Cisco Fabric Manager Fabric コンフィギュレーション ガイド

Cisco Fabric Manager Fabric Configuration Guide

Cisco Fabric Manager Release 4.2(1)
2009 年 8 月

Text Part Number: OL-19448-01-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、米国シスコシステムズ発行ドキュメントの参考和訳です。米国サイト掲載ドキュメントとの差異が生じる場合があるため、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。

Cisco Fabric Manager Fabric コンフィギュレーション ガイド

CONTENTS

新しい情報と変更された情報

Cisco MDS NX-OS Release 42（1）以降、ソフトウェアの設定に関する情報は、新機能ごとのコンフィギュレーション ガイドで参照できます。提供される情報は次のとおりです。

- システム管理
- インターフェイス
- ファブリック
- QoS（Quality Of Service）
- セキュリティ
- IP サービス
- ハイ アベイラビリティおよび冗長性

これらの新しいガイドの情報は、以前は『*Cisco MDS 9000 Family CLI Configuration Guide*』および『*Cisco MDS 9000 Family Fabric Manager Configuration Guide*』に記載されていました。これらのコンフィギュレーション ガイドは、Cisco.com に用意されており、MDS NX-OS Release 4.2（1）以前のすべてのソフトウェア リリース用に参照できます。各ガイドには、特定のリリースで導入された機能または使用可能な機能が記載されています。スイッチにインストールされているソフトウェアに関するコンフィギュレーション ガイドを選択し、参照してください。

資料のタイトルの一覧表については、「はじめに」の「関連資料」を参照してください。

Cisco MDS NX-OS Release 4.2（x）の詳細については、次のシスコシステムズの Web サイトから入手できる『*Cisco MDS 9000 Family Release Notes* 』を参照してください。

http://www.cisco.com/en/US/products/ps5989/prod_release_notes_list.htm

このマニュアルについて

新しい『*Cisco Fabric Manager Fabric Configuration Guide*』の情報は、以前は『*Cisco MDS 9000 Family Fabric Manager Configuration Guide*』の「Part 4: Fabric」に記載されていたものです。

表 1 に、このガイドで取り上げる MDS NX-OS Release 4.2（1）以降の新機能および変更された機能を示します。

表 1　Cisco Fabric Manager Release 4.2（x）の新機能および変更された機能

機能	GUI の変更	説明	変更時のリリース	記載箇所
Host Provision ウィザード	Host Provision ウィザード	Host Provision ウィザードに関する情報が追加されました。	4.2(1)	第 2 章「VSAN の設定と管理」
ゾーンおよびゾーンセット	ゾーン設定ウィンドウとゾーンセット設定ウィンドウ	ゾーンへの複数のエンド デバイスの追加およびゾーンセットへの複数のゾーンの追加に関する情報が追加されました。	4.2(1)	第 5 章「ゾーンの設定と管理」
デバイス エイリアス	インターフェイス設定ウィンドウ	インターフェイスの説明にデバイス エイリアスの入力に関する情報が追加されました。	4.2(1)	第 6 章「デバイス エイリアス サービスの配信」
X2 DWDM	モジュール設定ウィンドウ	X2 DWDM トランシーバ周波数	4.2(1)	第 8 章「DWDM の設定」
XRC アクセラレーション	インターフェイス設定ウィンドウ	XRC アクセラレーションの設定に関する情報が追加されました。	4.2(1)	第 11 章「FICON の設定」

はじめに

ここでは、『*Cisco MDS 9000 Family NX-OS Fabric Configuration Guide*』の対象読者、構成、および表記法について説明します。さらに、関連資料の入手方法についても説明します。

対象読者

このマニュアルは、マルチレイヤ ディレクタおよびファブリック スイッチの Cisco MDS 9000 ファミリの設定および保守を担当する、経験豊富なネットワーク管理者を対象にしています。

マニュアルの構成

『*Cisco Fabric Manager Fabric Configuration Guide*』は、次の章で構成されています。

章	タイトル	説明
第 1 章	ファブリックの概要	このマニュアルで説明されている機能の概要を示します。
第 2 章	VSAN の設定と管理	VSAN（仮想 SAN）の仕組み、デフォルト VSAN、分離された VSAN、VSAN ID、および属性について説明し、VSAN の作成、削除、および表示方法の詳細を示します。
第 3 章	SAN Device Virtualization の設定	Cisco MDS SAN-OS Release 3.1（2）および NX-OS Release 4.1（1a）を実行するスイッチの物理エンド デバイスを表すように仮想デバイスを設定する方法について説明します。
第 4 章	ダイナミック VSAN の作成	ホストまたはストレージ デバイス接続が 2 つの Cisco MDS スイッチ間で移動される場合に、ファブリック トポロジを維持するために使用される Dynamic Port VSAN Membership（DPVM）機能を定義します。
第 5 章	ゾーンの設定と管理	各ゾーニングの概念を定義し、ゾーン セットおよびゾーン管理機能の設定に関する詳細を示します。
第 6 章	デバイス エイリアス サービスの配信	Distributed Device Alias Services（デバイス エイリアス）を使用したファブリック全体でのデバイス エイリアス名の配布について説明します。
第 7 章	ファイバ チャネル ルーティング サービスおよびプロトコルの設定	ファイバ チャネル ルーティング サービスおよびプロトコルの詳細情報と設定情報を示します。
第 8 章	DWDM の設定	Dense Wavelength Division Multiplexing（DWDM; 高密度波長分割多重）は、1 つの光ファイバで複数のオプティカル キャリア信号を多重化します。DWDM は、異なる波長を使用してさまざまな信号を伝送します。
第 9 章	FLOGI、ネーム サーバ、FDMI、および RSCN データベースの管理	ストレージ デバイスの管理および Registered State Change Notification（RSCN）データベースの表示に必要となる、ネーム サーバおよびファブリックのログインについて詳述します。
第 10 章	SCSI ターゲットの検出	SCSI LUN 検出機能の開始方法および表示方法について説明します。
第 11 章	FICON の設定	Cisco MDS スイッチの FICON（FI-bre CON-nection）インターフェイス、ファブリック バインディング、および Registered Link Incident Report（RLIR）機能の詳細について説明します。
第 12 章	高度な機能および概念	高度な設定機能（TOV、fctrace、Fabric Analyzer、WWN、フラット FC ID、ループ モニタリング、およびスイッチの相互運用）について説明します。

表記法

コマンドの説明では、次の表記法を使用しています。

太字	コマンドおよびキーワードは太字で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で示しています。
[ ]	角カッコの中の要素は、省略可能です。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。

出力例では、次の表記法を使用しています。

`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、かぎカッコ（<>）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、このマニュアル以外の参照資料などを紹介しています。

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。

関連資料

Cisco MDS 9000 ファミリのマニュアル セットには、次の資料が含まれます。オンラインでドキュメントを検索するには、次の Web サイトにある Cisco MDS NX-OS Documentation Locator を使用してください。

http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/roadmaps/doclocater.htm

リリース ノート

- *Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Releases*
- *Cisco MDS 9000 Family Release Notes for Storage Services Interface Images*
- *Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images*

安全上の警告および準拠規格

- *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*

互換性情報

- *Cisco MDS 9000 NX-OS Hardware and Software Compatibility Information*
- *Cisco MDS NX-OS Release Compatibility Matrix for Storage Service Interface Images*
- *Cisco MDS 9000 Family Interoperability Support Matrix*
- *Cisco MDS NX-OS Release Compatibility Matrix for IBM SAN Volume Controller Software for Cisco MDS 9000*

ハードウェアのインストレーション

- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9200 Series Hardware Installation Guide*

ソフトウェアのインストレーションおよびアップグレード

- *Cisco MDS 9000 Family Software Upgrade and Downgrade Guide - For Cisco NX-OS*
- *Cisco MDS 9000 Family Storage Services Interface Image Install and Upgrade Guide - For Cisco NX-OS*
- *Cisco MDS 9000 Family Port Analyzer Adapter Installation and Configuration Note*

Cisco NX-OS

- *Cisco NX-OS Fundamentals Configuration Guide*
- *Cisco NX-OS Family Licensing Guide*
- *Cisco MDS 9000 Family NX-OS System Management Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Fabric Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Quality of Service Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Security Configuration Guide*

- *Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*
- *Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide*

Cisco Fabric Manager

- *Cisco MDS 9000 Family Fabric Manager Installation and Upgrade Guide*
- *Cisco MDS 9000 Family Fabric Manager Configuration Guide*
- *Cisco Fabric Manager Fundamentals Configuration Guide*
- *Cisco Fabric Manager System Management Configuration Guide*
- *Cisco Fabric Manager Interfaces Configuration Guide*
- *Cisco Fabric Manager Fabric Configuration Guide*
- *Cisco Fabric Manager Quality of Service Configuration Guide*
- *Cisco Fabric Manager Security Configuration Guide*
- *Cisco Fabric Manager IP Services Configuration Guide*
- *Cisco Fabric Manager Intelligent Storage Services Configuration Guide*
- *Cisco Fabric Manager High Availability and Redundancy Configuration Guide*
- *Cisco MDS 9000 Fabric Manager Online Help*
- *Cisco MDS 9000 Fabric Manager Web Services Online Help*
- *Cisco Fabric Manager Web Services Programming Guide*

コマンドライン インターフェイス

- *Cisco MDS 9000 Family CLI Configuration Guide*
- *Cisco MDS 9000 Family Command Reference*
- *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide*

インテリジェント ストレージ ネットワーク サービス コンフィギュレーション ガイド

- *Cisco MDS 9000 Family NX-OS Intelligent Storage Services Configuration Guide*
- *Cisco MDS 9000 Family SANTap Deployment Guide*
- *Cisco MDS 9000 Family Data Mobility Manager Configuration Guide*
- *Cisco MDS 9000 Family Storage Media Encryption Configuration Guide*
- *Cisco MDS 9000 Family Secure Erase Configuration Guide* - For Cisco MDS 9500 and 9200 Series

トラブルシューティングおよび参考資料

- *Cisco MDS 9000 Family Troubleshooting Guide*
- *Cisco MDS 9000 Family MIB Quick Reference*
- *Cisco MDS 9000 Family SMI-S Programming Reference*
- *Cisco MDS 9000 Family System Messages Reference*

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。

CHAPTER 1

ファブリックの概要

Cisco MDS 9000 ファミリ NX-OS コマンドライン インターフェイス（CLI）では、VSAN、SAN デバイスの仮想化、動的 VSAN、ゾーン、Distributed Device Alias Service、ファイバ チャネル ルーティング サービスおよびプロトコル、FLOGI、ネーム サーバ、FDMI、RSCN データベース、SCSI ターゲット、FICON、その他の高度な機能などの機能を設定および管理できます。

この章では、これらの機能のいくつかについて、次の内容を説明します。

仮想 SAN

仮想 SAN（VSAN）テクノロジーは、単一の物理 SAN を複数の VSAN に分割します。VSAN 機能を使用すると、Cisco NX-OS ソフトウェアで、大規模な物理ファブリックを個々の分離された環境に論理的に分割して、ファイバ チャネル SAN のスケーラビリティ、アベイラビリティ、管理性、およびネットワーク セキュリティを高めることができます。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 内にファブリック設定およびエラー条件を含めることにより、ネットワークの不安定さを大幅に軽減します。VSAN が実現する厳密なトラフィック分離は、特定の VSAN の制御およびデータ トラフィックを VSAN 独自のドメイン内に限定することにより、SAN セキュリティを高めるために役立ちます。VSAN は、アベイラビリティを低下させることなく、分離された SAN アイランドを共通のインフラストラクチャに容易に統合できるようにすることで、コスト削減に貢献します。

ユーザは、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、ネットワーク管理者ロールは、すべてのプラットフォーム固有の機能を設定できるように設定できます。一方、その他のロールは、特定の VSAN 内だけで設定および管理を行えるように設定できます。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 FCIP リンク全体にわたりサポートされます。Cisco MDS 9000 ファミリ 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。

ダイナミック ポート VLAN メンバシップ

スイッチのポート VSAN メンバ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。VSAN をデバイス WWN に基づいて割り当てることにより、VSAN メンバシップをポートに動的に割り当てることができます。この方法は Dynamic Port VSAN Membership（DPVM）機能といいます。DPVM により、柔軟性が高まり、ホストまたはストレージ デバイスの接続が 2 つの Cisco MDS スイッチ間またはスイッチ内の 2 つのポート間で移動される場合に、ファブリック トポロジを維持するためにポート VSAN メンバシップを再設定する必要がなくなります。DPVM ではデバイスが接続されているか、移動されているかに関係なく、設定済みの VSAN を保持します。

SAN デバイス仮想化

Cisco SAN デバイス仮想化（SDV）では、物理エンド デバイスを表す仮想デバイスを SAN 設定のために使用できます。SAN デバイスの仮想化によって、ハードウェアの交換に要する時間を大幅に削減できます。たとえば、ストレージ アレイが SDV を使用せずに交換された場合、SAN ゾーン分割の変更およびホスト オペレーティング システム設定の更新のためにサーバのダウンタイムが必要になります。SDV を使用すると、ハードウェアの交換後には仮想デバイスと物理デバイス間のマッピングを変更するだけで済み、広範囲の設定変更から SAN とエンド デバイスを分離することができます。

ゾーン分割

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

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

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

Distributed Device Alias Service

Cisco MDS 9000 ファミリのすべてのスイッチは、VSAN 単位およびファブリック全体での Distributed Device Alias Service（デバイス エイリアス）をサポートしています。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 サービスおよびプロトコル

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標準パス選択プロトコルです。FSPF 機能は、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。
- 指定されたパスに障害が発生した場合に、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。

マルチプロトコル サポート

ファイバ チャネル プロトコル（FCP）のサポートに加え、Cisco NX-OS ソフトウェアでは、単一プラットフォーム内で IBM Fibre Connection（FICON）、Small Computer System Interface over IP（iSCSI）、および Fibre Channel over IP（FCIP）をサポートしています。Cisco MDS 9000 ファミリ スイッチでの Native iSCSI のサポートは、顧客が広範囲に及ぶサーバのストレージを SAN 内の共通プールに統合するのに役立ちます。

CHAPTER 2

VSAN の設定と管理

Cisco MDS 9000 ファミリ スイッチおよび Cisco Nexus 5000 シリーズ スイッチでバーチャル SAN（VSAN）を使用すると、ファイバ チャネル ファブリックのセキュリティを強化し、安定性を高めることができます。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 を作成することができます。各 VSAN には最大 239 のスイッチを含めることができ、それぞれが独立したアドレス領域を持っているため、複数の VSAN で同時に同じ FC ID（ファイバ チャネル ID）を使用できます。この章の内容は、次のとおりです。

VSAN の概要

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 トラフィックの交換を目的にホストとストレージデバイス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。

ここでは VSAN について、次の内容を説明します。

VSAN トポロジ

VSAN を導入すると、ネットワーク管理者はスイッチ、リンク、および 1 つまたは複数の VSAN を含む単一のトポロジを構築できます。このトポロジの各 VSAN では、SAN の動作およびプロパティが同じです。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 Fibre Channel ID（FC ID）を別の VSAN 内のホストに割り当てて、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 などの必須プロトコル、ドメイン マネージャ、およびゾーン分割をすべて実行します。
- 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 に伝搬されません。

図 2-1 と 図 2-2 の両方に表示されているスイッチ アイコンは、これらの機能が Cisco MDS 9000 ファミリのすべてのスイッチに適用されることを示します。

図 2-1 に、各階にスイッチが 1 つある合計 3 つのスイッチによるファブリックを示します。スイッチと接続されたデバイスの地理的な配置は、論理 VSAN のセグメンテーションには依存しません。VSAN 間では、通信が行えません。各 VSAN 内で、すべてのメンバーが相互に対話できます。

図 2-1　論理 VSAN のセグメンテーション

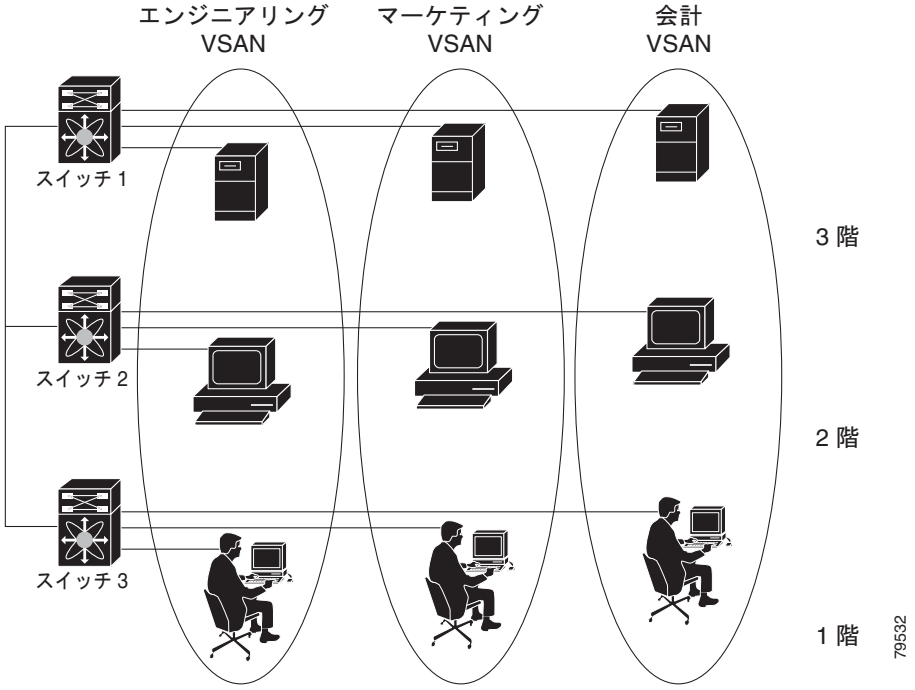
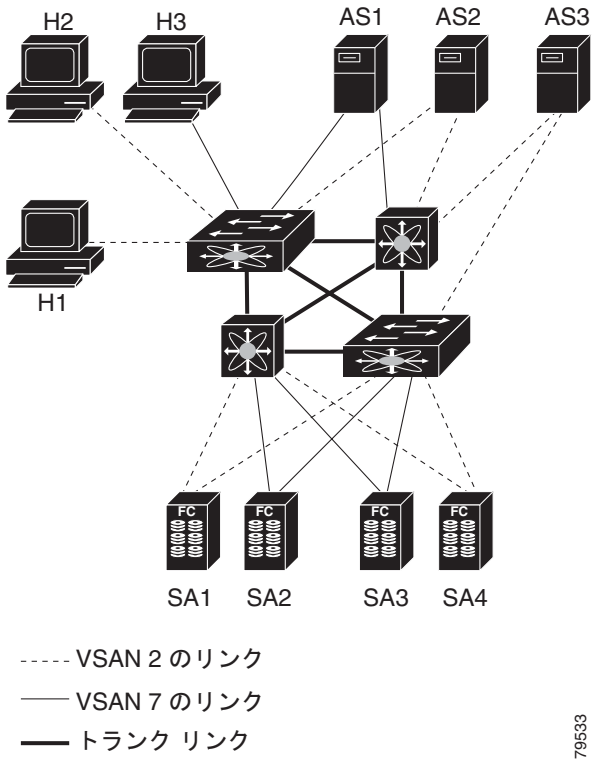


図 2-2 に、VSAN 2（点線）と VSAN 7（実線）の 2 つ VSAN が定義されている、物理ファイバ チャネル スイッチングのインフラストラクチャを示します。VSAN 2 には、ホスト H1 および H2、アプリケーション サーバ AS2 および AS3、およびストレージ アレイ SA1 および SA4 が含まれます。VSAN 7 は、H3、AS1、SA2、および SA3 と接続します。

図 2-2　2 つの VSAN の例



このネットワーク内の 4 つのスイッチは、VSAN 2 と VSAN 7 の両方のトラフィックを伝送するトランク リンクによって相互接続されます。VSAN 2 と VSAN 7 の両方のスイッチ間トポロジは同じです。これは要件ではないため、ネットワーク管理者は特定のリンクで特定の VSAN をイネーブルにして別の VSAN トポロジを作成できます。

VSAN がなければ、ネットワーク管理者は、別個の SAN に対して別個のスイッチとリンクが必要になります。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 で共有できます。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。図 2-2 に、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を行う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示します。

このようなグループを作成する基準は、VSAN トポロジに基づいて異なります。

- VSAN は、次の要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すことができます。

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 内だけにデバイスを常駐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の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拡張します。
- VSAN 単位のファブリック サービス：VSAN 単位でファブリック サービスを複製することにより、スケーラビリティとアベイラビリティが向上します。
- 冗長性：同一の物理 SAN 上に複数の VSAN を作成することにより、冗長性が保証されます。1 つの VSAN に障害が発生した場合、ホストとデバイスの間にあるバックアップ パスによって（同一の物理 SAN の別の 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 へデバイスを移動する場合は、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 つが分離 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

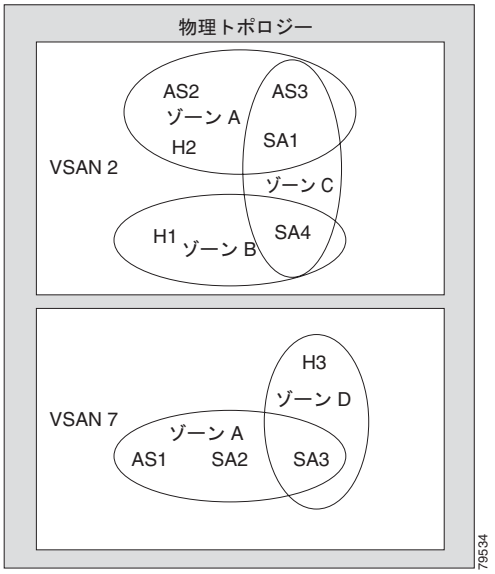
VSAN に複数のゾーンを定義できます。2 つの VSAN は未接続の 2 つの SAN に相当するので、VSAN 1 のゾーン A は、VSAN 2 のゾーン A とは異なり、別個のものです。表 2-1 に、VSAN とゾーンとの相違点を示します。

表 2-1　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、およびゾーン分割プロトコルは、ゾーン単位では利用できません
—	ゾーンは常に VSAN 内に含まれます。ゾーンが 2 つの VSAN にわたることはありません。
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。
メンバシップは、通常 VSAN ID を使用して Fx ポートに定義されます。	メンバシップは、通常 pWWN によって定義されます。
HBA またはストレージ デバイスは、1 つの VSAN（Fx 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、発信元ポート、および宛先ポートでメンバシップを実行します。	ゾーンは、発信元ポートおよび宛先ポートだけでメンバ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発信側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。

図 2-3 に、VSAN とゾーンの可能な組み合わせを示します。VSAN 2 では、ゾーン A、ゾーン B、およびゾーン C の 3 つのゾーンが定義されます。ゾーン C は、ファイバ チャネル標準により許可される場合、ゾーン A とゾーン B にオーバーラップします。VSAN 7 では、ゾーン A とゾーン D の 2 つのゾーンが定義されます。VSAN 境界を越えるゾーンはありません。ゾーン全体が VSAN 内に収まります。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 と異なり、別個のものです。

図 2-3　VSAN とゾーン分割



VSAN 設定

VSAN には次の属性があります。

- VSAN ID：VSAN ID は、デフォルト VSAN（VSAN 1）、ユーザ定義の VSAN（VSAN 2 ～ 4093）、および分離された 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 はさまざまな条件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 が設定されていて、イネーブルにされてい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：管理目的に VSAN を識別するテキスト ストリング。名前は、1 ～ 32 までの文字が可能で、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" と VSAN ID を表す 4 桁ストリングとを連結して、VSAN 名が付けられます。たとえば、VSAN 3 のデフォルト名は VSAN0003 です。

（注）　VSAN 名は一意のものである必要があります。

- ロード バランシング属性：ロード バランシング パスの選択に発信元/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）を使用するように指示する属性。

（注）　第 1 世代スイッチング モジュールでは、IVR 対応スイッチからの IVR トラフィックに対しては、OX ID ベースのロード バランシングがサポートされませんでした。IVR 非対応の MDS スイッチからの IVR トラフィックに対しては、OX ID ベースのロード バランシングが機能します。第 2 世代のスイッチング モジュールでは、IVR 対応スイッチからの IVR トラフィックに対して、OX ID ベースのロード バランシングがサポートされるようになりました。

ここでは、VSAN の作成および設定方法について、次の内容を説明します。

VSAN 作成の概要

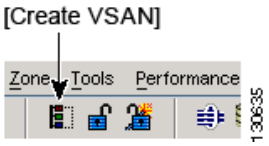
VSAN がアクティブで、最低 1 つのポートが起動していれば、VSAN は動作ステートにあります。このステートは、トラフィックがこの VSAN を通過できることを示します。このステートは設定できません。

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。Fabric Manager を使用して VSAN を作成および設定する手順は、次のとおりです。

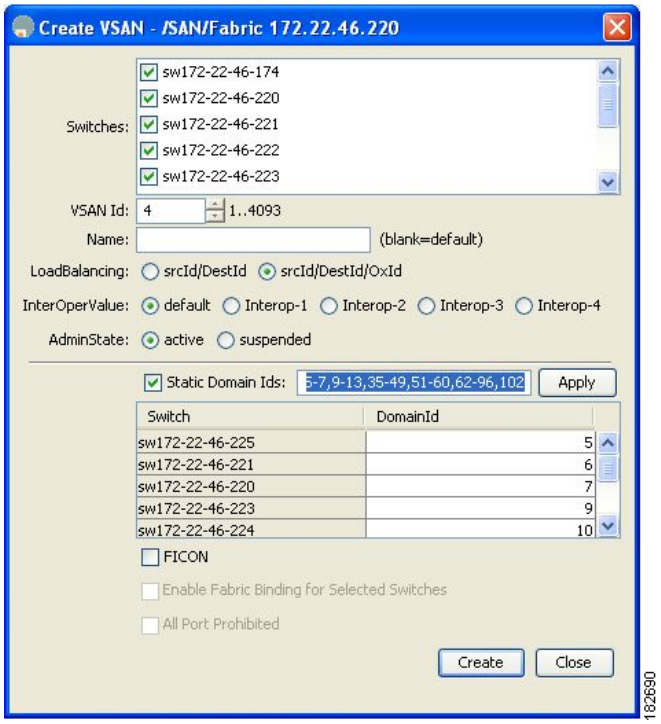
ステップ 1　[Create VSAN] アイコンをクリックします（図 2-4 を参照）。

図 2-4　[Create VSAN] アイコン



[Create VSAN] ダイアログボックスが表示されます（図 2-5 を参照）。

図 2-5　[Create VSAN] ダイアログボックス



（注）　Cisco SAN-OS Release 3.1(2) 以上の場合、[Static Domain Ids] チェックボックスがオンの場合、Fabric Manager によって中断モードの VSAN が作成され、自動的に VSAN がアクティブになります。

ステップ 2　この VSAN で必要なスイッチをオンにします。

ステップ 3　[VSAN Name] フィールドと [VSAN ID] フィールドに入力します。

ステップ 4　[LoadBalancing] 値と [InterOperValue] を設定します。

ステップ 5　[Admin State] を [active] または [suspended] に設定します。

ステップ 6　[Static Domain Ids] チェックボックスをオンにして、未使用の静的ドメイン ID を VSAN に割り当てます。

ステップ 7　（任意）この機能をイネーブルにする場合は、[FICON] オプションおよび [Enable Fabric Binding for Selected Switches] オプションをオンにします。

詳細については、「FICON の設定」（P.11-1）および『*Cisco MDS 9000 Family NX-OS Security Configuration Guide*』を参照してください。

ステップ 8　このダイアログボックスのフィールドへの入力が完了したら、[Create] をクリックして VSAN を追加するか、[Close] をクリックします。

ポート VSAN メンバシップの概要

スイッチのポート VSAN メンバ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 メンバシップを割り当てることができます。

- 静的：VSAN をポートに割り当てる

  「スタティック ポート VSAN メンバシップの概要」（P.2-8）を参照してください。

- 動的：デバイスの WWN に基づいて VSAN を割り当てる この方法は Dynamic Port VSAN Membership（DPVM）機能といいます。

  第 4 章「ダイナミック VSAN の作成」を参照してください。

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（『*Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide*』を参照）。

スタティック ポート VSAN メンバシップの概要

Fabric Manager を使用してインターフェイスの VSAN メンバシップを静的に割り当てる手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインから [Interfaces] > [FC Physical] を選択します。[Information] ペインにインターフェイス設定が表示されます。

ステップ 2　[General] タブをクリックします。

ファイバ チャネルの一般的物理情報が表示されます。[PortVSAN] フィールドをダブルクリックして入力します。

ステップ 3　変更内容を保存する場合は、[Apply Changes] をクリックします。保存されていない変更を破棄する場合は、[Undo Changes] をクリックします。

デフォルト VSAN の概要

Cisco MDS 9000 ファミリのスイッチの出荷時の設定値では、デフォルト VSAN 1 だけがイネーブルにされています。製造環境 VSAN として VSAN 1 を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。

（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 つが分離 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 の概要

VSAN 4094 は分離された VSAN です。ポートが属する VSAN が削除された場合、非トランキングポートがすべて、この VSAN に転送されます。これにより、デフォルト VSAN または別の設定済みの VSAN へのポートの暗黙的な転送が回避されます。削除された VSAN のポートはすべて、分離されます（ディセーブルされます）。

（注） VSAN 4094 内の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 分離された 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 つが分離 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 メンバシップの概要

Fabric Manager を使用して分離された VSAN に存在するインターフェイスを表示する手順は、次のとおりです。

ステップ 1　[Fabricxx] を展開し、[Logical Domains] ペインで [All VSANs] を選択します。

[Information] ペインに VSAN 設定が表示されます。

ステップ 2　[Isolated Interfaces] タブをクリックします。

分離された VSAN のインターフェイスが表示されます。

VSAN の動作ステート

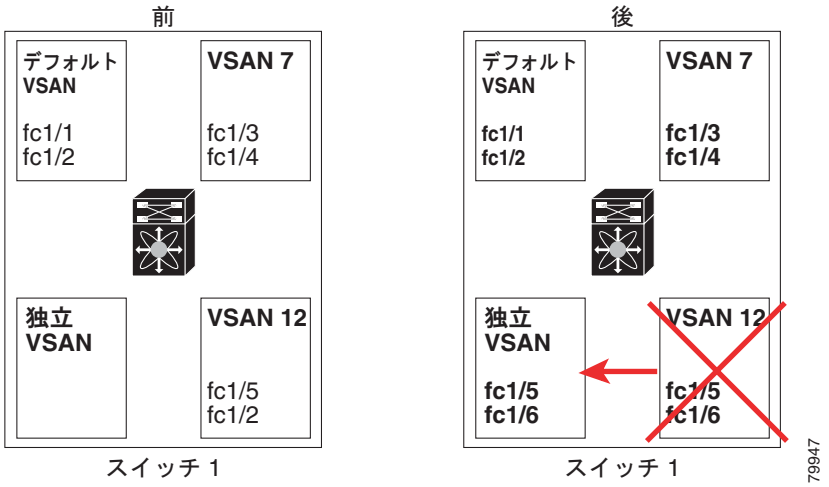
VSAN がアクティブで、最低 1 つのポートが起動していれば、VSAN は動作ステートにあります。このステートは、トラフィックがこの VSAN を通過できることを示します。このステートは設定できません。

スタティック VSAN の削除の概要

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、ポートは分離された 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ません。明示的にポート VSAN メンバシップを再設定する必要があります（図 2-6 を参照）。

図 2-6　　VSAN ポート メンバシップの詳細



- 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（『*Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide*』を参照）。

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。

スタティック VSAN の削除

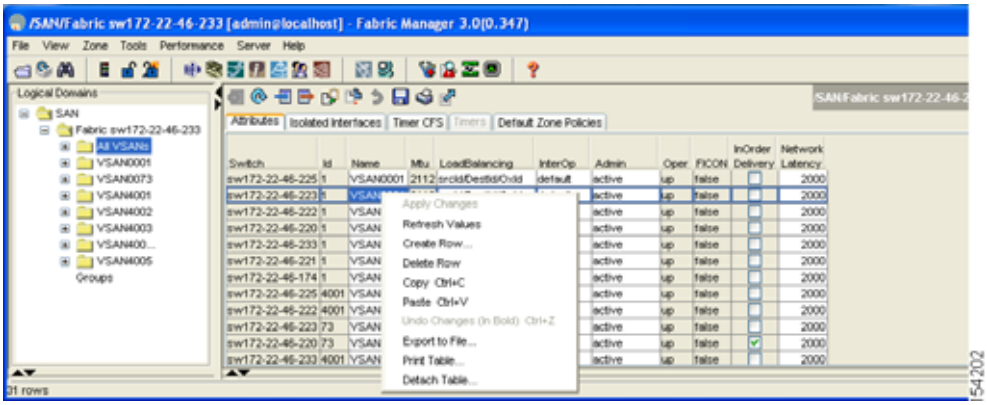
Fabric Manager を使用して VSAN とその属性を削除する手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [All VSANs] を選択します。

[Information] ペインにファブリック内の VSAN が表示されます。

ステップ 2　削除する VSAN を右クリックしてから、ドロップダウン メニューで [Delete Row] を選択します（図 2-7 を参照）。

図 2-7　VSAN の削除



確認ダイアログボックスが表示されます。

ステップ 3　削除を確認する場合は、[Yes] をクリックします。VSAN を削除しないでダイアログボックスを閉じる場合は、[No] をクリックします。

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 パス選択に対する発信元/宛先 ID（src-dst-id）または Originator Exchange（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

Fabric Manager を使用して既存の VSAN にロード バランシングを設定する手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [Fabricxx] > [All VSANs] を選択します。

[Information] ペインに VSAN 設定が表示されます（図 2-8 を参照）。

図 2-8　すべての VSAN の属性

ステップ 2　VSAN を選択して、[LoadBalancing] フィールドに入力します。

ステップ 3　変更内容を保存する場合は、[Apply Changes] をクリックします。保存されていない変更を破棄する場合は、[Undo Changes] をクリックします。

Interop モードの概要

相互運用性により、複数ベンダー製品間の相互接続が可能になっています。ファイバ チャネル標準規格では、ベンダーに対して共通の外部ファイバ チャネル インターフェイスを使用することを推奨しています。「スイッチの相互運用性」（P.12-9）を参照してください。

FICON VSAN の概要

最大 8 つの VSAN で FICON をイネーブルできます。「FICON VSAN の前提条件」（P.11-8）を参照してください。

Host Provisioning ウィザード

Host Provisioning ウィザードでは、複数のツールや機能を使用する必要なしに、直観的な方法で新しいホストを稼動または既存のホストを稼動中止できます。ウィザードに従って、デバイス エイリアスを作成し、DPVM、ゾーン、およびフロー作成の設定ができます。

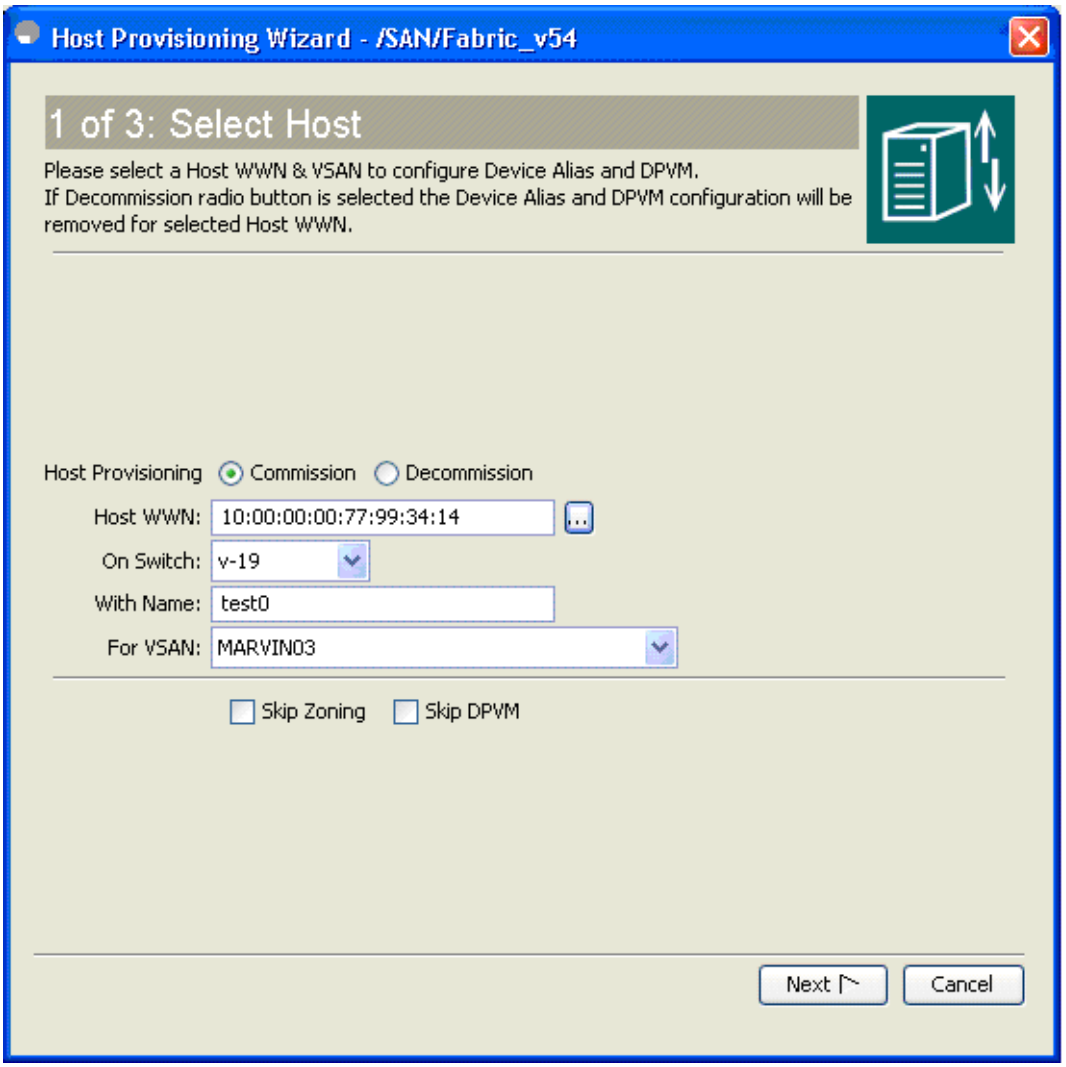
ここで説明する内容は、次のとおりです。

ホストの稼動

新しいホストを稼動する手順は、次のとおりです。

ステップ 1　[Fabric Manager] ウィンドウから、[Tools] > [Host Provisioning] を選択します。
Host Provisioning ウィザード ウィンドウが表示されます（図 2-9）。

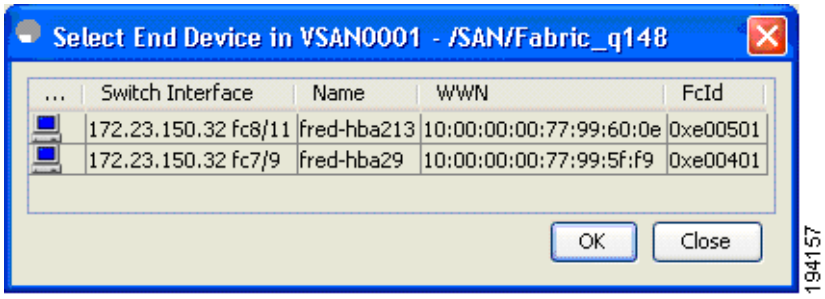
図 2-9　Host Provisioning ウィザード - Select Host



ステップ 2　[Commission] ラジオ ボタンをクリックします。

ステップ 3　[...] をクリックして既存の設定または VSAN のホストを選択します（図 2-10 を参照）か、VSAN 内にない、またはまだ設定されていないホストの WWN を入力します。

図 2-10　ホストの選択



ホスト設定がすでに存在する場合は、スイッチ、デバイス エイリアス、および VSAN 情報がウィンドウに読み込まれます。

設定がまだ存在しない場合は、WWN のデバイス エイリアスを入力し、設定が開始されるスイッチを入力して、ホストが属する VSAN を選択します。Host Provisioning ウィザード ウィンドウで [Next] をクリックすると、エントリが作成されて保存されます。

ステップ 4　[Skip Zoning] チェックボックスをオフにします。

[Next] をクリックした後、Select Targets（図 2-11）ウィンドウおよび Select Zone（図 2-12）ウィンドウが表示されます。

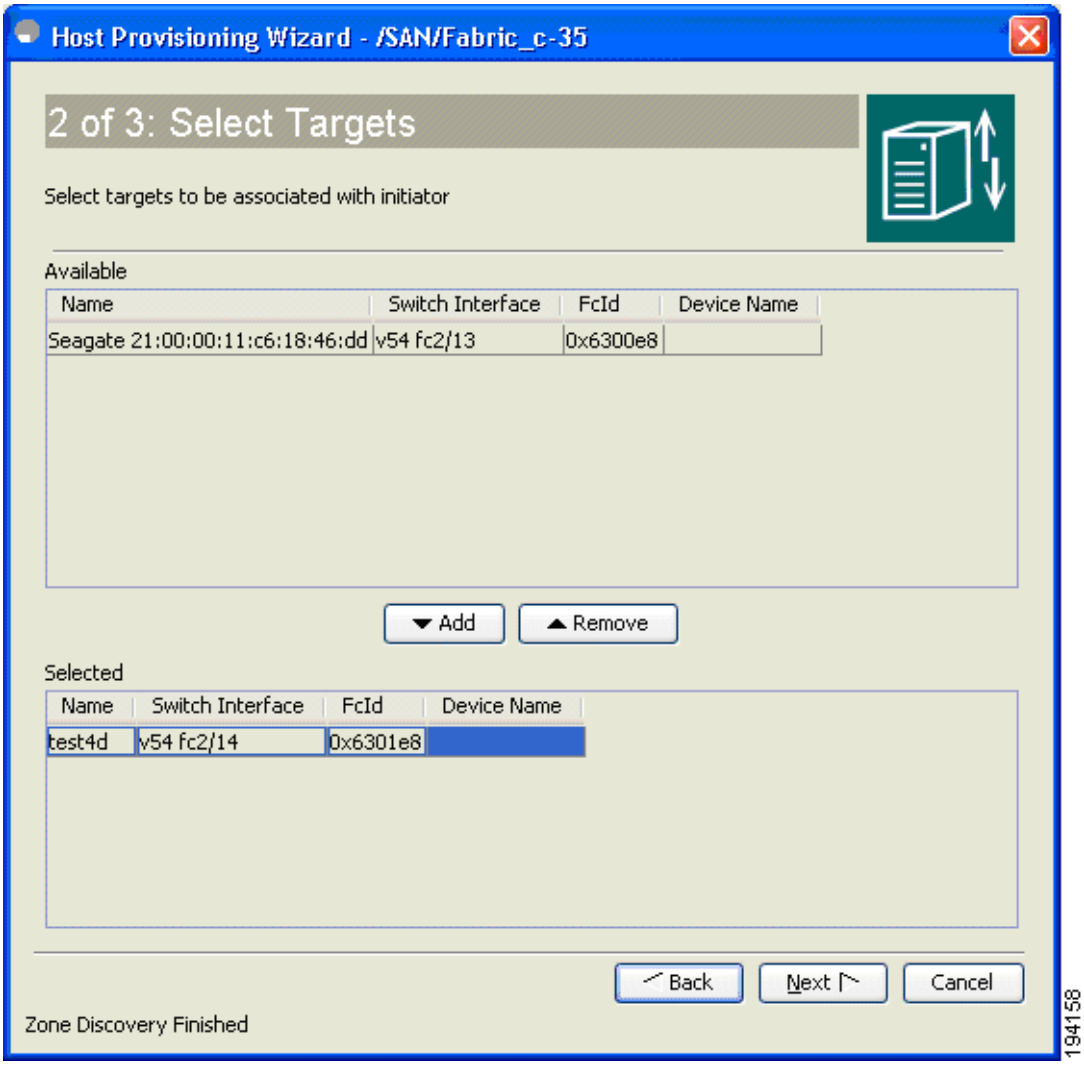
ステップ 5　[Skip DPVM] チェックボックスをオフにします。

[Next] をクリックすると、DPVM エントリが作成されます。

ステップ 6　[Next] をクリックします。

[Select Targets] ウィンドウが表示されます。

図 2-11　Host Provisioning ウィザード - Select Targets



（注）　Host Provisioning ウィザードでは、選択された VSAN 内のすべてのスイッチで、基本および拡張デバイス エイリアス、DPVM、および CFS がイネーブルになっている必要があります。

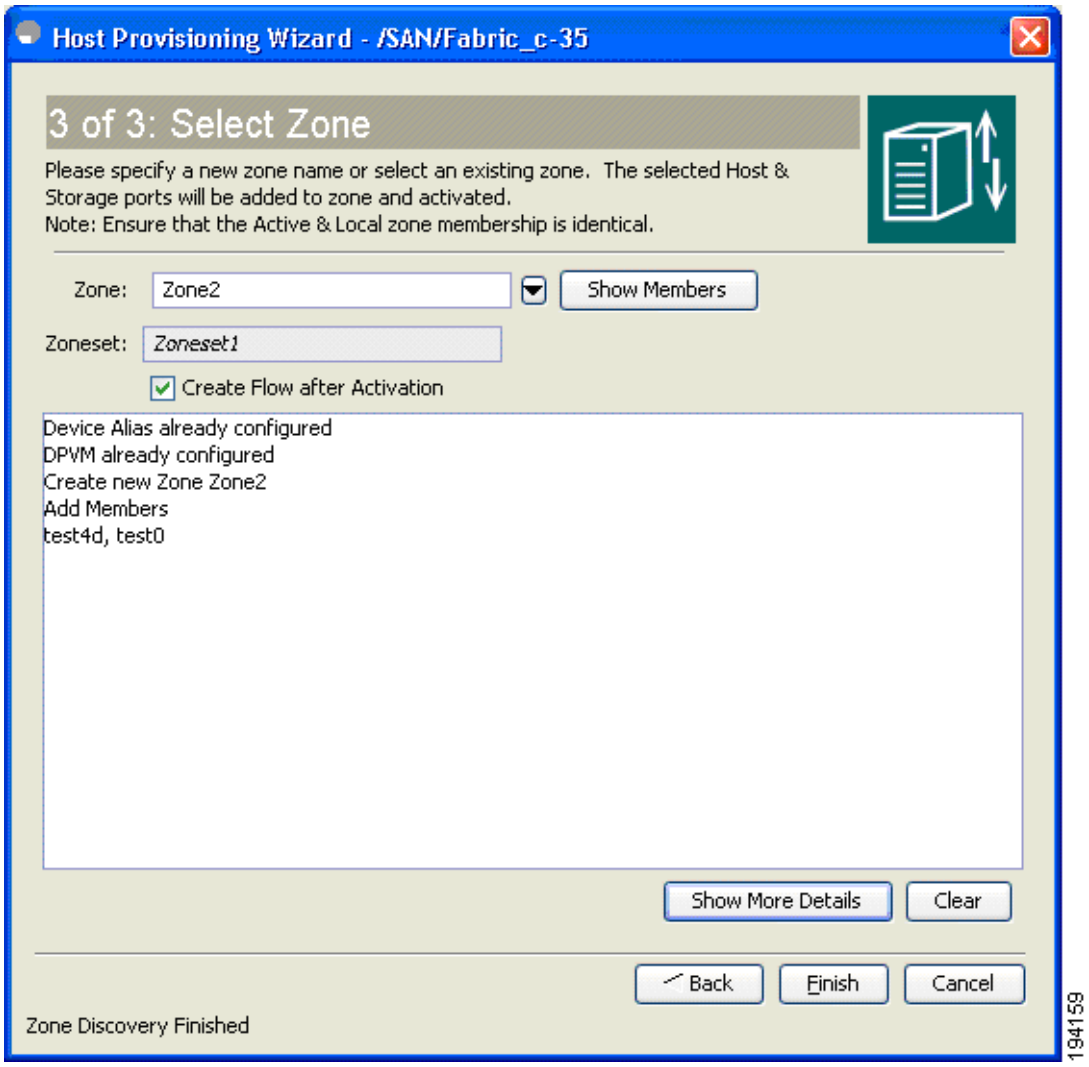
ステップ 7　ホストが通信する必要があるターゲットを選択し、[Add]（図 2-11）をクリックします。

ターゲット エントリがウィンドウの下部に移動します。

ステップ 8　[Next] をクリックします。

[Select Zone] ウィンドウが表示されます。

図 2-12　Host Provisioning ウィザード - Select Zone



ステップ 9　ゾーンを選択し、[Create Flow after Activation] チェックボックスをオンにします。

[Finish] をクリックすると、ホストおよびストレージがゾーンに追加され、ゾーンがアクティブになり、ホストとストレージの間のフローが作成されます。

ステップ 10　[Finish] をクリックします。

まず、デバイス エイリアスおよび DPVM エントリが作成されます。ゾーンは作成された後、アクティブになります。チェックボックスがオンになっているゾーンに対しては、フローが作成されます。

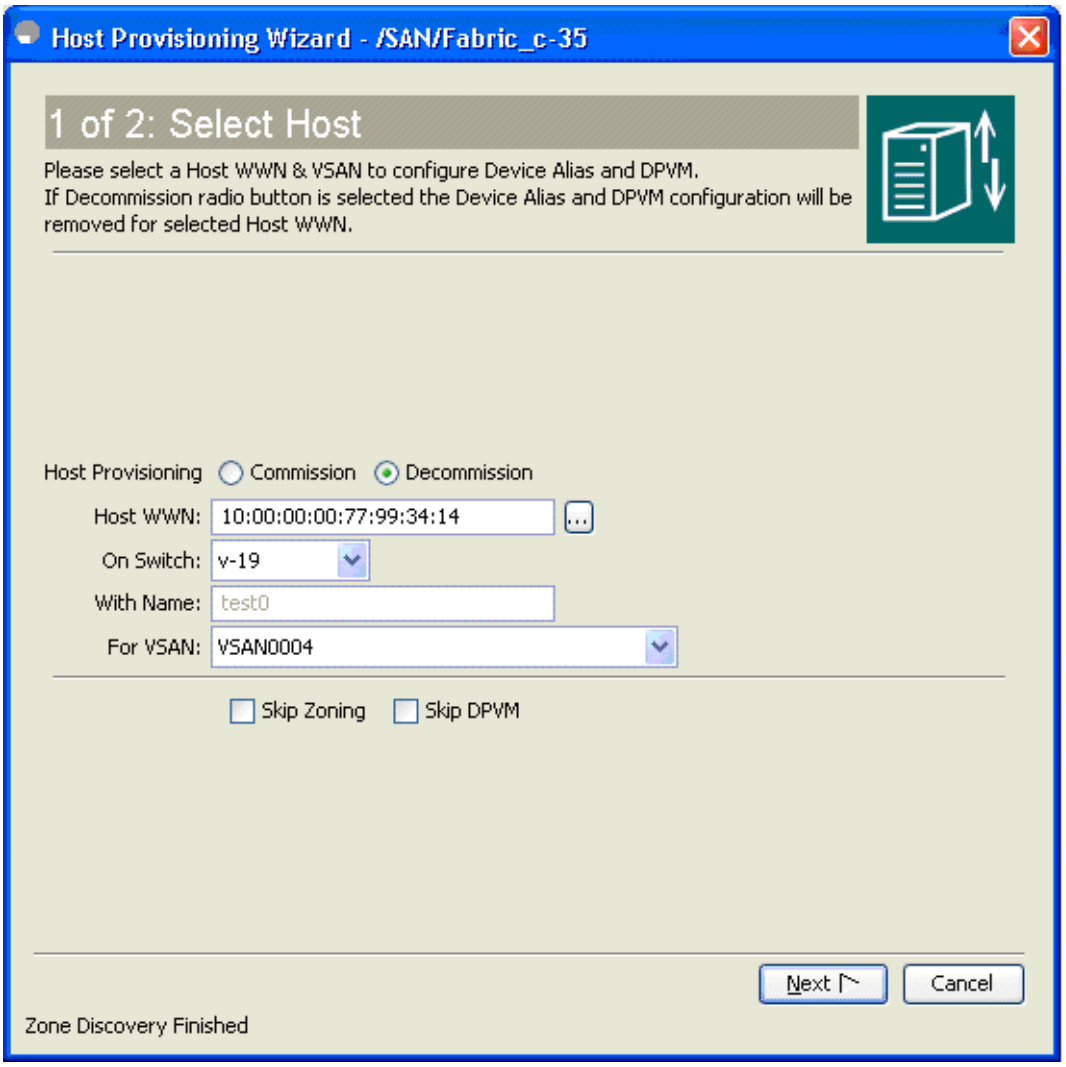
ホストの稼動中止

既存のホストを稼動中止する手順は、次のとおりです。

ステップ 1　[Fabric Manager] ウィンドウから、[Tools] > [Host Provisioning] を選択します。

[Select Host] ウィンドウが表示されます（図 2-13）。

図 2-13　Host Provisioning ウィザード - Select Host



ステップ 2　[Decommission] ラジオ ボタンをクリックします。

ステップ 3　**[...]** をクリックして既存の設定または VSAN からホストを選択するか、VSAN 内にないホストの WWN を入力します。

CFS および CFS DPVM のデバイス エイリアスがイネーブルになっていて、WWN が 8 バイトの数字の場合は、選択された VSAN 内のすべてのスイッチのデバイス エイリアスと DPVM が読み込まれます。[Finish] をクリックすると、デバイス エイリアス エントリが削除されます。

ステップ 4　[Skip Zoning] チェックボックスをオフにします。

WWN ゾーン メンバーがすべてのゾーンから削除されます。WWN メンバーのないゾーンは、いったん単一メンバー ゾーンになると、削除されます。ゾーンの削除によってローカルのアクティブ ゾーンセットが変更された場合は、[Finish] をクリックしたときに該当のゾーンセットがアクティブになります。

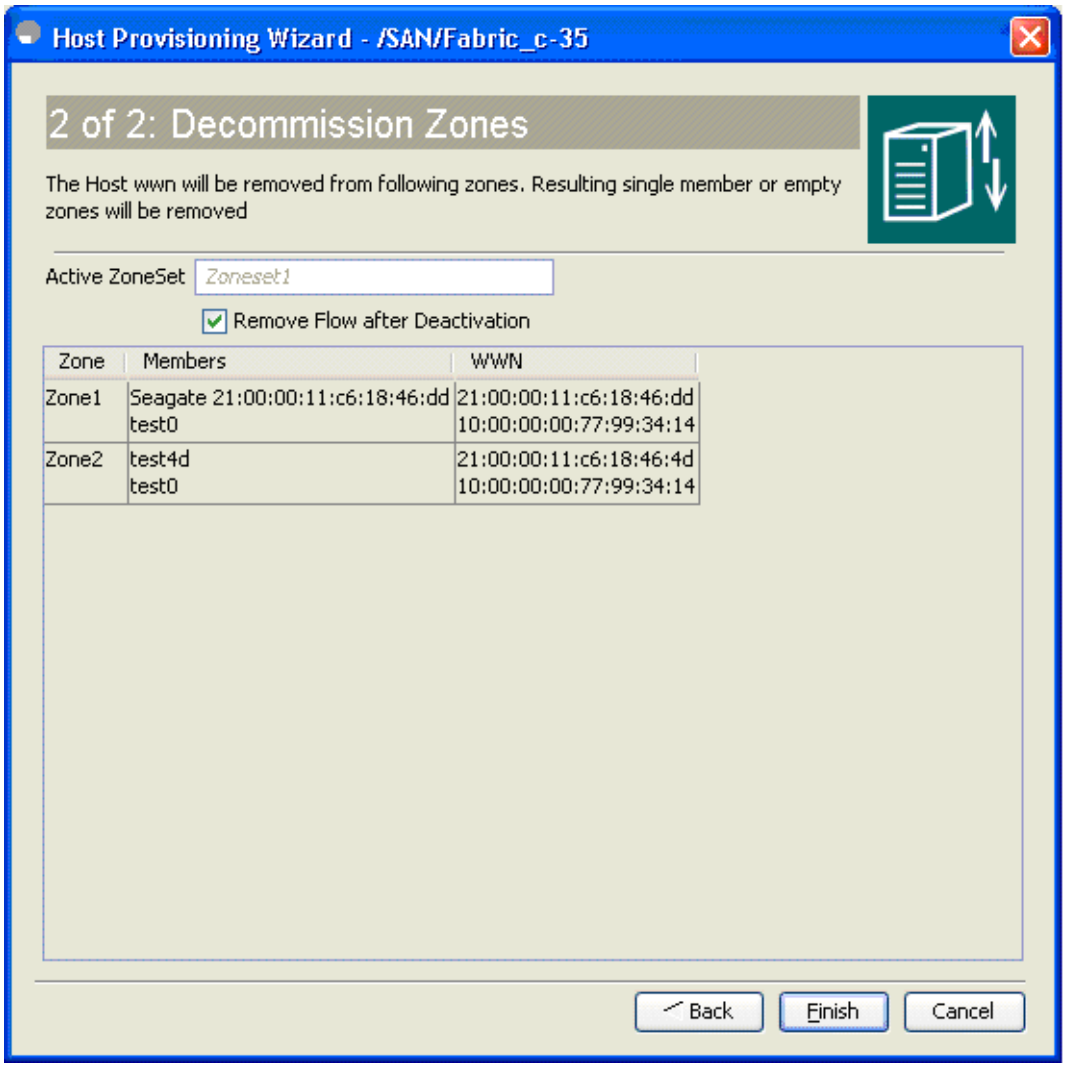
ステップ 5　[Skip DPVM] チェックボックスをオフにします。

[Finish] をクリックすると、DPVM エントリが削除されます。

ステップ 6　[Next] をクリックします。

[Decommission Zones] ウィンドウが表示されます（図 2-14）。

図 2-14　Host Provisioning ウィザード - Decomission Zones



ステップ 7　[Remove Flow after Deactivation] チェックボックスをオンにします。

[Finish] をクリックすると、ホストと関連付けられているフロー エントリが削除されます。

ステップ 8　[Finish] をクリックします。

まずデバイス エイリアスおよび DPVM エントリが削除されます。ホストが削除された後、メンバーが 1 つしか存在しないゾーンは非アクティブになって削除されます。チェックボックスがオンになっているゾーンに対しては、フローが削除されます。

デフォルト設定

表 2-2 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 2-2　デフォルトの 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 桁ストリングとを連結した名前。たとえば、VSAN 3 は VSAN0003 です。
ロード バランシング属性	OX ID（src-dst-ox-id）

CHAPTER 3

SAN Device Virtualization の設定

この章では、Cisco MDS SAN-OS Release 3.1（2）以降または NX-OS Release 4.1（1a）以降を実行するスイッチの物理エンド デバイスを表すように仮想デバイスを設定する方法について説明します。

