



Cisco MDS 9000 Family NX-OS ファブリック コンフィギュレーション ガイド

2016 年 1 月 28 日

Cisco Systems, Inc.

www.cisco.com

シスコは世界各国 200 箇所にオフィスを開設しています。
各オフィスの住所、電話番号、FAX 番号は
当社の Web サイトをご覧ください
(www.cisco.com/go/offices)

**【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。
リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco MDS 9000 Family NX-OS ファブリック コンフィギュレーション ガイド
© 2016 Cisco Systems, Inc. All rights reserved.



新機能および変更された機能に関する情報 1

はじめに 1

CHAPTER 1

ファブリックの概要 1-1

仮想 SAN 1-1

ダイナミック ポート VLAN メンバーシップ 1-2

SAN デバイス仮想化 1-2

ゾーン分割 1-2

Distributed Device Alias Service 1-3

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 1-3

マルチプロトコル サポート 1-4

CHAPTER 2

VSAN の設定と管理 2-1

VSAN の概要 2-1

VSAN トポロジ 2-2

VSAN の利点 2-4

VSAN とゾーン 2-4

VSAN 設定 2-5

予約済み VSAN 範囲と分離された VSAN 範囲のガイドライン 2-6

VSAN の作成 2-7

VSAN の静的な作成 2-7

VSAN の作成 2-7

ポート VSAN メンバーシップ 2-7

スタティック ポート VSAN メンバーシップの概要 2-8

VSAN スタティック メンバーシップの表示 2-8

デフォルト VSAN 2-9

分離された VSAN 2-9

分離された VSAN メンバーシップの概要 2-10

VSAN の動作ステート 2-10

スタティック VSAN の削除 2-10

スタティック VSAN の削除 2-11

ロード バランシング 2-11

ロード バランシングの設定 2-11

interop モード 2-12

FICON VSAN 2-12

スタティック VSAN 設定の表示 2-12

デフォルト設定 2-13

ファブリック スイッチ情報の表示 2-13

CHAPTER 3**ダイナミック VSAN の作成 3-1**

DPVM の概要 3-1

DPVM 設定の概要 3-2

DPVM のイネーブル化 3-2

DPVM データベースの概要 3-3

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 3-3

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 3-4

自動学習エントリの概要 3-5

自動学習のイネーブル化 3-5

学習エントリの消去 3-6

DPVM データベース配信 3-6

DPVM データベース配信の概要 3-6

DPVM データベース配信のディセーブル化 3-7

ファブリックのロックの概要 3-7

ファブリックのロック 3-7

変更のコミット 3-8

変更の廃棄 3-8

ロック済みセッションのクリア 3-8

データベース マージに関する注意事項 3-8

DPVM データベースのコピーの概要 3-9

DPVM データベースのコピー 3-9

データベースの差分の比較 3-10

DPVM マージのステータスおよび統計情報の表示 3-10

DPVM 設定の表示 3-11

DPVM の設定例 3-12

デフォルト設定 3-15

CHAPTER 4**ゾーンの設定と管理 4-1**

ゾーン分割の概要 4-1

ゾーン分割の例 4-3

ゾーン実装 4-4

ゾーン メンバー設定に関する注意事項 4-4

アクティブ ゾーン セットおよびフル ゾーン セットに関する考慮事項 4-5

Quick Config ウィザードの使用	4-7
ゾーン設定	4-10
Edit Local Full Zone Database ツールの概要	4-10
ゾーンの設定	4-12
Zone Configuration Tool を使用したゾーンの設定	4-13
ゾーン メンバーの追加	4-15
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	4-17
複数のゾーンへの複数のエンド デバイスの追加	4-17
ゾーン セット	4-17
ゾーン セットの作成	4-18
ゾーン セットの非アクティブ化	4-19
ゾーンセットの非アクティブ化	4-21
ゾーン メンバーシップ情報の表示	4-22
デフォルト ゾーン	4-24
デフォルト ゾーンへのアクセス権限の設定	4-25
FC エイリアスの作成の概要	4-26
FC エイリアスの作成	4-26
エイリアスへのメンバーの追加	4-28
ゾーンメンバーの pWWN ベースメンバーへの変換	4-29
ゾーン セットの作成とメンバゾーンの追加	4-30
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	4-32
複数のゾーン セットへの複数のゾーンの追加	4-32
ゾーン分割の実行	4-32
ゾーン セットの配信	4-33
フルゾーン セットの配信の有効化	4-33
ワンタイム配信の有効化	4-34
リンク分離からの回復の概要	4-35
ゾーン セットのインポートおよびエクスポート	4-36
ゾーン セットの複製	4-37
ゾーン セットのコピー	4-38
ゾーンのバックアップおよび復元の概要	4-39
ゾーンのバックアップ	4-39
ゾーンの復元	4-40
ゾーン、ゾーン セット、およびエイリアスの名前の変更	4-42
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	4-43
MDS 以外のデータベースの移行	4-44
ゾーン サーバデータベースのクリア	4-45
詳細なゾーン属性	4-45

ゾーンベースのトラフィックプライオリティの概要	4-46
ゾーンベースのトラフィックプライオリティの設定	4-46
デフォルトゾーンのQoSプライオリティ属性の設定	4-48
デフォルトゾーンポリシーの設定	4-49
ブロードキャストゾーン分割の概要	4-49
ブロードキャストゾーン分割の設定	4-50
スマートゾーン分割の概要	4-51
スマートゾーン分割のメンバー設定	4-52
VSANでのスマートゾーン分割の有効化	4-52
スマートゾーン分割のデフォルト値の設定	4-52
スマートゾーン分割へのゾーンの自動変換	4-53
ゾーンメンバーのデバイスタイプの設定	4-53
スマートゾーン分割設定の削除	4-54
ゾーンレベルでのスマートゾーン分割の無効化	4-54
LUNゾーン分割の概要	4-55
LUNベースのゾーンの設定	4-56
ストレージサブシステムへのLUNの割り当て	4-57
読み取り専用ゾーンの概要	4-58
読み取り専用ゾーンの設定	4-58
ゾーン情報の表示	4-59
拡張ゾーン分割	4-68
拡張ゾーン分割の概要	4-69
基本ゾーン分割から拡張ゾーン分割への変更	4-70
拡張ゾーン分割から基本ゾーン分割への変更	4-70
拡張ゾーン分割の有効化	4-71
ゾーンデータベースの変更	4-72
ゾーンの保留中差分の自動表示の有効化	4-73
ゾーンデータベースロックの解除	4-73
属性グループの作成	4-74
データベースのマージ	4-74
ゾーンマージの分析	4-84
ゾーンマージ制御ポリシーの設定	4-85
ゾーンによるFC2バッファのフラッシュの防止	4-86
デフォルトゾーンでのトラフィックの許可または拒否	4-86
ゾーンのブロードキャスト	4-86
システムのデフォルトゾーン分割設定値の設定	4-87
ゾーンのGeneric Serviceアクセス権限の設定	4-88
拡張ゾーン情報の表示	4-89
ダウングレード用のゾーンデータベースの圧縮	4-91

ゾーンおよびゾーン セットの分析	4-92
ゾーン サーバパフォーマンスの強化	4-94
ゾーン サーバファイバチャネル ネーム サーバ共有データベース	4-94
ゾーン サーバ SNMP 最適化	4-95
ゾーン サーバ差分配信	4-96
デフォルト設定	4-97

CHAPTER 5

DDAS 5-1

デバイス エイリアスについて	5-1
デバイス エイリアスのモード	5-1
モード設定の変更	5-2
デバイス エイリアス モード 配信	5-2
デバイス エイリアス差分限定配信	5-3
さまざまなモードのデバイス エイリアスのマージ	5-5
マージ失敗およびデバイス エイリアス モード不一致の解決	5-5
デバイス エイリアスの機能	5-6
デバイス エイリアスの前提条件	5-6
ゾーン エイリアスとデバイス エイリアスの比較	5-7
デバイス エイリアス データベース	5-7
デバイス エイリアスの作成	5-8
デバイス エイリアス配信の概要	5-8
デバイス エイリアスの作成の概要	5-9
デバイス エイリアス設定のベスト プラクティスの概要	5-9
変更のコミット	5-10
デバイス エイリアスの保留中差分表示の有効化	5-11
変更の廃棄	5-11
ファブリックのロックの上書き	5-12
データベースの内容のクリア	5-12
統計情報のクリア	5-12
デバイス エイリアス配信の無効化と有効化	5-12
レガシー ゾーン エイリアス設定の変換の概要	5-13
ゾーン エイリアスのインポート	5-14
デバイス エイリアス統計情報のクリア	5-14
データベース マージに関する注意事項	5-15
デバイス エイリアス設定の確認	5-15
デフォルト設定	5-17

FSPF の概要	6-1
FSPF の例	6-2
FSPF のグローバル設定	6-4
SPF 計算ホールド タイムの概要	6-4
Link State Record のデフォルトの概要	6-4
VSAN での FSPF の設定	6-5
FSPF のデフォルト設定へのリセット	6-5
FSPF の有効化または無効化	6-6
VSAN の FSPF カウンタのクリア	6-6
FSPF のインターフェイスでの設定	6-6
FSPF リンク コストの概要	6-7
FSPF リンク コストの設定	6-7
hello タイム インターバルの概要	6-7
hello タイム インターバルの設定	6-7
デッド タイム インターバルの概要	6-8
デッド タイム インターバルの設定	6-8
再送信インターバルの概要	6-8
再送信インターバルの設定	6-9
インターフェイス単位での FSPF のディセーブル化	6-9
特定のインターフェイスに対する FSPF のディセーブル化	6-9
インターフェイスの FSPF カウンタのクリア	6-10
FSPF ルート	6-10
ファイバチャネルのルートの概要	6-10
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	6-11
マルチキャスト ルート スイッチの概要	6-11
マルチキャスト ルート スイッチの設定	6-11
順序どおりの配信	6-12
ネットワーク フレーム順序の再設定の概要	6-13
ポート チャネル フレーム順序の再設定の概要	6-13
順序どおりの配信の有効化の概要	6-14
順序どおりの配信のグローバルなイネーブル化	6-14
特定の VSAN に対する順序どおりの配信のイネーブル化	6-15
順序どおりの配信のステータスの表示	6-15
ドロップ遅延時間の設定	6-15
遅延情報の表示	6-16
フロー統計情報の設定	6-16
フロー統計の概要	6-17
集約フロー統計情報のカウント	6-17

個々のフロー統計情報のカウント	6-17
FIB 統計情報のクリア	6-18
フロー統計情報の表示	6-18
グローバル FSPF 情報の表示	6-18
FSPF データベースの表示	6-19
FSPF インターフェイスの表示	6-20
デフォルト設定	6-21

CHAPTER 7

DWDM の設定 7-1

DWDM の概要	7-1
X2 DWDM トランシーバ周波数の設定	7-1

CHAPTER 8

FLOGI、ネーム サーバ、FDMI、および RSCN データベースの管理 8-1

FLOGI の概要	8-1
FLOGI の詳細の表示	8-1
ネーム サーバ	8-3
ネーム サーバから送信される一括通知	8-3
ネーム サーバの一括通知の有効化	8-3
ネーム サーバの一括通知の無効化	8-4
ネーム サーバプロキシ登録	8-5
ネーム サーバプロキシの登録	8-5
重複 pWWN の拒否の概要	8-5
重複 pWWN の拒否	8-5
ネーム サーバデータベース エントリ	8-6
ネーム サーバのデータベース同期の最適化	8-6
ネーム サーバデータベースのエントリ数の確認	8-6
ネーム サーバデータベースのエントリの表示	8-7
FDMI	8-8
FDMI の表示	8-8
RSCN	8-10
RSCN 情報について	8-11
RSCN 情報の表示	8-11
multi-pid オプション	8-12
multi-pid オプションの設定	8-12
ドメイン フォーマット SW-RSCN の抑制	8-12
結合 SW-RSCN	8-13
結合 SW RSCN の有効化	8-13
結合 SW-RSCN の無効化	8-14
RSCN 統計情報のクリア	8-14

CFS を使用した RSCN タイマー設定の配布	8-15
RSCN タイマーの設定	8-15
RSCN タイマー設定の確認	8-16
RSCN タイマー設定の配信	8-16
デフォルト設定	8-19
ポート ペーシングの有効化	8-19

CHAPTER 9

SCSI ターゲットの検出	9-1
SCSI LUN 検出の概要	9-1
SCSI LUN 検出の開始の概要	9-2
SCSI LUN 検出の開始	9-2
カスタマイズ検出開始の概要	9-2
カスタマイズ検出の開始	9-2
SCSI LUN 情報の表示	9-3

CHAPTER 10

FICON の設定	10-1
FICON の概要	10-1
FICON の要件	10-2
MDS 固有 FICON のメリット	10-3
FICON のカスケード化	10-7
FICON VSAN の前提条件	10-7
FICON ポート番号の設定	10-8
デフォルトの FICON ポート番号設定方式	10-9
ポートアドレス	10-11
実装ポートおよび非実装ポートのアドレス	10-11
予約済み FICON ポート番号設定方式の概要	10-11
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	10-12
FICON ポート番号設定に関するガイドライン	10-12
スロットへの FICON ポート番号の割り当て	10-13
FICON ポート番号割り当ての表示	10-13
FCIP およびポートチャネルのポート番号の概要	10-14
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	10-14
FC ID の割り当て	10-15
FICON の設定	10-16
VSAN の FICON を有効にする操作の概要	10-16
スイッチでの FICON の有効化	10-17
基本 FICON 設定のセットアップ	10-17
VSAN での手動での FICON のイネーブル化	10-20

[code-page] オプションの設定	10-21
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	10-22
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	10-22
ホストでタイムスタンプを制御できるようにする	10-22
タイムスタンプのクリア	10-23
FICON パラメータの SNMP 制御の設定	10-23
FICON デバイスの従属関係の概要	10-23
FICON デバイスの従属関係のクリア	10-24
実行コンフィギュレーションの自動保存	10-24
FICON ポートの設定	10-25
PortChannel へのポート番号のバインド	10-26
FCIP インターフェイスへのポート番号のバインド	10-26
ポート ブロックの設定	10-26
ポートの禁止	10-27
ポート アドレス名の割り当て	10-29
RLIR の概要	10-29
RLIR 優先ホストの指定	10-29
RLIR 情報の表示	10-30
RLIR 情報のクリア	10-34
FICON コンフィギュレーション ファイル	10-34
FICON コンフィギュレーション ファイルの概要	10-35
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	10-35
FICON コンフィギュレーション ファイルの編集	10-36
FICON コンフィギュレーション ファイルの表示	10-36
FICON コンフィギュレーション ファイルのコピー	10-38
ポート スワッピング	10-38
ポート スワッピングの概要	10-39
ポート スワッピング	10-40
FICON テープ アクセラレーション	10-40
FICON テープ アクセラレーション設定	10-42
FICON テープ読み取りアクセラレーション設定	10-43
XRC アクセラレーションの設定	10-44
FICON VSAN のオフライン状態への移行	10-44
CUP インバンド管理	10-45
ゾーンへの CUP の配置	10-45
制御ユニットの情報の表示	10-46
FICON 情報の表示	10-46
FICON アラートの受信	10-47

FICON ポート アドレス情報の表示	10-47
FICON コンフィギュレーション ファイル情報の表示	10-49
設定された FICON の状態の表示	10-50
ポート管理状態の表示	10-50
バッファ情報の表示	10-51
履歴バッファの表示	10-52
実行コンフィギュレーションの FICON 情報の表示	10-52
スタートアップ コンフィギュレーションの FICON 情報の表示	10-53
FICON 関連のログ情報の表示	10-53
デフォルト設定	10-54

CHAPTER 11

高度な機能および概念 11-1

共通情報モデル (CIM)	11-1
ファイバチャネル タイムアウト値	11-2
すべての VSAN のタイマー設定	11-2
VSAN ごとのタイマー設定	11-3
fctimer 配信の概要	11-3
fctimer 配信の有効化	11-4
fctimer 設定変更のコミット	11-4
fctimer 設定変更の廃棄	11-4
ファブリックのロックの上書き	11-4
データベース結合に関する注意事項	11-5
設定された fctimer 値の表示	11-5
組織固有識別子	11-6
注意事項と制約事項	11-6
OUI の追加および削除	11-6
OUI の追加と削除の設定例	11-6
World Wide Name (WWN)	11-7
WWN 情報の表示	11-7
リンク初期化時の WWN の使用方法	11-8
セカンダリ MAC アドレスの設定	11-8
HBA の FC ID 割り当て	11-9
デフォルトの企業 ID リスト	11-9
企業 ID の設定の確認	11-10
スイッチの相互運用性	11-11
Interop モードの概要	11-11
interop モード 1 の設定	11-13
デフォルト設定	11-18

CHAPTER 12**Fibre Channel Common Transport 管理セキュリティの設定 12-1**

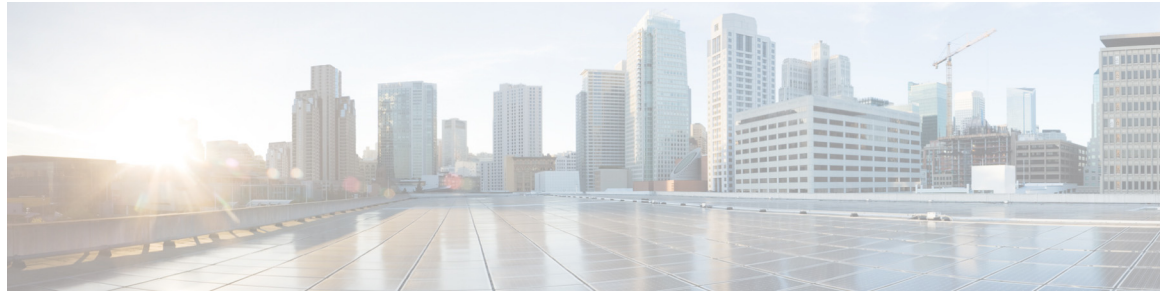
Fibre Channel Common Transport の概要 12-1

設定時の注意事項 12-1

Fibre Channel Common Transport クエリーの設定 12-2

Fibre Channel Common Transport 管理セキュリティの確認 12-2

デフォルト設定値 12-3



新機能および変更された機能に関する情報

表 1-1 に、このガイドで取り上げる MDS NX-OS リリース 5.0(1a) 以降の新機能および変更された機能を示します。

表 1-1 新機能および変更された機能

機能	追加または変更された内容	変更が行われたリリース	参照先
ゾーン サーバの機能 拡張	次の機能によりゾーン サーバのパフォーマンスが強化されました。 <ul style="list-style-type: none"> ゾーン サーバ FCNS 共有データベース ゾーン サーバ SNMP 最適化 ゾーン サーバ差分配信 	7.3(0)D1(1)	第 4 章「ゾーンの設定と管理」
デバイス エイリアス差分限定配信	ファブリック内のすべてのスイッチでこの機能を有効にすると、拡張性が向上します。	7.3(0)D1(1)	第 5 章「DDAS」
組織固有識別子	この機能により、組織固有識別子 (OUI) をシステム OUI データベースに動的に追加するための新しいコマンドが導入されました。	7.3(0)D1(1)	第 11 章「組織固有識別子」
デバイス エイリアスコミットの確認 ゾーン コミットの確認	ゾーンおよびデバイス エイリアスのコミット時に保留中差分の表示が追加されました。	6.2(9)	第 5 章「DDAS」 第 4 章「ゾーンの設定と管理」
FC および FCOE スケール: デバイス エイリアス	「デバイス エイリアス設定のベスト プラクティスの概要」の項が追加されました。	6.2(9)	第 5 章「DDAS」
Fibre Channel Common Transport 管理サーバクエリー	Fibre Channel Common Transport 管理サーバクエリーの設定	6.2(9)	第 12 章「Fibre Channel Common Transport 管理セキュリティの設定」
FCNS、RSCN	FCNS データベース変更をリッスンするすべてのコンポーネントのパフォーマンスを向上する一括通知機能が追加されました。 RSCN のパフォーマンス向上のため結合 SWRSCN が追加されました。	6.2(7)	第 8 章「FLOGI、ネーム サーバ、FDMI、および RSCN データベースの管理」
	「ファブリック スイッチ情報の表示」の項が追加されました。	6.2(7)	第 2 章「VSAN の設定と管理」

表 1-1 新機能および変更された機能(続き)

機能	追加または変更された内容	変更が行われたリリース	参照先
スマート ゾーン分割	コマンド出力が追加されました。	6.2(7)	第 4 章「ゾーンの設定と管理」
スマート ゾーン分割	「スマート ゾーン分割」の項が追加されました。	5.2.6	第 4 章「ゾーンの設定と管理」
FICON テープ読み取りアクセラレーション	「FICON テープ アクセラレーション」の項が追加されました。	5.0(1a)	第 10 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。また、関連マニュアル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 MDS 9000 Family NX-OS 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	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 4 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 5 章	DDAS	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 6 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。

章	タイトル	説明
第 7 章	DWDM の設定	高密度波長分割多重 (DWDM) 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 8 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な、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 9 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 10 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 11 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。



(注)

お客様のニーズを満たすためにドキュメントを更新するという継続的な取り組みの一環として、シスコでは設定タスクの文書化方法を変更しました。そのため、本ドキュメントには、従来とは異なるスタイルでの設定タスクが説明されている部分もあります。ドキュメントに新たに組み込まれるようになったセクションには、以下のセクションが含まれます。

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、山カッコ (<>) で囲んで示しています。
[]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!,#	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。



(注)

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



注意

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

関連資料

Cisco MDS 9000 ファミリのマニュアル セットには次のマニュアルが含まれます。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/doclocator.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 MDS SAN-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』

法規制の遵守と安全に関する情報

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

互換性に関する情報

- 『Cisco Data Center Interoperability Support Matrix』
- 『Cisco MDS 9000 NX-OS Hardware and Software Compatibility Information and Feature Lists』
- 『Cisco MDS NX-OS Release Compatibility Matrix for Storage Service Interface Images』
- 『Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide』

- 『Cisco MDS NX-OS Release Compatibility Matrix for IBM SAN Volume Controller Software for Cisco MDS 9000』
- 『Cisco MDS SAN-OS Release Compatibility Matrix for VERITAS Storage Foundation for Networks Software』

ハードウェアの設置

- 『Cisco MDS 9500 Series Hardware Installation Guide』
- 『Cisco MDS 9200 Series Hardware Installation Guide』
- 『Cisco MDS 9100 Series Hardware Installation Guide』
- 『Cisco MDS 9124 and Cisco MDS 9134 Multilayer Fabric Switch Quick Start Guide』

ソフトウェアのインストールおよびアップグレード

- 『Cisco MDS 9000 NX-OS Release 4.1(x)』および『SAN-OS 3(x) Software Upgrade and Downgrade Guide』
- 『Cisco MDS 9000 Family Storage Services Interface Image Install and Upgrade Guide』
- 『Cisco MDS 9000 Family Storage Services Module Software Installation and Upgrade Guide』

Cisco NX-OS

- 『Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS 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 Intelligent Storage Services Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide』

コマンドライン インターフェイス

- 『Cisco MDS 9000 Family Command Reference』

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

- 『Cisco MDS 9000 Family I/O Accelerator 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』
- 『Cisco MDS 9000 Family Cookbook for Cisco MDS SAN-OS』

トラブルシューティングおよび参考資料

- 『Cisco NX-OS System Messages Reference』
- 『Cisco MDS 9000 Family NX-OS Troubleshooting Guide』
- 『Cisco MDS 9000 Family NX-OS MIB Quick Reference』
- 『Cisco MDS 9000 Family NX-OS SMI-S Programming 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 の『What's New in Cisco Product Documentation』を参照してください。
<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

『What's New in Cisco Product Documentation』は、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し、RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。





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 \(1-1 ページ\)](#)
- [ダイナミック ポート VLAN メンバーシップ \(1-2 ページ\)](#)
- [SAN デバイス仮想化 \(1-2 ページ\)](#)
- [ゾーン分割 \(1-2 ページ\)](#)
- [Distributed Device Alias Service \(1-3 ページ\)](#)
- [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 \(1-3 ページ\)](#)
- [マルチプロトコル サポート \(1-4 ページ\)](#)

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) に基づいてメンバーシップを割り当てることができる、特定の VSAN に対するユーザ操作の効果を分離することにより、SAN の管理性を高め、人為的な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 ファミリースイッチは、VSAN のトランッキングも実装します。トランッキングでは、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 メンバーシップ

スイッチのポート VSAN メンバーシップは、ポート単位で割り当てられます。デフォルトでは、各ポートはデフォルト VSAN に属します。VSAN をデバイス WWN に基づいて割り当てることにより、VSAN メンバー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 メンバー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。



(注) SDV は、Cisco MDS NX-OS Release 4.x 以降ではサポートされていません。

ゾーン分割

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

- N ポート ゾーン分割: エンド デバイス (ホストおよびストレージ) ポートに基づいてゾーンメンバーを定義します。
 - WWN
 - ファイバ チャネル ID (FC-ID)
- Fx ポート ゾーン分割: スイッチ ポートに基づいてゾーンメンバーを定義します。
 - WWN
 - WWN およびインターフェイス インデックス、またはドメイン ID およびインターフェイス インデックス
- ドメイン ID およびポート番号 (Brocade の相互運用性用)。

- iSCSI ゾーン分割: ホスト ゾーンに基づいてゾーン メンバーを定義します。
 - iSCSI 名
 - IP アドレス
- LUN ゾーン分割: N ポート ゾーン分割と組み合わせて使用すると、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。



(注) LUN ゾーン分割および読み取り専用ゾーンは、Cisco MDS NX-OS Release 5.x 以降ではサポートされていません。

- 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 ファミリースイッチでの 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。



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 チャンネル 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 を作成できます。各 VSAN には最大 239 台のスイッチを組み込みます。それぞれの VSAN は、異なる VSAN で同じファイバ チャンネル ID (FC ID) を同時に使用できる独立したアドレス領域を持ちます。この章は、次の項で構成されています。

- [VSAN の概要 \(2-1 ページ\)](#)
- [VSAN 設定 \(2-5 ページ\)](#)
- [スタティック VSAN 設定の表示 \(2-12 ページ\)](#)
- [デフォルト設定 \(2-13 ページ\)](#)
- [ファブリック スイッチ情報の表示 \(2-13 ページ\)](#)

VSAN の概要

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

VSAN を導入することによって、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 を含むトポロジを 1 つ作成できます。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、ドメイン マネージャ、およびゾーン分割などの必要なすべてのプロトコルを実行します。
- VSAN 内のファブリック関連の設定は、別の VSAN 内の関連トラフィックに影響しません。
- ある VSAN 内のトラフィック中断を引き起こしたイベントはその VSAN 内にとどまり、他の VSAN に伝播されません。

ここでは VSAN について説明します。具体的な内容は次のとおりです。

- VSAN トポロジ(2-2 ページ)
- VSAN の利点(2-4 ページ)
- VSAN とゾーン(2-4 ページ)

VSAN トポロジ

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、3つのスイッチによるファブリック(各階にスイッチは1つ)を示します。スイッチと接続された装置の地理的な配置は、論理 VSAN の区分けには依存しません。VSAN 間では通信できません。各 VSAN 内では、すべてのメンバが相互に対話できます。

図 2-1 論理 VSAN の区分け

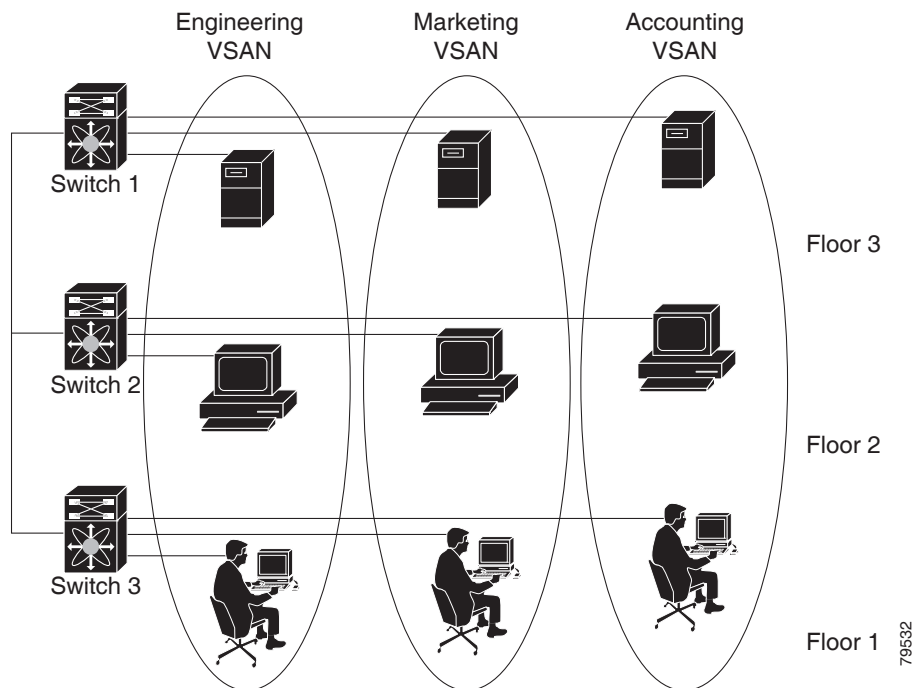
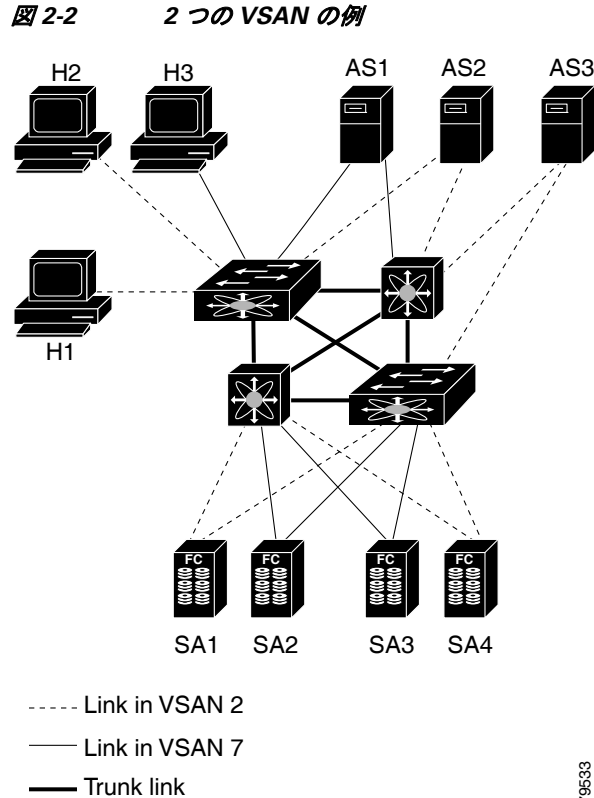


図 2-2 に、VSAN 2(破線)と VSAN 7(実線)の2つの定義済み VSAN からなるファイバチャネルスイッチングの物理インフラストラクチャを示します。VSAN 2 には、ホスト H1 と H2、アプリケーション サーバ AS2 と AS3、ストレージアレイ SA1 と SA4 が含まれます。VSAN 7 は、H3、AS1、SA2、および SA3 と接続します。



このネットワークにある4つのスイッチは、VSAN 2トラフィックおよびVSAN 7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ています。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がもしなければ、SANごとに別個のスイッチとリンクが必要です。VSANをイネーブルにすることによって、同一のスイッチとリンクが複数のVSANで共有されることがあります。VSANでは、スイッチ精度ではなく、ポート精度でSANを作成できます。図2-2は、VSANが物理SANで定義された仮想トポロジを使用して相互に通信するホストまたはストレージデバイスのグループであることを表しています。

このようなグループを作成する基準は、VSANトポロジによって異なります。

- VSANは、次の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 データセンター内の異なるお客様
 - 企業ネットワークの業務またはテスト
 - ローセキュリティおよびハイセキュリティの要件
 - 別個のVSANによるバックアップトラフィック
 - ユーザトラフィックからのデータの複製
- VSANは、特定の部門またはアプリケーションのニーズを満たせます。

VSAN の利点

VSAN には、次のような利点があります。

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

最大 256 の VSAN を 1つのスイッチに設定できます。これらの VSAN の 1つがデフォルト VSAN (VSAN 1)、もう 1つが独立 VSAN (VSAN 4094) です。ユーザ指定の VSAN ID 範囲は 2 ~ 4093 です。

VSAN とゾーン

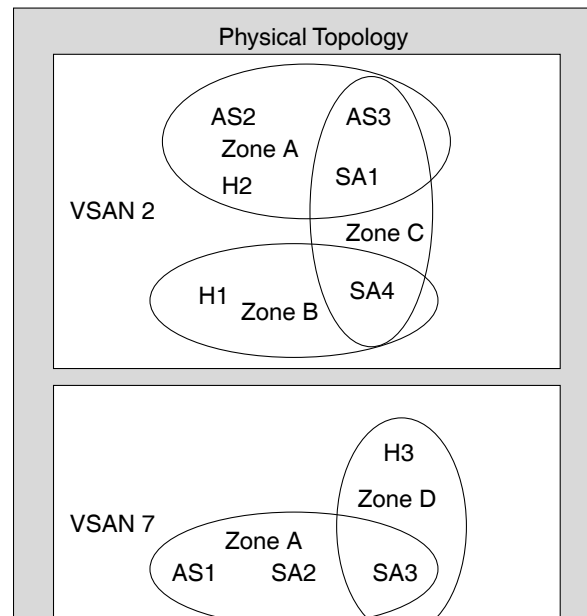
VSAN に複数のゾーンを定義できます。2つの VSAN は未接続の 2つの SAN に相当するので、VSAN 1 のゾーン A は、VSAN 2 のゾーン A とは異なる、別個のものです。表 2-1 に、VSAN とゾーンの相違点を示します。

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、およびゾーンングプロトコルは、ゾーン単位で利用できません。
—	ゾーンは、VSAN 内に常に含まれます。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。
メンバーシップは、通常 VSAN ID を使用して Fx ポートに定義されます。	メンバーシップは、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、送信元ポート、および宛先ポートでメンバーシップを実行します。	ゾーンは、送信元ポートおよび宛先ポートだけでメンバーシップを実行します。
VSAN は、規模が大きい環境 (ストレージ サービス プロバイダー) で定義されます。	ゾーンは、ゾーンの外部に表示されないイニシエータおよびターゲットのセットで定義されます。
VSAN は、ファブリック全体を網羅します。	ゾーンは、ファブリック エッジで設定されます。

図 2-3 に、VSAN とゾーンとの可能な組み合わせを示します。VSAN 2 には、ゾーン A、ゾーン B、ゾーン C の 3 つのゾーンが定義されています。ゾーン C は、ファイバ チャネル標準に準拠してゾーン A とゾーン B にオーバーラップしています。VSAN 7 には、ゾーン A とゾーン D の 2 つのゾーンが定義されています。VSAN 境界を越えるゾーンはありません。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 とは別個のもです。

