `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。
ステップ 4	**zone commit vsan** *vsan-id* 例： `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。

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	**system default zone default-zone permit** 例： `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。

	コマンドまたはアクション	目的
ステップ 3	**no system default zone default-zone permit** 例： `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** 例： `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** 例： `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。

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
```

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。

（注） 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。

手順

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的
ステップ 2	**no zone name** *zone-name* **vsan** *vsan-id* 例： `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* 例： `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。

表 *14*：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 8 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。

この章の内容は、次のとおりです。

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 エイリアスの概要

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、DPVM、ポート セキュリティなど）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、これらの機能の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。 デバイス名が間違っていると、予期しない結果を引き起こす可能性があります。 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、協調型配信モードおよびファブリック規模の配信範囲を使用します。
- 基本モードと拡張モード。
- ゾーン、IVR ゾーン、またはポートセキュリティ機能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。

関連トピック

デバイス エイリアスのモード, （118 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。

表 *15*： 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 エイリアス設定を FCNS、ゾーン、fcping、および traceroute 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。

手順

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的

ステップ 2	**device-alias database**
	
	例：
	`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* 例： `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* 例： `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* 例： `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

エイリアスが基本モードまたは拡張モードで動作するように指定できます。

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。

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、PSM、または DPVM 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。

（注） 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約事項

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。

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	**device-alias mode enhanced** 例： `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** 例： `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はありません。 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。

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。保留中のデータベースへの変更内容をコミットまたは廃棄（**中断**）するまで、保留中の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。

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	**device-alias commit** 例： `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。

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	**device-alias abort** 例： `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# show device-alias status
Fabric Distribution: Enabled
Database:- Device Aliases 24
Status of the last CFS operation issued from this switch:
==========================================================
Operation: Abort
Status: Success
```

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。

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 device-alias distribute** 例： `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** 例： `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: Enabled <-------------------------------Distribution is enabled

Database:-Device Aliases 24

Locked By:-User "Test" SWWN 20:00:00:0c:cf:f4:02:83<-Lock holder's user name and switch ID

Pending Database:- Device Aliases 24

Status of the last CFS operation issued from this switch:
```

```
=========================================================

Operation: Enable Fabric Distribution

Status: Success
```

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 24

Status of the last CFS operation issued from this switch:

=========================================================

Operation: Disable Fabric Distribution

Status: Success
```

レガシー ゾーン エイリアスの設定

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。 ファブリック内のほかのスイッチに設定を配布したくない場合、**abort** 操作を行うと、結合の変更内容が完全に廃棄されます。

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。

手順

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的
ステップ **2**	**device-alias import fcalias vsan** *vlan-id* 例： `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 エイリアス設定の確認

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。

表 *16*： 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
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 9 章

FLOGI、ネーム サーバ、FDMI、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、FDMI、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、FDMI、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 FC ID 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か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 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。

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
```

ネーム サーバ プロキシ

ネーム サーバ機能は、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 プロキシ登録の概要

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

ネーム サーバ プロキシを登録できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル 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	**fcns proxy-port** *wwn-id* **vsan** *vsan-id* 例： `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

別のデバイスの pWWN を使用した悪意のあるログインまたは偶発的なログインを回避するには、reject-duplicate-pwwn オプションをイネーブルにします。 このオプションをディセーブルにすると、このような pWWN のファブリックへのログインが許可され、ネーム サーバ データベースにある最初のデバイスと置き換えられます。

重複 pWWN の拒否

重複 pWWN を拒否できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal switch(config)#`	グローバル コ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* 例： `switch(config)# fcns reject-duplicate-pwwn vsan 100`	pWWN がすでに存在する場合は、デバイスがファブリックにログインする際に、デバイスをログアウトします。
ステップ 3	**no fcns reject-duplicate-pwwn vsan** *vsan-id* 例： `switch(config)# no fcns reject-duplicate-pwwn vsan 256`	同一の pWWN を持つ新しいデバイスでネーム サーバ データベースにある最初のデバイスのエントリを上書きします（デフォルト）。

ネーム サーバ データベース エントリ

ネーム サーバ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 サーバを使用すると、Nx ポートで（ネーム サーバへの）PLOGI 中に属性を登録し、その他のホストの属性を取得できます。 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 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 プロセスのインスタンスが実行されます。

ネーム サーバのデータベース エントリの表示

次に、すべての VSAN のネーム サーバ データベースを表示する例を示します。

```
switch# show fcns database
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x010000    N     50:06:0b:00:00:10:a7:80                   scsi-fcp fc-gs

0x010001    N     10:00:00:05:30:00:24:63 (Cisco)           ipfc

0x010002    N     50:06:04:82:c3:a0:98:52 (Company 1)       scsi-fcp 250

0x010100    N     21:00:00:e0:8b:02:99:36 (Company A)       scsi-fcp

0x020000    N     21:00:00:e0:8b:08:4b:20 (Company A)
0x020100    N     10:00:00:05:30:00:24:23 (Cisco)           ipfc

0x020200    N     21:01:00:e0:8b:22:99:36 (Company A)       scsi-fcp
```

次に、指定されたVSANのネーム サーバ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
--------------------------------------------------------------------------
0x030001    N     10:00:00:05:30:00:25:a3 (Cisco)         ipfc
0x030101    NL    10:00:00:00:77:99:60:2c (Interphase)
0x030200    N     10:00:00:49:c9:28:c7:01
0xec0001    NL    21:00:00:20:37:a6:be:14 (Seagate)       scsi-fcp
Total number of entries = 4
```

次に、すべての VSAN のネーム サーバ データベースの詳細を表示する例を示します。

```
switch# show fcns database detail
```

次に、すべての VSAN のネーム サーバ データベースの統計を表示する例を示します。

```
switch# show fcns statistics
```

FDMI

Cisco SAN スイッチは、FC-GS-4 規格で記述されている Fabric-Device 管理インターフェイス（FDMI）機能をサポートしています。 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 サーバおよび管理サーバ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
```

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。

（注） 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。

（注） 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
```

（注） 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 オプションをイネーブルに設定すると、登録済みの Nx ポートに対して生成された RSCN に、影響を受けた複数のポート ID が含まれる場合があります。 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 の multi-pid オプションがディセーブル：ホスト H に対して、2 つの RSCN（ディスク D1 とディスク D2 に関して 1 つずつ）が生成されます。
- スイッチ 1 の multi-pid オプションがイネーブル：ホスト H に対して単一の RSCN が生成されます。RSCN ペイロードには、影響を受けたポート ID が一覧表示されます（この場合は、D1 と D2 の両方）。

（注） 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 multi-pid オプションをディセーブルにしてください。

multi-pid オプションの設定

multi-pid オプションを設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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 multi-pid vsan** *vsan-id* 例： `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。

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 suppress domain-swrscn vsan** *vsan-id* 例： `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。

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** コマンドを入力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。

（注） 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。

（注） 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。

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 distribute** 例： `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。

	コマンドまたはアクション	目的
ステップ 3	**rscn event-tov** *timeout* **vsan** *vsan-id* 例： `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* 例： `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* 例： `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。 つまり、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。

（注） 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。 配信されるのは、**rscn event-tov tov vsan vsan** コマンドのみです。

注意 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。

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 distribute** 例： `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** 例： `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設定がコミットされます。 コミットが正常に行われると、設定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。

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 commit vsan** *timeout* 例： `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。

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 abort vsan** *timeout* 例： `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
```

（注） 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。

（注） 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
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 ms vsan 10
+ rscn event-tov 300 ms vsan 10
```

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。

表 *17*： 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	ディセーブル

第 10 章

SCSI ターゲットの検出

この章の内容は、次のとおりです。

SCSI ターゲットの検出

SCSI LUN 検出に関する情報

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 サーバに論理ユニット番号（LUN）を登録しません。

ネーム サーバには、次の理由により、LUN 情報が必要となります。

- NMS（Network Management System; ネットワーク管理システム）がアクセスできるように、LUN ストレージ デバイス情報を表示するため。
- デバイスのキャパシティ、シリアル番号、およびデバイス ID 情報を表示するため。
- ネーム サーバにイニシエータおよびターゲット機能を登録するため。

SCSI LUN 検出機能には、ローカル ドメイン コントローラ ファイバ チャネル アドレスが使用されます。 この機能はローカル ドメイン コントローラをソース FC ID として使用し、SCSI デバイス上で SCSI INQUIRY、REPORT LUNS、および READ CAPACITY コマンドを実行します。

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 デバイスの場合、この情報は近接スイッチとも同期されます。

SCSI LUN 検出の開始について

SCSI LUN 検出はオンデマンドで実行されます。

ネーム サーバ データベース内の Nx ポートのうち、FC4 Type = SCSI_FCP として登録されたものだけが検出されます。

SCSI LUN 検出の開始

SCSI LUN 検出を開始する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **discover scsi-target** {**custom-list** | **local** | **remote** | **vsan** *vsan-id* **fcid** *fc-id*} **os** {**aix** | **hpux** | **linux** | **solaris** | **windows**} [**lun** | **target**]	指定されたオペレーティング システム（OS）の SCSI ターゲットを検出します。

SCSI LUN 検出を開始する例

次に、すべてのオペレーティング システム（OS）のローカル SCSI ターゲットを検出する例を示します。

```
switch# discover scsi-target local os all
discovery started
```

次に、AIX OS に割り当てられたリモート SCSI ターゲットを検出する例を示します。

```
switch# discover scsi-target remote os aix
discovery started
```

次に、VSAN（仮想 SAN）1 および FC ID 0x9c03d6 に対応する SCSI ターゲットを検出する例を示します。

```
switch# discover scsi-target vsan 1 fcid 0x9c03d6
discover scsi-target vsan 1 fcid 0x9c03d6
VSAN:    1 FCID: 0x9c03d6 PWWN: 00:00:00:00:00:00:00:00
  PRLI RSP: 0x01 SPARM: 0x0012
  SCSI TYPE: 0 NLUNS: 1
  Vendor: Company 4 Model: ST318203FC    Rev: 0004
  Other: 00:00:02:32:8b:00:50:0a
```

次に、Linux OS に割り当てられたカスタマイズ リストから SCSI ターゲットを検出する例を示します。

```
switch# discover scsi-target custom-list os linux
discovery started
```

カスタマイズ検出の開始について

カスタマイズ検出は、検出を開始するように選択的に設定された VSAN とドメインのペア リストによって行われます。 この検出を開始するには、custom-list オプションを使用します。 ドメイン ID は 0 ～ 255 の数値（10 進数）、または 0x0 ～ 0xFF の数値（16 進数）です。

カスタマイズ検出の開始

カスタマイズ検出を開始する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **discover custom-list add vsan** *vsan-id* **domain** *domain-id*	指定されたエントリをカスタムリストに追加します。
ステップ 2	switch# **discover custom-list delete vsan** *vsan-id* **domain** *domain-id*	指定されたドメイン ID をカスタム リストから削除します。

SCSI LUN 情報の表示

検出結果を表示するには、**show scsi-target** および **show fcns database** コマンドを使用します。

次に、検出されたターゲットを表示する例を示します。

```
switch# show scsi-target status
discovery completed
```

（注） このコマンドを完了するには、数分間かかることがあります（特に、ファブリックが大規模である場合や、複数のデバイスの応答速度が遅い場合）。

次に、FCNS データベースを表示する例を示します。

```
switch# show fcns database
```

次に、SCSI ターゲット ディスクを表示する例を示します。

```
switch# show scsi-target disk
```

次に、すべてのオペレーティング システムの検出済み LUN を表示する例を示します。

```
switch# show scsi-target lun os all
```

次に、各オペレーティング システム（Windows、AIX、Solaris、Linux、または HPUX）に割り当てられたポート WWN を表示する例を示します。

```
switch# show scsi-target pwwn
```

第 11 章

FC-SP および DHCHAP の設定

この章では、Fibre Channel Security Protocol（FC-SP）と Diffie-Hellman Challenge Handshake Authentication Protocol（DHCHAP）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。