Cisco SAN Device Virtualization（SDV; SAN デバイス バーチャライゼーション）は、Cisco MDS 9000 Family Enterprise パッケージ（ENTERPRISE_PKG）に付属するライセンス機能です。ライセンスの取得の詳細については、『*Cisco NX-OS Family Licensing Guide*』を参照してください。

この章の内容は、次のとおりです。

SDV の概要

Cisco SAN-OS Release 3.1（2）および NX-OS Release 4.1（1a）以降では、Cisco SDV を使用して、物理エンドデバイスを表す仮想デバイスを作成できます。SAN デバイスのバーチャライゼーションは、交換用ディスク アレイへのスワップアウトまたはフェールオーバーを促進します。また、Host Bus Adapter（HBA; ホスト バス アダプタ）の交換時または別のサーバへのアプリケーションの再ホスティング時のダウンタイムを最小限に抑えます。

仮想化されている SAN デバイスは、発信側またはターゲットにすることができます。ターゲットを仮想化して*仮想ターゲット*を作成し、さらに発信側を仮想化して*仮想発信側*を作成することができます。このような設定では、仮想発信側と仮想ターゲットを区別しません（図 3-1 および図 3-2 を参照）。

図 3-1　　ターゲットのバーチャライゼーション

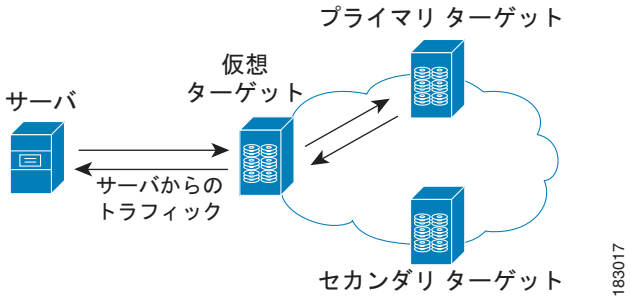
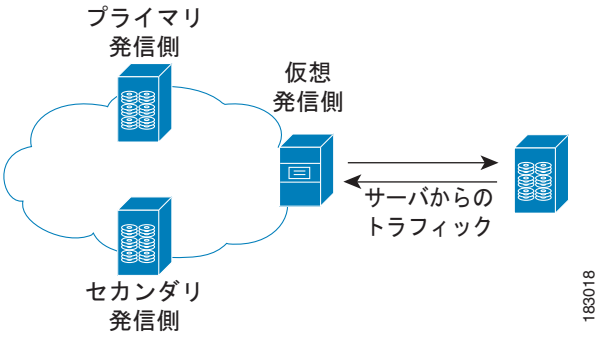


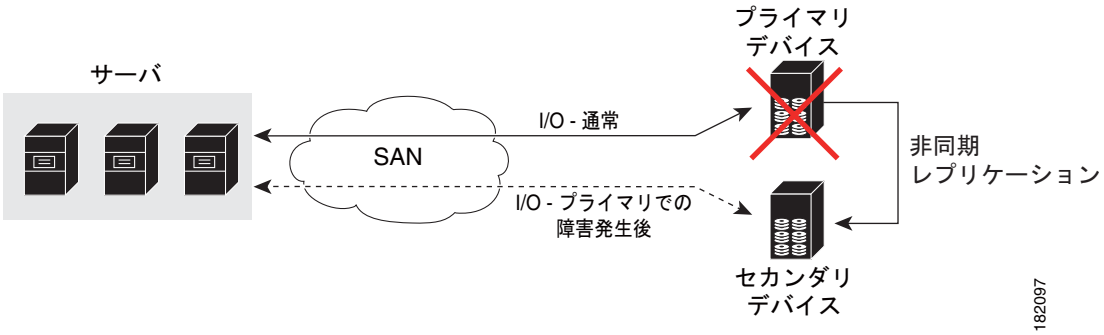
図 3-2　発信側のバーチャライゼーション



（注）　この章のほとんどの例では、ターゲットのバーチャライゼーションについて説明していますが、発信側のバーチャライゼーションも同様に機能します。

通常、今日のデバイス障害処理のための展開は、この設計の重要な部分を占める冗長性によってハイアベイラビリティ（HA）を実現するように設計されます。ターゲットに冗長性を持たせるように設計される場合を考えてみます。この場合、プライマリとセカンダリという 2 つのアレイが展開されます。企業では多くの場合、確実にセカンダリ アレイが実稼動 LUN のミラー コピーになるように、プライマリ アレイとセカンダリ アレイの間で一貫性を保つための何らかのテクノロジー（EMF SRDF など）を利用しています。ただし、プライマリ アレイで障害が発生した場合は、すべての I/O がセカンダリ アレイで処理されなければならないため、セカンダリ アレイに置き換える必要があります。ここで生じる可能性のある問題は、セカンダリ アレイを起動してから稼動するまでに要する時間が、ほとんどの企業にとって許容できないほど長くなってしまうことです（図 3-3 に、この問題を示します）。

図 3-3　SDV を使用する前のデバイス障害処理のための一般的な展開



Cisco SDV を使用*しないで*ストレージ アレイに置き換えた場合、次の作業が必要になることがあります。

- サーバを停止して、新しいアレイ用にゾーン分割とアカウントを変更します。
- 新しいアレイのファイバ チャネル ID（FC ID）と pWWN に対応するように、Cisco NX-OS 設定を変更します。
- 新しい FC ID と pWWN に対応するようにサーバ設定を変更します。

さらに具体的には、SDV を使用しないと、次のような状況になる可能性があります。

- 通常の実稼動環境用にセカンダリ デバイスを設定するのにかなりの時間を要する場合があります。
- ゾーン分割設定では、セカンダリ デバイスを使用してすべての発信側をゾーン分割し、さらに特定の発信側を再設定することが必要になります。たとえば、セカンダリ デバイスの WWN と FC ID が異なるため、ドライバ ファイルを変更し、サーバを再起動する必要があります。

- クラスタリング（複数の発信側）では問題がさらに悪化し、クラスタのサーバごとにフェールオーバー手順を繰り返し行う必要があります。サーバ クラスタが一連の HBA である場合、HBA ごとにすべてのストレージ アレイ FC ID の変更を行う必要があります。

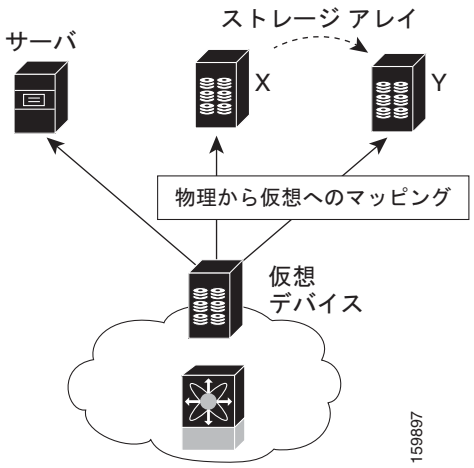
SDV を使用することにより、次のことが実現されます。

- データ マイグレーションに要する時間を短縮し、最終的には全体のダウンタイムを削減します。
- デバイス数の増加への対応が容易になります。

図 3-4 に、SDV の利点を示します。この設定では、ディスク アレイ Y がディスク アレイ X を置き換えます。ディスク アレイ X が配置された後で、ユーザが SDV を使用してすべてのファイバ チャネル インターフェイスの仮想デバイスを作成しました。ディスク アレイ X からのデータ レプリケーション後に、ユーザはアプリケーション サーバ上のアクティビティを一時停止し、サーバで使用されている仮想デバイスにディスク アレイ Y を再びリンクして、ディスク アレイ X のスワップアウトを完了しました。スワップの実行時に手早い対応が求められるときに、ゾーン分割の変更やホスト オペレーティング システム設定の変更を行う必要がなかったため、アプリケーションのダウンタイムが大幅に短縮されました。

（注）　アレイ管理者は多くの場合、仮想デバイスをアレイ Y の pWWN にリンクする前に、アレイ Y をプライマリ デバイスにし、サーバ ログインを受け入れるようにするための処理を行う必要があります。

図 3-4　SDV の例



重要な概念

この章では次の用語を使用します。

- 仮想デバイス：実デバイスの仮想化された表現またはプロキシ表現であり、ネーム サーバに登録され、pWWN と FC ID を持ちます。仮想デバイスは、実デバイス（物理デバイス）がオンラインである限り存在します。仮想デバイスの pWWN および FC ID は一意のものにし、実デバイスの pWWN および FC ID と重複しないようにする必要があります。
- 仮想ドメイン：SDV により予約され、FC ID を仮想デバイスに割り当てます。ドメインを予約したスイッチがダウンした場合、別のスイッチが同じドメインを使用してダウンしたスイッチの役割を引き継ぎます。

- プライマリ デバイス：プライマリとして設定されているデバイス。デフォルトでは、プライマリ デバイスがオンラインである場合、プライマリ デバイスがアクティブ デバイスになります。
- セカンダリ デバイス：設定されている追加のデバイス。デフォルトでは、セカンダリ デバイスはスタンバイ状態になります。
- アクティブ デバイス：現在仮想化されているデバイスは、アクティブ デバイスと呼ばれます。デフォルトでは、プライマリ デバイスがオンラインである場合、プライマリ デバイスがアクティブ デバイスになります。アクティブ デバイスは記号（*）で示されます。

自動フェールオーバーおよびフォールバック

Cisco MDS NX-OS Release 4.1（1a）以降では、SDV は、仮想デバイスの自動フェールオーバーおよびフォールバック設定をサポートしています。以前のすべてのリリースでは、障害が発生した場合には、デバイスをプライマリとしてアクティブにするために手動で設定を行う必要がありました。自動フェールオーバーおよびフォールバック設定の導入により、アクティブ デバイスは、記号（*）で示されるプライマリ デバイスと区別されています。

- 自動フェールオーバー：障害の発生時に、failover auto 属性は自動的にプライマリ デバイスをシャットダウンし、セカンダリ デバイスをアクティブ状態にします。プライマリ デバイスがオンライン状態に戻ったとき、スイッチオーバーを行うためにユーザの介入が必要になります。
- フォールバックを伴う自動フェールオーバー：自動フェールオーバーに加え、フェールオーバー後にプライマリ デバイスがオンラインに戻ったとき、プライマリ デバイスがアクティブ状態になり、セカンダリ デバイスがスタンバイ状態に移行します。

SDV の設定

SDV は、配信サービスであり、Cisco Fabric Services（CFS）配信を使用してデータベースを同期します。SDV は設定されると、CFS セッションを開始し、ファブリックをロックします。ファブリックがロックされると、Cisco NX-OS ソフトウェアではロックを保持しているスイッチ以外のスイッチからの設定変更を許可せず、ロックされたステータスにあることをユーザに通知するメッセージを発行します。設定変更は、アプリケーションの保留データベースで保持されます。設定をアクティブにし、すべてのスイッチのロックを解除するために、コミット動作を実行する必要があります。

CFS の詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。

（注） SDV をイネーブルにすると、CFS 配信もイネーブルになるため、SDV の CFS 配信はディセーブルにできません。

ここでは、SDV の設定方法について説明します。

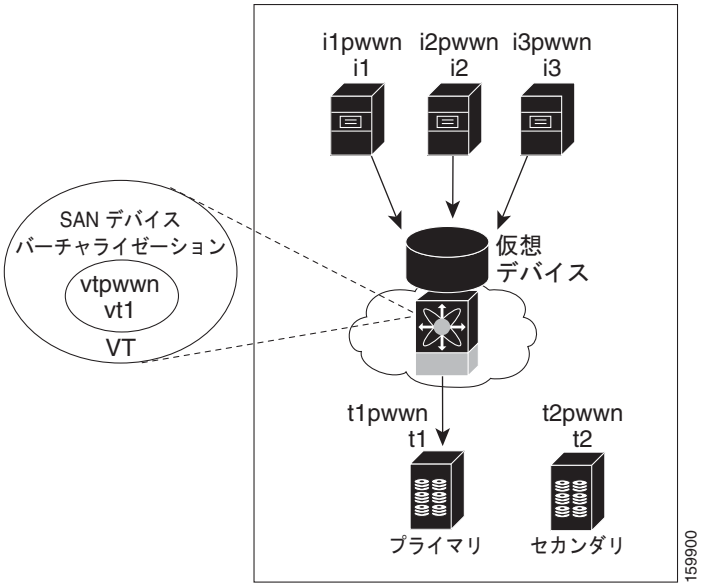
- 「仮想デバイスの設定」（P.3-5）
- 「仮想デバイスと物理デバイスのリンク」（P.3-7）
- 「ファブリック マージの矛盾の解決」（P.3-9）

仮想デバイスの設定

仮想デバイスは最大 32 文字の英数字の名前で識別され、その仮想デバイスが表すすべての実デバイス（1 つのプライマリと 1 つまたは複数のセカンダリ）を定義します。仮想デバイスが正常に作成されると、仮想デバイス名は、デバイス エイリアス名としてデバイス エイリアス データベースに内部的に登録されます。このとき、pWWN は、Cisco Organizational Unique Identifier（OUI; 組織固有識別子）を使用して自動的に割り当てられます。仮想デバイスは、実際の物理デバイスとして表示されます。最大 128 台のデバイスを 1 つの仮想デバイスとして表示できます。1 つの VSAN 内で作成できる仮想デバイス数の上限は、4,095 です。

図 3-5 に、新しい仮想デバイス（vt1）を含む設定を示します。

図 3-5　　仮想デバイスの作成



MDS NX-OS Release 4.1（1a）以降では、仮想デバイスの failover 属性を設定する場合に次の条件を考慮する必要があります。

- 属性の設定は、MDS NX-OS Release 4.1（1a）以降でだけサポートされています。以前のリリースが組み合わされている混合モードのファブリックでは、属性の設定は失敗します。
- failover 属性が設定されている場合に、プライマリ デバイスがオフラインであるとき、セカンダリ デバイスがアクティブになります。
- プライマリ デバイスがセカンダリ デバイスにフェールオーバーした後に failover 属性が削除されたとき、プライマリ デバイスがオンラインになっていればプライマリ デバイスがアクティブになります。プライマリ デバイスがオンラインになっていないと、SDV 仮想デバイスはシャットダウンします。

（注） SDV 属性の設定は、MDS Fabric Manager Release 4.1（2）以降でサポートされています。

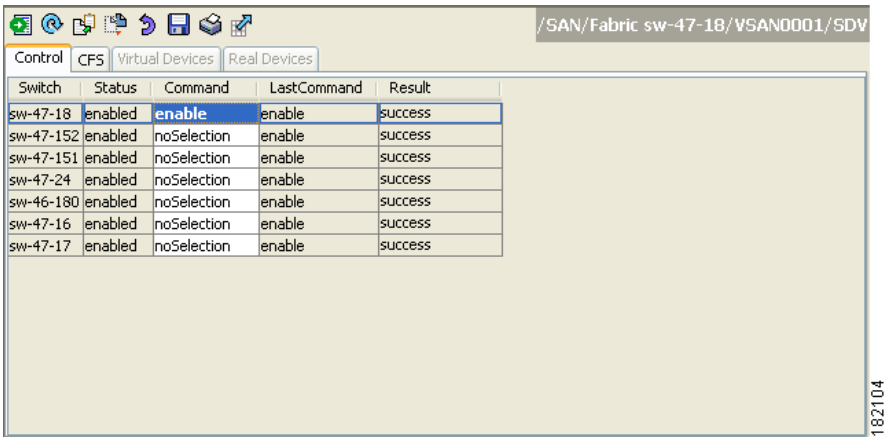
Fabric Manager を使用して仮想ターゲットを設定し、仮想ターゲットをファブリック設定にコミットする手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで SAN を展開します。次に、VSAN が存在しているファブリックを展開します。

ステップ 2　仮想ターゲットを作成する VSAN を展開し、[SDV] を選択します。[Information] ペインに、選択した VSAN 内のスイッチの一覧が表示されます。

ステップ 3　[Control] タブで、[Command] 列のドロップダウン メニューから [enable] を選択して、VSAN 内の特定のスイッチの SDV をイネーブルにします（図 3-6 を参照）。

図 3-6　SDV のイネーブル化



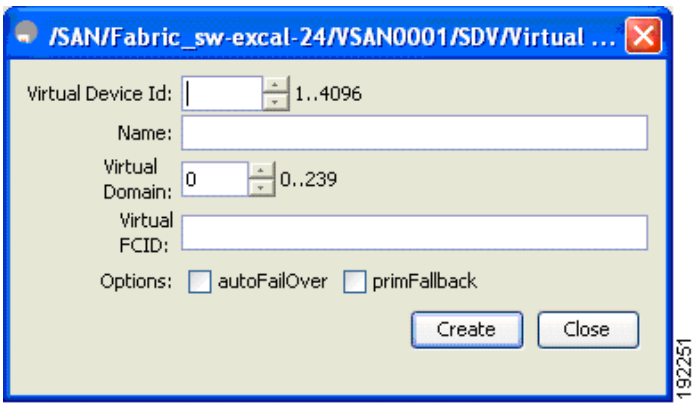
ステップ 4　[Apply Changes] アイコンをクリックして、設定変更をコミットします。

ステップ 5　[CFS] タブをクリックします。該当するスイッチの SDV 機能がイネーブルになっていることを確認します。

ステップ 6　[Virtual Devices] タブをクリックし、[Create Row] アイコンをクリックします。

[Create Virtual Devices] ダイアログボックスが表示されます（図 3-7 を参照）。

図 3-7　[Create Virtual Devices] ダイアログボックス

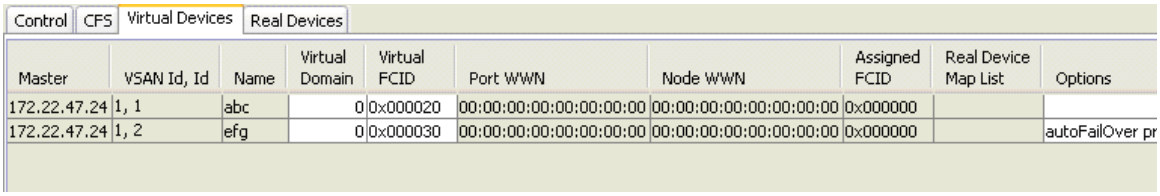


ステップ 7　[Virtual Device ID] ドロップダウン リストから 1 ～ 4096 の範囲内の ID を選択します。

ステップ 8　仮想デバイスの名前を入力します。仮想ドメインを選択し、[Virtual FC ID] に仮想ターゲットの仮想 FC ID を入力します。

ステップ 9　[autoFailover] チェックボックスだけをオンにするか、または [autoFailover] チェックボックスと [primFallback] チェックボックスをオンにします。詳細については、「自動フェールオーバーおよびフォールバック」（P.3-4）を参照してください。[Virtual Devices] タブの [Option] 列でオプションを変更することもできます。（図 3-8 を参照）。

図 3-8　[Virtual Devices] タブ



ステップ 10　[Create] をクリックして仮想ターゲットを作成します。

ステップ 11　[CFS] アイコンをクリックして、設定変更をコミットして配信します。

仮想ターゲットの pWWN は、Fabric Manager のゾーン分割エンド デバイスのデータベースには表示されません。pWWN で仮想デバイスのゾーン分割を行う場合は、ゾーンを作成するときにこれを [Add Member to Zone] ダイアログボックスに入力する必要があります。ただし、デバイス エイリアスが拡張モードの場合、仮想デバイス名は Fabric Manager の [Zoning] ウィンドウの [Device Alias Database] に表示されます。この場合、デバイス エイリアス名を選択するか、[Add Member to Zone] ダイアログボックスで pWWN を入力することができます。

詳細については、「ゾーン メンバーの追加」（P.5-14）を参照してください。

SDV を使用する場合はデバイス エイリアス モードを拡張に設定します（仮想デバイスの pWWN は変更される可能性があるため）。

たとえば、SDV がスイッチ上でイネーブルになり、仮想デバイスが定義されます。SDV は仮想デバイスの pWWN を割り当て、ゾーン内の pWWN に基づいてゾーン分割されます。後で SDV をディセーブルにした場合、この設定は失われます。SDV を再度イネーブルにし、同じ名前を使用して仮想デバイスを作成する場合、同じ pWWN が再び取得される保証はありません。pWWN ベースのゾーンを再びゾーン分割することが必要になる場合があります。ただし、デバイス/エイリアス名に基づくゾーン分割を実行する場合は、pWWN の変更時に設定変更は必要ありません。

デバイス エイリアス モードをイネーブルにする前に、デバイス エイリアス モードがどのように動作するのかを確認してください。デバイス エイリアス モードの詳細と要件については、第 6 章「デバイス エイリアス データベースの配信」を参照してください。

仮想デバイスと物理デバイスのリンク

仮想デバイスを作成し、ゾーンの一部として設定したら、**link** コマンドを使用して、仮想デバイスのプライマリ デバイスを定義できます。link コマンドはセカンダリ デバイスへのフェール オーバーにも使用できます。

（注）　リンク動作がセカンダリ デバイスにフェール オーバーすると、仮想デバイスはオフラインになった後で、オンラインになります。

MDS NX-OS Release 4.1（1a）以降では、デバイスをリンクする前に次の条件について考慮する必要があります。

- フェールオーバーのために現在アクティブになっているセカンダリ デバイスにリンクする場合、プライマリ タグがセカンダリ デバイスに移動され、セカンダリ デバイスがプライマリ デバイスになります。
- セカンダリ デバイスがアクティブであるときに、3 番目のデバイスにリンクし、フォールバック属性が設定されていない場合、3 番目のデバイスがプライマリ デバイスになりますが、セカンダリ デバイスはアクティブ デバイスのままになります。
- セカンダリ デバイスがアクティブであるときに、3 番目のデバイスにリンクし、フォールバック属性が設定されている場合、3 番目のデバイスがプライマリ デバイスにもアクティブ デバイスにもなります。

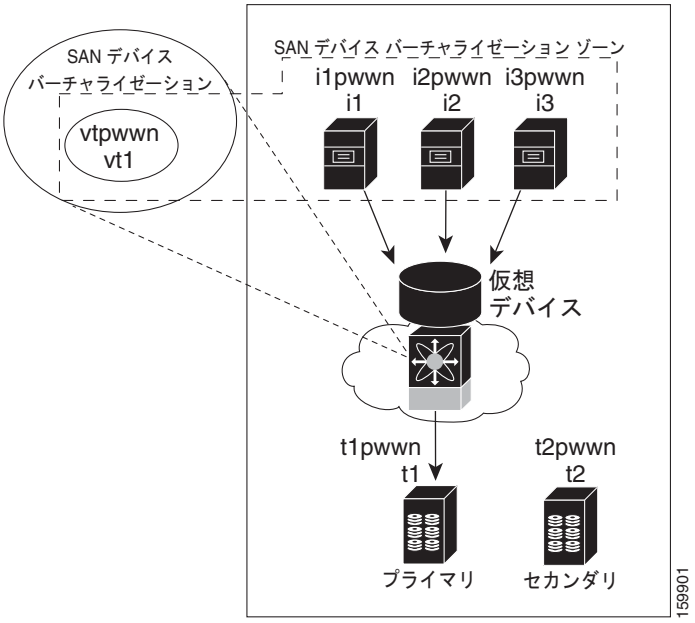
Fabric Manager を使用して仮想ターゲットを物理ターゲットとリンクする手順は、次のとおりです。

ステップ 1　[Real Devices] タブをクリックし、[Create Row] アイコンをクリックします。

ステップ 2　[Virtual Device ID] プルダウン リストで選択を行うか、または物理ターゲットとリンクしている仮想ターゲットの既存の ID を入力します（図 3-9 を参照）。

ステップ 3　[Real Device ID] で、仮想ターゲットとリンクしている物理ターゲットの ID を選択します。

図 3-9　[Create Real Devices] ダイアログボックス



ステップ 4　[pWWN] または [deviceAlias] のいずれかのオプション ボタンを選択し、プルダウン メニューから適切な pWWN またはデバイス エイリアスを選択します。pWWN またはデバイス エイリアスを選択したときに、[Name] フィールドに自動的に値が入力されます。

ステップ 5　[Map Type] の [primary] または [secondary] のいずれかのオプション ボタンを選択します。

ステップ 6　[CFS] アイコンをクリックして保存し、これらの変更を配信するか、または [Close] をクリックして保存していない変更を破棄します。

ファブリック マージの矛盾の解決

2 つのファブリックをマージするときは常に、SDV ではそのデータベースをマージします。ランタイム情報の矛盾や設定の不一致がある場合には、マージの矛盾が生じることがあります。次の場合にランタイムの矛盾が生じることがあります。

- 同じ pWWNs が異なる仮想デバイスに割り当てられている。
- 同じ仮想デバイスが異なる pWWNs に割り当てられている。
- 仮想デバイスと仮想 FC ID が一致しない。

*ブランク コミット*は、設定変更を含まず、コミットするスイッチ ファブリック全体の SDV 設定を適用するコミット動作です。ブランク コミット動作は、コミットするスイッチからファブリック全体に設定をプッシュすることにより、矛盾する仮想デバイスを再初期化して、マージの矛盾を解決します。この動作の実行中には、一部の仮想デバイスがオフラインになりやすいため、注意が必要です。

pWWN の矛盾から生じるマージ障害によって、デバイス エイリアスでも障害が発生することがあります。SDV 内のマージに失敗した VSAN でのブランク コミット動作により、デバイス エイリアスのマージ障害を解決する必要があります。

次のことを確実にすることにより、設定の不一致によって生じるマージの矛盾を回避できます。

- 仮想デバイスの pWWN およびデバイス エイリアス エントリが（プライマリとセカンダリで）同一である。
- ファブリック内の VSAN にわたって仮想デバイス名の矛盾がない。

SDV の要件と注意事項

SDV の計画および設定を行う際には、次の要件と注意事項について考慮してください。

- SDV ゾーンの一部になっているデバイスが接続されているスイッチ上で、SDV をイネーブルにする必要があります。
- SDV は、MDS 以外のスイッチに接続されているデバイスでは機能しません。
- ブロードキャスト ゾーン分割は、仮想デバイスのあるゾーンではサポートされていません。
- IVR および SDV は、同じデバイスでは使用できません。SDV 仮想化デバイスを IVR ゾーンまたはゾーンセットの一部にはできません。
- 仮想デバイス名は、すべての VSAN にわたって一意である必要があります。この理由は、仮想デバイス名は VSAN を認識しないデバイス エイリアス サーバで登録されるためです。たとえば、SDV をイネーブルにし、VSAN 1 と VSAN 2 の両方で vt1 という名前を登録した場合、これらの名前が同一であるため、デバイス エイリアス サーバではいずれのエントリも格納できません。
- 異なる仮想デバイスに対して同じプライマリ デバイスを指定できません。
- SDV は、ソフト ゾーン分割では機能しません（*ソフト ゾーン分割*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ることを意味します。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 FC ID を認識できる場合、そのデバイスにアクセスできます）。また、SDV は **zone default-zone permit vsan** 動作でも機能しません（SDV 以外の場合、この動作はデフォルト ゾーン内のメンバーにトラフィックを許可するか、拒否します）。

- デバイスが発信側によってまだゾーン分割されていない場合、否定的な影響を与えることなく、SDV 仮想デバイス ゾーンを設定できます。デバイスが既にゾーン分割されている場合、ゾーン分割の変更が必要になります。
- 実デバイス / 仮想デバイス ゾーンは、実デバイス / 実デバイス ゾーンとは共存できません。各実デバイスがともにまだゾーン分割されていない場合、否定的な影響を与えることなく、実デバイス / 仮想デバイス ゾーンを設定できます。これらのデバイスがすでにゾーン分割されている場合、実デバイス / 仮想デバイス ゾーンを追加すると、ゾーンのアクティブ化に失敗する可能性があります。この場合、アクティブ化する前に、ゾーンの 1 つを削除する必要があります。

  たとえば、ユーザが I という発信側と T というターゲット（I、T）で構成されるゾーン A、および VI という仮想発信側と T という実ターゲット（ゾーン VI、T）で構成されるゾーン B を使用して設定を作成しようとします。このような設定は失敗します。同様に、発信側 I とターゲット T で構成されるゾーン C を、発信側 I と仮想ターゲット VT（ゾーン I、VT）で構成されるゾーン D とともに設定しようとしても失敗します。

注意　サーバと仮想化されるデバイスとの間に、少なくとも 1 つの Cisco MDS 9124 スイッチ*以外の* SDV 対応のスイッチが必要です。発信側とプライマリ デバイスが同じ Cisco MDS 9124 スイッチに接続されている場合、SDV は機能しません。

デフォルト設定

表 3-1 に、SDV パラメータのデフォルト設定を示します。

表 3-1　デフォルトの SDV 設定パラメータ

パラメータ	デフォルト
イネーブル	ディセーブル

CHAPTER 4

ダイナミック VSAN の作成

スイッチのポート VSAN メンバ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。

VSAN をデバイス WWN に基づいて割り当てることにより、VSAN メンバシップをポートに動的に割り当てることができます。この方法は Dynamic Port VSAN Membership（DPVM）機能といいます。DPVM により、柔軟性が高まり、ホストまたはストレージ デバイスの接続が 2 つの Cisco MDS スイッチ間またはスイッチ内の 2 つのポート間で移動される場合に、ファブリック トポロジを維持するためにポート VSAN メンバシップを再設定する必要がなくなります。デバイスが接続されるか、移動されるかに関係なく、設定済みの VSAN が保持されます。VSAN を静的に割り当てるには、第 2 章「VSAN の設定と管理」を参照してください。

この章の内容は、次のとおりです。

DPVM

DPVM 設定は、Port World Wide Name（pWWN）および Node World Wide Name（nWWN）の割り当てに基づきます。DPVM データベースには、各デバイスの pWWN/nWWN 割り当ておよび対応する VSAN のマッピング情報が含まれます。Cisco NX-OS ソフトウェアは、デバイス FLOGI 中にデータベースをチェックし、必要な VSAN の詳細を取得します。

pWWN はホストまたはデバイスを識別し、nWWN は複数のデバイスで構成されるノードを識別します。これらの ID のいずれかを割り当てるか、またはこれらの ID の組み合わせを割り当てて、DPVM をマッピングを設定できます。組み合わせて割り当てると、pWWN が優先されます。

DPVM は、Cisco Fabric Services（CFS）インフラストラクチャを使用して、データベースを効率的に管理および配信できるようにします。DPVM では、アプリケーション駆動の調整済み配信モードが使用され、配信範囲はファブリック全体に及びます（CFS の詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください）。

（注） DPVM はデバイス アドレス指定への変更を引き起こしません。DPVM はデバイスの VSAN メンバシップだけに関連し、スイッチ上のいずれのポートでもホストが同じ VSAN メンバシップを確実に取得するようにします。たとえば、スイッチ上のポートでハードウェア障害が発生した場合は、ホスト接続をスイッチ上の別のポートに移動でき、VSAN メンバシップを手動で更新する必要はありません。

（注）　DPVM は FL ポートではサポートされません。DPVM がサポートされるのは F ポートだけです。

ここでは DPVM について、次の内容を説明します。

DPVM 設定の概要

DPVM 機能を設計どおりに使用するには、必ず次の要件が満たされていることを確認してください。

- ダイナミック デバイスが Cisco MDS 9000 ファミリ スイッチに接続するインターフェイスは、F ポートとして設定される必要があります。
- F ポートのスタティック ポート VSAN が有効になっている（分離されたり一時停止されたりしておらず、存在している）必要があります。
- DPVM データベースのデバイスに対して設定されているダイナミック VSAN が有効になっている（分離されたり一時停止されたりしておらず、存在している）必要があります。

（注）　DPVM 機能は、既存のスタティック ポート VSAN メンバシップ設定を上書きします。ダイナミック ポートに対応する VSAN が削除または一時停止されると、ポートはシャットダウンされます。

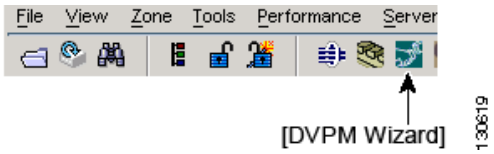
DPVM の設定を始めるには、ファブリック内の必要なスイッチで DPVM を明示的にイネーブルにする必要があります。デフォルトでは、この機能は Cisco MDS 9000 ファミリのすべてのスイッチでディセーブルになっています。

DPVM ウィザードを使用した DPVM の設定

Fabric Manager で DPVM Setup ウィザードを使用してダイナミック ポート VSAN メンバシップを設定する手順は、次のとおりです。

ステップ 1　Fabric Manager ツールバーで [DPVM Setup Wizard] アイコンをクリックします（図 4-1 を参照）。

図 4-1　[DPVM Wizard] アイコン



[Select Master Switch] ページが表示されます。

ステップ 2　マスター スイッチにするスイッチをクリックします。このスイッチは、ファブリック内の他のスイッチへの、DPVM データベースの配信を制御します。

ステップ 3　[Next] をクリックします。

[AutoLearn Current End Devices] ページが表示されます。

ステップ 4　（任意）自動学習を有効にする場合は、[Create Configuration From Currently Logged In End Devices] チェックボックスをオンにします。

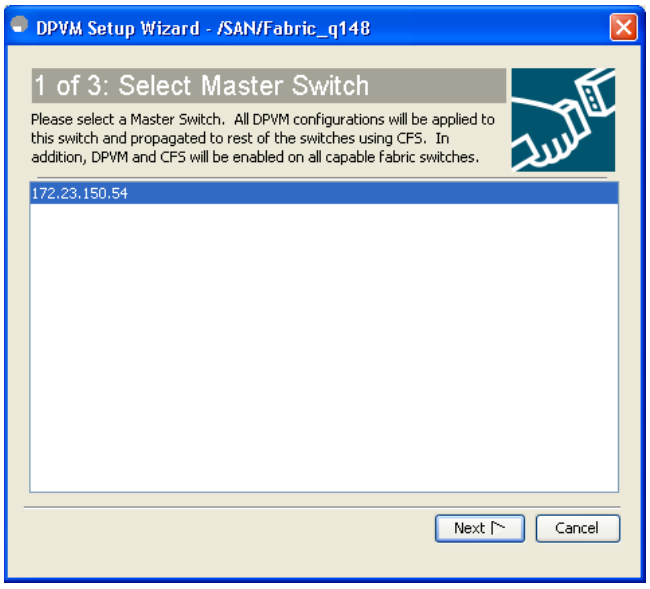
ステップ 5　[Next] をクリックします。

[Edit and Activate Configuration] ページが表示されます。

ステップ 6　現在の設定または自動学習された設定を確認します。（任意）[Insert] をクリックして、DPVM コンフィギュレーション データベースにエントリを追加します。

ステップ 7　DPVM コンフィギュレーション データベースを更新し、CFS を使用して変更を配信し、データベースをアクティブにするには [Finish] をクリックします。または、変更を保存せずに DPVM Setup ウィザードを終了するには [Cancel] をクリックします。

図 4-2　DPVM Setup ウィザード: Select Master Switch

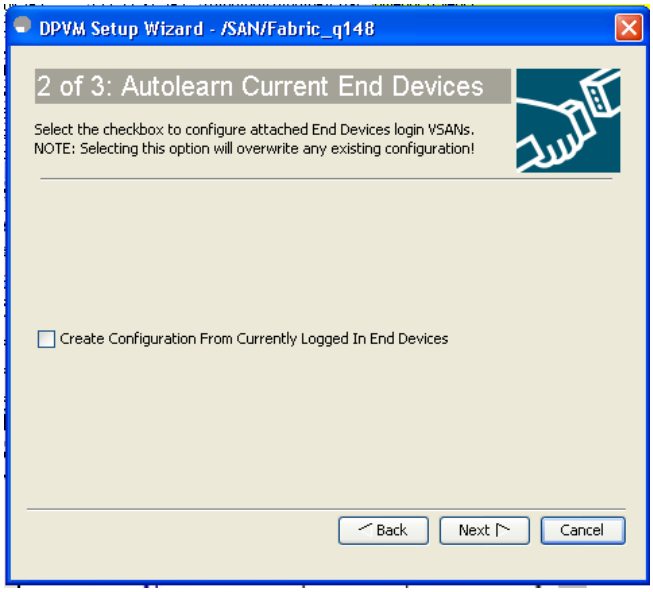


ステップ 8　マスター スイッチにするスイッチを選択します。このスイッチは、ファブリック内の他のスイッチへの、DPVM データベースの配信を制御します。

ステップ 9　[Next] をクリックします。

AutoLearn Current End Devices ページが表示されます（図 4-3 を参照）。

図 4-3　DPVM Setup ウィザード：AutoLearn Current End Devices

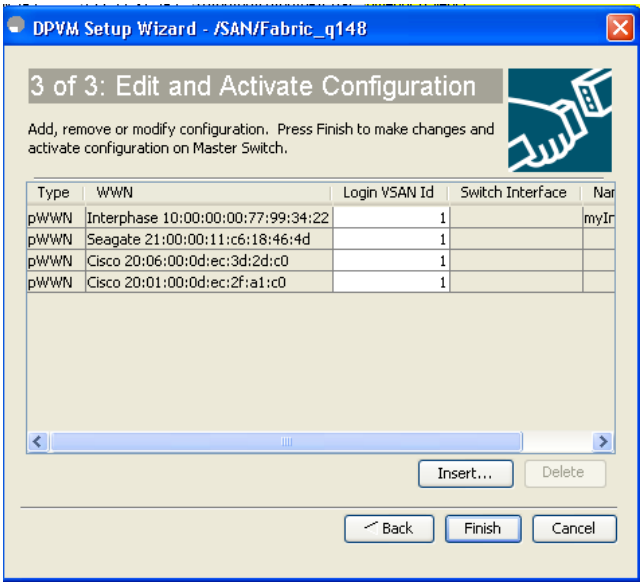


ステップ 10　（任意）自動学習をイネーブルにする場合は、[Create Configuration From Currently Logged In End Devices] チェックボックスをオンにします。

ステップ 11　[Next] をクリックします。

[Edit and Activate Configuration] ページが表示されます（図 4-4 を参照）。

図 4-4　DPVM Setup ウィザード：Edit and Activate Configuration



ステップ 12　現在の設定または自動学習された設定を確認します。（任意）[Insert] をクリックして、DPVM コンフィギュレーション データベースにエントリを追加します。

ステップ 13　DPVM コンフィギュレーション データベースを更新し、CFS を使用して変更を配信し、データベースをアクティブにするには [Finish] をクリックします。または、変更を保存せずに DPVM Setup ウィザードを終了するには [Cancel] をクリックします。

DPVM データベースの概要

DPVM データベースは、一連のデバイス マッピング エントリで構成されます。各エントリは、デバイス pWWN または nWWN 割り当て、および割り当てられるダイナミック VSAN で構成されます。最大 16,000 の DPVM エントリを DPVM データベース内で設定できます。このデータベースは、スイッチ全体（およびファブリック）に対してグローバルであり、VSAN ごとには保持されません。

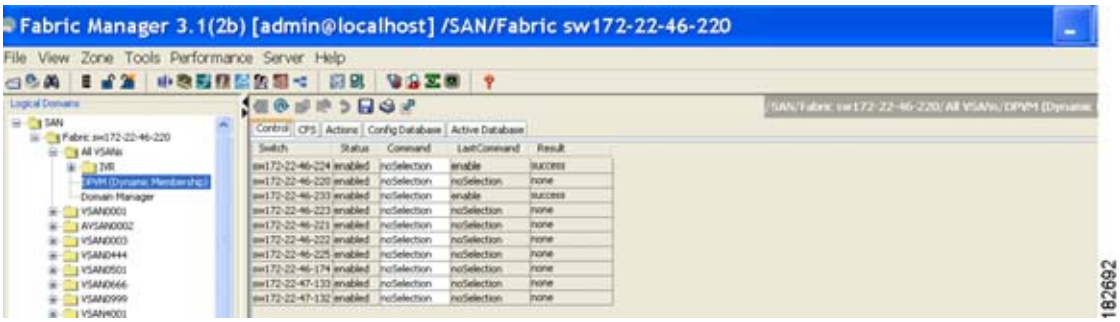
DPVM 機能は、これらのデータベースを使用して、設定を受け入れ、実装します。

- コンフィギュレーション（config）データベース：配信がディセーブルになっている場合、設定の変更はすべてコンフィギュレーション データベースに格納されます。
- アクティブ データベース：ファブリックで現在実行されているデータベースです。
- 保留データベース：配信がイネーブルになっている場合、設定の変更はすべて DPVM 保留データベースに格納されます（「DPVM データベース配信」（P.4-11）を参照）。

DPVM コンフィギュレーション データベースの変更は、DPVM コンフィギュレーション データベースをアクティブにするまでは、アクティブ DPVM データベースに反映されません。DPVM 保留データベースの変更は、DPVM 保留データベースをコミットするまでは、コンフィギュレーション データベースまたはアクティブ DPVM データベースに反映されません。このデータベース構造により、複数のエントリを作成し、変更を確認し、DPVM コンフィギュレーション データベースおよび保留データベースを有効にすることができます。

図 4-5 に、Fabric Manager の [Information] ペインの DPVM データベースの例を示します。

図 4-5　Fabric Manager での DPVM 設定



DPVM コンフィギュレーション データベースおよび保留データベースの設定

Fabric Manager を使用してコンフィギュレーション データベースと保留データベースの作成および入力を行う手順は、次のとおりです。

ステップ 1　[Fabricxx] > [All VSANs] を展開し、[Logical Attributes] ペインで [DPVM] を選択します。

[Information] ペインに DPVM 設定が表示されます。

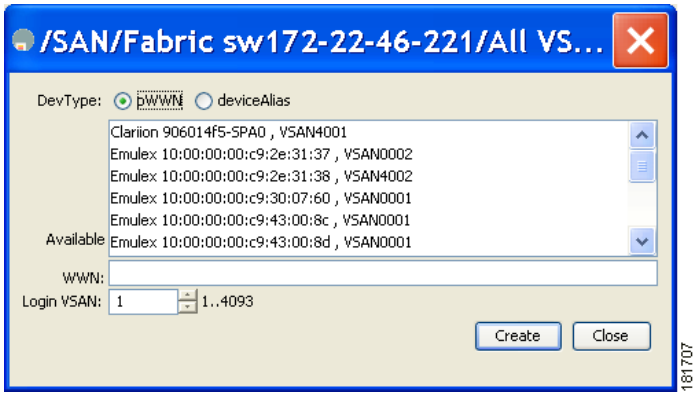
ステップ 2　[CFS] タブをクリックし、[Master] 列のチェックボックスをオンにしてマスター スイッチを選択します。

（注）　その他のタブをアクティブにするには、CFS タブをクリックする必要があります。

ステップ 3　[Config Database] タブをクリックし、[Create Row] をクリックして、新しいエントリを挿入します。

[Create Config Database] ダイアログボックスが表示されます（図 4-6 を参照）。

図 4-6　コンフィギュレーション データベースの作成



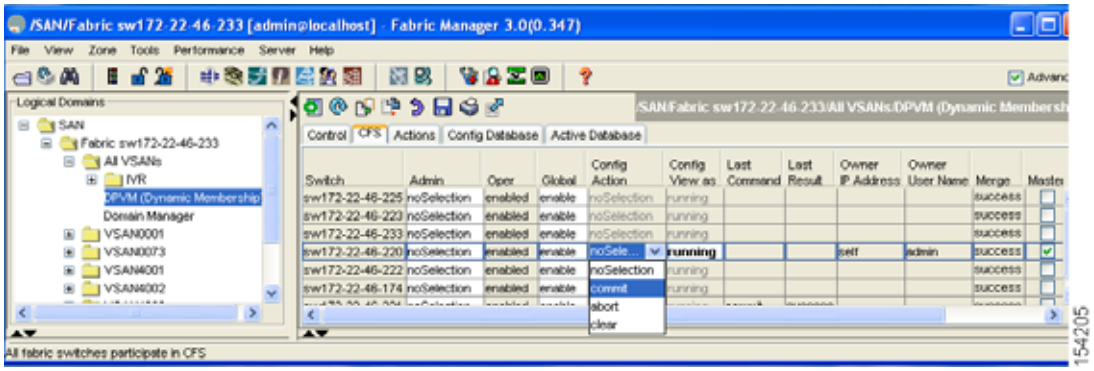
ステップ 4　使用可能な WWN と VSAN の組み合わせを選択するか、または [pWWN] フィールドと [Login VSAN] フィールドに値を入力します。

ステップ 5　[Create] をクリックしてこれらの変更をコンフィギュレーション データベースまたは保留データベースに保存するか、または [Close] をクリックして保存されていない変更を破棄します。

ステップ 6　[CFS] タブをクリックし、マスター データベースの [Config Action] ドロップダウン メニューを選択します。

オプションが表示されます（図 4-7 を参照）。

図 4-7　[Config Action] ドロップダウン メニュー



ステップ 7　ドロップダウン メニューから [commit] を選択してこれらの変更を配信するか、または [abort] を選択して変更を破棄します。

DPVM コンフィギュレーション データベースのアクティブ化

DPVM コンフィギュレーション データベースを明示的にアクティブにすると、DPVM コンフィギュレーション データベースはアクティブ DPVM データベースになります。DPVM コンフィギュレーション データベースと現在のアクティブ DPVM データベースの間で矛盾するエントリが見つかった場合、アクティブ化は失敗することがあります。ただし、アクティブ化を強制的に実行して、矛盾するエントリを上書きできます。

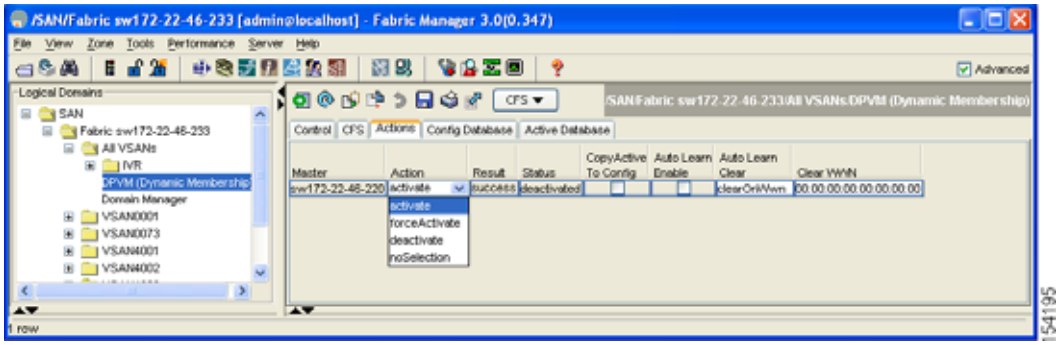
Fabric Manager を使用して DPVM コンフィギュレーション データベースをアクティブにする手順は、次のとおりです。

ステップ 1　[Fabricxx] > [All VSANs] を展開し、[Logical Attributes] ペインで [DPVM] を選択します。

[Information] ペインに DPVM 設定が表示されます。

ステップ 2　[Action] タブをクリックし、Action ドロップダウン メニューを [activate] または [forceActivate] に設定して、DPVM コンフィギュレーション データベースをアクティブにします（図 4-8 を参照）。

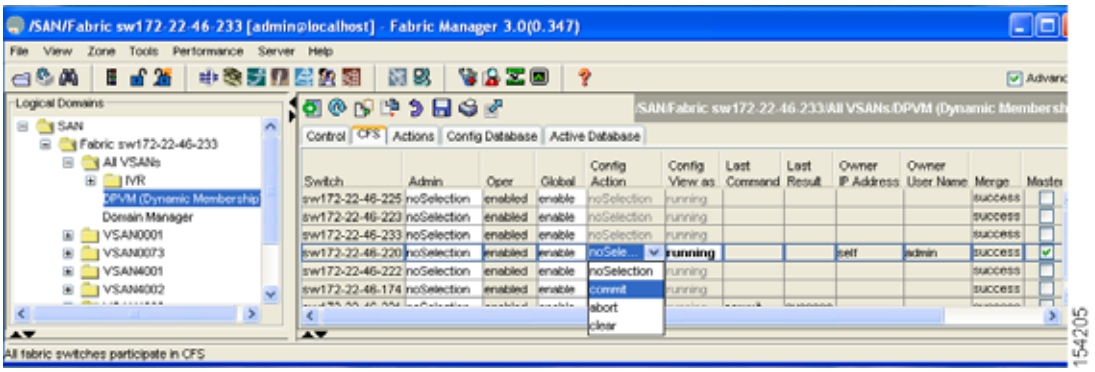
図 4-8　設定済みデータベースのアクティブ化



ステップ 3　[CFS] タブをクリックし、マスター データベースの [Config Action] ドロップダウン メニューを選択します。

オプションが表示されます（図 4-9 を参照）。

図 4-9　[Config Action] ドロップダウン メニュー



ステップ 4　ドロップダウン メニューから [commit] を選択してこれらの変更を配信するか、または [abort] を選択して変更を破棄します。

（注）　DPVM をディセーブルにするには、現在のアクティブ DPVM データベースを明示的に非アクティブにする必要があります。

保留データベースの表示

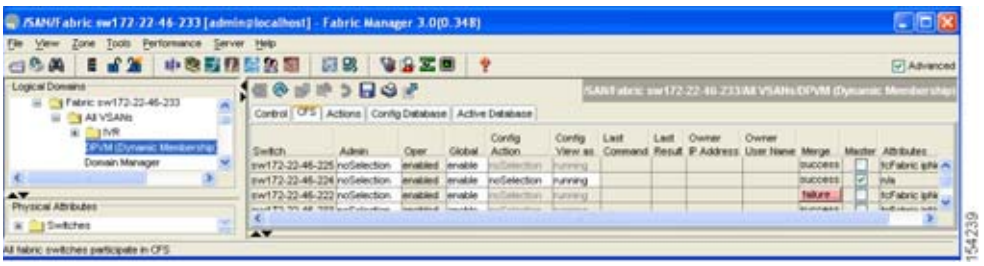
Fabric Manager を使用して保留データベースを表示する手順は、次のとおりです。

ステップ 1　[Fabricxx] > [All VSANs] を展開し、[Logical Attributes] ペインで [DPVM] を選択します。

[Information] ペインに DPVM 設定が表示されます。

ステップ 2　[CFS] タブをクリックし、[Config View] ドロップダウン メニューを [pending] に設定します（図 4-10 を参照）。

図 4-10　マスター スイッチがオンに設定されている CFS タブ



ステップ 3　[Apply Changes] をクリックします。

ステップ 4　[Config Database] タブをクリックします。

保留データベース エントリが表示されます。

自動学習エントリの概要

DPVM データベースは、各 VSAN 内の新規デバイスについて自動的に学習（自動学習）するように設定できます。自動学習機能は、いつでもイネーブルまたはディセーブルにすることができます。学習済みエントリは、アクティブ DPVM データベース内でデバイス pWWN および VSAN に入力することによって作成されます。自動学習をイネーブルにするには、アクティブ DPVM データベースが使用可能になっている必要があります。

自動学習をイネーブルにする場合、学習済みエントリをアクティブ DPVM データベースから削除できます。これらのエントリは、自動学習をディセーブルにする場合に限り、アクティブ DPVM データベース内で固定になります。

（注）　自動学習がサポートされるのは F ポートに接続されているデバイスの場合だけです。DPVM は FL ポートではサポートされていないため、FL ポートに接続されているデバイスは DPVM データベースに入力されません。

学習済みエントリには次の条件が適用されます。

- 自動学習がイネーブルになっているときにデバイスがログアウトした場合、そのエントリはアクティブ DPVM データベースから自動的に削除されます。
- 同じデバイスが異なるポートを通じてスイッチに複数回ログインした場合、最後のログインに対応する VSAN が認識されます。
- 学習済みエントリは、以前に設定されてアクティブにされたエントリを上書きしません。
- 学習は、自動学習をイネーブルにした後に自動学習をディセーブルにするという 2 つの部分から成るプロセスです。[auto-learn] オプションがイネーブルになっている場合、次の処理が行われます。
  - 現在ログインされているデバイスの学習：自動学習がイネーブルにされた時点から行われます。
  - 新規デバイスのログインの学習：新規デバイスがスイッチにログインした時点で行われます。

自動学習のイネーブル化

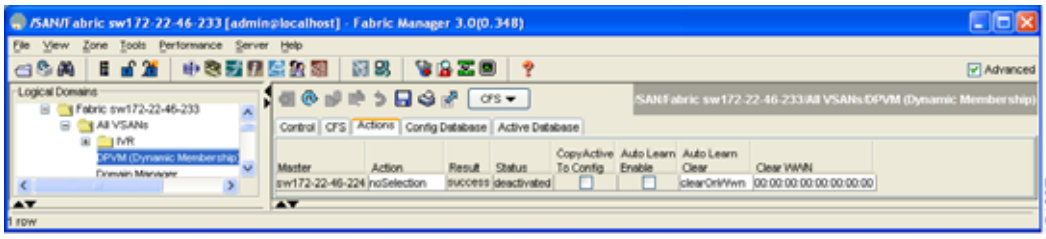
Fabric Manager を使用して自動学習をイネーブルにする手順は、次のとおりです。

ステップ 1　[Fabricxx] > [All VSANs] を展開し、[Logical Attributes] ペインで [DPVM] を選択します。

[Information] ペインに DPVM 設定が表示されます。

ステップ 2　[Actions] タブをクリックし、[Auto Learn Enable] チェックボックスをオンにして自動学習をイネーブルにします（図 4-11 を参照）。

図 4-11　[DPVM Actions] タブ



ステップ 3　[CFS] タブをクリックし、[commit] を選択してこれらの変更を配信するか、または [abort] を選択して変更を破棄します。

学習済みエントリの消去

2 つの方法のいずれかを使用して DPVM エントリをアクティブ DPVM データベースから消去できます（自動学習がイネーブルになっている場合）。

Fabric Manager を使用して 1 つの自動学習エントリを消去する手順は、次のとおりです。

ステップ 1　[Fabricxx] > [All VSANs] を展開し、[Logical Attributes] ペインで [DPVM] を選択します。

[Information] ペインに DPVM 設定が表示されます。

ステップ 2　[Actions] タブをクリックし、[Auto Learn Clear] ドロップダウン メニューで clearOnWWN を選択します。

ステップ 3　消去する自動学習エントリの横にある [clear WWN] チェックボックスをオンにします。

ステップ 4　[CFS] をクリックし、[commit] を選択してこれらの変更を配信するか、または [abort] を選択して変更を破棄します。

Fabric Manager を使用してすべての自動学習エントリを消去する手順は、次のとおりです。

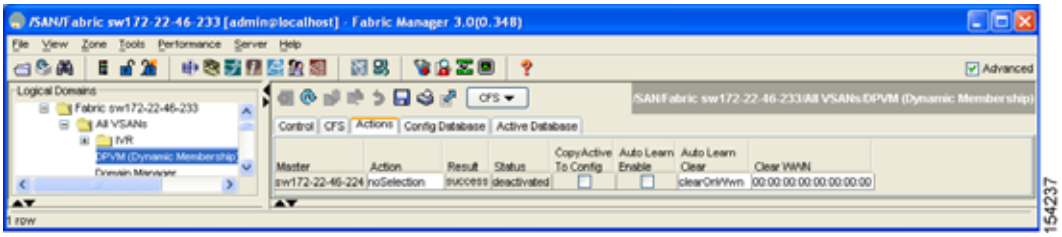
ステップ 1　[Fabricxx] > [All VSANs] を展開し、[Logical Attributes] ペインで [DPVM] を選択します。

[Information] ペインに DPVM 設定が表示されます。

ステップ 2　[Actions] タブをクリックします。

[DPVM Actions] メニューが表示されます（図 4-12 を参照）。

図 4-12　[DPVM Actions] タブ



ステップ 3　[Auto Learn Clear] ドロップダウン メニューから [clear] を選択します。

ステップ 4　[CFS] タブをクリックし、[commit] を選択してこれらの変更を配信するか、または [abort] を選択して変更を破棄します。

（注）　これらの 2 つの手順はセッションを開始せず、ローカル スイッチ内だけで発行できます。

DPVM データベース配信

DPVM データベースをファブリック内のすべてのスイッチで使用できる場合、デバイスはどの場所にでも移動でき、最も高い柔軟性を発揮します。近接スイッチへのデータベース配信をイネーブルにするには、データベースが常に管理され、ファブリック内のすべてのスイッチにわたって配信される必要があります。Cisco NX-OS ソフトウェアは、Cisco Fabric Services（CFS）インフラストラクチャを使用して、この要件を満たします（『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照）。

ここでは DPVM データベースを配信する方法について、次の内容を説明します。

DPVM データベース配信

CFS インフラストラクチャを使用して、各 DPVM サーバは、ISL 起動プロセス中に近接スイッチのそれぞれから DPVM データベースについて学習します。ローカルでデータベースを変更すると、DPVM サーバは近接スイッチに通知し、そのデータベースはファブリック内のすべてのスイッチによって更新されます。

ファブリック配信がイネーブルになっている場合、コンフィギュレーション データベースへのすべての変更は、DPVM 保留データベースに格納されます。これらの変更には次のタスクが含まれます。

- エントリの追加、削除、または変更
- コンフィギュレーション データベースのアクティブ化、非アクティブ化、または削除
- 自動学習のイネーブル化またはディセーブル化

これらの変更は、変更をコミットすると、ファブリック内のすべてのスイッチに配信されます。この時点で変更を破棄（abort）することもできます。

ヒント　保留データベースの内容を表示するには、「保留データベースの表示」（P.4-8）を参照してください。

DPVM データベース配信のディセーブル化

これらの変更は、変更をコミットすると、ファブリック内のすべてのスイッチに配信されます。この時点で変更を破棄（abort）することもできます。

ヒント　保留データベースの内容を表示するには、「保留データベースの表示」（P.4-8）を参照してください。

Fabric Manager を使用して近接スイッチへの DPVM データベース配信をディセーブルにする手順は、次のとおりです。

ステップ 1　[Fabricxx] > [All VSANs] を展開し、[Logical Attributes] ペインで [DPVM] を選択します。

[Information] ペインに DPVM 設定が表示されます。

ステップ 2　[CFS] タブをクリックし、[Admin] ドロップダウン メニューから [disable] を選択します。

ステップ 3　この変更を保存する場合は [Apply Changes] をクリックし、変更を破棄する場合は [Undo Changes] をクリックします。

ファブリックのロックの概要

既存設定の変更を開始すると、DPVM 保留データベースが作成され、ファブリック内の機能がロックされます。ファブリックをロックすると、次の条件が成立します。

- 他のユーザは、この機能の設定を変更できなくなります。
- コンフィギュレーション データベースのコピーが、DPVM 保留データベースになります。これ以降の変更は、DPVM 保留データベースに対して行われます。DPVM 保留データベースへの変更をコミットするか、または破棄（abort）するまでは、DPVM 保留データベースが有効な状態のままになります。