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)、および独立 VSAN (VSAN 4094) で VSAN を識別します。
- **状態:** VSAN の管理状態を **active** (デフォルト) または **suspended** に設定できます。VSAN が作成されると、VSAN はさまざまな状態またはステートに置かれます。
 - VSAN の **active** ステートは、VSAN が設定されイネーブルであることを示します。VSAN をイネーブルにすることによって、VSAN のサービスをアクティブにします。
 - VSAN の **suspended** ステートは、VSAN が設定されているがイネーブルではないことを示します。この VSAN にポートが設定されている場合、ポートはディセーブルの状態です。このステートを使用して、VSAN の設定を失うことなく VSAN を非アクティブにします。suspended ステートの VSAN のすべてのポートは、ディセーブルの状態です。VSAN を suspended ステートにすることによって、ファブリック全体のすべての VSAN パラメータを事前設定し、VSAN をただちにアクティブにできます。
- **VSAN 名:** このテキスト文字列は、管理目的で VSAN を識別します。名前は、1 ~ 32 文字で指定できます。また、すべての VSAN で一意である必要があります。デフォルトでは、VSAN 名は VSAN と VSAN ID を表す 4 桁のストリングを連結したものです。たとえば、VSAN 3 のデフォルト名は VSAN0003 です。



(注) VSAN 名は一意である必要があります。

- ロード バランシング属性: 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説明します。具体的な内容は次のとおりです。

- [予約済み VSAN 範囲と分離された VSAN 範囲のガイドライン \(2-6 ページ\)](#)
- [VSAN の静的な作成 \(2-7 ページ\)](#)
- [ポート VSAN メンバーシップ \(2-7 ページ\)](#)
- [スタティック ポート VSAN メンバーシップの概要 \(2-8 ページ\)](#)
- [VSAN スタティック メンバーシップの表示 \(2-8 ページ\)](#)
- [デフォルト VSAN \(2-9 ページ\)](#)
- [分離された VSAN \(2-9 ページ\)](#)
- [分離された VSAN メンバーシップの概要 \(2-10 ページ\)](#)
- [VSAN の動作ステート \(2-10 ページ\)](#)
- [スタティック VSAN の削除 \(2-10 ページ\)](#)
- [スタティック VSAN の削除 \(2-11 ページ\)](#)
- [ロード バランシング \(2-11 ページ\)](#)
- [ロード バランシングの設定 \(2-11 ページ\)](#)
- [interop モード \(2-12 ページ\)](#)
- [FICON VSAN \(2-12 ページ\)](#)

予約済み VSAN 範囲と分離された VSAN 範囲のガイドライン

いずれかのインターフェイスでトランキングが設定されている NPV スイッチ、またはトランキング F ポート チャンネル機能を有効にするために `f port-channel-trunk` コマンドが実行される標準スイッチでは、以下の予約済み VSAN と分離された VSAN の設定ガイドラインに従います。

- いずれかのインターフェイスでトランク モードがオンであるか、NP ポート チャンネルが稼働している場合、予約済み VSAN は 3840 ~ 4078 であり、ユーザ設定には使用できません。
- Exchange Virtual Fabric Protocol (EVFP) 分離 VSAN は 4079 であり、ユーザ設定には使用できません。

VSAN の作成

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

VSAN の静的な作成

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

VSAN の作成

VSAN を作成するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# vsan database switch(config-vsan-db)#	VSAN に対するデータベースを設定します。アプリケーション特有の VSAN パラメータは、このプロンプトから設定できません。
ステップ 3	switch(config-vsan-db) # vsan 2	指定された ID(2)の VSAN が存在しない場合は、指定された ID で VSAN を作成します。
ステップ 4	switch(config-vsan-db) # vsan 2 name TechDoc updated vsan 2	割り当てられた名前ですべて VSAN を更新します (TechDoc)。
ステップ 5	switch(config-vsan-db) # vsan 2 suspend	選択された VSAN を中断します。
ステップ 6	switch(config-vsan-db) # no vsan 2 suspend	前のステップで入力した suspend コマンドを無効にします。
ステップ 7	switch(config-vsan-db) # end switch#	EXEC モードに戻ります。

ポート VSAN メンバーシップ

スイッチのポート VSAN メンバーシップは、ポート単位で割り当てられます。デフォルトでは、各ポートはデフォルト VSAN に属します。2 つの方式のいずれかを使用して、ポートに VSAN メンバーシップを割り当てることができます。

- 静的: VSAN をポートに割り当てる
「[スタティック ポート VSAN メンバーシップの概要](#)」セクション(2-8 ページ)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式は、Dynamic Port VSAN Membership (DPVM) と呼ばれます。
参照先 [第 3 章「ダイナミック VSAN の作成」](#)

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 メンバーシップの概要

インターフェイスポートの VSAN メンバーシップを静的に割り当てるには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# vsan database switch(config-vsan-db)#	VSAN に対するデータベースを設定します。
ステップ 3	switch(config-vsan-db)# vsan 2	指定された ID(2)の VSAN が存在しない場合は、指定された ID で VSAN を作成します。
ステップ 4	switch(config-vsan-db)# vsan 2 interface fc1/8	指定された VSAN(VSAN 2)に、fc1/8 インターフェイスのメンバーシップを割り当てます。
ステップ 5	switch(config-vsan-db)# vsan 7	指定された ID(7)の VSAN が存在しない場合は、指定された ID で VSAN を新規に作成します。
ステップ 6	switch(config-vsan-db)# vsan 7 interface fc1/8	変更された VSAN を反映させるために、インターフェイスのメンバーシップ情報を更新します。
	switch(config-vsan-db)# vsan 1 interface fc1/8	VSAN 7 から インターフェイス fc1/8 を削除し、VSAN 1 (デフォルト VSAN) に割り当てます。 VSAN 7 から インターフェイス fc1/8 の VSAN メンバーシップを削除するには、別の VSAN に対して fc1/8 の VSAN メンバーシップを定義する必要があります。 ベスト プラクティスは、VSAN 1 に割り当て直すことです。

VSAN スタティック メンバーシップの表示

VSAN スタティック メンバーシップ情報を表示するには、**show vsan membership** コマンドを使用します(例 2-1 ~ 例 2-3 を参照)。

例 2-1 指定された VSAN のメンバーシップ情報の表示

```
switch # show vsan 1 membership
vsan 1 interfaces:
    fc1/1   fc1/2   fc1/3   fc1/4   fc1/5   fc1/6   fc1/7   fc1/9
    fc1/10  fc1/11  fc1/12  fc1/13  fc1/14  fc1/15  fc1/16  port-channel 99
```



(注)

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

例 2-2 すべての VSAN のスタティック メンバーシップ情報の表示

```
switch # show vsan membership
vsan 1 interfaces:
    fc2/16 fc2/15 fc2/14 fc2/13 fc2/12 fc2/11 fc2/10 fc2/9
    fc2/8 fc2/7 fc2/6 fc2/5 fc2/4 fc2/3 fc2/2 fc2/1
    fc1/16 fc1/15 fc1/14 fc1/13 fc1/12 fc1/11 fc1/10 fc1/9
    fc1/7 fc1/6 fc1/5 fc1/4 fc1/3 fc1/2 fc1/1
vsan 2 interfaces:
    fc1/8
vsan 7 interfaces:
vsan 100 interfaces:
vsan 4094(isolated vsan) interfaces:
```

例 2-3 指定されたインターフェイスのスタティック メンバーシップ情報の表示

```
switch # show vsan membership interface fc1/1
fc1/1
    vsan:1
    allowed list:1-4093
```

デフォルト VSAN

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



(注) VSAN 1 は削除できませんが、中断できます。



(注) 最大 256 の VSAN を 1 つのスイッチに設定できます。これらの VSAN の 1 つがデフォルト VSAN (VSAN 1)、もう 1 つが独立 VSAN (VSAN 4094) です。ユーザ指定の VSAN ID 範囲は 2 ~ 4093 です。

分離された VSAN

VSAN 4094 は独立 VSAN です。ポートが属する VSAN が削除された場合、非ランキング 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 内にポートを設定するか、ポートを VSAN 4094 に移動すると、このポートがすぐに分離されます。



注意 独立 VSAN を使用してポートを設定しないでください。



(注)

最大 256 の VSAN を 1 つのスイッチに設定できます。これらの VSAN の 1 つがデフォルト VSAN (VSAN 1)、もう 1 つが独立 VSAN (VSAN 4094) です。ユーザ指定の VSAN ID 範囲は 2 ~ 4093 です。

分離された VSAN メンバーシップの概要

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

VSAN の動作ステート

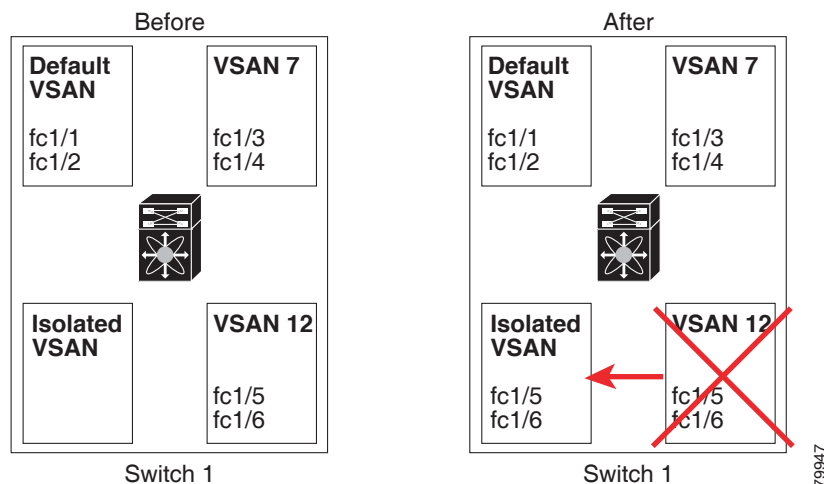
VSAN がアクティブの状態、最低 1 つのポートがアップの状態であれば、VSAN は動作ステートにあります。このステートは、トラフィックがこの VSAN を通過できることを示します。このステートは設定できません。

スタティック VSAN の削除

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

- VSAN 属性およびポート メンバーシップの詳細は、VSAN マネージャによって保持されます。コンフィギュレーションから VSAN を削除すると、この機能が影響を受けます。VSAN が削除されると、VSAN 内のすべてのポートが非アクティブになり、ポートが独立 VSAN に移動されます。同一の VSAN が再作成されると、ポートはその VSAN に自動的に割り当てられることはありません。明示的にポート VSAN メンバーシップを再設定する必要があります (図 2-4 を参照)。

図 2-4 VSAN ポート メンバーシップの詳細



79947

- 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

VSAN とその各種属性を削除するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# vsan database switch(config-db)#	VSAN データベースを設定します。
ステップ 3	switch-config-db# vsan 2 switch(config-vsan-db)#	VSAN コンフィギュレーション モードを開始します。
ステップ 4	switch(config-vsan-db)# no vsan 5 switch(config-vsan-db)#	データベースおよびスイッチから VSAN 5 を削除します。
ステップ 5	switch(config-vsan-db)# end switch#	EXEC モードに戻ります。

ロード バランシング

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

既存の VSAN にロード バランシングを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# vsan database switch(config-vsan-db)#	VSAN データベース コンフィギュレーション サブモードを開始します。
ステップ 3	switch(config-vsan-db)# vsan 2	既存の VSAN を指定します。

■ スタティック VSAN 設定の表示

	コマンド	目的
ステップ 4	<code>switch(config-vsan-db)# vsan 2 loadbalancing src-dst-id</code>	選択された VSAN に対してロード バランシングの保証をイネーブルにし、スイッチがパス選択プロセスで送信元/宛先 ID を使用するようになります。
	<code>switch(config-vsan-db)# no vsan 2 loadbalancing src-dst-id</code>	前のステップで実行したコマンドを無効にし、ロード バランシング パラメータのデフォルト値に戻します。
	<code>switch(config-vsan-db)# vsan 2 loadbalancing src-dst-ox-id</code>	送信元 ID、宛先 ID、OX ID (デフォルト) を使用するようにパス選択設定を変更します。
ステップ 5	<code>switch(config-vsan-db)# vsan 2 suspend</code>	選択された VSAN を中断します。
ステップ 6	<code>switch(config-vsan-db)# no vsan 2 suspend</code>	前のステップで入力した suspend コマンドを無効にします。
ステップ 7	<code>switch(config-vsan-db)# end switch#</code>	EXEC モードに戻ります。

interop モード

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](#)」セクション(11-11 ページ)を参照してください。

FICON VSAN

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](#)」セクション(10-7 ページ)を参照してください。

スタティック VSAN 設定の表示

設定されている VSAN に関する情報を表示するには、`show vsan` コマンドを使用します(例 2-4 ~ 2-6 を参照)。

例 2-4 特定の VSAN の設定の表示

```
switch# show vsan 100
vsan 100 information
      name:VSAN0100 state:active
      in-order guarantee:no interoperability mode:no
      loadbalancing:src-id/dst-id/oxid
```

例 2-5 VSAN の使用状況の表示

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

例 2-6 すべての VSAN の表示

```

switch# show vsan
vsan 1 information
    name:VSAN0001 state:active
    in-order guarantee:no interoperability mode:no
    loadbalancing:src-id/dst-id/oxid
vsan 2 information
    name:VSAN0002 state:active
    in-order guarantee:no interoperability mode:no
    loadbalancing:src-id/dst-id/oxid
vsan 7 information
    name:VSAN0007 state:active
    in-order guarantee:no interoperability mode:no
    loadbalancing:src-id/dst-id/oxid
vsan 100 information
    name:VSAN0100 state:active
    in-order guarantee:no interoperability mode:no
    loadbalancing:src-id/dst-id/oxid
vsan 4094:isolated vsan

```

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 VSAN パラメータ

パラメータ (Parameters)	デフォルト
デフォルト VSAN	VSAN 1
状態	active ステート
名前	VSAN と VSAN ID を表す 4 桁のストリングを連結したものです。たとえば、VSAN 3 は VSAN0003 です。
ロード バランシング属性	OX ID(src-dst-ox-id)

ファブリック スイッチ情報の表示

特定の VSAN のファブリック内の各スイッチに関する情報を表示するには、**show fabric switch information vsan** コマンドを使用します。

例 2-7 ファブリック内のすべてのスイッチに関する情報の表示

```

switch# show fabric switch information vsan 100

VSAN 1:
-----
SwitchName                Model                Version             SupMemory
-----
huashan12                 DS-C9148-48P-K9    5.2 (2d)           n/a
alishan-bgl-25           DS-C9250I-K9      6.2 (5a)           n/a
Hac18                     DS-C9506           6.2 (7)            2 GB
Hac17                     DS-C9506           6.2 (5)            n/a
Cocol                     DS-C9222I-K9      6.2 (7)            1 GB

switch#

```

■ ファブリックスイッチ情報の表示



(注) このコマンドは、Cisco NX-OS Release 6.2(7) より古いリリースではサポートされていません。



(注) Cisco NX-OS Release 6.2(7) より古いリリースが稼働しているスイッチでは、SUP メモリは表示されません。



(注) VSAN オプションを使用していない場合、このコマンドではすべての VSAN のスイッチに関する情報が表示されます。



ダイナミック VSAN の作成

この章は、次の項で構成されています。

- [DPVM の概要 \(3-1 ページ\)](#)
- [DPVM データベース配信 \(3-6 ページ\)](#)
- [データベース マージに関する注意事項 \(3-8 ページ\)](#)
- [DPVM 設定の表示 \(3-11 ページ\)](#)
- [DPVM の設定例 \(3-12 ページ\)](#)
- [デフォルト設定 \(3-15 ページ\)](#)

DPVM の概要

スイッチのポート VSAN メンバーシップは、ポート単位で割り当てられます。デフォルトでは、各ポートはデフォルト VSAN に属します。

VSAN をデバイス WWN に基づいて割り当てることにより、VSAN メンバー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 メンバー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。

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 メンバー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 メンバー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 メンバー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 \(3-2 ページ\)](#)
- [DPVM のイネーブル化 \(3-2 ページ\)](#)
- [DPVM データベースの概要 \(3-3 ページ\)](#)
- [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 \(3-3 ページ\)](#)
- [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 \(3-4 ページ\)](#)
- [自動学習エントリの概要 \(3-5 ページ\)](#)
- [自動学習のイネーブル化 \(3-5 ページ\)](#)
- [学習エントリの消去 \(3-6 ページ\)](#)

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 メンバー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 のイネーブル化

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 の設定および確認コマンドを使用できるのは、スイッチ上で DPVM がイネーブルに設定されている場合だけです。この機能をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

参加しているスイッチの DPVM を有効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# feature dpvm	スイッチ上で DPVM をイネーブルにします。
	switch(config)# no feature dpvm	スイッチ上の DPVM をディセーブルにします (デフォルト)。



(注) 重複する pWWN ログインでログイン情報を上書きするには、**dpvm overwrite-duplicate-pwwn** コマンドを入力します。

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: ファブリックが現在実行しているデータベース。
- 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」セクション \(3-6 ページ\)](#) 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。

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

DPVM 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。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# device-alias mode enhanced switch(config)# device-alias commit	拡張デバイス エイリアス モードを有効にします。これは、DPVM データベースのデバイス エイリアス設定に必要です。

	コマンド	目的
ステップ 3	switch(config)# dpvm database switch(config-dpvm-db)#	DPVM コンフィギュレーション データベースを作成します。
	switch(config)# no dpvm database	DPVM コンフィギュレーション データベースを削除します。
ステップ 4	switch(config-dpvm-db)# pwwn 12:33:56:78:90:12:34:56 vsan 100	指定したデバイス pWWN を VSAN 100 にマッピングします。
	switch(config-dpvm-db)# no pwwn 12:33:56:78:90:12:34:56 vsan 101	DPVM コンフィギュレーション データベースから指定されたデバイス pWWN マッピングを削除します。
ステップ 5	switch(config-dpvm-db)# nwwn 14:21:30:12:63:39:72:81 vsan 101	指定したデバイス nWWN を VSAN 101 にマッピングします。
	switch(config-dpvm-db)# no nwwn 14:21:30:12:63:39:72:80 vsan 101	DPVM コンフィギュレーション データベースから指定されたデバイス nWWN マッピングを削除します。
ステップ 6	switch(config-dpvm-db)# device-alias device1 vsan 102	指定したデバイス エイリアスを VSAN 102 にマッピングします。
	switch(config-dpvm-db)# no device-alias device1 vsan 102	DPVM コンフィギュレーション データベースから指定されたデバイス エイリアス マッピングを削除します。

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。

DPVM を無効にするには、**no dpvm activate** コマンドを実行して、現在アクティブな 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。

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には、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# dpvm activate	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。
	switch(config)# no dpvm activate	現在アクティブな DPVM データベースを非アクティブにします。
	switch(config)# dpvm activate force	競合するエントリを上書きするため、DPVM コンフィギュレーション データベースを強制的にアクティブにします。

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の場合、次のようになります。
 - 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

自動学習を有効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# dpvm auto-learn	スイッチ上で学習をイネーブルにします。
	switch(config)# no dpvm auto-learn	スイッチ上で学習を無効にします(デフォルト)。
	switch(config)# clear dpvm auto-learn	自動学習エントリのリストをクリアします。
	switch(config)# clear dpvm auto-learn pwwn pwwn	分散 DPVM データベースの自動学習 pWWN エントリのリストをクリアします。

学習エントリの消去

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)。

- 1つの自動学習エントリを消去するには、**clear dpvm auto-learn pwwn** コマンドを使用します。
switch# `clear dpvm auto-learn pwwn 55:22:33:44:55:66:77:88`
- すべての自動学習エントリを消去するには、**clear dpvm auto-learn** コマンドを使用します。
switch# `clear dpvm auto-learn`



(注) これらの2つのコマンド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 データベース配信の概要 \(3-6 ページ\)](#)
- [DPVM データベース配信のディセーブル化 \(3-7 ページ\)](#)
- [ファブリックのロックの概要 \(3-7 ページ\)](#)
- [ファブリックのロック \(3-7 ページ\)](#)
- [変更のコミット \(3-8 ページ\)](#)
- [変更の廃棄 \(3-8 ページ\)](#)
- [ロック済みセッションのクリア \(3-8 ページ\)](#)

DPVM データベース配信の概要

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

DPVM 保留データベースの内容を表示するには、**show dpvm pending** コマンドを実行します。

DPVM データベース配信のディセーブル化

近接スイッチへの DPVM データベース配信を無効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# no dpvm distribute	近接スイッチへの DPVM 配信をディセーブルにします。
	switch(config)# dpvm distribute	近接スイッチへの DPVM 配信をイネーブルにします(デフォルト)。

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、次の条件が適用されます。

- 他のユーザがこの機能の設定に変更を加えることができなくなります。
- コンフィギュレーション データベースのコピーが、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

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。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# dpvm database switch(config-dpvm-db)#	DPVM コンフィギュレーション データベースにアクセスします。
ステップ 3	switch(config-dpvm-db)# pwnn 11:22:33:44:55:66:77:88 vsan 11	DPVM コンフィギュレーション データベースに 1 つのエントリを追加します。
ステップ 4	switch(config-dpvm-db)# exit switch(config)#	コンフィギュレーション モードに戻ります。
ステップ 5	switch(config)# dpvm activate	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。

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ず。コミットが正常に行われると、設定の変更がファブリック全体に適用され、ロックが解除されます。

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。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# dpvm commit	DPVM 保留データベースに現在含まれているデータベース エントリをコミットします。

変更の廃棄

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。

DPVM 保留データベースを廃棄するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# dpvm abort	DPVM 保留データベースに現在含まれているデータベース エントリを廃棄します。

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。

管理者の特権を使用して、ロックされた DPVM セッションを解除するには、EXEC モードで **clear dpvm session** コマンドを使用します。

```
switch# clear dpvm session
```

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

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

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 \(3-9 ページ\)](#)
- [DPVM データベースのコピー \(3-9 ページ\)](#)
- [データベースの差分の比較 \(3-10 ページ\)](#)
- [DPVM マージのステータスおよび統計情報の表示 \(3-10 ページ\)](#)

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

現在アクティブな 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には、`dpvm database copy` コマンドを使用します。

```
switch# dpvm database copy active
Legend: "+" New Entry, "-" Missing Entry, "*" Possible Conflict Entry
-----
- pwn 12:33:56:78:90:12:34:56 vsan 100
- nwn 14:21:30:12:63:39:72:81 vsan 101
```

データベースの差分の比較

次のように DPVM データベースを比較できます。

- アクティブな DPVM データベースを DPVM コンフィギュレーション データベースと比較するには、**dpvm database diff active** コマンドを使用します。

```
switch# dpvm database diff active
Legend: "+" New Entry, "-" Missing Entry, "*" Possible Conflict Entry
-----
- pwn 44:22:33:44:55:66:77:88 vsan 44
* pwn 11:22:33:44:55:66:77:88 vsan 11
```

- DPVM コンフィギュレーション データベースをアクティブ DPVM データベースと比較するには、**dpvm database diff config** コマンドを使用します。

```
switch# dpvm database diff config
Legend: "+" New Entry, "-" Missing Entry, "*" Possible Conflict Entry
-----
+ pwn 44:22:33:44:55:66:77:88 vsan 44
* pwn 11:22:33:44:55:66:77:88 vsan 22
```

- DPVM 保留データベースを DPVM コンフィギュレーション データベースと比較するには、**show dpvm pending-diff** コマンドを使用します(CFS 配信がイネーブルの場合)。

DPVM コンフィギュレーション データベースに保留中のデータベース エントリを追加するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# dpvm distribute	CFS 配信を有効にします。
ステップ 3	switch(config)# dpvm database	DPVM コンフィギュレーション データベースにアクセスします。
ステップ 4	switch(config-dpvm-db)# pwn 44:22:33:44:55:66:77:88 vsan 55 switch(config-dpvm-db)# pwn 55:22:33:44:55:66:77:88 vsan 55	DPVM コンフィギュレーション データベースに 2 つのエントリを追加します。

DPVM マージのステータスおよび統計情報の表示

DPVM データベース マージの統計情報を表示するには、次の手順を実行します。

コマンド	目的
switch# show dpvm merge statistics switch(config)#	DPVM データベース マージの統計情報を表示します。
switch(config)# clear dpvm merge statistics switch(config)#	DPVM データベース マージの統計情報をクリアします。

次に、DPVM データベース マージでの競合の例を示します。

```
switch# show dpvm merge status
Last Merge Time Stamp   : Fri Aug  8 15:46:36 2008
Last Merge State        : Fail
Last Merge Result       : Fail
```

```
Last Merge Failure Reason : DPVM DB conflict found during merge [cfs_status: 76] Last
Merge Failure Details: DPVM merge failed due to database conflict
Local Switch WWN          : 20:00:00:0d:ec:24:e5:00
Remote Switch WWN        : 20:00:00:0d:ec:09:d5:c0
```

```
-----
Conflicting DPVM member(s)                Loc VSAN   Rem VSAN
-----
dev-alias dpvm_dev_alias_1 [21:00:00:04:cf:cf:45:ba]   1313      1414
dev-alias dpvm_dev_alias_2 [21:00:00:04:cf:cf:45:bb]   1313      1414
dev-alias dpvm_dev_alias_3 [21:00:00:04:cf:cf:45:bc]   1313      1414
[Total 3 conflict(s)]
rbadri-excal13#
```

次に、DDAS モードでの競合の例を示します。

```
switch# show dpvm merge status
Last Merge Time Stamp      : Fri Aug  8 15:46:36 2008
Last Merge State          : Fail
Last Merge Result         : Fail
Last Merge Failure Reason : DPVM DB conflict found during merge [cfs_status: 76] Last
Merge Failure Details: DPVM merge failed due to DDAS mode conflict
Local Switch WWN          : 20:00:00:0d:ec:24:e5:00
Remote Switch WWN        : 20:00:00:0d:ec:09:d5:c0
Local DDAS mode           : Basic
Remote DDAS mode          : Enhanced
```

DPVM 設定の表示

VSAN 単位で設定されている WWN に関する情報を表示するには、**show dpvm** コマンドを使用します(例 3-1 ~ 3-6 を参照)。

例 3-1 DPVM 設定ステータスの表示

```
switch# show dpvm status
DB is activated successfully, auto-learn is on
```

例 3-2 指定された VSAN の現在の DPVM ダイナミック ポートの表示

```
switch# show dpvm ports vsan 10
-----
Interface Vsan Device pWWN                Device nWWN
-----
fc1/2      10    29:a0:00:05:30:00:6b:a0 fe:65:00:05:30:00:2b:a0
```

例 3-3 DPVM コンフィギュレーション データベースの表示

```
switch# show dpvm database
pwwn 11:22:33:44:55:66:77:88 vsan 11
pwwn 22:22:33:44:55:66:77:88 vsan 22
pwwn 33:22:33:44:55:66:77:88 vsan 33
pwwn 44:22:33:44:55:66:77:88 vsan 44
[Total 4 entries]
```

例 3-4 DPVM データベースの表示

```
switch# show dpvm database active
pwwn 11:22:33:44:55:66:77:88 vsan 22
pwwn 22:22:33:44:55:66:77:88 vsan 22
pwwn 33:22:33:44:55:66:77:88 vsan 33
[Total 3 entries]
* is auto-learnt entry
```

例 3-5 DPVM コンフィギュレーション データベースの表示

```
switch# show dpvm database
pwwn 11:22:33:44:55:66:77:88 vsan 11
pwwn 22:22:33:44:55:66:77:88 vsan 22
pwwn 33:22:33:44:55:66:77:88 vsan 33
pwwn 44:22:33:44:55:66:77:88 vsan 44
[Total 4 entries]
```

例 3-6 保留中のデータベースと DPVM コンフィギュレーション データベースの比較

```
switch# show dpvm pending-diff
Legend: "+" New Entry, "-" Missing Entry, "*" Possible Conflict Entry
-----
+ pwwn 55:22:33:44:55:66:77:88 vsan 55
- pwwn 11:22:33:44:55:66:77:88 vsan 11
* pwwn 44:22:33:44:55:66:77:88 vsan 44
```

DPVM の設定例

基本的な DPVM シナリオを設定するには、次の手順を実行します。

- ステップ 1** DPVM をイネーブルにし、DPVM 配信をイネーブルにします。

```
switch1# config
Enter configuration commands, one per line.End with CNTL/Z.
switch1(config)# feature dpvm
switch1(config)# end
switch1# show dpvm database
switch1# show dpvm database active
switch1# show dpvm status
```

この段階では、設定にアクティブ DPVM データベースがなく、**auto-learn** オプションはディセーブルです。

- ステップ 2** ヌル(空の)データベースをアクティブにして、自動学習されたエントリが入力されるようにします。

```
switch1# config
Enter configuration commands, one per line.End with CNTL/Z.
switch1(config)# dpvm activate
switch1(config)# dpvm commit
switch1(config)# end
switch1# show dpvm database
switch1# show dpvm database active
switch1# show dpvm status
```

この段階では、データベースが正常にアクティブ化され、**auto-learn** オプションはディセーブルのままです。

ステップ 3 **auto-learn** オプションを有効にし、設定の変更をコミットします。

```
switch1# config
Enter configuration commands, one per line.End with CNTL/Z.
switch1(config)# dpvm auto-learn
switch1(config)# dpvm commit
switch1(config)# end
switch1# show dpvm database active
pwwn 21:00:00:e0:8b:0e:74:8a vsan 4(*)
pwwn 21:01:00:e0:8b:2e:87:8a vsan 5(*)
[Total 2 entries]
* is auto-learnt entry
switch1# show dpvm ports
-----
Interface   Vsan      Device pWWN      Device nWWN
-----
fc1/24      4         21:00:00:e0:8b:0e:74:8a  20:00:00:e0:8b:0e:74:8a
fc1/27      5         21:01:00:e0:8b:2e:87:8a  20:01:00:e0:8b:2e:87:8a
switch1# show flogi database
-----
INTERFACE   VSAN      FCID          PORT NAME          NODE NAME
-----
fc1/24      4         0xe70100      21:00:00:e0:8b:0e:74:8a  20:00:00:e0:8b:0e:74:8a
fc1/27      5         0xe80100      21:01:00:e0:8b:2e:87:8a  20:01:00:e0:8b:2e:87:8a

Total number of flogi = 2.

switch195# show dpvm status
DB is activated successfully, auto-learn is on
```

この時点で、現在ログインしているデバイス(および現在の VSAN 割り当て)が、アクティブ DPVM データベースに入力されます。ただし、エントリは、アクティブ DPVM データベースで永続的なものではありません。

show dpvm ports および **show flogi database** コマンドの出力には、ログインしている他の 2 台のデバイスが表示されます(この設定例では、switch9 および switch3)。

ステップ 4 switch9 にアクセスし、次のコマンドを実行します。

```
switch9# show dpvm database active
pwwn 21:00:00:e0:8b:0e:87:8a vsan 1(*)
pwwn 21:01:00:e0:8b:2e:74:8a vsan 1(*)
[Total 2 entries]
* is auto-learnt entry
switch9# show dpvm status
DB is activated successfully, auto-learn is on
```

ステップ 5 switch3 にアクセスし、次のコマンドを実行します。

```
switch3# show dpvm database active
pwwn 21:00:00:e0:8b:0e:76:8a vsan 1(*)
pwwn 21:01:00:e0:8b:2e:76:8a vsan 1(*)
[Total 2 entries]
* is auto-learnt entry
switch3# show dpvm status
DB is activated successfully, auto-learn is on
```

ステップ 6 switch1 で自動学習を無効にし、設定変更をコミットします。

```
switch1# config
Enter configuration commands, one per line.End with CNTL/Z.
switch1(config)# no dpvm auto-learn
switch1(config)# dpvm commit
switch1(config)# end
switch1# show dpvm status
```

```

DB is activated successfully, auto-learn is off
switch1# show dpvm database active
pwwn 21:00:00:e0:8b:0e:74:8a vsan 4
pwwn 21:01:00:e0:8b:2e:87:8a vsan 5
pwwn 21:00:00:e0:8b:0e:87:8a vsan 1
pwwn 21:01:00:e0:8b:2e:74:8a vsan 1
pwwn 21:00:00:e0:8b:0e:76:8a vsan 1
pwwn 21:01:00:e0:8b:2e:76:8a vsan 1
[Total 6 entries]
* is auto-learnt entry
switch1# show dpvm status
DB is activated successfully, auto-learn is off

```

この時点で、自動学習エントリは、アクティブ DPVM データベースで永続的なエントリになりました。

ステップ 7 switch9 にアクセスし、次のコマンドを実行します。

```

switch9# show dpvm database active
pwwn 21:00:00:e0:8b:0e:87:8a vsan 1
pwwn 21:01:00:e0:8b:2e:74:8a vsan 1
pwwn 21:00:00:e0:8b:0e:76:8a vsan 1
pwwn 21:01:00:e0:8b:2e:76:8a vsan 1
pwwn 21:00:00:e0:8b:0e:74:8a vsan 4
pwwn 21:01:00:e0:8b:2e:87:8a vsan 5
[Total 6 entries]
* is auto-learnt entry
switch9# show dpvm status
DB is activated successfully, auto-learn is off

```

ステップ 8 switch3 にアクセスし、次のコマンドを実行します。

```

switch3# show dpvm database active
pwwn 21:00:00:e0:8b:0e:76:8a vsan 1
pwwn 21:01:00:e0:8b:2e:76:8a vsan 1
pwwn 21:00:00:e0:8b:0e:87:8a vsan 1
pwwn 21:01:00:e0:8b:2e:74:8a vsan 1
pwwn 21:00:00:e0:8b:0e:74:8a vsan 4
pwwn 21:01:00:e0:8b:2e:87:8a vsan 5
[Total 6 entries]
* is auto-learnt entry
switch3# show dpvm status
DB is activated successfully, auto-learn is off

```



(注) これらの基本手順は、情報がファブリック内のすべてのスイッチで同じであることを確認するのに役立ちます。

これで、Cisco MDS 9000 ファミリ スイッチで基本的な DPVM シナリオを設定しました。

デフォルト設定

表 3-1 に、DPVM 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 DPVM パラメータ

パラメータ (Parameters)	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



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 コントロールの設定が可能になります。ファブリックで管理者権限を持つユーザは、ゾーンを作成してネットワーク セキュリティを強化し、データ損失またはデータ破壊を防止できます。ゾーン分割は、送信元/宛先 ID フィールドを検証することによって実行されます。

FC-GS-4 および FC-SW-3 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または規格に準拠した高度なゾーン分割機能のどちらも使用できます。