FC-SP および DHCHAP に関する情報

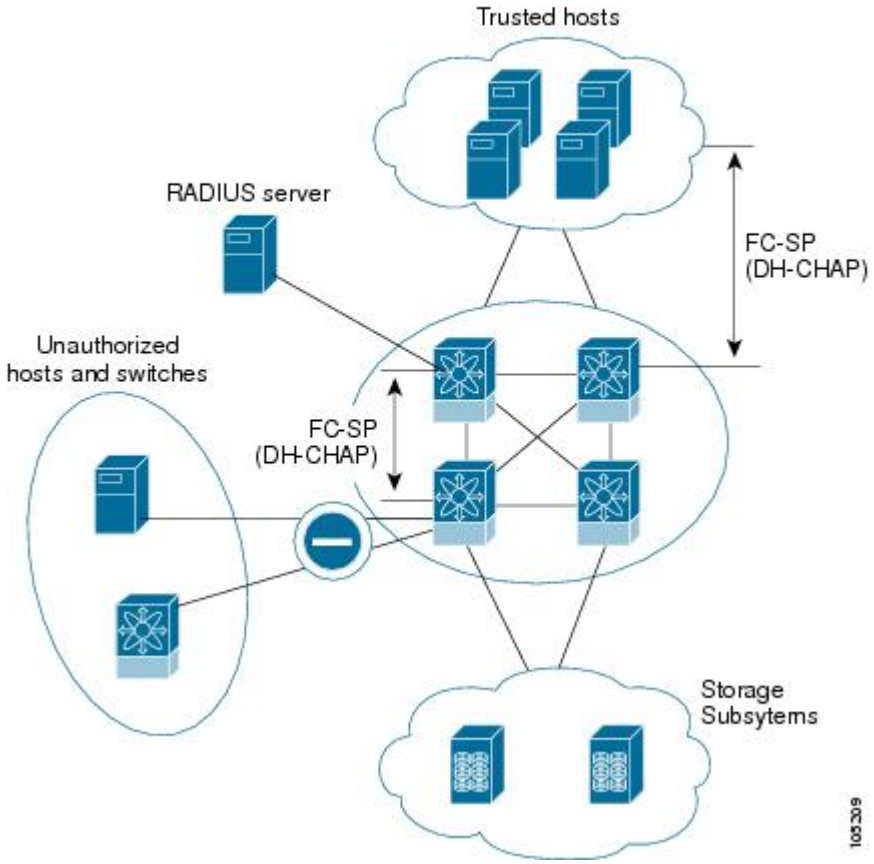
Fibre Channel Security Protocol（FC-SP）機能は、スイッチとスイッチ間およびホストとスイッチ間で認証を実行して、企業全体のファブリックに関するセキュリティ問題を解決します。Diffie-Hellman チャレンジハンドシェイク認証プロトコル（DHCHAP）は、Cisco SAN スイッチとその他のデバイス間で認証を行う FC-SP プロトコルです。 DHCHAP は、CHAP プロトコルと Diffie-Hellman 交換を組み合わせて構成されています。

ファブリック認証

Cisco SAN の全スイッチで、1 台のスイッチから他のスイッチへ、またはスイッチからホストへ、ファブリック規模の認証を実行できます。 これらのスイッチおよびホスト認証は、各ファブリックでローカルまたはリモートで実行できます。 ストレージアイランドを企業全体のファブリックに統合して、移行すると、新しいセキュリティ問題が発生します。 ストレージアイランドを保護する方法が、企業全体のファブリックで必ずしも保証されなくなります。 たとえば、スイッチが地理的に分散しているキャンパス環境では、他のユーザが故意に、またはユーザ自身が誤って、互換性のないスイッチに故意に相互接続すると、ISL（スイッチ間リンク）分離やリンク切断が発生することがあります。

Cisco SAN スイッチでは、物理的なセキュリティに対処する認証機能がサポートされます（次の図を参照）。

図 *26*：スイッチおよびホストの認証



（注） ホスト スイッチ認証には、適切なファームウェアおよびドライバを備えたファイバ チャネル Host Bus Adapter（HBA）が必要です。

DHCHAP 認証の設定

ローカル パスワード データベースを使用する DHCHAP 認証を設定できます。

はじめる前に

ファブリック認証用のコンフィギュレーション コマンドおよび確認コマンドにアクセスするには、DHCHAP機能をイネーブルにする必要があります。 この機能をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

手順

ステップ 1 DHCHAP をイネーブルにします。

ステップ 2 DHCHAP 認証モードを識別して設定します。

ステップ 3 ハッシュ アルゴリズムおよび DH グループを設定します。

ステップ 4 ローカル スイッチおよびファブリックの他のスイッチの DHCHAP パスワードを設定します。

ステップ 5 再認証の DHCHAP タイムアウト値を設定します。

ステップ 6 DHCHAP の設定を確認します。

ファイバ チャネル機能と DHCHAP の互換性

DHCHAP 機能を既存の Cisco NX-OS 機能と一緒に設定した場合、互換性の問題を考慮してください。

- SAN ポートチャネル インターフェイス：SAN ポートチャネルに属しているポートに対して DHCHAP がイネーブルの場合、DHCHAP 認証はポートチャネル レベルではなく、物理インターフェイス レベルで実行されます。
- ポート セキュリティまたはファブリック バインディング：ファブリック バインディング ポリシーは、DHCHAP によって認証される ID に基づいて実行されます。
- VSAN：DHCHAP 認証は、VSAN 単位では実行されません。

デフォルトでは、DHCHAP 機能はすべての Cisco SAN スイッチでディセーブルです。

DHCHAP イネーブル化の概要

デフォルトでは、DHCHAP 機能はすべての Cisco SAN スイッチでディセーブルです。

ファブリック認証用のコンフィギュレーション コマンドおよび確認コマンドにアクセスするには、DHCHAP機能をイネーブルにする必要があります。 この機能をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

DHCHAP のイネーブル化

Cisco Nexus デバイス の DHCHAP をイネーブルに設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**fcsp enable** 例： `switch(config)# fcsp enable`	このスイッチ上でDHCHAPをイネーブルにします。
ステップ 3	**no fcsp enable** 例： `switch(config)# no fcsp enable`	このスイッチ上でDHCHAPをディセーブル（デフォルト）にします。

DHCHAP：認証モード

各インターフェイスの DHCHAP 認証ステータスは、DHCHAP ポート モードの設定によって変化します。

スイッチ内で DHCHAP 機能がイネーブルの場合には、各ファイバ チャネル インターフェイスまたは FCIP インターフェイスを次の 4 つの DHCHAP ポート モードのいずれかに設定できます。

- On：接続元デバイスがDHCHAP認証をサポートしている場合、スイッチ初期化中に認証シーケンスが実行されます。 接続元デバイスが DHCHAP 認証をサポートしていない場合には、リンクが分離状態になります。
- auto-Active：接続元デバイスがDHCHAP認証をサポートしている場合、スイッチ初期化中に認証シーケンスが実行されます。 接続元デバイスが DHCHAP 認証をサポートしていない場合には、ソフトウェアにより、初期化シーケンスの残りが実行されます。
- auto-Passive（デフォルト）：スイッチは DHCHAP 認証を開始しませんが、接続元デバイスが DHCHAP 認証を開始すれば、DHCHAP 認証に参加します。
- Off：スイッチはDHCHAP認証をサポートしません。 このモードでポートに認証メッセージが送信された場合、開始元スイッチにエラー メッセージが戻されます。

（注） DHCHAP ポート モードを off モード以外のモードに変更すると、再認証が実行されます。

次の表で、さまざまなモードに設定した 2 台のシスコ スイッチ間での認証について説明します。

表 *18* : *2* 台の *SAN* スイッチ間の *DHCHAP* 認証ステータス

スイッチ N の DHCHAP モード	スイッチ 1 の DHCHAP モード			
	on	**auto-active**	**auto-passive**	**off**
on	FC-SP 認証が実行されます。	FC-SP 認証が実行されます。	FC-SP 認証が実行されます。	リンクがダウンになります。
auto-Active				FC-SP 認証は実行されません。
auto-Passive			FC-SP 認証は実行されません。	
off	リンクがダウンになります。	FC-SP 認証は実行されません。		

DHCHAP モードの設定

特定のインターフェイスの DHCHAP モードを設定できます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	switch(config)# **interface vfc** *vfc-id* - *vfc-id*	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。
ステップ 3	**fcsp on** 例 : `switch(config-if)# fcsp on`	選択したインターフェイスの DHCHAP モードを on ステートに設定します。
ステップ 4	**no fcsp on** 例 : `switch(config-if)# no fcsp on`	これら 3 つのインターフェイスを出荷時デフォルトの auto-passive に戻します。

	コマンドまたはアクション	目的
ステップ 5	**fcsp auto-active 0** 例： `switch(config-if)# fcsp auto-active 0`	選択したインターフェイスの DHCHAP 認証モードを auto-active に変更します。 0 は、ポートが再認証を実行しないことを表します。 （注） 再許可インターバル設定は、デフォルトの動作と同じです。
ステップ 6	**fcsp auto-active** *timeout-period* 例： `switch(config-if)# fcsp auto-active 10`	選択したインターフェイスの DHCHAP 認証モードを auto-active に変更します。 タイムアウト期間の値（分）では、最初の認証後の再認証の頻度を設定します。
ステップ 7	**fcsp auto-active** 例： `switch(config-if)# fcsp auto-active`	選択したインターフェイスの DHCHAP 認証モードを auto-active に変更します。 再認証はディセーブルになります（デフォルト）。 （注） 再許可インターバル設定は、0 に設定した場合と同じです。

DHCHAP ハッシュ アルゴリズム

Cisco SAN スイッチは、DHCHAP 認証のためのデフォルトのハッシュ アルゴリズムのプライオリティ リストとして、最初に MD5、次に SHA-1 をサポートします。

ハッシュ アルゴリズムの設定を変更する場合は、ファブリック上の全スイッチに対して設定をグローバルに変更してください。

注意 RADIUS および TACACS+ プロトコルは、CHAP 認証で常に MD5 を使用します。 SHA-1 をハッシュ アルゴリズムとして使用すると、DHCHAP 認証用に RADIUS および TACACS+ がイネーブルになっていても、これらの AAA プロトコルが使用できなくなる可能性があります。

DHCHAP ハッシュ アルゴリズムの設定

ハッシュ アルゴリズムを設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**fcsp dhchap hash** [**md5**] [**sha1**] 例： `switch(config)# fcsp dhchap hash md5 sha1`	MD5 または SHA-1 ハッシュ アルゴリズムを使用するように設定します。
ステップ 3	**no fcsp dhchap hash sha1** 例： `switch(config)# no fcsp dhchap hash sha1`	出荷時デフォルトのハッシュ アルゴリズム プライオリティ リスト（最初に MD5、次に SHA-1）に戻します。

DHCHAP グループ設定

すべての Cisco SAN スイッチは、規格 0（Diffie-Hellman 交換を実行しないヌルの DH グループ）、1、2、3、または 4 で指定されたすべての DHCHAP グループをサポートします。

DH グループの設定を変更する場合は、ファブリック内のすべてのスイッチの設定をグローバルに変更してください。

DHCHAP グループの設定

DH グループの設定を変更できます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**fcsp dhchap dhgroup** [**0** | **1** | **2** | **3** | **4**] 例： `switch(config)# fcsp dhchap dhgroup [0|1|2|3|4]`	DH グループを設定された順序で使用するようにプライオリティ リスト化します。

	コマンドまたはアクション	目的
ステップ 3	**no fcsp dhchap dhgroup [0 | 1 | 2| 3 |]4]** 例： `switch(config)# no fcsp dhchap dhgroup [0|1|2|3|4]`	DHCHAP の出荷時デフォルトの順序（0、1、2、3、4）に戻します。

DHCHAP パスワード

DHCHAP 認証を実行する方向ごとに、接続デバイス間の共有シークレット パスワードが必要です。 このパスワードを使用するために、次の 3 つの設定例のいずれかを使用して DHCHAP に参加するファブリック内のすべてのスイッチのパスワードを管理します。

- 設定例 1：ファブリック内の全スイッチに同じパスワードを使用します。 これは最も単純な設定例です。 新しいスイッチを追加する場合、このファブリック内では同じパスワードを使用してそのスイッチを認証します。 したがってこれは、ファブリック内のいずれかのスイッチに外部から不正アクセスが試みられた場合に最も脆弱な設定例です。
- 設定例 2：スイッチごとに異なるパスワードを使用して、ファブリック内のスイッチごとにパスワード リストを保持します。 新しいスイッチを追加する場合は、新規パスワード リストを作成して、この新規リストを使用してすべてのスイッチを更新します。 いずれかのスイッチにアクセスすると、このファブリック上のすべてのスイッチに関するパスワードリストが生成されます。
- 設定例 3：ファブリック内のスイッチごとに、異なるパスワードを使用します。 新しいスイッチを追加する場合は、ファブリック内の各スイッチに対応する複数の新規パスワードを生成して、各スイッチに設定する必要があります。 いずれかのスイッチが被害にあっても、他のスイッチのパスワードは引き続き保護されます。 この設定例では、ユーザ側で大量のパスワード メンテナンス作業が必要になります。

（注） パスワードはすべて 64 文字以内の英数字に制限されます。パスワードは変更できますが、削除はできません。

スイッチが 6 台以上のファブリックでは、RADIUS または TACACS+ の使用をお勧めします。ローカル パスワード データベースを使用する必要がある場合、パスワード データベースを管理するために、設定 3 および Cisco MDS 9000 ファミリ Fabric Manager を引き続き使用できます。

ローカル スイッチの DHCHAP パスワードの設定

ローカル スイッチの DHCHAP パスワードを設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**fcsp dhchap password** [**0** | **7**] *password* [**wwn** *wwn-id*] 例： `switch(config)# fcsp dhchap password [0|7] myword wwn 11:22:11:22:33:44:33:44`	ローカル スイッチのクリアテキスト パスワードを設定します。

リモート デバイスのパスワード設定

ファブリック内の他のデバイスのパスワードを、ローカル認証データベースに設定できます。 他のデバイスは、スイッチ WWN やデバイス WWN といったデバイス名で表されます。 パスワードは 64 文字に制限され、クリア テキスト（0）または暗号化テキスト（7）で指定できます。