ファブリックのロック

Fabric Manager を使用してファブリックをロックし、変更を DPVM 保留データベースに適用する手順は、次のとおりです。

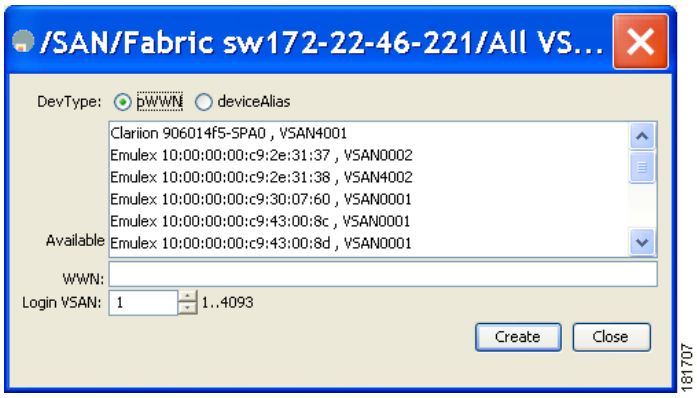
ステップ 1　[Fabricxx] > [All VSANs] を展開し、[Logical Attributes] ペインで [DPVM] を選択します。

[Information] ペインに DPVM 設定が表示されます。

ステップ 2　[Config Database] タブをクリックし、[Create Row] をクリックします。

[Create Config Database] ダイアログボックスが表示されます（図 4-13 を参照）。

図 4-13　コンフィギュレーション データベースの作成



ステップ 3　使用可能な pWWN を選択し、VSAN にログインします。

ステップ 4　この変更を保留データベースに保存する場合は [Create] をクリックし、保存されていない変更を破棄する場合は [Close] をクリックします。

変更のコミット

設定に変更をコミットすると、DPVM 保留データベースの設定が、他のスイッチに配信されます。コミットが正常に実行されると、ファブリック全体に設定の変更が適用され、ロックが解除されます。

Fabric Manager を使用して DPVM 保留データベースをコミットする手順は、次のとおりです。

ステップ 1　[Fabricxx] > [All VSANs] を展開し、[Logical Attributes] ペインで [DPVM] を選択します。

[Information] ペインに DPVM 設定が表示されます。

ステップ 2　[CFS] タブをクリックし、[Config Action] ドロップダウン メニューから [commit] を選択します。

ステップ 3　この変更を保存する場合は [Apply Changes] をクリックし、変更を破棄する場合は [Undo Changes] をクリックします。

変更の破棄

DPVM 保留データベースへの変更を破棄（abort）すると、設定は影響されずにロックが解除されます。

Fabric Manager を使用して DPVM 保留データベースを破棄する手順は、次のとおりです。

ステップ 1　[Fabricxx] > [All VSANs] を展開し、[Logical Attributes] ペインで [DPVM] を選択します。

[Information] ペインに DPVM 設定が表示されます。

ステップ 2　[CFS] タブをクリックし、[Config Action] ドロップダウン メニューから [abort] を選択します。

ステップ 3　この変更を保存する場合は [Apply Changes] をクリックし、変更を破棄する場合は [Undo Changes] をクリックします。

ロック済みセッションのクリア

DPVM タスクを実行し、変更の確定か破棄を行ってロックを解除していない場合、管理者はファブリック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した場合、DPVM 保留データベースへの変更は破棄され、ファブリックのロックが解除されます。

ヒント　DPVM 保留データベースは、一時的なディレクトリだけで使用可能であり、スイッチが再起動されると破棄されることがあります。

管理者権限を使用し、ロックされた DPVM セッションを Fabric Manager を使用して解除する手順は、次のとおりです。

ステップ 1　[Fabricxx] > [All VSANs] を展開し、[Logical Attributes] ペインで [DPVM] を選択します。

[Information] ペインに DPVM 設定が表示されます。

ステップ 2　[CFS] タブをクリックし、[Config Action] ドロップダウン メニューから [clear] を選択します。

ステップ 3　この変更を保存する場合は [Apply Changes] をクリックし、変更を破棄する場合は [Undo Changes] をクリックします。

データベース マージに関する注意事項

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 DPVM データベース内のスタティック（学習されていない）エントリの統合を意味します。CFS マージのサポートの詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。

2 つのファブリック間で DPVM データベースをマージする場合には、次の事項に注意してください。

- 両方のファブリックのアクティブ化および自動学習が同じ状態であることを確認してください。
- それぞれのデータベース内のデバイス エントリの総数が、16 K を超えていないことを確認してください。

注意　これらの 2 つの条件が満たされていない場合、マージは失敗します。次の配信によって、ファブリックのデータベースおよびアクティブ化の状態が強制的に同期化されます。

ここでは、DPVM データベースをマージする方法について説明します。ここで説明する内容は、次のとおりです。

- 「DPVM データベースのコピーの概要」（P.4-15）
- 「DPVM データベースのコピー」（P.4-15）
- 「データベースの差分の比較」（P.4-16）

DPVM データベースのコピーの概要

次の場合には、アクティブ DPVM データベースを DPVM 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が必要になる可能性があります。

- 学習済みエントリがアクティブ DPVM データベースだけに追加された場合
- DPVM コンフィギュレーション データベース、またはDPVM コンフィギュレーション データベースのエントリが誤って削除された場合

（注）　DPVM データベースをコピーし、ファブリック配信がイネーブルになっている場合は、変更をコミットする必要があります。

DPVM データベースのコピー

Fabric Manager を使用して現在のアクティブ DPVM データベースを DPVM コンフィギュレーション データベースにコピーする手順は、次のとおりです。

ステップ 1　[Fabricxx] > [All VSANs] を展開し、[Logical Attributes] ペインで [DPVM] を選択します。
[Information] ペインに DPVM 設定が表示されます。

ステップ 2　[Actions] タブをクリックし、[CopyActive to Config] チェックボックスをオンにします。

ステップ 3　[CFS] タブをクリックし、[Config Action] ドロップダウン メニューから [commit] を選択します。

データベースの差分の比較

Fabric Manager を使用して現在のアクティブ データベース エントリを DPVM コンフィギュレーション データベースと比較する手順は、次のとおりです。

ステップ 1　[Fabricxx] > [All VSANs] を展開し、[Logical Attributes] ペインで [DPVM] を選択します。

[Information] ペインに DPVM 設定が表示されます。

ステップ 2　[Active Database] タブをクリックします。

[Information] ペインに DPVM アクティブ データベースが表示されます。

ステップ 3　Compare With ドロップダウン メニューから [Config] を選択します。

比較ダイアログボックスが表示されます。

ステップ 4　[Close] を選択して比較ダイアログボックスを閉じます。

デフォルト設定

表 4-1 に、DPVM パラメータのデフォルト設定を示します。

表 4-1　デフォルトの DPVM パラメータ

パラメータ	デフォルト
DPVM	ディセーブル
DPVM 配信	イネーブル
自動学習	ディセーブル

CHAPTER 5

ゾーンの設定と管理

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制御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することができます。ゾーン分割は、発信元/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 標準で指定された高度なゾーン分割機能が提供されています。既存の基本ゾーン分割機能を使用したり、高度な標準準拠のゾーン分割機能を使用できます。

この章の内容は、次のとおりです。

（注） 表 2-1（P.2-4）に、ゾーンと VSAN の主な相違点を示します。

ゾーン分割の概要

ゾーン分割には、次の機能があります。

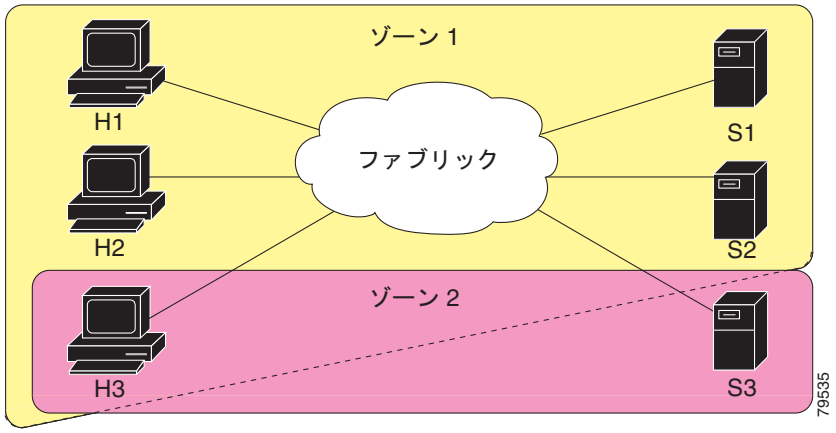
- 1 つのゾーンは、複数のゾーン メンバーから構成されます。
  - ゾーンのメンバー同士はアクセスできますが、異なるゾーンのメンバー同士はアクセスできません。
  - ゾーン分割がアクティブでない場合、すべてのデバイスがデフォルト ゾーンのメンバーとなります。
  - ゾーン分割がアクティブの場合、アクティブ ゾーン（アクティブ ゾーン セットに含まれるゾーン）にないデバイスがデフォルト ゾーンのメンバーとなります。
  - ゾーンのサイズを変更できます。
  - 2 つ以上のゾーンにデバイスが所属することができます。
  - 物理ファブリックには、最大 16,000 のメンバー を設定できます。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。
  - ゾーンを 2 つ以上のゾーン セットのメンバーにすることができます。
  - 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する場合、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 セットが配信されます（この機能が発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 メンバシップ基準は、WWN または FC ID に基づきます。
  - 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（スイッチ ポートの WWN）の WWN を指定します。このメンバシップは、ポートベース ゾーン分割ともいいます。
  - 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。このメンバシップは、インターフェイスベース ゾーン分割ともいいます。
  - 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：MDS ドメインのドメイン ID を指定し、他社製スイッチに属するポートを追加指定します。

  - IPv4 アドレス：接続されたデバイスの IPv4 アドレス（およびオプションでサブネット マスク）を指定します。
  - IPv6 アドレス：接続された複数のデバイスをコロンで区切った 16 進表記の 128 ビットの IPv6 アドレス。
- デフォルト ゾーン メンバシップには、特定のメンバ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、さらにスイッチ上のすべての VSAN 合計で最大 8000 までのゾーンを設定できます。

ゾーン分割の例

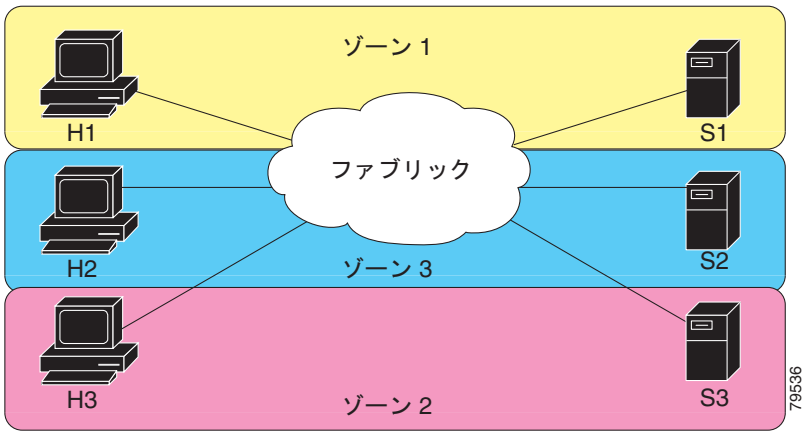
図 5-1 に、ファブリックの 2 つのゾーン（ゾーン 1 およびゾーン 2）で構成されるゾーン セットを示します。ゾーン 1 は、3 つすべてのホスト（H1、H2、H3）からストレージ システム S1 と S2 に常駐するデータへのアクセスを提供します。ゾーン 2 は、S3 のデータを H3 からのアクセスだけに限定します。H3 は両方のゾーンに存在することに注意してください。

図 5-1　　2 つのゾーンを持つファブリック



もちろん、このファブリックをゾーンに分割する方法は他にもあります。図 5-2 に、その他の方法を示します。新しいソフトウェアをテストする目的で、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 5-2　3 つのゾーンを持つファブリック



ゾーン実装

Cisco MDS 9000 ファミリのすべてのスイッチは、以下の基本ゾーン機能を自動的にサポートします（追加の設定は不要です）。

- ゾーンが VSAN（仮想 SAN）に含まれます。
- ハード ゾーン分割は、ディセーブルにできません。
- ネーム サーバ クエリがソフト ゾーン分割されます。
- アクティブ ゾーン セットだけが配信されます。
- ゾーンが分割できないデバイスは、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 は、フル データベースとアクティブ データベースを持ちます。
- 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、スイッチを再起動しても維持されます。
- フル データベースへの変更は、明示的に保存する必要があります。
- ゾーンの再アクティブ化（ゾーン セットがアクティブの状態で、別のゾーン セットをアクティブ化する場合）は、既存のトラフィックに干渉しません。

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。
- ゾーンに属さないメンバーのデフォルト ポリシーを変更します。
- VSAN を interop モードに設定して、他のベンダーと相互運用します。相互に干渉することなく、同じスイッチ内の 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 ポートの分離を解除します。

ゾーン メンバー設定に関する注意事項

ゾーンのすべてのメンバーは互いに通信できます。メンバー数が *N* のゾーンの場合、*N**(*N*-1) のアクセス権限をイネーブルにする必要があります。単一ゾーン内にターゲットまたは発信元を多数設定しないことを推奨します。多数設定してしまうと、実際には互いに通信することのない通信ペア（発信側と発信側間、ターゲットとターゲット間）の多くがプロビジョニング / 管理の対象となるため、スイッチ リソースの浪費になります。この理由から、1 つの発信側に対して 1 つのターゲットを設定するのが最も効率的なゾーン分割方法といえます。

ゾーン メンバーを作成するときは、以下の注意事項について検討する必要があります。

- ゾーンに対して 1 つの発信側と 1 つのターゲットだけ設定すると、スイッチ リソースの使用率が最も効率的になります。
- 複数のターゲットに同じ発信側を設定することは許容されます。
- 複数のターゲットに複数の発信側を設定することは推奨されません。

アクティブおよびフル ゾーン セットに関する考慮事項

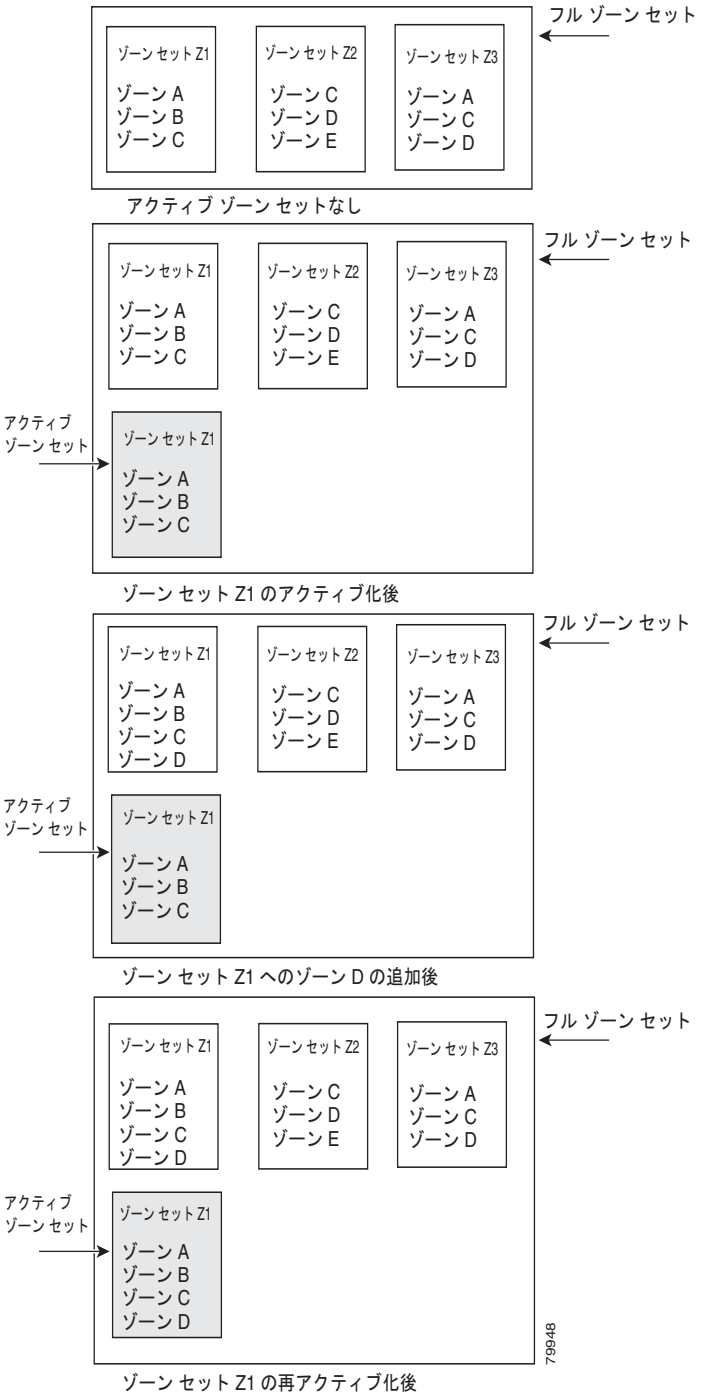
ゾーン セットを設定する前に、次の注意事項について検討してください。

- 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る場合も、フル ゾーン セットを変更することができます。ただし、再起動するまで変更は反映されません。
- 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がアクティブ 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の際に行われます。
- 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、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。

図 5-3 に、アクティブ化されたゾーン セットに追加されるゾーンを示します。

図 5-3　アクティブおよびフル ゾーン セット



Quick Config ウィザードの使用

（注）　Quick Config ウィザードは、スイッチ インターフェイス ゾーン メンバーだけをサポートします。

Cisco SAN-OS Release 3.1(1) および NX-OS Release 4.1(2) 以降では、Cisco MDS 9124 スイッチの Quick Config ウィザードを使用して VSAN ごとにゾーン メンバーの追加または削除を行えます。Quick Config ウィザードを使用してインターフェイスベースのゾーン分割を実行し、Device Manager を使用して複数の VSAN にゾーン メンバーを割り当てることができます。

（注）　Quick Config ウィザードは、Cisco MDS 9124 Fabric Switch、Cisco MDS 9134 Fabric Switch、Cisco Fabric Switch for HP c-Class BladeSystem、および Cisco Fabric Switch for IBM BladeCenter でサポートされます。

注意　Quick Config ウィザードは、スイッチで既存のゾーン分割が定義されていないスタンドアロン スイッチでだけ使用できます。

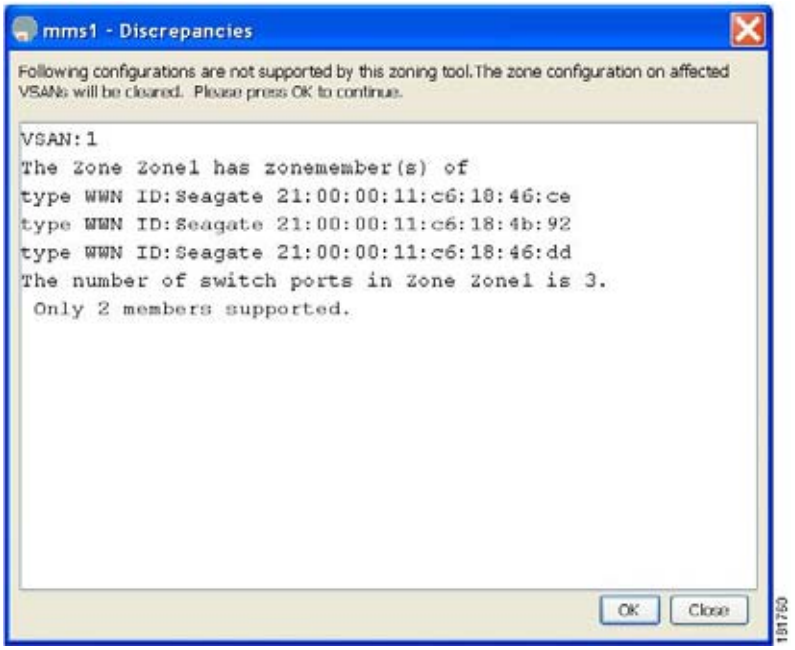
Cisco MDS 9124 スイッチで Device Manager を使用して、ゾーンにポートを追加またはゾーンからポートを削除し、特定の VSAN 内のデバイスだけをゾーン分割する手順は、次のとおりです。

ステップ 1　[FC] > [Quick Config] を選択するか、ツールバーの Zone アイコンをクリックします。

すべてのコントロールがディセーブルになっている Quick Config ウィザード（図 5-5 を参照）およびすべてのサポートされていない設定を表示する [Discrepancies] ダイアログボックス（図 5-4 を参照）が表示されます。

（注）　[Discrepancies] ダイアログボックスは、矛盾がある場合だけ表示されます。

図 5-4　[Discrepancies] ダイアログボックス

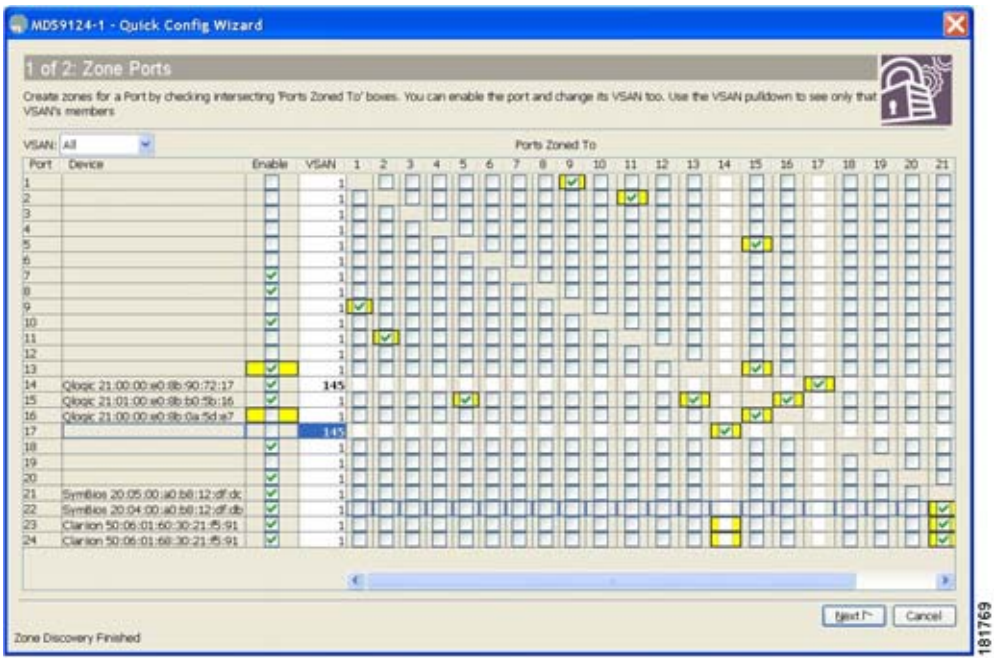


ステップ 2　[OK] をクリックして続行します。

図 5-5 に示す [Quick Config Wizard] ダイアログボックスが表示されます。

注意　矛盾がある場合、[OK] をクリックすると、ゾーン データベース内の VSAN のうち、影響を受けた VSAN がクリアされます。このため、スイッチが使用中の間、中断が生じることがあります。

図 5-5　Quick Config ウィザード



ステップ 3　ゾーンに追加する、またはゾーンから削除するポートの [Ports Zoned To] 列のチェックボックスをオンにします。一致するポートのチェックボックスが同様に設定されます。選択されたポート ペアがゾーンに追加またはゾーンから削除され、2 デバイス ゾーンが作成されます。

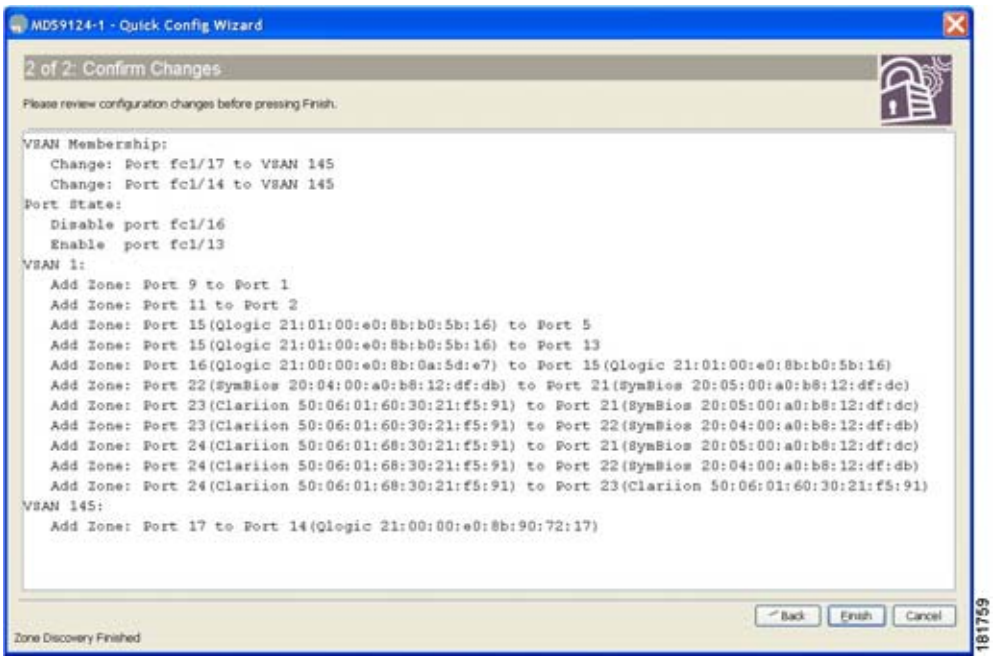
[VSAN] ドロップダウン メニューには、選択された VSAN 内のデバイスだけをゾーン分割できるフィルタが用意されています。

ステップ 4　列の表示と非表示を切り替えるには、列の名前を右クリックします。

ステップ 5　[Next] をクリックして変更を確認します。

図 5-6 に示す [Confirm Changes] ダイアログボックスが表示されます。

図 5-6　[Confirm Changes] ダイアログボックス



ステップ 6　CLI コマンドを確認する場合は、ダイアログボックスを右クリックし、ポップアップ メニューから [CLI Commands] をクリックします。

ステップ 7　[Finish] をクリックして設定変更を保存します。

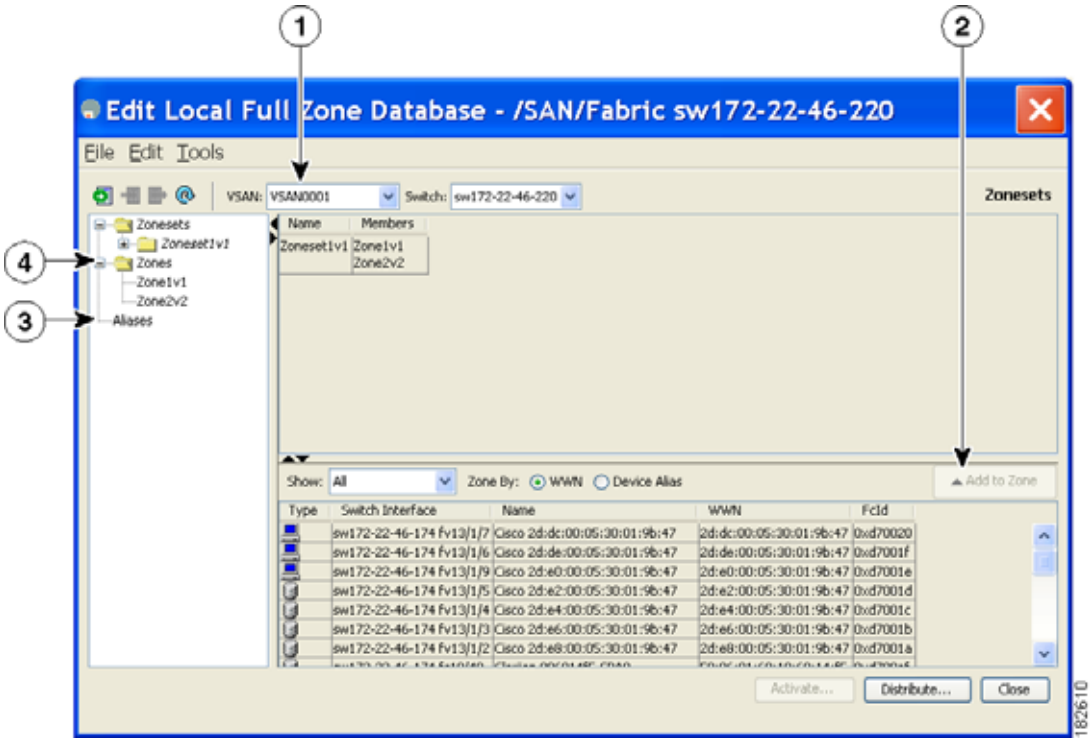
ゾーン設定

ここではゾーンの設定方法について、次の内容を説明します。

Edit Local Full Zone Database ツールの概要

Edit Local Full Zone Database ツールを使用すると、複数のスイッチでゾーン分割ができ、[Edit Local Full Zone Database] ダイアログボックスですべてのゾーン分割機能が使用可能になります（図 5-7 を参照）。

図 5-7　[Edit Local Full Zone Database] ダイアログボックス



1	ダイアログボックスを閉じずに、ドロップダウン メニューで VSAN を選択して再入力すると、VSAN 別の情報を表示できます。	3	複数のフォルダ内のエイリアスに基づいてゾーン分割特性を追加できます。
2	[Add to zone] ボタンを使用すると、エイリアスまたはゾーン単位でデバイスを上下に移動できます。	4	ツリー内のゾーン セット、ゾーン、またはエイリアスの名前を変更するには、トリプルクリックします。

（注）　[Device Alias] ラジオ ボタンは、デバイスのエイリアスが enhanced モードのときにだけ表示されます。詳細については、「デバイス エイリアスの作成」（P.6-7）を参照してください。

ヒント　[Physical Attributes] ペインから [Switches] を展開して 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。

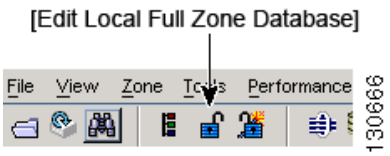
（注）　インターフェイスベース ゾーン分割は、Cisco MDS 9000 ファミリ スイッチでだけ機能します。インターフェイスベースゾーン分割は、その VSAN で interop モードが設定されている場合は動作しません。

Zone Configuration Tool を使用したゾーンの設定

Fabric Manager を使用してゾーンを作成し、これをゾーン セットに移動する手順は、次のとおりです。

ステップ 1　ツールバーにある [Zone] アイコンをクリックします（図 5-8 を参照）。

図 5-8　[Zone] アイコン

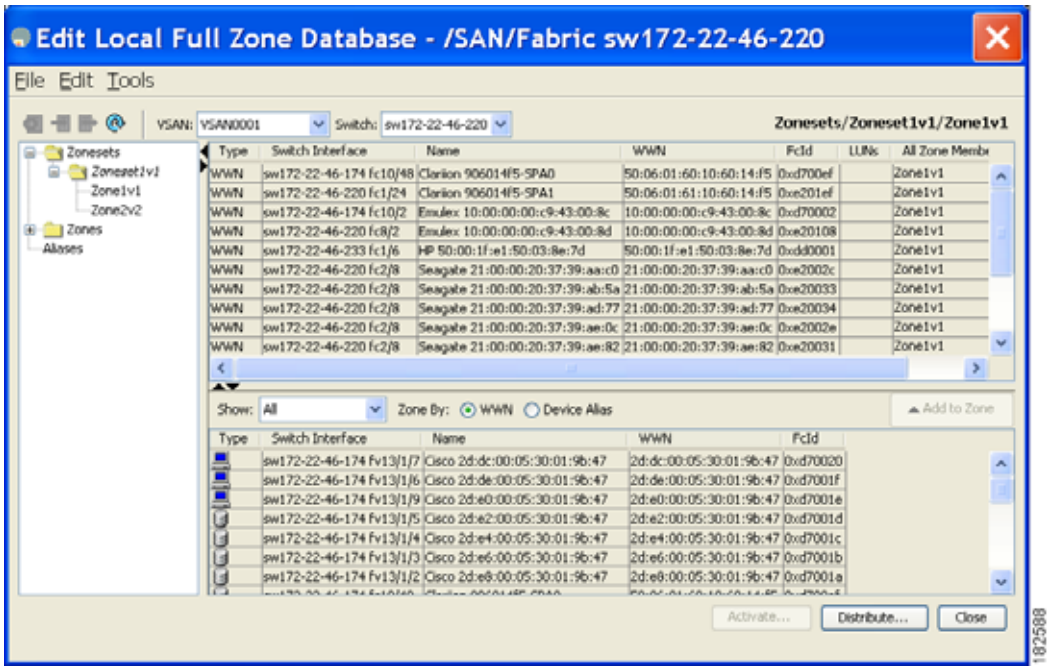


[Select VSAN] ダイアログボックスが表示されます。

ステップ 2　ゾーンを作成する VSAN を選択し、[OK] をクリックします。

図 5-9 に示す [Edit Local Full Zone Database] ダイアログボックスが表示されます。

図 5-9　[Edit Local Full Zone Database] ダイアログボックス

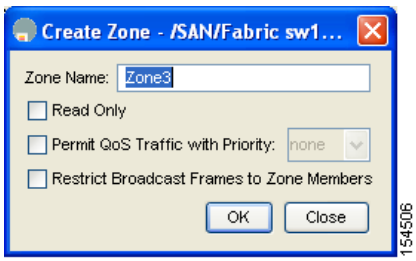


ゾーン メンバシップ情報を表示する場合は、[All Zone Membership(s)] 列を右クリックして、ポップアップ メニューで現在の行またはすべての行の [Show Details] をクリックします。

ステップ 3　左側のペインの [Zones] をクリックし、[Insert] アイコンをクリックして、ゾーンを作成します。

[Create Zone] ダイアログボックスが表示されます（図 5-10 を参照してください）。

図 5-10　[Create Zone] ダイアログボックス



ステップ 4　ゾーン名を入力します。

ステップ 5　次のチェックボックスのうち 1 つをオンにします。

a. **Read Only**: このゾーンでは読み込みを許可し、書き込みは拒否します。

b. **Permit QoS traffic with Priority**: ドロップダウン メニューでプライオリティを設定します。

c. **Restrict Broadcast frames to Zone Members（ブロードキャスト フレームをゾーン メンバーに制限）**

ステップ 6　[OK] をクリックしてゾーンを作成します。

このゾーンを既存のゾーン セットに移動する場合は、ステップ 8 へスキップします。

ステップ 7　左側のペインの [Zoneset] をクリックし、[Insert] アイコンをクリックして、ゾーン セットを作成します

[Zoneset Name] ダイアログボックスが表示されます（図 5-11 を参照）。

図 5-11　[Zoneset Name] ダイアログボックス

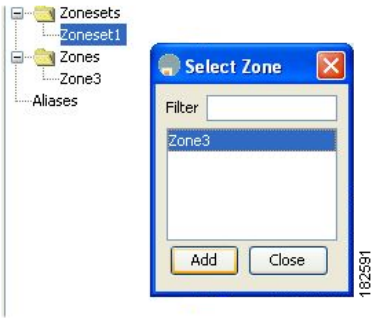
ステップ 8　ゾーン セット名を入力し、[OK] をクリックします。

（注）　シンボル（$、-、^、_）のうちの 1 つまたはすべての英数字がサポートされています。interop モード 2 と 3 では、シンボル（_）またはすべての英数字がサポートされています。

ステップ 9　ゾーンを追加するゾーン セットを選択して [Insert] アイコンをクリックするか、[Zoneset1] へ Zone3 をドラッグ アンド ドロップします。

[Select Zone] ダイアログボックスが表示されます（図 5-12 を参照）。

図 5-12　[Select Zone] ダイアログボックス



ステップ 10　[Add] をクリックして、ゾーンを追加します。

ゾーン メンバーの追加

ゾーンを作成すると、ゾーンにメンバーを追加できます。メンバーを追加するには、複数のポート識別タイプを使用します。

Fabric Manager を使用してゾーンにメンバーを追加する手順は、次のとおりです。

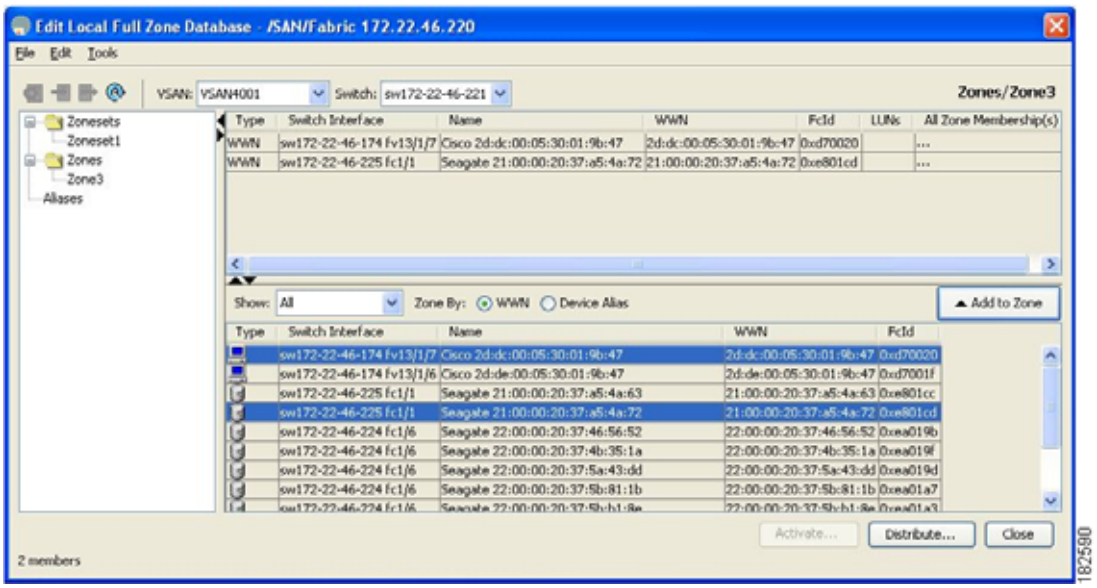
ステップ 1　[Zone] > [Edit Local Full Zone Database] を選択します。

[Select VSAN] ダイアログボックスが表示されます。

ステップ 2　VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます。

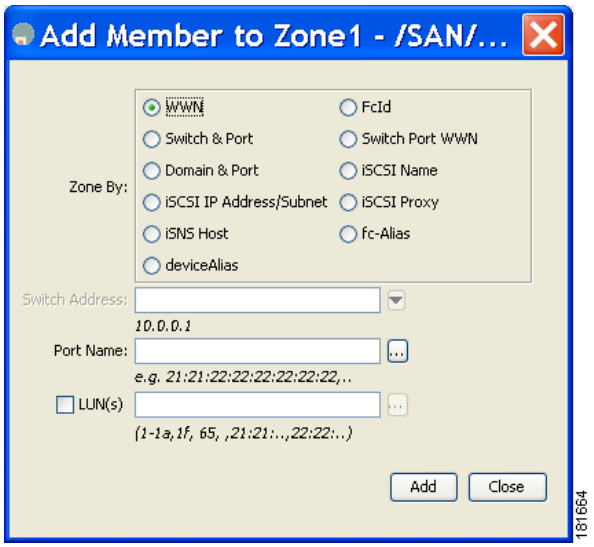
図 5-13　[Edit Local Full Zone Database] ダイアログボックス



ステップ 3　[Fabric] ペイン（図 5-13 を参照）から追加するメンバーを選択し、[Add to Zone] をクリックするか、メンバーを追加するゾーンをクリックし、[Insert] アイコンをクリックします。

図 5-14 に示す [Add Member to Zone] ダイアログボックスが表示されます。

図 5-14　[Add Member to Zone] ダイアログボックス



（注）　[Device Alias] ラジオ ボタンは、デバイスのエイリアスが enhanced モードのときにだけ表示されます。詳細については、「デバイス エイリアスの作成」（P.6-7）を参照してください。

ステップ 4　参照ボタンをクリックしてポート名を選択するか、[LUN] チェックボックスをクリックしてから参照ボタンをクリックして LUN を設定します。

ステップ 5　[Add] をクリックして、ゾーンにメンバーを追加します。

（注）　ゾーン メンバーを設定する場合は、OS ごとに異なる複数の ID が 1 つの Logical Unit Number（LUN）に設定されるように指定することができます。6 つの異なる OS から選択できます。

名前、WWN、または FC ID に基づくエンド デバイスのフィルタリング

エンド デバイスおよびデバイス エイリアスをフィルタする手順は、次のとおりです。

ステップ 1　ツールバーにある [Zone] アイコンをクリックします（図 5-8 を参照）。

ステップ 2　[With] ドロップダウン リストから名前、[WWN]、または [FC ID] を選択します。

ステップ 3　[Filter] テキストボックスに *zo1* などのフィルタ条件を入力します。

ステップ 4　[Go] をクリックします。

複数のゾーンへの複数のエンド デバイスの追加

複数のゾーンに複数のエンド デバイスを追加する手順は、次のとおりです。

ステップ 1　ツールバーにある [Zone] アイコンをクリックします（図 5-8 を参照）。

ステップ 2　Ctrl キーを使用して複数のエンド デバイスを選択します。

ステップ 3　右クリックし、[Add to Zone] を選択します。

ステップ 4　表示されるポップアップ ウィンドウから、Ctrl キーを使用して複数のゾーンを選択します。

ステップ 5　[Add] をクリックします。

選択されたエンド デバイスが選択されたゾーンに追加されます。

ゾーン セット

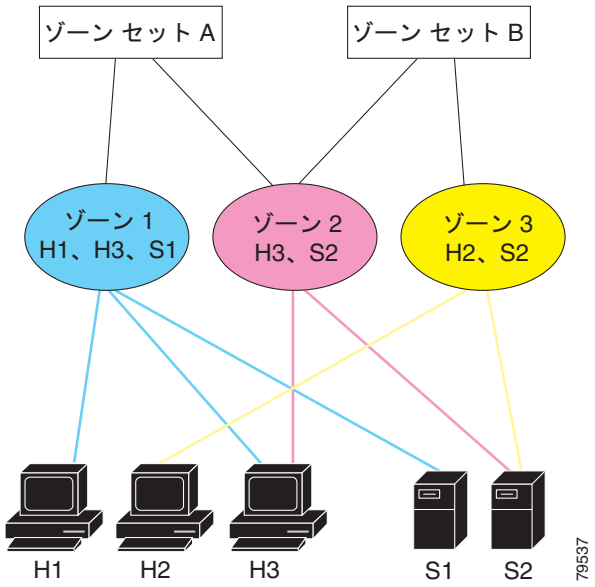
ゾーンではアクセス制御を指定するメカニズムが提供されています。それに対して、ファブリック内でのアクセス制御の実行を補強するためにゾーンをグループ化したものが、ゾーン セットです。

ここではゾーン セットについて、次の内容を説明します。

ゾーン セットの作成の概要

図 5-15 では、それぞれ独自のメンバシップ階層とゾーン メンバーを持つ別個の 2 つのセットが作成されています。

図 5-15　ゾーン セット、ゾーン、ゾーン メンバーの階層



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）をアクティブにすることができます。

ヒント　(ゾーン セットが設定済みの VSAN にある場合) ゾーン セットはメンバー ゾーンと VSAN の名前で設定されます。

ゾーン セットのアクティブ化

ゾーン セットをアクティブにするまで、ゾーン セットへの変更はフル ゾーン セットで有効になりません。

Fabric Manager を使用して既存のゾーンをアクティブにする手順は、次のとおりです。

ステップ 1　[Zone] > [Edit Local Full Zone Database] を選択します。

[Select VSAN] ダイアログボックスが表示されます。

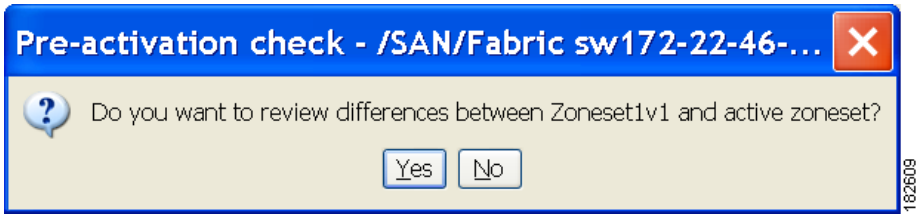
ステップ 2　VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 3　[Activate] をクリックして、ゾーン セットをアクティブにします。

[Pre-Activation Check] ダイアログボックスが表示されます（図 5-16 を参照）。

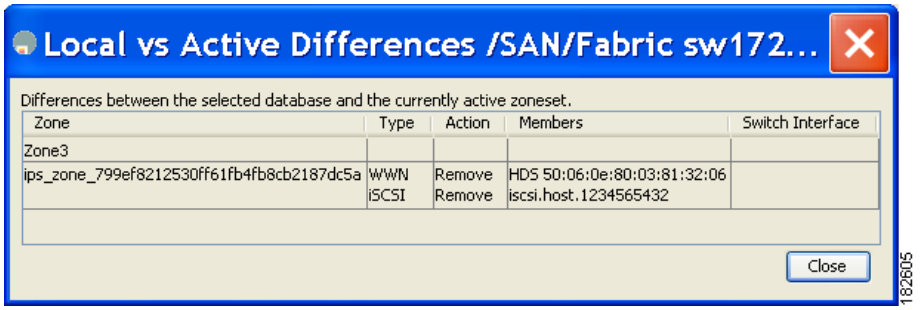
図 5-16　[Pre-Activation Check] ダイアログボックス



ステップ 4　[Yes] をクリックして、相違を確認します。

[Local vs.Active Differences] ダイアログボックスが表示されます（図 5-17 を参照）。

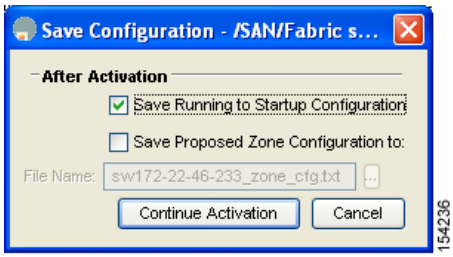
図 5-17　[Local vs. Active Differences] ダイアログボックス



ステップ 5　[Close] をクリックして、ダイアログボックスを閉じます。

[Save Configuration] ダイアログボックスが表示されます（図 5-18 を参照）。

図 5-18　[Save Configuration] ダイアログボックス

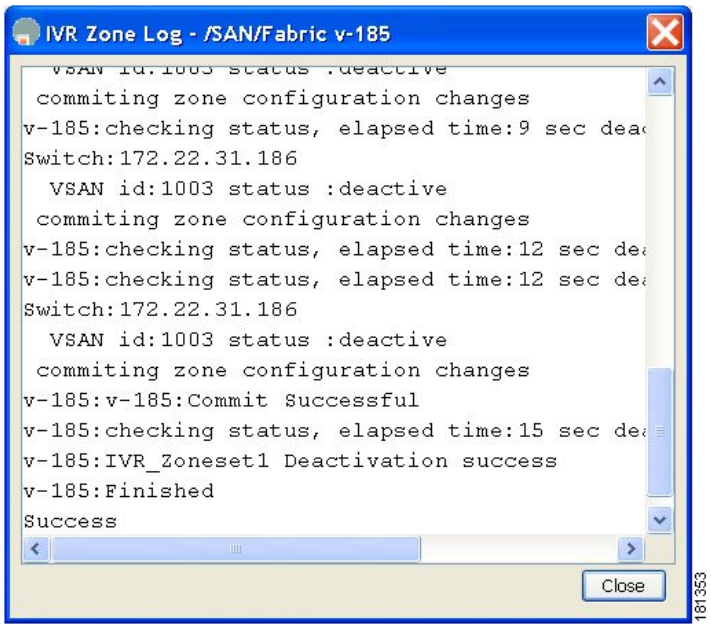


ステップ 6　すべての変更をスタートアップ コンフィギュレーションに保存するには、[Save Running to Startup Configuration] チェックボックスをオンにします。

ステップ 7　ゾーン セットをアクティブにするには [Continue Activation] をクリックします。ダイアログボックスを閉じて、保存されていない変更を破棄するには、[Cancel] をクリックします。

ゾーン セットのアクティブ化に成功したかどうかを示す [Zone Log] ダイアログボックスが表示されます（図 5-19 を参照）。

図 5-19　[Zone Log] ダイアログボックス



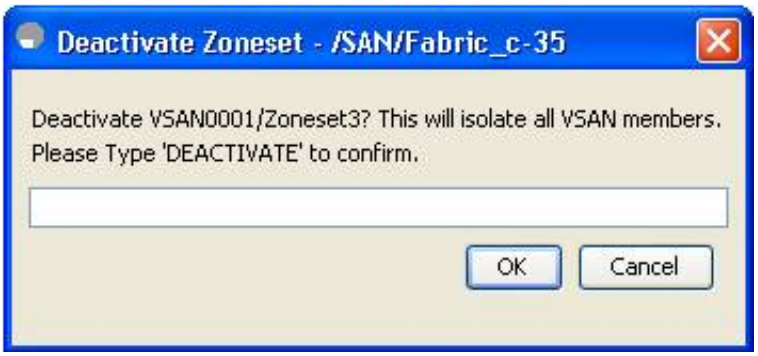
ゾーンセットの非アクティブ化

既存のゾーンを非アクティブ化する手順は、次のとおりです。

ステップ 1　非アクティブにするゾーン セットを右クリックし、ポップアップ メニューで [Deactivate] をクリックします。

[Deactivate Zoneset] ダイアログボックスが表示されます（図 5-20 を参照）。

図 5-20　[Deactivate Zoneset] ダイアログボックス



ステップ 2　テキストボックスに deactivate と入力し、[OK] をクリックします。

[Input] ダイアログボックスが表示されます（図 5-21 を参照）。

図 5-21　[Input] ダイアログボックス

ステップ 3　テキストボックスに deactivate と入力し、[OK] をクリックしてゾーン セットを非アクティブにします。

（注）　このオプションをイネーブルにするには、server.properties ファイルを修正する必要があります。server.properties ファイルの修正の詳細については、『*Cisco Fabric Manager Fundamentals Configuration Guide*』を参照してください。

ゾーン メンバシップ情報の表示

Fabric Manager を使用してゾーンに割り当てられたメンバーのゾーン メンバシップ情報を表示する手順は、次のとおりです。

ステップ 1　[Zone] > [Edit Local Full Zone Database] を選択します。

[Select VSAN] ダイアログボックスが表示されます。

ステップ 2　VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 3　左側のペインで、[Zones] をクリックします。右側のペインに各ゾーンのメンバーが表示されます。

（注）　デフォルト ゾーン メンバーは、デフォルト ゾーン ポリシーが **permit** に設定されている場合に限り、明示的に表示されます。デフォルト ゾーン ポリシーが **deny** に設定されている場合、このゾーンのメンバーは表示されません。「ゾーン情報の表示」（P.5-48）を参照してください。

デフォルト ゾーンの概要

ファブリック（Nx ポートに接続されているデバイス）の各メンバーは、任意のゾーンに所属することができます。どのアクティブ ゾーンにも所属しないメンバーは、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 ゾーンに所属すると見なされます。メンバー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ーは、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 ゾーンのメンバーかを判別します。

（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 ゾーンのメンバー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る場合、ゾーンは設定されておらず、すべてのメンバーがデフォルト ゾーンに所属すると見なされます。メンバー同士で相互に通信することは許可されていません。

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を変更できます。

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。

任意の VSAN のデフォルト ゾーン ポリシーを変更するには、Fabric Manager メニューで [VSANxx] > [Default Zone] を選択し、[Policies] タブをクリックします。デバイス間の接続を確立する場合は、これらのデバイスをデフォルト以外のゾーンに割り当てることを推奨します。

デフォルト ゾーンの設定

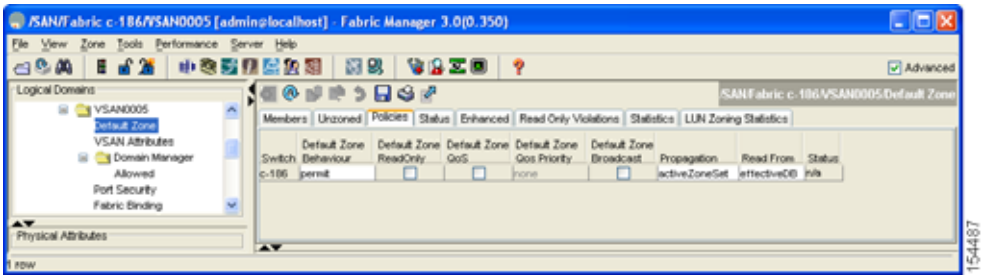
Fabric Manager を使用してデフォルト ゾーン内のメンバーに対するトラフィックを許可または拒否する手順は、次のとおりです。

ステップ 1　VSAN を開き、[Fabric Manager Logical Domains] ペインで [Default Zone] を選択します。

ステップ 2　[Information] ペインで [Policies] タブをクリックします。

[Information] ペインにゾーン ポリシー情報が表示されます（図 5-22 を参照）。

図 5-22　デフォルト ゾーン ポリシー



アクティブ ゾーン セットはイタリック体で表示されます。アクティブ ゾーン セットを変更してから変更をアクティブ化するまでの間は、このゾーン セットが太字のイタリック体で表示されます。

ステップ 3　[Default Zone Behaviour] フィールドで、ドロップダウン メニューから [permit] または [deny] を選択します。

FC エイリアスの作成の概要

次の値を使用して、エイリアス名を割り当て、エイリアス メンバーを設定できます。

- pWWN：N または NL ポートの WWN は、16 進形式です（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：N ポート ID は、0xhhhhhh 形式です（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。
- IPv4 アドレス：接続されたデバイスの IPv4 アドレスは、ドット付きの 10 進表記の 32 ビットで、オプションでサブネット マスクを伴います。マスクが指定されている場合、サブネット内のすべてのデバイスが指定されたゾーンのメンバーになります。
- IPv6 アドレス：接続されたデバイスの IPv6 アドレスは、コロン（:）で区切られた 16 進表記の 128 ビットです。

- インターフェイス：インターフェイスベースのゾーン分割ではポートベース ゾーン分割と同様に、ゾーン設定にスイッチ インターフェイスが使用されます。ローカルおよびリモート スイッチの両方で、スイッチ インターフェイスをゾーン メンバー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 sWWN またはドメイン ID を入力します。

ヒント　Cisco NX-OS ソフトウェアは、VSAN ごとに最大 2048 個のエイリアスをサポートしています。

FC エイリアスの作成

Fabric Manager を使用して FC エイリアスを作成する手順は、次のとおりです。

ステップ 1　[Zone] > [Edit Local Full Zone Database] を選択します。

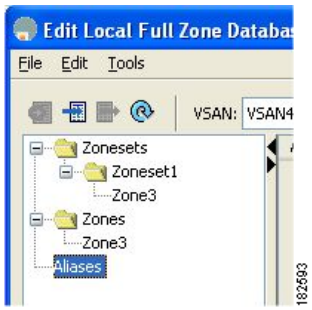
[Select VSAN] ダイアログボックスが表示されます。

ステップ 2　VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 3　左下のペインで、[Aliases] をクリックします（図 5-23 を参照）。右側のペインに既存のエイリアスが表示されます。

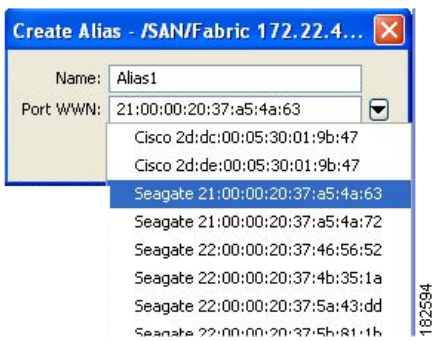
図 5-23　FC エイリアスの作成



ステップ 4　[Insert] アイコンをクリックして、エイリアスを作成します。

[Create Alias] ダイアログボックスが表示されます（図 5-24 を参照）。

図 5-24　[Create Alias] ダイアログボックス



ステップ 5　エイリアス名および pWWN を設定します。

ステップ 6　[OK] をクリックしてエイリアスを作成します。

エイリアスへのメンバーの追加

Fabric Manager を使用してエイリアスにメンバーを追加する手順は、次のとおりです。

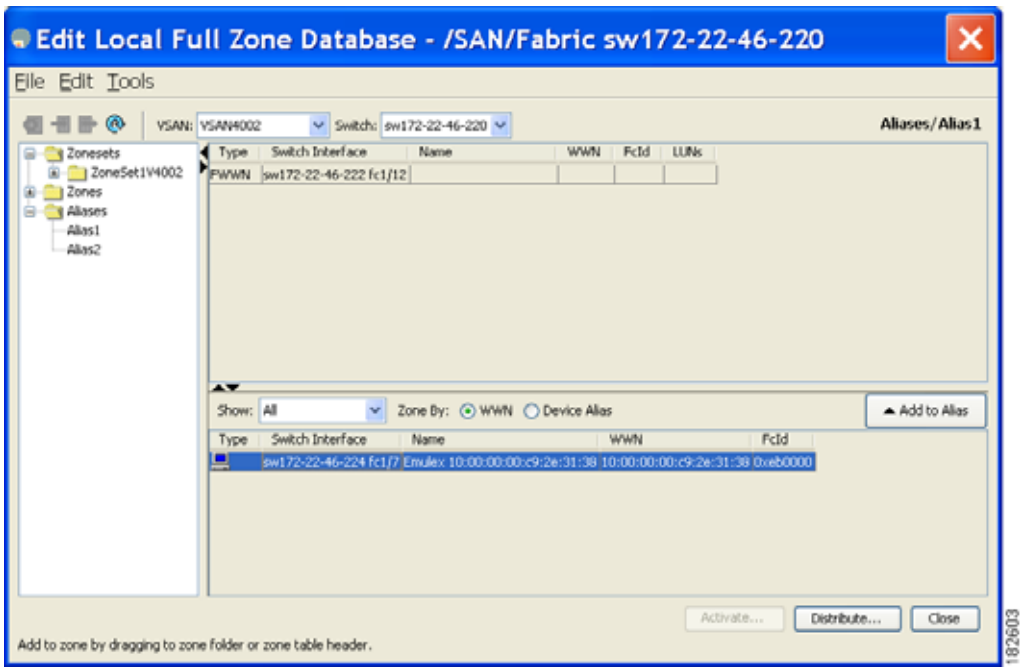
ステップ 1　[Zone] > [Edit Local Full Zone Database] を選択します。

[Select VSAN] ダイアログボックスが表示されます。

ステップ 2　VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます（図 5-25 を参照）。

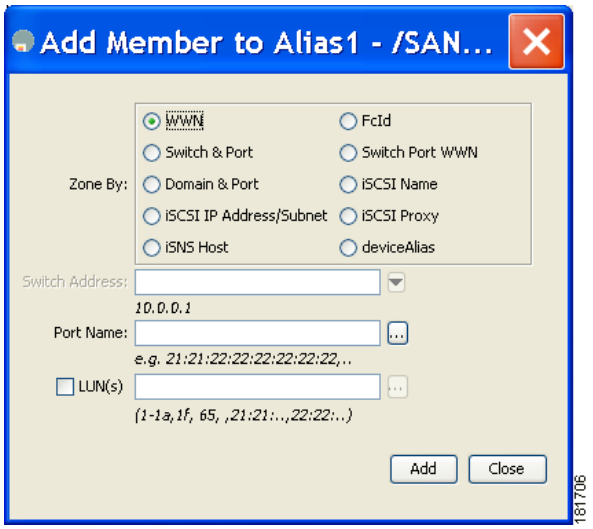
図 5-25　[Edit Local Full Zone Database] ダイアログボックス