この章は、次の項で構成されています。

- [ゾーン分割の概要 \(4-1 ページ\)](#)
- [ゾーン設定 \(4-10 ページ\)](#)
- [ゾーン セット \(4-17 ページ\)](#)
- [ゾーン セットの配信 \(4-33 ページ\)](#)
- [ゾーン セットの複製 \(4-37 ページ\)](#)
- [詳細なゾーン属性 \(4-45 ページ\)](#)
- [ゾーン情報の表示 \(4-59 ページ\)](#)
- [拡張ゾーン分割 \(4-68 ページ\)](#)
- [ダウングレード用のゾーン データベースの圧縮 \(4-91 ページ\)](#)
- [ゾーンおよびゾーン セットの分析 \(4-92 ページ\)](#)
- [ゾーン サーバ パフォーマンスの強化 \(4-94 ページ\)](#)
- [デフォルト設定 \(4-97 ページ\)](#)



(注) [表 2-1 \(2-4 ページ\)](#) に、ゾーンと VSAN の相違点を示します。

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。
 - ゾーンのメンバ同士はアクセスできますが、異なるゾーンのメンバ同士はアクセスできません。
 - ゾーン分割がアクティブでない場合、すべてのデバイスがデフォルト ゾーンのメンバとなります。

- ゾーン分割がアクティブの場合、アクティブ ゾーン(アクティブ ゾーン セットに含まれるゾーン)にないデバイスがデフォルト ゾーンのメンバーとなります。
- ゾーンのサイズを変更できます。
- デバイスは複数のゾーンに所属できます。
- ゾーン セットは、1 つまたは複数のゾーンで構成されます。
 - ゾーン セットは、単一エンティティとしてファブリックのすべてのスイッチでアクティブまたは非アクティブにできます。
 - アクティブにできるのは、常に 1 つのゾーン セットだけです。
 - 1 つのゾーンを複数のゾーン セットのメンバーにできます。
 - MDS スイッチあたりの最大ゾーン セット数は 1000 です。
- ゾーン分割は、ファブリックの任意のスイッチから管理できます。
 - 任意のスイッチからゾーンをアクティブにした場合、ファブリックのすべてのスイッチがアクティブゾーン セットを受信します。また、ファブリック内のすべてのスイッチにフルゾーン セットが配布されます(この機能が送信元スイッチでイネーブルである場合)。
 - 既存のファブリックに新しいスイッチが追加されると、新しいスイッチによってゾーン セットが取得されます。
- ゾーンの変更を中断せずに設定できます。影響を受けないポートまたはデバイスのトラフィックを中断させることなく、新しいゾーンおよびゾーン セットをアクティブにできます。
- ゾーン メンバーシップ基準は、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 ポートの WWN(スイッチ ポートの WWN)を指定します。このメンバーシップは、ポートベース ゾーン分割とも呼ばれます。
 - FC ID: スイッチに接続された N ポートの FC ID をゾーンのメンバーとして指定します。
 - インターフェイスおよび Switch WWN (sWWN): sWWN によって識別されたスイッチのインターフェイスを指定します。このメンバーシップは、インターフェイス ゾーン分割とも呼ばれます。
 - インターフェイスおよびドメイン ID: ドメイン ID によって識別されたスイッチのインターフェイスを指定します。
 - ドメイン ID およびポート番号: 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。
 - シンボル ノード名: メンバー シンボル ノード名を指定します。最大長は 240 文字です。
- デフォルト ゾーン メンバーシップには、特定のメンバーシップとの関係を持たないすべてのポートまたは WWN が含まれます。デフォルト ゾーン メンバー間のアクセスは、デフォルト ゾーン ポリシーによって制御されます。



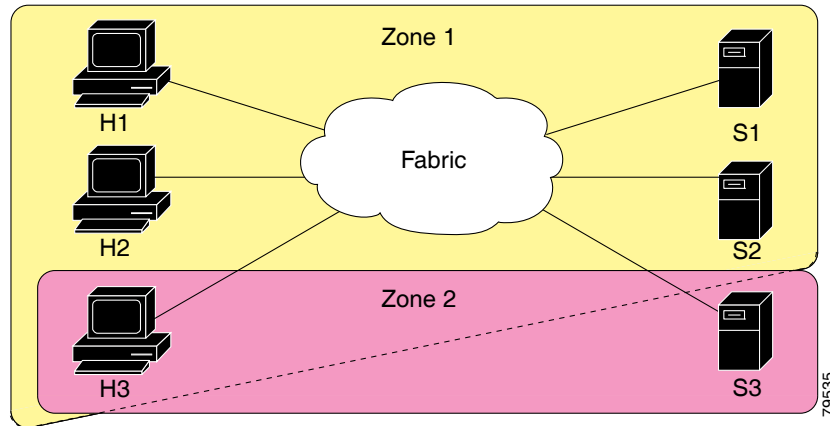
(注)

ゾーン、ゾーン メンバー、およびゾーン セットの数の設定時の制限については、『Cisco MDS NX-OS Configuration Limits』を参照してください。

ゾーン分割の例

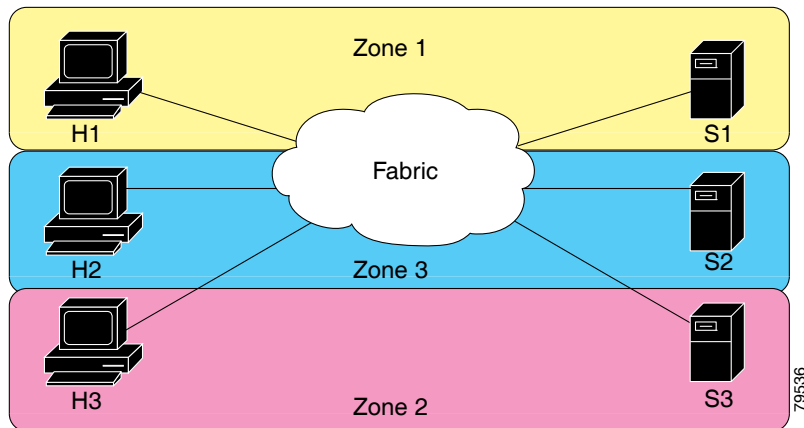
図 4-1 に、ファブリックの 2 つのゾーン(ゾーン 1 およびゾーン 2)で構成されるゾーン セットを示します。ゾーン 1 は、3 つすべてのホスト (H1、H2、H3) からストレージ システム S1 と S2 に存在するデータへのアクセスを提供します。ゾーン 2 では、S3 のデータに H3 からだけアクセスできます。H3 は両方のゾーンに存在することに注意してください。

図 4-1 2 つのゾーンによるファブリック



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 4-2 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ために、ストレージ システム S2 を分離する必要があると想定します。これを実行するために、ホスト H2 とストレージ S2 だけを含むゾーン 3 が設定されます。ゾーン 3 ではアクセスを H2 と S2 だけに限定し、ゾーン 1 ではアクセスを H1 と S1 だけに限定できます。

図 4-2 3 つのゾーンによるファブリック



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 に含まれます。
- ハード ゾーン分割をディセーブルにできません。
- ネーム サーバ クエリーがソフト ゾーン分割されます。
- アクティブ ゾーン セットだけが配布されます。
- ゾーン分割されていないデバイスは、相互にアクセスできません。
- 各 VSAN に同一名のゾーンまたはゾーン セットを含めることができます。
- 各 VSAN には、フル データベースとアクティブ データベースがあります。
- アクティブ ゾーン セットを変更するには、フル ゾーン データベースをアクティブ化する必要があります。
- アクティブ ゾーン セットは、スイッチの再起動後も維持されます。
- フル データベースに加えた変更は、明示的に保存する必要があります。
- ゾーンを再アクティブ化(ゾーン セットがアクティブの状態、別のゾーン セットをアクティブ化する場合)しても、既存のトラフィックは中断しません。

必要に応じて、さらに次のゾーン機能を設定できます。

- VSAN 単位ですべてのスイッチにフル ゾーン セットを伝播します。
- ゾーン分割されていないメンバのデフォルト ポリシーを変更します。
- VSAN を interop モードに設定することによって、他のベンダーと相互運用できます。相互に干渉することなく、同じスイッチ内で1つの VSAN を interop モードに、別の VSAN を基本モードに設定することもできます。
- E ポートを分離状態から復旧します。

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。
- インターフェイスに基づいてゾーン メンバーを設定するときには、ファブリック内でインターフェイス数が最も多い可能性があるファブリック スイッチを常に選択してください。

アクティブ ゾーン セットおよびフル ゾーン セットに関する考慮事項

ゾーン セットを設定する場合は、次の点に注意してください。

- 各 VSAN は、複数のゾーン セットを持つことができますが、アクティブにできるのは常に1つのゾーン セットだけです。
- ゾーン セットを作成すると、そのゾーン セットは、フルゾーン セットの一部となります。
- ゾーン セットがアクティブな場合は、フルゾーン セットのゾーン セットのコピーがゾーン 分割に使用されます。これは、アクティブ ゾーン セットと呼ばれます。アクティブ ゾーン セットは変更できません。アクティブ ゾーン セットに含まれるゾーンは、アクティブ ゾーン と呼ばれます。
- 管理者は、同一名のゾーン セットがアクティブであっても、フルゾーン セットを変更できます。ただし、加えられた変更が有効になるのは、再アクティブ化したときです。
- アクティブ化が実行されると、永続的なコンフィギュレーションにアクティブ ゾーン セットが自動保存されます。これにより、スイッチのリセットにおいてもスイッチはアクティブ ゾーン セット情報を維持できます。
- ファブリックのその他すべてのスイッチは、アクティブ ゾーン セットを受信するので、それぞれのスイッチでゾーン分割を実行できます。
- ハードおよびソフト ゾーン分割は、アクティブ ゾーン セットを使用して実装されます。変更は、ゾーン セットのアクティブ化によって有効になります。
- アクティブ ゾーン セットに含まれない FC ID または Nx ポートは、デフォルト ゾーンに所属します。デフォルト ゾーン情報は、他のスイッチに配信されません。

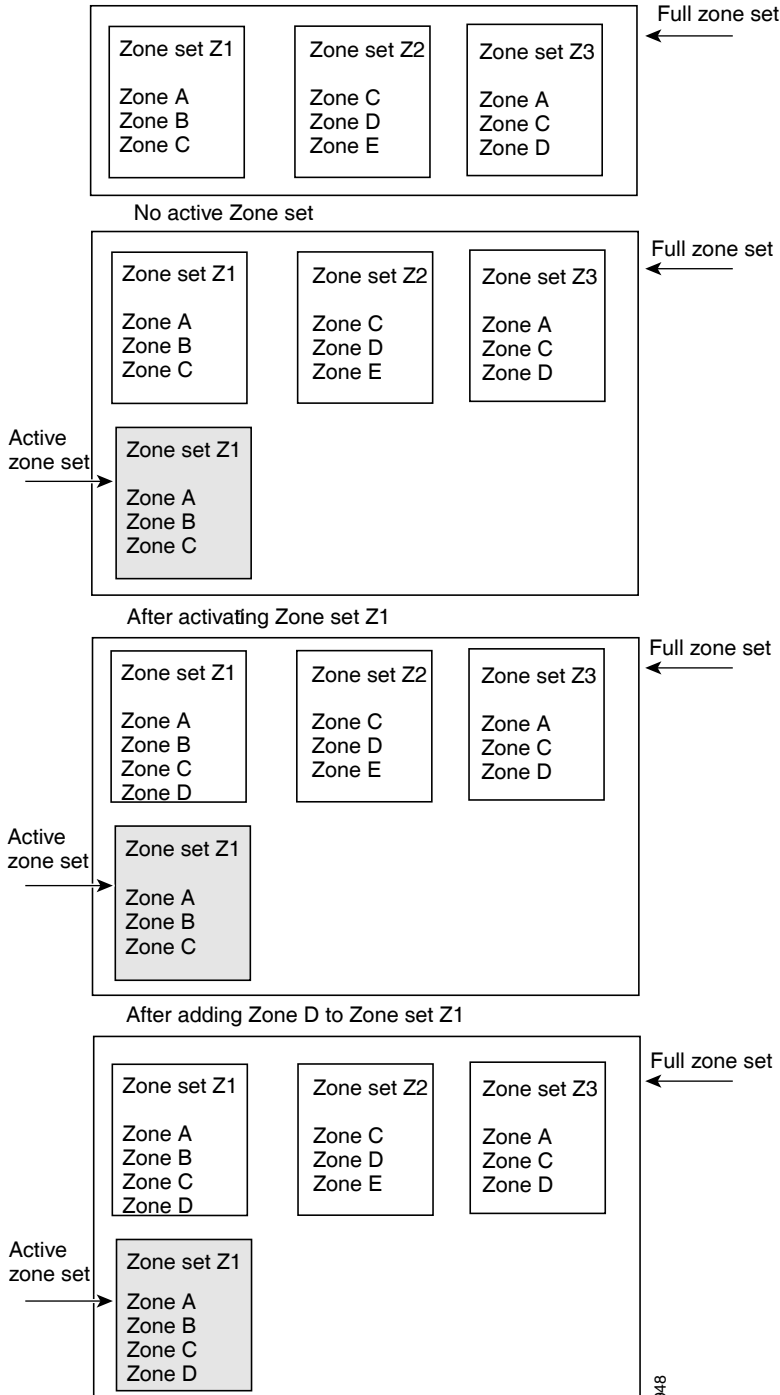


(注)

1つのゾーン セットがアクティブな場合に、別のゾーン セットをアクティブにすると、現在アクティブなゾーン セットが自動的に非アクティブになります。新しいゾーン セットをアクティブにする前に、現在のアクティブ ゾーン セットを明示的に非アクティブにする必要はありません。

図 4-3 に、アクティブにされたゾーン セットに追加されるゾーンを示します。

図 4-3 アクティブおよびフルゾーンセット



148

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スペ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。

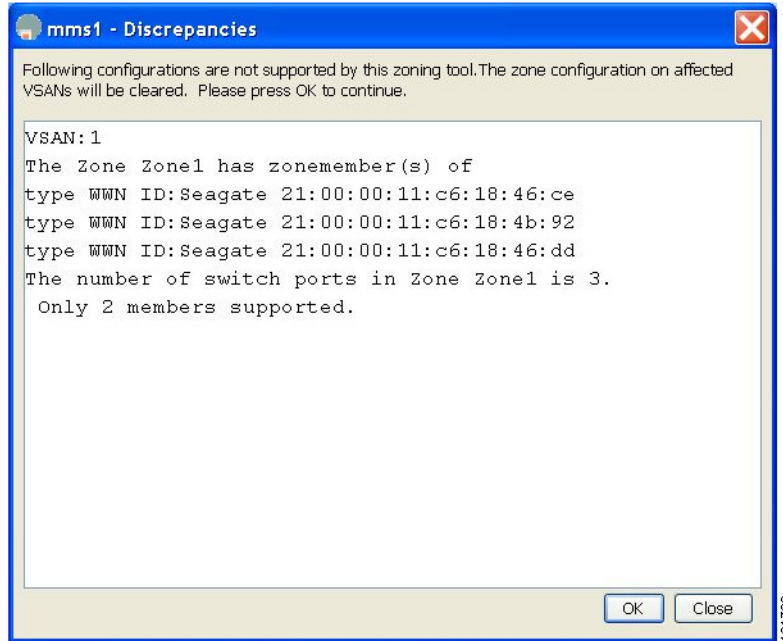
Cisco MDS 9124 スイッチで Device Manager を使用して、ゾーンにポートを追加またはゾーンからポートを削除し、特定の VSAN 内のデバイスだけをゾーン分割する手順は、次のとおりです。

ステップ 1 [FC] > [Quick Config] を選択するか、またはツールバーの [Zone] アイコンをクリックします。すべてのコントロールが無効になっている Quick Config ウィザード (図 4-5 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 4-4 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 4-4 [Discrepancies] ダイアログボックス



ステップ 2 [OK] をクリックして作業を続行します。

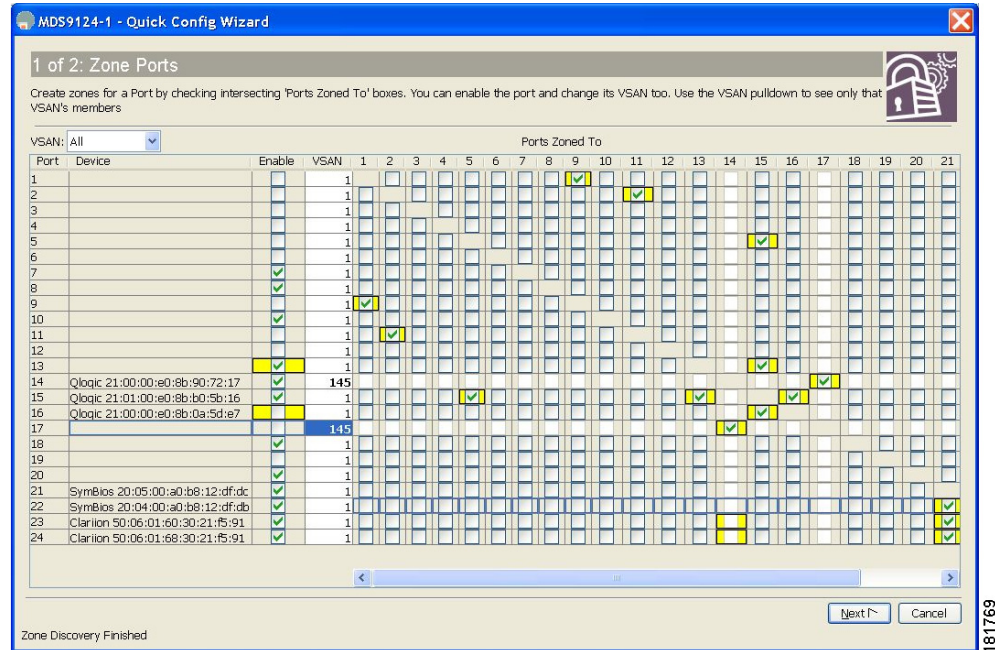
[Quick Config Wizard] ダイアログボックスが表示されます(図 4-5 を参照)。



注意

不一致があり、[OK] をクリックした場合、ゾーン データベースで影響を受ける VSAN は削除されます。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 4-5 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。

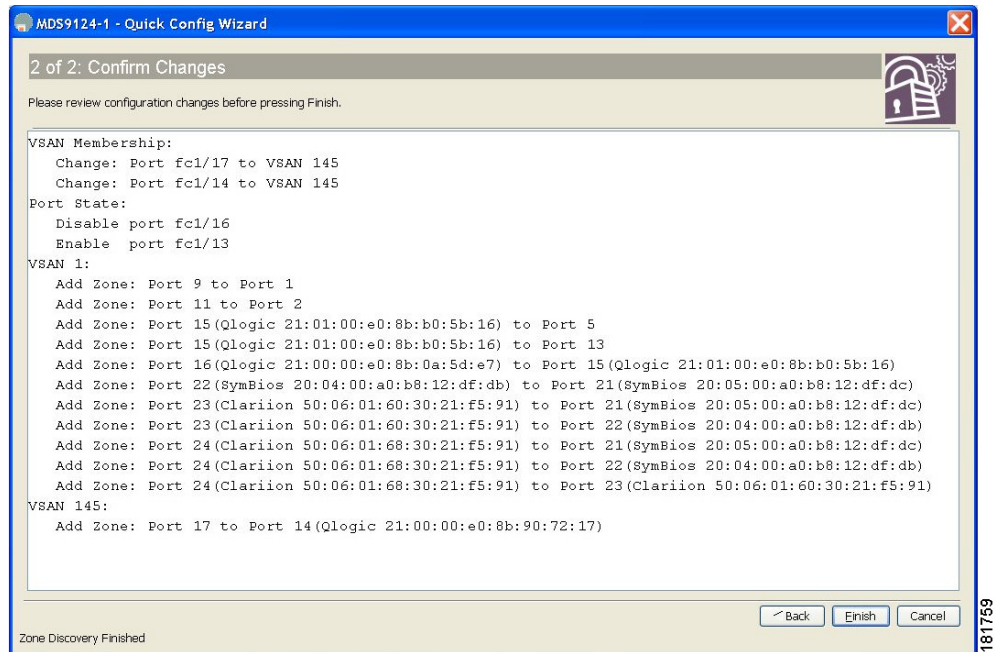
[VSAN] ドロップダウン メニューには、選択された VSAN 内のデバイスだけをゾーン分割できるフィルタが用意されています。

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の確認を行います。

[Confirm Changes] 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 [Confirm Changes] ダイアログボックス



ステップ 6 CLI コマンドを表示する場合は、このダイアログボックスを右クリックして、ポップアップメニューで [CLI Commands] をクリックします。

ステップ 7 設定変更を保存するには、[Finish] をクリックします。

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 \(4-10 ページ\)](#)
- [ゾーンの設定 \(4-12 ページ\)](#)
- [Zone Configuration Tool を使用したゾーンの設定 \(4-13 ページ\)](#)
- [ゾーン メンバーの追加 \(4-15 ページ\)](#)

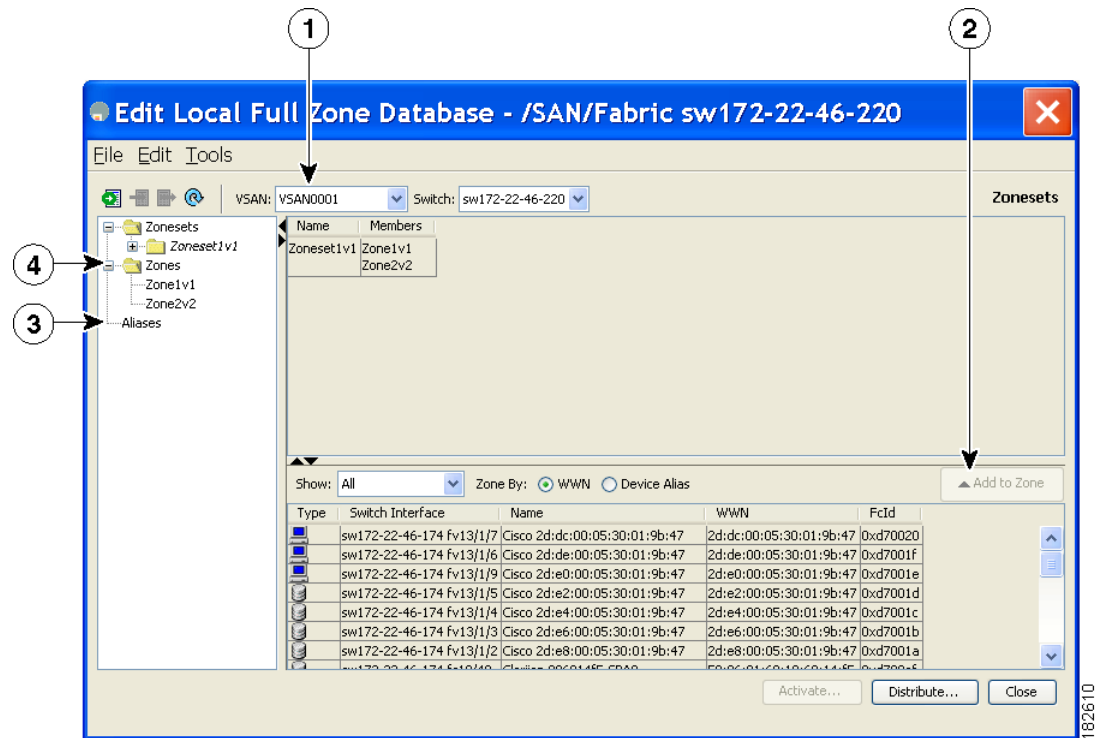
Edit Local Full Zone Database ツールの概要

Edit Local Full Zone Database ツールを使用して、次のタスクを実行できます。

- 画面から移動せずに、プルダウンメニューを使用して VSAN を選択して再入力すると、VSAN 別の情報を表示できます。
- [Add to zone or alias] 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。
- 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。
- 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。

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 4-7 を参照)。

図 4-7 [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] オプション 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」セクション (5-8 ページ) を参照してください。

ゾーンの設定

ゾーンを設定し、ゾーン名を割り当てるには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# zone name Zone1 vsan 3 switch(config-zone)#	vsan3 という VSAN に Zone1 というゾーンを設定します。 (注) すべての英数字か、または記号(\$,-,^,_)のうち1つがサポートされます。
ステップ 3	switch(config-zone)# member type value pWWN example: switch(config-zone)# member pwwn 10:00:00:23:45:67:89:ab Fabric pWWN example: switch(config-zone)# member fwwn 10:01:10:01:10:ab:cd:ef FC ID example: switch(config-zone)# member fcid 0xce00d1 FC alias example: switch(config-zone)# member fcalias Payroll Domain ID example: switch(config-zone)# member domain-id 2 portnumber 23 IPv4 address example: switch(config-zone)# member ip-address 10.15.0.0 255.255.0.0 IPv6 address example: switch(config-zone)# member ipv6-address 2001::db8:800:200c:417a/64 Local sWWN interface example: switch(config-zone)# member interface fc 2/1 Remote sWWN interface example: switch(config-zone)# member interface fc2/1 swwn 20:00:00:05:30:00:4a:de Domain ID interface example: switch(config-zone)# member interface fc2/1 domain-id 25 switch(config-zone)# member symbolic-nodename iqn.test	指定されたタイプ(pWWN、ファブリック pWWN、FC ID、FC エイリアス、ドメイン ID、IPv4 アドレス、IPv6 アドレス、またはインターフェイス)および値に基づいて、指定されたゾーン(Zone1)にメンバーを設定します。  注意 同じファブリック内に FabricWare を実行する Cisco MDS 9020 スイッチがある場合には、Cisco SAN-OS を実行するすべての MDS スイッチには、pWWN タイプのゾーン分割だけを設定する必要があります。 (注) Cisco MDS 9396S スイッチには 96 個のポートがあります。その他の Cisco MDS スイッチのポートの数はこれよりも少なくなります。したがって、インターフェイスに基づいてゾーン メンバーを設定するときには、ファブリック内でインターフェイス数が最も多いと考えられるファブリック スイッチを常に選択してください。



ヒント

該当する表示コマンド(たとえば、**show interface** または **show flogi database**)を使用して、必要な値を 16 進表記で取得します。



ヒント

show wwn switch コマンドを使用して sWWN を取得します。sWWN を指定しない場合、ソフトウェアは自動的にローカル sWWN を使用します。



ヒント

[Physical Attributes] ペインで [Switches] を開き、sWWN を検索します。sWWN を指定しない場合、ソフトウェアは自動的にローカル sWWN を使用します。



(注)

インターフェイスベースゾーン分割は、Cisco MDS 9000 ファミリー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。

設定されているゾーンの数が、すべての VSAN で許可されるゾーンの最大数を超えると、次のメッセージが表示されます。

```
switch(config)# zone name temp_zone1 vsan 300
cannot create the zone; maximum possible number of zones is already configured
```



(注)

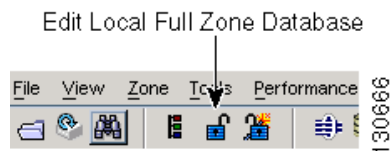
ゾーン、ゾーンメンバー、およびゾーンセットの数の設定時の制限については、『Cisco MDS NX-OS Configuration Limits』を参照してください。

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 4-8 を参照)。

図 4-8 [Zone] アイコン

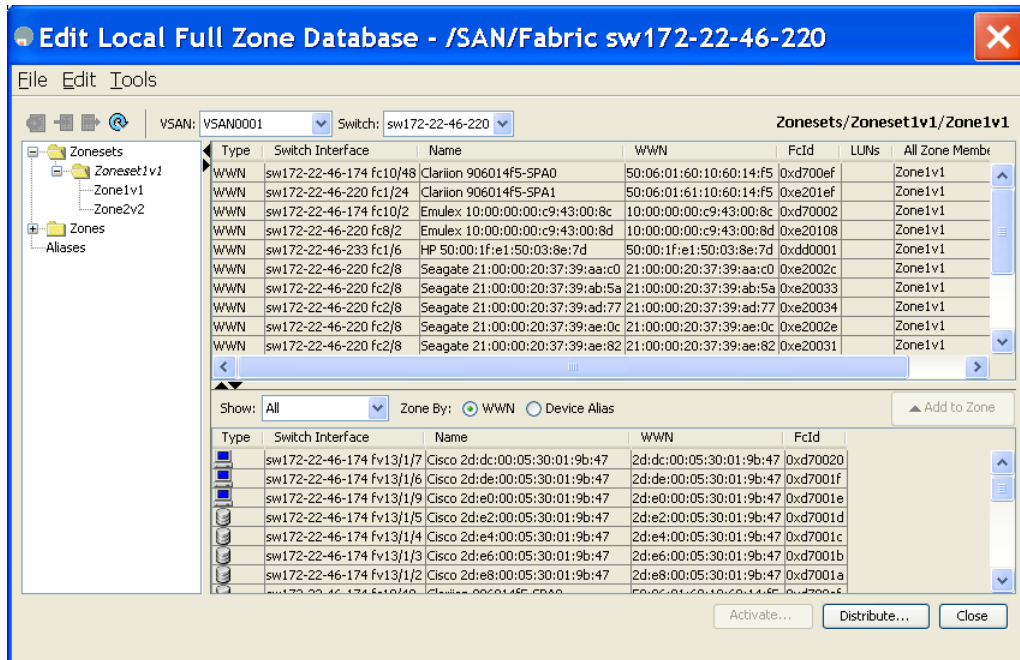


[Select VSAN] ダイアログボックスが表示されます。

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。

[Edit Local Full Zone Database] ダイアログボックスが表示されます(図 4-9 を参照)。

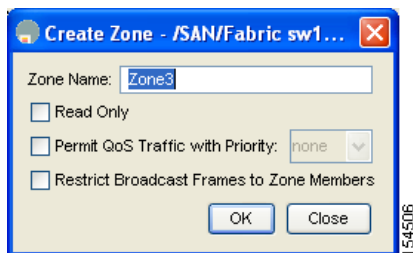
図 4-9 [Edit Local Full Zone Database] ダイアログボックス



ゾーンメンバーシップ情報を表示する場合は、[All Zone Membership(s)] カラムを右クリックして、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 4-10 を参照)。

図 4-10 [Create Zone] ダイアログボックス

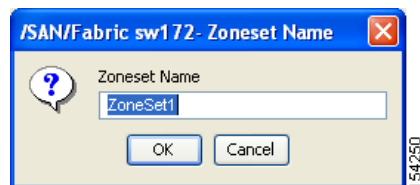


- ステップ 4** ゾーン名を入力します。
- ステップ 5** 次のチェックボックスのうち 1 つをオンにします。
- [Read Only]: このゾーンでは読み込みを許可しますが、書き込みは拒否します。
 - [Permit QoS traffic with Priority]: ドロップダウンメニューでプライオリティを設定します。
 - [Restrict Broadcast frames to Zone Members]
- ステップ 6** [OK] をクリックしてゾーンを作成します。
このゾーンを既存のゾーンセットに移動する場合は、ステップ 8 へスキップします。

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 4-11 を参照)。

図 4-11 [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。

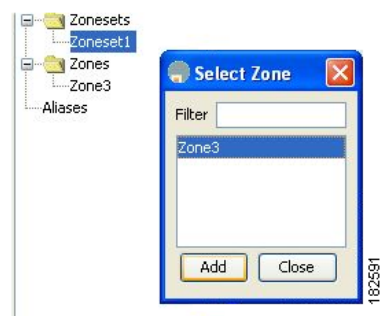


(注) シンボル(\$、-、^、_)のうちの1つまたはすべての英数字がサポートされています。interop モード 2 と 3 では、シンボル(_)またはすべての英数字がサポートされています。

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、または [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 4-12 を参照)。

図 4-12 [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。

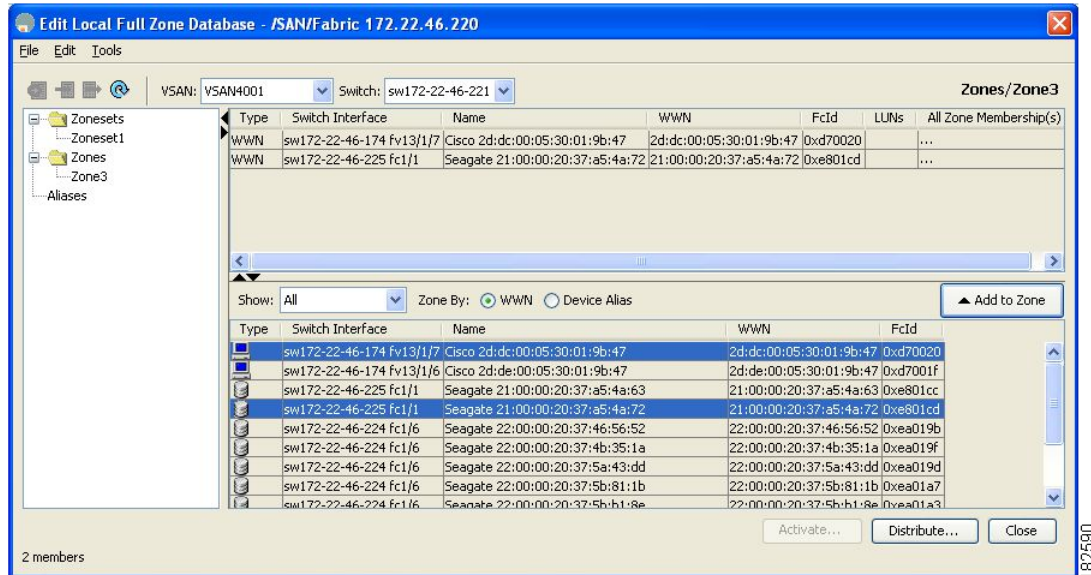
ステップ 1 [Zone] > [Edit Local Full Zone Database] を選択します。

[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。

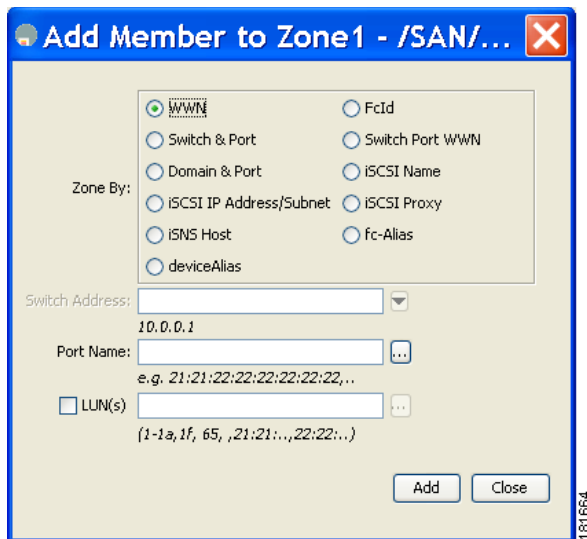
図 4-13 [Edit Local Full Zone Database] ダイアログボックス