（注） スイッチ WWN は、物理スイッチを識別します。 この WWN はスイッチの認証に使用されます。また、VSAN ノード WWN とは異なります。

リモート デバイスの DHCHAP パスワードの設定

ファブリック内の他のスイッチのリモート DHCHAP パスワードをローカル側で設定できます。

手順

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的
ステップ 2	**fcsp dhchap devicename** *switch-wwn* **password** *password* 例： `switch(config)# fcsp dhchap devicename 21:00:05:30:23:1a:11:03 password mypassword`	スイッチ WWN デバイス名で表される、ファブリック上の他のスイッチのパスワードを設定します。
ステップ 3	switch(config)# **no fcsp dhchap devicename** *switch-wwn* **password** *password* 例： `switch(config)# no fcsp dhchap devicename 21:00:05:30:23:1a:11:03 password mypassword`	ローカル認証データベースから、このスイッチのパスワードエントリを削除します。

DHCHAP タイムアウト値

DHCHAP プロトコル交換を実行するとき、スイッチが指定時間内に予期した DHCHAP メッセージを受信しない場合、認証は失敗したと見なされます。 この（認証が失敗したと見なされるまでの）時間は、20 ～ 1000 秒の範囲で設定できます。 デフォルトは 30 秒です。

タイムアウト値を変更する場合には、次の要因について考慮してください。

- 既存の RADIUS および TACACS+ タイムアウト値。
- ファブリック内のすべてのスイッチに同じ値を設定する必要もあります。

DHCHAP タイムアウト値の設定

DHCHAP タイムアウト値を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**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	**fcsp timeout** *timeout* 例： `switch(config)# fcsp timeout 60`	再認証タイムアウトを指定された値に設定します。 単位は秒です。

	コマンドまたはアクション	目的
ステップ 3	**no fcsp timeout** *timeout* 例： `switch(config)# no fcsp timeout 60`	出荷時デフォルトの 30 秒に戻します。

DHCHAP AAA 認証の設定

AAA 認証で RADIUS または TACACS+ サーバ グループを使用するように設定できます。 AAA 認証を設定しない場合、デフォルトでローカル認証が使用されます。

プロトコル セキュリティ情報の表示

ローカル データベースの設定を表示するには、**show fcsp** コマンドを使用します。

次に、指定されたインターフェイスに関する DHCHAP 設定を表示する例を示します。

```
switch# show fcsp interface vfc24
vfc24
        fcsp authentication mode:SEC_MODE_ON
        Status: Successfully authenticated
```

次に、指定されたインターフェイスに関する DHCHAP 統計情報を表示する例を示します。

```
switch# show fcsp interface vfc24 statistics
```

次に、指定されたインターフェイスに接続されたデバイスの FC-SP WWN を表示する例を示します。

```
switch# show fcsp interface vfc21 wwn
```

次に、スイッチに設定済みのハッシュ アルゴリズムおよび DHCHAP グループを表示する例を示します。

```
switch# show fcsp dhchap
```

次に、DHCHAP ローカル パスワード データベースを表示する例を示します。

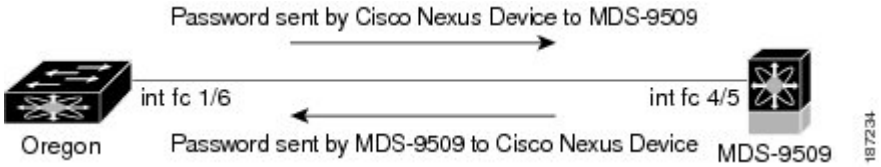
```
switch# show fcsp dhchap database
```

RADIUS サーバおよび TACACS+ サーバにスイッチ情報を設定する場合、デバイス WWN の ASCII 表記を使用してください。

ファブリック セキュリティの設定例

ここでは、次の図に示した例を設定するための手順について説明します。

図 *27*：***DHCHAP*** 認証の例



次の例は、認証の設定方法を示しています。

手順

ステップ 1 ファブリックの Cisco SAN スイッチのデバイス名を取得します。 ファブリックの Cisco SAN スイッチは、スイッチ WWN によって識別されます。

例：
```
switch# show wwn switch
Switch WWN is 20:00:00:05:30:00:54:de
```

ステップ 2 このスイッチで DHCHAP を明示的にイネーブルにします。

（注） DHCHAP をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

例：
```
switch(config)# fcsp enable
```

ステップ 3 このスイッチのクリア テキスト パスワードを設定します。 このパスワードは、接続先デバイスで使用されます。

例：
```
switch(config)# fcsp dhchap password rtp9216
```

ステップ 4 スイッチ WWN デバイス名で表される、ファブリック上の他のスイッチのパスワードを設定します。

例：
```
switch(config)# fcsp dhchap devicename 20:00:00:05:30:00:38:5e password rtp9509
```

ステップ 5 必要なインターフェイスの DHCHAP モードをイネーブルにします。

（注） DHCHAP ポート モードを off モード以外のモードに変更すると、再認証が実行されます。

例：
```
switch(config)# interface vfc24
switch(config-if)# fcsp on
```

ステップ 6 DHCHAP ローカル パスワード データベースを表示して、このスイッチに設定されたプロトコル セキュリティ情報を確認します。

例：
```
switch# show fcsp dhchap database
DHCHAP Local Password:
        Non-device specific password:*******
Other Devices' Passwords:
        Password for device with WWN:20:00:00:05:30:00:38:5e is *******
```

ステップ 7 インターフェイスの DHCHAP 設定を表示します。

例：
```
switch# show fcsp interface vfc24
vfc24
        fcsp authentication mode:SEC_MODE_ON
        Status:Successfully authenticated
```

ステップ 8 接続スイッチでこれらの手順を繰り返します。

例：
```
MDS-9509# show wwn switch
Switch WWN is 20:00:00:05:30:00:38:5e
MDS-9509(config)# fcsp enable
MDS-9509(config)# fcsp dhchap password rtp9509
MDS-9509(config)# fcsp dhchap devicename 20:00:00:05:30:00:54:de password rtp9216
MDS-9509(config)# interface vfc 45
MDS-9509(config-if)# fcsp on
MDS-9509# show fcsp dhchap database
DHCHAP Local Password:
        Non-device specific password:*******
Other Devices' Passwords:
        Password for device with WWN:20:00:00:05:30:00:54:de is *******
MDS-9509# show fcsp interface fc24
Fc24
        fcsp authentication mode:SEC_MODE_ON
        Status:Successfully authenticated
```

これで、設定例用の DHCHAP 認証が設定およびイネーブルにされました。

ファブリック セキュリティのデフォルト設定

次の表に、任意のスイッチにおけるすべてのファブリック セキュリティ機能のデフォルト設定を示します。

表 *19*：デフォルトのファブリック セキュリティ設定値

パラメータ	デフォルト
DHCHAP 機能	ディセーブル

パラメータ	デフォルト
DHCHAP ハッシュ アルゴリズム	最初に MD5、次に SHA-1 のプライオリティ リストで DHCHAP 認証を実行
DHCHAP 認証モード	auto-passive
DHCHAP グループのデフォルトの交換プライオリティ	0、4、1、2、3 の順
DHCHAP タイムアウト値	30 秒

第 12 章

ポート セキュリティの設定

この項では、ポート セキュリティの設定方法を説明します。

この章は、次の項で構成されています。

ポート セキュリティの設定

Cisco SAN スイッチには、侵入の試みを拒否して管理者に報告するポート セキュリティ機能が組み込まれています。

（注） ポート セキュリティは、仮想ファイバ チャネル ポートと物理ファイバ チャネル ポートでサポートされます。

ポート セキュリティについて

通常、SAN 内のすべてのファイバ チャネル デバイスを任意の SAN スイッチ ポートに接続して、ゾーン メンバーシップに基づいて SAN サービスにアクセスできます。 ポート セキュリティ機能は、次の方法を使用して、スイッチ ポートへの不正アクセスを防止します。

- 不正なファイバ チャネル デバイス（N ポート）およびスイッチ（xE ポート）からのログイン要求は拒否されます。
- 侵入に関するすべての試みは、システム メッセージを通して SAN 管理者に報告されます。
- 設定配信は CFS インフラストラクチャを使用し、CFS 対応スイッチに制限されています。配信はデフォルトでディセーブルになっています。
- ポート セキュリティ ポリシーを設定するには、ストレージ プロトコル サービス ライセンスが必要です。

（注） ポート セキュリティは、仮想ファイバ チャネル ポートと物理ファイバ チャネル ポートでサポートされます。

ポート セキュリティの実行

ポート セキュリティを実行するには、デバイスおよびスイッチ ポート インターフェイス（これらを通じて各デバイスまたはスイッチが接続される）を設定し、設定をアクティブにします。

- デバイスごとに N ポート接続を指定するには、Port World Wide Name（pWWN）または Node World Wide Name（nWWN）を使用します。
- スイッチごとに xE ポート接続を指定するには、Switch World Wide Name（sWWN）を使用します。

N および xE ポートをそれぞれ設定して、単一ポートまたはポート範囲に限定できます。

ポートセキュリティポリシーはポートがアクティブになるたび、およびポートを起動しようとした場合に実行されます。

ポート セキュリティ機能は 2 つのデータベースを使用して、設定の変更を受け入れ、実装します。

- コンフィギュレーションデータベース：すべての設定の変更がコンフィギュレーションデータベースに保存されます。
- アクティブ データベース：ファブリックが現在実行しているデータベース。 ポート セキュリティ機能を実行するには、スイッチに接続されているすべてのデバイスがポート セキュリティ アクティブ データベースに格納されている必要があります。 ソフトウェアはこのアクティブ データベースを使用して、認証を行います。

自動学習

指定期間内にポートセキュリティ設定を自動的に学習するように、スイッチを設定できます。 この機能を使用すると、任意のスイッチで、接続先のデバイスおよびスイッチについて自動的に学習できます。 ポートセキュリティ機能を初めてアクティブにするときに、この機能を使用してください。ポートごとに手動で設定する面倒な作業が軽減されます。 自動学習は、VSAN 単位で設定する必要があります。 この機能をイネーブルにすると、ポートアクセスを設定していない場合でも、スイッチに接続可能なデバイスおよびスイッチが自動学習されます。

自動学習がイネーブルのときは、まだスイッチにログインしていないデバイスまたはインターフェイスに関する学習だけ実行されます。 自動学習がまだイネーブルなときにポートをシャットダウンすると、そのポートに関する学習エントリが消去されます。

学習は、既存の設定済みのポートセキュリティポリシーを上書きしません。 たとえば、インターフェイスが特定の pWWN を許可するように設定されている場合、自動学習が新しいエントリを追

加して、そのインターフェイス上の他の pWWN を許可することはありません。 他のすべての pWWN は、自動学習モードであってもブロックされます。

シャットダウン状態のポートについては、学習エントリは作成されません。

ポート セキュリティ機能をアクティブにすると、自動学習も自動的にイネーブルになります。

（注） ポート セキュリティをアクティブにする前に自動学習をイネーブルにする場合、自動学習をディセーブルにするまでポート セキュリティをアクティブにできません。

ポート セキュリティのアクティブ化

デフォルトでは、ポート セキュリティ機能はアクティブにされていません。

ポート セキュリティ機能をアクティブにすると、次のようになります。

- 自動学習も自動的にイネーブルになります。つまり、
  - この時点から、スイッチにログインしていないデバイスまたはインターフェイスにかぎり、自動学習が実行されます。
  - 自動学習をディセーブルにするまで、データベースをアクティブにできません。
- すでにログインしているすべてのデバイスは学習され、アクティブ データベースに追加されます。
- 設定済みデータベースのすべてのエントリがアクティブ データベースにコピーされます。

データベースをアクティブにすると、以降のデバイスのログインは、自動学習されたエントリを除き、アクティブ化されたポートによってバインドされた WWN ペアの対象になります。 自動学習されたエントリがアクティブになる前に、自動学習をディセーブルにする必要があります。

ポート セキュリティ機能をアクティブにすると、自動学習も自動的にイネーブルになります。ポート セキュリティ機能をアクティブにし、自動学習をディセーブルにすることもできます。

ポートがログインを拒否されて停止している場合、その後でログインを許可するようにデータベースを設定しても、ポートは自動的に起動しません。 明示的に **no shutdown** コマンドを入力して、そのポートをオンラインに戻す必要があります。

ポート セキュリティの設定

自動学習と CFS 配信を使用するポート セキュリティの設定

自動学習と CFS 配信を使用するポート セキュリティを設定できます。

手順

ステップ 1 ポート セキュリティをイネーブルにします。

ステップ 2 CFS 配信をイネーブルにします。

ステップ 3 各 VSAN で、ポート セキュリティをアクティブにします。
デフォルトで自動学習が有効になります。

ステップ 4 CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。
すべてのスイッチで、ポート セキュリティがアクティブになり、自動学習がイネーブルになります。

ステップ 5 すべてのスイッチとすべてのホストが自動的に学習されるまで待ちます。

ステップ 6 各 VSAN で、自動学習をディセーブルにします。

ステップ 7 CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。
すべてのスイッチから自動学習されたエントリが、すべてのスイッチへ配信されるスタティックなアクティブ データベースに集約されます。

ステップ 8 各 VSAN のコンフィギュレーション データベースにアクティブ データベースをコピーします。

ステップ 9 CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。
これにより、ファブリック内のすべてのスイッチの設定済みデータベースが同一になります。

ステップ 10 ファブリック オプションを使用して、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。

関連トピック

ポート セキュリティのアクティブ化, （162 ページ）
変更のコミット, （172 ページ）
ポート セキュリティ データベースのコピー, （180 ページ）
自動学習のディセーブル化, （166 ページ）
ポート セキュリティのイネーブル化, （161 ページ）
ポート セキュリティの配信のイネーブル化, （171 ページ）