ステップ 3　[Fabric] ペインから追加するメンバーを選択し（図 5-25 を参照）、[Add to Alias] をクリックするか、メンバーを追加するエイリアスをクリックし、[Insert] アイコンをクリックします。

図 5-26 に示す [Add Member to Alias] ダイアログボックスが表示されます。

図 5-26　[Add Member to Alias] ダイアログボックス



（注）　[Device Alias] ラジオ ボタンは、デバイスのエイリアスが enhanced モードのときにだけ表示されます。詳細については、「デバイス エイリアスの作成」（P.6-7）を参照してください。

ステップ 4　参照ボタンをクリックしてポート名を選択するか、[LUN] チェックボックスをクリックしてから参照ボタンをクリックして LUN を設定します。

ステップ 5　[Add] をクリックして、エイリアスにメンバーを追加します。

ゾーンメンバーの pWWN ベースメンバーへの変換

ゾーンおよびエイリアス メンバーをスイッチ ポートまたは FC ID ベースのメンバシップから pWWN ベースのメンバシップに変換できます。この機能を利用して、pWWN へ変換すれば、カードまたはスイッチがファブリックで変更されてもゾーン設定は変更されません。

Fabric Manager を使用してスイッチ ポートと FC ID メンバーを pWWN メンバーに変換する手順は、次のとおりです。

ステップ 1　[Zone] > [Edit Local Full Zone Database] を選択します。

[Select VSAN] ダイアログボックスが表示されます。

ステップ 2　VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 3　変換するゾーンをクリックします。

ステップ 4　[Tools] > [Convert Switch Port/FCID members to By pWWN] を選択します。

変換するすべてのメンバーが列挙された [Conversion] ダイアログボックスが表示されます。

ステップ 5　変更を確認し、[Continue Conversion] をクリックします。

ステップ 6　確認ダイアログボックスで [Yes] をクリックして、そのメンバーを pWWN ベースのメンバシップに変更します。

（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。

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。スイッチのリセット時には使用できません。

注意　IVR に対しても設定されている VSAN 内のアクティブ ゾーン セットを非アクティブにした場合、アクティブ IVR ゾーン セット（IVZS）も非アクティブになり、スイッチとの間のすべての IVR トラフィックは停止されます。この非アクティブ化により、複数の VSAN でトラフィックが中断される場合があります。アクティブ ゾーン セットを非アクティブにする前に、VSAN のアクティブ ゾーン分析をチェックしてください。IVZS を再度アクティブ化するには、標準ゾーン セットを再度アクティブ化する必要があります（『*Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide*』を参照）。

注意　現在アクティブなゾーン セットに IVR ゾーンが含まれている場合、IVR がイネーブルになっていないスイッチからゾーン セットをアクティブにすると、その VSAN との間の IVR トラフィックが中断されます。常に IVR 対応のスイッチからゾーン セットをアクティブにして、IVR トラフィックの中断を回避することを強くお勧めします。

（注）　仮想ターゲットの pWWN は、Fabric Manager のゾーン分割エンド デバイスのデータベースには表示されません。pWWN で仮想デバイスのゾーン分割を行う場合は、ゾーンを作成するときにこれを [Add Member to Zone] ダイアログボックスに入力する必要があります。ただし、デバイス エイリアスが拡張モードの場合、仮想デバイス名は Fabric Manager の [Zoning] ウィンドウの [Device Alias Database] に表示されます。この場合、デバイス エイリアス名を選択するか、[Add Member to Zone] ダイアログボックスで pWWN を入力することができます。

詳細については、「ゾーン メンバーの追加」（P.5-14）を参照してください。

（注）　SDV を使用する場合はデバイス エイリアス モードを **enhanced** に設定します（仮想デバイスの pWWN が変化する可能性があるため）。

たとえば、SDV がスイッチでイネーブルになっていて、仮想デバイスが定義されているとします。SDV は仮想デバイスの pWWN を割り当て、ゾーン内の pWWN に基づいてゾーン分割されます。後で SDV をディセーブルにした場合、この設定は失われます。SDV を再度イネーブルにし、同じ名前を使用して仮想デバイスを作成する場合、同じ pWWN が再び取得される保証はありません。このため、pWWN ベースのゾーンを再度ゾーン分割する必要があります。ただし、デバイス/エイリアス名に基づくゾーン分割を実行する場合は、pWWN の変更時に設定変更は必要ありません。

デバイス エイリアス モードをイネーブルにする前に、デバイス エイリアス モードがどのように動作するのかを確認してください。デバイス エイリアス モードの詳細と要件については、第 6 章「デバイス エイリアス サービスの配信」を参照してください。

名前に基づくゾーン、ゾーン セット、およびデバイス エイリアスのフィルタリング

ゾーン、ゾーン セット、またはデバイス エイリアスをフィルタする手順は、次のとおりです。

ステップ 1　ツールバーにある [Zone] アイコンをクリックします（図 5-8 を参照）。

ステップ 2　[Filter] テキストボックスに *zo1* などのフィルタ条件を入力します。

ステップ 3　[Go] をクリックします。

複数のゾーン セットへの複数のゾーンの追加

複数のゾーン セットに複数のゾーンを追加する手順は、次のとおりです。

ステップ 1　ツールバーにある [Zone] アイコンをクリックします（図 5-8 を参照）。

ステップ 2　ツリー表示から、[Zoneset] を選択します。

ステップ 3　Ctrl キーを使用して複数のゾーンを選択します。

ステップ 4　右クリックし、[Add to Zoneset] を選択します。

ステップ 5　表示されたポップアップ ウィンドウから、Ctrl キーを使用して複数のゾーン セットを選択します。

ステップ 6　[Add] をクリックします。

選択されたゾーンが、選択されたゾーン セットに追加されます。

ゾーン分割の実行

ゾーン分割を実行するには、ソフトおよびハードの 2 とおりの方法があります。各エンド デバイス（N ポートまたは NL ポート）は、ネーム サーバにクエリを送信することでファブリック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 サーバはクエリ元デバイスがアクセスできるその他のデバイスのリストを返します。Nx ポートがゾーンの外部にあるその他のデバイスの FC ID 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 FC ID 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、Nx 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、発信元/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 MDS 9000 ファミリのスイッチは、ハードおよびソフトの両方のゾーン分割をサポートしています。

ゾーン セット配信

フル ゾーン セットを配信するには、ワンタイム配信またはフル ゾーン セット配信のいずれかの方法を使用します。表 5-1 に、これらの配信方法の相違を示します。

表 5-1　ゾーン セット配信の相違

ワンタイム配信	フル ゾーン セット配信
ただちにフル ゾーン セットを配信します。	すぐにはフル ゾーン セットを配信しません。
アクティブ化、非アクティブ化、またはマージ プロセス中は、アクティブなゾーン セットとともにフル ゾーン セット情報を配信しません。	アクティブ化、非アクティブ化、またはマージ プロセス中にアクティブなゾーン セットとともにフル ゾーン セット情報を配信することを記憶しています。

ここではゾーン セット配信について、次の内容を説明します。

- 「フル ゾーン セット配信のイネーブル化」（P.5-29）
- 「ワンタイム配信のイネーブル化」（P.5-29）
- 「リンクの分離からの回復の概要」（P.5-30）
- 「ゾーン セットのインポートおよびエクスポート」（P.5-31）

フル ゾーン セット配信のイネーブル化

Cisco MDS 9000 ファミリ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 でアクティブ化されたときに、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。

Fabric Manager を使用して VSAN ベースで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する手順は、次のとおりです。

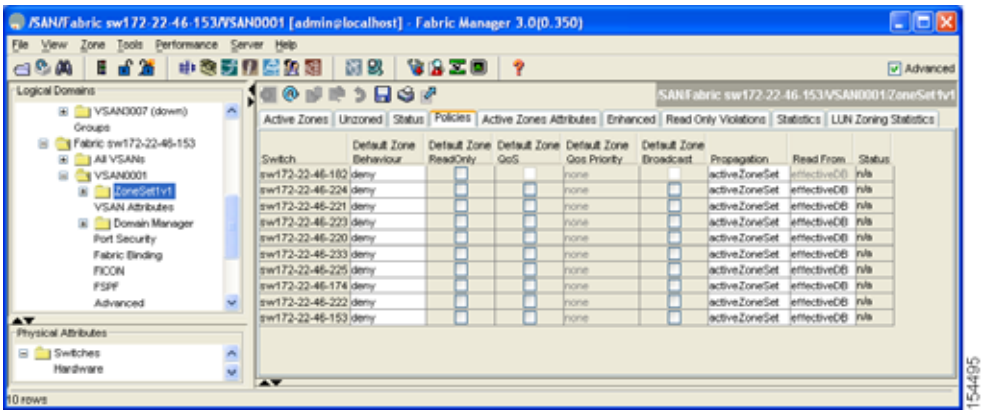
ステップ 1　VSAN を開き、[Logical Domains] ペインで、ゾーン セットを選択します。

[Information] ペインにゾーン セットの設定が表示されます。[Active Zones] タブはデフォルトです。

ステップ 2　[Policies] タブをクリックします。

ゾーンの設定されたポリシーが表示されます（図 5-27 を参照）。

図 5-27　ゾーンに設定されたポリシー



ステップ 3　[Propagation] 列で、ドロップダウン メニューから fullZoneset を選択します。

ステップ 4　[Apply Changes] をクリックして、フル ゾーン セットを伝播します。

ワンタイム配信のイネーブル化

ファブリック全体で、非アクティブ、非変更のゾーン セットのワンタイム配信が行えます。Fabric Manager からフル ゾーン セットのワンタイム配信を伝播する手順は、次のとおりです。

ステップ 1　[Zone] > [Edit Local Full Zone Database] を選択します。

[Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 2　左側のペインでリストから適切なゾーンをクリックします。

ステップ 3　[Distribute] ボタンをクリックして、ファブリック内でフル ゾーン セットを配信します。

この手順では、フル ゾーン セット情報が配信されるだけです。情報はスタートアップ コンフィギュレーションには保存されません。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明示的に保存する必要があります。

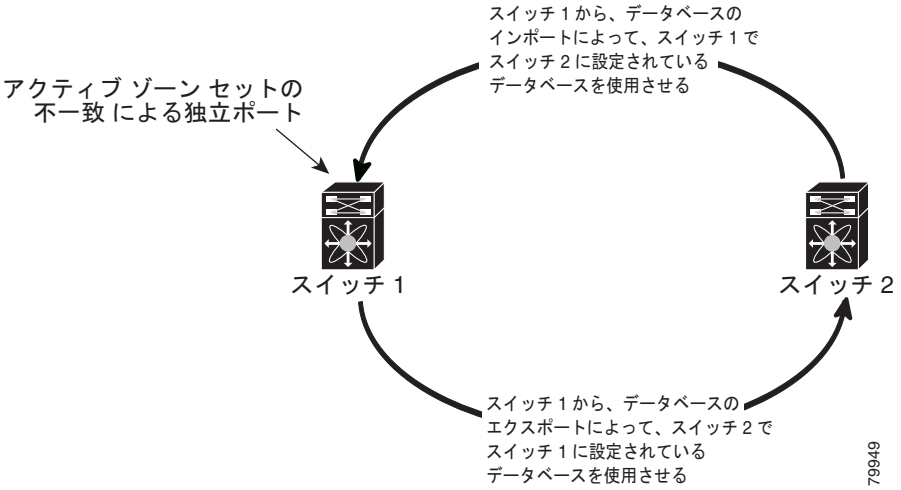
（注）　フル ゾーン セットのワンタイム配信は、**interop 2** および **interop 3** モードでサポートされていますが、**interop 1** モードではサポートされていません。

リンクの分離からの回復の概要

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。

- 近接スイッチのアクティブ ゾーン セットのデータベースをインポートし、現在のアクティブ ゾーン セットと交換します（図 5-28 を参照）。
- 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 5-28　　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

Fabric Manager を使用してゾーン セット情報を近接スイッチとの間でインポートまたはエクスポートする手順は、次のとおりです。

ステップ 1　[Tools] > [Zone Merge Fail Recovery] を選択します。

図 5-29 に示す [Zone Merge Failure Recovery] ダイアログボックスが表示されます。

図 5-29　[Zone Merge Failure Recovery] ダイアログボックス

ステップ 2　[Import Active Zoneset] または [Export Active Zoneset] ラジオ ボタンを選択します。

ステップ 3　ドロップダウン リストで、ゾーン セット情報のインポート元またはエクスポート先になるスイッチを選択します。

ステップ 4　ドロップダウン リストで、ゾーン セット情報のインポート元またはエクスポート先になる VSAN を選択します。

ステップ 5　インポート プロセスに使用するインターフェイスを選択します。

ステップ 6　[OK] をクリックして、アクティブ ゾーン セットをインポートまたはエクスポートします。

（注）　**import** および **export** は、単一のスイッチから発行します。1 つのスイッチからインポートし、別のスイッチからエクスポートすると、リンクが再び分離する可能性があります。

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することができます。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することができます。

- 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、または伝送されなかった場合に、既存のゾーン セットに変更を加え、アクティブにすることはできません。

注意　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際に、同一名のゾーンがフル ゾーン セット データベースにすでに存在する場合は、上書きされる可能性があります。

ここで説明する内容は、次のとおりです。

ゾーン セットのコピー

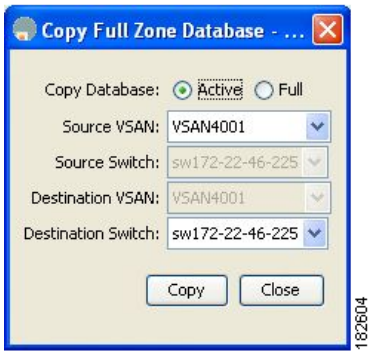
Cisco MDS ファミリ スイッチでは、アクティブ ゾーン セットを編集できません。ただし、アクティブ ゾーン セットをコピーして新しいゾーン セットを作成し、これを編集することはできます。

Fabric Manager を使用してゾーン セットをコピーする手順は、次のとおりです。

ステップ 1　[Zone] > [Copy Full Zone Database] を選択します。

[Copy Full Zone Database] ダイアログボックスが表示されます（図 5-30 を参照）。

図 5-30　[Copy Full Zone Database] ダイアログボックス



ステップ 2　コピーするデータベースのタイプに応じて、[Active] または [Full] ラジオ ボタンをクリックします。

ステップ 3　ドロップダウン リストでコピー元 VSAN を選択します。

ステップ 4　[Copy Full] を選択した場合は、ドロップダウン リストでコピー元スイッチおよびコピー先 VSAN を選択します。

ステップ 5　ドロップダウン リストでコピー先スイッチを選択します。

ステップ 6　[Copy] をクリックしてデータベースをコピーします。

注意　Inter-VSAN Routing（IVR）機能がイネーブルになっていて、IVR ゾーンがアクティブ ゾーン セット内に存在する場合、ゾーン セット コピー操作はすべての IVR ゾーンをフル ゾーン データベースにコピーします。IVR ゾーンへのコピーを防ぐには、コピー操作を実行する前に、フル ゾーン セット データベースから明示的に削除する必要があります。IVR 機能の詳細については、『*Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide*』を参照してください。

ゾーンのバックアップおよび復元の概要

ゾーン設定をワークステーションにバックアップするには、TFTP 使用します。このゾーン バックアップ ファイルは、スイッチにゾーン設定を復元する場合に使用できます。ゾーン設定を復元すると、スイッチの既存のゾーン設定が上書きされます。

ゾーンのバックアップ

Fabric Manager を使用してフル ゾーン設定をバックアップする手順は、次のとおりです。

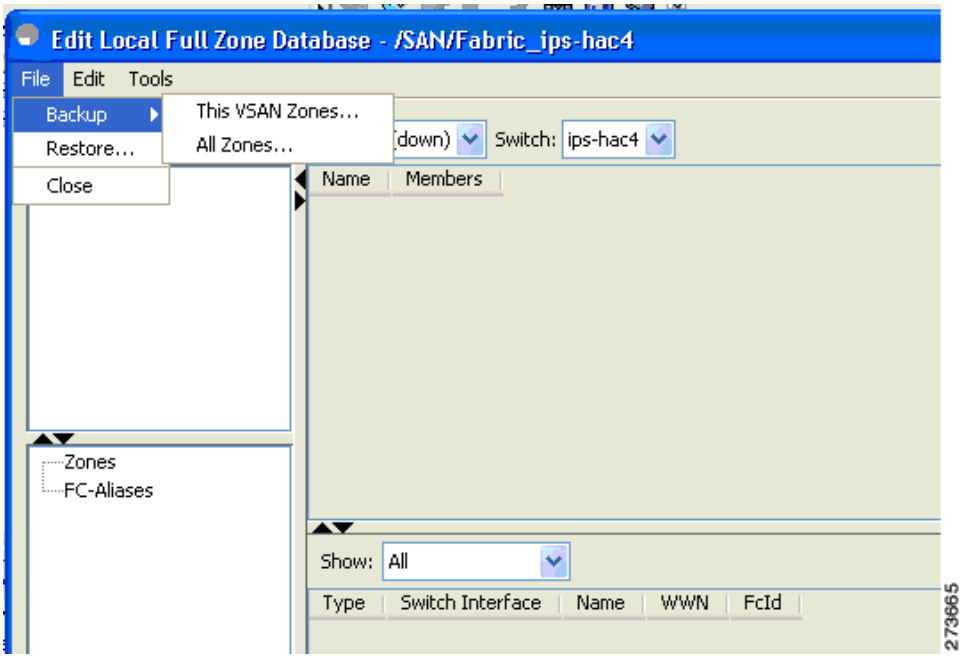
ステップ 1　[Zone] > [Edit Local Full Zone Database] を選択します。

[Select VSAN] ダイアログボックスが表示されます。

ステップ 2　VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます（図 5-31 を参照）。

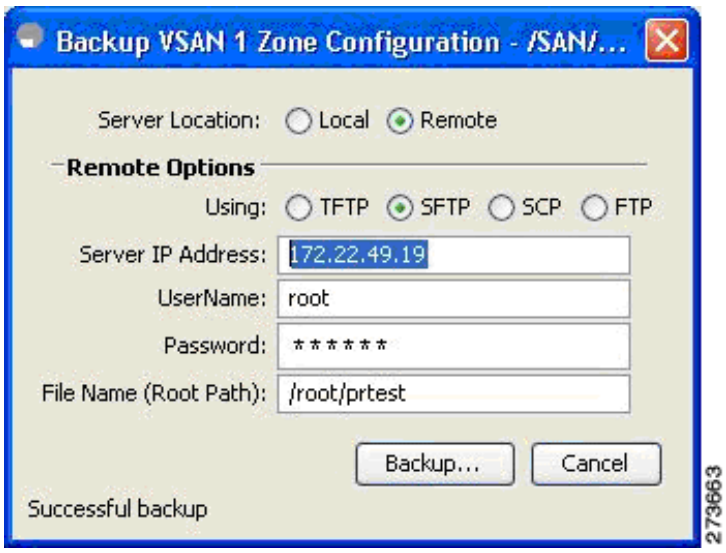
図 5-31　[Edit Local Full Zone Database] ダイアログボックス



ステップ 3　[File] > [Backup] > [This VSAN Zones] を選択して、TFTP、SFTP、SCP、または FTP を使用して既存のゾーン設定をワークステーションにバックアップします。

図 5-32 に示す [Backup Zone Configuration] ダイアログボックスが表示されます。

図 5-32　[Backup Zone Configuration] ダイアログボックス



データをリモート サーバにバックアップする前に、この設定を編集できます。

ステップ 4　次の [Remote Options] 情報を指定して、データをリモート サーバにバックアップします。

a. **Using**：プロトコルを選択します。

b. **Server IP Address**：サーバの IP アドレスを入力します。

c. **UserName**：ユーザの名前を入力します。

d. **Password**：ユーザのパスワードを入力します。

e. **File Name(Root Path)**：パスとファイル名を入力します。

ステップ 5　[Backup] をクリックするか、[Cancel] をクリックしてバックアップせずにダイアログボックスを閉じます。

ゾーンの復元

Fabric Manager を使用してゾーン設定を復元する手順は、次のとおりです。

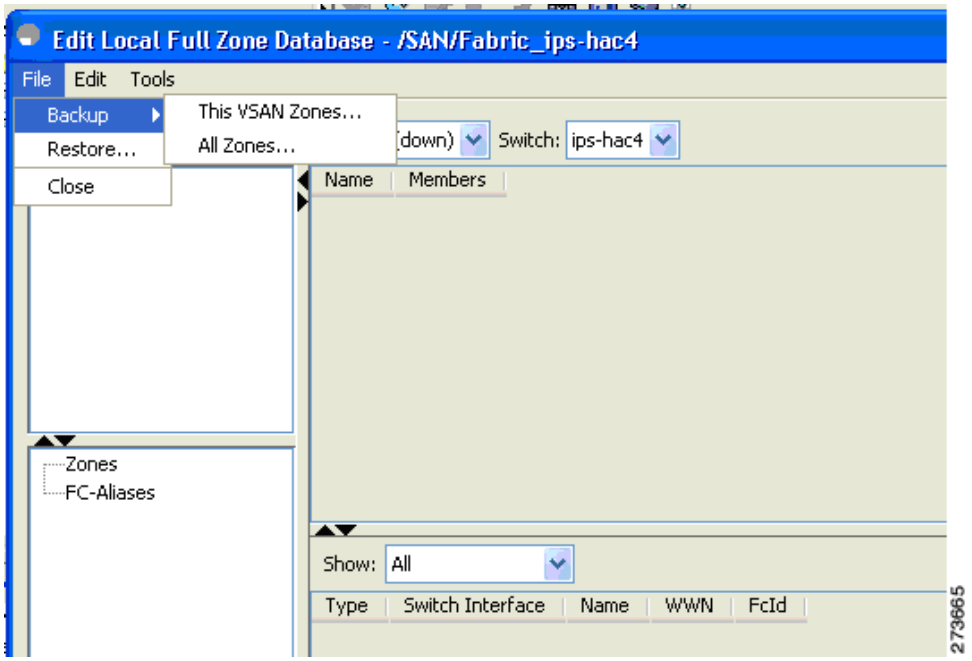
ステップ 1　[Zone] > [Edit Local Full Zone Database] を選択します。

[Select VSAN] ダイアログボックスが表示されます。

ステップ 2　VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます（図 5-33 を参照）。

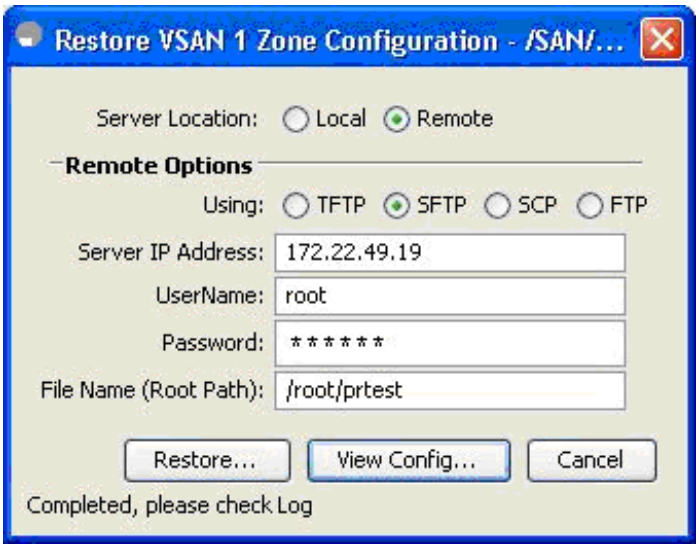
図 5-33　[Edit Local Full Zone Database] ダイアログボックス



ステップ 3　[File] > [Restore] を選択して、TFTP、SFTP、SCP、または FTP を使用して保存されたゾーン設定を復元します。

図 5-34 に示す [Restore Zone Configuration] ダイアログボックスが表示されます。

図 5-34　[Restore Zone Configuration] ダイアログボックス



スイッチにこの設定を復元する前に、設定を編集することもできます。

ステップ 4　次の [Remote Options] 情報を指定して、データをリモート サーバから復元します。

a. **Using**：プロトコルを選択します。

b. **Server IP Address**：サーバの IP アドレスを入力します。

c. **UserName**：ユーザの名前を入力します。

d. **Password**：ユーザのパスワードを入力します。

e. **File Name**：パスとファイル名を入力します。

ステップ 5　[Restore] をクリックして続行するか、[Cancel] をクリックして復元せずにダイアログボックスを閉じます。

（注）　[View Config] をクリックして、リモート サーバからゾーン設定ファイルを復元する方法に関する情報を確認します。このダイアログボックスで [Yes] をクリックすると、実行される CLI コマンドが表示されます。ダイアログボックスを閉じるには、[Close] をクリックします。

（注）　[Backup] オプションおよび [Restore] オプションは、Cisco NX-OS Release 4.1(3) 以降を実行するスイッチで使用できます。

ゾーン、ゾーン セット、およびエイリアスの名前の変更

Fabric Manager を使用してゾーン、ゾーン セット、またはエイリアスの名前を変更する手順は、次のとおりです。

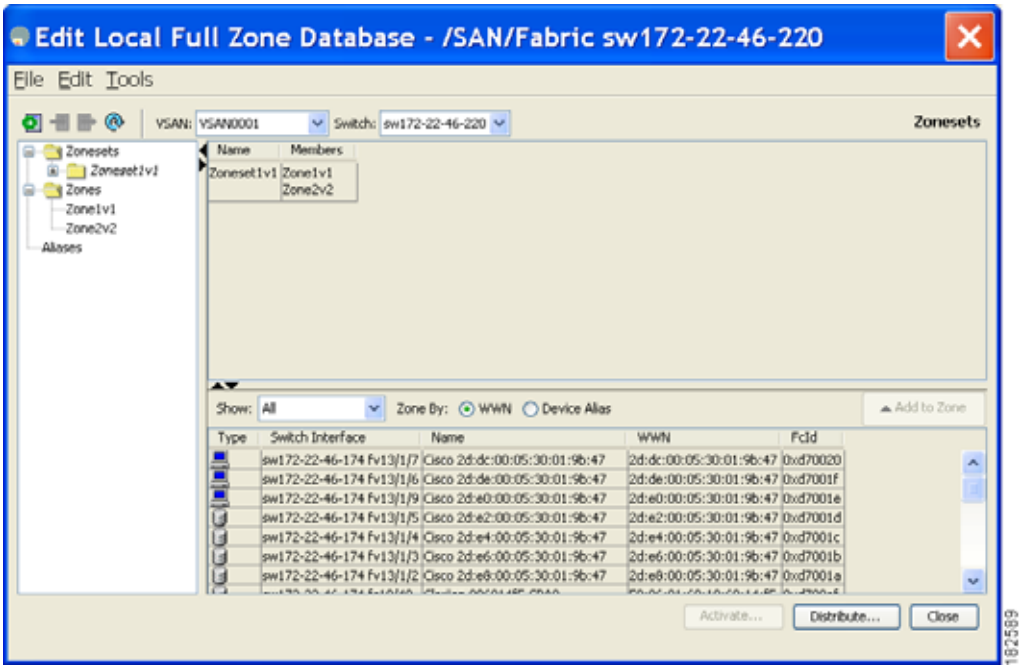
ステップ 1　[Zone] > [Edit Local Full Zone Database] を選択します。

[Select VSAN] ダイアログボックスが表示されます。

ステップ 2　VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます（図 5-35 を参照）。

図 5-35　[Edit Local Full Zone Database] ダイアログボックス



ステップ 3　左側のペインでゾーンまたはゾーン セットをクリックします。

ステップ 4　[Edit] > [Rename] を選択します。

ゾーンまたはゾーン セット名の周囲にエディット ボックスが表示されます。

ステップ 5　新しい名前を入力します。

ステップ 6　[Activate] または [Distribute] をクリックします。

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する手順は、次のとおりです。

ステップ 1　[Zone] > [Edit Local Full Zone Database] を選択します。

[Select VSAN] ダイアログボックスが表示されます。

ステップ 2　VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 3　[Edit] > [Clone] を選択します。

[Clone Zoneset] ダイアログボックスが表示されます（図 5-36 を参照）。デフォルトの名前は Clone の後ろに元の名前が付きます。

図 5-36　[Clone Zoneset] ダイアログボックス

ステップ 4　コピーされたエントリの名前を変更します。

ステップ 5　[OK] をクリックして新しいコピーを保存します。

コピーされたデータベースは、元のデータベースとともに表示されます。

MDS 以外のデータベースの移行

Zone Migration ウィザードを使用して Fabric Manager を使用した MDS 以外のデータベースを移行する手順は、次のとおりです。

ステップ 1　[Zone] > [Migrate Non-MDS Database] を選択します。

Zone Migration ウィザードが表示されます。

ステップ 2　ウィザードのプロンプトに従って、データベースを移行します。

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 データベースのクリアについては、『*Cisco MDS 9000 Family CLI Configuration Guide*』を参照してください。

（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。

（注）　ゾーン サーバ データベースをクリアした後に、明示的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、スイッチの再起動時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。

詳細なゾーン属性

ここでは詳細なゾーン属性について、次の内容を説明します。

ゾーンベースのトラフィック プライオリティの概要

ゾーン分割機能は、ファブリック内の特定のゾーンのプライオリティを設定し、デバイス間のアクセス制御を設定するための追加の分離メカニズムを提供します。この機能を使用して、Quality Of Service（QoS）プライオリティをゾーン属性として設定できます。QoS トラフィックプライオリティを high、medium、または low に割り当てることができます。デフォルトでは、プライオリティが指定されていないゾーンは暗黙的に low プライオリティを割り当てられます。詳細については、『*Cisco MDS 9000 NX-OS Family Quality of Service Configuration Guide*』を参照してください。

この機能を使用するには、ENTERPRISE_PKG ライセンスを取得し（『*Cisco NX-OS Family Licensing Guide*』を参照）、スイッチで QoS をイネーブルにする必要があります（『*Cisco MDS 9000 Family NX-OS Quality of Service Configuration Guide*』を参照）。

この機能により、SAN 管理者は使い慣れたデータ フロー識別パラダイムの観点から QoS を設定できます。この属性は、ゾーン メンバーごとではなく、ゾーン全体で設定できます。

注意　ゾーンベースの QoS がスイッチで実装される場合、その VSAN で interop モードを設定することはできません。

ゾーンベースのトラフィック プライオリティの設定

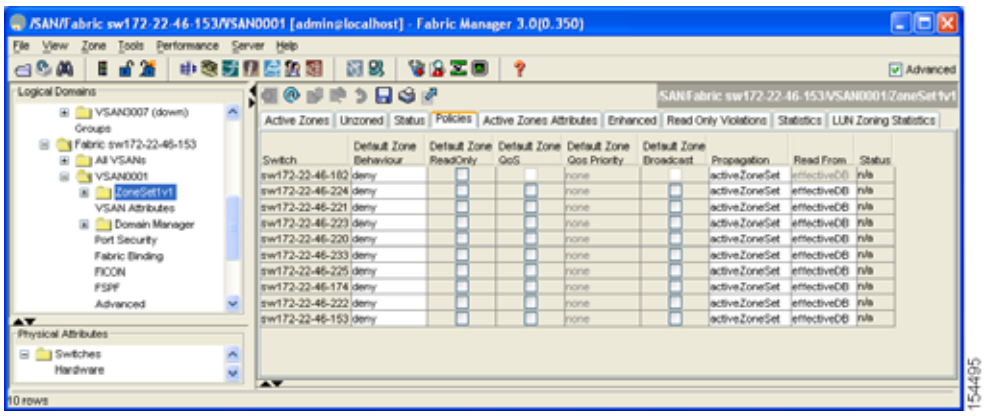
Fabric Manager を使用してゾーン プライオリティを設定する手順は、次のとおりです。

ステップ 1　VSAN を開き、[Logical Domains] ペインで、ゾーン セットを選択します。

ステップ 2　[Information] ペインで [Policies] タブをクリックします。

[Information] ペインにゾーン ポリシー情報が表示されます（図 5-37 を参照）。

図 5-37　[Information] ペインの [Zone Policies] タブ



ステップ 3　チェックボックスとドロップダウン メニューを使用して、デフォルト ゾーンの QoS を設定します。

ステップ 4　[Apply Changes] をクリックして、変更を保存します。

デフォルト ゾーンの QoS プライオリティ属性の設定

QoS プライオリティ属性の設定変更は、関連付けられたゾーンのゾーン セットをアクティブ化したときに有効になります。

（注）　メンバーが QoS プライオリティ属性が異なる 2 つのゾーンの一部の場合は、より高い QoS プライオリティ値が実装されます。最初の一致エントリが実装されるので、VSAN ベースの QoS ではこの状況は発生しません。

Fabric Manager を使用してデフォルト ゾーンの QoS プライオリティ属性を設定する手順は、次のとおりです。

ステップ 1　[Zone] > [Edit Local Full Zone Database] を選択します。

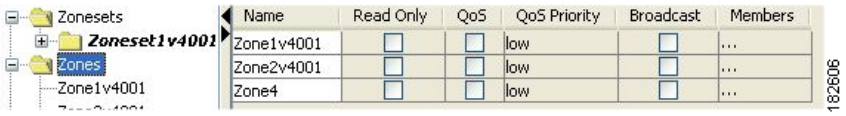
[Select VSAN] ダイアログボックスが表示されます。

ステップ 2　VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 3　デフォルト ゾーンに QoS プライオリティ属性を設定するには、[Edit] > [Edit Default Zone Attributes] を選択します（図 5-38 を参照）。

図 5-38　QoS プライオリティ属性



ステップ 4　[Permit QoS Traffic with Priority] チェックボックスをオンにし、[Qos Priority] ドロップダウン メニューを [low]、[medium]、または [high] に設定します。

ステップ 5　[OK] をクリックして変更を保存します。

デフォルト ゾーン ポリシーの設定

Fabric Manager を使用してデフォルト ゾーン内のトラフィックを許可または拒否する手順は、次のとおりです。

ステップ 1　[Zone] > [Edit Local Full Zone Database] を選択します。

[Select VSAN] ダイアログボックスが表示されます。

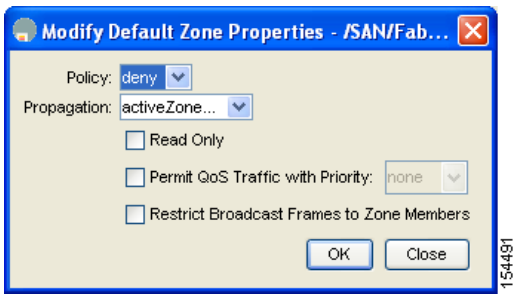
ステップ 2　VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 3　デフォルト ゾーンに QoS プライオリティ属性を設定するには、[Edit] > [Edit Default Zone Attributes] を選択します。

図 5-39 に示す [Modify Default Zone Properties] ダイアログボックスが表示されます。

図 5-39　[Modify Default Zone Properties] ダイアログボックス



ステップ 4　デフォルト ゾーンでトラフィックを許可するには [Policy] ドロップダウン メニューを [permit] に設定し、デフォルト ゾーンでトラフィックをブロックするには [deny] に設定します。

ステップ 5　[OK] をクリックして変更を保存します。

ブロードキャスト ゾーン分割の概要

（注）　ブロードキャスト ゾーン分割は、Cisco Fabric Switch for HP c-Class BladeSystem および Cisco Fabric Switch for IBM BladeCenter ではサポートされていません。

基本ゾーン分割モードでブロードキャスト フレームを設定できます。デフォルトでは、ブロードキャスト ゾーン分割はディセーブルになっており、ブロードキャスト フレームは VSAN 内のすべての Nx ポートに送信されます。イネーブルの場合、ブロードキャスト フレームは発信側と同じゾーンまたは複数のゾーンだけに送信されます。ブロードキャスト ゾーン分割は、ホストまたはストレージ デバイスがこの機能を使用する場合にイネーブルにします。

表 5-2 に、ブロードキャスト フレームの配信規則を示します。

表 5-2　ブロードキャスト要件

アクティブなゾーン分割？	ブロードキャストがイネーブル？	フレームのブロードキャスト？	説明
はい	はい	はい	ブロードキャスト フレームの発信元とブロードキャスト ゾーンを共有するすべての Nx ポートにブロードキャストします。
いいえ	はい	はい	すべての Nx ポートにブロードキャストします。
はい	いいえ	いいえ	ブロードキャストはディセーブルです。

ヒント　FL ポートに接続されている NL ポートがブロードキャスト フレームの発信元とブロードキャスト ゾーンを共有する場合、フレームはループ内のすべてのデバイスにブロードキャストされます。

注意　スイッチでブロードキャスト ゾーン分割がイネーブルになっている場合、その VSAN で interop モードを設定することはできません。

ブロードキャスト ゾーン分割の設定

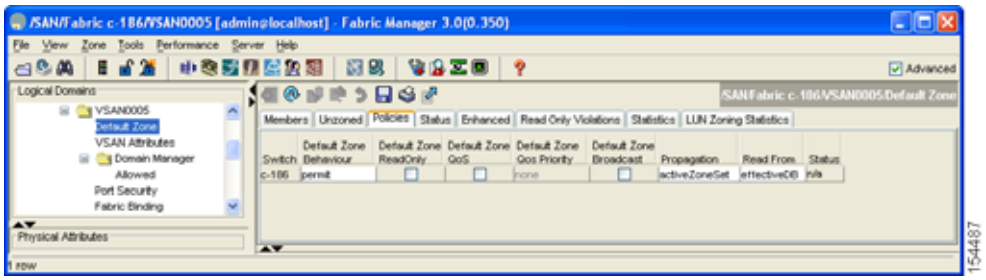
Fabric Manager を使用して基本ゾーン分割モードでフレームをブロードキャストする手順は、次のとおりです。

ステップ 1　VSAN を開き、[Logical Domains] ペインで、ゾーン セットを選択します。

ステップ 2　[Information] ペインで [Policies] タブをクリックします。

[Information] ペインにゾーン ポリシー情報が表示されます（図 5-40 を参照）。

図 5-40　ゾーン ポリシー情報



ステップ 3　[Broadcast] チェックボックスをオンにして、デフォルト ゾーンのブロードキャスト フレームをイネーブルにします。

ステップ 4　[Apply Changes] をクリックして、変更を保存します。

LUN ゾーン分割の概要

Logical Unit Number（LUN）ゾーン分割は、Cisco MDS 9000 ファミリのスイッチ固有の機能です。

注意　LUN ゾーン分割は、Cisco MDS 9000 ファミリ スイッチでだけ実装できます。LUN ゾーン分割が実装されているスイッチでは、interop モードを設定できません。

ストレージ デバイスは、その背後に複数の LUN を持つことができます。デバイス ポートがゾーンの一部である場合、ゾーンのメンバーはデバイス内のすべての LUN にアクセスできます。LUN ゾーン分割では、アクセスをデバイスと関連付けられている特定の LUN に制限できます。

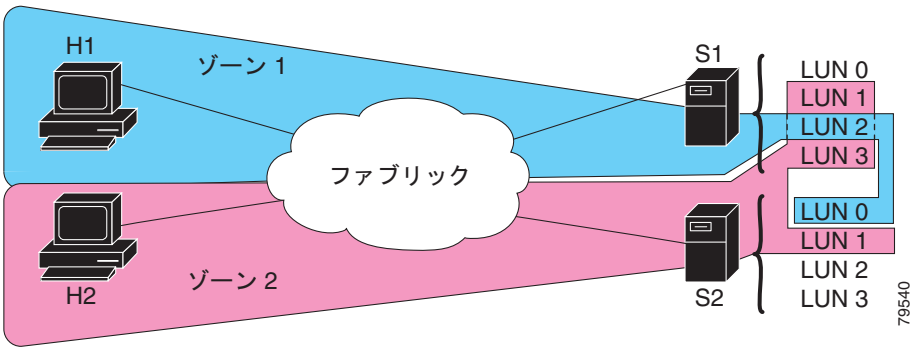
（注）　LUN 0 がゾーン内に含まれていない場合、標準要件により、LUN 0 への制御トラフィック（REPORT_LUNS、INQUIRY など）はサポートされますが、LUN 0 へのデータ トラフィック（READ、WRITE など）は拒否されます。

- ホスト H1 は、S1 内の LUN 2、および S2 内の LUN 0 にアクセスできます。S1 または S2 のその他の LUN にはアクセスできません。
- ホスト H2 は、S1 内の LUN 1 と 3、および S2 内の LUN 1 だけにアクセスできます。S1 または S2 のその他の LUN にはアクセスできません。

（注）　ゾーン分割されていない LUN は、自動的にデフォルト ゾーンのメンバーになります。

図 5-41 に、LUN ベースのゾーン分割の例を示します。

図 5-41　LUN ゾーン分割でのアクセス



LUN ベースのゾーンの設定

Fabric Manager を使用して LUN ベースのゾーンを設定する手順は、次のとおりです。

ステップ 1　[Zone] > [Edit Local Full Zone Database] を選択します。

[Select VSAN] ダイアログボックスが表示されます。

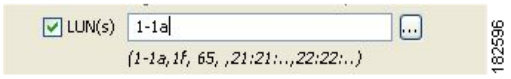
ステップ 2　VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 3　メンバーを追加するゾーンをクリックし、[Insert] アイコンをクリックします。

図 5-42 に示す [Add Member to Zone] ダイアログボックスが表示されます。

図 5-42　[Add Member to Zone] ダイアログボックス



ステップ 4　[Zone By] オプションから [WWN] または [FCID] ラジオ ボタンをクリックして、LUN ベースのゾーンを作成します。

ステップ 5　[LUN] チェックボックスをオンにし、参照ボタンをクリックして LUN を設定します。

ステップ 6　[Add] を追加して、この LUN ベースのゾーンを追加します。

ストレージ サブシステムへの LUN の割り当て

LUN のマスキングおよびマッピングは、サーバ アクセスを特定の LUN に制限します。LUN マスキングがストレージ サブシステムでイネーブルになっていて、Cisco MDS 9000 ファミリ スイッチで追加の LUN ゾーン分割を実行する場合は、ストレージ サブシステムから各 HBA（ホスト バス アダプタ）の LUN 番号を取得し、「LUN ベースのゾーンの設定」（P.5-46）の手順に従って LUN ベースのゾーンを設定します。

（注）　各 HBA の LUN 番号の取得については、該当のユーザ マニュアルを参照してください。

注意　LUN の割り当てを誤ると、データが失われる場合があります。

読み取り専用ゾーンの概要

デフォルトでは、発信側は、発信側とターゲットが同じファイバ チャネル ゾーンのメンバーである場合、ターゲットのメディアへの読み取りアクセスと書き込みアクセスの両方を持ちます。読み取り専用ゾーン機能により、メンバーが読み取り専用のファイバ チャネル ゾーン内のメディアに対して読み取りアクセスだけを持つようにすることができます。

LUN ゾーンを読み取り専用ゾーンとして設定することもできます。

どのゾーンも読み取り専用ゾーンとして識別できます。デフォルトでは、すべてのゾーンは、読み取り専用ゾーンとして明示的に設定されていない限り、読み取りと書き込みの両方のアクセス権限を持ちます。

読み取り専用ゾーンを設定するときは、次の注意事項に従ってください。

- 読み取り専用ゾーンが実装されている場合、スイッチはゾーン内のユーザ データへの書き込みアクセスを阻止します。
- 2 つのメンバーが読み取り専用ゾーンと読み取りと書き込みゾーンに属する場合は、読み取り専用ゾーンが優先され、書き込みアクセスは拒否されます。
- LUN ゾーン分割は、Cisco MDS 9000 ファミリ スイッチでだけ実装できます。LUN ゾーン分割が実装されているスイッチでは、interop モードを設定できません。
- 読み取り専用ボリュームは、オペレーティング システムとファイル システムの一部の組み合わせではサポートされていません（Windows NT または Windows 2000 と NTFS ファイル システムなど）。このようなホストからは、読み取り専用ゾーン内のボリュームを利用できません。ただし、読み取り専用ゾーンがアクティブ化された時点ですでに起動されていたホストは、読み取り専用ボリュームを利用できます。

  読み取り専用ゾーン機能は、FAT16 または FAT32 ファイル システムが前述の Windows オペレーティング システムと組み合わせて使用されている場合は、設計どおりに動作します。

読み取り専用ゾーンの設定

Fabric Manager を使用して読み取り専用ゾーンを設定する手順は、次のとおりです。

ステップ 1　[Zone] > [Edit Local Full Zone Database] を選択します。

[Select VSAN] ダイアログボックスが表示されます。

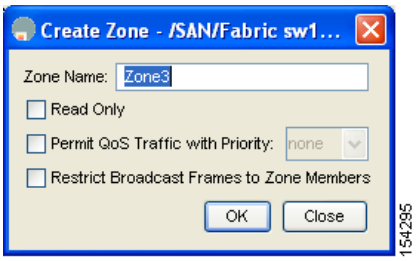
ステップ 2　VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 3　左側のペインの [Zones] をクリックし、[Insert] アイコンをクリックして、ゾーンを追加します。

[Create Zone] ダイアログボックスが表示されます（図 5-43 を参照）

図 5-43　[Create Zone] ダイアログボックス



ステップ 4　[Read Only] チェックボックスをオンにして読み取り専用ゾーンを作成します。

ステップ 5　[OK] をクリックします。

（注）　デフォルト ゾーンの読み取り専用オプションの設定については、「デフォルト ゾーン ポリシーの設定」（P.5-43）を参照してください。

ゾーン情報の表示

Fabric Manager を使用してゾーン情報と統計情報を表示する手順は、次のとおりです。

ステップ 1　VSAN を開き、[Logical Domains] ペインで、ゾーン セットを選択します。

[Information] ペインにゾーンの設定が表示されます。

ステップ 2　[Read Only Violations]、[Statistics] タブ、または [LUN Zoning Statistics] タブをクリックして、選択されたゾーンの統計情報を表示します。

拡張ゾーン分割

ゾーン分割機能は FC-GS-4 および FC-SW-3 標準に準拠しています。どちらの標準も前セクションで説明した基本ゾーン分割機能と本セクションで説明する拡張ゾーン分割機能をサポートしています。

ここで説明する内容は、次のとおりです。

拡張ゾーン分割の概要

表 5-3 に、Cisco MDS 9000 ファミリ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 5-3　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、管理者は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、サイズの縮小も顕著になります。
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 ゾーン設定の実行および交換を行います。	ポリシーがファブリック全体に適用されるため、トラブルシューティングの時間が短縮されます。
スイッチ単位でのアクティブ化の結果を取得するため、管理スイッチはアクティブ化に関する複合ステータスを提供します。この場合、障害のあるスイッチは特定されません。	各リモート スイッチからアクティブ化の結果と問題の特性を取得します。	エラー通知機能が強化されているため、トラブルシューティングが容易です。
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 スイッチとリモート スイッチのハード ゾーン分割のハードウェア変更が影響を受ける場合があります。	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 セットを配信するため、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。

表 5-3　拡張ゾーン分割の利点 （続き）

基本ゾーン分割	拡張ゾーン分割	拡張ゾーン分割の利点
MDS 固有のゾーン メンバー タイプ（IPv4 アドレス、IPv6 アドレス、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場合があります。マージ時に、MDS 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可能性があります。	メンバー 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。
シスコでは interop モードのときに限り、fWWN ベースのゾーン メンバシップがサポートされます。	標準 interop モード（interop モード 1）で fWWN ベースのメンバシップをサポートします。	fWWN ベースのメンバー 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

基本ゾーン分割モードから拡張ゾーン分割モードに変更する手順は、次のとおりです。

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できることを確認します。

1 つまたは複数のスイッチが拡張モードで動作できない場合、拡張モードへの移行要求は拒否されます。

ステップ 2　動作モードを拡張ゾーン分割モードに設定します。この操作を行うことにより、セッションが自動的に開始され、ファブリック全体のロックが取得され、拡張ゾーン分割データ構造を使用するアクティブおよびフル ゾーン分割データベースが配信され、ゾーン分割ポリシーが配信され、ロックが解除されます。ファブリック内のすべてのスイッチは、拡張ゾーン分割モードに移行します。

ヒント　基本ゾーン分割から拡張ゾーン分割への移行が完了したら、実行コンフィギュレーションを保存することを推奨します。

拡張ゾーン分割から基本ゾーン分割への変更

標準では、基本ゾーン分割に変更することを許可していません。ただし、Cisco MDS スイッチではこの変更を許可し、その他の Cisco SAN-OS または 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しています。

拡張ゾーン分割モードから基本ゾーン分割モードに変更する手順は、次のとおりです。

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。

このような設定が存在する場合は、この手順を進める前にこれらの設定を削除します。既存の設定は、削除しておかなくても Cisco NX-OS ソフトウェアにより自動的に削除されます。

ステップ 2　動作モードを基本ゾーン分割モードに設定します。この操作を行うことによって、セッションが自動的に開始され、ファブリック全体のロックが取得され、基本ゾーン分割データ構造を使用するゾーン分割情報が配信され、設定変更が適用され、ファブリック内のすべてのスイッチのロックが解除されます。ファブリック内のすべてのスイッチは、基本ゾーン分割モードに移行します。

（注）　拡張ゾーン分割をイネーブルにして Cisco SAN-OS Release 2.0(1b) および NX-OS 4(1b) 以降を実行しているスイッチが Cisco SAN-OS Release 1.3(4) 以前にダウングレードされた場合、スイッチは基本ゾーン分割モードになり、ファブリックに参加できません。これは、ファブリック内のその他すべてのスイッチが拡張ゾーン分割モードのままであるためです。

拡張ゾーン分割のイネーブル化

デフォルトでは、拡張ゾーン分割機能は Cisco MDS 9000 ファミリのすべてのスイッチでディセーブルです。

Fabric Manager を使用して VSAN 上で拡張ゾーン分割をイネーブルにする手順は、次のとおりです。

ステップ 1　VSAN を開き、[Logical Domains] ペインで、ゾーン セットを選択します。

[Information] ペインにゾーン セットの設定が表示されます。

ステップ 2　[Enhanced] タブをクリックします。

現在の拡張ゾーン分割設定が表示されます。

ステップ 3　[Action] ドロップダウン メニューから、[enhanced] を選択して、この VSAN で拡張ゾーン分割をイネーブルにします。

ステップ 4　[Apply Changes] をクリックして、変更を保存します。

属性グループの作成

拡張モードでは、属性グループを使用して属性を直接設定できます。

属性グループの設定については、『*Cisco MDS 9000 Family CLI Configuration Guide*』を参照してください。

データベースのマージ

マージの動作は、ファブリック全体のマージ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、表 5-4 で指定されたマージ規則を使用してマージされます。

表 5-4　データベースのゾーン マージ ステータス

ローカル データベース	隣接データベース	マージ ステータス	マージ結果
データベースに、名前は同じであるが[1]、ゾーン、エイリアス、および属性グループの異なるゾーン セットが含まれる。		成功	ローカル データベースおよび隣接データベースの結合。
データベースに、名前は同じ [1] であるが、メンバーの異なるゾーン、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る。		失敗	ISL は分離されます。
空	データあり	成功	隣接データベース情報がローカル データベースに読み込まれます。
データあり	空	成功	ローカル データベース情報が隣接データベースに読み込まれます。

1. 拡張ゾーン分割モードで、アクティブ ゾーン セットは interop モード 1 で名前を持ちません。ゾーン セット名は、フル ゾーン セットでだけ存在します。

注意　隣接ファブリックで FabricWare を実行している Cisco MDS 9020 スイッチがある場合は、ファブリックをマージする前に Cisco SAN-OS を実行しているすべての MDS スイッチで pWWN 以外のすべてのタイプを削除してください。

マージ プロセスは次のように動作します。

1. 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。
2. プロトコル バージョンが同じ場合、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。
3. ゾーン マージ オプションが同じである場合、マージ制御設定に基づいて比較が行われます。
   a. 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。同じでない場合、リンクは分離されます。
   b. 設定が「許可」の場合、マージ規則を使用してマージが行われます。

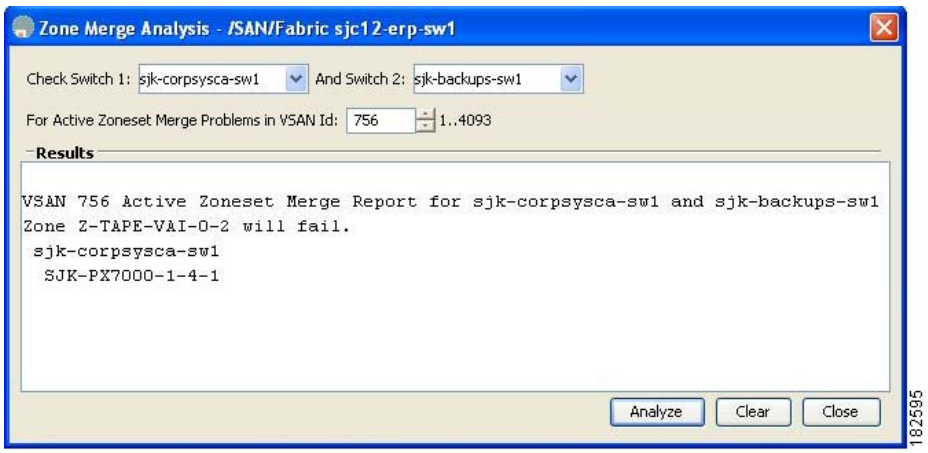
ゾーン マージの分析

Fabric Manager を使用してゾーン マージの分析を実行する手順は、次のとおりです。

ステップ 1　[Zone] > [Merge Analysis] を選択します。

図 5-44 に示す [Zone Merge Analysis] ダイアログボックスが表示されます。

図 5-44　[Zone Merge Analysis] ダイアログボックス



ステップ 2　[Check Switch 1] ドロップダウン リストで、最初に分析するスイッチを選択します。

ステップ 3　[And Switch 2] ドロップダウン リストで、2 番めに分析するスイッチを選択します。

ステップ 4　[For Active Zoneset Merge Problems in VSAN Id] フィールドに、ゾーン セット マージに失敗した VSAN の ID を入力します。

ステップ 5　[Analyze] をクリックして、ゾーン マージを分析します。

ステップ 6　[Zone Merge Analysis] ダイアログボックスから分析データをクリアするには、[Clear] をクリックします。

ゾーン マージ制御ポリシーの設定

マージ制御ポリシーの設定については、『*Cisco MDS 9000 Family CLI Configuration Guide*』を参照してください。

ゾーンの Generic Service アクセス権限設定は、Generic Service（GS）インターフェイス経由でのゾーン分割操作を制御するために使用されます。ゾーンの Generic Service アクセス権限は、読み取り専用、読み取りと書き込み、またはなし（拒否）にすることができます。

Generic Service（GS）設定を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# config t`	設定モードに入ります。

ステップ 2

`switch(config)# zone gs read vsan 3000`	gs のアクセス権限の値を、指定された VSAN で読み取り専用として設定します。
`switch(config)# zone gs read-write vsan 3000`	gs のアクセス権限の値を、指定された VSAN で読み取りと書き込みとして設定します。
`switch(config)# no zone gs read-write vsan 3000`	gs のアクセス権限の値を、指定された VSAN でなし（拒否）として設定します。

ダウングレード用のゾーン データベースの圧縮

Cisco SAN-OS Release 3.0(1) 以前では、VSAN あたり 2000 ゾーンだけがサポートされます。VSAN に 2000 を超えるゾーンを追加した場合、以前のリリースにダウンロードすると制限超過分のゾーンが失われる可能性のあることを示す、コンフィギュレーション チェックが登録されます。コンフィギュレーション チェックを回避するには、超過分のゾーンを削除し、VSAN のゾーン データベースを圧縮します。超過分のゾーンを削除した後、ゾーン数が 2000 以下になれば、圧縮プロセスによって新しい内部ゾーン ID が割り当てられ、設定は Cisco SAN-OS Release 2.x 以前によってサポートされます。この手順は、2000 を超えるゾーンを含む、スイッチ上のすべての VSAN で実行します。

（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、その隣接スイッチがサポートしていない場合、マージは失敗します。また、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。

ダウングレード用のゾーン データベースの圧縮については、『*Cisco MDS 9000 Family CLI Configuration Guide*』を参照してください。

デフォルト設定

表 5-5 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 5-5　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	すべてのメンバーで拒否。
フル ゾーン セット配信	フル ゾーン セットは配信されません。
ゾーン ベースのトラフィック プライオリティ	低。
読み取り専用ゾーン	すべてのゾーンで読み取りと書き込み属性。
ブロードキャスト フレーム	すべての Nx ポートに送信。
ブロードキャスト ゾーン分割	ディセーブル。
拡張ゾーン分割	ディセーブル。

CHAPTER 6

デバイス エイリアス サービスの配信

Cisco MDS 9000 ファミリのすべてのスイッチは、VSAN 単位およびファブリック全体での Distributed Device Alias Service（デバイス エイリアス）をサポートしています。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。

この章の内容は、次のとおりです。

デバイス エイリアスの概要

Cisco MDS 9000 ファミリ スイッチで機能（ゾーン分割、QoS、ポート セキュリティなど）を設定するために、デバイスの port WWN（pWWN）を指定する必要がある場合は、これらの機能を設定するたびに、正しいデバイス名を割り当てる必要があります。デバイス名が正しくないと、予期しない結果が生じることがあります。この問題を回避するには、わかりやすいポート WWN 名を定義し、必要に応じて、この名前をすべての設定コマンドで使用します。この章では、これらのわかりやすい名前を*デバイス エイリアス*と表します。

デバイス エイリアス モードの概要

デバイス エイリアスは、基本モードと拡張モードの 2 つをサポートしています。

- デバイス エイリアスは、基本モードで 3.0 スイッチ上のアプリケーションなどのすべてのアプリケーション機能を実行します。デバイス エイリアスを使用して基本モードを設定すると、アプリケーションは即座に pWWN に拡張します。この処理は、モードが拡張モードに変更されるまで続行されます。
- デバイス エイリアスが拡張モードで実行されると、すべてのアプリケーションはネイティブ フォーマットでデバイス エイリアス設定を受け付けます。デバイス エイリアス名は設定に格納され、デバイス エイリアス フォーマットで配信されます（pWWN には拡張されません）。アプリケーションは、デバイス エイリアス データベースの変更を追跡し、変更を適用するための処理を行います。

ネイティブ デバイス エイリアス設定は、interop モードの VSAN では受け付けられません。IVR ゾーンセットのアクティブ化は、注入対象の対応する不明瞭なゾーンがネイティブ デバイス エイリアス メンバーでない場合、interop モードの VSAN で失敗します。