ステップ 3 [Fabric] ペイン (図 4-13 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。

[Add Member to Zone] ダイアログボックスが表示されます (図 4-14 を参照)。

図 4-14 [Add Member to Zone] ダイアログボックス



(注) [Device Alias] オプション 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」セクション (5-8 ページ) を参照してください。

- ステップ 4** ブラウズ ボタンをクリックしてポート名を選択するか、または [LUN(s)] チェックボックスをオンにしてブラウズ ボタンをクリックし、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、オペレーティング システム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 つの異なるオペレーティング システムから選択できます。

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 4-8 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 4-8 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

ゾーンにより、アクセス コントロールを指定できます。ゾーン セットは、ファブリックでアクセス コントロールを実行するためのゾーンの分類です。

ここではゾーン セットについて説明します。具体的な内容は次のとおりです。

- [デフォルト ゾーンのアクセス権限の設定\(4-25 ページ\)](#)
- [FC エイリアスの作成の概要\(4-26 ページ\)](#)

- FC エイリアスの作成(4-26 ページ)
- エイリアスへのメンバーの追加(4-28 ページ)
- ゾーンメンバーの pWWN ベースメンバーへの変換(4-29 ページ)
- ゾーンセットの作成とメンバーの追加(4-30 ページ)
- ゾーン分割の実行(4-32 ページ)

ゾーンセットはメンバーゾーンおよび VSAN 名で設定します(設定された VSAN にゾーンセットが存在する場合)。

ゾーンセット配信: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。

ゾーンセットの複製:ゾーンセットのコピーを作成し、元のゾーンセットを変更することなく編集できます。アクティブゾーンセットを `bootflash:` ディレクトリ、`volatile:` ディレクトリ、または `slot0` から次のいずれかのエリアにコピーすることができます。

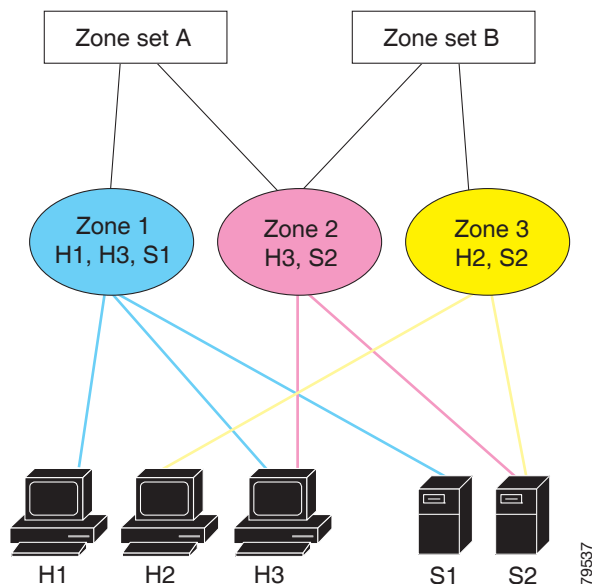
- フルゾーンセット
- リモートロケーション(FTP、SCP、SFTP、または TFTP を使用)

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。

ゾーンセットの作成

図 4-15 では、それぞれ独自のメンバーシップ階層とゾーンメンバーを持つ別個の 2 つのセットが作成されています。

図 4-15 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)をアクティブにできます。



ヒント

ゾーンセットはメンバゾーンおよび VSAN 名で設定します(設定された VSAN にゾーンセットが存在する場合)。

ゾーンセットの非アクティブ化

ゾーンセットに加えた変更は、それがアクティブ化されるまで、フルゾーンセットには反映されません。

既存のゾーンセットをアクティブまたは非アクティブにするには、次の手順を実行します。

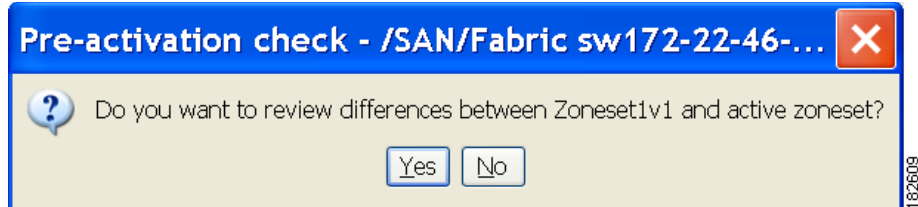
	コマンド	目的
ステップ 1	switch# config terminal switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# zoneset activate name Zoneset1 vsan 3	<p>指定されたゾーンセットをアクティブにします。</p> <p>フルゾーンセット配信が VSAN で設定されている場合、ゾーンセットのアクティブ化により、フルゾーン分割データベースがファブリック内の他のスイッチに配信されます。</p> <p>VSAN で拡張ゾーン分割が設定されている場合、ゾーンセットのアクティブ化は、zone commit vsan vsan-id コマンドが有効になるまで保留されます。show zone pending-diff vsan vsan-id は、保留中の変更を表示します。</p> <p>(注) ゾーンセットをアクティブにするときに、zoneset overwrite-control vsan id コマンドが有効であり、ゾーンセット名が現在のアクティブなゾーンセットとは異なる場合、アクティブ化は失敗しエラーメッセージが表示されます。詳細については、アクティブなゾーンセットの上書き制御を参照してください。</p> <pre>switch(config)# zoneset activate name Zoneset2 vsan 3 WARNING: You are trying to activate zoneset2, which is different from current active zoneset1.Do you want to continue? (y/n) [n] y</pre>
	switch(config)# no zoneset activate name Zoneset1 vsan 3	指定されたゾーンセットを非アクティブにします。

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。

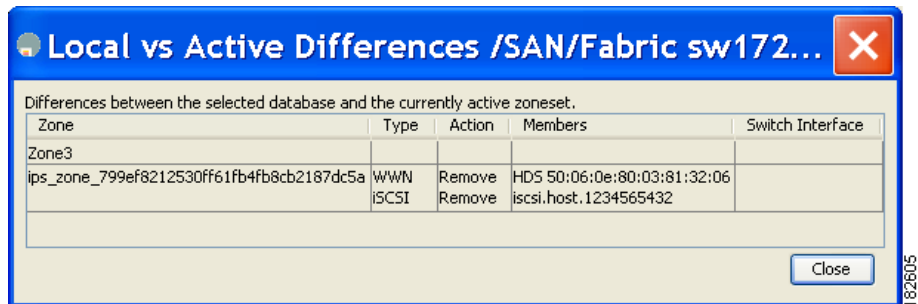
- ステップ 3** [Activate] をクリックして、ゾーンセットをアクティブにします。
[Pre-Activation Check] ダイアログボックスが表示されます(図 4-16 を参照)。

図 4-16 [Pre-Activation Check] ダイアログボックス



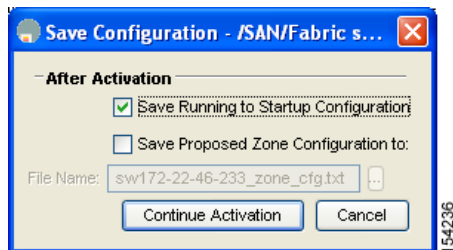
- ステップ 4** [Yes] をクリックして、相違を確認します。
[Local vs. Active Differences] ダイアログボックスが表示されます(図 4-17 を参照)。

図 4-17 [Local vs. Active Differences] ダイアログボックス



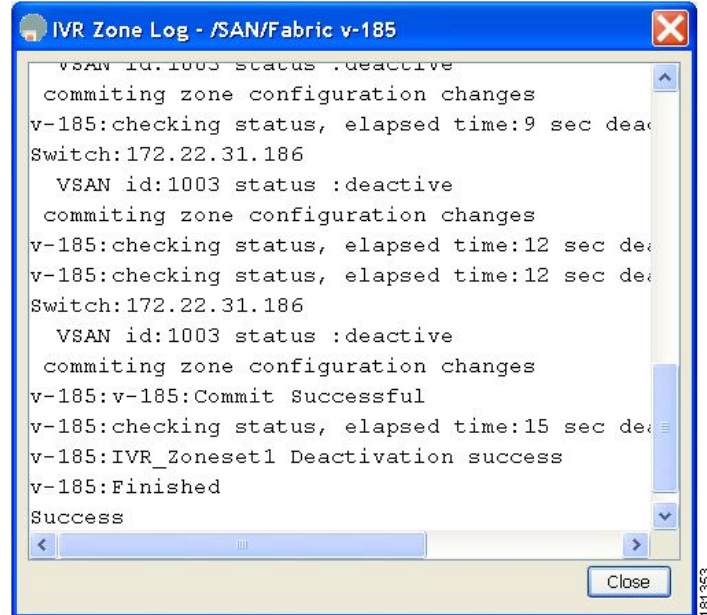
- ステップ 5** [Close] をクリックして、ダイアログボックスを閉じます。
[Save Configuration] ダイアログボックスが表示されます(図 4-18 を参照)。

図 4-18 [Save Configuration] ダイアログボックス



- ステップ 6** [Save Running to Startup Configuration] チェックボックスをオンにして、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廃棄するには、[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 4-19 を参照)。

図 4-19 [Zone Log] ダイアログボックス



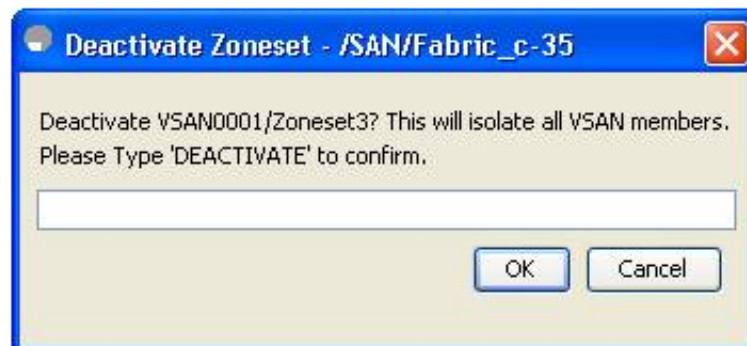
ゾーンセットの非アクティブ化

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] を選択します。

[Deactivate Zoneset] ダイアログボックスが表示されます(図 4-20 を参照)。

図 4-20 [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 4-21 を参照)。

図 4-21 [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 メンバーシップ情報の表示

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 メンバー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](#)」セクション(4-59 ページ)を参照してください。



ヒント

アクティブなゾーンセットを保存するために、**実行コンフィギュレーションをスタートアップコンフィギュレーションにコピー** `copy running-config startup-config` コマンドを実行する必要はありません。ただし、フルゾーンセットを明示的に保存するには、**実行コンフィギュレーションをスタートアップコンフィギュレーションにコピー** `copy running-config startup-config` コマンドを実行する必要があります。ファブリックに複数のスイッチが含まれている場合は、**copy running-config startup-config fabric** コマンドを実行する必要があります。キーワード **fabric** を指定すると、**copy running-config startup-config** コマンドがファブリック内のすべてのスイッチで実行され、フルゾーン情報がファブリック内のすべてのスイッチのスタートアップコンフィギュレーションに保存されます。これは、スイッチのリロードおよび電源再投入時に重要です。

アクティブなゾーンセットの上書き制御

新しいゾーンセットをアクティブにするときに、ユーザがゾーンセット名を誤って入力した場合、または入力した名前がすでにスイッチに存在している場合は、誤ったゾーンセットがアクティブになり、トラフィックが失われます。誤ったゾーンセットがアクティブになることを防ぐため、**zoneset overwrite-control vsan id** コマンドが導入されました。

	コマンド	目的
ステップ 1	<code>switch# config terminal</code> <code>switch(config)#</code>	コンフィギュレーションモードに入ります。
ステップ 2	<code>switch(config)# zoneset overwrite-control vsan 3</code>	指定した VSAN で上書き制御を有効にします。 <code>switch(config)# zoneset overwrite-control vsan 1</code> WARNING: This will enable Activation Overwrite control.Do you want to continue? (y/n) [n]
ステップ 3	<code>switch(config)# show zone status vsan 3</code>	VSAN のステータス(上書き制御が有効であるかどうか)を表示します。



(注)

zoneset overwrite-control vsan id コマンドが有効な場合でも、ユーザは **zoneset activate name zoneset name vsan vsanid force** コマンドを使用してこれを上書きし、新しいゾーンセットをアクティブにできます。

例 4-1 ゾーンステータスの表示

```
switch(config)# show zone status vsan 3
VSAN: 2 default-zone: deny distribute: full Interop: default
mode: enhanced merge-control: allow
session: none
hard-zoning: enabled broadcast: unsupported
smart-zoning: disabled
rscn-format: fabric-address
activation overwrite control: enabled
```

■ ゾーンセット

```

Default zone:
  qos: none broadcast: unsupported ronly: unsupported
Full Zoning Database :
  DB size: 348 bytes
  Zonesets:2 Zones:2 Aliases: 0 Attribute-groups: 1
Active Zoning Database :
  DB size: 68 bytes
  Name: hellset Zonesets:1 Zones:1
Current Total Zone DB Usage: 416 / 2097152 bytes (0 % used)
Pending (Session) DB size:
  Full DB Copy size: 0 bytes
  Active DB Copy size: 0 bytes
SFC size: 0 / 2097152 bytes (0 % used)
Status: Commit completed at 15:19:49 UTC Jun 11 2015

```

デフォルト ゾーン

ファブリックの各メンバは(デバイスが Nx ポートに接続されている状態)、任意のゾーンに所属できます。どのアクティブ ゾーンにも所属しないメンバは、デフォルト ゾーンの一部と見なされます。したがって、ファブリックにアクティブなゾーン セットがない場合、すべてのデバイスがデフォルト ゾーンに所属するものと見なされます。メンバは複数のゾーンに所属できますが、デフォルト ゾーンに含まれるメンバは、その他のゾーンに所属できません。接続されたポートが起動すると、スイッチは、ポートがデフォルト ゾーンのメンバか判別します。



(注) 設定されたゾーンとは異なり、デフォルト ゾーン情報は、ファブリックの他のスイッチに配信されません。

トラフィックをデフォルト ゾーンのメンバ間で許可または拒否できます。この情報は、すべてのスイッチには配信されません。各スイッチで設定する必要があります。



(注) スイッチが初めて初期化されたとき、ゾーンは設定されておらず、すべてのメンバがデフォルトゾーンに所属するものと見なされます。メンバ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値は変更できます。

デフォルト ポリシーが **permit** として設定されている場合、またはゾーン セットがアクティブの場合、デフォルト ゾーン メンバーが明示的に表示されます。デフォルト ポリシーが **deny** として設定されている場合は、**show zoneset active** コマンドを実行するアクティブ ゾーン セットを表示するときに、このゾーンのメンバーは明示的に一覧表示されません。



(注) 現在のデフォルト ゾーン分割ポリシーは **deny** です。非表示のアクティブ ゾーン セットは MDS の **d_default_cfg** です。2 つのスイッチのデフォルト ゾーン分割ポリシーに不一致がある場合(一方で **permit**、もう一方で **deny**)、ゾーン マージが失敗します。2 つの Brocade スイッチでこの動作は変わりません。次のようなエラー メッセージが表示されます。

次のようなエラーメッセージが表示されます。

Switch1 syslog:

```
switch(config-if)# 2014 Sep 2 06:33:21 hac15 %ZONE-2-ZS_MERGE_FAILED: %$VSAN 1%$ Zone
merge failure, isolating interface fc2/10 received reason: Default zoning policy conflict.Received rjt
from adjacent switch:[reason:0]
```

Switch2 syslog:

```
switch(config-if)# 2014 Sep 2 12:13:17 hac16 %ZONE-2-ZS_MERGE_FAILED: %$VSAN 1%$ Zone
merge failure, isolating interface fc3/10 reason: Default zoning policy conflict.: [reason:0]
```

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 ツリーで [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認する場合は、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アクセス権限の設定

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には、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <code>config t</code>	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# <code>zone default-zone permit vsan 1</code>	デフォルトゾーンメンバへのトラフィックフローを許可します。
	switch(config)# <code>no zone default-zone permit vsan 1</code>	デフォルトゾーンメンバへのトラフィックフローを拒否(デフォルト)します。

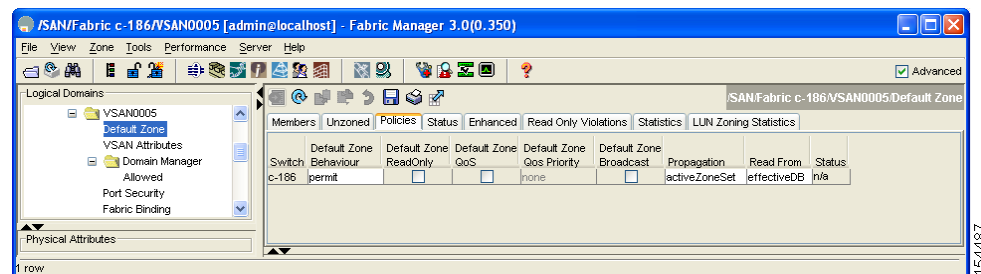
Fabric Manager を使用してデフォルトゾーン内のメンバーに対するトラフィックを許可または拒否する手順は、次のとおりです。

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 4-22 を参照)。

図 4-22 デフォルトのゾーンポリシー



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 Behavior] フィールドの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:0xhhhhhh 形式の N ポート ID(0xce00d1 など)
- ドメイン ID:ドメイン ID は 1 ~ 239 の整数です。このメンバーシップ設定を完了するには、他社製スイッチの必須ポート番号が必要です。
- 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 ゾーン分割は、スイッチ インターフェイスがゾーンを設定するのに使用される点でポートベース ゾーン分割と似ています。スイッチ インターフェイスをローカル スイッチとリモート スイッチの両方でゾーン メンバとして指定できます。リモート スイッチを指定するには、特定の VSAN 内のリモート Switch WWN (sWWN) またはドメイン ID を入力します。



ヒント

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

エイリアスを作成するには、次の手順を実行します。

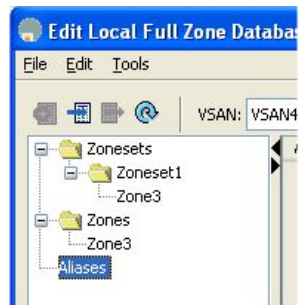
	コマンド	目的
ステップ 1	switch# <code>config t</code>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <code>fcalias name AliasSample vsan 3</code> switch(config-fcalias)#	エイリアス名 (AliasSample) を設定します。

	コマンド	目的
ステップ 3	<pre>switch(config-fcalias)# member type value pWWN の例: switch(config-fcalias)# member pwwn 10:00:00:23:45:67:89:ab fWWN の例: switch(config-fcalias)# member fwwn 10:01:10:01:10:ab:cd:ef FC ID の例: switch(config-fcalias)# member fcid 0x222222 ドメイン ID の例: switch(config-fcalias)# member domain-id 2 portnumber 23 IPv4 アドレスの例: switch(config-fcalias)# member ip-address 10.15.0.0 255.255.0.0 IPv6 アドレスの例: switch(config-fcalias)# member ipv6-address 2001::db8:800:200c:417a/64 ローカル sWWN インターフェイスの例: switch(config-fcalias)# member interface fc 2/1 リモート sWWN インターフェイスの例: switch(config-fcalias)# member interface fc2/1 swwn 20:00:00:05:30:00:4a:de ドメイン ID インターフェイスの例: switch(config-fcalias)# member interface fc2/1 domain-id 25</pre>	<p>指定されたタイプ (pWWN、ファブリック pWWN、FC ID、FC エイリアス、ドメイン ID、IPv4 アドレス、IPv6 アドレス、またはインターフェイス) および値に基づいて、指定された FC エイリアス (AliasSample) にメンバーを設定します。</p>
ステップ 4	(注) 複数のメンバを複数の行で指定できます。	

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。

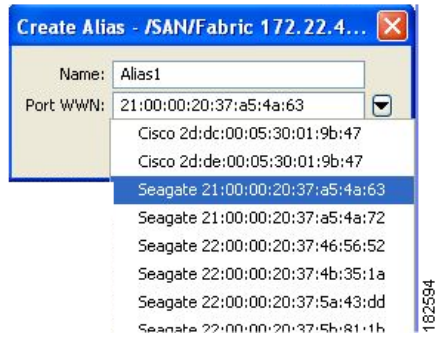
- ステップ 1 [Zone] > [Edit Local Full Zone Database] を選択します。
[Select VSAN] ダイアログボックスが表示されます。
- ステップ 2 VSAN を選択して、[OK] をクリックします。
選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます。
- ステップ 3 左下のペインで、[Aliases] をクリックします(図 4-23 を参照)。右側のペインに既存のエイリアスが表示されます。

図 4-23 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 4-24 を参照)。

図 4-24 [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。

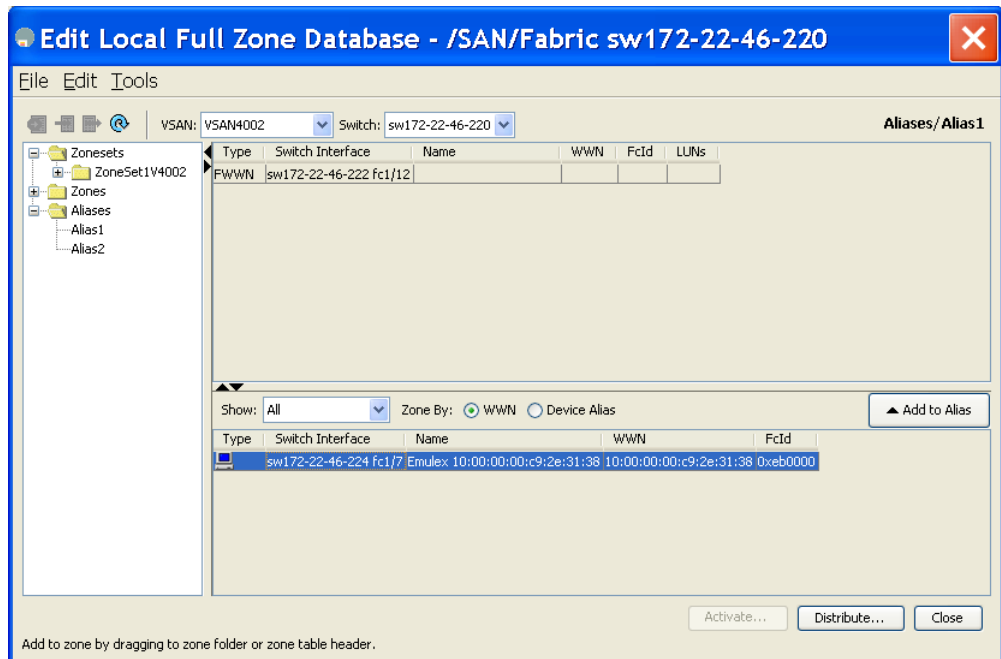
ステップ 1 [Zone] > [Edit Local Full Zone Database] を選択します。

[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。

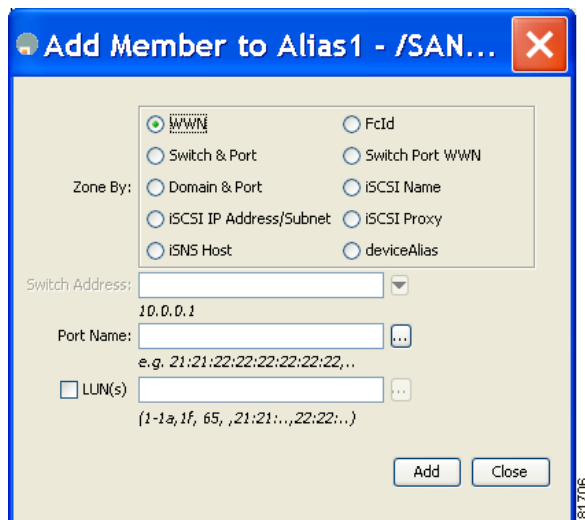
選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます (図 4-25 を参照)。

図 4-25 [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 4-25 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。
[Add Member to Alias] ダイアログボックスが表示されます(図 4-26 を参照)。

図 4-26 [Add Member to Alias] ダイアログボックス



(注) [Device Alias] オプション ボタンは、デバイスのエイリアスが enhanced モードのときだけに表示されます。詳細については、「デバイス エイリアスの作成」セクション(5-8 ページ)を参照してください。

- ステップ 4** ブラウズ ボタンをクリックしてポート名を選択するか、または [LUN] チェックボックスをオンにしてブラウズ ボタンをクリックし、[LUNs] 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 ベースのメンバーシップから pWWN ベースのメンバー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 ベースのメンバーシップに変更します。

ゾーンセットの作成とメンバゾーンの追加

複数のゾーンを含むゾーンセットを作成するには、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>switch# config t</code>	コンフィギュレーションモードに入ります。
ステップ 2	<code>switch(config)# zoneset name Zoneset1 vsan 3</code> <code>switch(config-zoneset)#</code>	Zoneset1 というゾーンセットを設定します。 ヒント ゾーンセットをアクティブにするには、まずゾーンとゾーンセットを1つ作成する必要があります。
ステップ 3	<code>switch(config-zoneset)# member Zone1</code>	指定されたゾーンセット (Zoneset1) に Zone1 をメンバーとして追加します。 ヒント 指定されたゾーン名が事前に設定されていない場合、このコマンドを実行すると「zone not present」エラーメッセージが返されます。
ステップ 4	<code>switch(config-zoneset)# zone name InlineZone1</code> <code>switch(config-zoneset-zone)#</code>	指定されたゾーンセット (Zoneset1) にゾーン (InlineZone1) を追加します。 ヒント ゾーンセットプロンプトからゾーンを作成する必要がある場合は、このステップを実行します。
ステップ 5	<code>switch(config-zoneset-zone)# member fcid 0x111112</code> <code>switch(config-zoneset-zone)#</code>	新しいゾーン (InlineZone1) に新しいメンバー (FC ID 0x111112) を追加します。 ヒント ゾーンセットプロンプトからゾーンにメンバーを追加する必要がある場合は、このステップを実行します。



(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

アクティブなゾーンセットを保存するために、**実行コンフィギュレーションをスタートアップコンフィギュレーションにコピー** `copy running-config startup-config` コマンドを実行する必要はありません。ただし、フルゾーンセットを明示的に保存するには、実行コンフィギュレーションをスタートアップコンフィギュレーションにコピー `copy running-config startup-config` コマンドを実行する必要があります。ファブリックに複数のスイッチが含まれている場合は、**copy running-config startup-config fabric** コマンドを実行する必要があります。キーワード **fabric** を指定すると、**copy running-config startup-config** コマンドがファブリック内のすべてのスイッチで実行され、フルゾーン情報がファブリック内のすべてのスイッチのスタートアップコンフィギュレーションに保存されます。これは、スイッチのリロードおよび電源再投入時に重要です。



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(「[ゾーンおよびゾーンセットの分析](#)」セクション(4-92 ページ)を参照)。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 が有効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](#)」セクション(4-15 ページ)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 がスイッチ上で有効になり、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有効にする前に、これらのモードについて十分に理解してください。デバイスエイリアスモードの詳細と要件については、[第5章「DDAS」](#)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 4-8 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 4-8 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

ゾーン分割は、ソフトとハードの2つの方法で実行できます。各エンド デバイス(N ポートまたは NL ポート)は、ネーム サーバにクエリーを送信することでファブリックの他のデバイスを検出します。デバイスがネーム サーバにログインすると、ネーム サーバはクエリー元デバイスがアクセスできる他のデバイスのリストを返します。Nx ポートがゾーンの外部にあるその他のデバイスの FCID を認識しない場合、そのデバイスにアクセスできません。

ソフトゾーン分割では、ゾーン分割制限がネーム サーバとエンド デバイス間の対話時にだけ適用されます。エンド デバイスが何らかの方法でゾーン外部のデバイスの FCID を認識できる場合、そのデバイスにアクセスできます。

ハードゾーン分割は、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。

ゾーンセットの配信

フルゾーンセットを配信するには、EXEC モード レベルでのワнтаイム配信またはコンフィギュレーション モード レベルでのフルゾーンセット配信のいずれかの方法を使用します。

フルゾーンセットを配信するには、ワнтаイム配信またはフルゾーンセット配信の2つの方法のうち、いずれかを使用します。

表 4-1 に、これらの配信方法の相違を示します。

表 4-1 ゾーンセット配信 `zoneset distribution` コマンドの相違点

一時配信 <code>zoneset distribute vsan</code> コマンド (EXEC モード)	フルゾーンセット配信 <code>zoneset distribute full vsan</code> コマンド (コンフィギュレーション モード)
フルゾーンセットはすぐに配信されます。	フルゾーンセットはすぐには配信されません。
アクティブ化、非アクティブ化、またはマージ時には、アクティブゾーンセットと同時にフルゾーンセット情報を配信しません。	アクティブ化、非アクティブ化、またはマージ時には、アクティブゾーンセットと同時にフルゾーンセット情報を必ず配信してください。



ヒント

アクティブなゾーンセットを保存するために、**実行コンフィギュレーションをスタートアップコンフィギュレーションにコピー** `copy running-config startup-config` コマンドを実行する必要はありません。ただし、フルゾーンセットを明示的に保存するには、実行コンフィギュレーションをスタートアップコンフィギュレーションにコピー `copy running-config startup-config` コマンドを実行する必要があります。ファブリックに複数のスイッチが含まれている場合は、**copy running-config startup-config fabric** コマンドを実行する必要があります。キーワード **fabric** を指定すると、`copy running-config startup-config` コマンドがファブリック内のすべてのスイッチで実行され、フルゾーン情報がファブリック内のすべてのスイッチのスタートアップコンフィギュレーションに保存されます。これは、スイッチのリロードおよび電源再投入時に重要です。

ここではゾーンセットの配信について説明します。具体的な内容は次のとおりです。

- [フルゾーンセットの配信の有効化 \(4-33 ページ\)](#)
- [ワнтаイム配信の有効化 \(4-34 ページ\)](#)
- [リンク分離からの回復の概要 \(4-35 ページ\)](#)
- [ゾーンセットのインポートおよびエクスポート \(4-36 ページ\)](#)

フルゾーンセットの配信の有効化

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、隣接スイッチへの結合要求の送信時、またはゾーンセットのアクティブ化の際に行われます。

■ ゾーンセットの配信

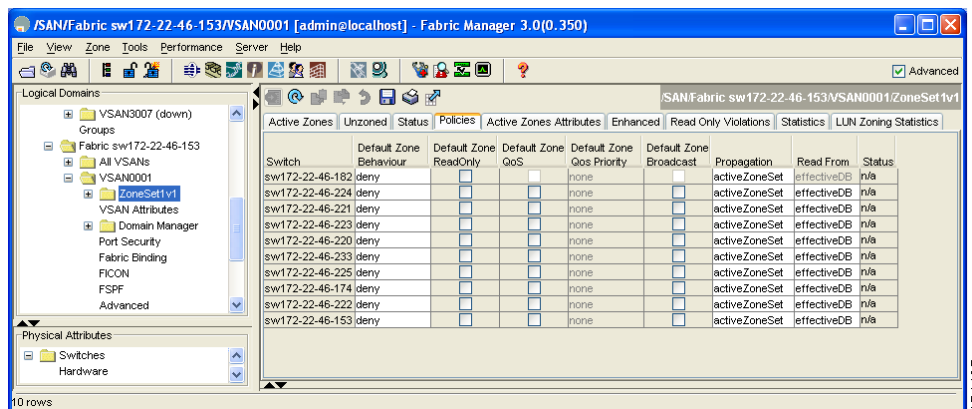
VSAN ベースですべてのスイッチへのフルゾーンセットおよびアクティブゾーンセットの配信を有効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# zoneset distribute full vsan 33	アクティブゾーンセットとともにフルゾーンセットの送信を有効にします。

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。
ゾーンに設定されたポリシーが表示されます(図 4-27 を参照)。

図 4-27 ゾーンに設定されたポリシー



- ステップ 3** [Propagation] カラムのドロップダウンメニューで [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。

ワンタイム配信の有効化

この配信を実行するには、EXEC モードで **zoneset distribute vsan vsan-id** コマンドを使用します。

```
switch# zoneset distribute vsan 2
Zoneset distribution initiated.check zone status
```

ファブリック全体に、非アクティブで未変更のゾーンセットを一度だけ配信します。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] 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。

この手順コマンドでは、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、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保存 `copy running-config startup-config` コマンドを実行する必要があります。



(注) `zoneset distribute vsan vsan-id` コマンドフルゾーンセットのワンタイム配信は、**interop 2** モードと **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。

ゾーンセット一時配信要求のステータスを確認するには、`show zone status vsan vsan-id` コマンドを使用します。

```
switch# show zone status vsan 9
VSAN: 9 default-zone: deny distribute: full Interop: default
mode: enhanced merge-control: allow
session: none
hard-zoning: enabled broadcast: enabled
smart-zoning: disabled
rscn-format: fabric-address
activation overwrite control:disabled
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 2002584 bytes
Zonesets:4 Zones:7004 Aliases: 0 Attribute-groups: 1
Active Zoning Database :
DB size: 94340 bytes
Name: zoneset-hac13-200 Zonesets:1 Zones:176
Current Total Zone DB Usage: 2096924 / 2097152 bytes (99 % used)
Pending (Session) DB size:
Full DB Copy size: 0 bytes
Active DB Copy size: 0 bytes
SFC size: 0 / 2097152 bytes (0 % used)
Status: Activation completed at 17:28:04 UTC Jun 16 2014
```

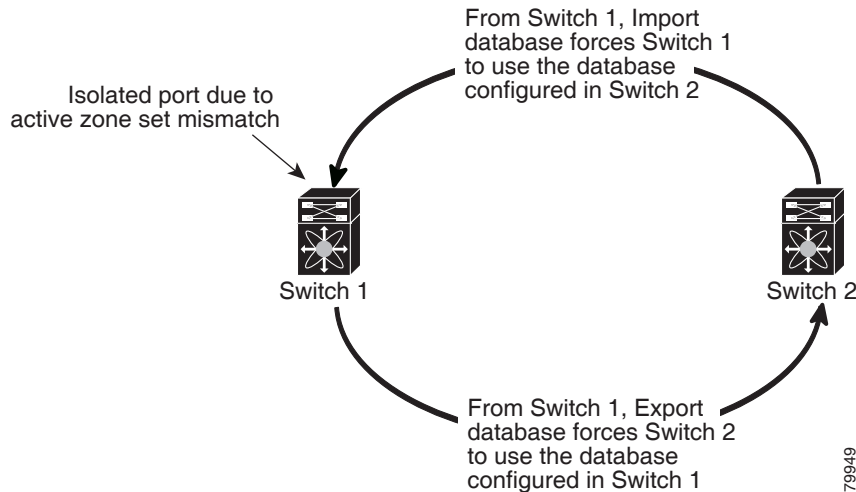
リンク分離からの回復の概要

ファブリックの2つのスイッチがTEポートまたはEポートを使用してマージされる場合、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 4-28 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 4-28 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