自動学習を使用し、CFS 配信を使用しないポート セキュリティの設定

自動学習を使用し、CFS 配信を使用しないポート セキュリティを設定できます。

手順

ステップ 1 ポート セキュリティをイネーブルにします。

ステップ 2 各 VSAN で、ポート セキュリティをアクティブにします。デフォルトで自動学習が有効になります。

ステップ 3 すべてのスイッチとすべてのホストが自動的に学習されるまで待ちます。

ステップ 4 各 VSAN で、自動学習をディセーブルにします。

ステップ 5 各 VSAN の設定済みデータベースにアクティブ データベースをコピーします。

ステップ 6 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。これにより、ポートセキュリティ コンフィギュレーションデータベースがスタートアップ コンフィギュレーションに保存されます。

ステップ 7 ファブリック内のすべてのスイッチに対して上記の手順を繰り返します。

関連トピック

ポート セキュリティのアクティブ化, （162 ページ）
ポート セキュリティ データベースのコピー, （180 ページ）
自動学習のディセーブル化, （166 ページ）
ポート セキュリティのイネーブル化, （161 ページ）

手動データベース設定によるポート セキュリティの設定

ポート セキュリティを設定し、手動でポート セキュリティ データベースを設定できます。

手順

ステップ 1 ポート セキュリティをイネーブルにします。

ステップ 2 各VSANの設定済みデータベースにすべてのポートセキュリティエントリを手動で設定します。

ステップ 3 各 VSAN で、ポート セキュリティをアクティブにします。 デフォルトで自動学習が有効になります。

ステップ 4 各 VSAN で、自動学習をディセーブルにします。

ステップ 5 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。これにより、ポートセキュリティ コンフィギュレーションデータベースがスタートアップ コンフィギュレーションに保存されます。

ステップ 6 ファブリック内のすべてのスイッチに対して上記の手順を繰り返します。

ポート セキュリティのイネーブル化

ポート セキュリティをイネーブルに設定できます。

デフォルトでは、ポート セキュリティ機能はディセーブルです。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**port-security enable** 例： `switch(config)# port-security enable`	スイッチ上でポート セキュリティをイネーブルにします。
ステップ 3	**no port-security enable** 例： `switch(config)# no port-security enable`	スイッチ上でポートセキュリティをディセーブル（デフォルト）にします。

ポート セキュリティのアクティブ化

ポート セキュリティのアクティブ化

ポート セキュリティをアクティブにできます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**port-security activate vsan** *vsan-id* 例： `switch(config)# port-security activate vsan 20`	指定された VSAN のポート セキュリティデータベースをアクティブにし、自動的に自動学習をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**port-security activate vsan** *vsan-id* **no-auto-learn** 例： `switch(config)# port-security activate vsan 20 no-auto-learn`	指定された VSAN のポート セキュリティ データベースをアクティブにし、自動学習をディセーブルにします。
ステップ 4	**no port-security activate vsan** *vsan-id* 例： `switch(config)# no port-security activate vsan 20`	指定された VSAN のポート セキュリティ データベースを無効にし、自動的に自動学習をディセーブルにします。

データベースのアクティブ化の拒否

次の場合は、データベースをアクティブ化しようとしても、拒否されます。

- 存在しないエントリや矛盾するエントリがコンフィギュレーションデータベースにあるが、アクティブ データベースにはない場合。
- アクティベーションの前に、自動学習機能がイネーブルに設定されていた場合。 この状態のデータベースを再アクティブ化するには、自動学習をディセーブルにします。
- 各ポート チャネル メンバに正確なセキュリティが設定されていない場合。
- 設定済みデータベースが空であり、アクティブ データベースが空でない場合。

上記のような矛盾が 1 つ以上発生したためにデータベース アクティベーションが拒否された場合は、ポート セキュリティ アクティベーションを強制して継続することができます。

ポート セキュリティの強制的なアクティブ化

ポート セキュリティ データベースを強制的にアクティブにできます。

手順

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

	コマンドまたはアクション	目的
ステップ 2	**port-security activate vsan** *vsan-id* **force** 例： `switch(config)# port-security activate vsan 210 force`	矛盾がある場合でも、指定された VSAN のポート セキュリティ データベースを強制的にアクティブにします。

データベースの再アクティブ化

ポート セキュリティのデータベースを再アクティブ化できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal switch(config)#`	グローバル コ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 no port-security auto-learn vsan** *vsan-id* 例： `switch(config)# no no port-security auto-learn vsan 35`	自動学習をディセーブルにし、スイッチにアクセスする新規デバイスをスイッチが学習しないように設定します。 また、このコマンドは、この時点までに学習されたデバイスに基づいてデータベースの内容を処理します。
ステップ 3	**exit** 例： `switch(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 4	**port-security database copy vsan** *vsan-id* 例： `switch# port-security database copy vsan 35`	アクティブ データベースから設定済みデータベースにコピーします。
ステップ 5	**configure terminal** 例： `switch# configure terminal switch(config)#`	コンフィギュレーション モードを再び開始します。

	コマンドまたはアクション	目的
ステップ 6	**port-security activate vsan** *vsan-id* 例： `switch(config)# port-security activate vsan 35`	指定された VSAN のポート セキュリティ データベースをアクティブにし、自動的に自動学習をイネーブルにします。

自動学習

自動学習のイネーブル化について

自動学習設定の状態は、ポート セキュリティ機能の状態によって異なります。

- ポートセキュリティ機能がアクティブでない場合、自動学習はデフォルトでディセーブルです。
- ポートセキュリティ機能がアクティブである場合、自動学習はデフォルトでイネーブルです（このオプションを明示的にディセーブルにしていない場合）。

ヒント　VSAN 上で自動学習がイネーブルの場合、force オプションを使用して、この VSAN のデータベースだけをアクティブにできます。

自動学習のイネーブル化

自動学習をイネーブルに設定できます。

自動学習設定の状態は、ポート セキュリティ機能の状態によって異なります。

- ポートセキュリティ機能がアクティブでない場合、自動学習はデフォルトでディセーブルです。
- ポートセキュリティ機能がアクティブである場合、自動学習はデフォルトでイネーブルです（このオプションを明示的にディセーブルにしていない場合）。

ヒント　VSAN 上で自動学習がイネーブルの場合、force オプションを使用して、この VSAN のデータベースだけをアクティブにできます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**port-security auto-learn vsan** *vsan-id* 例： `switch(config)# port-security auto-learn vsan 1`	自動学習をイネーブルにして、VSAN 1 へのアクセスが許可されたすべてのデバイスについて、スイッチが学習できるようにします。 これらのデバイスは、ポート セキュリティ アクティブ データベースに記録されます。

自動学習のディセーブル化

自動学習をディセーブルに設定できます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**no port-security auto-learn vsan** *vsan-id* 例： `switch(config)# no port-security auto-learn vsan 23`	自動学習をディセーブルにし、スイッチにアクセスする新規デバイスをスイッチが学習しないように設定します。 このコマンドは、この時点までに学習されたデバイスに基づいて、データベースの内容を処理します。

自動学習デバイスの許可

次の表に、デバイス要求に対して接続が許可される条件をまとめます。

表 *20*：許可される自動学習デバイス要求

条件	デバイス（pWWN、nWWN、sWWN）	接続先	認証
1	1 つまたは複数のスイッチ ポートに設定されている場合	設定済みスイッチ ポート	許可
2		他のすべてのスイッチ ポート	拒否
3	未設定	設定されていないスイッチ ポート	自動学習がイネーブルの場合は許可
4			自動学習がディセーブルの場合は拒否
5	設定されている場合、または設定されていない場合	任意のデバイスを接続許可するスイッチ ポート	許可
6	任意のスイッチ ポートにログインするように設定されている場合	スイッチ上の任意のポート	許可
7	未設定	その他のデバイスが設定されたポート	拒否

許可される場合

ポートセキュリティ機能がアクティブで、アクティブデータベースに次の条件が指定されていることが前提です。

- pWWN（P1）には、インターフェイス vfc 21（F1）からアクセスできます。
- pWWN（P2）には、インターフェイス vfc 22（F1）からアクセスできます。
- nWWN（N1）には、インターフェイス vfc 22（F2）からアクセスできます。
- インターフェイス vfc 31（F3）からは、任意の WWN にアクセスできます。
- nWWN（N3）には、任意のインターフェイスからアクセスできる。
- pWWN（P3）には、インターフェイス vfc 24（F4）からアクセスできます。
- sWWN（S1）には、インターフェイス vfc 31 ～ 33（F10 ～ F13）からアクセスできます。
- pWWN（P10）には、インターフェイス vfc 41（F11）からアクセスできます。

次の表に、このアクティブデータベースに対するポートセキュリティ許可の結果を要約します。

表 *21*：各シナリオの許可結果

デバイス接続要求	認証	条件	理由
P1、N2、F1	許可	1	競合しません。
P2、N2、F1	許可	1	競合しません。
P3、N2、F1	拒否	2	F1 が P1/P2 にバインドされています。
P1、N3、F1	許可	6	N3 に関するワイルドカード一致です。
P1、N1、F3	許可	5	F3 に関するワイルドカード一致です。
P1、N4、F5	拒否	2	P1 が F1 にバインドされています。
P5、N1、F5	拒否	2	N1 は F2 でだけ許可されます。
P3、N3、F4	許可	1	競合しません。
S1、F10	許可	1	競合しません。
S2、F11	拒否	7	P10 が F11 にバインドされています。
P4、N4、F5（自動学習が有効）	許可	3	競合しません。
P4、N4、F5（自動学習が無効）	拒否	4	一致しません。
S3、F5（自動学習が有効）	許可	3	競合しません。
S3、F5（自動学習が無効）	拒否	4	一致しません。
P1、N1、F6（自動学習が有効）	拒否	2	P1 が F1 にバインドされています。

デバイス接続要求	認証	条件	理由
P5、N5、F1（自動学習が有効）	拒否	7	P1 と P2 だけが F1 にバインドされています。
S3、F4（自動学習が有効）	拒否	7	P3 と F4 がペアになります。
S1、F3（自動学習が有効）	許可	5	競合しません。
P5、N3、F3	許可	6	F3 および N3 に関するワイルドカード（*）一致です。
P7、N3、F9	許可	6	N3 に関するワイルドカード（*）が一致しています。

関連トピック

自動学習デバイスの許可，（166 ページ）

ポート セキュリティの手動設定

ポート セキュリティを手動で設定できます。

手順

ステップ 1 保護する必要があるポートの WWN を識別します。

ステップ 2 許可された nWWN または pWWN に対して fWWN を保護します。

ステップ 3 ポート セキュリティ データベースをアクティブにします。

ステップ 4 設定を確認します。

WWN の識別に関する注意事項

WWN の識別に関する注意事項および制約事項は、次のとおりです。

- インターフェイスまたは fWWN でスイッチ ポートを識別します。
- pWWN または nWWN でデバイスを識別します。

- N ポートが SAN スイッチ ポート F にログインできる場合、その N ポートは指定された F ポートを介してだけログインできます。
- N ポートの nWWN が F ポート WWN にバインドされている場合、N ポートのすべての pWWN は暗黙的に F ポートとペアになります。
- TE ポート チェックは、VSAN トランク ポートの許可 VSAN リスト内の VSAN ごとに実行されます。
- 同じ SAN ポートチャネル内のすべてのポートチャネル xE ポートに、同じ WWN セットを設定する必要があります。
- E ポートのセキュリティは、E ポートのポート VSAN に実装されます。 この場合、sWWN を使用して許可チェックを保護します。
- アクティブ化されたコンフィギュレーション データベースは、アクティブ データベースに影響を与えることなく変更できます。
- 実行コンフィギュレーションを保存することにより、コンフィギュレーションデータベースおよびアクティブ データベース内のアクティブ化されたエントリを保存します。 アクティブ データベース内の学習済みエントリは保存されません。

許可済みのポート ペアの追加

バインドする必要がある WWN ペアを識別したら、これらのペアをポート セキュリティ データベースに追加します。

ヒント リモート スイッチのバインドは、ローカル スイッチで指定できます。 リモート インターフェイスを指定する場合、fWWN または sWWN インターフェイスの組み合わせを使用できます。

ポート セキュリティに関して許可済みのポート ペアを追加する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コ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)# **fc-port-security database vsan** *vsan-id*	指定された VSAN に対してポート セキュリティ データベース モードを開始します。
ステップ 3	switch(config)# **no fc-port-security database vsan** *vsan-id*	指定された VSAN からポート セキュリティ コンフィギュレーション データベースを削除します。

	コマンドまたはアクション	目的
ステップ 4	switch(fc-config-port-security)# **swwn** *swwn-id* **interface san-port-channel 5**	SAN ポート チャネル 5 を介した場合だけログインするように、指定された sWWN を設定します。
ステップ 5	switch(fc-config-port-security)# **any-wwn interface vfc** *if-number* - **vfc** *if-number*	指定されたインターフェイスを介してログインするようにすべての WWN を設定します。

次に、VSAN 2 に対してポート セキュリティ データベース モードを開始する例を示します。

```
switch(config)# fc-port-security database vsan 2
```