モード設定の変更

デバイス エイリアス モードが基本モードから拡張モードに変更されると、アプリケーションはこの変更について通知されます。アプリケーションでは、ネイティブ フォーマットでデバイス エイリアス ベース設定を受け付け始めます。

（注） デバイス エイリアスは以前に基本モードで実行されていたため、アプリケーションには前のネイティブ デバイス エイリアス設定はありません。

アプリケーションはネイティブ フォーマットの既存のデバイス エイリアス設定をチェックします。デバイス エイリアスがネイティブ フォーマットである場合、アプリケーションは要求を拒否し、デバイス エイリアス モードを基本に変更できません。

すべてのネイティブのデバイス エイリアス設定（ローカル スイッチとリモート スイッチの両方を含む）が明示的に削除されるか、またはモードを基本モードに戻す前にすべてのデバイス エイリアス メンバーが対応する pWWN に置き換えられる必要があります。

プロセスは force オプションを使用して自動化することができます。アプリケーションですべてのデバイス エイリアス メンバーを対応する pWWN に自動的に置き換えられるようにするには、**no device-alias mode enhanced force** コマンドを使用します。デバイス エイリアス メンバーがデバイス エイリアス データベース内に対応する pWWN マッピングを持っていない場合、設定は削除されます。

デバイス エイリアス モード配信

デバイス エイリアス配信が有効になっていると、モードの変更があった場合は常に、デバイス エイリアスがネットワーク内の他のスイッチに配信されます。すべてのスイッチが Release 3.1 にアップグレードされない限り、基本から拡張にモードを変更できません。ファブリック全体が Release 3.1 にアップグレードされない限り、デバイス エイリアスの機能拡張は適用されません。

（注） すべてのスイッチが Release 3.1 にアップグレードされたときは、自動的に拡張モードに変換できません。必ずしも拡張モードに変更する必要はなく、基本モードで作業を続けることができます。

デバイス エイリアスのマージ

異なるデバイス エイリアス モードで稼動している 2 つのファブリックを連結しても、デバイス エイリアスはマージされません。マージ プロセス中に、モードの自動変換は発生しません。この問題は解決する必要があります。

（注）　Release 3.0 スイッチは基本モードで動作します。

アプリケーション レベルでは、マージはアプリケーションとファブリックの間で行われます。たとえば、ゾーン マージは E ポートが稼動しているときに発生し、IVR/PSM/DPVM マージは CFS が原因で発生します。このマージは、デバイス エイリアス マージに全面的に依存するわけではありません。

拡張されたファブリック上で実行されるアプリケーションは、ネイティブのデバイス エイリアス設定がある場合、マージに失敗します。他のファブリックがネイティブのデバイス エイリアスベース設定をサポートできるが、基本モードで実行されている場合でも、アプリケーションはマージに失敗します。この問題は解決する必要があります。デバイス エイリアス マージの問題が解決されたら、各アプリケーションをそれに応じて修正する必要があります。

マージおよびデバイス エイリアス モードの不一致の解決

2 つのファブリックが異なるモードで実行され、デバイス エイリアス マージがファブリック間で失敗する場合、1 つのモードまたはもう 1 つのモードを選択することにより、矛盾を解決できます。拡張モードを選択する場合、すべてのスイッチが少なくとも Release 3.1 バージョンで実行されていることを確認します。そうでない場合には、拡張モードを有効にできません。基本モードを選択した場合、拡張ファブリック上で実行されているアプリケーションはデバイス エイリアス マージに準拠している必要があります。

ネイティブのデバイス エイリアス設定がない場合、アプリケーション マージは成功しますが、モードの不一致のため、デバイス エイリアス マージは失敗します。

ネイティブのデバイス エイリアス設定が Release 3.1 スイッチからのアプリケーション上で試行されると、一部のアプリケーションでのデバイス エイリアス モードの不一致のために、コミットが拒否されます。

（注）　デバイス エイリアスが特定のスイッチ上で基本モードで実行されている場合、アプリケーションは SNMP 経由のネイティブのデバイス エイリアス設定を受け付けないようにする必要があります。

（注）　拡張モードが有効になると Confcheck が追加され、拡張モードが無効になると Confcheck は削除されます。ネイティブ フォーマットのデバイス エイリアス設定がある場合、アプリケーションは confcheck を追加する必要があります。設定が削除されたら、アプリケーションは confcheck を削除する必要があります。

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機能があります。

- デバイス エイリアスの情報は、VSAN 設定に依存しません。
- デバイス エイリアスの設定および配信は、ゾーン サーバおよびゾーン サーバ データベースに依存しません。
- データを失うことなく、レガシー 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 アプリケーションでは、Cisco Fabric Services（CFS）インフラストラクチャを使用して、データベースを効率的に管理および配信することができます。デバイス エイリアスでは調整済み配信モードが使用され、配信範囲はファブリック全体に及びます（『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照）。
- デバイス エイリアスを使用してゾーン、IVR ゾーン、または QoS 機能を設定した場合に、これらの設定を表示すると、自動的にそれぞれの pWWN とともにデバイス エイリアスが表示されます。

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前提条件があります。

- デバイス エイリアスの割り当て先にできるのは、pWWN だけです。
- pWWN とそれがマッピングされるデバイス エイリアスとの間のマッピングは、1 対 1 の関係になる必要があります。pWWN は 1 つのデバイス エイリアスにだけマッピングでき、デバイス エイリアスは 1 つの pWWN にだけマッピングできます。
- デバイス エイリアス名は、次の文字を含む、64 文字の英数字に制限されています。
  - a ～ z および 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）

ゾーン エイリアスと デバイス エイリアスの比較

表 6-1 に、ゾーンベース エイリアスとデバイス エイリアスの設定の違いを示します。

表 6-1　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 エイリアス	デバイス エイリアス
エイリアスは指定された VSAN に限定されます。	VSAN 番号を指定しなくても、デバイス エイリアスを定義できます。また、制限なしに、1 つ以上の VSAN 内で同じ定義を使用することもできます。
ゾーン エイリアスはゾーン分割設定の一部です。エイリアス マッピングは、他の機能の設定には使用できません。	デバイス エイリアスは、pWWN を使用する任意の機能と併用できます。

表 6-1　ゾーン エイリアスとデバイス エイリアスの比較 （続き）

ゾーンベース エイリアス	デバイス エイリアス
任意のゾーン メンバー タイプを使用して、エンド デバイスを指定できます。	pWWN は、IP アドレスなどの新しいデバイス エイリアスと使用するときだけサポートされます。
設定はゾーン サーバ データベースに格納されていて、他の機能には使用できません。	デバイス エイリアスはゾーン分割に限定されません。デバイス エイリアスの設定は、FCNS、ゾーン、fcping、traceroute、および IVR アプリケーションに使用できます。

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 エイリアス設定の許可および実装を行います。

- 有効データベース：ファブリックで現在使用されているデータベースです。
- 保留データベース：デバイス エイリアス設定に関する以降の変更内容は、保留データベースに格納されます。

この期間中はファブリックがロック状態になっているため、デバイス エイリアス設定を変更する場合は、変更をコミットするか、または破棄する必要があります。

ここでは、次の内容について説明します。

- 「デバイス エイリアス配信の概要」（P.6-5）
- 「変更のコミット」（P.6-8）
- 「変更の破棄」（P.6-8）
- 「レガシー ゾーン エイリアス設定の変換の概要」（P.6-8）

デバイス エイリアス配信の概要

デフォルトでは、デバイス エイリアス配信がイネーブルです。デバイス エイリアス機能は、調整済み配信メカニズムを使用して、変更をファブリック内のすべてのスイッチに配信します。

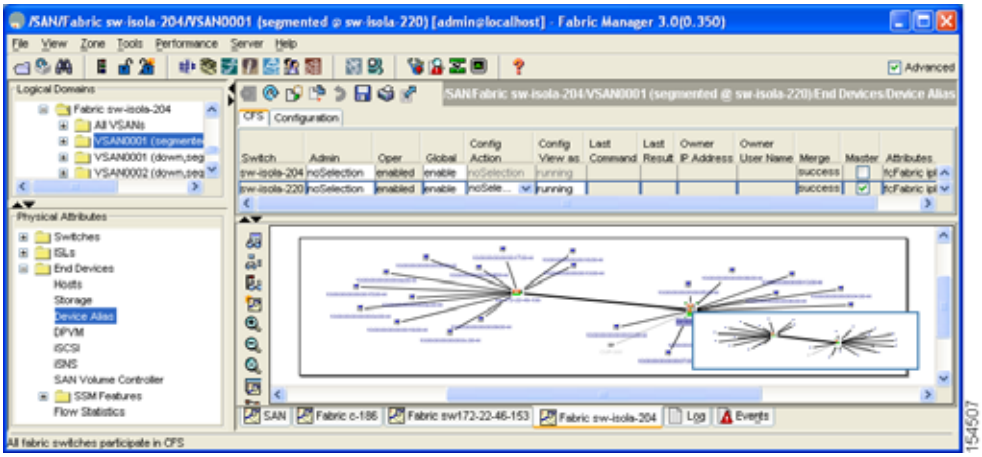
変更をコミットせずに配信をディセーブルにすると、コミット タスクは失敗します。

デバイス エイリアス データベースの配信

Fabric Manager を使用してデバイス エイリアス配信をイネーブルにする手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [End Devices] を展開し、[Device Alias] を選択します。
[Information] ペインにデバイス エイリアスの設定が表示されます（図 6-1 を参照）。

図 6-1　Fabric Manager 内のデバイス エイリアス



[CFS] タブがデフォルト タブです。

ステップ 2　スイッチ エイリアスをイネーブルにするには、[Global] ドロップダウン メニューから [enable] を選択します。

ステップ 3　新しくイネーブルにしたスイッチの [Config Action] ドロップダウン メニューから [commit] を選択します。

ステップ 4　これらの変更をコミットして配信する場合は、[Apply Changes] をクリックします。保存されていない変更を破棄する場合は、[Undo Changes] をクリックします。

デバイス エイリアスの作成の概要

最初のデバイス エイリアス タスクを実行すると、どのデバイス エイリアス タスクであるかに関係なく、デバイス エイリアス機能に対してファブリックが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。

- 他のユーザは、この機能の設定を変更できなくなります。
- 有効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。この時点からの変更は、保留データベースに対して行われます。保留データベースへの変更をコミットするかまたは破棄（**abort**）するまで、保留データベースは有効のままです。

デバイス エイリアスの作成

ファブリックをロックし、Fabric Manager を使用して保留データベースでデバイス エイリアスを作成する手順は、次のとおりです。

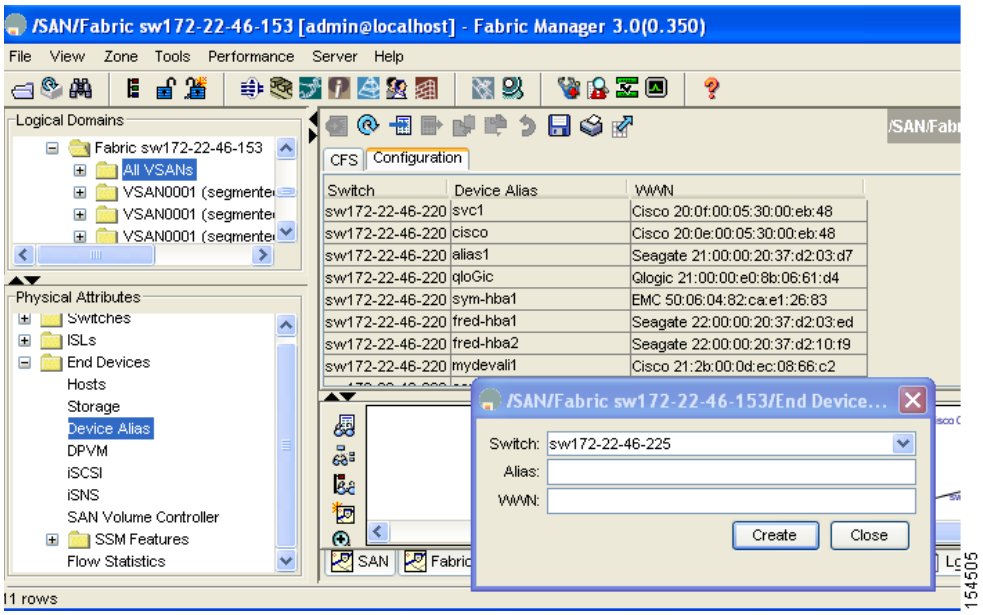
ステップ 1　[Physical Attributes] ペインで [End Devices] を展開し、[Device Alias] を選択します。

[Information] ペインにデバイス エイリアスの設定が表示されます。

ステップ 2　[Configuration] タブをクリックし、[Create Row] アイコンをクリックします。

[Device Alias Creation] ダイアログボックスが表示されます（図 6-2 を参照）。

図 6-2　[Create Device Alias] ダイアログボックス



ステップ 3　ドロップダウン メニューからスイッチを選択します。

ステップ 4　[Alias] フィールドおよび [pWWN] フィールドに入力します。

ステップ 5　このエイリアスを作成するには、[Create] をクリックします。保存されていない変更を破棄するには、[Close] をクリックします。

変更のコミット

保留データベースに対する変更をコミットすると、次のイベントが発生します。

1. 有効データベースの内容が、保留データベースの内容で上書きされます。
2. 保留データベースの内容が空になります。
3. この機能に対するファブリック ロックが解放されます。

Fabric Manager を使用して変更をデバイス エイリアス データベースにコミットする手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [End Devices] を展開し、[Device Alias] を選択します。

[Information] ペインにデバイス エイリアスの設定が表示されます。[CFS] タブがデフォルト タブです。

ステップ 2　スイッチ エイリアスをイネーブルにするには、[Global] ドロップダウン メニューから [enable] を選択します。

ステップ 3　新しくイネーブルにしたスイッチの [Config Action] ドロップダウン メニューから [commit] を選択します。

ステップ 4　これらの変更をコミットして配信する場合は、[Apply Changes] をクリックします。保存されていない変更を破棄する場合は、[Undo Changes] をクリックします。

変更の破棄

保留データベースに対する変更を破棄すると、次のイベントが発生します。

1. 有効データベースの内容はそのまま維持されます。
2. 保留データベースの内容が空になります。
3. この機能に対するファブリック ロックが解放されます。

Fabric Manager を使用してデバイス エイリアス セッションを破棄する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [End Devices] を展開し、[Device Alias] を選択します。

[Information] ペインにデバイス エイリアスの設定が表示されます。[CFS] タブがデフォルト タブです。

ステップ 2　[Config Action] ドロップダウン メニューから [abort] を選択します。

ステップ 3　[Apply Changes] をクリックして、セッションを破棄します。

レガシー ゾーン エイリアス設定の変換の概要

この機能を使用して、データを失うことなくレガシー ゾーン エイリアス設定をインポートできるのは、この設定が次の制限事項を満たす場合です。

- 各ゾーン エイリアスにメンバーが 1 つだけ存在する。
- メンバー タイプが pWWN である。

- ゾーン エイリアスの名前および定義は、既存のデバイス エイリアス名のものと同じであってはならない。

名前の競合がある場合、ゾーン エイリアスはインポートされません。

ヒント　ご使用の設定の要件に応じて、必要なゾーン 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。

インポート処理が完了したあとに、**commit** 処理を実行すると、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その他のすべてのスイッチに配信されます。この時点で、ファブリック内の他のスイッチに設定を配信する必要がない場合は、**abort** 処理を実行して、マージ変更内容をすべて破棄できます。

ここで説明する内容は、次のとおりです。

- 「デバイス エイリアスまたは FC エイリアスの使用」（P.6-9）
- 「デバイス エイリアス統計情報の消去」（P.6-10）

デバイス エイリアスまたは FC エイリアスの使用

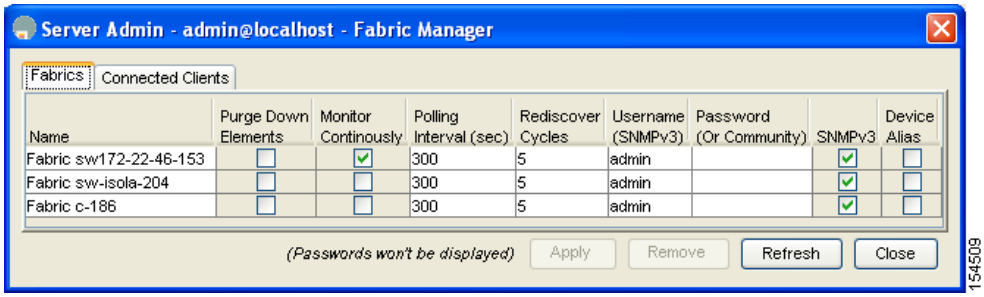
Fabric Manager Client では、Fabric Manager Server を再起動する必要なしに、Fabric Manager で使用するエイリアス（FC エイリアスまたはグローバル デバイス エイリアス）を変更できます。

Fabric Manager で FC エイリアスとグローバル デバイス エイリアスのどちらを使用するかを変更する手順は、次のとおりです。

ステップ 1　[Server] > [Admin] をクリックします。

[Admin] ダイアログボックスが表示されます（図 6-3 を参照）。

図 6-3　[Server Admin] ダイアログボックス



ステップ 2　グローバル デバイス エイリアスを使用する場合は、Fabric Manager Server で監視するファブリックごとに [Device Alias] チェックボックスをオンにします。FC エイリアスを使用する場合は、チェックボックスをオフにします。

ステップ 3　[Apply] をクリックして変更内容を保存するか、または [Close] をクリックして変更内容を保存せずにダイアログボックスを終了します。

デバイス エイリアス統計情報の消去

（デバッグの目的で）デバイス エイリアス統計情報を消去する方法については、『*Cisco MDS 9000 Family CLI Configuration Guide*』を参照してください。

データベース マージに関する注意事項

CFS マージのサポートの詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。

2 つのデバイス エイリアス データベースをマージする場合は、以下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 エイリアスが同じ pWWN にマッピングされていないことを確認します。
- 異なる 2 つの pWWN が同一のデバイス 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 エイリアスの総数が、8,191 個（8K）を超えていないことを確認してください。たとえば、データベース N に 6,000 個のデバイス エイリアスがあり、データベース M に 2,192 個のデバイス エイリアスがある場合、このマージ操作は失敗します。

インターフェイスの説明へのデバイス エイリアスの入力

エンド デバイスがスイッチにログインされていない場合、デバイス エイリアスはブランクになります。デバイスがログアウトされているときに FC ポートに接続することになっているデバイスを判別するために、デバイスのログイン中にインターフェイスの説明にデバイス エイリアスを入力できます。

インターフェイスの説明をデバイス エイリアスに入力する手順は、次のとおりです。

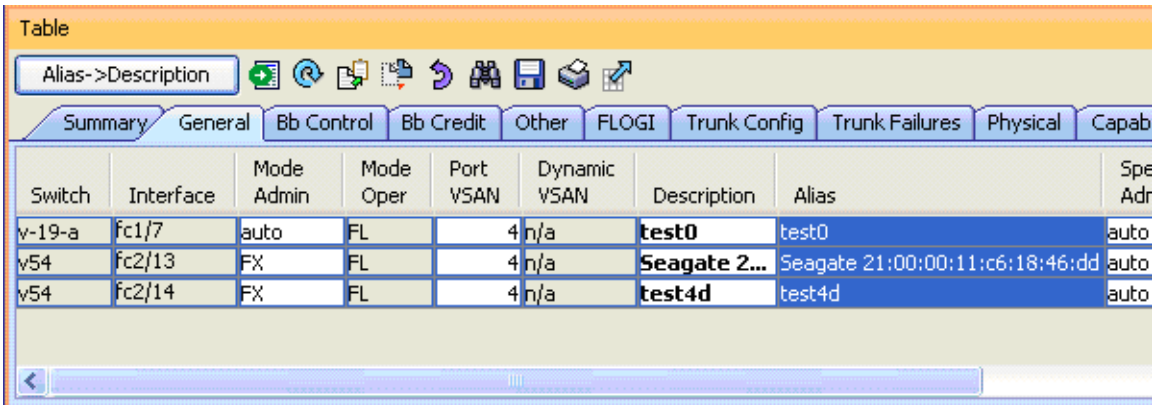
ステップ 1　[Physical Attributes] ペインで、[End Devices] を展開します。

ステップ 2　右側のペインで、[General] タブをクリックします。

ステップ 3　FC インターフェイスの行を選択します。

ステップ 4　[Alias] -> [Description] ボタンをクリックします。

図 6-4　デバイス エイリアスを [Interface Description] にコピーします。



ステップ 5　[commit] ボタンをクリックします。

デフォルト設定

表 6-2 に、デバイス エイリアスのパラメータの デフォルト設定を示します。

表 6-2　デバイス エイリアスのデフォルト パラメータ

パラメータ	デフォルト
使用中のデータベース	有効データベース
変更を受け入れるデータベース	保留データベース
デバイス エイリアス ファブリックのロック状態	最初のデバイス エイリアス タスクによってロックされる

CHAPTER 7

ファイバ チャネル ルーティング サービスおよびプロトコルの設定

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標準パス選択プロトコルです。FSPF 機能は、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。具体的に、FSPF は次の目的で使用されます。

- 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。
- 指定されたパスに障害が発生した場合に、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。

この章では、ファイバ チャネル ルーティング サービスおよびプロトコルの詳細を示します。この章の内容は、次のとおりです。

FSPF の概要

FSPF はファイバ チャネル ネットワークのルーティングに対応した、T11 委員会で現在標準化されているプロトコルです。FSPF プロトコルには次の特性および機能があります。

- マルチパス ルーティングをサポートします。
- パス ステータスはリンク ステート プロトコルによって決まります。
- ドメイン ID だけに基づいて、ホップ単位でルーティングします。
- FSPF が稼動するポートは E ポートまたは TE ポートに限られていて、トポロジはループ フリーです。
- VSAN 単位で稼動します。ファブリック内の指定 VSAN 内の接続は、この VSAN 内に設定されたスイッチに対してだけ保証されます。
- トポロジ データベースを使用して、ファブリック内のすべてのスイッチのリンク ステートを追跡し、各リンクにコストを関連付けます。
- トポロジが変更された場合、迅速な再コンバージェンスを保証します。標準ダイクストラ アルゴリズムを使用しますが、より強固で、効率的な増分ダイクストラ アルゴリズムを実行するための静的なダイナミック オプションがあります。ルート計算は VSAN 単位で実行されるため、再コンバージェンス時間は短く、効率的です。

FSPF の例

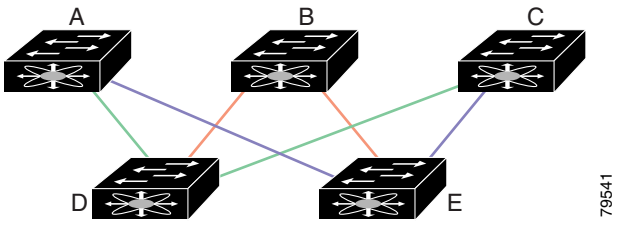
ここではトポロジおよびアプリケーションの例を使用して、FSPF の利点を示します。

（注）　FSPF 機能は任意のトポロジで使用できます。

フォールト トレラント ファブリック

図 7-1 に、部分メッシュ トポロジを使用するフォールト トレラント ファブリックを示します。ファブリック内でリンクが切断された場合でも、その切断位置に関係なく、ファブリック内のスイッチは他のどのスイッチとも通信できます。同様に、どのスイッチがダウンしても、ファブリックの残りの接続は維持されます。

図 7-1　　フォールト トレラント ファブリック



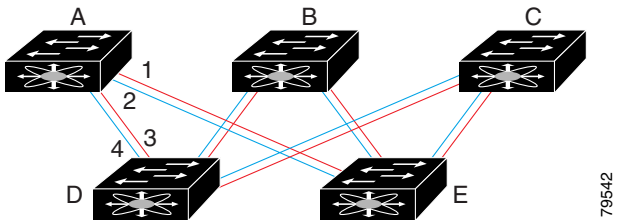
たとえば、すべてのリンクの速度が等しい場合、FSPF は A から C への同等パス 2 つ（緑色の A-D-C と青色の A-E-C）を計算します。

冗長リンク

図 7-1 のトポロジを改良するには、任意のスイッチ ペア間の接続をそれぞれ重複させます。スイッチ ペア間には、リンクを複数設定できます。図 7-2 に、この配置を示します。Cisco MDS 9000 ファミリのスイッチはポート チャネル機能をサポートしているため、物理リンクの各ペアは単一の論理リンクとして FSPF プロトコルに認識されます。

物理リンク ペアをバンドルすると、データベース サイズおよびリンク更新頻度が減るため、FSPF の効率が大幅に向上します。物理リンクを集約すると、障害は単一のリンクだけにとどまらずポート チャネル全体に波及します。このような設定は、ネットワークの復元力も向上します。ポート チャネルのリンクに障害が発生しても、ルートは変更されないため、ルーティング ループ、トラフィック消失、またはルート再設定のためのファブリック ダウンタイムが生じるリスクが軽減されます。

図 7-2　　冗長リンクを備えたフォールト トレラント ファブリック



たとえば、すべてのリンクの速度が等しく、ポートチャネルが存在しない場合、FSPF では A から C への同等パス 4 つ（A1-E-C、A2-E-C、A3-D-C、および A4-D-C）が計算されます。ポートチャネルが存在する場合、計算されるパスは 2 つに減ります。

ポートチャネルおよび FSPF リンクのフェールオーバー シナリオ

SmartBits トラフィック ジェネレータを使用して、図 7-3 に示されたシナリオを評価しました。スイッチ 1 とスイッチ 2 の間に存在する 2 つのリンクは、等コストの ISL リンクまたはポートチャネル リンクのどちらかです。トラフィック ジェネレータ 1 からトラフィック ジェネレータ 2 へのフローは、1 つ存在します。次のような 2 とおりのシナリオを想定して、100% の利用率、1 Gbps のトラフィックをテストしました。

- ケーブルを物理的に取り外して、トラフィック リンクをディセーブルにする（表 7-1 を参照）。
- スイッチ 1 またはスイッチ 2 のどちらか一方をシャットダウンする（表 7-2 を参照）。

図 7-3　　トラフィック ジェネレータを使用したフェールオーバー シナリオ

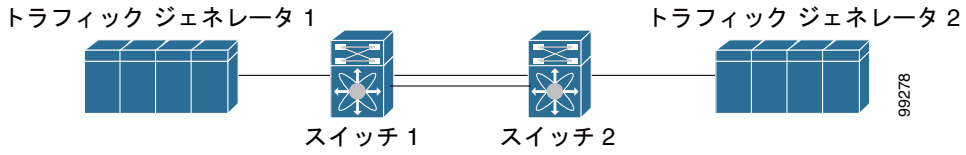


表 7-1　SmartBits ケーブルの物理的取り外しのシナリオ

ポートチャネル シナリオ		FSPF シナリオ（等コスト ISL）	
スイッチ 1	スイッチ 2	スイッチ 1	スイッチ 2
110 ミリ秒（削除フレーム数は 2 K 以下）		130+ ミリ秒（削除フレーム数は 4 K 以下）	
100 ミリ秒（標準の規定に従って信号損失を通知するときのホールド タイム）			

表 7-2　SmartBits スイッチのシャットダウン シナリオ

ポートチャネル シナリオ		FSPF シナリオ（等コスト ISL）	
スイッチ 1	スイッチ 2	スイッチ 1	スイッチ 2
～ 0 ミリ秒（削除フレーム数は 8 以下）	110 ミリ秒（削除フレーム数は 2 K 以下）	130+ ミリ秒（削除フレーム数は 4 K 以下）	
ホールド タイム不要	スイッチ 1 での信号損失	ホールド タイム不要	スイッチ 1 での信号損失

FSPF のグローバル設定

Cisco MDS 9000 ファミリのスイッチでは、FSPF はデフォルトでイネーブルです。

一部の FSPF 機能は、各 VSAN でグローバルに設定できます。VSAN 全体に機能を設定すると、コマンドごとに VSAN 番号を指定する必要がなくなります。このグローバル設定機能を使用すると、入力ミスや、その他のマイナーな設定エラーが発生する確率も少なくなります。

（注）　デフォルトで FSPF がイネーブルです。一般に、このような高度な機能を設定する必要はありません。

注意　バックボーン領域のデフォルトは 0（ゼロ）です。ご使用の領域がデフォルトと異なる場合を除き、この設定を変更する必要はありません。バックボーン領域を使用してシスコ製以外の製品で動作させている場合は、その製品の設定に適合するようにデフォルト値を変更できます。

ここで説明する内容は、次のとおりです。

SPF 計算ホールド タイムの概要

SPF 計算ホールド タイムは、VSAN 上の連続した 2 つの SPF 計算間の最小時間を設定します。小さな値を設定すると、FSPF が VSAN 上のパスを再計算して、すべてのファブリック変更への応答時間が短縮されます。SPF 計算ホールド タイムが小さいと、スイッチの CPU 使用時間が増加します。

Link State Records の概要

新しいスイッチをファブリックに追加するたびに、Link State Record（LSR）が隣接スイッチに送信されて、ファブリック全体にフラッディングされます。表 7-3 に、スイッチ応答に関するデフォルト設定を示します。

表 7-3　LSR のデフォルト設定

LSR オプション	デフォルト	説明
確認応答インターバル（RxmtInterval）	5 秒	スイッチが再送信までに LSR からの確認応答を待機する時間
リフレッシュ時間（LSRefreshTime）	30 分	スイッチが LSR リフレッシュを送信するまでの待機時間
最大有効期限（MaxAge）	60 分	スイッチがデータベースから LSR を削除するまでの待機時間

LSR 最小着信時間は、この VSAN で LSR アップデートを受信する間隔です。LSR 最小着信時間前に着信した LSR アップデートは、すべて破棄されます。

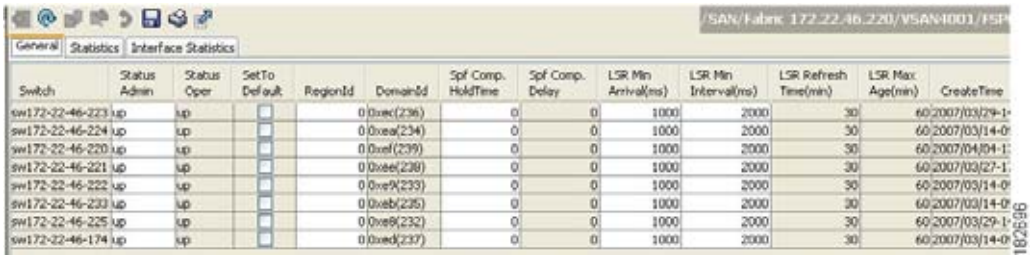
LSR 最小インターバルは、このスイッチが VSAN で LSR アップデートを送信する間隔です。

VSAN での FSPF の設定

Fabric Manager を使用して VSAN 全体に FSPF 機能を設定する手順は、次のとおりです。

ステップ 1　ファブリックを展開し、VSAN を展開して、**FSPF** を設定する VSAN に対して [FSPF] を選択します。[Information] ペインに FSPF 設定が表示されます（図 7-4 を参照）。

図 7-4　FSPF の一般情報



ステップ 2　RegionID、Spf Comp Holdtime、LSR Min Arrival、および LSR Min Interval の各フィールド値は、VSAN のすべてのインターフェイスに適用されます。ここで、フィールドの値を変更することも、あるいは値が存在しない場合は作成することもできます。

ステップ 3　変更内容を保存する場合は、[Apply Changes] をクリックします。保存されていない変更を破棄する場合は、[Undo Changes] をクリックします。

FSPF のデフォルト設定へのリセット

Fabric Manager を使用して FSPF VSAN のグローバル設定を出荷時のデフォルト設定に戻す手順は、次のとおりです。

ステップ 1　ファブリックを展開し、VSAN を展開して、FSPF を設定する VSAN に対して [FSPF] を選択します。[Information] ペインに FSPF 設定が表示されます（図 7-4 を参照）。

ステップ 2　スイッチの [SetToDefault] チェックボックスをオンにします。

ステップ 3　変更内容を保存する場合は、[Apply Changes] をクリックします。保存されていない変更を破棄する場合は、[Undo Changes] をクリックします。

FSPF のイネーブル化またはディセーブル化

Fabric Manager を使用して FSPF をイネーブルまたはディセーブルにする手順は、次のとおりです。

ステップ 1　ファブリックを展開し、VSAN を展開して、FSPF を設定する VSAN に対して [FSPF] を選択します。[Information] ペインに FSPF 設定が表示されます（図 7-4 を参照）。

ステップ 2　FSPF をイネーブルにする場合は、[Status Admin] ドロップダウン メニューを [up] に設定します。FSPF をディセーブルにする場合は、[down] に設定します

ステップ 3　変更内容を保存する場合は、[Apply Changes] をクリックします。保存されていない変更を破棄する場合は、[Undo Changes] をクリックします。

FSPF インターフェイスの設定

一部の FSPF コマンドはインターフェイス単位で使用できます。これらの設定手順は、特定の VSAN の特定のインターフェイスに適用されます。

ここで説明する内容は、次のとおりです。

- 「FSPF 統計情報の表示」（P.7-12）

FSPF リンク コストの概要

FSPF はファブリック内のすべてのスイッチのリンク ステートを追跡し、データベース内の各リンクにコストを関連付けて、最小コストのパスを選択します。インターフェイスに関連付けられたコストを管理上変更して、FSPF ルート選択を実行できます。コストの値には、1 ～ 65,535 の範囲内の整数値を指定できます。1 Gbps ならデフォルト コストは 1000 で、2 Gbps ならデフォルト コストは 500 です。

FSPF リンク コストの設定

Fabric Manager を使用して FSPF リンク コストを設定する手順は、次のとおりです。

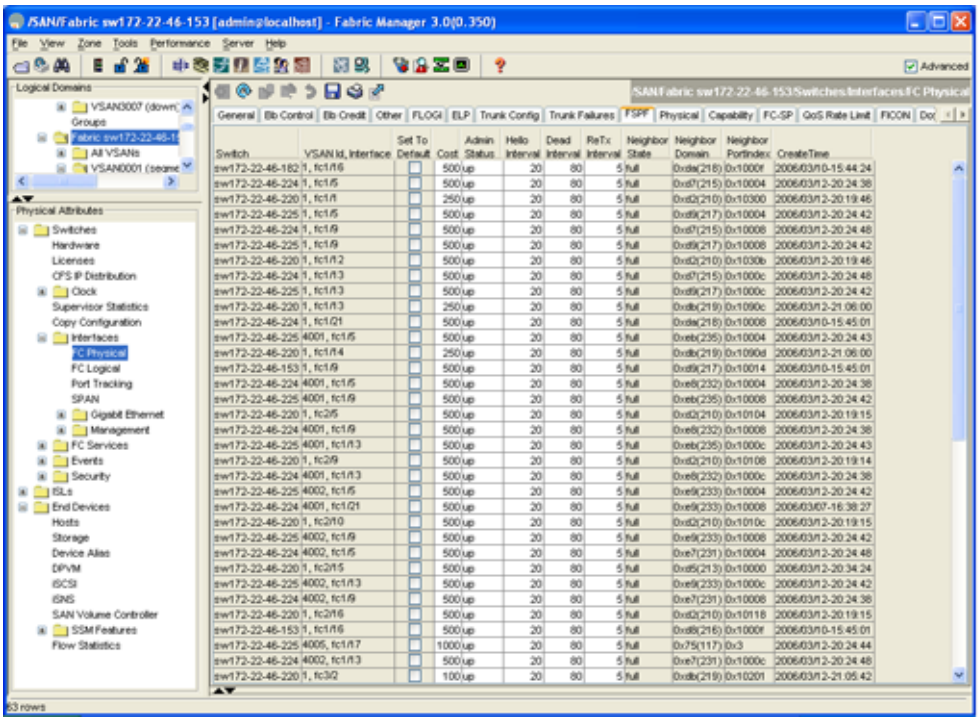
ステップ 1　[Switches] を展開し、[Interfaces] を展開して、[FC Physical] を選択します。

[Information] ペインにインターフェイス設定が表示されます。

ステップ 2　[FSPF] タブをクリックします。

[Information] ペインに FSPF インターフェイスの設定が表示されます（図 7-5 を参照）。

図 7-5　ファイバ チャネルの物理 FSPF インターフェイス



ステップ 3　スイッチの [Cost] フィールドをダブルクリックして、値を変更します。

ステップ 4　変更内容を保存する場合は、[Apply Changes] をクリックします。保存されていない変更を破棄する場合は、[Undo Changes] をクリックします。

ハロー タイム インターバルの概要

FSPF ハロー タイム インターバルを設定して、リンク状態を検証するために定期的に送信される hello メッセージのインターバルを指定できます。指定できる値は、整数値で 1 ～ 65,535 秒です。

（注）　この値は、ISL の両端のポートで同じ値にする必要があります。

ハロー タイム インターバルの設定

Fabric Manager を使用して FSPF ハロー タイム インターバルを設定する手順は、次のとおりです。

ステップ 1　[Switches] を展開し、[Interfaces] を展開して、[FC Physical] を選択します。

[Information] ペインにインターフェイス設定が表示されます。

ステップ 2　[FSPF] タブをクリックします。

[Information] ペインに FSPF インターフェイスの設定が表示されます（図 7-5 を参照）。

ステップ 3　スイッチの [Hello Interval] フィールドを変更します。

ステップ 4　変更内容を保存する場合は、[Apply Changes] をクリックします。保存されていない変更を破棄する場合は、[Undo Changes] をクリックします。

デッド タイム インターバルの概要

FSPF デッド タイム インターバルを設定し、hello メッセージが受信される最大間隔を指定することができます。この期間を過ぎると、ネイバーは存在しないと見なされ、データベースから削除されます。指定できる値は、整数値で 1 ～ 65,535 秒です。

（注）　この値は、ISL の両端のポートで同じ値にする必要があります。

注意　設定されたデッド タイム インターバルがハロー タイム インターバル未満の場合、コマンド プロンプトにエラーが通知されます。

デッド タイム インターバルの設定

Fabric Manager を使用して FSPF デッド タイム インターバルを設定する手順は、次のとおりです。

ステップ 1　[Switches] を展開し、[Interfaces] を展開して、[FC Physical] を選択します。

[Information] ペインにインターフェイス設定が表示されます。

ステップ 2　[FSPF] タブをクリックします。

[Information] ペインに FSPF インターフェイスの設定が表示されます（図 7-5 を参照）。

ステップ 3　スイッチの [Dead Interval] フィールドをダブルクリックして、新しい値を入力します。

ステップ 4　変更内容を保存する場合は、[Apply Changes] をクリックします。保存されていない変更を破棄する場合は、[Undo Changes] をクリックします。

再送信インターバルの概要

確認応答されていないリンク ステート アップデートをインターフェイスから送信するまでの時間を指定します。再送信インターバルを指定する値には、1 ～ 65,535 秒の整数値を指定できます。

（注）　この値は、インターフェイスの両端のスイッチで同じ値にする必要があります。

再送信インターバルの設定

Fabric Manager を使用して FSPF 再送信タイム インターバルを設定する手順は、次のとおりです。

ステップ 1　[Switches] を展開し、[Interfaces] を選択して、[FC Physical] を選択します。

[Information] ペインにインターフェイス設定が表示されます。

ステップ 2　[FSPF] タブをクリックします。

[Information] ペインに FSPF インターフェイスの設定が表示されます（図 7-5 を参照）。

ステップ 3　[ReTx Interval] フィールドをダブルクリックして、値を入力します。

ステップ 4　変更内容を保存する場合は、[Apply Changes] をクリックします。保存されていない変更を破棄する場合は、[Undo Changes] をクリックします。

特定のインターフェイスに対する FSPF のディセーブル化の概要

選択したインターフェイスに対して、FSPF プロトコルをディセーブルに設定できます。デフォルトでは、FSPF はすべての E ポートおよび TE ポートでイネーブルです。このデフォルトをディセーブルにするには、インターフェイスをパッシブに設定します。

（注）　FSPF プロトコルを機能させるには、インターフェイスの両端で FSPF をイネーブルにする必要があります。

特定のインターフェイスに対する FSPF のディセーブル化

選択したインターフェイスに対して、FSPF プロトコルをディセーブルに設定できます。デフォルトでは、FSPF はすべての E ポートおよび TE ポートでイネーブルです。このデフォルトをディセーブルにするには、インターフェイスをパッシブに設定します。

Fabric Manager を使用して特定のインターフェイスに対して FSPF をディセーブルにする手順は、次のとおりです。

ステップ 1　[Switches] を展開し、[Interfaces] を展開して、[FC Physical] を選択します。

[Information] ペインにインターフェイス設定が表示されます。

ステップ 2　[FSPF] タブをクリックします。

[Information] ペインに FSPF インターフェイスの設定が表示されます（図 7-5 を参照）。

ステップ 3　スイッチの [Admin Status] ドロップダウン メニューを [down] に設定します。

ステップ 4　変更内容を保存する場合は、[Apply Changes] をクリックします。保存されていない変更を破棄する場合は、[Undo Changes] をクリックします。

選択したインターフェイスに対して、FSPF プロトコルをディセーブルに設定できます。デフォルトでは、FSPF はすべての E ポートおよび TE ポートでイネーブルです。このデフォルトをディセーブルにするには、インターフェイスをパッシブに設定します。

FSPF データベースの表示

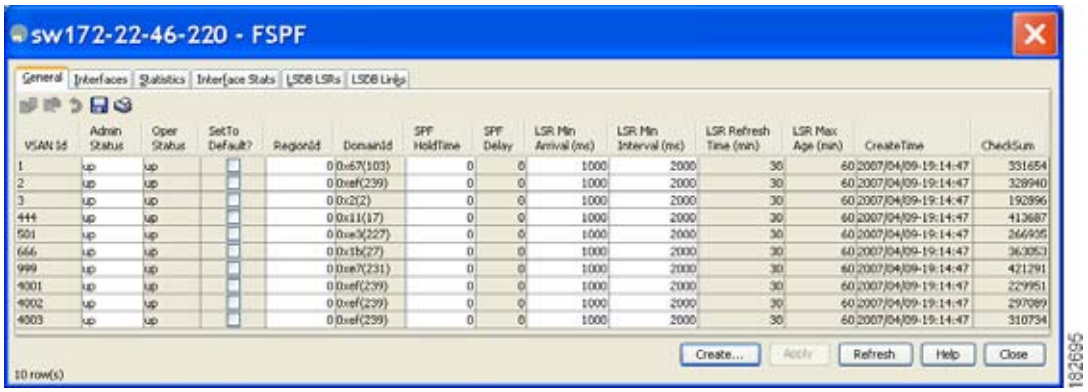
指定された VSAN の FSPF データベースには、次の情報が格納されています。

- LSR タイプ
- LSR 所有者のドメイン ID
- アドバタイジング ルータのドメイン ID
- LSR の経過時間
- LSR を示す番号
- リンク数

Device Manager を使用して FSPF データベースを表示する手順は、次のとおりです。

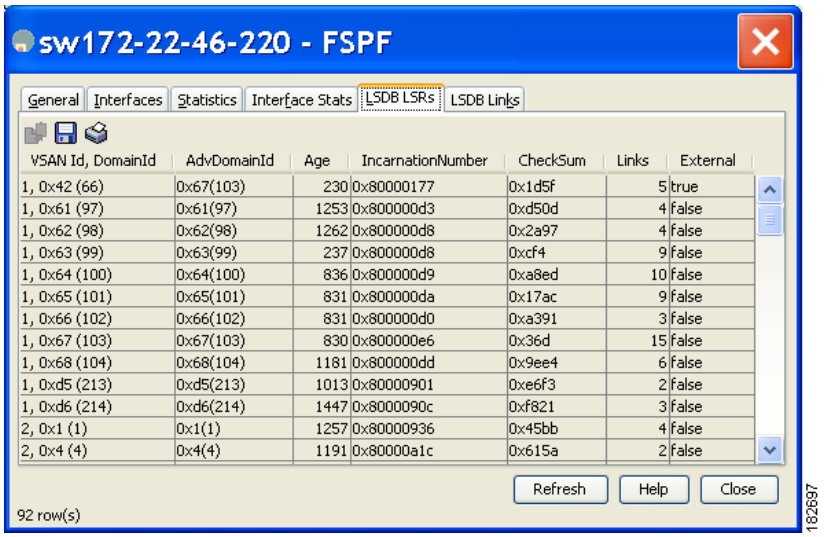
ステップ 1　[FC] > [Advanced] > [FSPF] を選択します。
FSPF ダイアログボックスが表示されます（図 7-6 を参照）。

図 7-6　Device Manager の [FSPF] ダイアログボックス



ステップ 2　[LSDB LSRs] タブをクリックします。
FSPF データベース情報が表示されます（図 7-7 を参照）。

図 7-7　[LSDB LSRs] タブの FSPF データベース情報



ステップ 3　[Close] をクリックして、ダイアログボックスを閉じます。

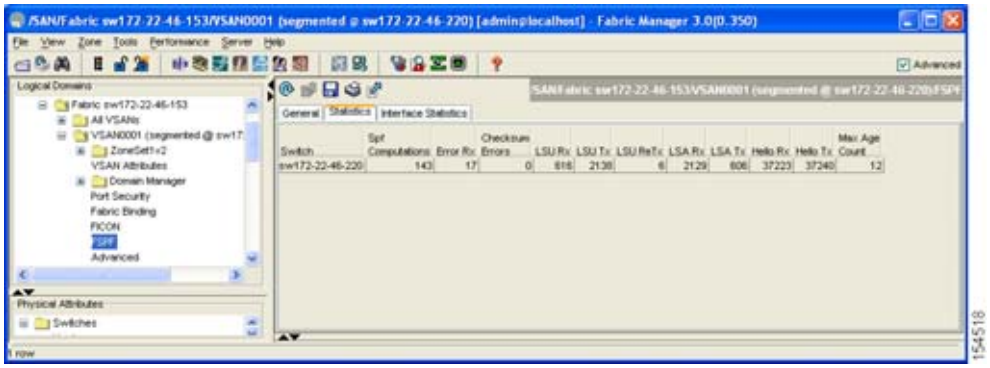
FSPF 統計情報の表示

Fabric Manager を使用して FSPF の統計情報を表示する手順は、次のとおりです。

ステップ 1　ファブリックを展開し、VSAN を展開して、[Logical Domains] ペインで [FSPF] を選択します。
[FSPF] 設定ダイアログボックスが表示されます。

ステップ 2　[Statistics] タブをクリックします。
[Information] ペインに FSPF VSAN の統計情報が表示されます（図 7-8 を参照）。

図 7-8　FSPF VSAN の統計情報



ステップ 3　[Interface Statistics] タブをクリックします。
[Information] ペインに FSPF インターフェイスの統計情報が表示されます。

FSPF ルート

FSPF は FSPF データベースのエントリに基づいて、ファブリック内でトラフィックをルーティングします。これらのルートは動的に学習したり、静的に設定したりできます。

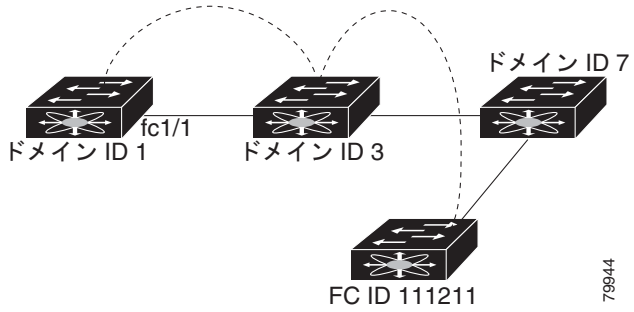
ここで説明する内容は、次のとおりです。

- 「ファイバ チャネル ルートの概要」（P.7-13）
- 「ファイバ チャネル ルートの設定」（P.7-13）
- 「ブロードキャストおよびマルチキャストルーティングの概要」（P.7-14）
- 「マルチキャスト ルート スイッチの概要」（P.7-15）
- 「マルチキャスト ルート スイッチの設定」（P.7-15）

ファイバ チャネル ルートの概要

各ポートに実装されている転送ロジックに従って、FC ID に応じたフレームが転送されるようになっています。特定のインターフェイスおよびドメイン用の FC ID を使用することにより、ドメイン ID 1 のスイッチで特定のルート（例：FC ID 111211、ドメイン ID 3）を設定できます（図 7-9 を参照）。

図 7-9　ファイバ チャネルのルート



（注） VSAN 外部では、設定済みスタティック ルートおよび一時停止中のスタティック ルートに対してランタイム チェックは実行されません。

ファイバ チャネル ルートの設定

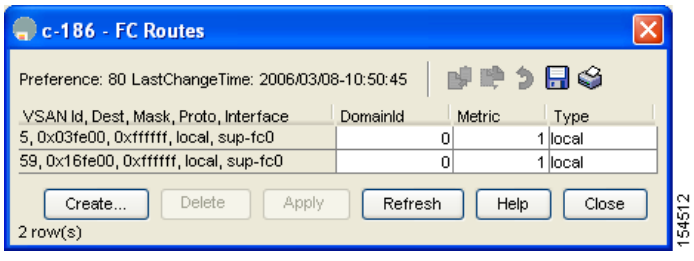
FSPF をディセーブルにした場合は、ファイバ チャネル ルートを手動で設定できます。

Device Manager を使用してファイバ チャネル ルートを設定する手順は、次のとおりです。

ステップ 1　[FC] > [Advanced] > [Routes] をクリックします。

[FC Static Route Configuration] ダイアログボックスが表示されます（図 7-10 を参照）。

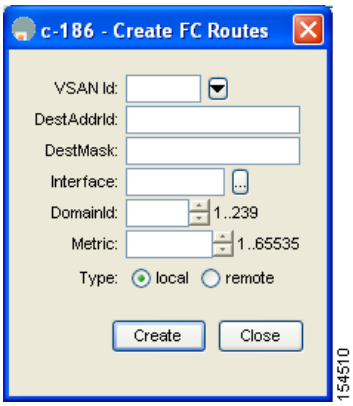
図 7-10　[Fibre Channel Static Route Configuration] ダイアログボックス



ステップ 2　[Create] をクリックして、スタティック ルートを作成します。

[Create Route] ダイアログボックスが表示されます（図 7-11 を参照）。

図 7-11　[Create Fibre Channel Route] ダイアログボックス



ステップ 3　このルートの設定に使用する VSAN ID を選択します。

ステップ 4　ルートを設定しているデバイスの宛先アドレスおよび宛先マスクを入力します。

ステップ 5　この宛先に到達するために使用するインターフェイスを選択します。

ステップ 6　ネクストホップのドメイン ID およびルート メトリックを選択します。

ステップ 7　[local] または [remote] ラジオ ボタンを選択します。

ステップ 8　変更内容を保存するには、[Create] をクリックします。変更を保存せずに終了するには、[Close] をクリックします。

ブロードキャストおよびマルチキャストルーティングの概要

ファイバ チャネル ファブリック内のブロードキャストおよびマルチキャストは、配信ツリーの概念に基づいて、ファブリック内のすべてのスイッチに到達します。

配信ツリーを計算するためのトポロジ情報は、FSPF によって提供されます。ファイバ チャネルには、VSAN ごとに 256 個のマルチキャスト グループ、および 1 個のブロードキャスト アドレスが定義されます。Cisco MDS 9000 ファミリ スイッチで使用されるのは、ブロードキャスト ルーティングだけです。デフォルトでは、ルート ノードとして主要スイッチが使用され、VSAN 内でマルチキャスト ルーティングおよびブロードキャスト ルーティング用のループフリー配信ツリーが取得されます。

注意　同じ配信ツリーが得られるようにするために、ファブリック内のすべてのスイッチで同一のマルチキャストおよびブロードキャスト配信ツリー アルゴリズムを実行する必要があります。

他のベンダーのスイッチ（FC-SW3 ガイドラインに準拠）と相互運用するために、SAN-OS および NX-OS 4.1(1b) 以降のソフトウェアは最も小さなドメイン スイッチをルートとして使用し、interop モードでマルチキャスト ツリーを計算します。

マルチキャスト ルート スイッチの概要

ネイティブ（非 interop）モードでは、主要スイッチがデフォルトのルートとして使用されます。デフォルトを変更する場合は必ず、ファブリック内のすべてのスイッチに同じモードを設定してください。同じモードを設定しないと、マルチキャスト トラフィックがループし、フレームが削除されるなどの問題が発生する可能性があります。

（注）　動作モードが、設定されている interop モードと異なる場合があります。interop モードでは常に、最も小さなドメイン スイッチがルートとして使用されます。

マルチキャスト ルート スイッチの設定

Fabric Manager を使用して、マルチキャスト ツリー計算に最も小さなドメイン スイッチを使用する手順は、次のとおりです。

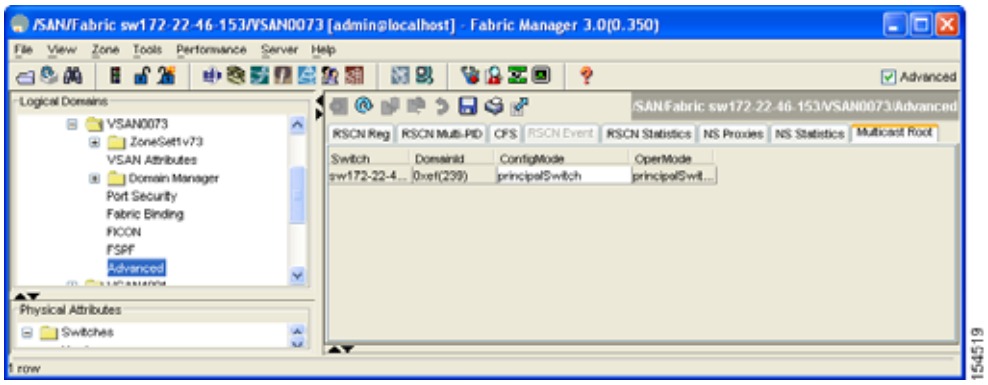
ステップ 1　ファブリックを展開し、VSAN を展開して、FSPF を設定する VSAN に対して [Advanced] を選択します。

[Information] ペインに、ファイバ チャネルの詳細設定が表示されます。

ステップ 2　[Multicast Root] タブを選択します。

[Information] ペインに、マルチキャスト ルートの設定が表示されます（図 7-12 を参照）。

図 7-12　マルチキャスト ルートの設定



ステップ 3　[Config Mode] ドロップダウン メニューを [lowestDomainSwitch] に設定します。

ステップ 4　変更内容を保存する場合は、[Apply Changes] をクリックします。保存されていない変更を破棄する場合は、[Undo Changes] をクリックします。

順序どおりの配信

データ フレームの In-Order Delivery（IOD; 順序どおりの配信）機能を使用すると、フレームは送信元から送信されたときと同じ順番で宛先に配信されます。

一部のファイバ チャネル プロトコルまたはアプリケーションでは、順序どおりではないフレーム配信は処理できません。このような場合、Cisco MDS 9000 ファミリのスイッチではフレーム フローのフレーム順序が維持されます。フレームのフローは、Source ID（SID）、Destination ID（DID）、およびオプションとして Originator eXchange ID（OX ID）で識別されます。

IOD がイネーブルのスイッチでは、特定の入力ポートで受信されて特定の出力ポートに送信されるすべてのフレームは常に、受信時と同じ順序で配信されます。

IOD は、順不同のフレーム配信を使用環境でサポートできない場合に限り使用してください。

ヒント　順序どおりの配信機能がイネーブルな場合、グレースフル シャットダウン機能は実装されません。

ここで説明する内容は、次のとおりです。

ネットワーク フレーム順序の再設定の概要

ネットワーク内のルートが変更された場合は、新規に選択されたパスが古いルートよりも高速であったり、輻輳が少なかったりすることがあります。

図 7-13　ルート変更配信

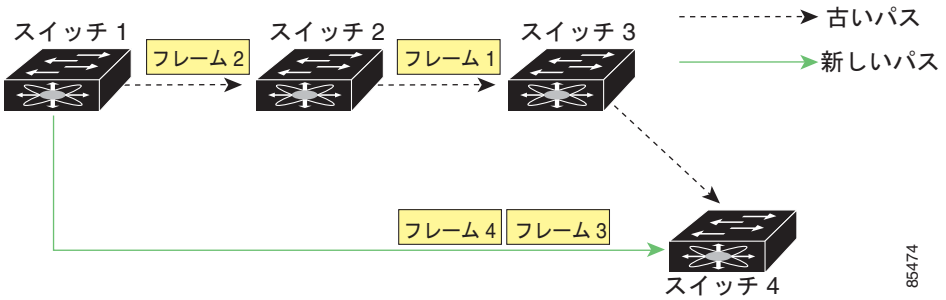


図 7-13 では、スイッチ 1 からスイッチ 4 への新しいパスの方が高速です。このシナリオでは、フレーム 3、フレーム 4 が、フレーム 1、フレーム 2 よりも先に配信されることがあります。

順序保証機能がイネーブルな場合、ネットワーク内のフレームは次のように配信されます。

- ネットワーク内のフレームは、送信時に順序どおりに配信されます。
- ネットワーク遅延ドロップ期間内に順序どおりに配信されなかったフレームは、ネットワーク内でドロップされます。

ポート チャネル フレーム順序の再設定の概要

ポート チャネル内でリンクが変更されると、同じ交換処理または同じフロー内のフレームが、元のパスから、より高速な別のパスに切り替えられることがあります。

図 7-14　　リンク輻輳配信

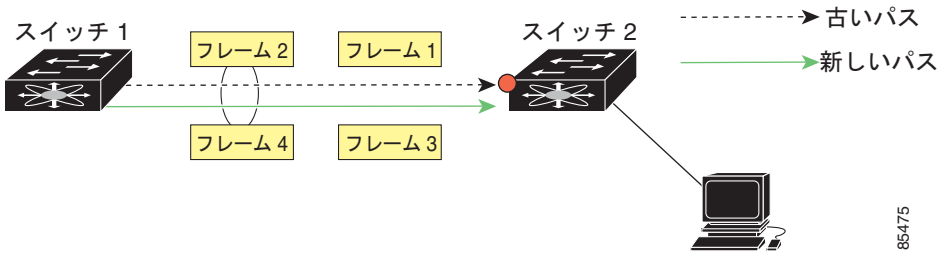


図 7-14 では、古いパスのポート（レッドの点）が輻輳しています。この場合、フレーム 3、フレーム 4 が、フレーム 1 およびフレーム 2 よりも先に配信されることがあります。

該当ポートチャネルのすべてのフレームをフラッシュする要求を、ポートチャネル上のリモート スイッチに送信して、順序どおりの配信機能をイネーブルにしておくと、ポートチャネル リンクの変更時に削除されるフレーム数が最小限に抑えられます。

（注）　この IOD 拡張機能を実行するには、ポートチャネル上の両方のスイッチで Cisco SAN-OS Release 3.0(1) が稼動している必要があります。これより古いリリースでは、IOD はスイッチ遅延期間だけ待機してから、新しいフレームを送信します。