ゾーンセット情報を隣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には、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>switch# zoneset import interface fc1/3 vsan 2</code>	VSAN 2 の fc 1/3 インターフェイスを介して接続された隣接スイッチからゾーンセットをインポートします。
	<code>switch# zoneset import interface fc1/3 vsan 2-5</code>	VSAN 範囲 2 ~ 5 の fc 1/3 インターフェイスを介して接続された隣接スイッチからゾーンセットをインポートします。
ステップ 2	<code>switch# zoneset export vsan 5</code>	VSAN 5 を介して接続された隣接スイッチにゾーンセットをエクスポートします。
	<code>switch# zoneset export vsan 5-8</code>	VSAN 5 ~ 8 の範囲を介して接続された隣接スイッチにゾーンセットをエクスポートします。

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。
 [Zone Merge Failure Recovery] ダイアログボックスが表示されます(図 4-29 を参照)。

図 4-29 [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] オプション 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** コマンドは、単一のスイッチから実行します。インポートとエクスポートをそれぞれ別のスイッチから行うと、再びリンクが分離する可能性があります。

ゾーンセットの複製

コピーを作成し、既存のアクティブ ゾーン セットを変更することなく編集できます。アクティブ ゾーン セットを `bootflash:` ディレクトリ、`volatile:` ディレクトリ、または `slot0` から次のいずれかのエリアにコピー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。

この項では、次のトピックについて取り上げます。

- ゾーンセットのコピー(4-38 ページ)
- ゾーンのバックアップおよび復元の概要(4-39 ページ)

■ ゾーンセットの複製

- ゾーンのバックアップ(4-39 ページ)
- ゾーン、ゾーンセット、およびエイリアスの名前の変更(4-42 ページ)
- 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(4-43 ページ)
- MDS 以外のデータベースの移行(4-44 ページ)
- ゾーン サーバデータベースのクリア(4-45 ページ)

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、編集可能な新しいゾーンセットを作成できます。

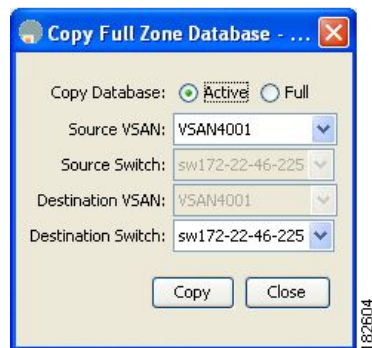
ゾーンセットのコピーを作成するには、次の手順を実行します。

	コマンド	目的
ステップ 1	<pre>switch# zone copy active-zoneset full-zoneset vsan 2 Please enter yes to proceed.(y/n) [n]? ?</pre>	VSAN 2 のアクティブ ゾーンセットのコピーをフルゾーンセットに作成します。
	<pre>switch# zone copy vsan 3 active-zoneset scp://guest@myserver/tmp/active_zoneset.txt</pre>	SCP を使用して、VSAN 3 のアクティブゾーンをリモート ロケーションにコピーします。

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** [Edit] > [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 4-30 を参照)。

図 4-30 [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] オプション 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 リストでコピー先の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) 機能が有効になっていて、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

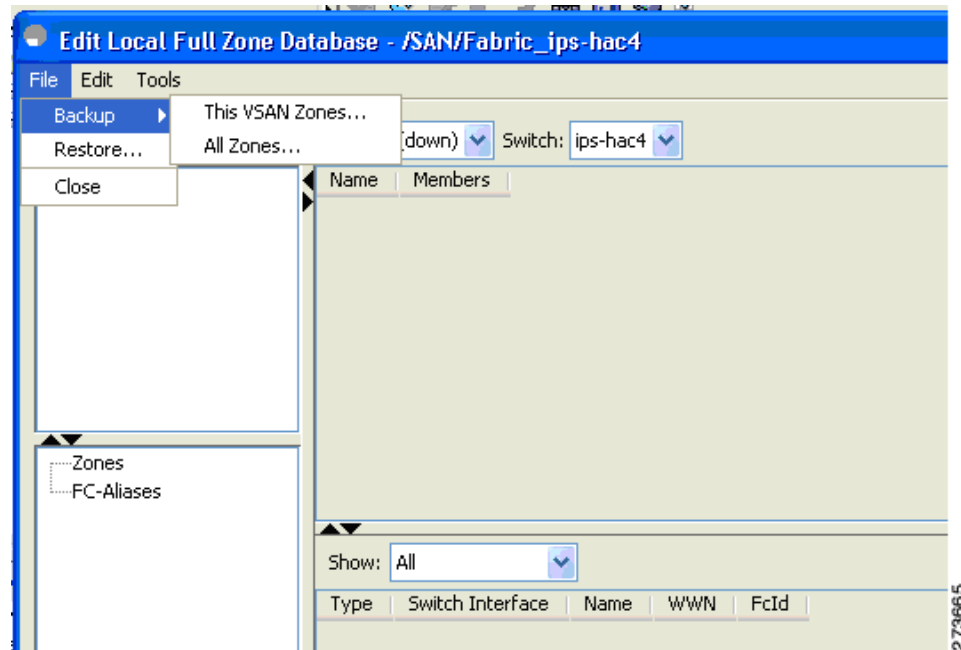
Fabric Manager を使用してフル ゾーン設定をバックアップする手順は、次のとおりです。

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。

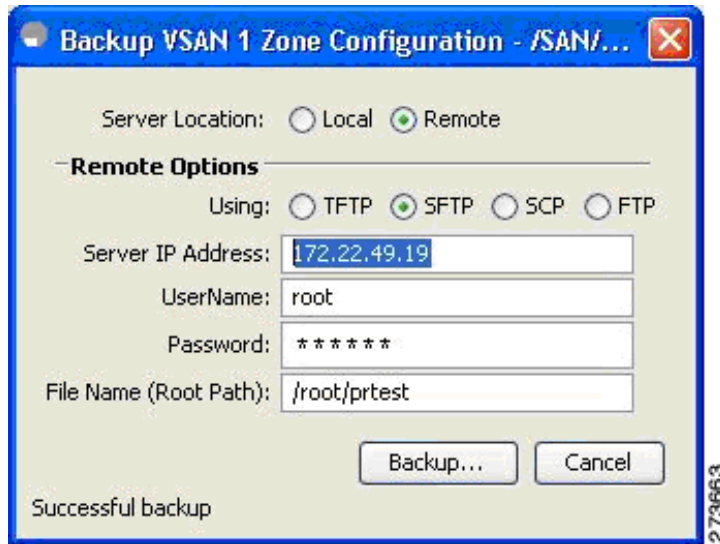
選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます(図 4-31 を参照)。

図 4-31 [Edit Local Full Zone Database]



- 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。
- [Backup Zone Configuration] ダイアログボックスが表示されます(図 4-32 を参照)。

図 4-32 [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。

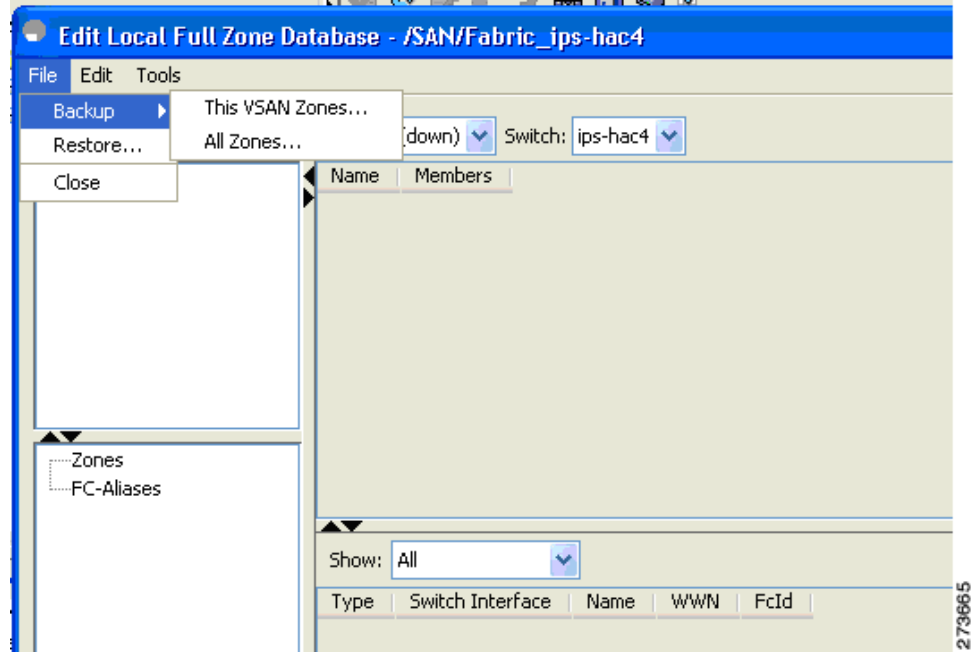
- ステップ 4** 次の [Remote Options] 情報を指定して、データをリモート サーバにバックアップします。
- a. [Using]: プロトコルを選択します。
 - b. [Server IP Address]: サーバの IP アドレスを入力します。
 - c. [UserName]: ユーザの名前を入力します。
 - d. [Password]: ユーザのパスワードを入力します。
 - e. [File Name(Root Path)]: パスおよびファイル名を入力します。
- ステップ 5** [Backup] をクリックするか、[Cancel] をクリックしてバック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 4-33 を参照)。

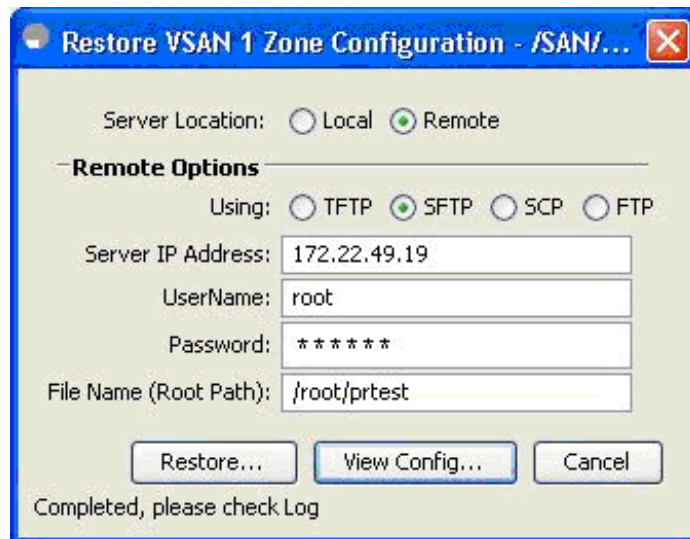
図 4-33 [Edit Local Full Zone Database]



ステップ 3 [File] > [Restore] を選択し、TFTP、SFTP、SCP、または FTP を使用して、保存済みのゾーン設定を復元します。

[Restore Zone Configuration] ダイアログボックスが表示されます(図 4-34 を参照)。

図 4-34 [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] の情報を指定して、リモート サーバからデータを復元します。

- 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。

■ ゾーンセットの複製

- 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 続行するには [Restore] をクリックします。復元を実行しないでダイアログボックスを閉じるには [Cancel] をクリックします。



(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。復元オプションは、Cisco Fabric Manager Release 4.1(3) 以降でのみサポートされています。

ゾーン、ゾーンセット、およびエイリアスの名前の変更

ゾーン、ゾーンセット、FC エイリアス、またはゾーン属性グループの名前を変更するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <code>config t</code>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <code>zoneset rename oldname newname vsan 2</code>	指定された VSAN のゾーンセット名を変更します。
	switch(config)# <code>zone rename oldname newname vsan 2</code>	指定された VSAN のゾーン名を変更します。
	switch(config)# <code>fcalias rename oldname newname vsan 2</code>	指定された VSAN の fcalias 名を変更します。
	switch(config)# <code>zone-attribute-group rename oldname newname vsan 2</code>	指定された VSAN のゾーン属性グループ名を変更します。
ステップ 3	switch(config)# <code>zoneset activate name newname vsan 2</code>	ゾーンセットをアクティブにし、アクティブゾーンセット内の新しいゾーン名に更新します。

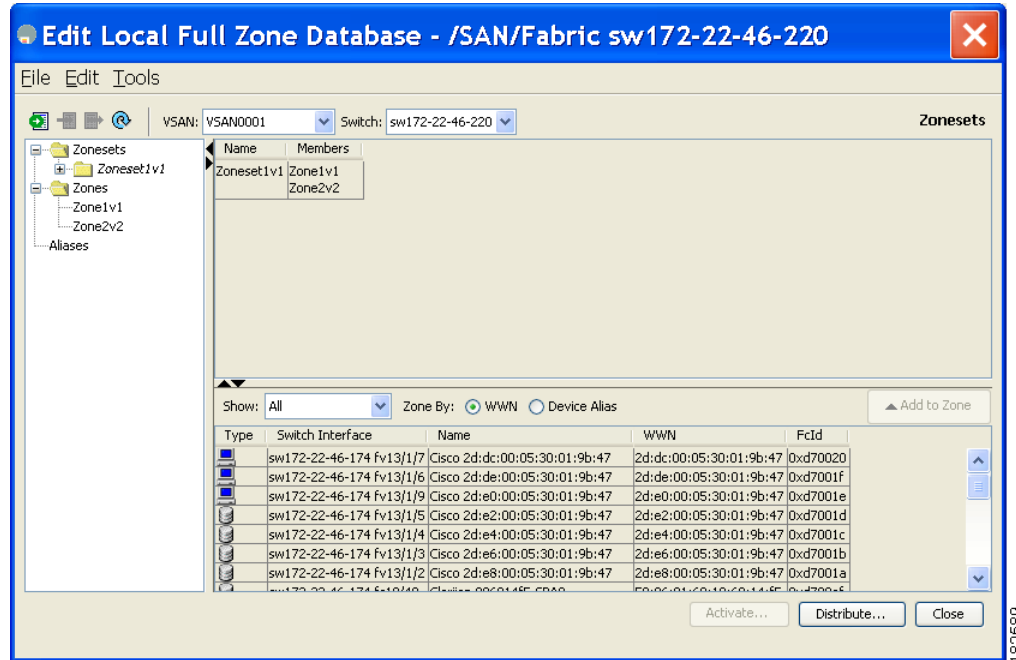
Fabric Manager を使用してゾーン、ゾーンセット、またはエイリアスの名前を変更する手順は、次のとおりです。

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 4-35 を参照)。

図 4-35 [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には、次の手順を実行します。

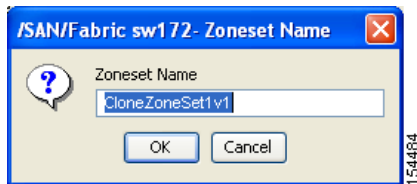
	コマンド	目的
ステップ 1	switch# <code>config t</code>	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# <code>zoneset clone oldname newname vsan 2</code>	指定された VSAN のゾーンセットをコピーします。
	switch(config)# <code>zone clone oldname newname vsan 2</code>	指定された VSAN 内のゾーンをコピーします。
	switch(config)# <code>fcalias clone oldname newname vsan 2</code>	指定された VSAN の FC エイリアス名をコピーします。

コマンド	目的
switch(config)# zone-attribute-group clone oldname newname vsan 2	指定された VSAN のゾーン属性グループをコピーします。
ステップ 3 switch(config)# zoneset activate name newname vsan 2	ゾーンセットをアクティブにし、アクティブゾーンセット内の新しいゾーン名に更新します。

ゾーン、ゾーンセット、FC エイリアス、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 4-36 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 4-36 [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 データベースをクリアするには、次のコマンドを使用します。

```
switch# clear zone database vsan 2
```

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 NX-OS Fabric Configuration Guide』を参照してください。



(注) **clear zone database** コマンドを実行した後に、明示的に **copy running-config startup-config** を実行して、スイッチの再起動時に確実に実行コンフィギュレーションが使用されるようにする必要があります。



(注) ゾーン セットをクリアすると、フルゾーン データベースだけが消去され、アクティブ ゾーン データベースは消去されません。



(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 \(4-46 ページ\)](#)
- [ゾーンベースのトラフィック プライオリティの設定 \(4-46 ページ\)](#)
- [デフォルト ゾーンの QoS プライオリティ属性の設定 \(4-48 ページ\)](#)
- [デフォルト ゾーン ポリシーの設定 \(4-49 ページ\)](#)
- [ブロードキャスト ゾーン分割の概要 \(4-49 ページ\)](#)
- [ブロードキャスト ゾーン分割の設定 \(4-50 ページ\)](#)
- [スマート ゾーン分割の概要](#)
- [VSAN でのスマート ゾーン分割の有効化](#)
- [ゾーン メンバーのデバイス タイプの設定](#)
- [ゾーン レベルでのスマート ゾーン分割の無効化](#)
- [LUN ゾーン分割の概要 \(4-55 ページ\)](#)
- [LUN ベースのゾーンの設定 \(4-56 ページ\)](#)
- [ストレージ サブシステムへの LUN の割り当て \(4-57 ページ\)](#)
- [読み取り専用ゾーンの概要 \(4-58 ページ\)](#)
- [読み取り専用ゾーンの設定 \(4-58 ページ\)](#)

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コントロール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 を有効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

ゾーンプライオリティを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>switch# config t</code>	コンフィギュレーションモードに入ります。
ステップ 2	<code>switch(config)# zone name QosZone vsan 2</code> <code>switch(config-zone)#</code>	エイリアス名 (QosZone) を設定し、ゾーンコンフィギュレーションサブモードを開始します。
ステップ 3	<code>switch(config-zone)# attribute-group qos</code> <code>priority high</code>	このゾーンを設定して、拡張モードでこのゾーンと一致する各フレームに高プライオリティの QoS トラフィックを割り当てます。
ステップ 4	<code>switch(config-zone)# attribute qos priority high</code>	このゾーンを設定して、このゾーンと一致する各フレームに高プライオリティの QoS トラフィックを割り当てます。
	<code>switch(config-zone)# attribute qos priority medium</code>	このゾーンを設定して、このゾーンと一致する各フレームに中プライオリティの QoS トラフィックを割り当てます。
	<code>switch(config-zone)# attribute qos priority low</code>	このゾーンを設定して、このゾーンと一致する各フレームに低プライオリティの QoS トラフィックを割り当てます。
ステップ 5	<code>switch(config-zone)# no attribute qos priority high</code>	このゾーンをデフォルトの低プライオリティを使用するように戻します。
	<code>switch(config-zone)# exit</code> <code>switch(config)#</code>	コンフィギュレーションモードに戻ります。

	コマンド	目的
ステップ 6	switch(config)# zoneset name QosZoneset vsan 2 switch(config-zoneset)#	指定された VSAN (vsan 2) のゾーンセット QosZoneset を設定し、ゾーンセット コンフィギュレーション サブモードを開始します。 ヒント ゾーンセットをアクティブにするには、まずゾーンとゾーンセットを1つ作成する必要があります。
ステップ 7	switch(config-zoneset)# member QosZone	指定されたゾーンセット (QosZoneset) に QosZone をメンバーとして追加します。 ヒント 指定されたゾーン名が事前に設定されていない場合、このコマンドを実行すると「zone not present」エラーメッセージが返されます。
ステップ 8	switch(config-zoneset)# exit switch(config)#	コンフィギュレーション モードに戻ります。
ステップ 9	switch(config)# zoneset activate name QosZoneset vsan 2	指定されたゾーンセットをアクティブにします。

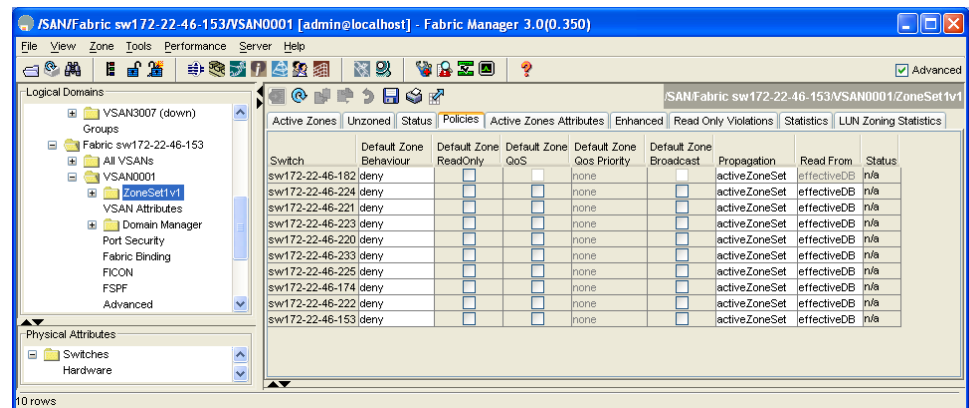
Fabric Manager を使用してゾーンプライオリティを設定する手順は、次のとおりです。

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 4-37を参照)。

図 4-37 [Information] ペインの [Zone Policies] ペイン



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。

デフォルト ゾーンの QoS プライオリティ属性を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# zone default-zone vsan 1 switch(config-default-zone)#	ゾーン コンフィギュレーション サブモードを開始します。
ステップ 3	switch(config-default-zone)# attribute qos priority high	これらのゾーンと一致するフレームに対して QoS プライオリティ属性を設定します。
	switch(config-default-zone)# no attribute qos priority high	デフォルト ゾーンの QoS プライオリティ属性を削除して、デフォルトの低プライオリティに戻します。

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 4-38 を参照)。

図 4-38 QoS プライオリティ属性

Name	Read Only	QoS	QoS Priority	Broadcast	Members
Zone1v4001	<input type="checkbox"/>	<input type="checkbox"/>	low	<input type="checkbox"/>	...
Zone2v4001	<input type="checkbox"/>	<input type="checkbox"/>	low	<input type="checkbox"/>	...
Zone4	<input type="checkbox"/>	<input type="checkbox"/>	low	<input type="checkbox"/>	...

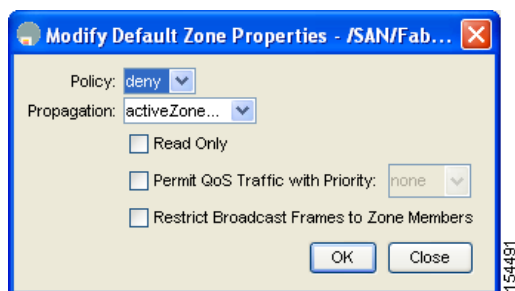
- ステップ 4 [Permit QoS Traffic with Priority] チェックボックスをオンにし、[Qos Priority] ドロップダウンメニューを [low]、[medium]、または [high] に設定します。
- ステップ 5 [OK] をクリックして変更を保存します。

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** [Edit] > [Edit Default Zone Attributes] を選択して、デフォルトゾーンの QoS プライオリティ属性を設定します。
[Modify Default Zone Properties] ダイアログボックスが表示されます(図 4-39 を参照)。

図 4-39 [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 4-2 に、ブロードキャスト フレームの配信規則を示します。

表 4-2 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?	注
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

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には、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# zone broadcast enable vsan 2	指定された VSAN のフレームをブロードキャストします。
	switch(config)# no zone broadcast enable vsan 3	指定された VSAN のブロードキャストを無効にします(デフォルト)。
ステップ 3	switch(config)# zone name BcastZone vsan 2 switch(config-zone)#	指定された VSAN にブロードキャスト ゾーンを作成し、ゾーン コンフィギュレーション サブモードを開始します。
ステップ 4	switch(config-zone)# member pwnn 21:00:00:20:37:f0:2e:4d	このゾーンに指定されたメンバーを追加します。

	コマンド	目的
ステップ 5	switch(config-zone)# attribute broadcast	このゾーンを他のデバイスにブロードキャストするように指定します。
ステップ 6	switch(config-zone)# end switch# show zone vsan 2 zone name bcast-zone vsan 2 attribute broadcast pwwn 21:00:00:e0:8b:0b:66:56 pwwn 21:00:00:20:37:f0:2e:4d	ブロードキャスト設定を表示します。



(注) ゾーンブロードキャストは、Cisco NX-OS Release 5.x 以降ではサポートされていません。

デフォルトゾーンのブロードキャスト属性を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# zone default-zone vsan 1 switch(config-default-zone)#	ゾーンコンフィギュレーションサブモードを開始します。
ステップ 3	switch(config-default-zone)# attribute broadcast switch(config-default-zone)# no attribute broadcast	デフォルトゾーンにブロードキャスト属性を設定します。 デフォルトゾーン属性を読み取り/書き込みに戻します(デフォルト)。

スマートゾーン分割の概要

スマートゾーン分割では、従来必要とされていたよりも少ないハードウェアリソースで、大きなゾーンのハードゾーン分割が行われます。従来のゾーン分割方式では、ゾーン内の各デバイスが相互に通信できます。管理者はゾーン設定ガイドラインに従って個々のゾーンを管理する必要があります。スマートゾーン分割では、1つのターゲットゾーンへの1つのイニシエータを作成する必要がありません。FCNSのデバイスタイプ情報を分析することで、Cisco MDS NX-OSソフトウェアによりハードウェアレベルで有用な組み合わせが実装されます。使用されていない組み合わせは無視されます。たとえば、イニシエータとイニシエータのペアではなく、イニシエータとターゲットのペアが設定されます。

スマートゾーン内の各デバイスのデバイスタイプ情報は、ファイバチャネルネームサーバ(FCNS)データベースから *host*、*target*、または *both* として自動的に取り込まれます。この情報により、イニシエータターゲットペアが指定され、ハードウェアではそれらのペアだけが設定されるため、スイッチハードウェアをより効率的に使用できるようになります。特殊な状況(別のディスクコントローラと通信する必要があるディスクコントローラなど)では、完全な制御を実現するため、スマートゾーン分割のデフォルトが管理者により上書きされることがあります。



- (注)
- スマートゾーン分割はVSANレベルで有効にできますが、ゾーンレベルで無効にすることもできます。
 - DMM、IOA、またはSMEアプリケーションが有効になっているVSANでは、スマートゾーン分割はサポートされていません。

スマート ゾーン分割のメンバー設定

表 4-3 に、サポートされているスマート ゾーン分割のメンバー設定を示します。

表 4-3 スマート ゾーン分割の設定

機能	サポートあり
PWWN	はい
FCID	はい
FC エイリアス	はい
デバイス エイリアス	はい
インターフェイス	いいえ
IP address	いいえ
シンボル ノード名	いいえ
FWWN	いいえ
Domain ID	いいえ

VSAN でのスマート ゾーン分割の有効化

VSAN に対してスマート ゾーン分割を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# zone smart-zoning enable vsan 1 switch(config)#	VSAN でスマート ゾーン分割を有効にします。
	switch(config)# no zone smart-zoning enable vsan 1	VSAN でスマート ゾーン分割を無効にします。

スマート ゾーン分割のデフォルト値の設定

デフォルト値を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# system default zone smart-zone enable switch(config)#	指定されたデフォルト値に基づいて作成された VSAN でスマート ゾーン分割を有効にします。
ステップ 3	switch(config)# no system default zone smart-zone enable switch(config)#	VSAN でスマート ゾーン分割を無効にします。


スマート ゾーン分割へのゾーンの自動変換

ネーム サーバからデバイス タイプ情報を取得し、その情報をメンバーに追加するには、次の手順を実行します。これは、ゾーン、ゾーン セット、FC エイリアス、および VSAN のレベルで実行できます。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# zone convert smart-zoning fcalias name <alias-name> vsan <vsan no>	FC エイリアス メンバーのデバイス タイプ情報をネーム サーバから取得します。
ステップ 3	switch(config)# zone convert smart-zoning zone name <zone name> vsan <vsan no>	ゾーン メンバーのデバイス タイプ情報をネーム サーバから取得します。
ステップ 4	switch(config)# zone convert smart-zoning zoneset name <zoneset name> vsan <vsan no>	指定されたゾーンセットで、すべてのゾーンと FC エイリアス メンバーのデバイス タイプ情報をネーム サーバから取得します。
ステップ 5	switch(config)# zone convert smart-zoning vsan <vsan no>	VSAN 内に存在するすべてのゾーン セットのすべてのゾーンと FC エイリアス メンバーのデバイス タイプ情報をネーム サーバから取得します。

ゾーン メンバーのデバイス タイプの設定

ゾーン メンバーのデバイス タイプを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config-zoneset-zone)# member device-alias <name> both	デバイス エイリアス メンバーのデバイス タイプを both として設定します。サポートされる各メンバー タイプでは、 init 、 target 、および both がサポートされています。
ステップ 3	switch(config-zoneset-zone)# member pwwn <number> target	pwwn メンバーのデバイス タイプを target として設定します。サポートされる各メンバー タイプでは、 init 、 target 、および both がサポートされています。
ステップ 4	switch(config-zoneset-zone)# member fcid <number>	FCID メンバーのデバイス タイプを設定します。設定されている特定のデバイス タイプがありません。サポートされる各メンバー タイプでは、 init 、 target 、および both がサポートされています。
		 <p>(注) ゾーン メンバーに対して特定のデバイス タイプが設定されていない場合は、バックエンドで、生成されたゾーン エントリがデバイス タイプ both として作成されます。</p>


スマート ゾーン分割設定の削除

スマート ゾーン分割設定を削除するには、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>switch(config)# clear zone smart-zoning fcalias name <alias-name> vsan <vsan no></code>	指定された FC エイリアスのすべてのメンバーのデバイス タイプ設定を削除します。
ステップ 2	<code>switch(config)# clear zone smart-zoning zone name <zone name> vsan <vsan no></code>	指定されたゾーンのすべてのメンバーのデバイス タイプ設定を削除します。
ステップ 3	<code>switch(config)# clear zone smart-zoning zoneset name <zoneset name> vsan <vsan no></code>	指定されたゾーン セットの FC エイリアスとゾーンのすべてのメンバーのデバイス タイプ設定を削除します。
ステップ 4	<code>switch(config)# clear zone smart-zoning vsan <vsan no></code>	VSAN の指定されたゾーン セットの FC エイリアスとゾーンのすべてメンバーのデバイス タイプ設定を削除します。

ゾーンレベルでのスマート ゾーン分割の無効化

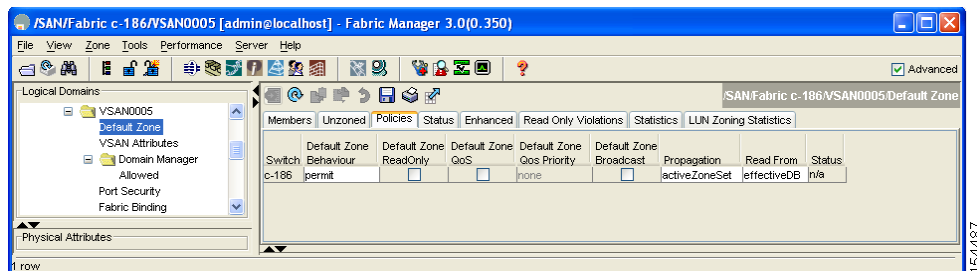
ゾーンレベルでスマート ゾーン分割を無効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>switch# config t switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>switch(config)# zone name zone1 vsan 1</code>	ゾーン名を設定します。
ステップ 3	<code>switch(config-zone)# no attribute disable-smart-zoning</code>	選択されたゾーンに対してスマート ゾーン分割が無効になります。
		 <p>(注) このコマンドでは、選択されたゾーンのスマート ゾーン分割が無効になるだけです。デバイス タイプ設定は削除されません。</p>

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 4-40 を参照)。

図 4-40 ゾーン ポリシー情報

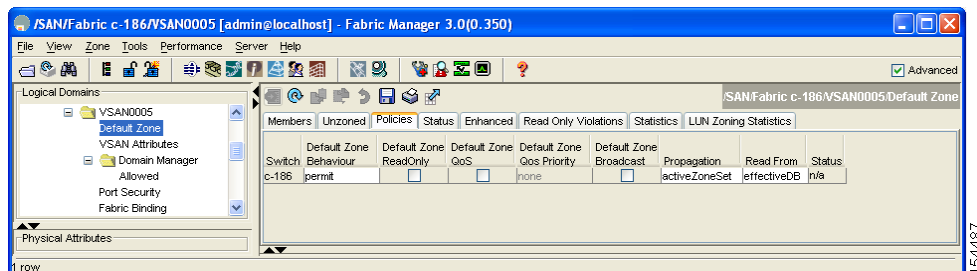


- ステップ 3** [Broadcast] チェックボックスをオンにして、デフォルト ゾーン上でブロードキャスト フレームをイネーブルにします。
- ステップ 4** [Apply Changes] をクリックして、変更を保存します。

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 4-40を参照)。

図 4-41 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 ゾーン上でブロードキャスト 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 ファミリー 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。



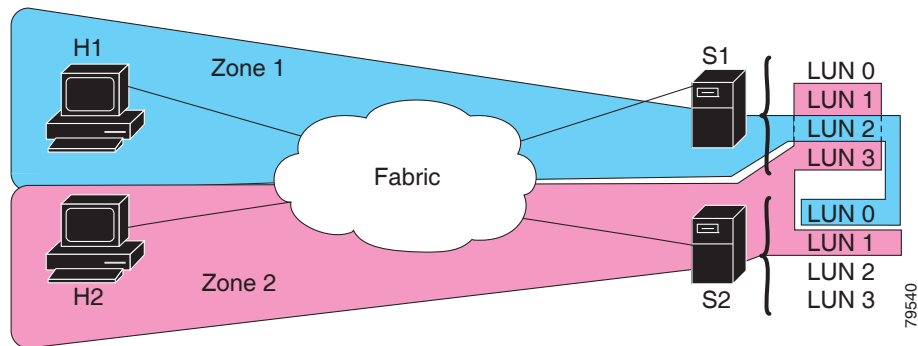
(注) ゾーン分割されていない LUN は、自動的にデフォルト ゾーンのメンバーになります。



(注) LUN ゾーン分割 は、Cisco MDS NX-OS Release 5.x 以降ではサポートされていません。

図 4-42 に、LUN ベースのゾーン分割の例を示します。

図 4-42 LUN ゾーン分割でのアクセス



LUN ベースのゾーンの設定

LUN ベースのゾーンを設定するには、次の手順を実行します。

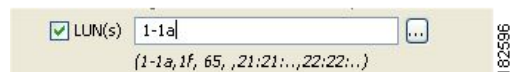
	コマンド	目的
ステップ 1	switch# <code>config t</code> switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <code>zone name LunSample vsan 2</code> switch(config-zone)#	指定された VSAN (vsan 2) のゾーン LunSample を設定し、ゾーン コンフィギュレーション サブモードを開始します。

コマンド	目的
ステップ 3 <pre>switch(config-zone)# member pwwn 10:00:00:23:45:67:89:ab lun 0x64</pre>	指定された pWWN と LUN 値に基づいてゾーンメンバーを設定します。 (注) CLI は、 0x プレフィックスが含まれているかどうかに関係なく、LUN ID の値を 16 進値として解釈します。16 進形式の LUN 0x64 は、10 進形式の 100 に対応します。
<pre>switch(config-zone)# member fcid 0x12465 lun 0x64</pre>	FC ID と LUN 値に基づいてゾーンメンバーを設定します。