次に、SAN ポート チャネル 5 を介した場合だけログインするように、指定された sWWN を設定する例を示します。

```
switch(fc-config-port-security)#
swwn 20:01:33:11:00:2a:4a:66 interface san-port-channel 5
```

次に、指定されたスイッチの指定されたインターフェイスを介してログインするように、指定された pWWN を設定する例を示します。

```
switch(fc-config-port-security)#
pwwn 20:11:33:11:00:2a:4a:66 swwn 20:00:00:0c:85:90:3e:80
 interface vfc 2
```

次に、任意のスイッチの指定されたインターフェイスを介してログインするようにすべての WWN を設定する例を示します。

```
switch(fc-config-port-security)# any-wwn interface vfc 2
```

ポート セキュリティ設定の配信

ポート セキュリティ機能は 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管理を実現し、VSAN 内のファブリック全体に 1 つの設定を提供します。また、ファブリック全体でポート セキュリティ ポリシーを実行します。

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。

ポート セキュリティの配信のイネーブル化

ポート セキュリティの配信をイネーブルに設定できます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**port-security distribute** 例： `switch(config)# port-security distribute`	配信をイネーブルにします。
ステップ 3	**no port-security distribute** 例： `switch(config)# no port-security distribute`	配信をディセーブルにします。

関連トピック

アクティベーション設定と自動学習設定の配信，（173 ページ）

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が実行されると、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保留中のデータベースになります。

変更のコミット

指定された VSAN のポート セキュリティ設定の変更をコミットできます。

設定に加えられた変更をコミットする場合、保留中のデータベースの設定が他のスイッチに配信されます。 コミットが正常に行われると、設定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。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**port-security commit vsan** *vsan-id* 例： `switch(config)# port-security commit vsan 100`	指定された VSAN のポート セキュリティの変更をコミットします。

変更の廃棄

指定された VSAN のポート セキュリティ設定の変更を廃棄できます。

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、設定は影響されないまま、ロックが解除されます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**port-security abort vsan** *vsan-id* 例： `switch(config)# port-security abort vsan 35`	指定されたVSANのポートセキュリティの変更を廃棄し、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。

アクティベーション設定と自動学習設定の配信

配信モードのアクティベーション設定および自動学習設定は、保留中のデータベースの変更をコミットするときに実行する処理として記憶されます。

学習済みエントリは一時的なもので、ログインを許可するか否かを決定するロールを持ちません。そのため、学習済みエントリは配信に参加しません。 学習をディセーブルにし、保留中のデータベースの変更をコミットする場合、学習済みエントリはアクティブ データベース内のスタティッ

クエントリになり、ファブリック内のすべてのスイッチに配信されます。コミット後、すべてのスイッチのアクティブ データベースが同一になり、学習をディセーブルにできます。

保留中のデータベースに複数のアクティベーションおよび自動学習設定が含まれる場合、変更をコミットすると、アクティベーションおよび自動学習の変更が統合され、動作が変化する場合があります（次の表を参照）。

表 *22*：配信モードのアクティベーション設定および自動学習設定のシナリオ

シナリオ	アクション	配信がオフの場合	配信がオンの場合
コンフィギュレーション データベースにAおよびBが存在し、アクティベーションが行われておらず、デバイスCおよびDがログインされています。	1. ポートセキュリティデータベースをアクティブにし、自動学習をイネーブルにします。	コンフィギュレーション データベース = {A、B} アクティブ データベース = {A、B、C[1]、D*}	コンフィギュレーション データベース = {A、B} アクティブ データベース = {ヌル} 保留中のデータベース = {A、B + アクティベーション（イネーブル）}
	2. 新規のエントリ E がコンフィギュレーション データベースに追加されました。	コンフィギュレーション データベース = {A、B、E} アクティブ データベース = {A、B、C*、D*}	コンフィギュレーション データベース = {A、B} アクティブ データベース = {ヌル} 保留中のデータベース = {A、B、E + アクティベーション（イネーブル）}
	3. コミットを行います。	N/A	コンフィギュレーション データベース = {A、B、E} アクティブ データベース = {A、B、E、C*、D*} 保留中のデータベース = 空の状態

シナリオ	アクション	配信がオフの場合	配信がオンの場合
コンフィギュレーションデータベースにAおよびBが存在し、アクティベーションが行われておらず、デバイスCおよびDがログインされています。	1. ポートセキュリティデータベースをアクティブにし、自動学習をイネーブルにします。	コンフィギュレーションデータベース = {A、B} アクティブデータベース = {A、B、C*、D*}	コンフィギュレーションデータベース = {A、B} アクティブデータベース = {ヌル} 保留中のデータベース = {A、B + アクティベーション（イネーブル）}
	2. 学習をディセーブルにします。	コンフィギュレーションデータベース = {A、B} アクティブデータベース = {A、B、C、D}	コンフィギュレーションデータベース = {A、B} アクティブデータベース = {ヌル} 保留中のデータベース = {A、B + アクティベーション（イネーブル）+ 学習（ディセーブル）}
	3. コミットを行います。	N/A	コンフィギュレーションデータベース = {A、B} アクティブデータベース = {A、B}、デバイスCおよびDがログアウトされます。これは、自動学習をディセーブルにした場合のアクティベーションと同じです。 保留中のデータベース = 空の状態

[1] *（アスタリスク）は学習されたエントリを意味します。

ポート セキュリティ データベースの結合

データベースのマージとは、コンフィギュレーションデータベースとアクティブデータベース内のスタティック（学習されていない）エントリの統合を指します。

2 つのファブリック間のデータベースをマージする場合は、次のことに気をつけて行ってください。

- アクティベーションステータスと自動学習ステータスが両方のファブリックで同じであることを確認します。
- 両方のデータベースの各 VSAN の設定を合わせた数が 2000 を超えていないことを確認します。

注意 この 2 つの条件に従わない場合は、マージに失敗します。 次の配信がデータベースとファブリック内のアクティベーション ステートを強制的に同期化します。

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。

データベースの相互作用

次の表に、アクティブデータベースとコンフィギュレーションデータベースの差異および相互作用を示します。

表 *23*：アクティブおよびコンフィギュレーション ポート セキュリティ データベース

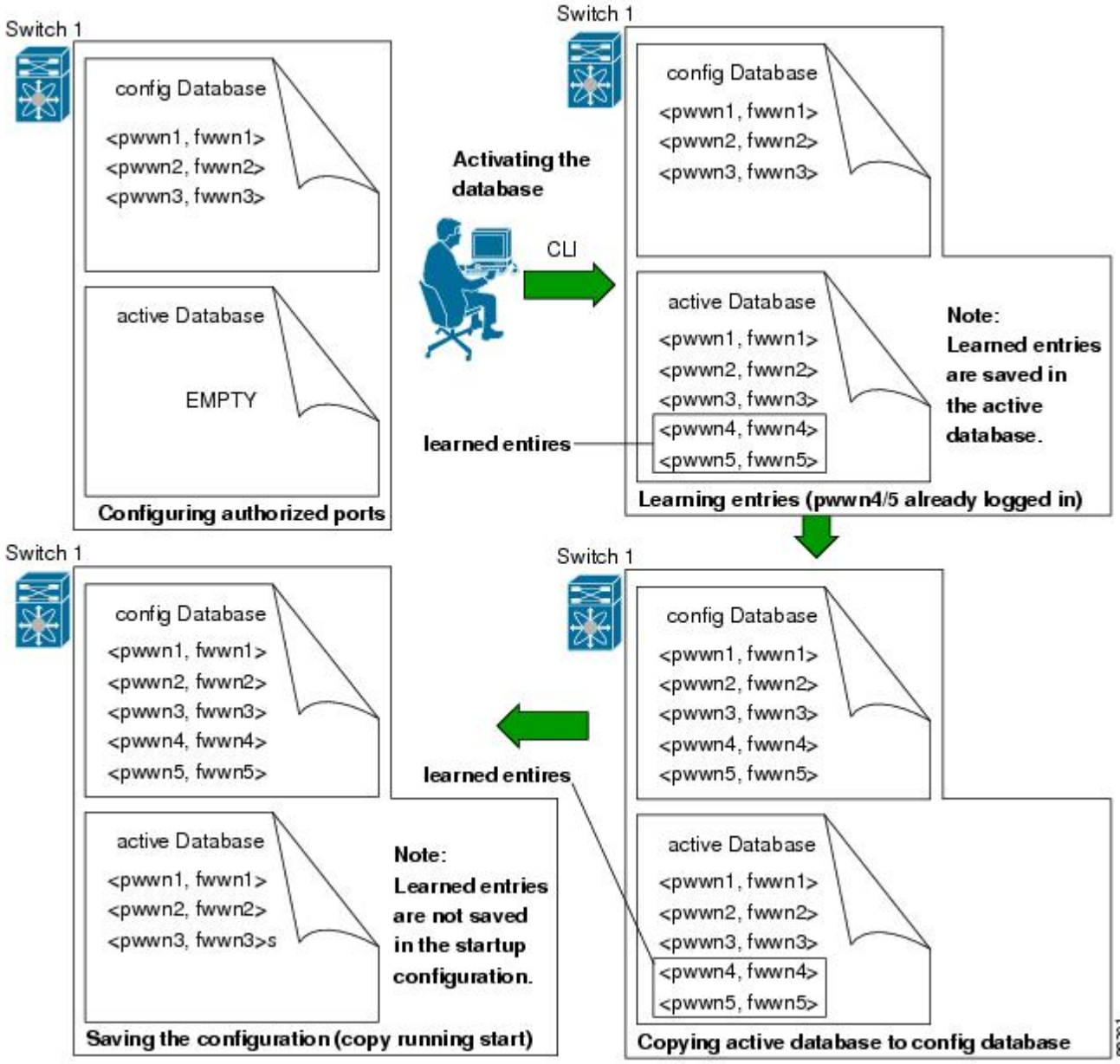
アクティブ データベース	コンフィギュレーション データベース
読み取り専用。	読み取りと書き込み。
設定を保存すると、アクティブなエントリだけが保存されます。 学習済みエントリは保存されません。	設定を保存すると、コンフィギュレーションデータベース内のすべてのエントリが保存されます。
アクティブ化すると、VSAN にログイン済みのすべてのデバイスも学習され、アクティブデータベースに追加されます。	アクティブ化されたコンフィギュレーションデータベースは、アクティブデータベースに影響を与えることなく変更できます。

アクティブ データベース	コンフィギュレーション データベース
アクティブデータベースを設定済みデータベースで上書きするには、ポートセキュリティデータベースをアクティブ化します。 強制的にアクティブにすると、アクティブデータベースの設定済みエントリに違反が生じることがあります。	コンフィギュレーション データベースをアクティブ データベースで上書きできます。

（注） **port-security database copy vsan** コマンドを使用すると、コンフィギュレーション データベースをアクティブ データベースで上書きできます。 **port-security database diff active vsan** コマンドは、アクティブ データベースとコンフィギュレーション データベースの差異を示します。