順序どおりの配信機能がイネーブルになっているときに、ポート チャネル リンクの変更が発生した場合、ポート チャネルを経由するフレームは、次のように扱われます。

- 古いパスを使用するフレームは、新しいフレームが着信する前に配信されます。
- ネットワーク遅延ドロップ期間が経過して古いフレームがすべてフラッシュされると、新しいフレームは新しいパス経由で配信されます。

ネットワーク遅延ドロップ期間が経過した時点で、古いパス経由で順序どおりに配信できないフレームはドロップされます。「ドロップ遅延時間の設定」（P.7-19）を参照してください。

順序どおりの配信のイネーブル化の概要

特定の VSAN またはスイッチ全体に対して、順序どおりの配信機能をイネーブルに設定できます。Cisco MDS 9000 ファミリのスイッチでは、順序どおりの配信はデフォルトでディセーブルになります。

ヒント　この機能は、順序どおりではないフレームを処理できないデバイスがスイッチ内にある場合に限り、イネーブルにすることを推奨します。Cisco MDS 9000 ファミリのロード バランシング アルゴリズムによって、通常のファブリック処理中に、フレームの順序どおりの配信が保証されます。送信元 FC ID、宛先 FC ID、および exchange ID（OX ID）に基づくロード バランシング アルゴリズムはハードウェア内で実行され、パフォーマンスは低下しません。ただし、ファブリックに障害が発生した場合、順序どおりの配信機能がイネーブルになっていると、ファブリック転送の意図的な一時停止によって、無秩序に転送された可能性のある常駐フレームがファブリックから除去されるため、リカバリが遅延します。

順序どおりの配信のグローバルなイネーブル化

MDS スイッチ上のどの VSAN に対しても、順序どおりの配信パラメータを一様に設定するには、順序どおりの配信をグローバルにイネーブルにします。

順序どおりの配信をグローバルにイネーブル化するのは、ファブリック全体で必要な場合だけにしてください。それ以外の場合は、IOD 機能が必要な VSAN に対してだけ、IOD をイネーブルにしてください。

（注）　Cisco MDS SAN-OS Release 1.3(3) 以前のリリースにダウングレードする際は、事前にスイッチ全体に対する順序どおりの配信をイネーブルにしてください。

特定の VSAN に対する順序どおりの配信のイネーブル化

VSAN を作成した場合、作成された VSAN には、グローバルな順序保証値が自動的に継承されます。このグローバル値を上書きするには、新しい VSAN の順序保証をイネーブルまたはディセーブルにします。

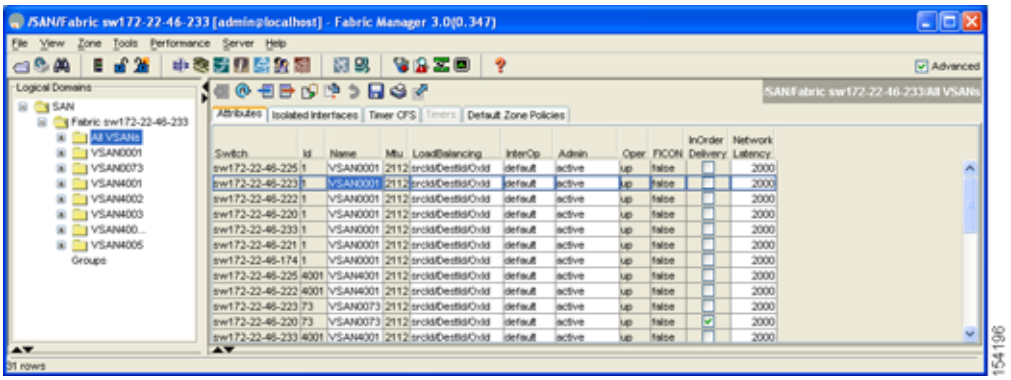
Fabric Manager を使用して、マルチキャスト ツリー計算に最も小さなドメイン スイッチを使用する手順は、次のとおりです。

ステップ 1　ファブリックを展開して、[All VSANS] を選択します。

ステップ 2　[Attributes] タブをクリックします。

[Information] ペインに、VSAN の一般属性が表示されます（図 7-15 を参照）。

図 7-15　VSAN の一般属性



ステップ 3　[InOrder Delivery] チェックボックスをオンにして、スイッチに対して IOD をイネーブルにします。

ステップ 4　変更内容を保存する場合は、[Apply Changes] をクリックします。保存されていない変更を破棄する場合は、[Undo Changes] をクリックします。

ドロップ遅延時間の設定

スイッチ全体またはスイッチ内の特定の VSAN のデフォルトの遅延時間を変更できます。

Fabric Manager を使用して特定のスイッチのドロップ遅延時間を設定する手順は、次のとおりです。

ステップ 1　ファブリックを展開して、[All VSANS] を選択します。

[Information] ペインに VSAN 設定が表示されます。

ステップ 2　[Attributes] タブをクリックします。

[Information] ペインに、VSAN の一般属性が表示されます（図 7-16 を参照）。

図 7-16　VSAN の一般属性

ステップ 3　[Network Latency] フィールドをダブルクリックして、値を変更します。

ステップ 4　変更内容を保存する場合は、[Apply Changes] をクリックします。保存されていない変更を破棄する場合は、[Undo Changes] をクリックします。

デフォルト設定

表 7-4 に、FSPF 機能のデフォルト設定を示します。

表 7-4　FSPF のデフォルト設定

パラメータ	デフォルト
FSPF	すべての E ポートおよび TE ポートでイネーブル
SPF 計算	ダイナミック
SPF ホールド タイム	0
バックボーン領域	0
確認応答インターバル（RxmtInterval）	5 秒
リフレッシュ時間（LSRefreshTime）	30 分
最大有効期限（MaxAge）	60 分
Hello インターバル	20 秒
デッド インターバル	80 秒
配信ツリーの情報	主要スイッチ（ルート ノード）から取得
ルーティング テーブル	FSPF によって、指定された宛先への等コスト パスが最大 16 個格納されます。
ロード バランシング	各等コスト パスの宛先 ID および送信元 ID に基づきます。
順序どおりの配信	ディセーブル
ドロップ遅延	ディセーブル
スタティック ルート コスト	ルートのコスト（メトリック）が指定されていない場合、デフォルト コストは 10 です。
リモート宛先スイッチ	リモート宛先スイッチが指定されていない場合、デフォルトはダイレクトです。
マルチキャスト ルーティング	主要スイッチを使用して、マルチキャスト ツリーを計算します。

CHAPTER 8

DWDM の設定

この章の内容は、次のとおりです。

DWDM の概要

Dense Wavelength Division Multiplexing（DWDM; 高密度波長分割多重）は、1 つの光ファイバで複数のオプティカル キャリア信号を多重化します。DWDM は、異なる波長を使用してさまざまな信号を伝送します。

DWDM リンクを確立するには、スイッチ間リンク（ISL）の両側を、リンクのそれぞれの端で、DWDM Small Form-Factor Pluggable（SFP; 着脱可能小型フォーム ファクタ）によって接続する必要があります。DWDM リンクを識別するために、Fabric Manager は、ファイバ チャネル（FC）ポートでコネクタ タイプを検出します。ISL リンクが両端で FC ポートと関連付けられている場合、FC ポートは DWDM SFP を使用してリンクを接続します。

Fabric Manager Server は、DWDM SFP を持つ FC ポート、および FC ポートに関連付けられている ISL を検出します。Fabric Manager Client は、トポロジ マップ上に DWDM 属性を持つ ISL を表示します。

（注） Fabric Shortest Path First（FSPF）データベースは、両端で DWDM SFP によって接続されている ISL リンクだけを表示します。

DWDM リンクの表示

Fabric Manager Client には、破線で DWDM リンクが表示されます。リンクのツールチップには、リンク タイプを示す「DWDM」が表示されます。

DWDM リンクを表示する手順は、次のとおりです。

ステップ 1　[Logical Domain] 領域内でスイッチを選択します。

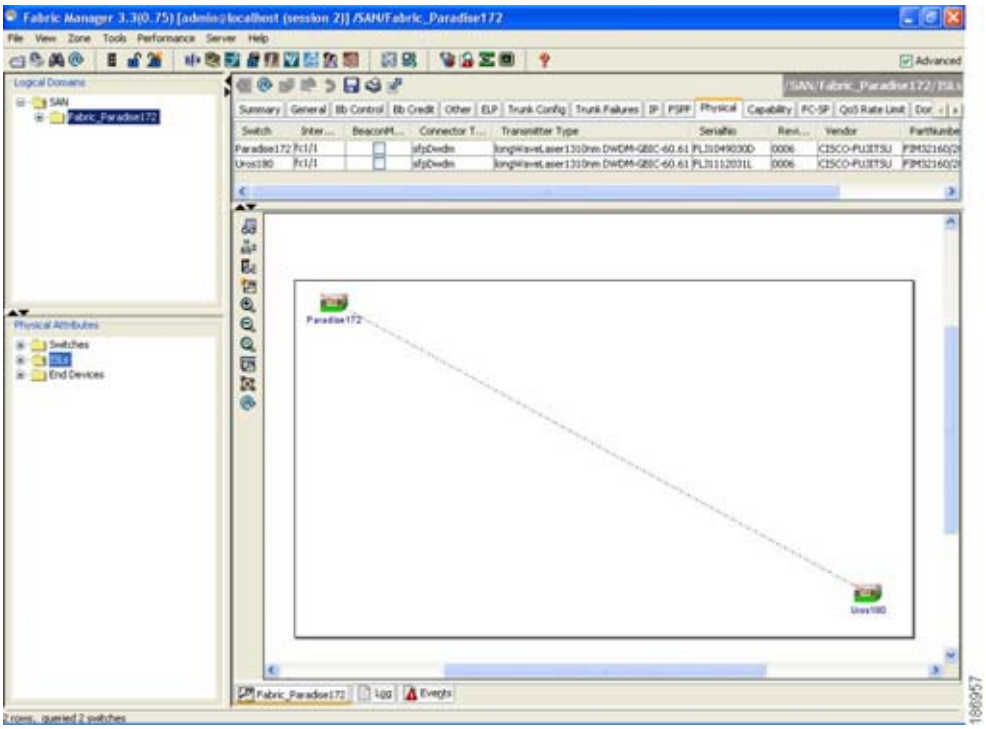
ステップ 2　[Physical Attribute] 領域 ISL を選択します。

[Information] ペインに ISL の情報が表示されます。

ステップ 3　[Physical] タブをクリックします。

[Information] ペインに ISL 設定が表示されます（図 8-1 を参照）。

図 8-1　ISL リンクが表示されている Fabric Manager

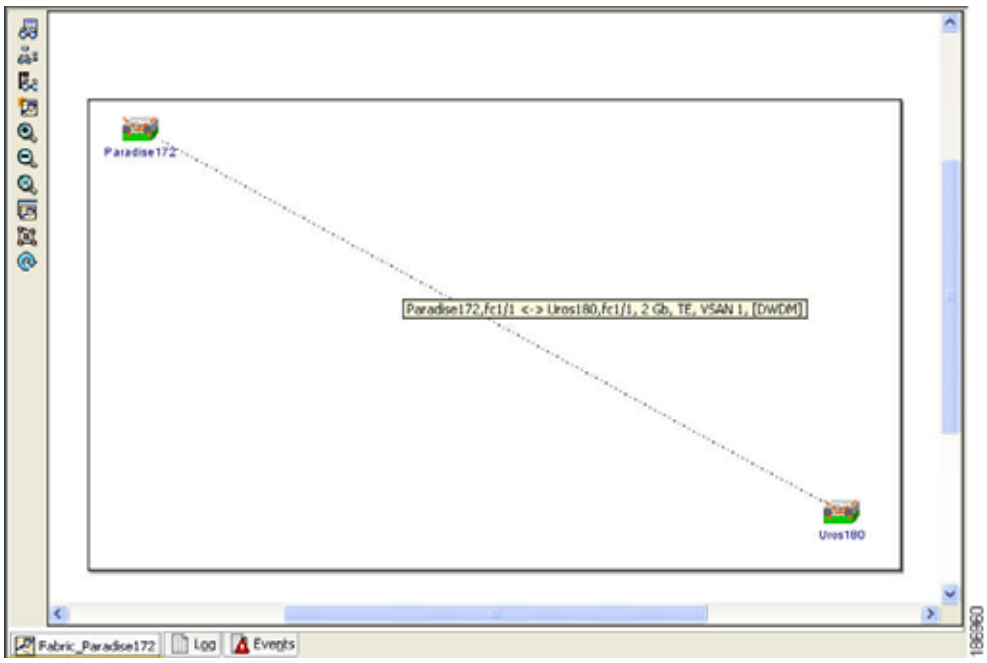


ステップ 4　ISL の [Physical] テーブルには、「sfpDwdm」としてコネクタ タイプが表示されます（図 8-2 を参照）。

図 8-2　「sfpDwdm」として表示されるコネクタ タイプ

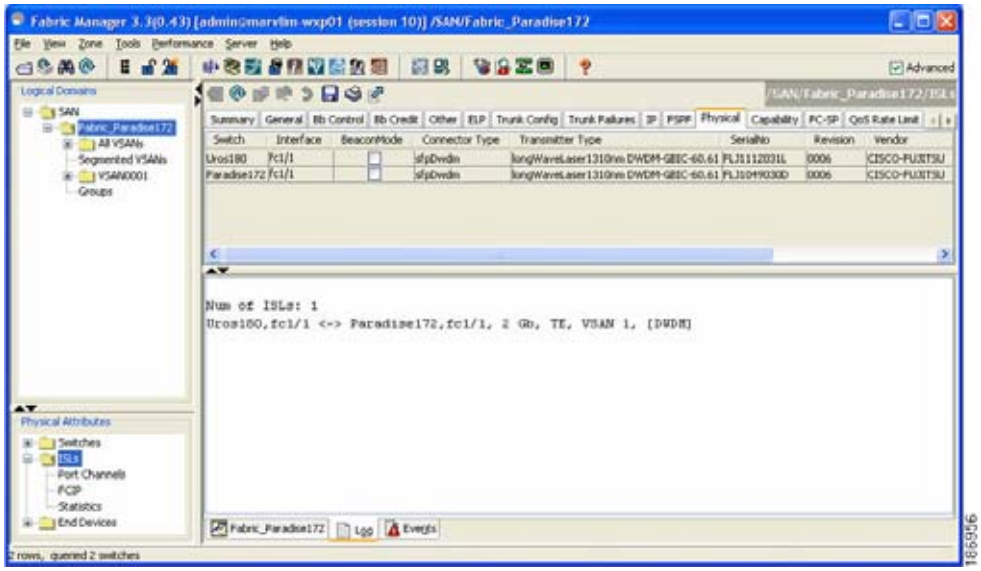
ステップ 5　リンク タイプとして DWDM が示されるツールチップを表示するには、マウスをリンクの上に移動します（図 8-3 を参照）。

図 8-3　DWDM を示すツールチップ



ステップ 6　ISL の Dump Discovery を実行してすべての ISL の一覧を表示します。DWDM リンクは「[DWDM]」とともに表示されます（図 8-4 を参照）。

図 8-4　[Information] ペインに表示される ISL リスト



X2 DWDM トランシーバ周波数の設定

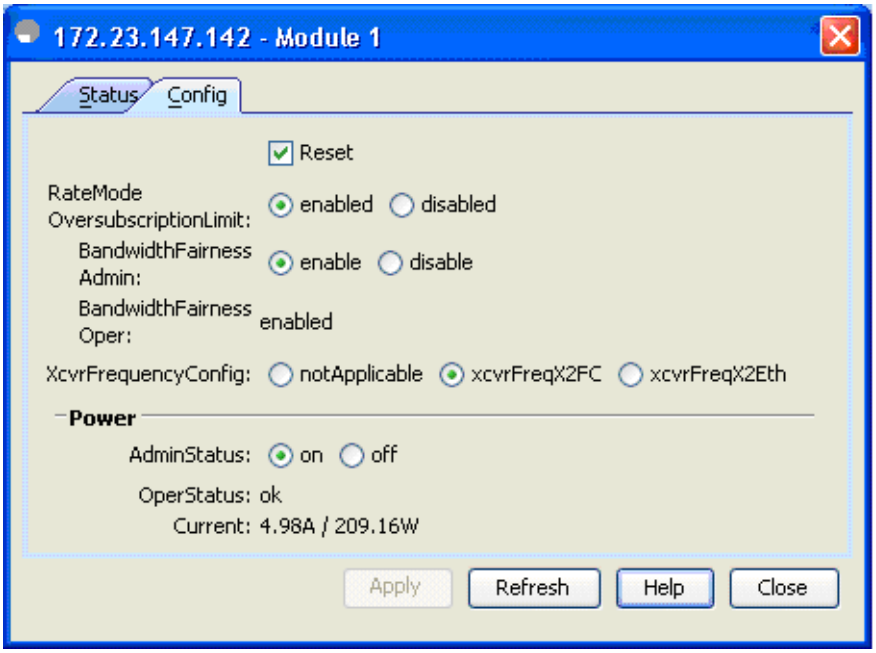
（注）　この機能は、UROS 以外のモジュールではサポートされていません。UROS モジュールでは、X2 トランシーバ周波数を設定すると、10 ギガビット イーサネット ポートはダウン状態になります。

Device Manager を使用して X2 DWDM トランシーバ周波数を設定する手順は、次のとおりです。

ステップ 1　[Device Manager] メニューバーから、[Physical] > [Modules] を選択します。

モジュール設定ウィンドウが表示されます（図 8-5 を参照）。

図 8-5　Device Manager での X2 DWDM トランシーバの設定



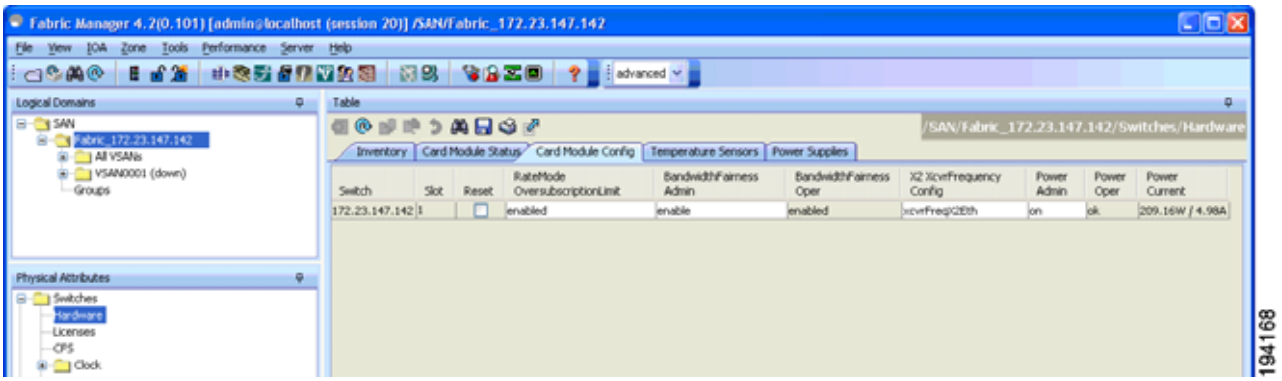
ステップ 2　[XcvrFrequencyConfig] オプション ボタンを選択します。

ステップ 3　[Apply] をクリックします。

Fabric Manager を使用して X2 DWDM トランシーバ周波数を設定する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインから、[Hardware] を選択します。
モジュール設定ウィンドウが表示されます。

図 8-6　Fabric Manager での X2 DWDM トランシーバの設定



ステップ 2　[Card Module Config] タブをクリックします。

ステップ 3　[X2 XcvrFrequencyConfig] カラムで、オプションを選択します。

ステップ 4　[Apply] をクリックします。

CHAPTER 9

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、Cisco MDS 9000 ファミリが提供する Fabric Login（FLOGI; ファブリック ログイン）データベース、ネーム サーバ機能、Fabric-Device Management Interface、Registered State Change Notification（RSCN）の情報について説明します。この章の内容は、次のとおりです。

FLOGI の概要

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。必要なデバイスが FLOGI テーブルに表示されている場合は、ファブリック ログインに成功しています。ホスト Host Bus Adapter（HBA）および接続先ポートに直接接続されたスイッチで、FLOGI データベースを調べてください。「デフォルトの企業 ID リスト」（P.12-8）および「スイッチの相互運用性」（P.12-9）を参照してください。

FLOGI の詳細の表示

Fabric Manager を使用して FLOGI テーブル内にストレージ デバイスがあるか確認する手順は、次のとおりです。

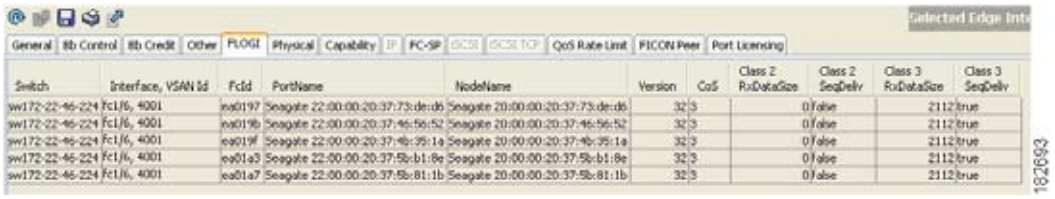
ステップ 1 [Switches] を展開し、[Interfaces] を展開して、[FC Physical] を選択します。

[Information] ペインにインターフェイス設定が表示されます。

ステップ 2 [FLOGI] タブをクリックします。

ファブリックにログインしているエンド デバイスがすべて表示されます（図 9-1 を参照）。

図 9-1　FLOGI 物理インターフェイス



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 デバイスの属性が格納されたデータベースをメンテナンスします。ネーム サーバを使用すると、情報が本来登録されていたデバイスからデータベース エントリを変更することができます。

別のデバイスによって登録済みのデータベース エントリの内容を変更（アップデートまたは削除）する必要がある場合は、プロキシ機能が便利です。

ここで説明する内容は、次のとおりです。

ネーム サーバ プロキシ登録の概要

すべてのネーム サーバ レジストレーション要求は、パラメータが登録または変更されたポートから送信されます。これ以外のポートから送信された要求は拒否されます。

この認証により、WWN は別のノードに特定のパラメータを登録することができます。

ネーム サーバ プロキシの登録

Fabric Manager を使用してネーム サーバ プロキシを登録する手順は、次のとおりです。

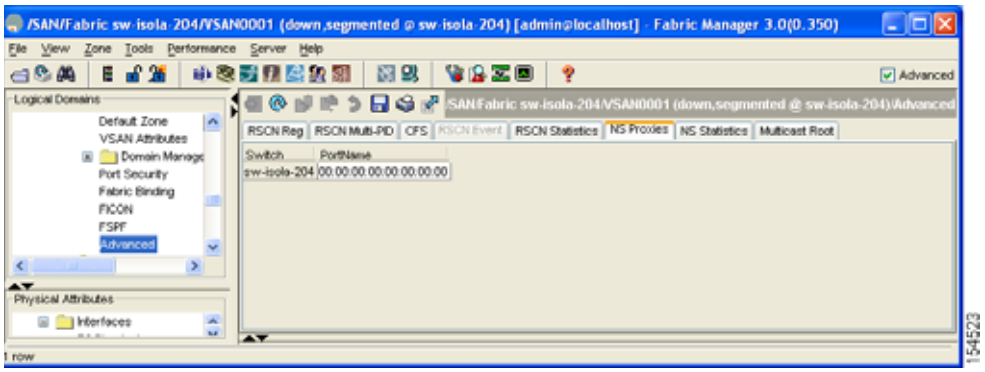
ステップ 1　ファブリックを展開し、VSAN を展開してから、[Advanced] を選択します。

[Information] ペインに VSAN の詳細な設定が表示されます。

ステップ 2　[NS Proxies] タブをクリックします。

選択した VSAN の既存のネーム サーバ プロキシが表示されます（図 9-2 を参照）。

図 9-2　ネーム サーバ プロキシ



ステップ 3　新しいネーム サーバ プロキシを登録するには、[PortName] フィールドをダブルクリックします。

ステップ 4　これらの変更を保存する場合は、[Apply Changes] をクリックします。保存されていない変更をキャンセルする場合は、[Undo Changes] をクリックします。

重複 pWWN の拒否の概要

別のデバイスの pWWN を使用した悪意のあるログイン、または予期せぬログインを防止することができます。これらの pWWN を使用すると、ファブリックにログインして、ネーム サーバ データベース内の最初のデバイスを置き換えることができます。

重複 pWWN の拒否

重複 pWWN の拒否については、『Cisco MDS 9000 Family CLI Configuration Guide』を参照してください。

ネーム サーバ データベース エントリの概要

ネーム サーバの FCNS データベースには、すべてのホストのネーム エントリが格納されています。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と、これらの属性は登録解除されます。

複数スイッチのファブリック設定の場合、配信されたデータベース内の情報は、各スイッチで稼動している複数のネーム サーバ インスタンスで共有されます。スイッチごとに、ネーム サーバ プロセスのインスタンスが 1 つ実行されます。

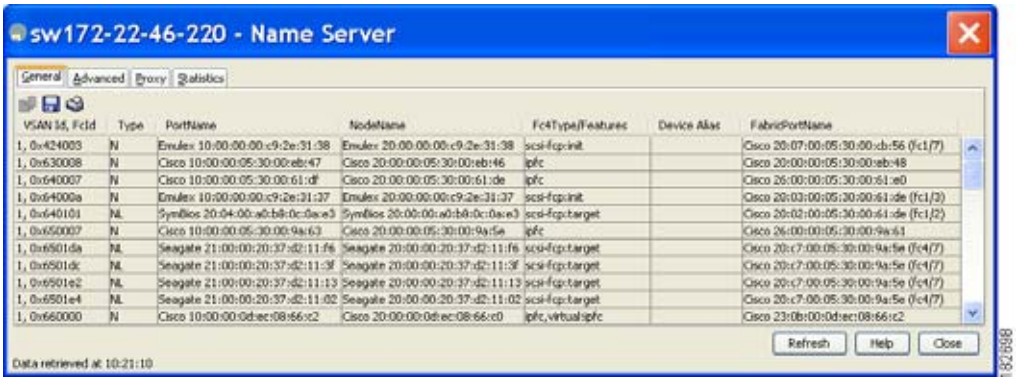
ネーム サーバ データベース エントリの表示

Device Manager を使用してサーバ データベース エントリを表示する手順は、次のとおりです。

ステップ 1　[FC] > [Name Server] をクリックします。

[Name Server] ダイアログボックスが表示されます（図 9-3 を参照）。

図 9-3　[Name Server] ダイアログボックス



デフォルト タブは [General] タブです。ネーム サーバ データベースが表示されます。

ステップ 2　[Statistics] タブをクリックします。

ネーム サーバの統計情報が表示されます。

ステップ 3　[Close] をクリックして、ダイアログボックスを閉じます。

FDMI

Cisco MDS 9000 ファミリ スイッチでは、FC-GS-4 規格に記述されている FDMI 機能がサポートされます。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を介して管理できます。この追加機能によって、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が補完されます。

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、NX-OS ソフトウェアは接続先 HBA およびホスト OS（オペレーティング システム）に関する次の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 バージョン
- ホスト OS の名前およびバージョン番号

すべての FDMI エントリは永続ストレージに格納され、FDMI プロセスの起動時に取得されます。

FDMI の表示

Device Manager を使用して FDMI データベース情報を表示するには、[FC] > [Advanced] > [FDMI] を選択します。[FDMI] ダイアログボックスが表示されます。

RSCN

RSCN は、ファブリック内の変更をホストに通知するファイバ チャネル サービスです。ホストが受信したこの情報は、（SCR を介して）ファブリック コントローラに登録されます。これらの通知により、1 つまたは複数の次のイベントが、適切なタイミングで示されます。

- ファブリックへのディスクの追加または削除
- ネーム サーバの登録内容の変更
- 新しいゾーンの適用
- 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

ここで説明する内容は、次のとおりです。

RSCN 情報の概要

登録先ホストにこれらのイベントを送信するだけでなく、スイッチ RSCN（SW-RSCN）がファブリック内のすべての到達可能なスイッチに送信されます。

（注）　スイッチは RSCN を送信して、変更が発生したことを登録先ノードに通知します。ネーム サーバに問い合わせて、新しい情報を取得する作業は、ノードが行います。ノードに送信された RSCN 内のスイッチからは、変更された情報の詳細は配信されません。

RSCN 情報の表示

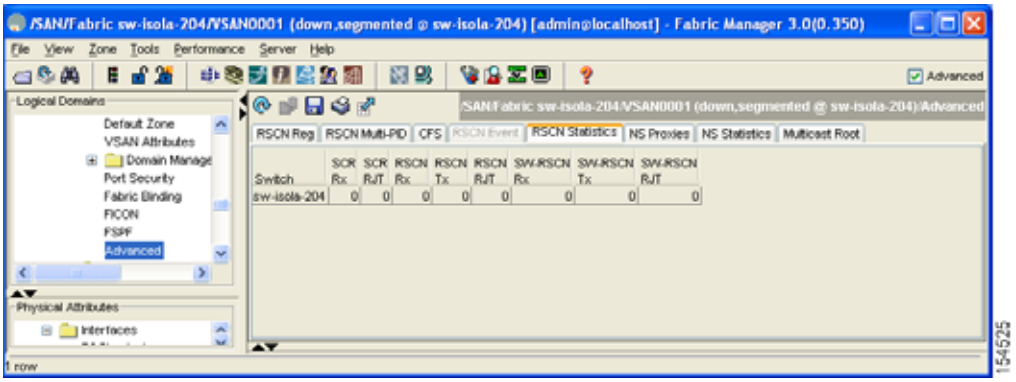
Fabric Manager を使用して RSCN 情報を表示する手順は、次のとおりです。

ステップ 1　ファブリックを展開し、VSAN を展開してから、[Advanced] を選択します。

[Information] ペインに VSAN の詳細な設定が表示されます。

ステップ 2　[RSCN Reg] タブまたは [RSCN Statistics] タブをクリックします（図 9-4 を参照）。

図 9-4　　RSCN 統計情報



[multi-pid] オプションの概要

RSCN の [multi-pid] オプションがイネーブルな場合、登録済みの Nx ポートに対して生成された RSCN には、関連ポート ID を複数格納できます。この場合、複数の関連ポート ID を単一 RSCN に格納する前に、ゾーン分割ルールが適用されます。このオプションをイネーブルにすると、RSCN 数を削減できます。たとえば、2 つのディスク（D1 と D2）およびホスト（H）がスイッチ 1 に接続されているとします。ホスト H は RSCN を受信するように登録されています。D1、D2、および H は同じゾーンに属します。ディスク D1 および D2 が同時にオンラインになると、次のいずれかの処理が適用されます。

- スイッチ 1 で [multi-pid] オプションがディセーブルになります。ホスト H に対して 2 つの RSCN が生成されます（1 つはディスク D1 用、もう 1 つはディスク D2 用）。
- スイッチ 1 で [multi-pid] オプションがイネーブルになります。ホスト H に対して RSCN が 1 つ生成され、RSCN ペイロードによって関連ポート ID がリストされます（この場合は D1 および D2）。

（注）　一部の Nx ポートでは、multi-pid RSCN ペイロードをサポートできないことがあります。その場合は、RSCN の [multi-pid] オプションをディセーブルにしてください。

[multi-pid] オプションの設定

Fabric Manager を使用して [multi-pid] オプションを設定する手順は、次のとおりです。

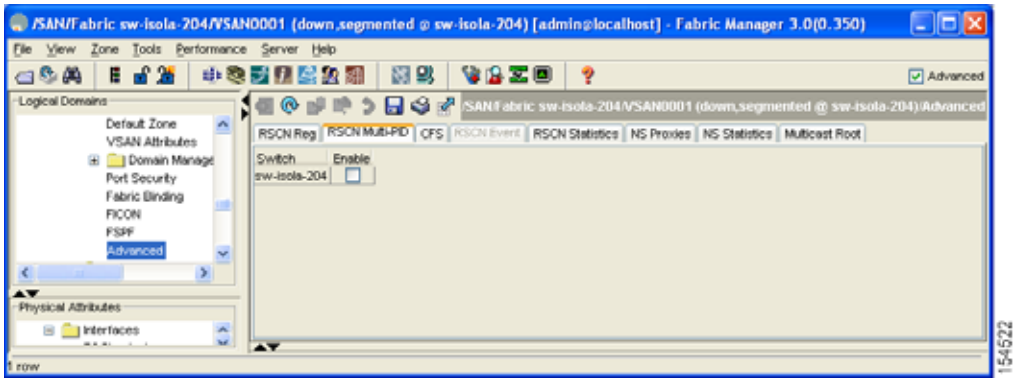
ステップ 1　ファブリックを展開し、VSAN を展開してから、[Advanced] を選択します。

[Information] ペインに VSAN の詳細な設定が表示されます。

ステップ 2　[RSCN Multi-PID] タブをクリックします。

図 9-5 のように情報が表示されます。

図 9-5　RSCN Multi-PID



ステップ 3　[Enable] チェックボックスをオンにします。

ステップ 4　これらの変更を保存する場合は、[Apply Changes] をクリックします。保存されていない変更をキャンセルする場合は、[Undo Changes] をクリックします。

RSCN 統計情報のクリア

カウンタをクリアし、そのあとで、別の一連のイベントに対するカウンタを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）に対して生成される RSCN 数または SW-RSCN 数を追跡できます。これらの統計情報を使用すると、VSAN 内のイベントごとに応答を監視できます。

指定した VSAN の RSCN 統計情報のクリアについては、『*Cisco MDS 9000 Family CLI Configuration Guide*』を参照してください。

CFS を使用した RSCN タイマー設定の配信

各スイッチのタイムアウト値は手動で設定されるため、複数のスイッチがさまざまな時刻にタイムアウトする場合は設定ミスが生じます。つまり、ネットワーク内の複数の N ポートが異なる時刻に RSCN を受信することがあります。Cisco Fabric Services（CFS）を使用すると、設定情報がファブリック内のすべてのスイッチに自動配信されて、この状況が回避されます。また、SW-RSCN 数も削減されます。

RSCN は配信モードと非配信モードをサポートします。配信モードの場合、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信します。非配信モードの場合、ローカル スイッチの設定コマンドだけが影響を受けます。

（注）　すべての設定コマンドが配布されるわけではありません。**rscn event-tov** ***tov*** **vsan** ***vsan*** コマンドだけが配信されます。

RSCN タイマーは、初期化およびスイッチオーバー中に CFS に登録されます。ハイ アベイラビリティ構成の場合に、RSCN タイマー配信がクラッシュし、再起動またはスイッチオーバーが発生すると、クラッシュまたはスイッチオーバーの前の状態から標準機能が再開します。

（注）　ダウングレードを実行する場合は、ネットワーク内の RCSN タイマー値をデフォルト値に戻しておいてください。そうしないと、VSAN およびその他のデバイス間のリンクがディセーブルになります。

アップグレードまたはダウングレード中の各 Cisco MDS NX-OS リリースの互換性は、CFS が提供する **conf-check** によってサポートされます。Cisco MDS SAN-OS Release 30 からダウングレードしようとすると、**conf-check** 警告が表示されます。ダウングレードの前に、RSCN タイマー配信サポートをディセーブルにするように要求されます。

デフォルトでは、RSCN タイマー配信機能はディセーブルになっているため、Cisco MDS SAN-OS Release 3.0 よりも前のリリースからアップグレードするときに互換性があります。

CFS による RSCN タイマーの設定

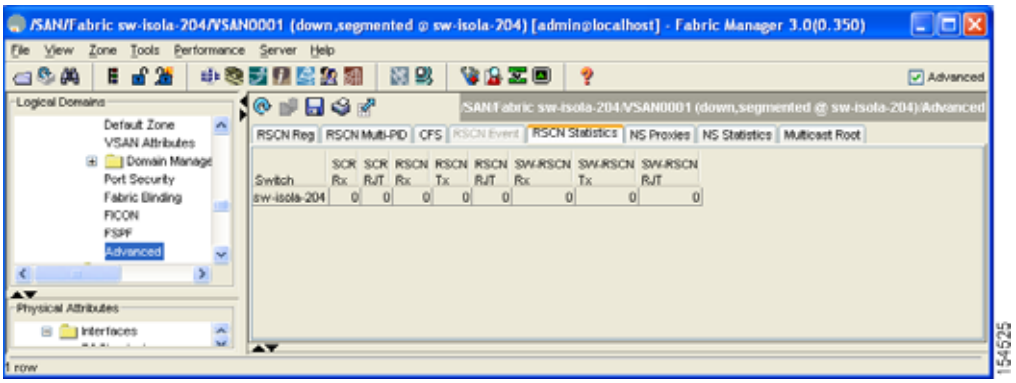
Fabric Manager を使用して CFS に RSCN タイマーを設定する手順は、次のとおりです。

ステップ 1　ファブリックを展開し、VSAN を展開してから、[Logical Domains] ペインで [Advanced] を選択します。

ステップ 2　[RSCN Event] タブをクリックします。

[Information] ペインに VSAN の詳細な設定が表示されます。図 9-6 を参照)。

図 9-6　VSAN の詳細な設定



ステップ 3　[TimeOut] 値をダブルクリックして、選択した VSAN の値を変更します（ミリ秒）。

ステップ 4　これらの変更を保存する場合は、[Apply Changes] をクリックします。保存されていない変更をキャンセルする場合は、[Undo Changes] をクリックします。

デフォルト設定

表 9-1 に、RSCN のデフォルト設定を示します。

表 9-1　RSCN のデフォルト設定

パラメータ	デフォルト
RSCN タイマー値	2,000 ミリ秒（ファイバ チャネル VSAN の場合） 1,000 ミリ秒（FICON VSAN の場合）
RSCN タイマー設定の配信	ディセーブル

CHAPTER 10

SCSI ターゲットの検出

この章では、Cisco MDS 9000 ファミリのスイッチが提供する SCSI LUN 検出機能について説明します。この章の内容は、次のとおりです。

SCSI LUN 検出の概要

Small Computer System Interface（SCSI）ターゲットは、ディスク、テープ、およびその他のストレージ デバイスなどです。これらのターゲットの Logical Unit Number（LUN）は、ネーム サーバに登録されません。

ネーム サーバに LUN 情報が必要な理由は、次のとおりです。

- LUN ストレージ デバイス情報を表示して NMS がこの情報にアクセスできるようにするため
- デバイス容量、シリアル番号、およびデバイス ID 情報を報告するため
- ネーム サーバに発信側およびターゲット機能を登録するため

SCSI LUN 検出機能では、ローカル ドメイン コントローラのファイバ チャネル アドレスを使用します。ローカル ドメイン コントローラは送信元 FC ID として使用され、SCSI デバイス上で SCSI INQUIRY、REPORT LUNS、および READ CAPACITY コマンドが実行されます。

SCSI LUN 検出機能は CLI または SNMP を使用して、オンデマンドで開始されます。隣接スイッチが Cisco MDS 9000 ファミリに含まれる場合、この情報は隣接スイッチとも同期されます。

ここで説明する内容は、次のとおりです。

SCSI LUN 検出開始の概要

SCSI LUN 検出はオンデマンドで実行されます。

ネーム サーバ データベースに格納された Nx ポートのうち、FC4 Type = SCSI_FCP として登録されているものだけが、検出されます。

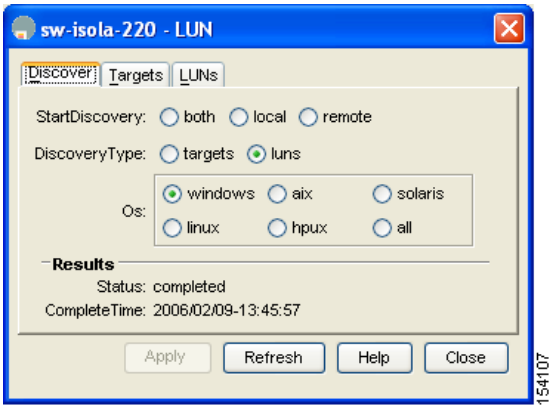
SCSI LUN 検出の開始

Device Manager を使用して SCSI LUN 検出を開始する手順は、次のとおりです。

ステップ 1　[FC] > [Advanced] > [LUNs] を選択します。

[LUN Configuration] ダイアログボックスが表示されます。

図 10-1　[LUN Configuration] ダイアログボックス



ステップ 2　[StartDiscovery] を [local]、[remote]、または [both] に設定します。

ステップ 3　[DiscoveryType] および [OS] を選択します。

ステップ 4　[Apply] をクリックして、検出を開始します。

カスタマイズ検出開始の概要

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/ドメイン ペアのリストで構成されます。ドメイン ID は 0 ～ 255 の 10 進数、または 0x0 ～ 0xFF の 16 進数です。

カスタマイズ検出の開始

Device Manager を使用してカスタマイズ検出を開始する手順は、次のとおりです。

ステップ 1　[VSAN] ドロップダウン メニューをクリックして、カスタマイズ検出を開始する VSAN を選択します。

ステップ 2　[FC] > [Advanced] > [LUNs] をクリックします。

[LUN Configuration] ダイアログボックスが表示されます。

ステップ 3　[StartDiscovery] を [local]、[remote]、または [both] に設定します。

ステップ 4　[DiscoveryType] フィールドおよび [OS] フィールドに入力します。

ステップ 5　[Apply] をクリックして、検出を開始します。

SCSI LUN 情報の表示

Device Manager を使用して検出結果を表示する手順は、次のとおりです。

ステップ 1　[FC] > [Advanced] > [LUNs] をクリックします。

[LUN Configuration] ダイアログボックスが表示されます。

ステップ 2　[LUN] タブまたは [Targets] タブをクリックします。

CHAPTER 11

FICON の設定

Fibre Connection（FICON）インターフェイスの機能は、開放型システムとメイン フレーム ストレージ ネットワーク環境の両方をサポートすることによって、Cisco MDS 9000 ファミリを拡張します。Control Unit Port（CUP）のサポートを含めた結果、FICON プロセッサからスイッチの帯域内管理ができるようになり、MDS オファリングが格段に拡張されています。

ファブリック バインディング機能は、無許可のスイッチがファブリックに接続したり、現在のファブリック操作を中断するのを防止するのに役立ちます（『*Cisco MDS 9000 Family NX-OS Security Configuration Guide*』を参照）。Registered Link Incident Report（RLIR）アプリケーションを使用することにより、スイッチ ポートから登録済み Nx ポートに LIR を送信できます。

（注） Cisco Fabric Manager リリース 3.x では、SAN-OS リリース 2.（x）を実行している Cisco MDS 9000 ファミリ スイッチでの FICON の管理はサポートされていません。

この章の内容は、次のとおりです。

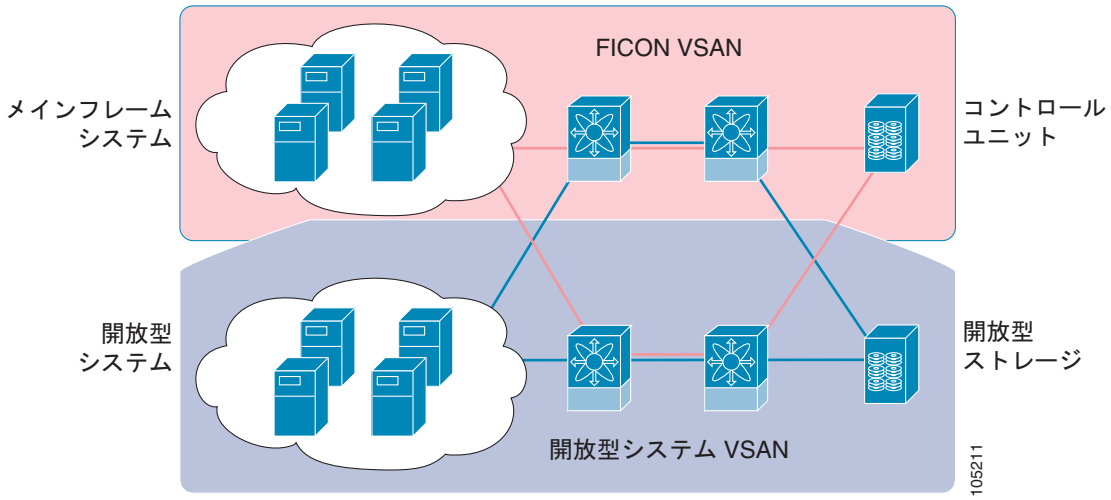
FICON の概要

FICON 機能は、以下ではサポートされていません。

- Cisco MDS 9120 スイッチ
- Cisco MDS 9124 スイッチ
- Cisco MDS 9140 スイッチ
- 32 ポート ファイバ チャネル スイッチング モジュール
- HP c-Class BladeSystem 用の Cisco ファブリック スイッチ
- IBM BladeSystem 用の Cisco ファブリック スイッチ

Cisco MDS 9000 ファミリは、単一のハイ アベイラビリティ プラットフォーム内で Fibre Channel Protocol（FCP）、FICON、iSCSI、および FCIP 機能をサポートします。このソリューションによって、購買を簡略化し、導入/管理コストを削減できるとともに、メインフレーム システムと開放型システムから共有されているストレージ ネットワークの複雑化を解消できます（図 11-1 を参照）。

図 11-1　共有システム ストレージ ネットワーク



FCP と FICON は別個の FC4 プロトコルであり、トラフィックは互いに独立しています。これらのプロトコルを使用しているデバイス間の切り離しには、VSAN を使用する必要があります。

ここで説明する内容は、次のとおりです。

- 「FICON の要件」（P.11-3）
- 「MDS 固有 FICON のメリット」（P.11-3）
- 「FICON のカスケード化」（P.11-8）
- 「FICON VSAN の前提条件」（P.11-8）

FICON の要件

FICON 機能の要件として、次のものが挙げられます。

- FICON 機能を実装できるスイッチは、次のとおりです。
  - Cisco MDS 9500 シリーズのあらゆるスイッチ
  - Cisco MDS 9200 シリーズのあらゆるスイッチ（例 : Cisco MDS 9222i マルチサービス モジュラ スイッチ）
  - Cisco MDS 9134 マルチレイヤ ファブリック スイッチ
  - MDS 9000 ファミリの 18/4 ポート マルチサービス モジュール
- FICON パラメータを設定するには、MAINFRAME_PKG のライセンスが必要です。FCIP が使用されている WAN 回線を介して FICON 設定を展開するには、使用しているモジュールに対応した所定の SAN_EXTN_OVER_IP ライセンスが必要です。詳細については、『*Cisco NX-OS Family Licensing Guide*』を参照してください。

MDS 固有 FICON のメリット

ここでは、Cisco MDS スイッチのその他の FICON のメリットについて説明します。また、次のトピックを取り上げます。

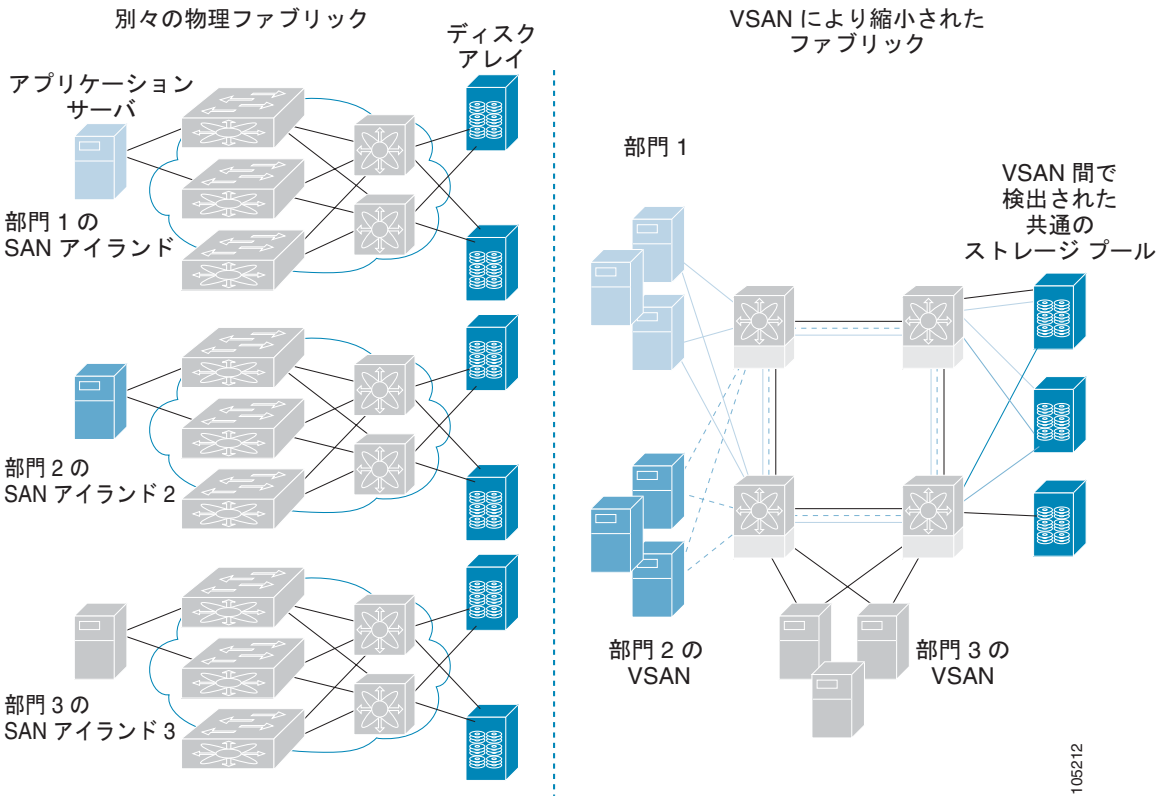
- 「VSAN によるファブリックの最適化」（P.11-3）
- 「FCIP のサポート」（P.11-5）
- 「ポートチャネルのサポート」（P.11-5）
- 「VSAN による、FICON と FCP の混在への対応」（P.11-5）
- 「Cisco MDS でサポートされている FICON 機能」（P.11-6）

VSAN によるファブリックの最適化

別々の物理ファブリックを実装すると、高度なスイッチ管理が必要になるため、実装コストがかさむのが一般的です。ファブリック設定によっては、各アイランド内のポートのプロビジョニングが過剰になることがあります。

Cisco MDS 固有の VSAN テクノロジーを導入すると、過剰なプロビジョニング コストの節減、および管理対象スイッチ数の軽減につながるため、これらの物理ファブリック間の効率を向上できます。また、VSAN を使用すると、中断せずに未使用ポートを移動し、共通の冗長物理インフラストラクチャを提供できます（図 11-2 を参照）。

図 11-2　VSAN 固有ファブリックの最適化



VSAN を使用すると、SAN のグローバル統合が可能になり、単一の物理ネットワーク上の既存の SAN アイランドを仮想 SAN アイランドに変換できます。これにより、ハードウェアレベルでセキュリティが適用され、アプリケーションどうしまたは部門どうしが切り離されて単一のネットワーク上で共存できるようになります。また、仮想再配線が可能になり、ストレージ インフラストラクチャが強化されます。機器に経費をかけたり機器の物理的再配置を破壊したりせずに、部門間またはアプリケーション間でアセットを移動できます。

（注）　どの Cisco MDS スイッチにも VSAN を設定できます。ただし、FICON をイネーブルにできる VSAN は 8 つ以下に限られます。設定可能な VSAN の数は、プラットフォームごとに異なります。

（注）　メインフレーム ユーザであれば、VSAN を MDS SAN ファブリック内の FICON LPAR と同様のものと考えればわかりやすいでしょう。スイッチ リソースは、互いに切り離された FICON LPAR（VSAN）にパーティション化できます。このパーティション化の操作は、zSeries または DS8000 上でリソースをパーティション化する操作とほぼ同じです。各 VSAN は、固有のファブリック サービス（たとえば、ファブリック サーバやネーム サーバ）、FICON コントロール ユニット ポート、ドメイン ID、Fabric Shortest Path First（FSPF）ルーティング、動作モード、IP アドレス、およびセキュリティ プロファイルのセットで構成されています。

FICON LPAR は複数のライン カードにわたって設置でき、そのサイズが動的に調整されます。たとえば、10 ポート付き FICON LPAR 1 つを 10 のラインカードにわたって設置することもできます。FICON LPAR には、カスケード設定の複数のスイッチのポートを含めることもできます。Cisco MDS 9000 スイッチング アーキテクチャには一貫した妥当性があるため、「すべてのポートが同等に作成」されます。

FICON LPAR へのポートの追加は、無中断プロセスです。FICON アドレス指定の制限を受けるため、FICON LPAR の最大ポート数は 255 です。

FCIP のサポート

Cisco MDS 9000 ファミリのマルチレイヤ アーキテクチャは、プロトコルを認識しないスイッチ ファブリックを介して一貫したフィーチャ セットを可能にしています。Cisco MDS 9500 シリーズおよび 9200 シリーズ スイッチは、ファイバ チャネル、FICON、および Fibre Channel over IP（FCIP）を 1 つのシステムに透過的に統合します。FICON over FCIP 機能を使用すると、遠く離れた場所にあるメインフレーム リソースにも、コスト効率よくアクセスできます。Cisco MDS 9000 ファミリのプラットフォームでは、ビジネス継続ストラテジをシンプルにするユビキタス IP インフラストラクチャを使用して、IBM PPRC や XRC などのストレージ レプリケーション サービスを、メトロを介してグローバルな距離にまで展開できます。

『*Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*』を参照してください。

ポートチャネルのサポート

FICON の Cisco MDS 実装では、効率的利用がサポートされているため、安定した大規模 SAN 環境の構築に要する Inter-Switch Link （ISL; スイッチ間リンク）のアベイラビリティが向上しています。Cisco MDS スイッチ内での ISL のアベイラビリティおよびパフォーマンスは、ポートチャネルによって強化されます。

ポートチャネルの詳細については、『*Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide*』を参照してください。

VSAN による、FICON と FCP の混在への対応

Cisco MDS 9000 ファミリの FICON 対応スイッチは、きわめて複雑な混在環境にも簡単に導入できるようになっています。各サービスに必要な VSAN を簡単に作成して、複数の論理 FICON、Z-Series Linux/FCP、および Open-Systems Fibre Channel Protocol（FCP）ファブリックを 1 つの物理ファブリックにオーバーレイできます。VSAN にはハードウェア隔離サービスとプロトコル固有のファブリック サービスの両方が用意されているため、ゾーンベースの混在方式のような複雑さがなく、不安定になるおそれもありません。

Cisco MDS 9000 ファミリのどのスイッチにおいても、FICON 機能はデフォルトでディセーブルになっています。FICON 機能がディセーブルのときは、FC ID をシームレスに割り当てることが可能です。Cisco NX-OS ソフトウェアは混在環境に対応しています。FCP プロトコルと FICON プロトコルの混在に関する問題は、VSAN を実装すれば、Cisco MDS スイッチによって対処されます。

Cisco MDS 9000 ファミリのスイッチおよびディレクタは、FCP プロトコルと FICON プロトコルの混在をポートレベルでサポートしています。これらのプロトコルが同一スイッチ内に混在している場合は、VSAN を使用して FCP ポートと FICON ポートを切り離せます。

ヒント　混在環境を作成する際は、すべての FICON デバイスを（デフォルト VSAN 以外の）1 つの VSAN に配置し、FCP スイッチ ポートを（デフォルト VSAN 以外の）別個の VSAN に隔離してください。このようにして FCP と FICON を切り離すことにより、接続しているすべてのデバイスに対して正常な通信が保証されます。

Cisco MDS でサポートされている FICON 機能

Cisco MDS 9000 ファミリの FICON 機能としては、次のものがあります。

- 柔軟性と投資の保護：Cisco MDS 9500 シリーズおよび 9200 シリーズ間で共通のスイッチング モジュールとサービス モジュールは、Cisco MDS 9000 ファミリによって共有されます。

  『*Cisco MDS 9500 Series Hardware Installation Guide*』および『*Cisco MDS 9200 Series Hardware Installation Guide*』を参照してください。

- ハイ アベイラビリティ FICON 対応ディレクタ：Cisco MDS 9500 シリーズは、すべての主要コンポーネントに対して稼動中のソフトウェア アップグレード、ステートフルなプロセス再起動/フェールオーバー、および十分な冗長性を可能にしたことで、ディレクタ クラスのアベイラビリティの新標準に準拠しています。4/2/1 Gbps、10 Gbps の自動検知 FICON ポートまたは FCP ポートの任意の組み合せを最大 528 個まで 1 つのシャーシに搭載できます。『*Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide*』を参照してください。

- インフラストラクチャの保護：共通ソフトウェア リリースによって、すべての Cisco MDS 9000 プラットフォーム間でインフラストラクチャを保護できます。『*Cisco MDS 9000 Family NX-OS Software Upgrade and Downgrade Guide*』を参照してください。

- VSAN テクノロジー：Cisco MDS 9000 ファミリには、ハードウェアレベルで適用される VSAN テクノロジーが採用されています。VSAN テクノロジーは、単一物理ファブリック内の隔離環境に対応しているため、物理インフラストラクチャを安全に共有しながら、FICON 混在のサポートを強化できます。第 2 章「VSAN の設定と管理」を参照してください。

- ポートレベルでの設定：BB_credits、ビーコン モード、およびポート セキュリティをポートごとに設定できます。バッファ間クレジット、ビーコン LED、およびトランキングについては、『*Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide*』を参照してください。

- エイリアス名の設定：スイッチおよび接続されているノード デバイスに、WWN でなくユーザフレンドリなエイリアスを設定できます。第 5 章「ゾーンの設定と管理」を参照してください。

- 包括的なセキュリティ フレームワーク：Cisco MDS 9000 ファミリは、RADIUS および TACACS+ 認証、Simple Network Management Protocol Version 3（SNMPv3; 簡易ネットワーク管理プロトコル バージョン 3）、ロールベース アクセス コントロール、Secure Shell Protocol（SSH; セキュア シェル プロトコル）、Secure File Transfer Protocol（SFTP; セキュア ファイル転送プロトコル）、VSAN、ハードウェアベースのゾーン分割、ACL、ファブリック バインディング、Fibre Channel Security Protocol（FC-SP）、LUN ゾーン分割、読み取り専用ゾーン、および VSAN ベースのアクセス コントロールをサポートしています。RADIUS、TACACS+、FC-SP、および DHCHAP の詳細については、『*Cisco MDS 9000 Family NX-OS Security Configuration Guide*』を参照してください。

- トラフィックの暗号化：FCIP を介した IP セキュリティがサポートされています。FCIP を介して伝送された FICON およびファイバ チャネル トラフィックを暗号化できます。『*Cisco MDS 9000 Family NX-OS Security Configuration Guide*』を参照してください。
- ローカル アカウンティング ログ：ローカル アカウンティング ログを表示して、FICON イベントを検出できます。MSCHAP 認証およびローカル AAA サービスの詳細については、『*Cisco MDS 9000 Family NX-OS Security Configuration Guide*』を参照してください。
- 統合型ストレージ管理：Cisco MDS 9000 FICON 対応スイッチは、IBM CUP 規格に適合しており、IBM S/A OS/390 I/O 操作コンソールを使用した帯域内管理が可能です。「CUP 帯域内管理」（P.11-41）を参照してください。
- ポート アドレスベースの設定：ポート名、ブロック ステートまたはブロック解除ステート、および接続制限属性を設定します。「FICON ポートの設定」（P.11-26）を参照してください。
- 表示できる情報には、次のものがあります。
  - 個別のファイバ チャネル ポート（例：ポート名、ポート番号、ファイバ チャネル アドレス、動作ステート、ポート タイプ、ログイン データなど）
  - ポートに接続されているノード
  - ポートのパフォーマンスおよび統計情報