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。
[Add Member to Zone] ダイアログボックスが表示されます(図 4-43 を参照)。

図 4-43 [Add Member to Zone] ダイアログボックス



- ステップ 4** [Zone By] オプションの [WWN] または [FCID] オプション ボタンをクリックして、LUN ベース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てからブラウズ ボタンをクリックし、LUN を設定します。
- ステップ 6** [Add] をクリックして、この LUN ベース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 ファミリースイッチで追加の 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」セクション(4-56 ページ)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。



(注) 読み取り専用ゾーンは、Cisco MDS NX-OS Release 5.x 以降ではサポートされていません。

読み取り専用ゾーンの設定

読み取り専用ゾーンを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# zone name Sample2 vsan 2 switch(config-zone)#	指定された VSAN (vsan 2) のゾーン Sample2 を設定し、ゾーン コンフィギュレーション サブモードを開始します。
ステップ 3	switch(config-zone)# attribute read-only	Sample2 ゾーンに読み取り専用属性を設定します。 (注) デフォルトでは、すべてのゾーンで読み取り/書き込みです。
	switch(config-zone)# no attribute read-only	Sample2 ゾーン属性を読み取り/書き込みに戻します。

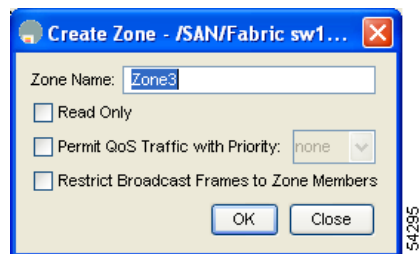
デフォルト ゾーンに **read-only** オプションを設定するには、次の手順を実行します。

コマンド	目的
ステップ 1 switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2 switch(config)# zone default-zone vsan 1 switch(config-default-zone)#	ゾーン コンフィギュレーション サブモードを開始します。
ステップ 3 switch(config-default-zone)# attribute read-only	デフォルト ゾーンに読み取り専用属性を設定します。
switch(config-default-zone)# no attribute read-only	デフォルト ゾーン属性を読み取り/書き込みに戻します(デフォルト)。

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 4-44 を参照)。

図 4-44 [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](#)」セクション(4-49 ページ)を参照してください。

ゾーン情報の表示

ゾーン情報を表示するには、**show** コマンドを使用します。特定のオブジェクトの情報(たとえば、特定のゾーン、ゾーン セット、VSAN、エイリアス、または **brief** や **active** などのキーワード)を要求する場合、指定されたオブジェクトの情報だけが表示されます。特定の情報を要求しない場合、入手できるすべての情報が表示されます。例 4-2 ~ 4-17 を参照してください。

例 4-2 すべての VSAN のゾーン情報の表示

```

switch# show zone
zone name Zone3 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:9c:48:e5

zone name Zone2 vsan 2
  fwwn 20:41:00:05:30:00:2a:1e
  fwwn 20:42:00:05:30:00:2a:1e
  fwwn 20:43:00:05:30:00:2a:1e

zone name Zone1 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:a6:be:2f
  pwwn 21:00:00:20:37:9c:48:e5
  fcalias Alias1

zone name Techdocs vsan 3
  ip-address 10.15.0.0 255.255.255.0

zone name Zone21 vsan 5
  pwwn 21:00:00:20:37:a6:be:35
  pwwn 21:00:00:20:37:a6:be:39
  fcid 0xe000ef
  fcid 0xe000e0
  symbolic-nodename iqn.test
  fwwn 20:1f:00:05:30:00:e5:c6
  fwwn 12:12:11:12:11:12:12:10
  interface fc1/5 swwn 20:00:00:05:30:00:2a:1e
  ip-address 12.2.4.5 255.255.255.0
  fcalias name Alias1 vsan 1
    pwwn 21:00:00:20:37:a6:be:35

zone name Zone2 vsan 11
  interface fc1/5 pwwn 20:4f:00:05:30:00:2a:1e

zone name Zone22 vsan 6
  fcalias name Alias1 vsan 1
    pwwn 21:00:00:20:37:a6:be:35

zone name Zone23 vsan 61
  pwwn 21:00:00:04:cf:fb:3e:7b lun 0000

```

例 4-3 特定の VSAN のゾーン情報の表示

```

switch# show zone vsan 1
zone name Zone3 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:9c:48:e5

zone name Zone2 vsan 1
  fwwn 20:4f:00:05:30:00:2a:1e
  fwwn 20:50:00:05:30:00:2a:1e
  fwwn 20:51:00:05:30:00:2a:1e
  fwwn 20:52:00:05:30:00:2a:1e
  fwwn 20:53:00:05:30:00:2a:1e

zone name Zone1 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:a6:be:2f
  pwwn 21:00:00:20:37:9c:48:e5
  fcalias Alias1

```

設定されたゾーン セットを表示するには、**show zoneset** コマンドを使用します。

例 4-4 設定されたゾーン セット情報の表示

```
switch# show zoneset vsan 1
zoneset name ZoneSet2 vsan 1
  zone name Zone2 vsan 1
    fwwn 20:4e:00:05:30:00:2a:1e
    fwwn 20:4f:00:05:30:00:2a:1e
    fwwn 20:50:00:05:30:00:2a:1e
    fwwn 20:51:00:05:30:00:2a:1e
    fwwn 20:52:00:05:30:00:2a:1e

  zone name Zone1 vsan 1
    pwwn 21:00:00:20:37:6f:db:dd
    pwwn 21:00:00:20:37:a6:be:2f
    pwwn 21:00:00:20:37:9c:48:e5
    fcalias Alias1

zoneset name ZoneSet1 vsan 1
  zone name Zone1 vsan 1
    pwwn 21:00:00:20:37:6f:db:dd
    pwwn 21:00:00:20:37:a6:be:2f
    pwwn 21:00:00:20:37:9c:48:e5
    fcalias Alias1
```

例 4-5 VSAN 範囲の設定されたゾーン セット情報の表示

```
switch# show zoneset vsan 2-3
zoneset name ZoneSet2 vsan 2
  zone name Zone2 vsan 2
    fwwn 20:52:00:05:30:00:2a:1e
    fwwn 20:53:00:05:30:00:2a:1e
    fwwn 20:54:00:05:30:00:2a:1e
    fwwn 20:55:00:05:30:00:2a:1e
    fwwn 20:56:00:05:30:00:2a:1e

  zone name Zone1 vsan 2
    pwwn 21:00:00:20:37:6f:db:dd
    pwwn 21:00:00:20:37:a6:be:2f
    pwwn 21:00:00:20:37:9c:48:e5
    fcalias Alias1

zoneset name ZoneSet3 vsan 3
  zone name Zone1 vsan 1
    pwwn 21:00:00:20:37:6f:db:dd
    pwwn 21:00:00:20:37:a6:be:2f
    pwwn 21:00:00:20:37:9c:48:e5
    fcalias Alias1
```

特定のゾーンのメンバーを表示するには、**show zone name** コマンドを使用します。

例 4-6 ゾーンのメンバーの表示

```
switch# show zone name Zone1
zone name Zone1 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:a6:be:2f
  pwwn 21:00:00:20:37:9c:48:e5
  fcalias Alias1
```

FC エイリアス設定を表示するには、**show fcalias** コマンドを使用します。

例 4-7 FC エイリアス設定の表示

```
switch# show fcalias vsan 1
fcalias name Alias2 vsan 1

fcalias name Alias1 vsan 1
  pwn 21:00:00:20:37:6f:db:dd
  pwn 21:00:00:20:37:9c:48:e5
```

FC ID を使用してメンバーが所属するすべてのゾーンを表示するには、**show zone member** コマンドを使用します。

例 4-8 メンバーシップステータスの表示

```
switch# show zone member pwn 21:00:00:20:37:9c:48:e5
      VSAN: 1
zone Zone3
zone Zone1
fcalias Alias1
```

他のスイッチで交換された制御フレームの数を表示するには、**show zone statistics** コマンドを使用します。

例 4-9 ゾーン統計情報の表示

```
switch# show zone statistics
Statistics For VSAN: 1
*****
Number of Merge Requests Sent: 24
Number of Merge Requests Recvd: 25
Number of Merge Accepts Sent: 25
Number of Merge Accepts Recvd: 25
Number of Merge Rejects Sent: 0
Number of Merge Rejects Recvd: 0
Number of Change Requests Sent: 0
Number of Change Requests Recvd: 0
Number of Change Rejects Sent: 0
Number of Change Rejects Recvd: 0
Number of GS Requests Recvd: 0
Number of GS Requests Rejected: 0
Statistics For VSAN: 2
*****
Number of Merge Requests Sent: 4
Number of Merge Requests Recvd: 4
Number of Merge Accepts Sent: 4
Number of Merge Accepts Recvd: 4
Number of Merge Rejects Sent: 0
Number of Merge Rejects Recvd: 0
Number of Change Requests Sent: 0
Number of Change Requests Recvd: 0
Number of Change Rejects Sent: 0
Number of Change Rejects Recvd: 0
Number of GS Requests Recvd: 0
Number of GS Requests Rejected: 0
```

例 4-10 LUN ゾーン統計情報の表示

```

switch# show zone statistics lun-zoning
LUN zoning statistics for VSAN: 1
*****
S-ID: 0x123456, D-ID: 0x22222, LUN: 00:00:00:00:00:00:00:00
-----
Number of Inquiry commands received: 10
Number of Inquiry data No LU sent: 5
Number of Report LUNs commands received: 10
Number of Request Sense commands received: 1
Number of Other commands received: 0
Number of Illegal Request Check Condition sent: 0

S-ID: 0x123456, D-ID: 0x22222, LUN: 00:00:00:00:00:00:00:01
-----
Number of Inquiry commands received: 1
Number of Inquiry data No LU sent: 1
Number of Request Sense commands received: 1
Number of Other commands received: 0
Number of Illegal Request Check Condition sent: 0

```

例 4-11 LUN ゾーン統計情報の表示

```

Need the latest output
switch# show zone statistics read-only-zoning
Read-only zoning statistics for VSAN: 2
*****
S-ID: 0x33333, D-ID: 0x11111, LUN: 00:00:00:00:00:00:00:64
-----
Number of Data Protect Check Condition Sent: 12

```

例 4-12 アクティブ ゾーン セットの表示

```

switch# show zoneset active
zoneset name ZoneSet1 vsan 1
  zone name zone1 vsan 1
    fcid 0x080808
    fcid 0x090909
    fcid 0x0a0a0a
  zone name zone2 vsan 1
    * fcid 0xef0000 [pwn 21:00:00:20:37:6f:db:dd]
    * fcid 0xef0100 [pwn 21:00:00:20:37:a6:be:2f]

```

例 4-13 ゾーン セットの簡単な説明の表示

```

switch# show zoneset brief
zoneset name ZoneSet1 vsan 1
  zone zone1
  zone zone2

```

例 4-14 アクティブ ゾーンの表示

```

switch# show zone active
zone name Zone2 vsan 1
* fcid 0x6c01ef [pwn 21:00:00:20:37:9c:48:e5]

```

■ ゾーン情報の表示

```

zone name IVRZ_IvrZone1 vsan 1
  pwn 10:00:00:00:77:99:7a:1b
* fcid 0xce0000 [pwn 10:00:00:00:c9:2d:5a:dd]

zone name IVRZ_IvrZone4 vsan 1
* fcid 0xce0000 [pwn 10:00:00:00:c9:2d:5a:dd]
* fcid 0x6c01ef [pwn 21:00:00:20:37:9c:48:e5]

zone name Zone1 vsan 1667
  fcid 0x123456

zone name $default_zone$ vsan 1667

```

例 4-15 アクティブゾーンセットの表示

```

switch# show zoneset active
zoneset name ZoneSet4 vsan 1
  zone name Zone2 vsan 1
  * fcid 0x6c01ef [pwn 21:00:00:20:37:9c:48:e5]

  zone name IVRZ_IvrZone1 vsan 1
    pwn 10:00:00:00:77:99:7a:1b
  * fcid 0xce0000 [pwn 10:00:00:00:c9:2d:5a:dd]

zoneset name QosZoneset vsan 2
  zone name QosZone vsan 2
  attribute qos priority high
  * fcid 0xce0000 [pwn 10:00:00:00:c9:2d:5a:dd]
  * fcid 0x6c01ef [pwn 21:00:00:20:37:9c:48:e5]

Active zoneset vsan 1667
  zone name Zone1 vsan 1667
    fcid 0x123456

  zone name $default_zone$ vsan 1667

```

例 4-16 ゾーンステータスの表示

```

switch(config)# show zone status
VSAN: 1 default-zone: deny distribute: active only Interop: default
mode: basic merge-control: allow
session: none
hard-zoning: enabled broadcast: disabled
smart-zoning: disabled
rscn-format: fabric-address
activation overwrite control:disabled
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 4 bytes
Zonesets:0 Zones:0 Aliases: 0
Active Zoning Database :
Database Not Available
Current Total Zone DB Usage: 4 / 2097152 bytes (0 % used)
Pending (Session) DB size:
Full DB Copy size: n/a
Active DB Copy size: n/a
SFC size: 4 / 2097152 bytes (0 % used)
Status:

```



```
VSAN: 8 default-zone: deny distribute: full Interop: default
mode: basic merge-control: allow
session: none
hard-zoning: enabled broadcast: disabled
smart-zoning: disabled
rscn-format: fabric-address
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 1946498 bytes
Zonesets:6 Zones:8024 Aliases: 0
Active Zoning Database :
DB size: 150499 bytes
Name: zoneset-1000 Zonesets:1 Zones:731
Current Total Zone DB Usage: 2096997 / 2097152 bytes (99 % used)
Pending (Session) DB size:
Full DB Copy size: n/a
Active DB Copy size: n/a
SFC size: 2096997 / 2097152 bytes (99 % used)
Status: Zoneset distribution failed [Error: Fabric changing Dom 33]:
at 17:05:06 UTC Jun 16 2014
```

```
VSAN: 9 default-zone: deny distribute: full Interop: default
mode: enhanced merge-control: allow
session: none
hard-zoning: enabled broadcast: enabled
smart-zoning: disabled
rscn-format: fabric-address
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 2002584 bytes
Zonesets:4 Zones:7004 Aliases: 0 Attribute-groups: 1
Active Zoning Database :
DB size: 94340 bytes
Name: zoneset-hac13-200 Zonesets:1 Zones:176
Current Total Zone DB Usage: 2096924 / 2097152 bytes (99 % used)
Pending (Session) DB size:
Full DB Copy size: 0 bytes
Active DB Copy size: 0 bytes
SFC size: 0 / 2097152 bytes (0 % used)
Status: Activation completed at 17:28:04 UTC Jun 16 2014
```

```
VSAN: 12 default-zone: deny distribute: full Interop: default
mode: enhanced merge-control: allow
session: none
hard-zoning: enabled broadcast: enabled
smart-zoning: disabled
rscn-format: fabric-address
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 84 bytes
Zonesets:0 Zones:1 Aliases: 0 Attribute-groups: 1
Active Zoning Database :
DB size: 144 bytes
Name: zs1 Zonesets:1 Zones:2
Current Total Zone DB Usage: 228 / 2097152 bytes (0 % used)
Pending (Session) DB size:
Full DB Copy size: 0 bytes
Active DB Copy size: 0 bytes
SFC size: 0 / 2097152 bytes (0 % used)
Status: Commit completed at 14:39:33 UTC Jun 27 201
switch(config)#
```

設定されたすべてのゾーンのゾーン属性を表示するには、**show zone** コマンドを使用します。

例 4-17 ゾーン統計情報の表示

```
switch# show zone
zone name lunSample vsan 1 <-----読み取り/書き込み属性
zone name ReadOnlyZone vsan 2
      attribute read-only <-----読み取り専用属性
```

設定されたインターフェイスベースゾーンを表示するには、**show running** コマンドおよび **show zone active** コマンドを使用します(例 4-18 および例 4-19 を参照)。

例 4-18 インターフェイス ベース ゾーン の表示

```
switch# show running
zone name if-zone vsan 1
  member interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2
  member fwwn 20:4f:00:0c:88:00:4a:e2
  member interface fc2/1 swwn 20:00:00:05:30:00:4a:9e
  member pwwn 22:00:00:20:37:39:6b:dd
```

例 4-19 アクティブ ゾーン の fWWN および インターフェイス の表示

```
switch# show zone active
zone name if-zone vsan 1
 * fcid 0x7e00b3 [interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2]
 * fcid 0x7e00b1 [interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2]
 * fcid 0x7e00ac [interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2]
 * fcid 0x7e00b3 [fwwn 20:4f:00:0c:88:00:4a:e2]
 * fcid 0x7e00b1 [fwwn 20:4f:00:0c:88:00:4a:e2]
 * fcid 0x7e00ac [fwwn 20:4f:00:0c:88:00:4a:e2]
      interface fc2/1 swwn 20:00:00:05:30:00:4a:9e
```

同様の出力は、リモート スイッチでも入手できます(例 4-20 を参照)。

例 4-20 リモート スイッチ の ローカル インターフェイス の アクティブ ゾーン 詳細 の表示

```
switch# show zone active
zone name if-zone vsan 1
 * fcid 0x7e00b3 [interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2]
 * fcid 0x7e00b1 [interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2]
 * fcid 0x7e00ac [interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2]
 * fcid 0x7e00b3 [fwwn 20:4f:00:0c:88:00:4a:e2]
 * fcid 0x7e00b1 [fwwn 20:4f:00:0c:88:00:4a:e2]
 * fcid 0x7e00ac [fwwn 20:4f:00:0c:88:00:4a:e2]
      interface fc2/1 swwn 20:00:00:05:30:00:4a:9e
```

例 4-21 VSAN の ゾーン ステータス の表示

```
switch(config)# show zone status vsan 1
VSAN: 1 default-zone: deny distribute: active only Interop: default
mode: basic merge-control: allow
session: none
hard-zoning: enabled broadcast: disabled
smart-zoning: disabled
rscn-format: fabric-address
activation overwrite control:disabled
Default zone:
```

```

gos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 4 bytes
Zonesets:0 Zones:0 Aliases: 0
Active Zoning Database :
Database Not Available
Current Total Zone DB Usage: 4 / 2097152 bytes (0 % used)
Pending (Session) DB size:
Full DB Copy size: n/a
Active DB Copy size: n/a
SFC size: 4 / 2097152 bytes (0 % used)
Status:
switch(config)#

```

例 4-22 VSAN のゾーン ポリシーの表示

```

switch# show zone policy vsan 1
Vsan: 1
  Default-zone: deny
  Distribute: full
  Broadcast: enable
  Merge control: allow
  Generic Service: read-write
  Smart-zone: enabled

```

例 4-23 ゾーンに設定されているスマート ゾーン分割属性を無効にする方法の表示

```

config# zone-attribute-group name <name> vsan 1
config-attribute-group# disable-smart-zoning
config-attribute-group# exit
config# zone commit vsan 1

```

例 4-24 ゾーンの自動変換方法の表示

```

config# show zoneset vsan 1
zoneset name ZSv1 vsan 1
  zone name ddasZone vsan 1
    device-alias Init1
    device-alias Init2
    device-alias Init3
    device-alias Target1

config# zone convert smart-zoning vsan 1
smart-zoning auto_convert initiated.This operation can take few minutes.Please wait..
config#
config# show zoneset vsan1
zoneset name ZSv1 vsan 1
  zone name ddasZone vsan 1
    device-alias Init1 init
    device-alias Init2 init
    device-alias Init3 init
    device-alias Target1 target

```

例 4-25 メンバーのデバイス タイプ設定をクリアする方法の表示

```

config# show zoneset vsan 1
zoneset name ZSv1 vsan 1
  zone name ddasZone vsan 1
    device-alias Init1 init
    device-alias Init2 init
    device-alias Init3 init
    device-alias Target1 target

config# clear zone smart-zoning vsan1

config# show zoneset vsan 1
zoneset name ZSv1 vsan 1
  zone name ddasZone vsan 1
    device-alias Init1
    device-alias Init2
    device-alias Init3
    device-alias Target1

```

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 規格に準拠しています。どちらの規格も、前の項で説明した基本ゾーン分割機能と、この項で説明する拡張ゾーン分割機能をサポートしています。

この項では、次のトピックについて取り上げます。

- [拡張ゾーン分割の概要 \(4-69 ページ\)](#)
- [基本ゾーン分割から拡張ゾーン分割への変更 \(4-70 ページ\)](#)
- [拡張ゾーン分割から基本ゾーン分割への変更 \(4-70 ページ\)](#)
- [拡張ゾーン分割の有効化 \(4-71 ページ\)](#)
- [ゾーン データベースの変更 \(4-72 ページ\)](#)
- [ゾーンの保留中差分の自動表示の有効化 \(4-73 ページ\)](#)
- [属性グループの作成 \(4-74 ページ\)](#)
- [データベースのマージ \(4-74 ページ\)](#)
- [ゾーン マージの分析 \(4-84 ページ\)](#)
- [ゾーン マージ制御ポリシーの設定 \(4-85 ページ\)](#)
- [デフォルト ゾーンでのトラフィックの許可または拒否 \(4-86 ページ\)](#)
- [ゾーンのブロードキャスト \(4-86 ページ\)](#)
- [システムのデフォルト ゾーン分割設定値の設定 \(4-87 ページ\)](#)
- [拡張ゾーン情報の表示 \(4-89 ページ\)](#)

拡張ゾーン分割の概要

表 4-4 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 4-4 拡張ゾーン分割の利点

基本ゾーン分割	拡張ゾーン分割	拡張ゾーン分割の利点
複数の管理者が設定変更を同時に行うことができます。アクティブ化すると、ある管理者が別の管理者の設定変更を上書きできます。	単一のコンフィギュレーションセッションですべての設定を実行できます。セッションを開始すると、スイッチは変更を行うファブリック全体をロックします。	ファブリック全体を1つのコンフィギュレーションセッションで設定するため、ファブリック内での整合性が確保されます。
ゾーンが複数のゾーンセットに含まれる場合、各ゾーンセットにこのゾーンのインスタンスを作成します。	ゾーンが定義されると、必要に応じて、ゾーンセットがゾーンを参照します。	ゾーンが参照されるため、ペイロードサイズが縮小されています。データベースが大きくなるほど、サイズ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ず、ファブリックをスムーズに動作させるため、ファブリック内のスイッチはすべて同一のデフォルトゾーン設定を使用する必要があります。	ファブリック全体でデフォルトゾーン設定を実行および交換します。	ポリシーがファブリック全体に適用されるため、トラブルシューティングの時間が短縮されます。
スイッチ単位でのアクティブ化の結果を取得するため、管理スイッチはアクティブ化に関する複合ステータスを提供します。この場合、障害のあるスイッチは特定されません。	各リモートスイッチからアクティブ化の結果と問題の特性を取得します。	エラー通知機能が強化されているため、トラブルシューティングが容易です。
ゾーン分割データベースを配信するには、同じゾーンセットを再度アクティブ化する必要があります。再度アクティブ化すると、ローカルスイッチおよびリモートスイッチのハードゾーン分割のハードウェア変更に影響することがあります。	ゾーン分割データベースに対して変更を行い、再度アクティブ化することなく変更を配信します。	アクティブ化せずにゾーンセットを配信すると、スイッチのハードゾーン分割のハードウェア変更が回避されます。

表 4-4 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 タイプを一意に識別するために、ベンダー固有のタイプ値とベンダー ID が提供されます。	ベンダー タイプが一意です。
fWWN ベースのゾーン メンバーシップは、シスコの interop モードでだけサポートされます。	標準の interop モード (interop モード 1) で fWWN ベースのメンバーシップがサポートされます。	fWWN ベースのメンバタイプは標準化されています。

基本ゾーン分割から拡張ゾーン分割への変更

基本ゾーン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 つ以上のスイッチが拡張モードで動作できない場合、拡張モードへ変更できません。
- 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、次に進む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。

拡張ゾーン分割の有効化

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。

VSAN で拡張ゾーン分割を有効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# zone mode enhanced vsan 3000 Set zoning mode command initiated.Check zone status	指定された VSAN で拡張ゾーン分割をイネーブルにします。
	switch(config)# no zone mode enhanced vsan 150 Set zoning mode command initiated.Check zone status	指定された VSAN で拡張ゾーン分割をディセーブルにします。

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 メニューで [enhanced] を選択して、この VSAN の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。

ゾーン データベースの変更

ゾーン データベースに対する変更は、セッション内で実行されます。セッションは、コンフィギュレーション コマンドが初めて正常に実行されたときに作成されます。セッションが作成されると、ゾーン データベースのコピーが作成されます。セッションでの変更は、ゾーン分割データベースのコピー上で実行されます。ゾーン分割データベースのコピー上で行われる変更は、コミットするまで有効なゾーン分割データベースには適用されません。変更を適用すると、セッションはクローズします。

ファブリックが別のユーザによってロックされ、何らかの理由でロックがクリアされない場合は、強制的に実行し、セッションをクローズします。このスイッチでロックをクリアする権限（ロール）が必要です。また、この操作は、セッションが作成されたスイッチから実行する必要があります。

VSAN 内のゾーン分割データベースに対する変更をコミットまたは廃棄するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# zone commit vsan 2 No pending info found	拡張ゾーン データベースに変更を適用し、セッションをクローズします。
	switch(config)# zone commit vsan 3 force	拡張ゾーン データベースに変更を強制的に適用し、別のユーザが作成したセッションをクローズします。
	switch(config)# no zone commit vsan 2	拡張ゾーン データベースへの変更を廃棄し、セッションをクローズします。
	switch(config)# no zone commit vsan 3 force	拡張ゾーン データベースへの変更を強制的に廃棄し、別のユーザが作成したセッションをクローズします。



ヒント

アクティブなゾーン セットを保存するために、**実行コンフィギュレーションをスタートアップコンフィギュレーションにコピー** `copy running-config startup-config` コマンドを実行する必要はありません。ただし、フルゾーン セットを明示的に保存するには、**実行コンフィギュレーションをスタートアップコンフィギュレーションにコピー** `copy running-config startup-config` コマンドを実行する必要があります。ファブリックに複数のスイッチが含まれている場合は、**copy running-config startup-config fabric** コマンドを実行する必要があります。キーワード `fabric` を指定すると、`copy running-config startup-config` コマンドがファブリック内のすべてのスイッチで実行され、フルゾーン情報がファブリック内のすべてのスイッチのスタートアップコンフィギュレーションに保存されます。これは、スイッチのリロードおよび電源再投入時に重要です。

ゾーンの保留中差分の自動表示の有効化

拡張モードでの `zone commit` 発行時の保留中差分の表示とそれ以降の確認を有効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>switch# config t</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>switch(config)# zone confirm-commit enable</code> <code>vsan vsan-id</code>	特定の VSAN のゾーン データベースに対して confirm-commit オプションを有効にします。
ステップ 3	<code>switch(config-zone)# zone commit vsan 12</code> The following zoning changes are about to be committed +zone name zone-1 vsan 12 Do you want to continue? (y/n) [n]	VSAN に対して zone confirm-commit コマンドが有効な場合、保留中のデータベースをコミットすると、コンソールに <code>pending-off</code> が表示され、ユーザに対し [Yes] または [No] を選択するように求められます。 zone confirm-commit コマンドが無効な場合、保留中差分は表示されず、ユーザに対し [Yes] または [No] を選択するように求められません。
ステップ 4	<code>switch(config)# no zone commit vsan 12</code> The following zoning changes are about to be discarded +zone name zone-1 vsan 12 Do you want to continue? (y/n) [n] <code>switch(config)#</code>	VSAN に対して zone confirm-commit コマンドが有効な場合、保留中のデータベースを廃棄すると、コンソールに <code>pending-off</code> が表示され、ユーザに対し [Yes] または [No] を選択するように求められます。 zone confirm-commit コマンドが無効な場合、保留中差分は表示されず、ユーザに対し [Yes] または [No] を選択するように求められません。

ゾーン データベース ロックの解除

VSAN 内のスイッチのゾーン分割 データベースのセッション ロックを解除するには、最初にデータベースをロックしたスイッチから **no zone commit vsan** コマンドを使用します。

```
switch# config t
switch(config)# no zone commit vsan 2
```

no zone commit vsan コマンドを実行したあとも、リモート スイッチ上でセッションがロックされたままの場合、リモート スイッチ上で **clear zone lock vsan** コマンドを使用できます。

```
switch# clear zone lock vsan 2
```



(注)

ファブリック内のセッション ロックを解除するには、最初に **no zone commit vsan** コマンドを使用することを推奨します。それが失敗した場合には、セッションがロックされたままのリモート スイッチで、**clear zone lock vsan** コマンドを使用してください。

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。
属性グループを設定するには、次の手順を実行します。

ステップ 1 属性グループを作成します。

```
switch# conf t
switch(config)# zone-attribute-group name SampleAttributeGroup vsan 2
switch(config-attribute-group)#
```

ステップ 2 属性グループ オブジェクトに属性を追加します。

```
switch(config-attribute-group)# readonly
switch(config-attribute-group)# broadcast
switch(config-attribute-group)# qos priority medium
readonly および broadcast コマンドは、5.2 リリース以降ではサポートされていません。
```

ステップ 3 ゾーンに属性グループを対応付けます。

```
switch(config)# zone name Zone1 vsan 2
switch(config-zone)# attribute-group SampleAttributeGroup
switch(config-zone)# exit
switch(config)#
```

ステップ 4 ゾーンセットをアクティブ化します。

```
switch(config)# zoneset activate name Zoneset1 vsan 2
```

属性グループが展開され、アクティブ ゾーン セットには設定された属性だけが存在します。

属性グループの設定については、『Cisco MDS 9000 Family NX-OS Fabric 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 4-5 で指定された結合規則を使用して結合されます。

表 4-5 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	結合ステータス	結合結果
データベースに、名前 ¹ は同じだが、異なるゾーン、エイリアス、および属性グループを持つ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が結合されます。
データベースに、名前は ¹ で同じだが、異なる番号を持つゾーン、ゾーン エイリアス、またはゾーン属性グループ オブジェクトが含まれる。		失敗	ISL は分離されます。

表 4-5 データベースのゾーン マージステータス(続き)

ローカル データベース	隣接データベース	結合ステータス	結合結果
データなし	データあり	成功	ローカル データベースには隣接データベースの情報が存在します。
データあり	データなし	成功	隣接データベースにはローカル データベースの情報が存在します。

1. 拡張ゾーン分割モードでは、interop モード 1 のアクティブ ゾーン セットには名前がありません。ゾーン セット名が存在するのは、フルゾーン セットの場合だけです。



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

すでにアクティブ ゾーン セットが設定されており、まだ接続されていない 2 つのファイバチャネル (FC) スイッチが、拡張 ISL (EISL) リンクで接続されると、ゾーン セットがマージされます。ただし、新しいゾーンを設定してアクティブ化する前に、ゾーンの整合性を確保するための手順を実行する必要があります。

ベスト プラクティス

ゾーン マージが発生すると、矛盾する情報がない限り、各スイッチは他のゾーンについて学習します。各スイッチには 3 種類の設定要素があります。スイッチには次の設定があります。

- NVRAM に保存された設定。これは、**copy running-configuration startup-configuration** コマンドの最終実行時の設定です。
- 実行コンフィギュレーション。これは、MDS の前回起動時にメモリに取り込まれた設定と、設定に対して行われたすべての変更を表します。ゾーン分割情報に関しては、実行コンフィギュレーションは設定可能なデータベース (フル データベース) を表します。
- 実行コンフィギュレーションからの設定されたゾーン分割情報と、ゾーン マージから学習されたゾーン分割情報。この設定されたゾーン分割情報と学習されたゾーン分割情報の組み合わせが、アクティブ ゾーン セットです。

結合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である場合、ゾーン ポリシーが比較されます。ゾーン ポリシーが異なる場合、ISL は分離されます。
3. ゾーン結合オプションが同じである場合、結合制御設定に基づいて比較が行われます。
 - 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。これらが同じでない場合、リンクは分離されます。
 - b. 設定が「許可」の場合、結合規則を使用して結合が行われます。

MDS は、起動時に NVRAM に以前に保存された設定を使用します。NVRAM から設定をロードした後でスイッチを設定した場合、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保存されるまでは、ブートアップ コンフィギュレーションと実行コンフィギュレーションの間に差異があります。これは、PC のローカルハードドライブにファイルが保存されていることに関連している可能性があります。ファイルは保存されておりスタティックですが、ファイルを開いて編集すると、変更後のファイルと、保存ストレージに存在するファイルの間に差異が生じます。変更の保存時にのみ、保存されたエンティティがファイルに対して行われた変更を表します。

ゾーン マージからゾーン分割情報が学習される場合、学習された情報は実行コンフィギュレーションには含まれません。学習された情報が実行コンフィギュレーションに組み込まれるのは、**zone copy active-zoneset full-zoneset vsan X** コマンドの実行時のみです。ゾーン マージが新しい EISL リンクにより開始されるか、またはゾーン セットのアクティブ化により開始された場合、ゾーン セット部分はもう一方のスイッチにより無視され、メンバー ゾーン情報は局所的と見なされるため、これは重要です。



注意

zone copy コマンドは、FC エイリアス設定をすべて削除します。

例

たとえば、2つのスタンドアロン MDS スイッチがすでに配置されており、それぞれに固有のゾーンとゾーン セット情報が設定されているとします。スイッチ 1 のアクティブ ゾーン セットはセット A、スイッチ 2 のアクティブ ゾーン セットはセット B であり、スイッチ 1 のセット A 内にゾーン 1 があり、スイッチ 2 のセット B にメンバーゾーン 2 があるとします。この 2つのスイッチ間で ISL リンクが作成されると、各スイッチは各自のゾーン セット (ゾーン情報を含む) をもう一方のスイッチに送信します。マージ時には、スイッチは ASCII 値が大きい方のゾーン セット名を選択し、その後ゾーン メンバーをマージします。マージ後は、両方のスイッチにセット B という名前のゾーン セットが含まれます。このゾーン セットにはメンバーゾーン 1 とゾーン 2 が含まれています。

ゾーン 1 とゾーン 2 のすべてのデバイスに対して、これまでと同様にすべてが適切に機能します。新しいゾーンを追加するには、新しいゾーンを作成してゾーン セットに追加し、そのゾーン セットをアクティブにする必要があります。