次の図は、ポートセキュリティ設定に基づくアクティブデータベースとコンフィギュレーションデータベースのステータスを示すさまざまなシナリオを示します。

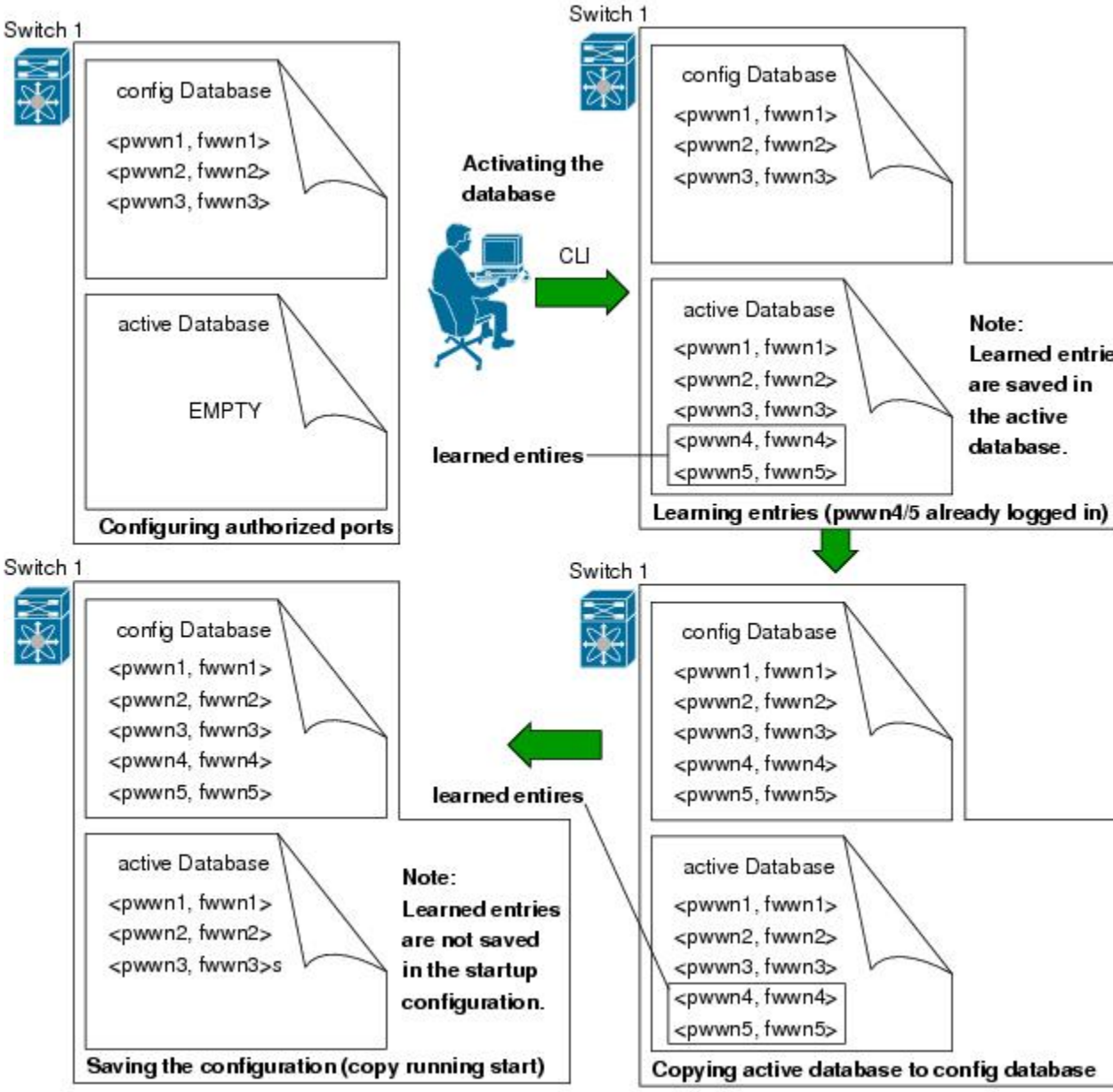
図 *28*： ポート セキュリティ データベースのシナリオ



データベースのシナリオ

次の図は、ポートセキュリティ設定に基づくアクティブデータベースとコンフィギュレーションデータベースのステータスを示すさまざまなシナリオを示します。

図 *29*： ポート セキュリティ データベースのシナリオ



ポート セキュリティ データベースのコピー

ヒント 自動学習をディセーブルにしてから、アクティブ データベースをコンフィギュレーション データベースにコピーすることを推奨します。 これにより、コンフィギュレーション データベースとアクティブ データベースを確実に同期化できます。 配信がイネーブルの場合、このコマンドによってコンフィギュレーション データベースの一時的なコピーが作成され、結果としてファブリックがロックされます。 ファブリックがロックされた場合、すべてのスイッチのコンフィギュレーション データベースに変更をコミットする必要があります。

アクティブ データベースから設定済みデータベースにコピーするには、 **port-security database copy vsan** コマンドを使用します。 アクティブ データベースが空の場合、このコマンドは受け付けられません。

```
switch# port-security database copy vsan 1
```

アクティブ データベースとコンフィギュレーション データベースとの相違を表示するには、**port-security database diff active vsan** コマンドを使用します。 このコマンドは、矛盾を解決する場合に使用できます。

```
switch# port-security database diff active vsan 1
```

コンフィギュレーションデータベースとアクティブデータベースとの違いに関する情報を取得するには、**port-security database diff config vsan** コマンドを使用します。

```
switch# port-security database diff config vsan 1
```

ポート セキュリティ データベースの削除

ヒント 配信がイネーブルの場合、削除によってデータベースのコピーが作成されます。 実際にデータベースを削除するには、明示的に **port-security commit** コマンドを入力する必要があります。

指定された VSAN の設定済みデータベースを削除するには、コンフィギュレーション モードで **no port-security database vsan** コマンドを使用します。

```
switch(config)# no port-security database vsan 1
```

ポート セキュリティ データベースのクリア

指定された VSAN のポート セキュリティ データベースから既存の統計情報をすべてクリアするには、**clear port-security statistics vsan** コマンドを使用します。

```
switch# clear port-security statistics vsan 1
```

VSAN 内の指定されたインターフェイスに関するアクティブ データベース内の学習済みエントリをすべてクリアするには、**clear port-security database auto-learn interface** コマンドを使用します。

```
switch# clear port-security database auto-learn interface vfc21 vsan 1
```

VSAN 全体に関するアクティブ データベース内の学習済みエントリをすべてクリアするには、**clear port-security database auto-learn vsan** コマンドを使用します。

```
switch# clear port-security database auto-learn vsan 1
```

（注） **clear port-security database auto-learn** および **clear port-security statistics** コマンドはローカルスイッチのみに関連するため、ロックを取得しません。 また、学習済みエントリはスイッチにだけローカルで、配信に参加しません。

VSAN 内で、任意のスイッチから VSAN の保留中のセッションをクリアするには、**port-security clear vsan** コマンドを使用します。

```
switch# clear port-security session vsan 5
```

ポート セキュリティ設定の表示

show port-security database コマンドを実行すると、設定されたポート セキュリティ情報が表示されます。 **show port-security** コマンドで fWWN や VSAN、またはインターフェイスや VSAN を指定すると、アクティブなポート セキュリティの出力を表示することもできます。

各ポートのアクセス情報は個別に表示されます。 fWWN または interface オプションを指定すると、（その時点で）アクティブ データベース内で指定された fWWN またはインターフェイスとペアになっているすべてのデバイスが表示されます。

次に、ポート セキュリティ コンフィギュレーション データベースを表示する例を示します。

```
switch# show port-security database
```

次に、VSAN 1 のポート セキュリティ コンフィギュレーション データベースを表示する例を示します。

```
switch# show port-security database vsan 1
```

次に、アクティブなデータベースを表示する例を示します。

```
switch# show port-security database active
```

次に、一時的なコンフィギュレーションデータベースとコンフィギュレーションデータベースの相違を表示する例を示します。

```
switch# show port-security pending-diff vsan 1
```

次に、VSAN 1 内の設定済み fWWN ポート セキュリティを表示する例を示します。

```
switch# show port-security database fwwn 20:01:00:05:30:00:95:de vsan 1
20:00:00:0c:88:00:4a:e2(swwn)
```

次に、ポート セキュリティ統計情報を表示する例を示します。

```
switch# show port-security statistics
```

次に、アクティブ データベースのステータスおよび自動学習設定を確認する例を示します。

```
switch# show port-security status
```

ポート セキュリティのデフォルト設定

次の表に、任意のスイッチにおけるすべてのポート セキュリティ機能のデフォルト設定を示します。

表 *24*： セキュリティのデフォルト設定値

パラメータ	デフォルト
自動学習	ポートセキュリティがイネーブルの場合は、イネーブル。
ポート セキュリティ	ディセーブル。
配信	ディセーブル。 （注） 配信をイネーブルにすると、スイッチ上のすべてのVSANの配信がイネーブルになります。

第 13 章

ファブリック バインディングの設定

この章では、ファブリック バインディング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。

ファブリック バインディングの設定

ファブリック バインディングについて

ファブリック バインディング機能を使用すると、ファブリック内で指定されたスイッチ間でだけ、ISL（スイッチ間リンク）をイネーブルにできます。 ファブリック バインディングは、VSAN 単位で設定します。

この機能を使用すると、不正な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されることがなくなります。 この機能では、Exchange Fabric Membership Data（EFMD）プロトコルを使用することによって、ファブリック内の全スイッチで、許可されたスイッチのリストが同一になるようにします。

ファブリック バインディングのライセンス要件

ファブリック バインディングを使用するには、ストレージ プロトコル サービス ライセンスが必要です。

ポート セキュリティとファブリック バインディングの比較

ポート セキュリティとファブリック バインディングは、相互補完するように設定可能な、2 つの独立した機能です。 次の表で、2 つの機能を比較します。

表 *25*：ファブリック バインディングとポート セキュリティの比較

ファブリック バインディング	ポート セキュリティ
一連の sWWN および永続的ドメイン ID を使用します。	pWWN/nWWN または fWWN/sWWN を使用します。
スイッチ レベルでファブリックをバインドします。	インターフェイス レベルでデバイスをバインドします。
ファブリック バインディング データベースに格納された設定済み sWWN にだけ、ファブリックへの参加を許可します。	設定済みの一連のファイバ チャネル デバイスを SAN ポートに論理的に接続できます。 WWN またはインターフェイス番号で識別されるスイッチ ポートは、同様に WWN で識別されるファイバ チャネル デバイス（ホストまたは別のスイッチ）に接続されます。 これらの 2 つのデバイスをバインドすると、これらの 2 つのポートがグループ（リスト）にロックされます。
VSAN 単位のアクティベーションが必要です。	VSAN 単位のアクティベーションが必要です。
ピア スイッチが接続されている物理ポートに関係なく、ファブリックに接続可能な特定のユーザ定義のスイッチを許可します。	別のデバイスを接続できる特定のユーザ定義の物理ポートを許可します。
ログインしているスイッチについて学習しません。	学習モードがイネーブルの場合、ログインしているスイッチまたはデバイスについて学習します。
CFS によって配信できず、ファブリック内の各スイッチで手動で設定する必要があります。	CFS によって配信できます。

xE ポートのポート レベル チェックは、次のように実行されます。

- スイッチ ログインは、指定された VSAN にポート セキュリティ バインディングとファブリック バインディングの両方を使用します。
- バインディング検査は、ポート VSAN で次のように実行されます。
  - ポート VSAN での E ポート セキュリティ バインディング検査
  - 許可された各 VSAN での TE ポート セキュリティ バインディング検査

ポート セキュリティはファブリック バインディングを補完する関係にありますが、これらの機能は互いに独立していて、個別にイネーブルまたはディセーブルにできます。

ファブリック バインディングの実行

ファブリックバインディングに参加するファブリック内のスイッチごとに、ファブリックバインディング機能をイネーブルにする必要があります。 デフォルトでは、この機能はディセーブルになっています。ファブリックバインディング機能に関する設定および確認コマンドを使用できるのは、スイッチ上でファブリックバインディングがイネーブルな場合だけです。 この設定をディセーブルにした場合、関連するすべての設定は自動的に廃棄されます。

ファブリック バインディングを実行するには、Switch World Wide Name（sWWN）を設定して、スイッチごとに xE ポート接続を指定します。 ファブリック バインディング ポリシーは、ポートがアクティブになるたび、およびポートを起動しようとした場合に実行されます。 ファイバチャネル VSAN では、ファブリック バインディング機能を実行するには、すべての sWWN をスイッチに接続し、ファブリックバインディングアクティブデータベースに格納する必要があります。

ファブリック バインディングの設定

ファブリックバインディング機能を使用すると、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でだけ、ISL をイネーブルにできます。 ファブリック バインディングは VSAN 単位で設定されます。

ファブリック バインディングの設定

ファブリック内の各スイッチにファブリック バインディングを設定できます。

手順

ステップ 1 ファブリック設定機能をイネーブルにします。

ステップ 2 ファブリックにアクセス可能なデバイスに sWWN のリスト、および対応するドメイン ID を設定します。

ステップ 3 ファブリック バインディング データベースをアクティブにします。

ステップ 4 ファブリック バインディング アクティブ データベースをファブリック バインディング設定データベースにコピーします。

ステップ 5 ファブリック バインディング設定を保存します。

ステップ 6 ファブリック バインディング設定を確認します。

ファブリック バインディングのイネーブル化

参加しているスイッチ上でファブリック バインディングをイネーブルに設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**fabric-binding enable** 例： `switch(config)# fabric-binding enable`	現在のスイッチ上でファブリック バインディングをイネーブルにします。
ステップ 3	**no fabric-binding enable** 例： `switch(config)# no fabric-binding enable`	現在のスイッチ上でファブリック バインディングをディセーブル（デフォルト）にします。

スイッチの WWN リスト

ユーザ指定のファブリック バインディング リストには、ファブリック内の sWWN のリストが含まれています。 リストにない sWWN、または許可リストで指定されているドメイン ID と異なるドメイン ID を使用する sWWN がファブリックへの参加を試みると、スイッチとファブリック間の ISL が VSAN 内で自動的に隔離され、スイッチはファブリックへの参加を拒否されます。

スイッチ WWN リストの設定

ファイバ チャネル VSAN 用の sWWN とオプションのドメイン ID のリストを設定する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**fabric-binding database vsan** *vsan-id* 例： `switch(config)# fabric-binding database vsan 35`	指定された VSAN のファブリック バインディング サブモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**no fabric-binding database vsan** *vsan-id* 例： `switch(config)# no fabric-binding database vsan 35`	指定されたVSANのファブリック バインディング データベースを削除します。
ステップ 4	**swwn** *swwn-id* **domain** *domain-id* 例： `switch(config-fabric-binding)# swwn 21:00:05:30:23:1a:11:03 domain 25`	設定されたデータベース リストに、特定のドメインID用の別のスイッチのsWWNを追加します。
ステップ 5	**no swwn** *swwn-id* **domain** *domain-id* 例： `switch(config-fabric-binding)# no swwn 21:00:05:30:23:1a:11:03 domain 25`	設定されたデータベース リストから、スイッチの sWWN およびドメイン ID を削除します。

ファブリック バインディングのアクティベーションおよび非アクティベーション

ファブリック バインディング機能では、コンフィギュレーションデータベース（config database）およびアクティブ データベースが維持されます。 config database は、実行された設定を収集する読み取りと書き込みのデータベースです。 これらの設定を実行するには、データベースをアクティブにする必要があります。データベースがアクティブになると、アクティブデータベースがconfig databaseの内容で上書きされます。アクティブ データベースは、ログインを試みる各スイッチをチェックする読み取り専用データベースです。