  「FICON フロー ロードバランスの計算」（P.11-42）を参照してください。
- コンフィギュレーション ファイル：コンフィギュレーション ファイルを保存し、適用します。「FICON コンフィギュレーション ファイル」（P.11-30）を参照してください。
- FICON および開放型システム管理サーバ機能（インストール済みの場合）。「VSAN による、FICON と FCP の混在への対応」（P.11-5）を参照してください。
- 拡張カスケード サポート：「CUP 帯域内管理」（P.11-41）を参照してください。
- 日時：スイッチの日時設定を行います。「ホストでタイムスタンプを制御できるようにする」（P.11-23）を参照してください。
- SNMP トラップの受け取り側およびコミュニティ名を設定します（「FICON パラメータの SNMP 制御の設定」（P.11-24）を参照）。
- コール ホームの設定：ディレクタ名、場所、説明、および担当者を設定します。『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。
- 優先するドメイン ID、FC ID の永続性、および主要スイッチの優先度の設定：ドメイン パラメータの設定の詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。
- 高度な SPAN 診断:Cisco MDS 9000 ファミリは、業界初のインテリジェント診断、プロトコル デコーディング、ネットワーク分析ツール、および統合型コール ホーム機能の搭載によって、信頼性の向上、問題解決の迅速化、およびサービス コストの削減を実現しています。SPAN を使用したネットワーク トラフィックのモニタリングの詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。
- R_A_TOV、E_D_TOV の設定：「ファイバ チャネル タイムアウト値」（P.12-2）を参照してください。
- ディレクタレベルのメンテナンス作業：障害分析をサポートするために、ディレクタのメンテナンス作業（たとえば、ファームウェア レベルのメンテナンス、ディレクタ ログへのアクセス、データ収集など）を実行します。システム プロセスおよびログのモニタリングの詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。

FICON のカスケード化

Cisco MDS NX-OS ソフトウェアを使用して、FICON ネットワーク内で複数のスイッチの共存が可能になります。複数のスイッチを設定するには、該当スイッチ内でファブリック バインディングをイネーブルにし、設定する必要があります（「FICON フロー ロードバランスの計算」（P.11-42）、および『*Cisco MDS 9000 Family NX-OS Security Configuration Guide*』を参照）。

FICON VSAN の前提条件

FICON VSAN を稼動状態にするには、次の前提条件を満たしているかどうか確認してください。

- ゾーン分割機能を使用していない場合は、デフォルト ゾーンを許可するように設定します。「デフォルト ゾーンの概要」（P.5-21）を参照してください。
- VSAN 上で順序どおりの配信をイネーブルにします。第 7 章「ファイバ チャネル ルーティング サービスおよびプロトコルの設定」を参照してください。
- VSAN 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（必要に応じて設定します）。「FICON フロー ロードバランスの計算」（P.11-42）を参照してください。ファブリック バインディングの詳細については、『*Cisco MDS 9000 Family NX-OS Security Configuration Guide*』を参照してください。
- スイッチ内に衝突する永続 FC ID が存在していないことを確認します。ドメイン パラメータの設定の詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。
- 設定済みドメイン ID と要求したドメイン ID が一致していることを確認します。ドメイン パラメータの設定の詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。
- ゾーン分割を使用している場合は、ゾーンに CUP （エリア FE）を追加します。「CUP 帯域内管理」（P.11-41）を参照してください。

上記の前提条件がいずれか 1 つでも満たされていないと、FICON 機能をイネーブルにできません。

FICON ポート番号の設定

FICON 機能に関しては、Cisco MDS スイッチ内のポートが、静的に定義された 8 ビット値（*ポート番号*）で識別されます。ポート番号は、最大 255 個まで使用できます。使用できるポート番号設定方式には、次のものがあります。

- シャーシ タイプに基づくデフォルト ポート番号
- 予約済みポート番号

ここで説明する内容は、次のとおりです。

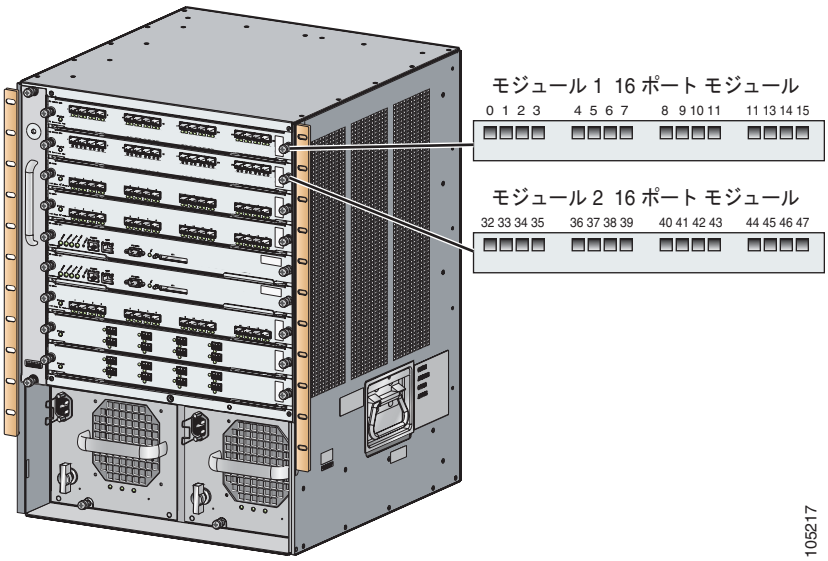
- 「FCIP およびポートチャネルのポート番号の概要」（P.11-14）
- 「予約済み FICON ポート番号設定方式の概要」（P.11-12）
- 「FC ID の割り当て」（P.11-15）

（注）　FICON ポート番号を予約する前に、スイッチ上で FICON をイネーブルにしておく必要があります（「VSAN の FICON をイネーブルにする操作の概要」（P.11-17）を参照）。

デフォルトの FICON ポート番号設定方式

Cisco MDS NX-OS ソフトウェアは、シャーシ内のモジュールとスロットに基づいて、デフォルトの FICON ポート番号を割り当てます。スイッチ内の最初のポートは、常にゼロ（0）で開始します（図 11-3 を参照）。

図 11-3　Cisco MDS 9000 ファミリ スイッチのデフォルトの FICON ポート番号設定



デフォルトの FICON ポート番号は、前面パネル上のポートの位置に基づいて、モジュールが属しているスロットに固有の値が割り当てられます。Cisco MDS 9513 ディレクタの場合、各スロットに 16 個のポート番号が割り当てられています。それ以外の Cisco MDS 9000 ファミリ スイッチではいずれも、各スロットに 32 個のポート番号が割り当てられています。これらのデフォルト番号は、シャーシ内にモジュールが物理的に存在するかどうか、ポートのステータス（アップまたはダウン）、またはモジュールのポート数（4、12、16、24、または 48）に関係なく割り当てられます。モジュールのポートの数の方が、スロットに割り当てられたポート番号の個数よりも少ない場合、超過分のポート番号は使用されません。モジュールのポート数が、スロットに割り当てられたポート番号の個数よりも多い場合、ポート番号を手動で割り当てない限り、超過分のポートは FICON に使用できません。

（注）　超過分のポートを利用するには、「スロットへの FICON ポート番号の割り当て」（P.11-14）の手順に従って 、手動でさらに他のポート番号をスロットに割り当てます。ただし、この手順を実行する前に、Cisco MDS 9000 スイッチのデフォルトのポート番号の割り当て（ 表 11-3（P.11-46））を確認し、「予約済み FICON ポート番号設定方式の概要」（P.11-12）セクション、「FICON ポート番号設定に関するガイドライン」（P.11-13）セクション、および「スロットへの FICON ポート番号の割り当て」（P.11-14）セクションを読んで、FICON ポートの番号設定を十分に理解しておくことをお勧めします。

（注）　FICON ポート番号にマッピングされるのは、ファイバ チャネル、ポートチャネル、および FCIP ポートだけです。それ以外のタイプのインターフェイスでは、対応するポート番号が生成されません。

表 11-3 は、Cisco MDS 9000 ファミリのスイッチおよびディレクタ用のデフォルトのポート番号の割り当ての一覧です。

表 11-1　Cisco MDS 9000 ファミリのデフォルト FICON ポート番号

製品	スロット番号	実装ポート割り当て		非実装ポート	注意
		割り当て先ポート	割り当て先ポートチャネル/FCIP		
Cisco MDS 9200 シリーズ	スロット 1	0 ～ 31	64 ～ 89	90 ～ 253、およびポート 255	スイッチング モードと同様。
	スロット 2	32 ～ 63			
Cisco MDS 9222i シリーズ	スロット 1	0 ～ 31	64 ～ 89	90 ～ 253、およびポート 255	4 ポート、12 ポート、16 ポート、または 24 ポートのモジュールでは、最初の 4、12、16、または 24 個のポート番号が使用され、残りは未使用のままです。48 ポート モジュール上の余分な 16 個のポートには、ポート番号が割り当てられません。
	スロット 2	32 ～ 63			
Cisco MDS 9506 ディレクタ	スロット 1	0 ～ 31	128 ～ 153	154 ～ 253、およびポート 255	スーパーバイザ モジュールにはポート番号が割り当てられません。
	スロット 2	32 ～ 63			
	スロット 3	64 ～ 95			
	スロット 4	96 ～ 127			
	スロット 5	なし			
	スロット 6	なし			
Cisco MDS 9134 ディレクタ	スロット 1	0 ～ 33	34 ～ 59	60 ～ 253、およびポート 255	

表 11-1　Cisco MDS 9000 ファミリのデフォルト FICON ポート番号 （続き）

製品	スロット番号	実装ポート割り当て		非実装ポート	注意
		割り当て先ポート	割り当て先ポートチャネル/FCIP		
Cisco MDS 9509 ディレクタ	スロット 1	0 ～ 31	224 ～ 249	250 ～ 253、およびポート 255	4 ポート、12 ポート、16 ポート、または 24 ポートのモジュールでは、最初の 4、12、16、または 24 個のポート番号が使用され、残りは未使用のままです。48 ポート モジュール上の余分な 16 個のポートには、ポート番号が割り当てられません。
	スロット 2	32 ～ 63			
	スロット 3	64 ～ 95			
	スロット 4	96 ～ 127			
	スロット 5	なし			スーパーバイザ モジュールにはポート番号が割り当てられません。
	スロット 6	なし			
	スロット 7	128 ～ 159			4 ポート、12 ポート、16 ポート、または 24 ポートのモジュールでは、最初の 4、12、16、または 24 個のポート番号が使用され、残りは未使用のままです。48 ポート モジュール上の余分な 16 個のポートには、ポート番号が割り当てられません。
	スロット 8	160 ～ 191			
	スロット 9	192 ～ 223			
Cisco MDS 9513 ディレクタ	スロット 1	0 ～ 15	224 ～ 249	250 ～ 253、およびポート 255	4 ポート、12 ポート、または 16 ポートのモジュールでは、最初の 4、12、または 16 個のポート番号が使用され、残りは未使用のままです。24 ポート、32 ポート、および 48 ポートのモジュール上の余分なポートには、ポート番号が割り当てられません。
	スロット 2	16 ～ 31			
	スロット 3	32 ～ 47			
	スロット 4	48 ～ 63			
	スロット 5	64 ～ 79			
	スロット 6	80 ～ 95			
	スロット 7	なし			スーパーバイザ モジュールにはポート番号が割り当てられません。
	スロット 8	なし			
	スロット 9	96 ～ 111			4 ポートまたは 12 ポートのモジュールでは、最初の 4 または 12 個のポート番号が使用され、残りは未使用のままです。24 ポート、32 ポート、および 48 ポートのモジュール上の余分なポートには、ポート番号が割り当てられません。
	スロット 10	112 ～ 127			
	スロット 11	128 ～ 143			
	スロット 12	144 ～ 159			
	スロット 13	160 ～ 175			

ポート アドレス

デフォルトでは、ポート番号はポート アドレスと同じです。ポート アドレスはスワッピングできます（「ポート スワッピング」（P.11-34）を参照）。

実装ポートおよび非実装ポートのアドレス

実装ポートとは、デフォルトでシャーシ内のスロットに割り当てられるすべてのポート アドレスです（表 11-3 を参照）。非実装ポートとは、デフォルトでシャーシ内のスロットに割り当てられないすべてのポート アドレスです（表 11-3 を参照）。

予約済み FICON ポート番号設定方式の概要

250 個のポート番号のいずれかを使用して、スイッチ上のすべてのポートへの割り当てができます。表 11-3 に示すように、スイッチの物理ポート数が 250 個を超えた場合、デフォルト番号設定方式では超過分のポートにポート番号を設定できません。スイッチの物理ポート数が 250 個を超えた場合は、FICON VSAN に存在しないポートにはポート番号を割り当てないでおく、あるいは同一の FICON VSAN で使用されていない重複ポート番号を割り当てるなどの方法で対処できます。たとえば、FICON VSAN 10 のインターフェイス fc1/1、および FICON VSAN 20 のインターフェイス fc10/1 に、ポート番号 1 を設定できます。

（注）　1 つの VSAN に設定できるポート数は、最大 250 個です。

（注）　アクティブになっているポートの FICON ポート番号は変更されません。最初に **shutdown** コマンドを使用して、インターフェイスをディセーブルにする必要があります。

（注）　スロットにモジュールが設置されていない場合でも、ポート番号を設定できます。

インストレーション ポートおよび非インストレーション ポート

インストレーション ポートとは、必要なすべてのハードウェアが搭載されているポートです。次の条件のいずれか 1 つが適用される場合、VSAN 内の指定のポート番号を実装ポートにできます。ただし、インストレーション ポートにはできません。

- モジュールが存在しない場合（たとえば、モジュール 1 が Cisco MDS 9509 ディレクタのスロット 1 に物理的に存在していない場合）、ポート番号 0 ～ 31 は非インストレーション ポートと見なされます。
- Small Form-factor Pluggable（SFP）ポートが存在しない場合（たとえば、Cisco MDS 9509 ディレクタのスロット 2 に 16 ポート モジュールが挿入されている場合）、ポート 48 ～ 63 は非インストレーション ポートと見なされます。

- スロット 1 には、ポート 0 ～ 31、またはポート 0 ～ 15 が割り当てられています。VSAN 2 内に存在する物理ポートは、ポート番号 4 の 物理ポート fc1/5 だけです。残りの物理ポートは VSAN 2 内に存在していません。FICON 対応 VSAN では常に、ポート番号 0 ～ 249 は実装ポートと見なされます。つまり、VSAN 2 に存在しているのは、ポート番号 0 ～ 249 と、1 つの物理ポート fc1/4 です。対応する物理ポート 0 ～ 3、および 5 ～ 249 は VSAN 2 内に存在しません。これらのポート番号は VSAN 2 内に物理ポートが存在しないため、FICON VSAN ポート アドレスを表示したときにインストレーション ポート（例：ポート 0 ～ 3、5 ～ 249 など）としては表示されません。

  もう 1 つのシナリオは、VSAN 1 ～ 5 が FICON に対応していて、トランキング対応インターフェイス fc1/1 に VSAN 3 ～ 10 が設定してある場合です。この場合、VSAN 1 と VSAN 2 ではポート アドレス 0 が非インストレーション ポートになります。
- 該当のポートがポートチャネルの一部であると想定した場合（たとえば、インターフェイス fc 1/1 がポートチャネル 5 に属している場合）、すべての FICON VSAN でポート アドレス 0 が非インストレーション ポートになります。表 11-3 を参照してください。

FICON ポート番号設定に関するガイドライン

FICON ポート番号には、次のガイドラインが適用されます。

- スーパーバイザ モジュールには、ポート番号割り当てがありません。
- ポート番号は TE ポートに応じて変更されません。TE ポートは複数の VSAN で使用されるため、TE ポート用にシャーシ規模の一意のポート番号を予約しておく必要があります。
- 各ポートチャネルを FICON ポート番号に明示的に関連付ける必要があります。
- 物理ポートチャネルのポート番号が非インストレーション ポートと一致したとき、その物理ポートには、関連するポートチャネルの設定が適用されます。
- 各 FCIP トンネルを FICON ポート番号に明示的に関連付ける必要があります。ポートチャネルまたは FCIP トンネルに対してポート番号が割り当てられていない場合、関連付けられているポートは起動しません。

  「FCIP およびポートチャネルのポート番号の概要」（P.11-14）を参照してください。

スロットへの FICON ポート番号の割り当て

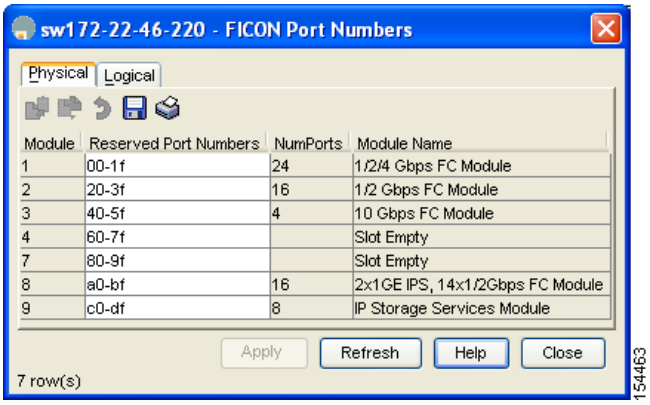
注意　ポート番号を割り当て、変更、またはリリースすると、ポートが再ロードされます。

Device Manager を使用して FICON ポート番号を割り当てる手順は、次のとおりです。

ステップ 1　[FICON] をクリックして、[Port Numbers] を選択します。

FICON ポート番号が表示されます（図 11-4 を参照）。

図 11-4　FICON ポート番号



ステップ 2　[Reserved Port Numbers] フィールドにシャーシ スロット ポート番号を入力します。

ステップ 3　[Apply] をクリックします。

FCIP およびポートチャネルのポート番号の概要

FCIP およびポートチャネルは、ポート番号に明示的にバインドしておかないと、FICON 対応 VSAN で使用できません。

「FICON ポートの設定」（P.11-26）および「FICON およびポートチャネル インターフェイス用の FICON ポート番号の予約」（P.11-14）を参照してください。

デフォルト ポート番号が使用可能な場合（表 11-1（P.11-10）を参照）、あるいはファイバ チャネル インターフェイス用に予約されていないポート番号のプールからポート番号を予約する場合（「FICON ポート番号の設定」（P.11-8）を参照）、デフォルト ポート番号を使用できます。

FICON およびポートチャネル インターフェイス用の FICON ポート番号の予約

FCIP やポートチャネルなどの論理インターフェイスを使用する予定がある場合は、使用する論理インターフェイス用にポート番号を予約しておく必要があります。

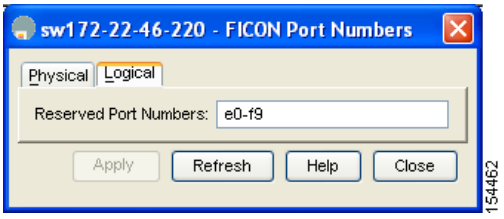
Device Manager を使用して FCIP およびポートチャネル インターフェイス用に FICON ポート番号を予約する手順は、次のとおりです。

ステップ 1　[FICON] > [Port Numbers] をクリックします。

[FICON port numbers] ダイアログボックスが表示されます（図 11-4 を参照）。

ステップ 2　[Logical] タブをクリックして、スロット用に予約されているポート番号を表示します（図 11-5 を参照）。

図 11-5　選択したスロット用に予約されているポート番号



ステップ 3　シャーシ スロットのポート番号を入力します。このポート番号は、あるシャーシ スロット用に予約されているポート番号です。シャーシ内のスロットごとに、最大 64 個のポート番号を予約できます。

ステップ 4　[Apply] をクリックします。

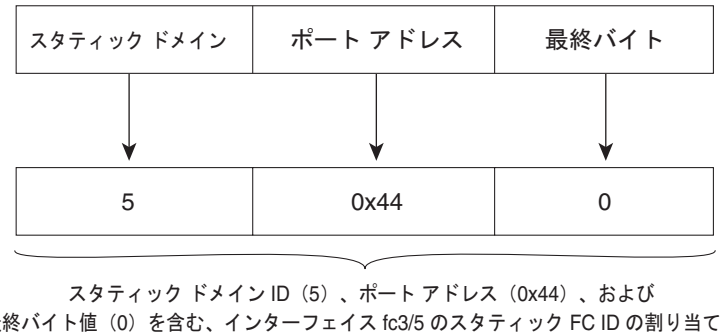
FC ID の割り当て

FICON には予測可能なスタティック FC ID 割り当て方式が必要です。FICON がイネーブルのときは、接続先ポートのポート アドレスに応じた FC ID がデバイスに割り当てられます。ポートアドレスは、ファブリック アドレスの中央バイトを構成しています。また、ファブリック内のデバイスはすべて、ファブリック アドレスの最終バイトが同一である必要があります。最終バイト値はデフォルトでは 0 ですが、他の値を設定することも可能です（「FC ID の最終バイトの割り当て」（P.11-22）を参照）。

（注）　FICON 対応 VSAN では、固定的 FC ID を設定できません

Cisco MDS スイッチ用に、ダイナミック FC ID 割り当て方式が用意されています。VSAN 上で FICON をイネーブルまたはディセーブルにすると、すべてのポートがシャット ダウンし、ダイナミック FC ID からスタティック FC ID に、あるいはその逆方向にスイッチングされます（図 11-6 を参照）。

図 11-6　FICON 用スタティック FC ID の割り当て



スタティック ドメイン ID（5）、ポート アドレス（0x44）、および最終バイト値（0）を含む、インターフェイス fc3/5 のスタティック FC ID の割り当て。

FICON の設定

Cisco MDS 9000 ファミリのどのスイッチにおいても FICON はデフォルトでディセーブルになります。Device Manager を使用すると、VSAN 単位で FICON をイネーブルにできます。

ここで説明する内容は、次のとおりです。

VSAN の FICON をイネーブルにする操作の概要

スイッチ上のどの VSAN においても FICON はデフォルトでディセーブルになります。

VSAN 単位で FICON をイネーブルにするには、次の方法があります。

- 各前提条件を手動でアドレッシングします。

  「FICON の概要」（P.11-2）を参照してください。

- Device Manager を使用します。

Cisco MDS スイッチで FICON FICON 機能をイネーブルにすると、次の制約が適用されます。

- FICON 対応 VSAN では、順序どおりの配信をディセーブルにできません。
- FICON 対応 VSAN では、ファブリック バインディングまたはスタティック ドメイン ID 設定をディセーブルにできません。
- ロードバランシング方式が Source ID（SID）-Destination ID（DID）に変更されます。SID—DID—OXID に戻すことはできません。
- IPL コンフィギュレーション ファイルが自動的に作成されます。

  「FICON コンフィギュレーション ファイルの概要」（P.11-31）を参照してください。

ヒント　同一の FICON 対応スイッチにログオンしている複数ユーザは、Device Manager を使用して、FICON の自動保存を起動できます。Device Manager は FICON 対応スイッチであれば機種に関係なく定期自動保存を実行するため、結果として FICON キー カウンタが増加します。キー カウンタの増加から、実際には発生しなかった変更を特定できます。こうした変更を回避するために、FICON 対応スイッチを Device Manager の 1 インスタンスだけに監視させる設定を推奨します。

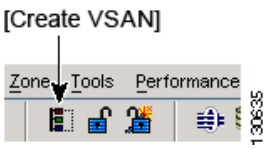
基本 FICON 設定のセットアップ

ここでは、Cisco MDS 9000 ファミリ スイッチの特定の VSAN で FICON をセットアップする方法を、手順を追って説明します。

Fabric Manager を使用して FICON 対応 VSAN を作成する手順は、次のとおりです。

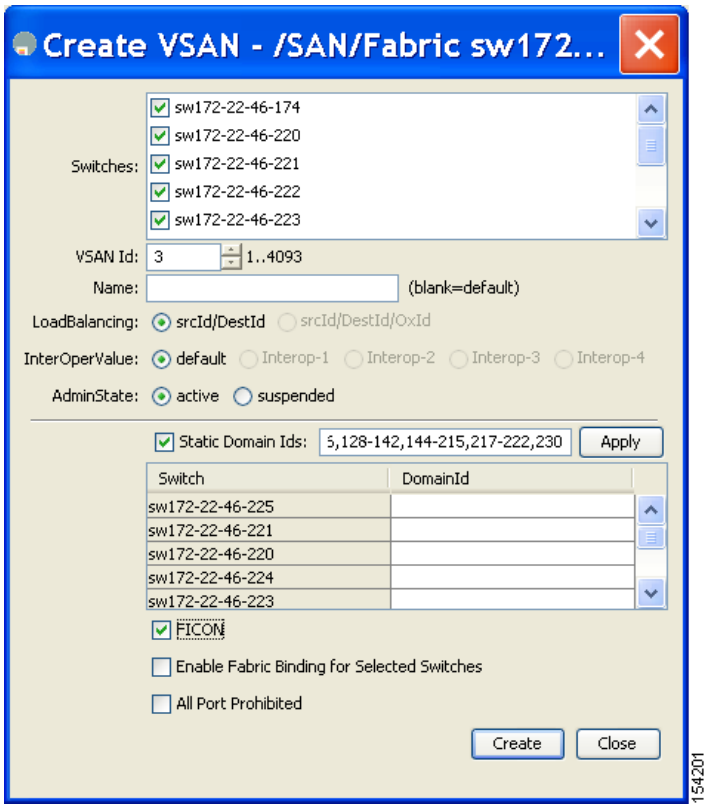
ステップ 1　[Create VSAN] アイコンをクリックします（図 11-7 を参照）。

図 11-7　[Create VSAN] アイコン



[Create VSAN] ダイアログボックスが表示されます（図 11-8 を参照）。

図 11-8　[Create VSAN] ダイアログボックス



ステップ 2　VSAN に追加するスイッチを選択します。

ステップ 3　VSAN ID を入力します。

ステップ 4　必要に応じて、VSAN の名前を入力します。

ステップ 5　この VSAN 用にロードバランシングのタイプ、INTEROP 値、および管理ステートを選択します。

ステップ 6　[FICON] チェックボックスをオンにします。

（注）　FICON 対応 VSAN では、INTEROP モードをイネーブルにできません。

ステップ 7　必要に応じて、選択したスイッチのファブリック バインディングをイネーブルにするオプションをオンにします。

ステップ 8　この VSAN 内のすべてのポートを禁止する場合は、[All Ports Prohibited] オプションをオンにします。

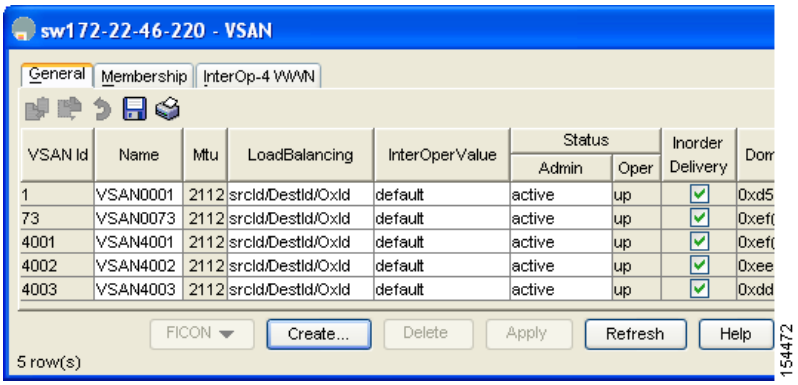
ステップ 9　[Create] をクリックして、VSAN を作成します。

ステップ 10　[Tools] > [Device Manager] を選択して、FICON VSAN でスイッチごとに Device Manager を開きます。

ステップ 11　[FC] > [VSANs] をクリックします。

[VSAN] ダイアログボックスが表示されます（図 11-9 を参照）。

図 11-9　Device Manager の [VSAN] ダイアログボックス



ステップ 12　VSAN メンバシップ情報を入力します。

ステップ 13　FICON VSAN にする VSAN をクリックし、[FICON] ドロップダウン メニューから [Add] を選択します。

ステップ 14　[Apply] をクリックして、変更内容を保存します。

VSAN での手動での FICON のイネーブル化

（注）　ここでは、VSAN 上で手動で FICON をイネーブルにする手順について説明します。自動セットアップを使用して（推奨）、所定の VSAN 上で FICON をイネーブルにしてある場合は、「実行コンフィギュレーションの自動保存」（P.11-25）に進んでください。

Fabric Manager を使用して VSAN 上で FICON を手動でイネーブルにする手順は、次のとおりです。

ステップ 1　[VSAN] > [FICON] を選択します。

[Information] ペインに FICON VSAN 設定情報が表示されます。

ステップ 2　VSAN 内で、FICON をイネーブルにするスイッチを選択します。

ステップ 3　[Command] ドロップダウン メニューで [enable] をクリックします。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

FICON VSAN の削除

Fabric Manager を使用して FICON VSAN を削除する手順は、次のとおりです。

ステップ 1　[All VSANS] を選択します。

[Information] ペインに VSAN テーブルが表示されます（図 11-10 を参照）。

図 11-10　[All VSANs] テーブル

ステップ 2　削除する VSAN の行内の任意の場所をクリックします。

ステップ 3　[Delete Row] をクリックして、VSAN を削除します。

（注）　VSAN を削除すると、関連付けられている FICON コンフィギュレーション ファイルも削除されます。ファイルを元に戻すことはできません。

FICON VSAN の一時停止

Fabric Manager を使用して FICON 対応 VSAN を一時停止する手順は、次のとおりです。

ステップ 1　[All VSANs] をクリックします。

[Information] ペインに、すべての VSAN が一覧表示されます。

ステップ 2　一時停止する VSAN を選択します。

ステップ 3　VSAN 用の [Admin] ドロップダウン メニューを [suspended] に設定します。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

（注）　このコマンドは、このコマンドの発行が許可されているホストから発行できます（「ホストでスイッチをオフラインに移行できるようにするには」（P.11-22）を参照）。

[code-page] オプションの設定

FICON ストリングは、Extended Binary-Coded Decimal Interchange Code（EBCDIC; 拡張 2 進化 10 進コード）フォーマットで符号化されます。コード ページ オプションの詳細については、メインフレームのマニュアルを参照してください。

Cisco MDS スイッチでは、**international-5**、**france**、**brazil**、**germany**、**italy**、**japan**、**spain-latinamerica**、**uk**、および **us-canada**（デフォルト）の EBCDIC フォーマット オプションがサポートされています。

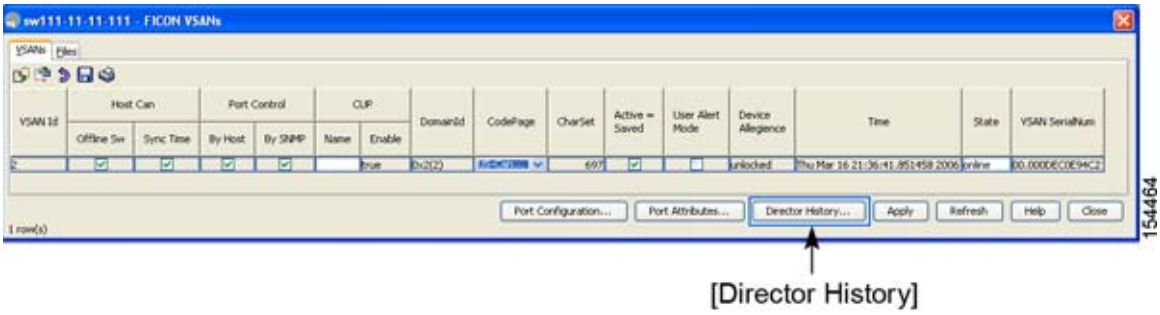
ヒント　この設定は任意指定です。どの EBCDIC フォーマットを使用したらよいかわからない場合は、[us-canada]（デフォルト）オプションをそのまま使用することをお勧めします。

Device Manager を使用して [code-page] オプションを変更する手順は、次のとおりです。

ステップ 1　[FICON] > [VSANs] を選択します。

[FICON VSAN] 設定ダイアログボックスが表示されます（図 11-11 を参照）。デフォルトのタブは、[VSANs] タブです。

図 11-11　Device Manager の [FICON VSANs] タブ



ステップ 2　設定する FICON VSAN の [CodePage] ドロップダウン メニューで、オプションを選択します（US-Canada の設定については、図 11-11 を参照してください）。

ステップ 3　[Apply] をクリックして、変更内容を保存します。

FC ID の最終バイトの割り当て

注意　FICON 機能がカスケード モードで設定されている場合、Cisco MDS スイッチは ISL を使用して、他のスイッチに接続します。

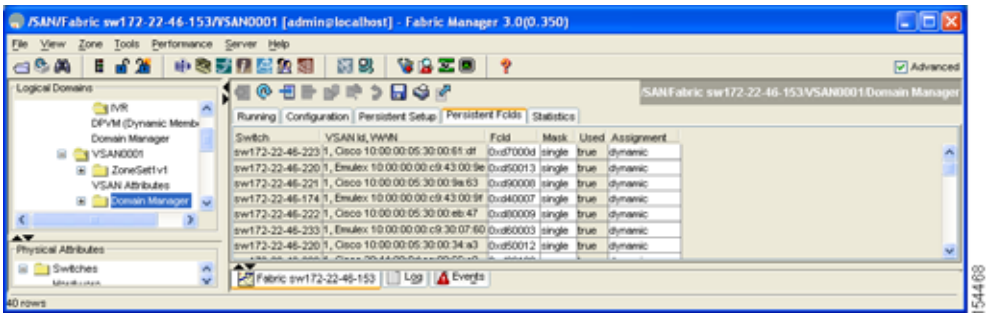
Fabric Manager を使用して FC ID の最終バイトを割り当てる手順は、次のとおりです。

ステップ 1　[All VSANs] > [Domain Manager] を選択します。

ステップ 2　[Persistent FC ID] タブをクリックします。

[Persistent FcIds] タブが表示されます（図 11-12 を参照）。

図 11-12　[Persistent FcIds] タブ



ステップ 3　[Mask] 列で [single] を選択し、FC ID 全体を一括して割り当てます。[single] オプションを選択した場合、FC ID を ###### フォーマットで入力できます。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

ホストでスイッチをオフラインに移行できるようにするには

デフォルトでは、ホストでスイッチをオフライン状態に移行できます。デフォルト設定のままスイッチをオフラインにするには、ホストから "Set offline" コマンド（x'FD'）を Control Unit Port（CUP）に送信します。

ホスト（メインフレーム）で Fabric Manager を使用して、スイッチをオフライン状態に移行できるようにする手順は、次のとおりです。

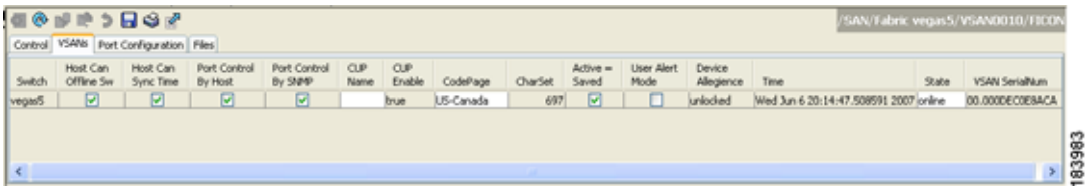
ステップ 1　[VSAN] > [FICON] を選択します。

[Information] ペインの [Control] タブに、スイッチが一覧表示されます。

ステップ 2　[VSANs] タブをクリックします。

[Information] ペインに FICON VSAN 設定情報が表示されます（図 11-13 を参照）。

図 11-13　Fabric Manager の FICON VSANs



ステップ 3　[Host Can Offline Sw] チェックボックスをオンにして、メインフレームでスイッチをオフライン状態に移行できるようにします。

ステップ 4　[Host Can Sync Time] チェックボックスをオンにして、メインフレームでスイッチのシステム時刻を設定できるようにします。

ステップ 5　[Apply Changes] アイコンをクリックして、変更内容を保存します。

ホストで FICON ポート パラメータを変更できるようにするには

デフォルトでメインフレーム ユーザに許可されるのはスイッチのクエリーだけであり、Cisco MDS スイッチの FICON パラメータ設定は許可されません。

Fabric Manager を使用して、ホスト（メインフレーム）で Cisco MDS スイッチの FICON パラメータ設定を許可する手順は、次のとおりです。

ステップ 1　[VSAN] > [FICON] を選択します。

[Information] ペインの [Control] タブに、スイッチが一覧表示されます。

ステップ 2　[VSANs] タブをクリックします。

[Information] ペインに FICON VSAN 設定情報が表示されます（図 11-13 を参照）。

ステップ 3　[Port Control By Host] チェックボックスをオンにして、メインフレームでスイッチを制御できるようにします。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

ホストでタイムスタンプを制御できるようにする

デフォルトでは、各 VSAN のクロックはスイッチ ハードウェアと同一のクロックになります。Cisco MDS 9000 ファミリ スイッチにおいて各 VSAN は、仮想ディレクタとなっています。仮想ディレクタごとに、表示されるクロックと時刻が異なることがあります。VSAN ごとの別々のクロックを保守するために、VSAN 固有のクロックとハードウェアベースのディレクタ クロックとの差分が Cisco NX-OS ソフトウェアによって保守されています。ホスト（メインフレーム）で時刻が設定されると、クロック間の差異が Cisco NX-OS ソフトウェアにより更新されます。ホストがクロックを読み取ると、VSAN クロックと現在のディレクタ ハードウェア クロックとの差分が計算され、値がメインフレームに提示されます。

Fabric Manager を使用して、ホスト（メインフレーム）での VSAN タイム スタンプ制御を設定する手順は、次のとおりです。

ステップ 1　[VSAN] > [FICON] を選択します。

[Information] ペインの [Control] タブに、スイッチが一覧表示されます。

ステップ 2　[VSANs] タブをクリックします。

[Information] ペインに FICON VSAN 設定情報が表示されます（図 11-13 を参照）。

ステップ 3　[Host Can Sync Time] チェックボックスをオンにして、メインフレームでスイッチのシステム時刻を設定できるようにします。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

FICON パラメータの SNMP 制御の設定

デフォルトでは、SNMP ユーザは Cisco MDS 9000 ファミリの Fabric Manager で FICON パラメータを設定できます。

（注）　Cisco MDS スイッチで SNMP をディセーブルにすると、Fabric Manager を使って FICON パラメータを設定できなくなります。

Fabric Manager を使用して FICON パラメータの SNMP 制御を設定する手順は、次のとおりです。

ステップ 1　[VSAN] > [FICON] を選択します。

[Information] ペインの [Control] タブに、スイッチが一覧表示されます。

ステップ 2　[VSANs] タブをクリックします。

[Information] ペインに FICON VSAN 設定情報が表示されます（図 11-13 を参照）。

ステップ 3　[Port Control By SNMP] チェックボックスをオンにして、SNMP ユーザがスイッチで FICON を設定できるようにします。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

FICON 情報のリフレッシュ

[Device Manager] ダイアログボックスで FICON 情報を表示するときは、[Refresh] ボタンをクリックし、ディスプレイを手動でリフレッシュして最新の更新内容を表示する必要があります。このリフレッシュ手順は、FICON の設定に CLI または Device Manager のどちらを使用するかに関係なく必要です。

FICON 情報の自動リフレッシュ機能は用意されていません。FICON 情報を頻繁にリフレッシュした場合、パフォーマンスに影響するためです。

FICON デバイスの従属関係の概要

FICON では、現在実行されているセッションのデバイス従属関係を制御することによって、Cisco MDS 9000 ファミリ スイッチ上で複数のメインフレーム、CLI、および SNMP セッション間のアクセスをシリアル化する必要があります。他のセッションに設定変更の実行を許可するには、所定の従属関係を使用可能にする必要があります。

注意　この作業により、現在実行中のセッションが破棄されます。

実行コンフィギュレーションの自動保存

Cisco MDS NX-OS には、スタートアップ コンフィギュレーションに加えられた設定変更を自動保存するオプションが用意されています。この自動保存によって、スイッチのリブート後も、新しい設定が消去されずに済みます。[Active=Saved] オプションは、どの FICON VSAN 上でもイネーブルにできます。

表 11-2 は、さまざまなシナリオで [Active = Saved] オプションをイネーブルにし、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暗黙的にコピー（**copy running start**）した結果を示したものです。

[Active=Saved] オプションがファブリック内のどの FICON 対応 VSAN でもイネーブルになっている場合は、次の保存方式が適用されます（表 11-2 の番号 1 および 2 を参照）。

- 設定変更はすべて（FICON 固有のものかどうかに関係なく）、永続ストレージに自動的に保存され（暗黙的に **copy running start** が実行され）、さらにスタートアップ コンフィギュレーション内に保管されます。
- FICON 固有の設定変更は、ただちに IPL ファイルに保存されます（「FICON コンフィギュレーション ファイル」（P.11-30）を参照）。

[Active=Saved] オプション がイネーブルになっていない場合、FICON 固有の設定は IPL ファイルに自動保存されず、暗黙的な **copy running startup** コマンドが発行されないので、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明示的に保存しておく必要があります（表 11-2 の 3 を参照）。

表 11-2　アクティブな FICON およびスイッチ設定の保存

番号	FICON 対応 VSAN かどうか	`active equals saved` がイネーブルかどうか	暗黙的な `copy running startup` が発行されたかどうか	注意
1	FICON 対応	（すべての FICON VSAN で）イネーブル	暗黙的	FICON の変更内容は IPL ファイルに書き込まれました。 FICON 以外の変更内容は、スタートアップ コンフィギュレーションおよび永続ストレージに保存されます。
2	FICON 対応	（1 つの FICON VSAN で）イネーブル	暗黙的	VSAN で [active equals saved] オプションがイネーブルになっている 場合に限り、FICON の変更内容が IPL ファイルに書き込まれます。 FICON 以外の変更内容は、スタートアップ コンフィギュレーションおよび永続ストレージに保存されます。

表 11-2　アクティブな FICON およびスイッチ設定の保存 （続き）

番号	FICON 対応 VSAN かどうか	active equals saved がイネーブルかどうか	暗黙的な copy running startup が発行されたかどうか	注意
3	FICON 対応	（すべての FICON VSAN で）ディセーブル	非暗黙的	FICON の変更内容は IPL ファイルに書き込まれません。 **copy running start** コマンドを明示的に発行した場合に限り、FICON 以外の変更内容が永続ストレージに保存されます。
4	FICON 非対応	適用外		

実行設定を自動保存する手順は、次のとおりです。

ステップ 1　[VSAN] > [FICON] を選択します。

[Information] ペインの [Control] タブに、スイッチが一覧表示されます。

ステップ 2　[VSANs] タブをクリックします。

[Information] ペインに FICON VSAN 設定情報が表示されます（図 11-13 を参照）。

ステップ 3　[Active=Saved] チェックボックスをオンにします。これにより、FICON の設定変更時に毎回、実行コンフィギュレーションがスタートアップ コンフィギュレーションに自動保存されます。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

FICON ポートの設定

Cisco MDS 9000 ファミリ スイッチでは、ポート アドレス単位で FICON の設定を実行できます。

ポートが非インストレーション ポートの場合でも、Cisco MDS スイッチではポート アドレスベースの設定が可能です。この設定がポートに適用されるのは、ポートがインストレーション ポートになった場合です。

ここで説明する内容は、次のとおりです。

ポート ブロックの設定

ポートをブロックした場合、ポートは運用停止状態のままになります。ポートのブロックを解除すると、ポートの初期化が試行されます。ブロックされているポート上では、データおよび制御トラフィックが許可されません。

物理ファイバ チャネル ポートをブロックした場合は引き続き、ブロックされたポート上に Off-Line State（OLS）プリミティブ シーケンスが転送されます。

注意　CUP ポート（0XFE）は、ブロックまたは禁止できません。

シャットダウンしているポートは、ブロック解除しても初期化されません。

（注）　shutdown/no shutdown ポート状態は、block/no block ポート状態に依存しません。

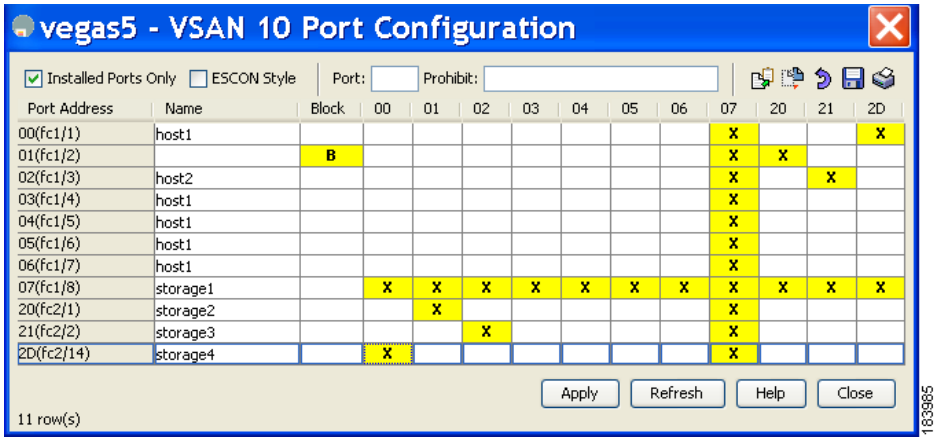
Device Manager を使用して、VSAN のポート アドレスをブロックまたはブロック解除する手順は、次のとおりです。

ステップ 1　[FICON] > [VSANs] を選択します。

ステップ 2　VSAN ID を選択して、[Port Configuration] をクリックします。

選択した VSAN の [FICON Port Configuration] ダイアログボックスが表示されます（図 11-14 を参照）。

図 11-14　[FICON Port Configuration] ダイアログボックス



ステップ 3　ブロックするポート用の [Blocked] チェックボックスをオンにします。

ステップ 4　[Apply] をクリックして、変更内容を保存します。

ESCON 形式ポートの表示

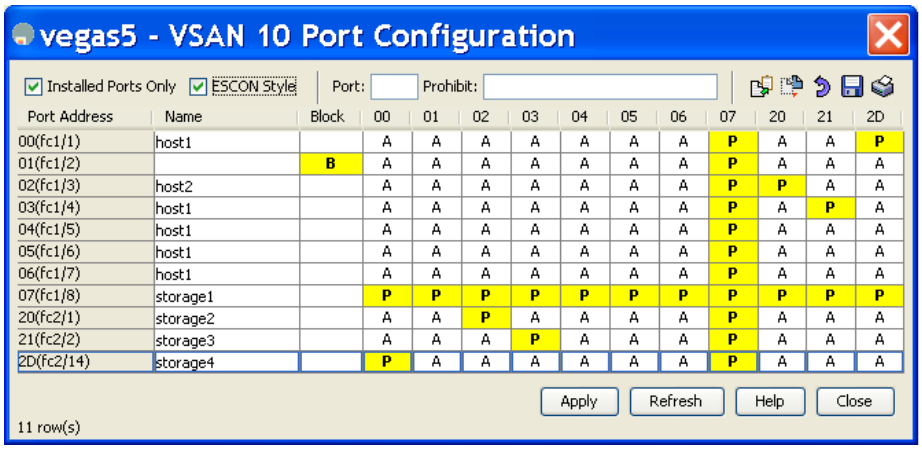
Device Manager を使用して、使用可能および使用禁止の ESCON 形式ポートを表示する手順は、次のとおりです。

ステップ 1　[ESCON Style] チェックボックスをオンにして、使用可能または使用禁止の ESCON 形式ポートを表示します。

図 11-15 で、A は使用可能ポート、P は使用禁止ポートです。

赤色で強調表示されたポート アドレスは、E/TE ポート インターフェイスまたは複数インターフェイスを示しています。

図 11-15　ESCON 形式



ステップ 2　[Apply] をクリックして、変更内容を保存します。

ポートの禁止

実装ポート間の相互通信を禁止するには、複数ポート間の禁止を設定します。複数ポート間の禁止により、指定されたポート間の相互通信は禁止されます。

ヒント　ポートチャネル インターフェイスまたは FCIP インターフェイスは、使用禁止には設定できません。

非実装ポートは、常に使用禁止になります。また、禁止設定は常に対称的に適用されます。ポート 0 に対してポート 15 との通信を禁止すると、ポート 15 に対しても自動的にポート 0 との通信が禁止されます。

（注）　インターフェイスがすでに E モードまたは TE モードに設定されている場合は、対象のポートを使用禁止にしようとしても、禁止設定が拒否されます。同様に、非稼動状態のポートは、使用禁止にしてしまうと E モードまたは TE モードで起動できません。

ポート禁止の設定

Device Manager を使用して、VSAN のポート アドレスを禁止する手順は、次のとおりです。

ステップ 1　[FICON] > [VSANs] を選択します。

ステップ 2　VASAN ID を選択して、[Port Configuration] をクリックします。

[FICON Port Configuration] ダイアログボックスが表示されます（図 11-14 を参照）。

ステップ 3　選択した FICON VSAN 用に、ポート禁止設定を設定します。

ステップ 4　[Apply] をクリックして、変更内容を保存します。

ポート アドレス名の割り当て

（注）　最新の FICON 情報を表示するには、[Refresh] ボタンをクリックする必要があります。「実行コンフィギュレーションの自動保存」（P.11-25）を参照してください。

Device Manager でポート アドレス名を割り当てる手順は、次のとおりです。

ステップ 1　[FICON] > [VSANs] を選択します。

ステップ 2　VSAN ID を選択して、[Port Configuration] をクリックします。

[FICON Port Configuration] ダイアログボックスが表示されます（図 11-14 を参照）。

ステップ 3　ポート設定情報を入力します。

ステップ 4　[Apply] をクリックして、設定情報を保存します

RLIR の概要

Registered Link Incident Report（RLIR）アプリケーションを使用することにより、スイッチ ポートから登録済み Nx ポートに Link Incident Record（LIR）を送信できます。RLIR はアベイラビリティに優れたアプリケーションです。

Cisco MDS 9000 ファミリの FICON 対応スイッチでは、RLIR Extended Link Service（ELS）から検出された LIR が、Established Registration List（ERL）に登録済みのメンバーに送信されます。

マルチスイッチ トポロジの場合、Distribute Registered Link Incident Record（DRLIR）の Inter-Link Service（ILS）が RLIR ELS とともに、到達可能なすべてのリモート ドメインに送信されます。スイッチは DRLIR ILS を受信すると、RLIR ELS を抽出して ERL のメンバーに送信します。

RLIR ELS の受信に関与する Nx ポートは、Link Incident Record Registration（LIRR）ELS 要求をスイッチ上の管理サーバに送信します。RLIR は VSAN 単位で処理されます。

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**すると、RLIR データが永続的ストレージに書き込まれます。

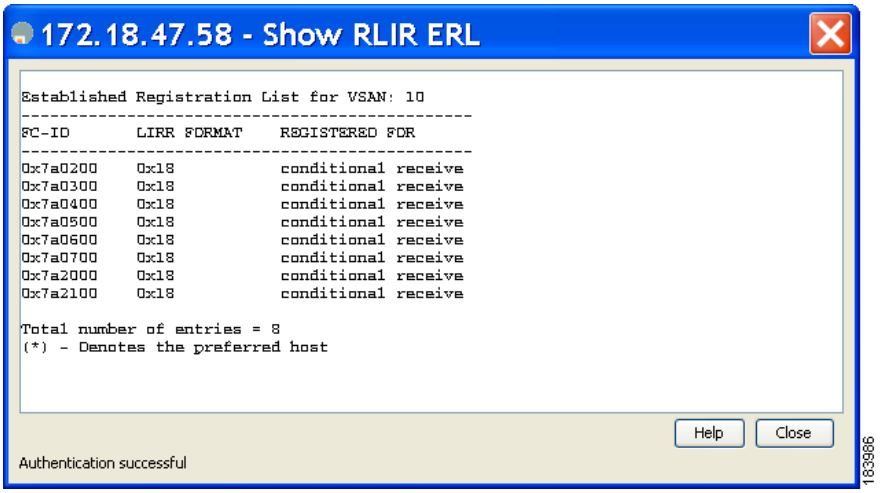
RLIR 情報の表示

Device Manager を使用して RLIR 情報を表示する手順は、次のとおりです。

ステップ 1　[FICON] > [RLIR ERL] を選択します。

[Show RLIR ERL] ダイアログボックスが表示されます（図 11-16 を参照）。

図 11-16　[Show RLIR ELR] ダイアログボックス



ステップ 2　[Close] をクリックして、ダイアログボックスを閉じます。

FICON コンフィギュレーション ファイル

各 FICON 対応 VSAN 上で、最大 16 個の FICON コンフィギュレーション ファイルを（永続ストレージに）保存できます。ファイル フォーマットの所有権は IBM に帰属します。これらのファイルは、帯域内 CUP プロトコルを使用して IBM ホストから読み取りおよび書き込みできます。また、これらの FICON コンフィギュレーション ファイルを処理するには、Cisco MDS CLI または Fabric Manager アプリケーションを使用します。

（注）　名前が同じ複数の FICON コンフィギュレーション ファイルは、それぞれ別個の VSAN に属している限り、同一のスイッチに配置できます。たとえば、VSAN 1 と VSAN 3 の両方で、XYZ という名前のコンフィギュレーション ファイルを作成することもできます。

VSAN で FICON 機能がイネーブルになっているときは常に、IPL という名前のスタートアップ FICON コンフィギュレーション ファイルが使用されます。この IPL ファイルは、VSAN で FICON をイネーブルにするとただちに、デフォルトのコンフィギュレーションで作成されます。

注意　VSAN 上で FICON をディセーブルにした場合、FICON コンフィギュレーション ファイルはすべて失われます。いったん失われると復元できません。

FICON コンフィギュレーション ファイルには、次のコンフィギュレーションが実装ポート アドレスごとに格納されています。

- ブロック
- 禁止マスク
- ポート アドレス名

（注）　Cisco MDS スイッチで使用される標準コンフィギュレーション ファイルには、VSAN の FICON 対応属性、ポートチャネル インターフェイスと FCIP インターフェイスに対するポート番号のマッピング、ポート番号とポートアドレスのマッピング、ポートおよびトランクで許可されている各ポートの VSAN 設定、順序保証、スタティック ドメイン ID の設定、ファブリック バインディング設定などが格納されています。

Cisco MDS スイッチで使用される標準コンフィギュレーション ファイルの詳細については、『*Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide*』を参照してください。

ここで説明する内容は、次のとおりです。

FICON コンフィギュレーション ファイルの概要

コンフィギュレーション ファイルに同時にアクセスできるのは、常に 1 人のユーザだけです。

- このファイルにユーザ 1 がアクセスしている間、ユーザ 2 はアクセスできません。
- このファイルへのアクセスを試みたユーザ 2 に対しては、エラーが出されます。
- ユーザ 1 が非アクティブ状態のまま 15 秒が過ぎると、ファイルは自動的に閉じられ、許可されている他のユーザが使用できるようになります。

スイッチへのアクセスを許可されているホスト、SNMP、または CLI ユーザはいずれも、FICON コンフィギュレーション ファイルにアクセスできます。Cisco NX-OS ソフトウェアのロック メカニズムによって、同時アクセスは 1 人のユーザだけに許可されます。このロックは、新規に作成されたファイル、および以前に保存されたファイルに適用されます。どのファイルにアクセスする際にも、あらかじめファイルをロックし、ファイル キーを取得する必要があります。ロック要求が発生するたびに毎回、新しいファイル キーがロック メカニズムによって使用されます。15 秒間のロック タイムアウト期限が切れると、キーは廃棄されます。ロック タイムアウト値は変更できません。

保存済みコンフィギュレーション ファイルの実行コンフィギュレーションへの適用

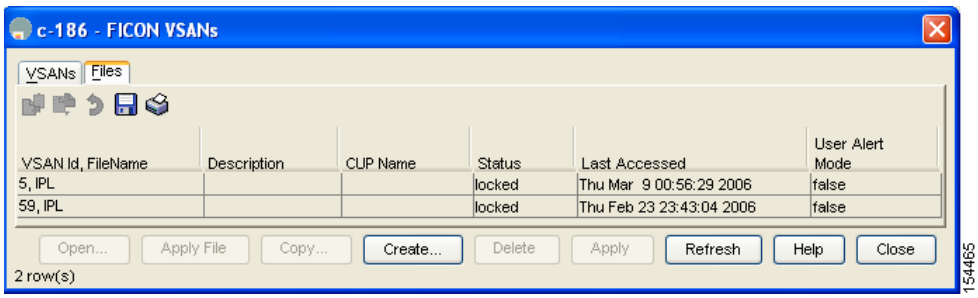
Device Manager を使用して、保存済みコンフィギュレーション ファイルを実行コンフィギュレーションに適用する手順は、次のとおりです。

ステップ 1　[FICON] > [VSANs] を選択します。

ステップ 2　[Files] タブをクリックします。

[FICON Files] ダイアログボックスが表示されます（図 11-17 を参照）。

図 11-17　[FICON VSANs] ダイアログボックス



ステップ 3　適用するファイルをハイライト表示し、[Apply File] をクリックして、該当のコンフィギュレーションを実行コンフィギュレーションに適用します。

FICON コンフィギュレーション ファイルの編集

コンフィギュレーション ファイル サブモードでは、FICON コンフィギュレーション ファイルの作成および編集が許可されます。指定したファイルが存在しない場合は、作成されます。保存可能なファイル数は最大 16 個です。各ファイル名には、最大 8 文字の英数字を使用できます。

（注）　最新の FICON 情報を表示するには、[Refresh] ボタンをクリックする必要があります。「実行コンフィギュレーションの自動保存」（P.11-25）を参照してください。