段階的にスイッチが起動します。スイッチにはゾーン分割情報は含まれません。スイッチでゾーンを作成し、そのゾーンをゾーン セットに追加する必要があります。

基本モード: ゾーンが基本モードの場合は、次に示すコマンド出力例を参照してください。

1. ゾーンとゾーン セットを作成します。スイッチ 1 でアクティブ化します。

```
Switch1# config t
Enter configuration commands, one per line.End with CNTL/Z.

Switch1#(config)# vsan database
Switch1#(config-vsan-db)# vsan 100
Switch1#(config-vsan-db)# exit

Switch1#(config)# zone name zone1 vsan 100
Switch1#(config-zone)# member pwnn 11:11:11:11:11:11:11:1a
Switch1#(config-zone)# member pwnn 11:11:11:11:11:11:11:1b
Switch1#(config-zone)# exit

Switch1#(config)# zoneset name setA vsan 100
Switch1#(config-zoneset)# member zone1
Switch1#(config-zoneset)# exit
```

```
Switch1#(config)# zoneset activate name setA vsan 100
Zoneset activation initiated.check zone status
Switch1#(config)# exit
```

```
Switch1# sh zoneset active vsan 100
zoneset name setA vsan 100
  zone name zone1 vsan 100
    pwn 11:11:11:11:11:11:11:1a
    pwn 11:11:11:11:11:11:11:1b
Switch1#
```

2. ゾーンとゾーン セットを作成します。スイッチ 2 でアクティブ化します。

```
Switch2# config t
Enter configuration commands, one per line.End with CNTL/Z.
```

```
Switch2#(config)# vsan database
Switch2#(config-vsan-db)# vsan 100
Switch2#(config-vsan-db)# exit
```

```
Switch2#(config)# zone name zone2 vsan 100
Switch2#(config-zone)# member pwn 22:22:22:22:22:22:22:2a
Switch2#(config-zone)# member pwn 22:22:22:22:22:22:22:2b
Switch2#(config-zone)# exit
```

```
Switch2#(config)# zoneset name setB vsan 100
Switch2#(config-zoneset)# member zone2
Switch2#(config-zoneset)# exit
```

```
Switch2#(config)# zoneset activate name setB vsan 100
Zoneset activation initiated.check zone status
Switch2#(config)# exit
```

```
Switch2# sh zoneset active vsan 100
zoneset name setB vsan 100
  zone name zone2 vsan 100
    pwn 22:22:22:22:22:22:22:22
    pwn 22:22:22:22:22:22:22:2b
Switch2#
```

3. ISL リンクを起動し、スイッチ 1 でゾーン マージを確認します。

```
Switch1# config t
Enter configuration commands, one per line.End with CNTL/Z.
Switch1(config)# int fc1/5
Switch1(config-if)# no shut
Switch1(config-if)# exit
Switch1(config)# exit
```



(注) Ensure that vsan 100 is allowed on ISL

```
Switch1# sh zoneset active vsan 100
zoneset name setB vsan 100
  zone name zone1 vsan 100
    pwn 11:11:11:11:11:11:11:1a
    pwn 11:11:11:11:11:11:11:1b
```

```
zone name zone2 vsan 100
  pwwn 22:22:22:22:22:22:22:2a
  pwwn 22:22:22:22:22:22:22:2b
```

```
Switch1# sh zoneset vsan 100
zoneset name setA vsan 100
  zone name zone1 vsan 100
    pwwn 11:11:11:11:11:11:11:1a
    pwwn 11:11:11:11:11:11:11:1b
```

4. ISL リンクを起動し、スイッチ 2 でゾーン マージを確認します。

```
Switch2# config t

Enter configuration commands, one per line.End with CNTL/Z.

Switch2(config)# int fc2/5
Switch2(config-if)# no shut
Switch2(config-if)# exit
Switch2(config)# exit

Switch2# sh zoneset active vsan 100

zoneset name setB vsan 100
  zone name zone1 vsan 100
    pwwn 11:11:11:11:11:11:11:1a
    pwwn 11:11:11:11:11:11:11:1b

  zone name zone2 vsan 100
    pwwn 22:22:22:22:22:22:22:2a
    pwwn 22:22:22:22:22:22:22:2b

Switch2# sh zoneset vsan 100
zoneset name setB vsan 100
  zone name zone2 vsan 100
    pwwn 22:22:22:22:22:22:22:2a
    pwwn 22:22:22:22:22:22:22:2b
```



(注)

新しくマージされたゾーン セットの名前は、アルファベット順で大きな値のゾーン セット名になります。上記の例では、アクティブゾーン セットは setB です。今後ゾーン セットのアクティブ化の問題が発生しないようにするため、この時点でスイッチで **zone copy active-zoneset full-zoneset vsan 100** コマンドを実行する必要があります。このコマンドが実行されるかどうかと、新しいゾーン分割情報の処理方法を確認します。

zone copy コマンドを実行すると、学習したゾーン情報(この例ではゾーン 2)が実行コンフィギュレーションに追加されます。ゾーン 2 がメモリ内から実行コンフィギュレーションにコピーされていない場合、ゾーン 2 情報はプッシュして戻されません。



注意

zone copy コマンドは、FC エイリアス設定をすべて削除します。

Switch1 の実行コンフィギュレーション(「zone copy active-zoneset full-zoneset vsan 100」コマンドの実行前)

```
Switch1# sh run | b "Active Zone Database Section for vsan 100"
!Active Zone Database Section for vsan 100
zone name zone1 vsan 100
    pwnn 11:11:11:11:11:11:11:1a
    pwnn 11:11:11:11:11:11:11:1b

zone name zone2 vsan 100
    pwnn 22:22:22:22:22:22:22:2a
    pwnn 22:22:22:22:22:22:22:2b

zoneset name setB vsan 100
    member zone1
    member zone2

zoneset activate name setB vsan 100
do clear zone database vsan 100
!Full Zone Database Section for vsan 100
zone name zone1 vsan 100
    pwnn 11:11:11:11:11:11:11:1a
    pwnn 11:11:11:11:11:11:11:1b

zoneset name setA vsan 100
    member zone1
```

Switch1 の実行コンフィギュレーション(「zone copy active-zoneset full-zoneset vsan 100」コマンドの実行後)

```
Switch1# zone copy active-zoneset full-zoneset vsan 100
WARNING: This command may overwrite common zones in the full zoneset.Do you want to
continue? (y/n) [n] y

Switch1# sh run | b "Active Zone Database Section for vsan 100"
!Active Zone Database Section for vsan 100
zone name zone1 vsan 100
    pwnn 11:11:11:11:11:11:11:1a
    pwnn 11:11:11:11:11:11:11:1b

zone name zone2 vsan 100
    pwnn 22:22:22:22:22:22:22:2a
    pwnn 22:22:22:22:22:22:22:2b

zoneset name setB vsan 100
    member zone1
    member zone2

zoneset activate name setB vsan 100
do clear zone database vsan 100
!Full Zone Database Section for vsan 100
zone name zone1 vsan 100
    pwnn 11:11:11:11:11:11:11:1a
    pwnn 11:11:11:11:11:11:11:1b

zone name zone2 vsan 100
    pwnn 22:22:22:22:22:22:22:2a
    pwnn 22:22:22:22:22:22:22:2b

zoneset name setA vsan 100
    member zone1
```

```
zoneset name setB vsan 100
  member zone1
  member zone2
```

Switch2 の実行コンフィギュレーション(「zone copy active-zoneset full-zoneset vsan 100」コマンドの実行前)

```
Switch2# sh run | b "Active Zone Database Section for vsan 100"
!Active Zone Database Section for vsan 100
zone name zone2 vsan 100
  pwn 22:22:22:22:22:22:2a
  pwn 22:22:22:22:22:22:2b

zone name zone1 vsan 100
  pwn 11:11:11:11:11:11:1a
  pwn 11:11:11:11:11:11:1b

zoneset name setB vsan 100
  member zone2
  member zone1

zoneset activate name setB vsan 100
do clear zone database vsan 100
!Full Zone Database Section for vsan 100
zone name zone2 vsan 100
  pwn 22:22:22:22:22:22:2a
  pwn 22:22:22:22:22:22:2b

zoneset name setB vsan 100
  member zone2
```

Switch2 の実行コンフィギュレーション(「zone copy active-zoneset full-zoneset vsan 100」コマンドの実行後)

```
Switch2# zone copy active-zoneset full-zoneset vsan 100
WARNING: This command may overwrite common zones in the full zoneset.Do you want to
continue? (y/n) [n] y

Switch2# sh run | b "Active Zone Database Section for vsan 100"
!Active Zone Database Section for vsan 100
zone name zone2 vsan 100
  pwn 22:22:22:22:22:22:2a
  pwn 22:22:22:22:22:22:2b

zone name zone1 vsan 100
  pwn 11:11:11:11:11:11:1a
  pwn 11:11:11:11:11:11:1b

zoneset name setB vsan 100
  member zone2
  member zone1

zoneset activate name setB vsan 100
do clear zone database vsan 100
!Full Zone Database Section for vsan 100
zone name zone2 vsan 100
  pwn 22:22:22:22:22:22:2a
  pwn 22:22:22:22:22:22:2b

zone name zone1 vsan 100
  pwn 11:11:11:11:11:11:1a
  pwn 11:11:11:11:11:11:1b
```



```
zoneset name setB vsan 100
  member zone2
  member zone1
```

設定の3つの要素に戻ると、これらはゾーン マージ前のゾーン 1 では次のようになります。

- 保存済みの設定: `copy run start` コマンドを実行してゾーン情報を保存する操作が行われていないため、何も保存されていません。
- 実行コンフィギュレーション: ゾーン 1 で構成されます。
- 設定および学習された情報: ゾーン 1 で構成されます。

ゾーン マージ後は、これらの要素は次のようになります。

- 保存済みコンフィギュレーション: 何も保存されていません。
- 実行コンフィギュレーション: ゾーン 1 で構成されます。
- 設定および学習された情報: ゾーン 1 とゾーン 2 で構成されます。

ゾーン 2 は実行コンフィギュレーションの一部ではありません。ゾーン 2 は学習され、アクティブゾーン セットに含まれています。学習されたゾーン 2 がコピーされ、実行コンフィギュレーションに追加されるのは、`zone copy active-zoneset full-zoneset vsan 100` コマンドの実行時のみです。このコマンドの実行後のコンフィギュレーションは次のようになります。



注意

`zone copy` コマンドは、FC エイリアス設定をすべて削除します。

- 保存済みコンフィギュレーション: 何も保存されていません。
- 実行コンフィギュレーション: ゾーン 1 とゾーン 2 で構成されます。
- 設定および学習された情報: ゾーン 1 とゾーン 2 で構成されます。

コマンド

基本モードではデフォルトでアクティブゾーン セット データベースだけが配信されます。このコマンドは 1.0.4 SAN-OS で導入されました。アクティブゾーン セットとフルゾーン セット データベースを伝播します。

```
zoneset distribute full vsan <vsan_id>
```

ゾーン更新またはゾーン セット アクティブ化が進行中の場合、上記のコマンドを各スイッチの各 VSAN で明示的に有効にする必要があります。

拡張モード: ゾーンが拡張モードのときは、次に示すコマンド出力例を参照してください。

1. ゾーンとゾーン セットを作成します。Switch1 でアクティブにします。

```
Switch1# config t
Enter configuration commands, one per line.End with CNTL/Z.
Switch1(config)# vsan database
Switch1(config-vsan-db)# vsan 200
Switch1(config-vsan-db)# zone mode enhanced vsan 200
WARNING: This command would distribute the zoning database of this switch throughout the
fabric.Do you want to continue? (y/n) [n] y
Set zoning mode command initiated.Check zone status
Switch1(config-vsan-db)# zone name zone1 vsan 200
Enhanced zone session has been created.Please \qcommit\q the changes when done.
Switch1(config-zone)# member pwn 11:11:11:11:11:11:11:1a
Switch1(config-zone)# member pwn 11:11:11:11:11:11:11:1b
Switch1(config-zone)# zoneset name SetA vsan 200
Switch1(config-zoneset)# member zone1
```

```

Switch1(config-zoneset)# zoneset activate name SetA vsan 200
Switch1(config)# zone commit vsan 200
Commit operation initiated.Check zone status
Switch1(config)# exit
Switch1# show zoneset activate vsan 200
zoneset name SetA vsan 200
  zone name zone1 vsan 200
    pwnn 11:11:11:11:11:11:11:1a
    pwnn 11:11:11:11:11:11:11:1b
Switch1# show zoneset vsan 200
zoneset name SetA vsan 200
  zone name zone1 vsan 200
    pwnn 11:11:11:11:11:11:11:1a
    pwnn 11:11:11:11:11:11:11:1b

```

2. ゾーンとゾーン セットを作成します。Switch2 でアクティブにします。

```

Switch2# config t
Enter configuration commands, one per line.End with CNTL/Z.
Switch2(config)# vsan database
Switch2(config-vsan-db)# vsan 200
Switch2(config-vsan-db)# zone mode enhanced vsan 200
WARNING: This command would distribute the zoning database of this switch throughout the
fabric.Do you want to continue? (y/n) [n] y
Set zoning mode command initiated.Check zone status
Switch2(config)# zone name zone2 vsan 200
Enhanced zone session has been created.Please \qcommit\q the changes when done.
Switch2(config-zone)# member pwnn 22:22:22:22:22:22:22:2a
Switch2(config-zone)# member pwnn 22:22:22:22:22:22:22:2b
Switch2(config-zone)# zoneset name SetB vsan 200
Switch2(config-zoneset)# member zone2
Switch2(config-zoneset)# zoneset act name SetB vsan 200
Switch2(config)# zone commit vsan 200
Commit operation initiated.Check zone status
Switch2(config)# exit
Switch2# show zoneset activate vsan 200
zoneset name SetB vsan 200
  zone name zone2 vsan 200
    pwnn 22:22:22:22:22:22:22:2a
    pwnn 22:22:22:22:22:22:22:2b
Switch2# show zoneset vsan 200
zoneset name SetB vsan 200
  zone name zone2 vsan 200
    pwnn 22:22:22:22:22:22:22:2a
    pwnn 22:22:22:22:22:22:22:2b

```

3. ISL リンクを起動し、Switch1 でゾーン マージを確認します。

```

Switch1# config t
Enter configuration commands, one per line.End with CNTL/Z.
Switch1(config)# interface fc4/1
Switch1(config-if)# no shut
Switch1(config-if)# exit
Switch1(config)# exit

Switch1(config-if)# show zoneset activate vsan 200
zoneset name SetB vsan 200
  zone name zone1 vsan 200
    pwnn 11:11:11:11:11:11:11:1a
    pwnn 11:11:11:11:11:11:11:1b

```

```
zone name zone2 vsan 200
  pwn 22:22:22:22:22:22:22:2a
  pwn 22:22:22:22:22:22:22:2b
```

```
Switch1(config-if)# show zoneset vsan 200
zoneset name SetA vsan 200
  zone name zone1 vsan 200
    pwn 11:11:11:11:11:11:11:1a
    pwn 11:11:11:11:11:11:11:1b

zoneset name SetB vsan 200
  zone name zone2 vsan 200
    pwn 22:22:22:22:22:22:22:2a
    pwn 22:22:22:22:22:22:22:2b
```



(注)

基本モードとは異なり、拡張モードではゾーン データベース全体がマージされ、Switch1 には元々 Switch2 で設定されたゾーン セットの情報が含まれ、Switch2 には元々 Switch1 で設定された情報が含まれます。

4. ISL リンクを起動し、Switch2 でゾーン マージを確認します。

2 つのスイッチ間での ISL の起動後:

```
Switch2# config t
Enter configuration commands, one per line.End with CNTL/Z.
Switch2(config)# interface fc4/1
Switch2(config-if)# no shut
Switch2(config-if)# exit
Switch2(config)# exit
```

```
Switch2(config-zoneset)# show zoneset activate vsan 200
zoneset name SetB vsan 200
  zone name zone2 vsan 200
    pwn 22:22:22:22:22:22:22:2a
    pwn 22:22:22:22:22:22:22:2b

  zone name zone1 vsan 200
    pwn 11:11:11:11:11:11:11:1a
    pwn 11:11:11:11:11:11:11:1b
```

```
Switch2(config-zoneset)# show zoneset vsan 200
zoneset name SetB vsan 200
  zone name zone2 vsan 200
    pwn 22:22:22:22:22:22:22:2a
    pwn 22:22:22:22:22:22:22:2b

zoneset name SetA vsan 200
  zone name zone1 vsan 200
    pwn 11:11:11:11:11:11:11:1a
    pwn 11:11:11:11:11:11:11:1b
```

5. 拡張ゾーンに対して **zone copy** コマンドを実行します。

スイッチ 1

```
Switch1# zone copy active-zoneset full-zoneset vsan 200
WARNING: This command may overwrite common zones in the full zoneset.Do you want to
continue? (y/n) [n] y
Switch1(config-if)# show zoneset activate vsan 200
zoneset name SetB vsan 200
  zone name zone1 vsan 200
```

```

pwwn 11:11:11:11:11:11:1a
pwwn 11:11:11:11:11:11:1b

zone name zone2 vsan 200
  pwwn 22:22:22:22:22:22:2a
  pwwn 22:22:22:22:22:22:2b

Switch1(config-if)# show zoneset vsan 200
zoneset name SetB vsan 200
  zone name zone1 vsan 200
    pwwn 11:11:11:11:11:11:1a
    pwwn 11:11:11:11:11:11:1b

  zone name zone2 vsan 200
    pwwn 22:22:22:22:22:22:2a
    pwwn 22:22:22:22:22:22:2b

```

スイッチ 2

```

Switch2# zone copy active-zoneset full-zoneset vsan 200
WARNING: This command may overwrite common zones in the full zoneset.Do you want to
continue? (y/n) [n] y
Switch2(config-zoneset)# show zoneset activate vsan 200
zoneset name SetB vsan 200
  zone name zone2 vsan 200
    pwwn 22:22:22:22:22:22:2a
    pwwn 22:22:22:22:22:22:2b

  zone name zone1 vsan 200
    pwwn 11:11:11:11:11:11:1a
    pwwn 11:11:11:11:11:11:1b

Switch2(config-zoneset)# show zoneset vsan 200
zoneset name SetB vsan 200
  zone name zone2 vsan 200
    pwwn 22:22:22:22:22:22:2a
    pwwn 22:22:22:22:22:22:2b

  zone name zone1 vsan 200
    pwwn 11:11:11:11:11:11:1a
    pwwn 11:11:11:11:11:11:1b

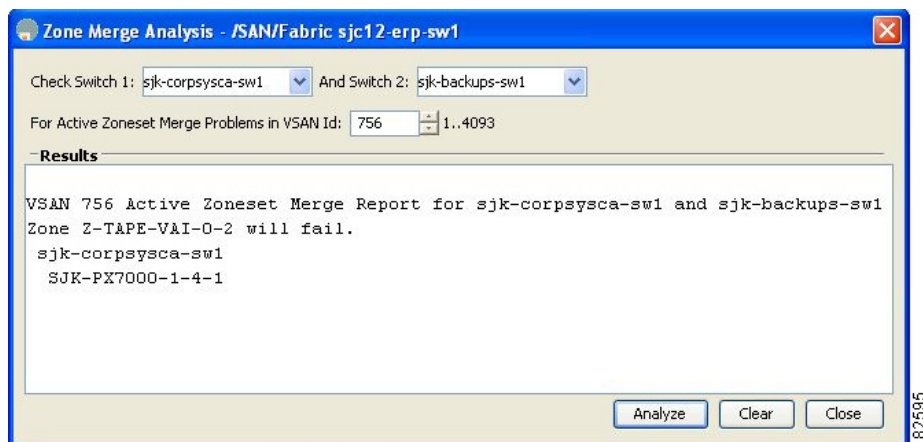
```

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。
 [Zone Merge Analysis] ダイアログボックスが表示されます(図 4-45 を参照)。

図 4-45 [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** [Clear] をクリックして [Zone Merge Analysis] ダイアログボックスから分析データを削除します。

ゾーン マージ制御ポリシーの設定

マージ制御ポリシーを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# zone merge-control restrict vsan 4	現在の VSAN の結合制御設定を「制限」に設定します。
	switch(config)# no zone merge-control restrict vsan 2	現在の VSAN の結合制御設定をデフォルトの「許可」に設定します。
	switch(config)# zone commit vsan 4	VSAN 4 への変更をコミットします。

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

ゾーンによる FC2 バッファのフラッシングの防止

zone fc2 merge throttle enable コマンドを使用して、ゾーンから FC2 に送信されるマージ要求をスロットルし、ゾーンによる FC2 バッファのフラッシングを防止できます。このコマンドは、デフォルトでイネーブルにされています。このコマンドは、多数のゾーンがある場合にゾーンマージの拡張性の問題を防ぐ目的で使用できます。ゾーンマージのスロットル情報を表示するには、**show zone status** コマンドを使用します。

デフォルト ゾーンでのトラフィックの許可または拒否

デフォルト ゾーンでトラフィックを許可または拒否するには、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>switch# config t</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>switch(config)# zone default-zone permit vsan 5</code>	デフォルト ゾーン メンバへのトラフィックフローを許可します。
	<code>switch(config)# no zone default-zone permit vsan 3</code>	デフォルト ゾーン メンバへのトラフィックフローを拒否し、出荷時の設定に戻します。
ステップ 3	<code>switch(config)# zone commit vsan 5</code>	VSAN 5 への変更をコミットします。

ゾーンのブロードキャスト

拡張ゾーンは、このゾーンのメンバーによって生成されたフレームのブロードキャストを、そのゾーン内のメンバーに制限するように指定できます。ホストまたはストレージデバイスがブロードキャストをサポートしている場合に、この機能を使用します。



(注)

broadcast コマンドは 5.x 以降のリリースではサポートされていません。

表 4-6 に、ブロードキャスト フレームの配信規則を示します。

表 4-6 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?
はい	はい	はい
いいえ	はい	はい
はい	いいえ	いいえ
データあり	データなし	成功



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。

拡張ゾーン分割モードでフレームをブロードキャストするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# zone-attribute-group name BroadcastAttr vsan 2	目的の VSAN のゾーン属性グループを設定します。
	switch(config)# no zone-attribute-group name BroadAttr vsan 1	目的の VSAN のゾーン属性グループを削除します。
ステップ 3	switch(config-attribute-group)# broadcast switch(config-attribute-group)# exit switch(config)#	このグループのブロードキャスト属性を作成し、このサブモードを終了します。
	switch(config-attribute-group)# no broadcast	このグループのブロードキャスト属性を削除し、このサブモードを終了します。
ステップ 4	switch(config)# zone name BroadcastAttr vsan 2 switch(config-zone)#	VSAN 2 で BroadcastAttr という名前のゾーンを設定します。
ステップ 5	switch(config-zone)# member pwnn 21:00:00:e0:8b:0b:66:56 switch(config-zone)# member pwnn 21:01:00:e0:8b:2e:80:93 switch(config-zone)# attribute-group name BroadcastAttr switch(config-zone)# exit switch(config)#	指定されたメンバーをこのゾーンに追加し、このサブモードを終了します。
ステップ 6	switch(config)# zone commit vsan 1 Commit operation initiated switch(config)# end	拡張ゾーン設定に変更を適用し、このサブモードを終了します。
ステップ 7	switch# show zone vsan 1 zone name BroadcastAttr vsan 1 zone-attribute-group name BroadcastAttr vsan 1 broadcast pwnn 21:00:00:e0:8b:0b:66:56 pwnn 21:01:00:e0:8b:2e:80:93	ブロードキャスト設定を表示します。

システムのデフォルト ゾーン分割設定値の設定

スイッチ上の新しい VSAN のデフォルトのゾーン ポリシー、フル ゾーン配信、および Generic Service アクセス権限のデフォルト設定を設定できます。スイッチ全体のデフォルト設定を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# system default zone default-zone permit	スイッチ上の新しい VSAN のデフォルト ゾーン分割ポリシーとして permit (許可)を設定します。
	switch(config)# no system default zone default-zone permit	スイッチ上の新しい VSAN のデフォルト ゾーン分割ポリシーとして deny (拒否) (デフォルト)を設定します。

	コマンド	目的
ステップ 3	<code>switch(config)# system default zone distribute full</code>	スイッチ上の新しい VSAN のデフォルトとして、フルゾーンデータベース配信をイネーブルにします。
	<code>switch(config)# no system default zone distribute full</code>	スイッチ上の新しい VSAN のデフォルトとして、フルゾーンデータベース配信をディセーブル(デフォルト)にします。アクティブゾーンデータベースだけが配信されます。
ステップ 4	<code>switch(config)# system default zone gs read</code>	スイッチ上の新しい VSAN のデフォルト Generic Service アクセス権限として読み取り専用を設定します。
	<code>switch(config)# system default zone gs read-write</code>	スイッチ上の新しい VSAN のデフォルト Generic Service アクセス権限として読み取り/書き込み(デフォルト)を設定します。
	<code>switch(config)# no system default zone gs read-write</code>	スイッチ上の新しい VSAN のデフォルト Generic Service アクセス権限としてなし(拒否)を設定します。



(注) VSAN 1 はデフォルト VSAN であり、常にスイッチ上に存在するため、`system default zone` コマンドは VSAN 1 に対しては無効です。

ゾーンの Generic Service アクセス権限の設定

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	<code>switch# config t</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>switch(config)# zone gs read vsan 3000</code>	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。
	<code>switch(config)# zone gs read-write vsan 3000</code>	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。
	<code>switch(config)# no zone gs read-write vsan 3000</code>	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。

拡張ゾーン情報の表示

ゾーン情報を表示するには、**show** コマンドを使用します。例 4-26 ~ 4-37 を参照してください。

例 4-26 指定された VSAN のアクティブゾーンセット情報の表示

```
switch(config)# show zoneset active vsan 1
zoneset name qoscfg vsan 1
  zone name qos1 vsan 1
    * fcid 0xe80200 [pwwn 50:08:01:60:01:5d:51:11]
    * fcid 0xe60000 [pwwn 50:08:01:60:01:5d:51:10]
    * fcid 0xe80100 [pwwn 50:08:01:60:01:5d:51:13]

  zone name qos3 vsan 1
    * fcid 0xe80200 [pwwn 50:08:01:60:01:5d:51:11]
    * fcid 0xe60100 [pwwn 50:08:01:60:01:5d:51:12]
    * fcid 0xe80100 [pwwn 50:08:01:60:01:5d:51:13]

  zone name sb1 vsan 1
    * fcid 0xe80000 [pwwn 20:0e:00:11:0d:10:dc:00]
    * fcid 0xe80300 [pwwn 20:0d:00:11:0d:10:da:00]
    * fcid 0xe60200 [pwwn 20:13:00:11:0d:15:75:00]
    * fcid 0xe60300 [pwwn 20:0d:00:11:0d:10:db:00]
```

例 4-27 指定された VSAN のゾーンセット情報の表示

```
switch(config)# show zoneset vsan 1
zoneset name qoscfg vsan 1
  zone name qos1 vsan 1
    zone-attribute-group name qos1-attr-group vsan 1
      pwwn 50:08:01:60:01:5d:51:11
      pwwn 50:08:01:60:01:5d:51:10
      pwwn 50:08:01:60:01:5d:51:13

  zone name qos3 vsan 1
    zone-attribute-group name qos3-attr-group vsan 1
      pwwn 50:08:01:60:01:5d:51:11
      pwwn 50:08:01:60:01:5d:51:12
      pwwn 50:08:01:60:01:5d:51:13

  zone name sb1 vsan 1
    pwwn 20:0e:00:11:0d:10:dc:00
    pwwn 20:0d:00:11:0d:10:da:00
    pwwn 20:13:00:11:0d:15:75:00
    pwwn 20:0d:00:11:0d:10:db:00
```

例 4-28 指定された VSAN のゾーン属性グループ情報の表示

```
switch# show zone-attribute-group vsan 2
zone-attribute-group name $default_zone_attr_group$ vsan 2
  read-only
  qos priority high
  broadcast
zone-attribute-group name testattgp vsan 2
  read-only
  broadcast
  qos priority high
```

例 4-29 指定された VSAN の FC エイリアス情報の表示

```
switch# show fcalias vsan 2
fcalias name testfcalias vsan 2
  pwwn 21:00:00:20:37:39:b0:f4
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:a6:be:2f
```

例 4-30 指定された VSAN のゾーン ステータスの表示

```
switch(config)# show zone status vsan 1
VSAN: 1 default-zone: deny distribute: active only Interop: default
mode: basic merge-control: allow
session: none
hard-zoning: enabled broadcast: disabled
smart-zoning: disabled
rscn-format: fabric-address
activation overwrite control:disabled
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 4 bytes
Zonesets:0 Zones:0 Aliases: 0
Active Zoning Database :
Database Not Available
Current Total Zone DB Usage: 4 / 2097152 bytes (0 % used)
Pending (Session) DB size:
Full DB Copy size: n/a
Active DB Copy size: n/a
SFC size: 4 / 2097152 bytes (0 % used)
Status:
switch(config)#
```

例 4-31 コミットされる VSAN の保留中のゾーン セット情報の表示

```
switch# show zoneset pending vsan 2
No pending info found
```

例 4-32 コミットされる VSAN の保留中のゾーン情報の表示

```
switch# show zone pending vsan 2
No pending info found
```

例 4-33 コミットされる VSAN の保留中のゾーン情報の表示

```
switch# show zone-attribute-group pending vsan 2
No pending info found
```

例 4-34 コミットされる VSAN の保留中のアクティブゾーン セット情報の表示

```
switch# show zoneset pending active vsan 2
No pending info found
```

例 4-35 指定された VSAN に関する保留中のゾーン情報と有効なゾーン情報の相違点の表示

```
switch# show zone pending-diff vsan 2
zone name testzone vsan 2
- member pwwn 21:00:00:20:37:4b:00:a2
+ member pwwn 21:00:00:20:37:60:43:0c
```

Exchange Switch Support (ESS) は、2 つのスイッチがサポートされている各種機能を交換するためのメカニズムを定義しています(例 4-36 を参照)。

例 4-36 指定された VSAN のすべてのスイッチに関する ESS 情報の表示

```
switch# show zone ess vsan 2
ESS info on VSAN 2 :
Domain : 210, SWWN : 20:02:00:05:30:00:85:1f, Cap1 : 0xf3, Cap2 : 0x0
```

例 4-37 コミットされる VSAN の保留中の FC エイリアス情報の表示

```
switch# show fcalias pending vsan 2
No pending info found
```

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 6.2(7) 以前では、VSAN あたり 8000 ゾーンだけがサポートされます。VSAN に 8000 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があることを示す、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 チェックを避けるには、過剰なゾーンを削除し、VSAN のゾーン データベースをコンパクトにします。超過分のゾーンを削除した後、ゾーン数が 8000 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 6.2(5) 以前によってサポートされます。この手順は、8000 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 8000 を超えるゾーンをサポートしていても、ネイバーがサポートしていない場合、結合は失敗します。また、そのスイッチが VSAN あたり 8000 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 8000 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。

VSAN のゾーンを削除し、ゾーン データベースを圧縮するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# no zone name ExtraZone vsan 10	ゾーンを削除し、ゾーン数を 8000 以下にします。
ステップ 3	switch(config)# zone compact vsan 10	VSAN 10 のゾーン データベースを圧縮し、ゾーンが削除されたときに開放されたゾーン ID を回復します。

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 NX-OS Fabric Configuration Guide』を参照してください。

ゾーンおよびゾーンセットの分析

スイッチ上のゾーンおよびゾーンセットをよりの確に管理するために、**show zone analysis** コマンドを使用して、ゾーン情報とゾーンセット情報を表示できます(例 4-38 ~ 例 4-42 を参照)。

例 4-38 フル ゾーン分割の分析

```
switch# show zone analysis vsan 1
Zoning database analysis vsan 1
Full zoning database
  Last updated at: 15:57:10 IST Feb 20 2006
  Last updated by: Local [ CLI ]
  Num zonesets: 1
  Num zones: 1
  Num aliases: 0
  Num attribute groups: 0
  Formatted size: 36 bytes / 2048 Kb

Unassigned Zones: 1
  zone name z1 vsan 1
```



(注) VSAN あたりのフルゾーン データベースの最大サイズは 4096 KB です。

例 4-39 アクティブ ゾーン分割データベースの分析

```
switch(config-zone)# show zone analysis active vsan 1
Zoning database analysis vsan 1
Active zoneset: qoscfg
  Activated at: 14:40:55 UTC Mar 21 2014
  Activated by: Local [ CLI ]
  Default zone policy: Deny
  Number of devices zoned in vsan: 8/8 (Unzoned: 0)
  Number of zone members resolved: 10/18 (Unresolved: 8)
  Num zones: 4
  Number of IVR zones: 0
  Number of IPS zones: 0
  Formatted size: 328 bytes / 4096 Kb
minishan1(config-zone)#
```



(注) VSAN あたりのゾーン データベースの最大サイズは 4096 KB です。

例 4-40 ゾーンセットの分析

```
switch(config-zone)# show zone analysis zoneset qoscfg vsan 1
Zoning database analysis vsan 1
Zoneset analysis: qoscfg
  Num zonesets: 1
  Num zones: 4
  Num aliases: 0
  Num attribute groups: 1
  Formatted size: 480 bytes / 4096 Kb
minishan1(config-zone)#
```

例 4-41 ゾーン ステータスの表示

```
switch(config-zone)# show zone status
VSAN: 1 default-zone: deny distribute: active only Interop: default
mode: basic merge-control: allow
session: none
hard-zoning: enabled broadcast: disabled
smart-zoning: disabled
rscn-format: fabric-address
activation overwrite control:disabled
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 4 bytes
Zonesets:0 Zones:0 Aliases: 0
Active Zoning Database :
Database Not Available
Current Total Zone DB Usage: 4 / 2097152 bytes (0 % used)
Pending (Session) DB size:
Full DB Copy size: n/a
Active DB Copy size: n/a
SFC size: 4 / 2097152 bytes (0 % used)
Status:

VSAN: 8 default-zone: deny distribute: full Interop: default
mode: basic merge-control: allow
session: none
hard-zoning: enabled broadcast: disabled
smart-zoning: disabled
rscn-format: fabric-address
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 1946498 bytes
Zonesets:6 Zones:8024 Aliases: 0
Active Zoning Database :
DB size: 150499 bytes
Name: zoneset-1000 Zonesets:1 Zones:731
Current Total Zone DB Usage: 2096997 / 2097152 bytes (99 % used)
Pending (Session) DB size:
Full DB Copy size: n/a
Active DB Copy size: n/a
SFC size: 2096997 / 2097152 bytes (99 % used)
Status: Zoneset distribution failed [Error: Fabric changing Dom 33]:
at 17:05:06 UTC Jun 16 2014

VSAN: 9 default-zone: deny distribute: full Interop: default
mode: enhanced merge-control: allow
session: none
hard-zoning: enabled broadcast: enabled
smart-zoning: disabled
rscn-format: fabric-address
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 2002584 bytes
Zonesets:4 Zones:7004 Aliases: 0 Attribute-groups: 1
Active Zoning Database :
DB size: 94340 bytes
Name: zoneset-hac13-200 Zonesets:1 Zones:176
Current Total Zone DB Usage: 2096924 / 2097152 bytes (99 % used)
Pending (Session) DB size:
Full DB Copy size: 0 bytes
Active DB Copy size: 0 bytes
```

```

SFC size: 0 / 2097152 bytes (0 % used)
Status: Activation completed at 17:28:04 UTC Jun 16 2014

VSAN: 12 default-zone: deny distribute: full Interop: default
mode: enhanced merge-control: allow
session: none
hard-zoning: enabled broadcast: enabled
smart-zoning: disabled
rscn-format: fabric-address
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 84 bytes
Zonesets:0 Zones:1 Aliases: 0 Attribute-groups: 1
Active Zoning Database :
DB size: 144 bytes
Name: zsl Zonesets:1 Zones:2
Current Total Zone DB Usage: 228 / 2097152 bytes (0 % used)
Pending (Session) DB size:
Full DB Copy size: 0 bytes
Active DB Copy size: 0 bytes
SFC size: 0 / 2097152 bytes (0 % used)
Status: Commit completed at 14:39:33 UTC Jun 27 201
switch(config)#