デフォルトでは、ファブリックバインディング機能は非アクティブです。コンフィギュレーション データベース内の既存のエントリがファブリックの現在の状態と矛盾する場合は、スイッチでファブリック バインディング データベースをアクティブにできません。 たとえば、ログイン済みのスイッチの 1 つが config database によってログインを拒否される場合があります。 これらの状態を強制的に上書きできます。

（注） アクティベーションのあと、現在アクティブなデータベースに違反するログイン済みのスイッチは、ログアウトされ、ファブリック バインディング制限によってログインが拒否されたすべてのスイッチは再初期化されます。

ファブリック バインディングのアクティベーション

ファブリック バインディング機能をアクティブにできます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**fabric-binding activate vsan** *vsan-id* 例： `switch(config)# fabric-binding activate vsan 25`	指定された VSAN のファブリック バインディング データベースをアクティブにします。
ステップ 3	**no fabric-binding activate vsan** *vsan-id* 例： `switch(config)# no fabric-binding activate vsan 25`	指定された VSAN のファブリック バインディング データベースを非アクティブにします。

ファブリック バインディングの強制的なアクティベーション

ファブリック バインディング データベースを強制的にアクティブにできます。

上記のような矛盾が 1 つまたは複数発生したためにデータベースのアクティブ化が拒否された場合は、force オプションを使用してアクティブ化を継続できます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**fabric-binding activate vsan** *vsan-id* **force** 例： `switch(config)# fabric-binding activate vsan 12 force`	指定された VSAN のファブリック バインディング データベースを、設定が許可されない場合でも、強制的にアクティブにします。
ステップ 3	**no fabric-binding activate vsan** *vsan-id* **force** 例： `switch(config)# no fabric-binding activate vsan 12 force`	元の設定状態、または（状態が設定されていない場合は）出荷時の設定に戻します。

ファブリック バインディング設定のコピー

ファブリック バインディング設定をコピーすると、コンフィギュレーションデータベースが実行コンフィギュレーションに保存されます。

次のコマンドを使用して、コンフィギュレーション データベースにコピーできます。

- アクティブ データベースからコンフィギュレーション データベースにコピーするには、**fabric-binding database copy vsan** コマンドを使用します。 設定されたデータベースが空の場合、このコマンドは受け付けられません。

  ```
  switch# fabric-binding database copy vsan 1
  ```

- アクティブデータベースとコンフィギュレーションデータベース間の違いを表示するには、**fabric-binding database diff active vsan** コマンドを使用します。 このコマンドは、矛盾を解決する場合に使用できます。

  ```
  switch# fabric-binding database diff active vsan 1
  ```

- コンフィギュレーション データベースとアクティブ データベース間の違いに関する情報を取得するには、**fabric-binding database diff config vsan** コマンドを使用します。

  ```
  switch# fabric-binding database diff config vsan 1
  ```

- 再起動後にファブリック バインディング設定データベースを使用できるよう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保存するには、**copy running-config startup-config** コマンドを使用します。

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

ファブリック バインディング統計情報のクリア

指定された VSAN のファブリック バインディング データベースから既存の統計情報をすべてクリアするには、**clear fabric-binding statistics** コマンドを使用します。

```
switch# clear fabric-binding statistics vsan 1
```

ファブリック バインディング データベースの削除

指定された VSAN の設定済みデータベースを削除するには、コンフィギュレーション モードで **no fabric-binding** コマンドを使用します。

```
switch(config)# no fabric-binding database vsan 10
```

ファブリック バインディング設定の確認

ファブリック バインディング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	
show fabric-binding database [**active**]	設定されたファブリック バインディング データベースを表示します。 キーワード active を追加し、アクティブなファブリック バインディング データベースだけを表示できます。
show fabric-binding database [**active**] [**vsan** *vsan-id*]	指定された VSAN の設定済みファブリック バインディング データベースを表示します。
show fabric-binding statistics	ファブリック バインディング データベースの統計情報を表示します。
show fabric-binding status	すべての VSAN のファブリック バインディング ステータスを表示します。
show fabric-binding violations	ファブリック バインディング違反を表示します。
show fabric-binding efmd [**vsan** *vsan-id*]	指定された VSAN の設定済みファブリック バインディング データベースを表示します。

次に、VSAN 4 のアクティブ ファブリック バインディングの情報を表示する例を示します。

```
switch# show fabric-binding database active vsan 4
```

次に、ファブリック バインディングの違反を表示する例を示します。

```
switch# show fabric-binding violations
--------------------------------------------------------------------------------
VSAN Switch WWN [domain]     Last-Time             [Repeat count] Reason
--------------------------------------------------------------------------------
2    20:00:00:05:30:00:4a:1e [0xeb] Nov 25 05:46:14 2003   [2]    Domain mismatch
3    20:00:00:05:30:00:4a:1e [*] Nov 25 05:44:58 2003      [2]    sWWN not found
4    20:00:00:05:30:00:4a:1e [*] Nov 25 05:46:25 2003      [1]    Database mismatch
```

（注） VSAN 3 では、sWWN がリストで見つかりませんでした。 VSAN 2 では、sWWN がリストで見つかりましたが、ドメイン ID が一致しませんでした。

次に、VSAN 4 の EFMD 統計情報を表示する例を示します。

```
switch# show fabric-binding efmd statistics vsan 4
```

ファブリック バインディングのデフォルト設定

次の表に、ファブリック バインディング機能のデフォルト設定を示します。

表 *26*： ファブリック バインディングのデフォルト設定

パラメータ	デフォルト
ファブリック バインディング	ディセーブル

第 14 章

FCS の設定

この章の内容は、次のとおりです。

FCS の設定

FCS の概要

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コンフィギュレーション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。 FCS は次のオブジェクトに基づいて、ファブリック全体を表示します。

- Interconnect Element（IE）オブジェクト：ファブリック内の各スイッチは IE オブジェクトに対応しています。 ファブリックは 1 つまたは複数の IE オブジェクトで構成されます。
- ポート オブジェクト：IE の各物理ポートはポート オブジェクトに対応しています。 ポート オブジェクトにはスイッチ ポート（xE および F ポート）および接続された N ポートが含まれます。
- プラットフォーム オブジェクト：一連のノードをプラットフォーム オブジェクトとして定義して、管理可能な単一のエンティティにできます。 これらのノードはファブリックに接続されたエンドデバイス（ホスト システム、ストレージ サブシステム）です。 プラットフォーム オブジェクトは、ファブリックのエッジ スイッチ上にあります。

各オブジェクトには、それぞれ独自の属性および値のセットがあります。 一部の属性にはヌル値も定義できます。

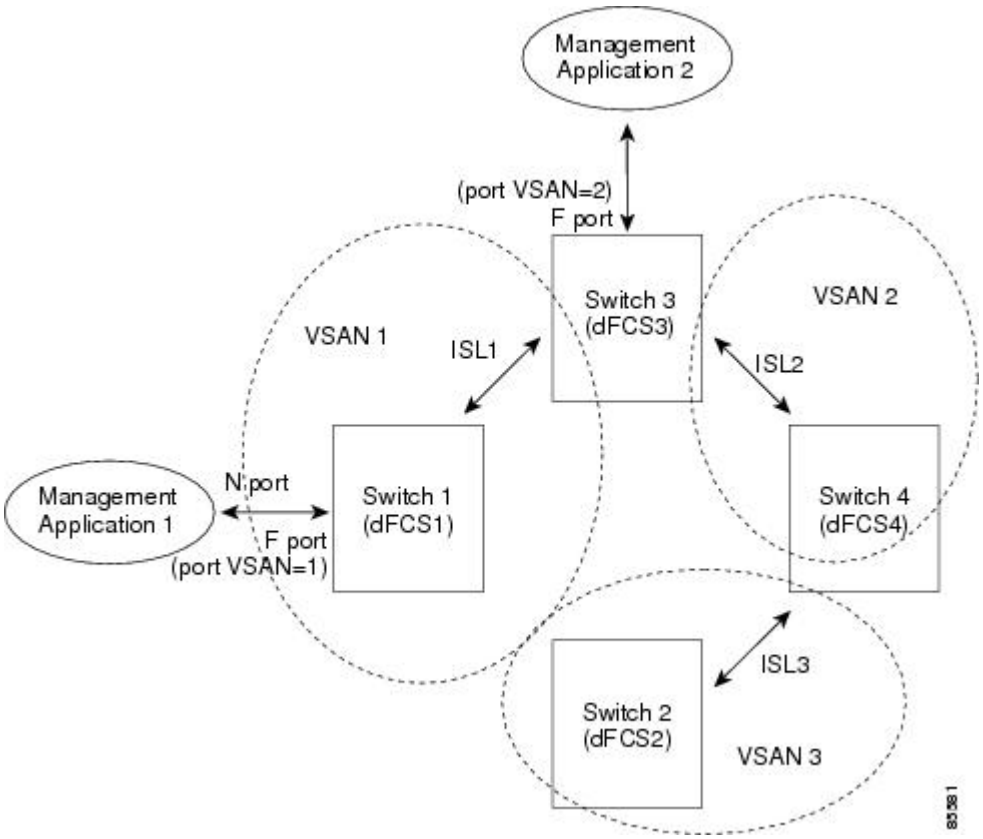
Cisco Nexus デバイス環境では、ファブリックは複数の VSAN（仮想 SAN）で構成される場合があります。 VSAN ごとに FCS インスタンスが 1 つ存在します。

FCS は仮想デバイスの検出をサポートします。 **fcs virtual-device-add** コマンドを FCS コンフィギュレーション サブモードで入力すると、特定の VSAN またはすべての VSAN の仮想デバイスを検出できます。

スイッチに管理アプリケーションが接続されている場合、スイッチの FCS に転送されるすべてのフレームは、スイッチ ポート（F ポート）のポート VSAN に属します。 管理アプリケーションの表示対象はこの VSAN に限定されます。 ただし、このスイッチが属する他の VSAN に関する情報は、SNMP または CLI を使用して取得できます。

次の図では、管理アプリケーション 1（M1）は、ポート VSAN ID が 1 の F ポートを介して接続され、管理アプリケーション 2（M2）はポート VSAN ID が 2 の F ポートを介して接続されています。 M1 はスイッチ S1 および S3 の FCS 情報を、M2 はスイッチ S3 および S4 の FCS 情報をそれぞれ問い合わせることができます。 スイッチ S2 情報はどちらにも提供されません。 FCS は、VSAN で表示可能なこれらのスイッチ上でだけ動作します。 S3 は VSAN 1 にも属していますが、M2 は VSAN 2 にだけ FCS 要求を送信できます。

図 *30*： ***VSAN*** 環境における ***FCS***



FCS の特性

FCS には次の特性があります。

- 次のようなネットワーク管理をサポートしています。

- Nポート管理アプリケーションはファブリック要素に関する情報を問い合わせて、取得できます。
- SNMP マネージャは FCS 管理情報ベース（MIB）を使用して、ファブリック トポロジ情報の検出を開始して、取得できます。

- 標準 F および E ポートだけでなく、TE ポートもサポートします。
- プラットフォームに登録された論理名および管理アドレスを持つ一連のノードを維持できます。 FCS はすべての登録情報のバックアップをセカンダリ ストレージに維持し、変更があるたびに更新します。 再起動またはスイッチオーバーが発生すると、FCS はセカンダリ ストレージ情報を取得し、データベースを再構築します。
- SNMP マネージャは FCS に、ファブリック内のすべての IE、ポート、およびプラットフォームについて問い合わせることができます。

FCS 名の指定

一意の名前の確認をファブリック全体（グローバル）に行うのか、または登録されたプラットフォームにローカル（デフォルト）に行うのかを指定できます。

（注） このコマンドのグローバル設定は、ファブリック内のすべてのスイッチが Cisco MDS 9000 ファミリまたは Cisco Nexus デバイスである場合にかぎり実行してください。

プラットフォーム名のグローバル チェックをイネーブルにする手順は、次のとおりです。

プラットフォーム属性を登録する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **fcs plat-check-global vsan** *vsan-id*	プラットフォーム名のグローバル チェックをイネーブルにします。
ステップ 3	switch(config)# **no fcs plat-check-global vsan** *vsan-id*	プラットフォーム名のグローバル チェックをディセーブル（デフォルト）にします。

FCS 情報の表示

WWN 設定のステータスを表示するには、**show fcs** コマンドを使用します。

次に、FCS ローカル データベースを表示する例を示します。

```
switch# show fcs database
```

次に、VSAN 1 のすべての IE のリストを表示する例を示します。

```
switch# show fcs ie vsan 1
```

次に、特定のプラットフォームに関する情報を表示する例を示します。

```
switch# show fcs platform name SamplePlatform vsan 1
```

次に、特定の pWWN のポート情報を表示する例を示します。

```
switch# show fcs port pwwn 20:51:00:05:30:00:16:de vsan 24
```

FCS のデフォルト設定

次の表に、FCS のデフォルト設定を示します。

表 *27*： *FCS* のデフォルト設定

パラメータ	デフォルト
プラットフォーム名のグローバル チェック	ディセーブル
プラットフォームのノード タイプ	不明

第 15 章

ポート トラッキングの設定

この章では、ポート トラッキング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。

ポート トラッキングの設定

Cisco SAN スイッチは、（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ポート トラッキング機能を提供します。 この機能はリンクの動作ステートに関する情報を利用して、エッジデバイスを接続するリンクの障害を引き起こします。 この処理では、間接障害が直接障害に変換されるため、冗長リンクへの復旧処理が迅速化されます。 ポート トラッキング機能がイネーブルになっている場合、この機能はリンク障害時に設定されたリンクをダウンにし、トラフィックを別の冗長リンクに強制的にリダイレクトします。