Device Manager を使用して、特定の FICON コンフィギュレーション ファイルの内容を編集する手順は、次のとおりです。

ステップ 1　[FICON] > [VSANs] を選択します。

ステップ 2　[Files] タブをクリックします。

[FICON VSANs] ダイアログボックスが表示されます（図 11-17 を参照）。

ステップ 3　VSAN ID を選択し、[Open] をクリックして、FICON コンフィギュレーション ファイルを編集します。

ステップ 4　VSAN ID を選択し、[Delete] をクリックして、FICON コンフィギュレーション ファイルを削除します。

ステップ 5　[Apply] をクリックして、変更された FICON コンフィギュレーション ファイルを適用します。

FICON コンフィギュレーション ファイルの表示

Fabric Manager でコンフィギュレーション ファイル開いて表示する手順は、次のとおりです。

ステップ 1　[FICON] > [VSAN] を選択します。

[Information] ペインに FICON 設定テーブルが表示されます。

ステップ 2　[Files] タブをクリックします。

ステップ 3　開きたいファイルを選択します。

ステップ 4　[Open] をクリックします。

FICON コンフィギュレーション ファイルのコピー

Device Manager を使用して既存の FICON コンフィギュレーション ファイルをコピーする手順は、次のとおりです。

ステップ 1　[FICON] > [VSANs] を選択します。

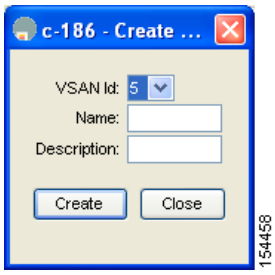
ステップ 2　[Files] タブをクリックします。

[FICON VSANs] ダイアログボックスが表示されます（図 11-17 を参照）。

ステップ 3　[Create] をクリックして、FICON コンフィギュレーション ファイルを作成します。

[Create FICON VSAN File] ダイアログボックスが表示されます（図 11-18 を参照）。

図 11-18　Device Manager の [Create FICON VSANs Files] ダイアログボックス



a.　設定する FICON VSAN 用に VSAN ID を選択します。

b.　ファイル名とその説明を入力します。

c.　[Create] をクリックして、ファイルを作成します。

ステップ 4　[Copy] をクリックして、ファイルを新しいファイルにコピーします。

ステップ 5　[Apply] をクリックして、FICON コンフィギュレーション ファイルを適用します。

ポート スワッピング

FICON ポート スワッピング機能は、メンテナンス専用に提供されています。

FICON ポート スワッピング機能を実行すると、*old-port-number* および *new port-number* に関連付けられているすべての設定（例：VSAN 設定）がスワッピングされます。

Cisco MDS スイッチは、実在しないポートに対してもポート スワッピングを実行できますが、その際は次のような制約が伴います。

- スワッピング対象は、FICON 固有の設定（禁止、ブロック、およびポート アドレスのマッピング）だけです。
- 他のシステム設定はスワッピングされません。
- 他のシステム設定はいずれも、既存のポートでだけ維持されます。
- 無制限の加入過多率がイネーブルになっているモジュール内のポートを、加入過多率が制限されているモジュール内のポートとスワッピングすると、帯域幅が劣化することがあります。

ヒント　どの FICON VSAN 上でも [Active=Saved] チェックボックス がオンになっているときは、スワッピングされた設定が自動的にスタートアップ コンフィギュレーションに保存されます。このチェックボックスがオフになっているときは、ポートをスワッピングした後すぐに、実行コンフィギュレーションを明示的に保存しておく必要があります。

いったんポートをスワッピングし終えると、次の処理が自動的に実行されます。

- 古いポートと新しいポートがシャットダウンされます。
- ポート設定がスワッピングされます。

ポートを稼動状態にする際は、対象のポートを明示的にシャットダウンしてから、トラフィックを再開する必要があります。

（注）　最新の FICON 情報を表示するには、[Refresh] ボタンをクリックする必要があります。「実行コンフィギュレーションの自動保存」（P.11-25）を参照してください。

ここで説明する内容は、次のとおりです。

ポート スワッピングの概要

FICON ポート スワッピング機能を使用する際は必ず、次のガイドラインに従ってください。

- 論理ポート（ポートチャネル、FCIP リンク）に対しては、ポート スワッピングがサポートされません。*old-port-number* と *new-port-number* はいずれも、論理ポートとして設定できません。
- ポートチャネルに属する物理ポート間では、ポート スワッピングがサポートされません。*old-port-number* と *new-port-number* はいずれも、ポートチャネルに属する物理ポートとしては設定できません。
- ポート スワッピングを実行する前に、Cisco NX-OS ソフトウェアは互換性チェックを実行します。2 つのポート設定に互換性がないと、ポート スワッピングが拒否され、該当する理由コードが出力されます。たとえば、BB_credits に 25 が割り当てられているポートと、BB_credits（設定不能なパラメータ）に許可されている最大値が 12 の OSM ポートとをスワッピングしようとした場合、ポート スワッピング操作は拒否されます。
- ポート スワッピングを実行する前に、Cisco NX-OS ソフトウェアは互換性チェックを実行して、拡張 BB_credits 設定を検証します。
- ポートに（一部の非互換パラメータ用の）デフォルト値がある場合、ポート スワッピング操作が許可され、ポートはそのデフォルト値を保持します。
- ポート スワッピングには、ポート トラッキング情報が取り込まれません。ポート トラッキング情報は、個別に設定する必要があります（『*Cisco MDS 9000 Family NX-OS Quality of Service Configuration Guide*』を参照）。

（注）　32 ポート モジュールに関するガイドラインは、ポート スワッピング設定にも適用されます。

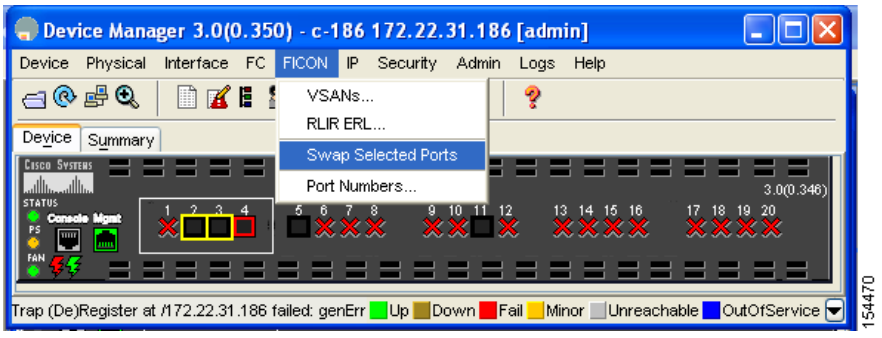
ポート スワッピング

Device Manager を使用してポートをスワッピングする手順は、次のとおりです。

ステップ 1　**CTRL** キーを押しながら、2 つのファイバ チャネル ポートをマウスでクリックして選択します。

ステップ 2　[FICON] > [Swap Selected Ports] を選択します（図 11-19 を参照）。

図 11-19　[FICON] > [Swap Selected Ports]



FICON テープ アクセラレーション

テープ デバイスには順次性があるため、FCIP リンクを介したテープ デバイスに対して I/O 操作が実行されるたびに、FCIP リンクに遅延が発生します。FCIP リンクを介したラウンドトリップ時間が増えると、スループットは著しく減少するため、結果としてバックアップ時間は長くなります。また、各 I/O 操作を終えてから次の I/O に達するまで、テープ デバイスはアイドル状態になります。I/O 操作が仮想テープを対象する場合を除き、テープ ヘッドの走査開始と停止によってテープ寿命が縮まります。

Cisco MDS NX-OS ソフトウェアは、次のリンクを介した FICON テープ書き込み操作に対してアクセラレーションを提供します。

- メインフレーム ドライブとネイティブ テープ ドライブ（IBM と Sun/STK の両方）の間のリンク
- Virtual Storage Management（VSM）とテープ ドライブ（Sun/STK）の間のバックエンド リンク

FCIP を介した FICON テープ アクセラレーションにより、次のようなメリットがあります。

- アイドル時間が短縮される結果、テープ デバイスが効率的に利用されます。
- 遅延が増加したときのスループットの持続性が向上します。
- FCP テープ アクセラレーションと似ていますが、競合は発生しません。

（注）　FCIP を介した FICON テープ読み込みアクセラレーションはサポートされていません。

図 11-20 ～図 11-23 に、サポートされている設定を示します。

図 11-20　IBM/StorageTek（STK）ライブラリに直接アクセスするホスト

図 11-21　スタンドアロン IBM-Virtual Tape Server（VTS）/STK-Virtual Shared Memory（VSM）にアクセスするホスト

図 11-22　ピアツーピア Virtual Tape Server（VTS）にアクセスするホスト

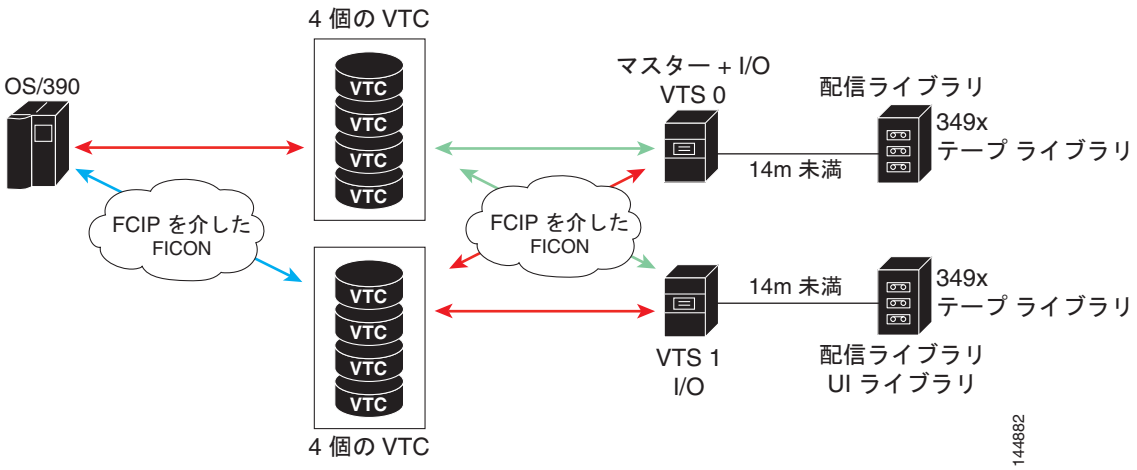
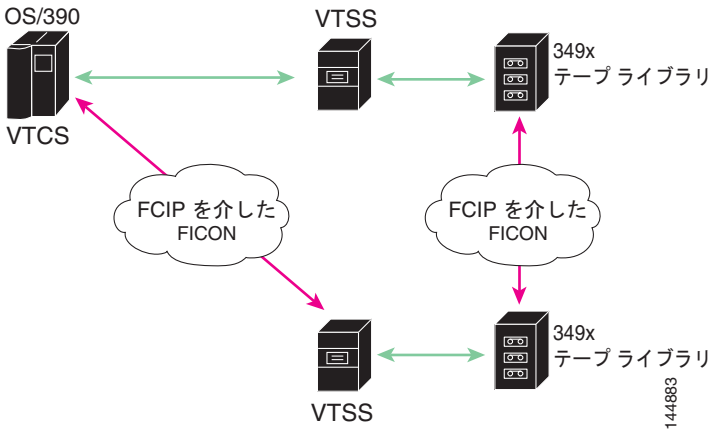


図 11-23　ピアツーピア Virtual Tape Server（VTS）にアクセスするホスト



（注）　FCIP テープ アクセラレーションの詳細については、『*Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*』を参照してください。

FICON テープ アクセラレーション設定

FICON テープ アクセラレーションの設定に関しては、次のような考慮事項があります。

- 標準 FICON 設定だけでなく、FICON テープ アクセラレーションも、FCIP インターフェイスの両端でイネーブルにしておく必要があります。一端だけで FICON テープ アクセラレーションをイネーブルにした場合、アクセラレーションは発生しません。
- FICON テープ アクセラレーションは、VSAN 単位でイネーブルになります。
- 複数の ISL が同一の VSAN 内に存在する（ポートチャネルまたは FSPF でロード バランスされている）場合、FICON テープ アクセラレーション機能は無効になります。
- 同じ FCIP インターフェイス上で、ファイバ チャネル書き込みアクセラレーションと FICON テープ アクセラレーションの両方をイネーブルに設定できます。
- FICON テープ アクセラレーションをイネーブルまたはディセーブルにすると、FCIP インターフェイス上のトラフィックが中断されます。

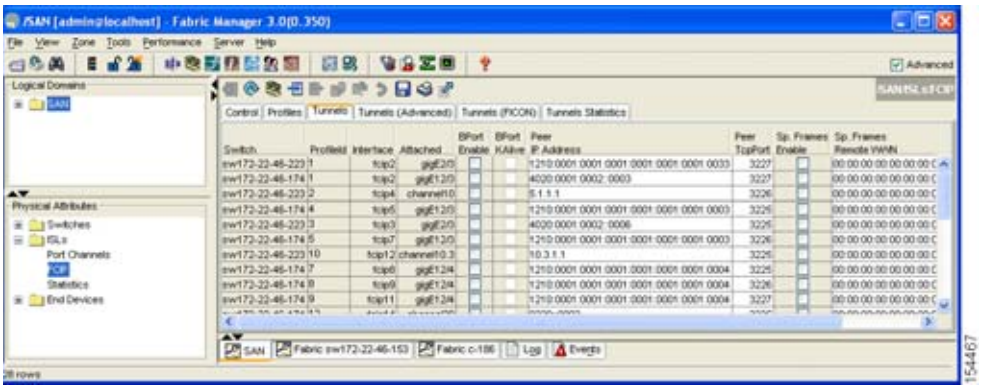
Fabric Manager で FCIP を介した FICON テープ アクセラレーションを設定する手順は、次のとおりです。

ステップ 1　ISL を展開し、[Physical Attributes] ペインで [FCIP] を選択します。

ステップ 2　[Information] ペインで、[Tunnels] タブをクリックします。

使用可能なスイッチが一覧表示されます（図 11-24 を参照）。

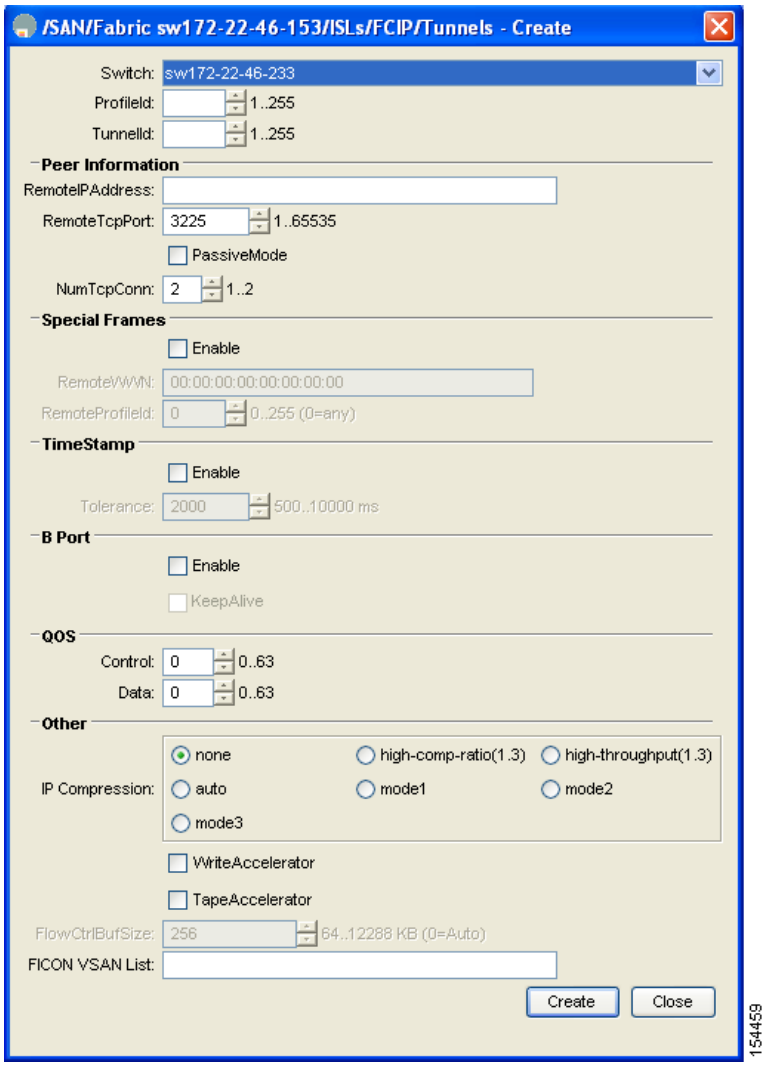
図 11-24　Fabric Manager の [FCIP Tunnels] タブ



ステップ 3　[Create Row] アイコンをクリックして、FCIP トンネルを作成します。

[Create FCIP Tunnel] ダイアログボックスが表示されます（図 11-25 を参照）。

図 11-25　[Create FCIP Tunnel] ダイアログボックス



ステップ 4　オプションを使用して、トンネルを設定します（図 11-25 を参照）。

ステップ 5　[TapeAccelerator] チェックボックスをオンにし、この FCIP トンネルを介した FICON テープ アクセラレーションをイネーブルにします。

ステップ 6　[Create] をクリックします。

XRC アクセラレーションの設定

IBM z/OS Global Mirror eXtended Remote Copy（XRC）は、MSM-18+4 モジュールでサポートされています。XRC を正しく機能させるには、FCIP トンネル インターフェイスの両端で XRC アクセラレーションをイネーブルにする必要があります。XRC アクセラレーションはデフォルトではディセーブルです。

（注）　XRC アクセラレーションと FICON テープ アクセラレーションは、同一の FCIP トンネル インターフェイス上ではイネーブルにできないため、同一の VSAN 上には存在できません。

Fabric Manager を使用して FCIP トンネル インターフェイス上で XRC アクセラレーションを設定する手順は、次のとおりです。

ステップ 1　ISL を展開し、[Physical Attributes] ペインで [FCIP] を選択します。

ステップ 2　[Information] ペインで、[Tunnels(Advanced)] タブをクリックします。

使用可能な FCIP インターフェイスが一覧表示されます。

ステップ 3　[XRC Emulator] 列のチェックボックスをオンして、FCIP トンネルを介した XRC アクセラレーションをイネーブルにします。

ステップ 4　[Apply] をクリックします。

Device Manager を使用して FCIP トンネル インターフェイス上で XRC アクセラレーションを設定する手順は、次のとおりです。

ステップ 1　Device Manager ウィンドウで、[IP] をクリックし、メニューから [FCIP] を選択します。

ステップ 2　[Information] ペインで、[Tunnels(Advanced)] タブをクリックします。

FCIP インターフェイスが一覧表示されます。

ステップ 3　[XRC Emulator] 列のチェックボックスをオンして、FCIP トンネルを介した XRC アクセラレーションをイネーブルにします。

ステップ 4　[Apply] をクリックします。

XRC アクセラレーションの統計情報の表示

Fabric Manager を使用して XRC アクセラレーションの統計情報を表示する手順は、次のとおりです。

ステップ 1　ISL を展開し、[Physical Attributes] ペインで [FCIP] を選択します。

ステップ 2　[Information] ペインで、[XRC Statistics] タブをクリックします。

XRC セッションの統計情報が表示されます。

Device Manager を使用して XRC アクセラレーションの統計情報を表示する手順は、次のとおりです。

ステップ 1　Device Manager ウィンドウで、[IP] をクリックし、メニューから [FCIP] を選択します。

ステップ 2　[Information] ペインで、[XRC Statistics] タブをクリックします。

XRC セッションの統計情報が表示されます。

CUP 帯域内管理

Control Unit Port（CUP）プロトコルを介して、アクセス制御の設定が行われ、メインフレーム コンピュータから統合型ストレージ管理機能が提供されます。Cisco MDS 9000 FICON 対応スイッチは、IBM CUP 規格に適合しており、IBM S/A OS/390 I/O 操作コンソールを使用した帯域内管理が可能です。

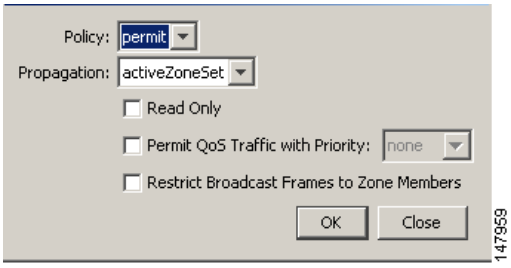
（注）　CUP 仕様の所有権は IBM に帰属します。

CUP は Cisco MDS 9000 ファミリのスイッチおよびディレクタによってサポートされます。CUP 機能を使用することにより、メインフレームで Cisco MDS スイッチを管理できます。

ホスト通信用に、制御（例：ポートのブロック / ブロック解除）、モニタリング、エラー レポートなどの機能が用意されています。

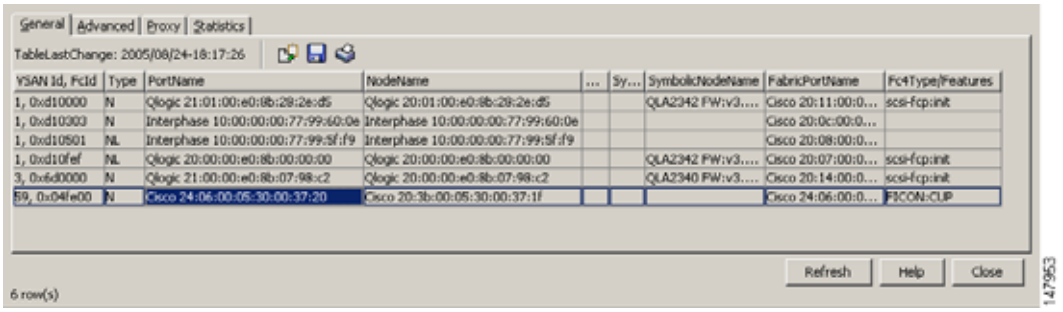
ステップ 1　Fabric Manager で、[Zone] > [Edit Full Zoneset] を選択し、[Edit] > [Edit Default Zone Attributes] を選択して、所定の VSAN に許可するデフォルト ゾーンを設定します （図 11-26 を参照）。

図 11-26　デフォルト ゾーン ポリシーの設定



ステップ 2　Device Manager で、[FC] > [Name Server...] を選択し、所定の VSAN の FICON:CUP WWN を取得します。図 11-27 を参照してください。

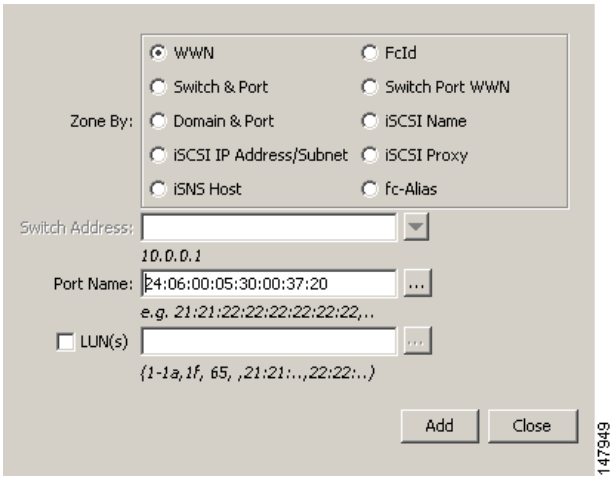
図 11-27　FICON:CUP の pWWN の検索



（注）　このファブリック内に複数の FICON:CUP WWN が存在する場合は、所定のゾーンに FICON:CUP の pWWNs をすべて追加する必要があります。

ステップ 3　Fabric Manager で、[Zone] > [Edit Full Zoneset] を選択し、FICON:CUP の pWWN をゾーン データベースに追加します （図 11-28 を参照）。

図 11-28　FICON:CUP WWN をゾーンに追加するには



FICON フロー ロードバランスの計算

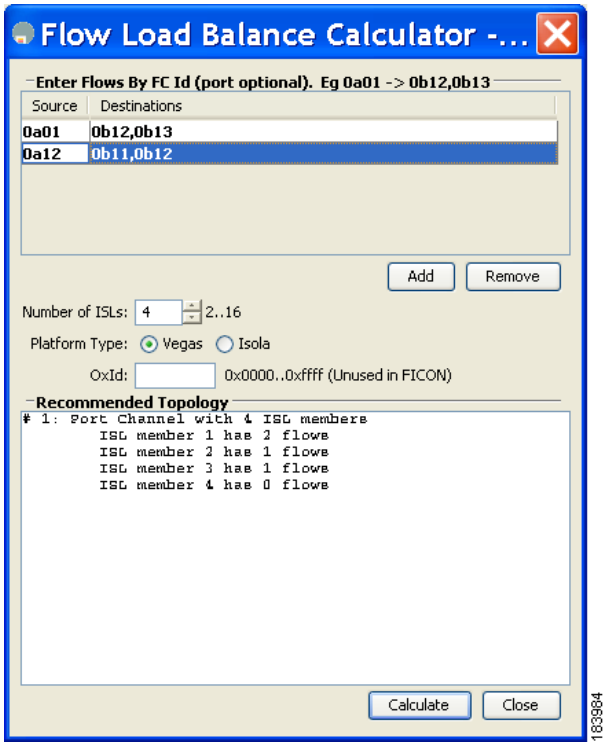
FICON フロー ロードバランス計算機能を使用することにより、対象の FICON フローに合った最適なロードバランスを設定できます。この計算機能は、ファブリック内のスイッチ検出またはフロー検出に依存しません。Fabric Manager の [Tools] メニューから選択できます。

Fabric Manager で FICON フロー ロードバランス計算機能を使用する手順は、次のとおりです。

ステップ 1　[Tools] > [Other] > [Flow Load Balance Calculator] を選択します。

フロー ロードバランス計算機能が表示されます（図 11-29 を参照）。

図 11-29　フロー ロードバランス計算機能



ステップ 2　[Add] をクリックして、送信元および宛先（複数可）のフローを入力します。

ステップ 3　2 バイトの 16 進数（ドメイン ID およびエリア ID）を使用して、送信元および宛先を入力します。これらの ID をコピーして貼り付け、必要に応じて編集できます。

ステップ 4　2 つのスイッチ（例：ドメイン ID 0a と 0b）間の ISL 数を入力（または選択）します。

ステップ 5　削除する行を選択して、[Remove] をクリックします。

ステップ 6　ロード バランスを計算するモジュールを選択します。

ステップ 7　[Calculate] をクリックして、推奨トポロジを表示します。

（注）　フローまたは ISL を変更する場合は、[Calculate] をクリックして、新しい推奨設定を表示する必要があります。

FICON 情報の表示

ここで説明する内容は、次のとおりです。

FICON アラートの受信

Device Manager を使用して、既存の FICON 設定の変更を示すアラートを受信する手順は、次のとおりです。

ステップ 1　[FICON] > [VSANs] を選択します。

[FICON VSAN] ダイアログボックスが表示されます。

ステップ 2　[User Alert Mode] チェックボックスをオンにします。これにより、FICON 設定が変更された場合に、アラートが受信されるようになります。

ステップ 3　[Apply] をクリックして、この変更内容を適用します。

FICON ポート アドレス情報の表示

Device Manager を使用して FICON ポート アドレス情報を表示する手順は、次のとおりです。

ステップ 1　[FICON] > [VSANs] を選択します。

[FICON VSAN] ダイアログボックスが表示されます。

ステップ 2　VSAN ID を選択して、[Port Configuration] をクリックします。

[FICON Port Configuration] ダイアログボックスが表示されます。

ステップ 3　[Close] をクリックして、ダイアログボックスを閉じます。

IPL ファイル情報の表示

Device Manager を使用して IPL ファイル情報を表示する手順は、次のとおりです。

ステップ 1　メニューから [VSANs] を選択します。

ステップ 2　[Files] タブをクリックします。

[FICON VSAN] ダイアログボックスが表示されます。

ステップ 3　表示するファイルを選択して、[Open] をクリックします。

履歴バッファの表示

ディレクトリ履歴バッファの [Key Counter] 列に、Cisco MDS スイッチに保持されている 32 ビット値が表示されます。この値は、該当する VSAN のいずれかのポートの状態が変わったときに増加します。キー カウンタ（32 ビット値）は、FICON 関連の設定が変更されたときに増加します。チャネル プログラムの起動時に、この値がホスト プログラムによって増加し、複数のポートに対して操作が実行されることがあります。ディレクトリ履歴バッファには、キー カウンタ値ごとに、変更されたポート アドレス設定のログが記録されます。

ディレクトリ履歴バッファは、前回キー カウンタに値が格納された後にポート状態が変わったかどうかを判別するためのメカニズムを備えています。

Device Manager を使用してディレクトリ履歴バッファを表示する手順は、次のとおりです。

ステップ 1　[FICON] > [VSANs] を選択します。

[FICON VSAN] ダイアログボックスが表示されます。

ステップ 2　[Director History] ボタンをクリックします。

履歴バッファ ダイアログボックスが表示されます。

ステップ 3　[Close] をクリックして、ダイアログボックスを閉じます。

デフォルト設定

表 11-3 に、FICON 機能のデフォルト設定を示します。

表 11-3　FICON のデフォルト設定

パラメータ	デフォルト
FICON 機能	ディセーブル
ポート番号	ポート アドレスと同じ
FC ID の最終バイト値	0（ゼロ）
EBCDIC フォーマット オプション	US-Canada
スイッチのオフライン状態	ホストでスイッチをオフライン状態に移行可能
メインフレーム ユーザ	Cisco MDS スイッチで FICON パラメータを設定可能
各 VSAN のクロック	スイッチのハードウェア クロックと同じ
ホストのクロック制御	このスイッチのクロックを、ホストで設定可能
SNMP ユーザ	FICON パラメータの設定
ポート アドレス	ブロック対象外
使用禁止ポート	Cisco MDS 9200 シリーズ スイッチのポート 90 ～ 253、およびポート 255 Cisco MDS 9500 シリーズ スイッチのポート 250 ～ 253、およびポート 255

CHAPTER 12

高度な機能および概念

この章では、Cisco MDS 9000 ファミリのスイッチが提供する高度な機能について説明します。この章の内容は、次のとおりです。

Common Information Model

Common Information Model（CIM; 共通情報モデル）は、既存の規格を拡張してネットワークやエンタープライズ環境の管理情報を記述するオブジェクト指向の情報モデルです。

CIM メッセージは、N Extensible Markup Language（XML）で符号化されるため、プラットフォームおよび実装に依存しません。CIM は仕様とスキーマで構成されます。仕様には、管理データの記述および他の管理モデルとの統合に用いられる、構文とルールが定義されています。スキーマは、システム、アプリケーション、ネットワーク、およびデバイスの実際のモデルの説明を提供します。

CIM の詳細については、次の URL にある Distributed Management Task Force（DMTF）の Web サイトから入手可能な仕様を参照してください。http://www.dmtf.org/

Cisco MDS 9000 ファミリでの CIM サーバのサポートの詳細については、『*Cisco MDS 9000 Family CIM Programming Reference Guide*』を参照してください。

CIM サーバにアクセスするには、CIM クライアントが必要です。CIM をサポートするクライアントであれば、どのようなクライアントでも利用できます。

SSL 認証の要件および形式

認証済みクライアントしか CIM サーバにアクセスできないようにするには、CIM サーバとクライアント間の HTTPS 転送プロトコルをイネーブルにします。スイッチ側では、クライアント上で生成された Secure Socket Layer（SSL）証明書をインストールし、HTTPS サーバをイネーブルにする必要があります。証明書は、OpenSSL（UNIX、Mac、および Windows 用）などのサードパーティ製ツールを使用して生成でき、CA により認証されるか、自己署名にすることができます。

スイッチにインストールする SSL 証明書は、次の要件を満たしている必要があります。

- 証明書ファイルに証明書と秘密鍵が含まれている。
- 秘密鍵は RSA タイプでなければならない。
- 証明書ファイルは PEM（Private Electronic Mail）スタイル形式にし、.pem という拡張子が付いている必要がある。

```
-----BEGIN CERTIFICATE-----
(certificate goes here)
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
(private key goes here)
-----END RSA PRIVATE KEY-----
```

証明書ファイルは一度に 1 つだけインストールできます。

ファイバ チャネル タイムアウト値

ファイバ チャネル プロトコルに関連するスイッチのタイマー値を変更するには、次の Timeout Value（TOV）値を設定します。

- Distributed Services TOV（D_S_TOV）：有効範囲は 5,000 ～ 10,000 ミリ秒です。デフォルトは 5,000 ミリ秒です。
- Error Detect TOV（E_D_TOV）- 有効範囲は 1,000 ～ 10,000 ミリ秒です。デフォルトは 2,000 ミリ秒です。この値は、ポート初期化中に他端と比較されます。
- Resource Allocation TOV（R_A_TOV）- 有効範囲は 5,000 ～ 10,000 ミリ秒です。デフォルトは 10,000 ミリ秒です。この値は、ポート初期化中に他端と比較されます。

（注）　Fabric Stability TOV（F_S_TOV）定数は設定できません。

ここで説明する内容は、次のとおりです。

すべての VSAN のタイマー設定

スイッチでファイバ チャネル プロトコルに関連するタイマー値を変更できます。

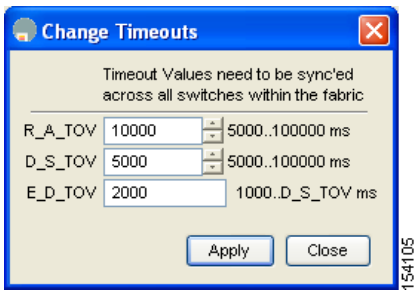
注意　D_S_TOV、E_D_TOV、および R_A_TOV 値は、スイッチ内のすべての VSAN を一時停止しないかぎり、グローバルに変更できません。

（注）　タイマー値を変更するときに VSAN を指定しない場合は、変更された値がスイッチ内のすべての VSAN に適用されます。

Fabric Manager でタイマーを設定するには、[Switches] > [FC] [Services] を展開し、[Physical Attributes] ペインで [Timers & Policies] を選択します。[Information] ペインに複数のスイッチのタイマーが表示されます。[Change Timeouts] ボタンをクリックして、タイムアウト値を設定します。

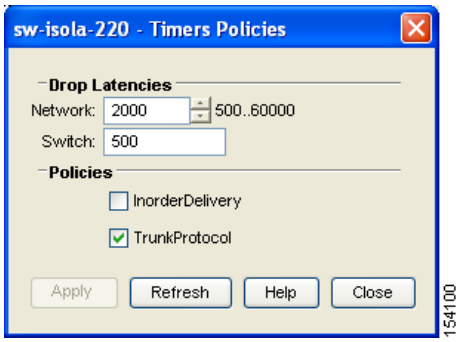
ダイアログボックスが表示されます（図 12-1 を参照）。

図 12-1　Fabric Manager でのタイマーの設定



Device Manager でタイマーを設定するには、[FC] > [Advanced] > [Timers/Policies] をクリックします。ダイアログボックスに単一スイッチのタイマーが表示されます（図 12-2 を参照）。

図 12-2　Device Manager でのタイマーの設定



VSAN 単位のタイマー設定

VSAN を指定して fctimer を発行し、VSAN に異なる TOV 値を設定して FC や IP トンネルなどに特別にリンクさせることができます。個別の VSAN に、異なる E_D_TOV、R_A_TOV、D_S_TOV 値を設定できます。タイマー値が変更されると、アクティブな VSAN は一時停止してアクティブになります。

注意　以前のバージョンでは VSAN ごとの FC タイマーをサポートしておらず、中断のないダウングレードは実行できません。

（注）　この設定はファブリックのすべてのスイッチに伝播する必要があります。ファブリックのすべてのスイッチが同じ値に設定されていることを確認してください。

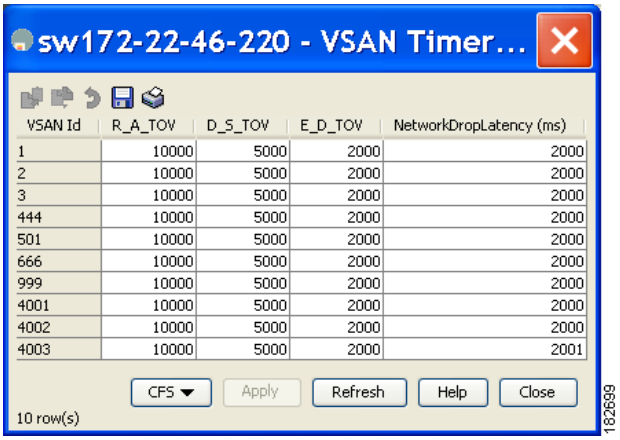
タイマーを VSAN 用に設定した後にスイッチが Cisco MDS SAN-OS Release 1.2 または 1.1 にダウングレードされると、厳密に互換性がないことを警告するエラー メッセージが表示されます。『*Cisco MDS 9000 Family Troubleshooting Guide*』を参照してください。

Device Manager を使用して VSAN 単位のファイバ チャネル タイマーを設定する手順は、次のとおりです。

ステップ 1　[FC] > [Advanced] > [VSAN Timer] をクリックします。

[VSANs Timer] ダイアログボックスが表示されます（図 12-3 を参照）。

図 12-3　Device Manager の VSAN タイマー



ステップ 2　設定するタイマー値を入力します。

ステップ 3　[Apply] をクリックして、変更内容を保存します。

fctimer 配信の概要

ファブリック内のすべての Cisco MDS スイッチで、VSAN 単位の fctimer ファブリック配信をイネーブルにできます。fctimer を設定して、配信をイネーブルにすると、この設定がファブリック内のすべてのスイッチに配信されます。

スイッチでの配信をイネーブルにした後で最初の設定コマンドを発行すると、ファブリック全体が自動的にロックされます。fctimer アプリケーションは有効/保留データベース モデルを使用して、ご使用の設定に基づいてコマンドを格納したり、コミットしたりします。

CFS アプリケーションの詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。

fctimer 配信のイネーブル化またはディセーブル化

Device Manager を使用して fctimer 設定変更をイネーブルにして配信する手順は、次のとおりです。

ステップ 1　[FC] > [Advanced] > [VSAN Timers] を選択します。

[VSANs Timer] ダイアログボックスが表示されます（図 12-3 を参照）。

ステップ 2　設定するタイマー値を入力します。

ステップ 3　[Apply] をクリックして、変更内容を保存します。

ステップ 4　変更内容を配信するには、[CFS] ドロップダウン メニューで [commit] を選択します。変更内容を保存しないで終了するには、[abort] を選択します。

fctimer 設定の変更をコミットすると、有効データベースが保留データベースの設定変更で上書きされ、ファブリック内のすべてのスイッチが同じ設定になります。セッション機能を実行しないで、fctimer の設定変更をコミットすると、fctimer 設定は物理ファブリック内のすべてのスイッチに配信されます。

データベース マージに関する注意事項

CFS マージ サポートの詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。

2 つのファブリックを結合する場合は、次の注意事項に従ってください。

- マージに関する次の条件に注意してください。
  - マージ プロトコルが実装済みでも fctimer 値は配信されるとはかぎりません。ファブリックをマージするときは、fctimer 値を手動でマージする必要があります。VSAN 単位の fctimer 設定は、物理ファブリック内に配信されます。
  - fctimer 設定が適用されるのは、fctimer 値が変更された VSAN を含むスイッチだけです。
  - グローバル fctimer 値は配信されません。
- 配信がイネーブルな場合は、グローバル タイマー値を設定しないでください。

（注）　保留中の fctimer 設定処理の最大数は 15 です。この数に達した時点で、さらに処理を実行するには、保留中の設定をコミットするか、打ち切る必要があります。

World Wide Names（WWN）

スイッチの WWN は、イーサネット MAC アドレスと同等です。MAC アドレスと同様に、デバイスごとに WWN を一意に対応付ける必要があります。主要スイッチを選択するとき、およびドメイン ID を割り当てるときは、WWN を使用します。WWN は、スイッチのスーパーバイザ モジュールのプロセス レベル マネージャである WWN マネージャによって、各スイッチに割り当てられます。

Cisco MDS 9000 ファミリのスイッチは、3 つの Network Address Authority（NAA）アドレス フォーマットをサポートしています（表 12-1 を参照）。

表 12-1　NAA WWN の標準フォーマット

NAA アドレス	NAA タイプ	WWN フォーマット	
IEEE 48 ビット アドレス	タイプ 1 = 0001b	000 0000 0000b	48 ビット MAC アドレス
IEEE 拡張	タイプ 2 = 0010b	ローカルに割り当て	48 ビット MAC アドレス
IEEE 登録	タイプ 5 = 0101b	IEEE 企業 ID：24 ビット	VSID：36 ビット

注意　WWN の変更は、管理者や、スイッチの動作に精通した担当者が実行してください。

ここで説明する内容は、次のとおりです。

- 「WWN 情報の表示」（P.12-6）
- 「リンク初期化 WWN の使用法」（P.12-6）
- 「セカンダリ MAC アドレスの設定」（P.12-7）

WWN 情報の表示

Device Manager を使用して WWN 情報を表示するには、[FC] > [Advanced] > [WWN Manager] を選択します。割り当てられた WWN のリストが表示されます。

リンク初期化 WWN の使用法

ELP および Exchange Fabric Protocol（EFP）は、リンク初期化中に WWN を使用します。使用方法の詳細は、Cisco NX-OS ソフトウェア リリースごとに異なります。

ELP と EFP のどちらも、リンク初期化中にデフォルトで VSAN WWN を使用します。ただし、ELP の使用方法はピア スイッチの使用方法に応じて変わります。

- ピア スイッチの ELP がスイッチ WWN を使用する場合、ローカル スイッチもスイッチ WWN を使用します。
- ピア スイッチの ELP が VSAN WWN を使用する場合、ローカル スイッチも VSAN WWN を使用します。

（注）　Cisco SAN-OS Release 2.0(2b) 時点で、ELP は FC-SW-3 に準拠するように機能拡張されました。

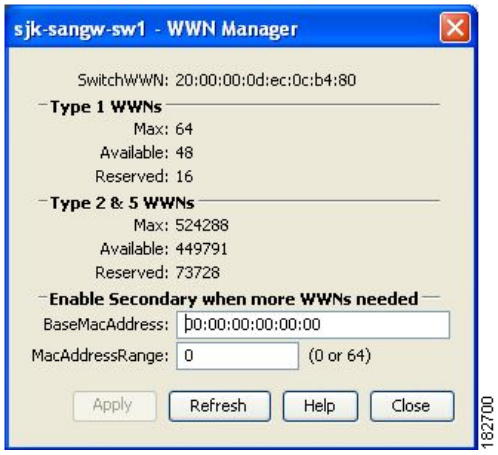
セカンダリ MAC アドレスの設定

Device Manager を使用してセカンダリ MAC アドレスを割り当てるには、次の手順を実行します。

ステップ 1　[FC] > [Advanced] > [WWN Manager] を選択します。

割り当てられた WWN のリストが表示されます（図 12-4 を参照）。

図 12-4　Device Manager で割り当てられた WWN



ステップ 2　[BaseMacAddress] フィールドと [MacAddressRange] フィールドに値を入力します。

ステップ 3　変更内容を保存するには、[Apply] をクリックします。変更内容を保存しないで終了するには、[Close] をクリックします。

HBA の FC ID 割り当て

ファイバ チャネル標準では、任意のスイッチの Fx 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。FC ID の使用数を節減するために、Cisco MDS 9000 ファミリ スイッチには特殊な割り当て方式が使用されています。

Host Bus Adapter（HBA）で、ドメインと領域が同じ FC ID を持つターゲットを検出しないことがあります。Cisco SAN-OS Release 2.0(1b) よりも前の Cisco SAN-OS ソフトウェアでは、この動作をサポートしないテスト済みの企業 ID のリストを保持していました。これらの HBA には単一の FC ID が割り当てられ、他の HBA には、領域全体が割り当てられていました。

Release 1.3 以前で使用可能な FC ID 割り当て方式では、これらの HBA に領域全体を割り当てます。このように割り当てることによって、これらの HBA が該当領域から分離され、ファブリック ログイン時に pWWN とともにリストされるようになります。割り当てられた FC ID は常にキャッシュされ、Cisco SAN-OS Release 2.0(1b) でも使用できます（「HBA の FC ID 割り当て」（P.12-7）を参照）。

多数のポートを備えたスイッチのスケーラビリティを高めるために、Cisco NX-OS ソフトウェアはこの動作をサポートする HBA のリストを保持します。各 HBA は、ファブリック ログイン中に pWWN で使用される企業 ID で識別されます。企業 ID は Organizational Unique Identifier（OUI; 組織固有識別子）とも呼ばれます。リストされた企業 ID を持つ N ポートには領域全体が割り当てられ、他のポートには単一の FC ID が割り当てられます。割り当てられる FC ID の種類（領域全体または単一）に関係なく、FC ID エントリは保持されます。

ここで説明する内容は、次のとおりです。

- 「デフォルトの企業 ID リスト」（P.12-8）
- 「企業 ID の設定の確認」（P.12-9）

デフォルトの企業 ID リスト

Cisco SAN-OS Release 2.0(1b) 以降または NX-OS 4.1(1) に付属の Cisco MDS 9000 ファミリ内のすべてのスイッチには、領域の割り当てが必要な企業 ID のデフォルト リストが格納されています。企業 ID を使用すると、設定される永続的 FC ID エントリ数が削減されます。これらのエントリを設定または変更するには、CLI を使用します。

注意　永続的エントリは、企業 ID 設定よりも優先します。HBA がターゲットの検出に失敗した場合、HBA およびターゲットが同じスイッチに接続されていて、これらの FC ID の領域が同じであることを確認してから、次の手順を実行します。

1.HBA に接続されたポートをシャットダウンします。
2. 永続的 FC ID エントリを消去します。
3. ポート WWN から企業 ID を取得します。
4. 企業 ID を領域割り当てが必要なリストに追加します。
5. ポートを起動します。

企業 ID のリストには、次の特性があります。

- 永続的 FC ID 設定は常に企業 ID リストよりも優先します。領域を受信するように企業 ID が設定されている場合でも、永続的 FC ID 設定によって、単一 FC ID が割り当てられます。
- 以降のリリースに追加された新しい企業 ID は、既存の企業 ID に自動的に追加されます。
- 企業 ID のリストは、実行コンフィギュレーションおよび保存されたコンフィギュレーションの一部として保存されます。
- 企業 ID リストが使用されるのは、fcinterop FC ID 割り当て方式が auto モードの場合だけです。interop FC ID 割り当てモードは、変更しないかぎり、デフォルトで auto です。

ヒント　fcinterop FC ID 割り当て方式を auto に設定し、企業 ID リストおよび永続的 FC ID 設定を使用して、FC ID デバイス割り当てを操作することを推奨します。

FC ID の割り当てを変更する方法については、『*Cisco MDS 9000 Family CLI Configuration Guide*』を参照してください。

企業 ID の設定の確認

Device Manager を使用して、設定された企業 ID を表示するには、[FC] > [Advanced] > [FcId Area Allocation] を選択します。特定のリリースに付属のデフォルト エントリを暗黙的に取得するには、何も指定しない場合に表示された企業 ID リストと、削除されたエントリ リストを結合します。

一部の WWN フォーマットは、企業 ID をサポートしていません。これらの場合は、FC ID の永続的エントリを設定しなければならないことがあります。

スイッチの相互運用性

相互運用性を使用すると、複数ベンダーによる製品の間で相互接続できます。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使用することを推奨しています。

すべてのベンダーが同じ方法で標準に従っていれば、異なる製品の相互接続が問題になることはありません。ただし、同じ方法で標準に従っていないベンダーもあるため、interop モードが開発されました。ここでは、これらのモードの基本的な概念について簡単に説明します。

各ベンダーには標準モード、および同等の相互運用性モードがあります。interop モードでは拡張機能または独自の機能が無効になり、より使いやすい標準準拠の実装が可能になります。

ここで説明する内容は、次のとおりです。

- 「Interop モードの概要」（P.12-9）
- 「interop モード 1 の設定」（P.12-11）
- 「相互運用性ステータスの確認」（P.12-12）

Interop モードの概要

Cisco NX-OS ソフトウェアは、次の 4 つの interop モードをサポートします。

- モード 1：ファブリック内のその他のすべてのベンダーを interop モードにする必要がある、標準ベースの interop モード
- モード 2：Brocade ネイティブ モード（Core PID 0）
- モード 3：Brocade ネイティブ モード（Core PID 1）
- モード 4：McData ネイティブ モード

interop モード 2、3、および 4 の設定方法については、『*Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*』を参照してください。

表 12-2 に、interop モードをイネーブルにした場合のスイッチ動作の変更点を示します。これらは、interop モードになっている Cisco MDS 9000 ファミリのスイッチに固有の変更点です。

表 12-2　相互運用性がイネーブルの場合のスイッチ動作の変更点

スイッチ機能	相互運用性がイネーブルの場合の変更点
ドメイン ID	ファブリック内の 239 のドメインの一部を使用できないベンダーもあります。 ドメイン ID は 97 ～ 127 の範囲に制限されています。これは、McData の通常の制限をこの範囲に収めるためです。ドメイン ID の設定方法には、静的に設定する（Cisco MDS スイッチは 1 つのドメイン ID だけを受け入れ、そのドメイン ID を取得できない場合はファブリックから隔離する）方法と、優先設定を使用する （スイッチが要求したドメイン ID を取得できない場合、割り当てられた任意のドメイン ID を受け入れる）方法があります。
タイマー	ISL（スイッチ間リンク）を確立するときにファイバ チャネル タイマー値が E ポートで交換されるため、すべてのスイッチでこれらのタイマーをすべて同じにする必要があります。タイマーは F_S_TOV、D_S_TOV、E_D_TOV、および R_A_TOV です。
F_S_TOV	Fabric Stability TOV タイマーが正確に一致するか確認します。
D_S_TOV	Distributed Services TOV タイマーが正確に一致するか確認します。
E_D_TOV	Error Detect TOV タイマーが正確に一致するか確認します。
R_A_TOV	Resource Allocation TOV が正確に一致するか確認します。
トランキング	2 つの異なるベンダー製のスイッチ間では、トランキングはサポートされません。この機能はポート単位、またはスイッチ単位でディセーブルに設定できます。
デフォルト ゾーン	ゾーンのデフォルトの許可動作（すべてのノードから他のすべてのノードを認識可能）または拒否動作（明示的にゾーンに配置されていないすべてのノードが隔離される）は、変更できます。
ゾーン分割属性	ゾーンを pWWN に制限したり、その他の独自のゾーン分割方式（物理ポート番号）を除去できます。 **（注）** Brocade では、**cfgsave** コマンドを使用して、ファブリック全体のゾーン分割設定を保存します。このコマンドは、同じファブリックに属す Cisco MDS 9000 ファミリ スイッチには影響しません。Cisco MDS 9000 ファミリの各スイッチに、設定を明示的に保存する必要があります。
ゾーンの伝播	ベンダーによっては、他のスイッチにゾーン設定全体を渡さず、アクティブ ゾーンセットだけが渡されることがあります。 ファブリック内の他のスイッチにアクティブ ゾーンセットまたはゾーン設定が正しく伝播されたかどうかを確認してください。
VSAN	interop モードが適用されるのは、指定した VSAN だけです。 **（注）** FICON 対応 VSAN では interop モードをイネーブルにできません。
TE ポートとポート チャネル	TE ポートとポート チャネルを使用して、Cisco MDS を Cisco 以外の MDS スイッチに接続することはできません。Cisco MDS 以外のスイッチに接続できるのは、E ポートだけです。TE ポートとポート チャネルを使用すると、interop モードの場合でも、Cisco MDS をその他の Cisco MDS スイッチに接続できます。
FSPF	interop モードにしても、ファブリック内のフレームのルーティングは変更されません。スイッチは引き続き src-id、dst-id、および ox-id を使用して、複数の ISL リンク間で負荷を分散します。
ドメインの中断再設定	これは、スイッチ全体に影響するイベントです。Brocade および McData では、ドメイン ID を変更するときにスイッチ全体をオフライン モードにしたり、再起動する必要があります。

表 12-2　相互運用性がイネーブルの場合のスイッチ動作の変更点 （続き）

スイッチ機能	相互運用性がイネーブルの場合の変更点
ドメインの非中断再設定	これは、関連する VSAN に限定されるイベントです。スイッチ全体ではなく、関連する VSAN の Domain Manager プロセスだけが再起動される機能は、Cisco MDS 9000 ファミリのスイッチだけに組み込まれています。
ネーム サーバ	すべてのベンダーのネームサーバ データベースに正しい値が格納されていることを確認してください。
IVR	IVR 対応の VSAN は、**no interop**（デフォルト）モード、または **interop** モードのいずれかで設定できます。

interop モード 1 の設定

Cisco MDS 9000 ファミリ スイッチの interop モード 1 のイネーブル化は、中断を伴うかまたは中断を伴わずに行うことができます。

（注）　Brocade スイッチから Cisco MDS 9000 ファミリ スイッチまたは McData スイッチに接続する前に、Brocade の msplmgmtdeactivate コマンドを確実に実行する必要があります。このコマンドでは、Brocade 独自のフレームを使用して、Cisco MDS 9000 スイッチまたは McData スイッチが認識しないプラットフォーム情報を交換します。これらのフレームを拒否すると、一般的な E ポートが隔離されます。

Fabric Manager を使用して VSAN に interop モード 1 を設定する手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSANxxx] > [VSAN Attributes] を選択します。

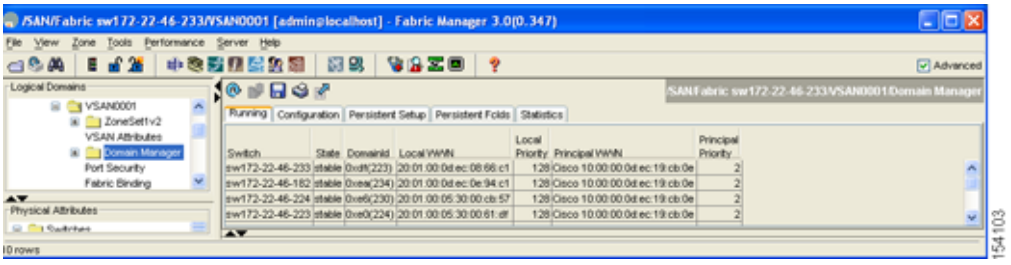
ステップ 2　[Interop] ドロップダウン メニューで [Interop-1] を選択します。

ステップ 3　[Apply Changes] をクリックして、この interop モードを保存します。

ステップ 4　Logical Domains ペインで [VSANxxx] を展開し、[Domain Manager] を選択します。

[Information] ペインに Domain Manager の設定が表示されます（図 12-5 を参照）。

図 12-5　Domain Manager の設定



ステップ 5　ドメイン ID を、97（0x61）～ 127（0x7F）の範囲で設定します。

a. [Configuration] タブをクリックします。

b. [Configuration] タブの [Configure Domain ID] 列をクリックします。

c. [Running] タブをクリックして、ドメイン ID が変更されたことを確認します。

（注）　これは、McData スイッチによって課せられる制限です。

（注）　ドメイン ID を変更すると、N ポートに割り当てられた FC ID も変更されます。

ステップ 6　ファイバ チャネル タイマーを変更します（システムのデフォルト値以外の場合）。

（注）　Cisco MDS 9000、Brocade、McData FC Error Detect（ED_TOV）、および Resource Allocation（RA_TOV）の各タイマーは、同じ値にデフォルト設定されています。これらの値は、必要に応じて変更できます。RA_TOV のデフォルト値は 10 秒、ED_TOV のデフォルト値は 2 秒です。FC-SW2 標準に基づく場合、これらの値は、ファブリック内の各スイッチで一致している必要があります。

a. [Switches] > [FC Services] を展開し、[Timers and Policies] を選択します。[Information] ペインにタイマーの設定が表示されます。

b. [Change Timeouts] をクリックして、タイムアウト値を変更します。

c. [Apply] をクリックして、新しいタイムアウト値を保存します。

ステップ 7　（任意）[VSANxxx] > [Domain Manager] > [Configuration] タブを選択し、[Restart] 列で [disruptive] または [nonDisruptive] を選択して、ドメインを再起動します。

相互運用性ステータスの確認

ここでは、ファブリックが起動していて、interop モードで稼動しているかを確認する場合に使用する手順について説明します。

Fabric Manager を使用して Cisco MDS 9000 ファミリのスイッチの相互運用性ステータスを確認するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで [Switches] を選択し、[Information] ペインでリリース番号を調べて、Cisco NX-OS リリースを確認します。

ステップ 2　各スイッチのインターフェイス モードを確認するために、[Switches] > [Interfaces] を展開し、[FC Physical] を選択します。

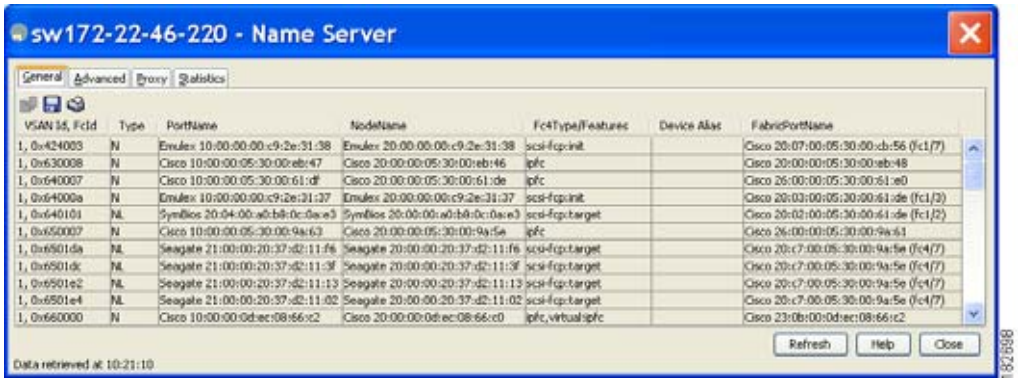
ステップ 3　[Logical Domains] ペインで [Fabricxx] を展開し、[All VSANs] を選択して、すべての VSAN の interop モードを確認します。

ステップ 4　[Fabricxx] > [All VSANs] を展開し、[Domain Manager] を選択して、すべての VSAN のドメイン ID、ローカル、および主要 sWWN を確認します（図 12-6 を参照）。

図 12-6　Domain Manager の情報

ステップ 5　Device Manager を使用して、[FC] > [Name Server] を選択し、ネーム サーバ情報を確認します。[Name Server] ダイアログボックスが表示されます（図 12-7 を参照）。

図 12-7　[Name Server] ダイアログボックス



ステップ 6　[Close] をクリックして、ダイアログボックスを閉じます。

（注）　Cisco MDS ネーム サーバには、ローカル エントリとリモート エントリの両方が表示され、エントリはタイムアウトしません。

デフォルト設定

表 12-3 に、この章で説明した機能のデフォルト設定を示します。

表 12-3　拡張機能のデフォルト設定

パラメータ	デフォルト
CIM サーバ	ディセーブル
CIM サーバ セキュリティ プロトコル	HTTP
D_S_TOV	5,000 ミリ秒
E_D_TOV	2,000 ミリ秒
R_A_TOV	10,000 ミリ秒
fctrace を起動するためのタイムアウト期間	5 秒
fcping 機能で送信されるフレーム数	5 フレーム
リモート キャプチャ接続プロトコル	TCP
リモート キャプチャ接続モード	パッシブ
ローカル キャプチャ フレームの制限	10 フレーム
FC ID の割り当てモード	auto モード
ループ モニタリング	ディセーブル
D_S_TOV	5,000 ミリ秒
E_D_TOV	2,000 ミリ秒
R_A_TOV	10,000 ミリ秒
interop モード	ディセーブル

INDEX

B

C

D

E

F

H

I

L

M

N

P

R

S

T

V

W

X

あ

せ

そ

た

て

と

ね

は

ふ

ほ

ま

め

よ

り

る

ろ