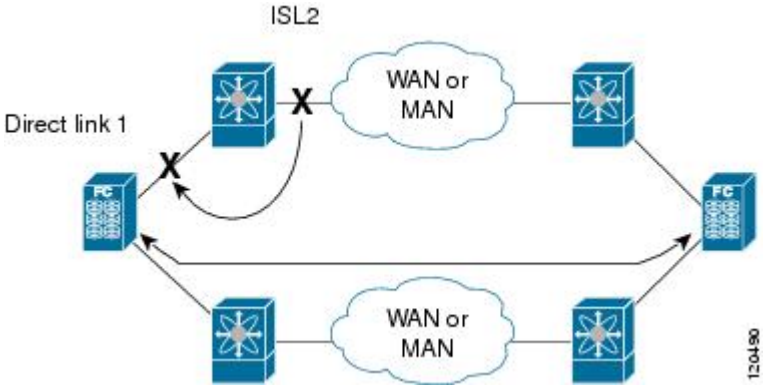
ポート トラッキングに関する情報

ポートトラッキング機能はリンクの動作ステートに関する情報を利用して、エッジデバイスを接続するリンクの障害を引き起こします。 この処理では、間接障害が直接障害に変換されるため、冗長リンクへの復旧処理が迅速化されます。 ポートトラッキング機能がイネーブルになっている場合、この機能はリンク障害時に設定されたリンクをダウンにし、トラフィックを別の冗長リンクに強制的にリダイレクトします。

一般的に、ホストはスイッチに直接接続されているリンク（直接リンク）上でのリンク障害からすぐに復旧できます。 しかし、キープアライブ メカニズムを備えた WAN や MAN ファブリック内のスイッチ間で発生する間接的なリンク障害からのリカバリは、タイムアウト値（TOV）や Registered State Change Notification（RSCN）情報などの複数の要因に左右されます。

次の図では、ホストへの直接リンク 1 に障害が発生した場合、即時にリカバリできます。 ただし、2 つのスイッチ間の ISL 2 に障害が発生した場合、復旧は TOV や RSCN などに左右されます。

図 *31*： ポート トラッキングによるトラフィックの復旧



ポート トラッキング機能は、トポロジの変化を引き起こし、接続デバイスを接続しているリンクをダウンさせる障害を監視し、検出します。 この機能をイネーブルにして、リンク対象ポートとトラッキング対象ポートを明示的に設定すると、スイッチ ソフトウェアはトラッキング対象ポートを監視します。リンク ステートの変化を検出した場合、スイッチ ソフトウェアはリンク対象ポートの動作ステートを変更します。

この章では次の用語を使用します。

- トラッキング対象ポート：動作ステートが継続的に監視されるポート。 トラッキング対象ポートの動作ステートを使用して、1 つまたは複数のポートの動作ステートを変更します。トラッキング対象ポートは、ファイバ チャネル、VSAN、SAN ポート チャネル、またはギガビット イーサネットのポートです。 一般的に、E および TE ポート モードのポートは F ポートにもなります。
- リンク対象ポート：トラッキング対象ポートの動作ステートに基づいて動作ステートが変更されるポート。 物理ファイバ チャネル ポートのみをリンク対象ポートにできます。

ポート トラッキングには、次の機能があります。

- トラッキング対象ポートがダウンすると、アプリケーションはリンク対象ポートをダウンさせます。 追跡されたポートが障害から復旧して再度アップになると、リンクされたポートも自動的にアップになります（特に別の設定がないかぎり）。
- トラッキング対象ポートがアップしても、リンク対象ポートを強制的にダウンしたままにできます。 この場合、必要に応じてリンク対象ポートを明示的にアップする必要があります。

関連トピック

RSCN 情報の概要, （132 ページ）

ファイバ チャネルのタイムアウト値

ポート トラッキングのデフォルト設定

次の表に、ポート トラッキング パラメータのデフォルト設定を示します。

表 *28*：ポート トラッキング パラメータのデフォルト設定値

パラメータ	デフォルト
ポート トラッキング	ディセーブル
動作バインディング	イネーブル（ポート トラッキングと同時）

ポート トラッキングの設定

ポート トラッキングを設定する際、次の点に注意してください。

- トラッキング対象ポートとリンク対象ポートが同じシスコ スイッチ上に存在することを確認します。
- トラッキング対象ポートがダウンしたときに、リンク対象ポートが自動的にダウンすることを確認します。
- 再帰依存を回避するためにリンク対象ポートに再度トラッキングしないでください（例：ポート vfc22 からポート vfc24 にトラッキングし、さらにポート vfc22 に戻す）。

ポート トラッキングのイネーブル化

ポートトラッキング機能は、デフォルトでディセーブルです。この機能をイネーブルにすると、ポート トラッキングはスイッチ全体でグローバルにイネーブルになります。

ポートトラッキングを設定するには、ポートトラッキング機能をイネーブルにして、トラッキング対象ポートに対応するリンク対象ポートを設定します。

ポート トラッキングをイネーブルに設定できます。

手順

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的
ステップ 2	**port-track enable** 例： `switch(config)# port-track enable`	ポート トラッキングをイネーブルにします。
ステップ 3	**no port-track enable** 例： `switch(config)# no port-track enable`	現在適用されているポート トラッキング設定を削除し、ポート トラッキングをディセーブルにします。

リンク対象ポートの設定

ポートをリンクするには、次の 2 通りの方法があります。

- リンク対象ポートからトラッキング対象ポートへの動作バインディングを設定します（デフォルト）。
- リンク対象ポートを強制的にダウンしたままにします（トラッキング対象ポートがリンク障害から回復した場合も同様）。

トラッキング対象ポートの動作バインディング

最初のトラッキング対象ポートを設定すると、動作バインディングは自動的に有効になります。この方法を使用すると、複数のポートを監視したり、1 つの VSAN 内のポートを監視したりできます。

トラッキング対象ポートの動作バインディングを設定するには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	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*	リンク対象ポートでインターフェイス コンフィギュレーションモードを開始します。 これで、トラッキング対象ポートを設定できるようになります。

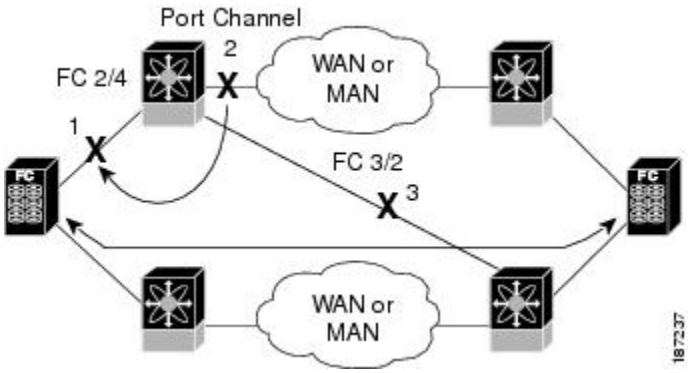
	コマンドまたはアクション	目的
ステップ 3	switch(config-if)# **port-track interface vfc** *vfc-id* | **san-port-channel** *port*	トラッキング対象ポートを指定します。 トラッキング対象ポートがダウンすると、リンク対象ポートもダウンします。
ステップ 4	switch(config-if)# **no port-track interface vfc** *vfc-id* | **san-port-channel** *port*	インターフェイスに現在適用されているポートトラッキング設定を削除します。

複数ポートのトラッキング

複数のトラッキング対象ポートの動作ステートに基づいて、リンク対象ポートの動作ステートを制御できます。 複数のトラッキング対象ポートが 1 つのリンク対象ポートに対応付けられている場合、対応付けられたトラッキング対象ポートがすべてダウンしたときにかぎり、リンク対象ポートの動作ステートはダウンに設定されます。 トラッキング対象ポートが 1 つでもアップしている場合、リンク対象ポートはアップしたままになります。

次の図では、ISL 2 および 3 の両方が失敗した場合のみ、直接リンク 1 がダウンします。 ISL 2 または 3 が動作しているかぎり、直接リンク 1 はダウンしません。

図 *32*： ポート トラッキングによるトラフィックの復旧



複数ポートのトラッキング

複数のポートをトラッキングするには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	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。 これで、トラッキング対象ポートを設定できるようになります。
ステップ 3	switch(config-if)# **port-track interface interface vfc** *vfc-id* | **san-port-channel** *port*	指定されたインターフェイスのあるリンク対象ポートをトラッキングします。 トラッキング対象ポートがダウンすると、リンク対象ポートもダウンします。

VSAN 内のポートのモニタリングの概要

トラッキング対象ポート上のすべての動作 VSAN から VSAN をリンク対象ポートに対応付けるには、必要な VSAN を指定します。 このため、トラッキング対象ポートの詳細な設定が可能になります。 トラッキング対象ポートが TE ポートの場合、ポートの動作ステートがダウンにならずに、ポート上の動作 VSAN がダイナミックに変わる場合があります。 この場合、リンク対象ポートのポート VSAN は、トラッキング対象ポート上の動作 VSAN 上で監視できます。

この機能を設定すると、トラッキング対象ポート上で VSAN がアップしている場合にだけリンク対象ポートがアップします。

指定する VSAN は、リンク対象ポートのポート VSAN と同じである必要はありません。

VSAN 内のポートのモニタリングの概要

特定の VSAN でトラッキング対象ポートをモニタできます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コ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

	コマンドまたはアクション	目的
		ドを開始します。 これで、トラッキング対象ポートを設定できるようになります。
ステップ 3	**port-track interface san-port-channel 1 vsan 2** 例： `switch(config-if)# port-track interface san-port-channel 1 vsan 2`	VSAN 2 で SAN ポート チャネルのトラッキングをイネーブルにします。
ステップ 4	**no port-track interface san-port-channel 1 vsan 2** 例： `switch(config-if)# port-track interface san-port-channel 1 vsan 2`	リンク対象ポートに対する VSAN の対応付けを削除します。 SAN ポート チャネル リンクは有効なままです。

強制シャットダウン

トラッキング対象ポートで頻繁にフラップが発生する場合、動作バインディング機能を使用するトラッキング ポートは頻繁にトポロジを変えることがあります。 この場合、頻繁なフラップの原因が解決されるまで、ポートをダウンしたままにできます。 フラップが発生するポートをダウン状態のままにしておくと、プライマリのトラッキング対象ポートの問題が解決されるまで、トラフィックは冗長パスを流れるよう強制されます。 問題が解決されて、トラッキング対象ポートが再びアップした場合には、インターフェイスを明示的にイネーブルにできます。

この機能を設定すると、トラッキング対象ポートが再びアップになっても、リンク対象ポートはシャットダウン状態のままになります。 トラッキング対象ポートがアップして安定したら、（このインターフェイスを管理上アップして）リンク対象ポートの強制シャットダウン状態を明示的に解除する必要があります。

トラッキング対象ポートの強制シャットダウン

トラッキング対象ポートを強制シャットダウンできます。

手順

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

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **interface vfc** *vfc-id*	指定され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。 これで、トラッキング対象ポートを設定できるようになります。
ステップ 3	**port-track force-shut** 例： `switch(config-if)# port-track force-shut`	トラッキング対象ポートを強制的にシャットダウンします。
ステップ 4	**no port-track force-shut** 例： `switch(config-if)# no port-track force-shut`	トラッキング対象ポートのポートシャットダウン設定を解除します。

ポート トラッキング情報の表示

スイッチの現在のポート トラッキング設定を表示するには、**show** コマンドを使用します。

次に、特定のインターフェイスのトラッキング対象ポートの設定を表示する例を示します。

```
switch# show interface vfc21
vfc21 is down (Administratively down)
    Hardware is Fibre Channel, FCOT is short wave laser w/o OFC (SN)
    Port WWN is 20:01:00:05:30:00:0d:de
    Admin port mode is FX
    Port vsan is 1
    Receive data field Size is 2112
    Beacon is turned off
    Port tracked with interface vc22 (down)
    Port tracked with interface san-port-channel 1 vsan 2 (down)
5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
...
```

次に、SAN ポート チャネルのトラッキング対象ポートの設定を表示する例を示します。

```
switch# show interface san-port-channel 1
port-channel 1 is down (No operational members)
    Hardware is Fibre Channel
    Port WWN is 24:01:00:05:30:00:0d:de
    Admin port mode is auto, trunk mode is on
    Port vsan is 2
    Linked to 1 port(s)
      Port linked to interface vfc21
...
```

次に、ポート トラッキング モードを表示する例を示します。

```
switch# show interface vfc 24
vfc24 is up
    Hardware is Fibre Channel, FCOT is short wave laser
...
    Transmit B2B Credit is 64
    Receive B2B Credit is 16
    Receive data field Size is 2112
    Beacon is turned off
    Port track mode is force_shut <-- this port remains shut even if the tracked port is
back up
```

索 引

H

L

N

P

R

S

T

V

あ

い

え

か

け

こ

し

す

せ

そ

て

と

に

ね

は

ふ

ほ

も

り

れ

ろ