```

例 4-42 システムのデフォルトゾーンの表示

```

switch(config)# show system default zone
system default zone default-zone deny
system default zone distribute active only
system default zone mode basic
system default zone gs read-write
system default zone smart-zone disabled

```

コマンドの詳細については、『[Cisco MDS 9000 Family Command Reference](#)』を参照してください。

ゾーンサーバパフォーマンスの強化

次のオプションを使用してゾーンサーバのパフォーマンスを強化できます。

- [ゾーンサーバファイバチャネルネームサーバ共有データベース\(4-94 ページ\)](#)
- [ゾーンサーバSNMP最適化\(4-95 ページ\)](#)
- [ゾーンサーバ差分配信\(4-96 ページ\)](#)

ゾーンサーバファイバチャネルネームサーバ共有データベース

このオプションは、ゾーンサーバとファイバチャネルネームサーバ(FCNS)が相互に通信できるようにするための共有データベースを提供します。データベースを共有すると、ソフトゾーン分割の管理におけるゾーンサーバのFCNSへの依存が軽減されます。



(注) デフォルトでは、ゾーンサーバ - FCNS 共有データベース オプションは有効になっています。

ゾーン サーバ-FCNS 共有データベースの有効化

ゾーン サーバ-FCNS 共有データベースを有効にするには、次の手順を実行します。

- ステップ 1** コンフィギュレーション モードを開始します。

```
switch # configure terminal
```

- ステップ 2** VSAN 1 でアクティブ ゾーン セットのデータベース共有を有効にします。

```
switch(config)# zoneset capability active mode shared-db vsan 1
```

例 4-43 ゾーン サーバ-FCNS 共有データベースの有効化

次に、VSAN 1 でのみアクティブ ゾーン セットのデータベース共有を有効にする例を示します。

```
switch(config)# zoneset capability active mode shared-db vsan 1
SDB Activation success
switch(config)#
```

ゾーン サーバ-FCNS 共有データベースの無効化

VSAN 1 でアクティブ ゾーン セットを無効にするには、次のコマンドを実行します。

```
switch(config)# no zoneset capability active mode shared-db vsan 1
```

例 4-44 ゾーン サーバ-FCNS 共有データベースの無効化

次に、VSAN 1 でアクティブ ゾーン セットのデータベース共有を無効にする例を示します。

```
switch(config)# no zoneset capability active mode shared-db vsan 1
SDB Deactivation success
switch(config)#
```

ゾーン サーバ SNMP 最適化

このオプションでは、Simple Network Management Protocol (SNMP) 操作のためのゾーン サーバ スケーリング拡張が有効になります。これにより、SNMP により実行されるすべてのゾーン クエリーにゾーン サーバが使用されなくなります。



(注) デフォルトでは、ゾーン サーバ SNMP 最適化オプションは有効になっています。

ゾーン サーバ SNMP 最適化の有効化

SNMP 操作のためにゾーン サーバ スケーリング拡張を有効にするには、次の手順を実行します。

- ステップ 1** コンフィギュレーション モードを開始します。

```
switch # configure terminal
```

ステップ 2 ゾーンサーバ SNMP 最適化を有効にします。

```
switch(config)# zone capability shared-db app snmp
```

ステップ 3 設定のステータスを表示します。

```
switch(config)# show running | i shared-db
```

例 4-45 ゾーンサーバ SNMP 最適化の有効化

次に、ゾーンサーバ SNMP 最適化を有効にする例を示します。

```
switch(config)# zone capability shared-db app snmp
```

ゾーンサーバ SNMP 最適化の無効化

ゾーンサーバ SNMP 最適化を無効にするには、次のコマンドを実行します。

```
switch(config)# no zone capability shared-db app snmp
```

例 4-46 ゾーンサーバ SNMP 最適化の無効化

次に、ゾーンサーバ SNMP 最適化を無効にする例を示します。

```
switch(config)# no zone capability shared-db app snmp
```

ゾーンサーバ差分配信

この機能により、既存のゾーンデータベースと更新されたゾーンデータベース間でのゾーン変更の差分を、ファブリック内のすべてのスイッチに配信できます。この差分変更の配信により、ゾーンデータベースが変更されるたびにスイッチ間で大きなペイロードの配信が発生することを回避できます。



(注)

- デフォルトでは、ゾーンサーバ差分配信機能は無効です。この機能は拡張モードでのみ動作します。
- ファブリック内のすべてのスイッチで、ゾーンサーバ差分配信機能が有効になっている必要があります。ゾーンサーバ差分配信機能が無効なファブリックにスイッチを追加すると、ファブリック内のすべてのスイッチでゾーンサーバ差分配信機能が無効になります。
- ゾーンサーバ差分配信機能は Cisco MDS スイッチ (Cisco MDS NX-OS Release 7.3(0)D1(1)以降)でのみサポートされています。
- ゾーンサーバ差分配信機能は、自動音声応答 (IVR) 機能に対応した VSAN では使用できません。

ゾーン サーバ差分配信の有効化

ゾーン サーバでのデータ変更の配信を有効にするには、次の手順を実行します。

ステップ 1 コンフィギュレーション モードを開始します。

```
switch # configure terminal
```

ステップ 2 拡張モードでゾーンのデータ変更の配信を有効にします。

```
switch(config)# zone capability mode enhanced distribution diffs-only
```

ステップ 3 ファブリックの差分配信 (データ変更) ステータスを表示します。

```
switch(config)# show running | include diffs-only
```

例 4-47 ゾーン サーバ差分配信の有効化

次に、ゾーン サーバでのデータ変更の配信を有効にする例を示します。

```
switch(config)# zone capability mode enhanced distribution diffs-only
switch(config)#
```

ゾーン サーバ差分配信の無効化

ゾーンでのデータ変更の配信を無効にするには、次のコマンドを実行します。

```
switch(config)# no zone capability mode enhanced distribution diffs-only
```

例 4-48 ゾーン サーバ差分配信の無効化

次に、ゾーン サーバでデータ変更の配信を無効にする例を示します。

```
switch(config)# no zone capability mode enhanced distribution diffs-only
switch(config)#
```

デフォルト設定

表 4-7 に、基本ゾーン パラメータのデフォルト設定値を示します。

表 4-7 デフォルトの基本ゾーンパラメータ

パラメータ (Parameters)	デフォルト
デフォルト ゾーン ポリシー	すべてのメンバで拒否
フルゾーン セット 配信	フルゾーン セットは配信されない
ゾーン ベースのトラフィック プライオリティ	低。
Broadcast frames	サポート対象外
拡張ゾーン 分割	ディセーブル
スマート ゾーン 分割	ディセーブル



DDAS

Cisco MDS 9000 ファミリのすべてのスイッチは、仮想ストレージ エリア ネットワーク (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。

この章は、次の項で構成されています。

- [デバイス エイリアスについて \(5-1 ページ\)](#)
- [デバイス エイリアス データベース \(5-7 ページ\)](#)
- [レガシー ゾーン エイリアス設定の変換の概要 \(5-13 ページ\)](#)
- [デバイス エイリアス統計情報のクリア \(5-14 ページ\)](#)
- [デバイス エイリアス設定の確認 \(5-15 ページ\)](#)
- [デフォルト設定 \(5-17 ページ\)](#)

デバイス エイリアスについて

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 pWWN 名を定義し、必要に応じて、この名前をすべてのコンフィギュレーション 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 エイリアスのモード

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 エイリアスが基本モードで実行されると、すべてのアプリケーションは、3.0 スイッチ上のアプリケーションと似た方法で機能します。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入れます。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に必要な処理を行います。

ネイティブデバイスエイリアス設定は、interopモードのVSANでは受け入れられません。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。

- デバイスエイリアスが基本モードである場合にデバイスエイリアスメンバーをゾーンに追加しようとすると、デバイスエイリアスメンバーではなくpWWNメンバーとして追加されます。したがって、デバイスエイリアスエントリのpWWNを変更しても、これは更新されません。そのデバイスエイリアスが含まれているゾーンを手動で編集し、古いエントリを削除して同じデバイスエイリアスでゾーンを再設定してから、ゾーンをアクティブにする必要があります。この更新は、拡張デバイスエイリアスモードで行われます。このモードでは、設定がネイティブ形式で受け付けられるため、デバイスエイリアスのpWWNが変更されると、そのデバイスエイリアスが含まれているゾーンが新しいpWWNで自動的に更新されます。

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、対応する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ペ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。

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後では、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差分限定配信

Cisco MDS NX-OS リリース 7.3(0)D1(1) 以降、Cisco MDS スイッチではデバイスエイリアス差分限定配信機能がサポートされています。

この機能がファブリック内のすべてのスイッチで有効な場合は、ファブリック内でデータベース全体ではなくセッションコマンドだけが送信されます。これにより、拡張性が向上します。

ファブリック内のすべてのスイッチでデバイスエイリアス差分限定配信機能が有効な場合、DDAS では 20,000 エントリに対応できます。この機能はデフォルトで有効になっている点に注意してください。



(注) ファブリック内のすべてのスイッチで Cisco MDS NX-OS Release 7.3(0)D1(1) が稼働しており、デバイスエイリアス差分限定配信機能が有効であることを確認してください。

デバイスエイリアス差分限定配信の設定

デバイスエイリアス差分限定配信機能を設定するには、次の手順を実行します。

ステップ 1 コンフィギュレーション モードを開始するため、次のコマンドを入力します。

```
switch# configure terminal
```

ステップ 2 スイッチで差分限定配信を有効にするため、次のコマンドを使用します。

```
switch(config)# device-alias distribute diffs-only
```

差分限定配信を無効にするには、次のコマンドを使用します。

```
switch(config)# no device-alias distribute diffs-only
```

例 5-1 デバイスエイリアス差分限定配信の有効化

次に、スイッチでデバイスエイリアス差分限定配信機能を有効にし、この機能のステータスを表示する例を示します。

```
switch(config)# device-alias distribute diffs-only
switch(config)# show device-alias status
Fabric Distribution: Enabled
Diffs-only Distribution: Enabled
Database:- Device Aliases 1 Mode: Basic
Checksum: 0x43a9fe35852e91354543d712c3ec9d3
```

例 5-2 デバイスエイリアス差分限定配信の無効化

次に、スイッチでデバイスエイリアス差分限定配信機能を無効にし、この機能のステータスを表示する例を示します。

```
switch(config)# no device-alias distribute diffs-only
switch(config)# show device-alias status
Fabric Distribution: Enabled
Diffs-only Distribution: Disabled
Database:- Device Aliases 1 Mode: Basic
Checksum: 0x43a9fe35852e91354543d712c3ec9d3
```

例 5-3 デバイスエイリアス差分限定配信ステータスの表示

次に、ファブリックとスイッチでデバイスエイリアス差分限定配信機能が有効である場合に、アクティブセッション中のデバイスエイリアスのステータスを表示する例を示します。

```
switch(config-device-alias-db)# show device-alias status
Fabric Distribution: Enabled
Diffs-only Distribution: Disabled
Database:- Device Aliases 0 Mode: Basic
Checksum: 0xf6bd6b3389b87233d462029172c8612
Locked By:- User "CLI/SNMPv3:admin" SWWN 20:00:54:7f:ee:1c:2d:40
Pending Database:- Device Aliases 1 Mode: Basic
Diffs-only Distribution capability in the fabric: Enabled
Diffs-only distribution in Session: Enabled
```

次に、ファブリックとスイッチでデバイスエイリアス差分限定配信機能が無効である場合に、アクティブセッション中のデバイスエイリアスのステータスを表示する例を示します。

```
switch(config-device-alias-db)# show device-alias status
Fabric Distribution: Enabled
Diffs-only Distribution: Disabled
Database:- Device Aliases 0 Mode: Basic
Checksum: 0xf6bd6b3389b87233d462029172c8612
Locked By:- User "CLI/SNMPv3:admin" SWWN 20:00:54:7f:ee:1c:2d:40
Pending Database:- Device Aliases 1 Mode: Basic
Diffs-only Distribution capability in the fabric: Disabled
SWWN which doesnot support Diffs-only Distribution:
20:00:54:7f:ee:1c:2d:40
20:00:54:7f:e1:1c:2c:40
Diffs-only distribution in Session: Disabled
```



(注) セッション中は、*Diffs-only distribution in session* のステータスは変化しません。

差分限定配信機能が有効なデバイスエイリアスのマージ

次の状況では、デバイスエイリアスのマージが失敗します。

- 12,000 を超えるエントリが設定されており、デバイスエイリアス差分限定配信機能が有効なスイッチを、この機能をサポートしていないファブリックに追加する場合。
- デバイスエイリアス差分限定配信機能が無効なスイッチを、12,000 を超えるエントリが設定されており、デバイスエイリアス差分限定配信機能が有効なファブリックに追加する場合。

例 5-4 マージ失敗の表示

次に、ファブリックの1つで12,000 を超えるエントリがサポートされていない場合にデバイスエイリアスのマージに失敗する例を示します。

```
switch(config)# show cfs merge status name device-alias

Physical-fc Merge Status: Failed [ Wed Jan 20 10:00:34 2016 ]
Failure Reason: One of the merging fabrics cannot support more than 12Kdevice-aliases
```



(注) 12,000 を超えるデバイス エイリアス エントリをサポートするには、ファブリック内のすべてのスイッチで差分限定配信機能を有効にする必要があります。ファブリック内のすべてのスイッチで差分限定配信機能が有効になっていない場合は、12,000 を超えるエントリを設定しないことを推奨します。

さまざまなモードのデバイス エイリアスのマージ

2つのファブリックが異なるデバイス エイリアス モードで稼働している場合は、デバイス エイリアスのマージが失敗します。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ポートが稼働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。

拡張ファブリックで実行されているアプリケーションに、ネイティブ デバイス エイリアス設定がある場合は、他のファブリックがネイティブ デバイス エイリアススペースの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。

同じファブリック内にある複数のスイッチでデバイス エイリアス データベースの不一致がある場合、次の問題が発生します。

pWWN に関連付けられているデバイス エイリアスのメンバーがスイッチに存在しない場合でも、そのデバイス エイリアスがポート セキュリティ/DPVM データベースに含まれている。pWWN に関連付けられているデバイス エイリアスのメンバーがスイッチに存在している場合でも、そのデバイス エイリアスがポート セキュリティ/DPVM データベースに含まれていない。

マージ失敗およびデバイス エイリアス モード不一致の解決

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られ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 を追加し、設定の削除後に 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、次のような特徴があります。

- 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 データベースとは無関係です。
- データを失うことなく、従来のゾーン エイリアス設定をインポートできます。
- デバイスエイリアスアプリケーションは Cisco Fabric Services (CFS) インフラストラクチャを使用して、効率的なデータベースの管理および配布を実現します。デバイスエイリアス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、次の要件があります。

- デバイスエイリアスを割り当てることができるのは pWWN だけです。
- pWWN と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には、最大 64 文字の英数字を使用でき、次の文字を1つまたは複数加えることができます。
 - a～z および A～Z
 - 1～9
 - -(ハイフン) および _(アンダースコア)
 - \$(ドル記号) および ^ (キャレット) 記号



(注) デバイスエイリアス名の長さが 64 文字の場合、DPVM とその他のアプリケーション データベースが適切に更新されません。デバイスエイリアス名の長さを 63 文字に制限してください。

ゾーンエイリアスとデバイスエイリアスの比較

表 5-1 に、ゾーンベースのエイリアス設定とデバイスエイリアス設定の違いを示します。

表 5-1 ゾーンエイリアスとデバイスエイリアスの比較

ゾーンベースのエイリアス	デバイスエイリアス
エイリアスは指定した VSAN に限定されます。	VSAN 番号を指定せずにデバイスエイリアスを定義できます。また、同一の定義を何の制約もなく 1 つまたは複数の VSAN で使用できます。
ゾーンエイリアスは、ゾーン分割設定の一部です。他の機能の設定にはエイリアスマッピングを使用できません。	pWWN を使用するすべての機能にデバイスエイリアスを使用できます。
エンドデバイスを指定するのにすべてのゾーンメンバタイプを使用できます。	pWWN 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ていません。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。
show zoneset active、show flogi database、show fcns database などの show コマンドの出力には、FC エイリアスは関連付けられている WWN と共に表示されません。	show zoneset active、show flogi database、show fcns database などの show コマンドの出力には、デバイスエイリアスは関連付けられている WWN と共に表示されます。
FC エイリアスはアクティブゾーンセットの一部として配信されず、FC 標準に基づき完全なゾーンデータベースの一部としてのみ配信されます。	デバイスエイリアスは CFS を介して配信されます。

デバイスエイリアスデータベース

デバイスエイリアス機能は 2 つのデータベースを使用して、デバイスエイリアス設定を受け入れ、実装します。

- 有効なデータベース: ファブリックが現在使用しているデータベース
- 保留中のデータベース: 保留中のデバイスエイリアス設定の変更は保留中のデータベースに保存されます。

デバイスエイリアス設定を変更する場合、変更している間はファブリックがロックされたままの状態なので、変更をコミットまたは廃棄する必要があります。

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の作成 \(5-8 ページ\)](#)
- [デバイスエイリアス配信の概要 \(5-8 ページ\)](#)
- [デバイスエイリアスの作成の概要 \(5-9 ページ\)](#)
- [デバイスエイリアス設定のベストプラクティスの概要 \(5-9 ページ\)](#)
- [変更のコミット \(5-10 ページ\)](#)
- [変更の廃棄 \(5-11 ページ\)](#)
- [レガシーゾーンエイリアス設定の変換の概要 \(5-13 ページ\)](#)
- [デバイスエイリアス配信の無効化と有効化 \(5-12 ページ\)](#)

デバイスエイリアスの作成

保留データベースにデバイスエイリアスを作成する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# device-alias database switch(config-device-alias-db)#	保留データベースコンフィギュレーションサブモードを開始します。
ステップ 3	switch(config-device-alias-db)# device-alias name Device1 pwwn 21:01:00:e0:8b:2e:80:93	pWWN によって識別されるデバイスのデバイス名 (Device1) を指定します。これが最初に入力されたデバイスエイリアスコンフィギュレーション コマンドであるため、保留データベースへの書き込みを開始し、同時にファブリックをロックします。
	switch(config-device-alias-db)# no device-alias name Device1	pWWN によって識別されるデバイスのデバイス名 (Device1) を削除します。
	switch(config-device-alias-db)# device-alias rename Device1 Device2	既存のデバイスエイリアス (Device1) を新しい名前 (Device2) に変更します。

デバイスエイリアス設定を表示するには、**show device-alias name** コマンドを使用します。

```
switch# show device-alias name x
device-alias name x pwwn 21:01:00:e0:8b:2e:80:93
```

デバイスエイリアス配信の概要

デフォルトでは、デバイスエイリアスの配布はイネーブルになっています。デバイスエイリアス機能は、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。

変更をコミットしていない状態で配布をディセーブルにすると、コミット作業は失敗します。

例 5-5 失敗ステータスの表示

```
switch# show device-alias status
Fabric Distribution: Disabled
Database:- Device Aliases 25
Status of the last CFS operation issued from this switch:
=====
Operation: Commit
Status: Failed (Reason: Operation is not permitted as the fabric distribution is
currently disabled.)
```



(注)

Cisco MDS NX-OS Release 6.2.9 以降では、**write erase** コマンドを使用しない場合、DDAS (分散デバイスエイリアス サービス) の ASCII 設定の再生に長い時間がかかります。

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。

- 他のユーザがこの機能の設定に変更を加えることができなくなります。
- 有効なデータベースのコピーが取得され、保留データベースとして使用されます。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設定のベストプラクティスの概要

デバイスエイリアス設定のベストプラクティスの一部として、デバイスエイリアスセッションでは次のガイドラインを取り入れる必要があります。

rename コマンドの設定時にデバイスエイリアス名を再利用する場合、コマンドが失敗し、拒否リストに移動されます。

例 5-6 拒否された `device-alias` コマンドの表示

```
switch(config-device-alias-db)# device-alias name dev10 pwnn 10:10:10:10:10:10:10:10
switch(config-device-alias-db)# device-alias rename dev10 new-dev10
Command rejected.Device-alias reused in current session :dev10
Please use 'show device-alias session rejected' to display the rejected set of commands
and for the device-alias best-practices recommendation.
switch(config-device-alias-db)#
```

add または **delete** コマンドの設定時に PWWN を再利用する場合、コマンドが失敗し、拒否リストに移動されます。

例 5-7 拒否された `device-alias` コマンドの表示

```
switch(config-device-alias-db)# device-alias name dev11 pwnn 11:11:11:11:11:11:11:11
switch(config-device-alias-db)# no device-alias name dev11
Command rejected.Pwnn reused in current session: 11:11:11:11:11:11:11:11 is mapped to
device-alias dev11
Please use 'show device-alias session rejected' to display the rejected set of commands
and for the device-alias best-practices recommendation.
switch(config-device-alias-db)#
```

以前に **rename** コマンドで名前が変更されたデバイスエイリアス名を **add** コマンドで再利用する場合、コマンドが失敗し、拒否リストに移動されます。

```
switch(config-device-alias-db)# device-alias rename da3 new-da3
switch(config-device-alias-db)# device-alias name da3 pwnn 2:2:2:2:3:3:3:3
Command rejected.Device-alias name reused in current session: da3
Please use 'show device-alias session rejected' to display the rejected set of commands
and for the device-alias best-practices recommendation.
switch(config-device-alias-db)#
```

例 5-8 拒否された device-alias コマンドの表示

拒否されたコマンドのセットを表示するには、**show device-alias session rejected** コマンドを使用します。

```
switch(config-device-alias-db)# show device-alias session rejected
To avoid command rejections, within a device alias session
Do not reuse:
a) a device alias name while configuring a rename command
b) a PWWN while configuring an add or delete command
c) a device alias name already renamed while configuring add command

Rejected commands must be committed in a separate device alias session
which may cause traffic interruption for those devices. Plan accordingly.
Refer to this command in the NX-OS Command Reference Guide
for more information about device alias configuration best practices

Rejected Command List
-----
device-alias rename dev10 new-dev10
no device-alias name dev11
device-alias name da3 pwn 02:02:02:02:03:03:03:03
switch(config-device-alias-db)# #
```

変更のコミット

保留中のデータベースに行われた変更内容をコミットした場合、次のイベントが発生します。

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. 保留中のデータベースの内容が空になります。
3. ファブリック ロックがこの機能に対して解除されます。

変更をコミットするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# device-alias commit	現在アクティブなセッションに対する変更をコミットします。

ファブリック内のスイッチがロックされ、ブランク コミットになるたびに、次の警告が表示されます。

```
WARNING: Device-alias DB is empty in this switch.
Initiating a commit from this switch will clear [wipe out] Device-alias DB across all the
switches in the fabric, losing Device-alias full DB config permanently.
Do you want to continue? (y/n) [n]
```



(注)

「**device-alias commit**」が完了すると、デバイスエイリアス配信に参加しているすべてのスイッチで実行コンフィギュレーションが変更されます。その後、**copy running-config startup-config fabric** コマンドを使用して、ファブリック内のすべてのスイッチ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保存できます。

デバイスエイリアスの保留中差分表示の有効化

device-alias commit 実行時の保留中差分の表示とその後の確認を有効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# device-alias confirm-commit	デバイスエイリアスの confirm commit オプションを有効にします。
ステップ 3	switch(config)# device-alias commit The following device-alias changes are about to be committed + device-alias name Device1 pwwn 21:01:00:e0:8b:2e:80:93 Do you want to continue? (y/n) [n] y	device-alias confirm-commit コマンドが有効な場合、保留中のデータベースがコミットされると、コンソールに保留中差分が表示され、ユーザに対し [Yes] または [No] を選択するよう求めるプロンプトが表示されます。 device-alias confirm-commit コマンドが無効な場合は、保留中差分は表示されず、ユーザに対して [Yes] または [No] の選択は求められません。

変更の廃棄

保留中のデータベースで行われた変更内容を廃棄した場合、次のイベントが発生します。

1. 有効なデータベースの内容は影響を受けません。
2. 保留中のデータベースの内容が空になります。
3. ファブリック ロックがこの機能に対して解除されます。

デバイスエイリアスセッションを廃棄する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# device-alias abort	現在アクティブなセッションを廃棄します。

廃棄操作のステータスを表示するには、show device alias status コマンドを使用します。

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

ファブリックのロックの上書き

ユーザがデバイスエイリアス作業を行ったが、変更のコミットや廃棄を行ってロックを解除するのを忘れていた場合、管理者はファブリック内の任意のスイッチからロックを解除できます。管理者がこの操作を行うと、ユーザによる保留データベースの変更は廃棄され、ファブリックのロックは解除されます。



ヒント

変更は `volatile` ディレクトリだけで使用でき、スイッチを再起動すると廃棄されます。

デバイスエイリアスセッションをクリアするには、CONFIGURATION モードで `clear device-alias session` コマンドを使用します。

```
switch(config)# clear device-alias session
```

クリア操作のステータスを確認するには、`show device-alias session status` コマンドを使用します。

```
switch(config)# show device-alias session status
Last Action Time Stamp      : None
Last Action                  : None
Last Action Result          : None
Last Action Failure Reason  : none
```

データベースの内容のクリア

すべてのデータベースの内容をクリアするには、CONFIGURATION モードで `clear device-alias database` コマンドを使用します。

```
switch(config)# clear device-alias database
```

`clear device-alias database` コマンドのステータスを確認するには、`show device-alias database` コマンドを使用します。

```
switch(config)# show device-alias database
```

統計情報のクリア

すべての統計情報をクリアするには、CONFIGURATION モードで `clear device-alias statistics` コマンドを使用します。

```
switch# clear device-alias statistics
```

デバイスエイリアス配信の無効化と有効化

デバイスエイリアスの配信をディセーブルまたはイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	<code>switch# config t</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>switch(config)# no device-alias distribute</code>	配布をディセーブルにします。
	<code>switch(config)# device-alias distribute</code>	配布をイネーブルにします(デフォルト)。

デバイスエイリアス配信のステータスを表示するには、**show device-alias status** コマンドを使用します(例 5-9 および例 5-10 を参照)。

例 5-9 配信が有効な場合のデバイスエイリアスステータスの表示

```
switch# show device-alias status
Fabric Distribution: Enabled <-----配信の有効化
Database:-Device Aliases 24
Locked By:-User "Test" SWWN 20:00:00:0c:cf:f4:02:83<-ロック所有者のユーザ名とスイッチ ID
Pending Database:- Device Aliases 24
Status of the last CFS operation issued from this switch:
=====
Operation: Enable Fabric Distribution
Status: Success
```

例 5-10 配信がディセーブルの場合のデバイスエイリアスステータスの表示

```
switch# show device-alias status
Fabric Distribution: Disabled
Database:- Device Aliases 24
Status of the last CFS operation issued from this switch:
=====
Operation: Disable Fabric Distribution
Status: Success
```

レガシーゾーンエイリアス設定の変換の概要

次の制約事項を満たす場合、レガシーゾーンエイリアス設定をインポートし、データを失うことなくこの機能を使用できます。

- 各ゾーンエイリアスには、メンバが1つだけあります。
- メンバのタイプはpWWNです。
- 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。

インポート操作が終了し、**commit** 操作を行うと、変更されたエイリアスデータベースが物理ファブリック内のほかのすべてのスイッチに配布されます。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。

この項では、次のトピックについて取り上げます。

- [ゾーンエイリアスのインポート \(5-14 ページ\)](#)
- [デバイスエイリアス統計情報のクリア \(5-14 ページ\)](#)

ゾーンエイリアスのインポート

特定の VSAN のゾーンエイリアスをインポートするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# device-alias import fcalias vsan 3	指定された VSAN の fcalias 情報をインポートします。

ゾーンセットのデバイスエイリアス情報を表示するには、**show zoneset** コマンドを使用します (例 5-11 および例 5-12 を参照)。

例 5-11 ゾーンセット情報のデバイスエイリアスの表示

```
switch# show zoneset
zoneset name s1 vsan 1
  zone name z1 vsan 1
    pwwn 21:01:00:e0:8b:2e:80:93 [x] <-----pWWN ごとに表示されるデバイスエイリアス
    pwwn 21:00:00:20:37:39:ab:5f [y]
  zone name z2 vsan 1
    pwwn 21:00:00:e0:8b:0b:66:56 [SampleName]
    pwwn 21:00:00:20:37:39:ac:0d [z]
```

例 5-12 アクティブゾーンセットのデバイスエイリアスの表示

```
switch# show zoneset active
zoneset name s1 vsan 1
  zone name z1 vsan 1
    * fcid 0x670100 [pwwn 21:01:00:e0:8b:2e:80:93] [x]
    pwwn 21:00:00:20:37:39:ab:5f [y]

  zone name z2 vsan 1
    * fcid 0x670200 [pwwn 21:00:00:e0:8b:0b:66:56] [SampleName]
    pwwn 21:00:00:20:37:39:ac:0d [z]
```

デバイスエイリアス統計情報のクリア

(デバッグ目的で)デバイスエイリアス統計情報をクリアするには、**clear device-name statistics** コマンドを使用します。

```
switch# clear device-alias statistics
```


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結合する場合は、次の注意事項に従ってください。

- 名前が異なる2つのデバイスエイリアスが同一のpWWNにマッピングされていないことを確認します。
- 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合計数が、Cisco MDS SAN-OS Release 3.0(x)以前が稼働しているファブリックでは8191個(8000)、SAN-OS Release 3.1(x)以降が稼働しているファブリックでは20,000を超えていないことを確認します。デバイスエントリの合計数がサポートされる制限値を超えた場合、マージは失敗します。
- マージ対象の両方のファブリックで類似のデバイスエイリアスモードであることを確認します。

デバイスエイリアス設定の確認

デバイスエイリアス情報を表示するには、`show device-alias` コマンドを使用します。例 5-13 ~ 5-24 を参照してください。

例 5-13 有効なデータベースの設定されているすべてのデバイスエイリアスの表示

```
switch# show device-alias database
device-alias name SampleName pwwn 21:00:00:e0:8b:0b:66:56
device-alias name x pwwn 21:01:00:e0:8b:2e:80:93

Total number of entries = 2
```

例 5-14 変更のない保留中のデータベースの表示

```
switch# show device-alias database pending
There are no pending changes
```

例 5-15 変更された保留中のデータベースの表示

```
switch# show device-alias database pending
device-alias name x pwwn 21:01:00:e0:8b:2e:80:93
device-alias name SampleName pwwn 21:00:00:e0:8b:0b:66:56
device-alias name y pwwn 21:00:00:20:37:39:ab:5f
device-alias name z pwwn 21:00:00:20:37:39:ac:0d

Total number of entries = 4
```

例 5-16 保留中のデータベースの指定されたデバイス名の表示

```
switch# show device-alias name x pending
device-alias name x pwwn 21:01:00:e0:8b:2e:80:93
```

例 5-17 保留中のデータベースの指定された pWWN の表示

```
switch# show device-alias pwwn 21:01:00:e0:8b:2e:80:93 pending
device-alias name x pwwn 21:01:00:e0:8b:2e:80:93
```

例 5-18 保留中のデータベースと有効なデータベースの差異の表示

```
switch# show device-alias database pending-diff
- device-alias name Doc pwwn 21:01:02:03:00:01:01:01
+ device-alias name SampleName pwwn 21:00:00:e0:8b:0b:66:56
```

例 5-19 指定された pWWN の表示

```
switch# show device-alias pwwn 21:01:01:01:01:11:01:01
device-alias name Doc pwwn 21:01:01:01:01:11:01:01
```

例 5-20 FLOGI データベースのデバイスエイリアスの表示

```
switch# show flogi database
-----
INTERFACE  VSAN      FCID          PORT NAME          NODE NAME
-----
fc2/9      1         0x670100     21:01:00:e0:8b:2e:80:93  20:01:00:e0:8b:2e:80:93
           [x] <-----デバイスエイリアス名
fc2/12     1         0x670200     21:00:00:e0:8b:0b:66:56  20:00:00:e0:8b:0b:66:56
           [SampleName] <-----デバイスエイリアス名

Total number of flogi = 2
```

例 5-21 FCNS データベースのデバイスエイリアスの表示

```
switch# show fcns database

VSAN 1:
-----
FCID      TYPE  PWWN          (VENDOR)          FC4-TYPE:FEATURE
-----
0x670100  N    21:01:00:e0:8b:2e:80:93 (Qlogic)          scsi-fcp:init
           [x]
0x670200  N    21:00:00:e0:8b:0b:66:56 (Qlogic)          scsi-fcp:init
           [SampleName]

Total number of entries = 2
```

例 5-22 指定デバイスエイリアスの fcping 統計情報の表示

```
switch# fcping device-alias x vsan 1
28 bytes from 21:01:00:e0:8b:2e:80:93 time = 358 usec
28 bytes from 21:01:00:e0:8b:2e:80:93 time = 226 usec
28 bytes from 21:01:00:e0:8b:2e:80:93 time = 372 usec
```

例 5-23 指定デバイス エイリアスの fctrace 情報の表示

```
switch# fctrace device-alias x vsan 1
Route present for : 21:01:00:e0:8b:2e:80:93
20:00:00:05:30:00:4a:e2(0xffffc67)
```

デバイス エイリアスは、使用可能な場合、**device-alias** コマンドまたはゾーン固有の **member pwwn** コマンドを使用して設定されるメンバーに関係なく表示されます(例 5-11 と例 5-12 を参照)。

例 5-24 デバイス エイリアス アプリケーションの統計情報の表示

```
switch# show device-alias statistics
Device Alias Statistics
=====
Lock requests sent: 2
Database update requests sent: 1
Unlock requests sent: 1
Lock requests received: 1
Database update requests received: 1
Unlock requests received: 1
Lock rejects sent: 0
Database update rejects sent: 0
Unlock rejects sent: 0
Lock rejects received: 0
Database update rejects received: 0
Unlock rejects received: 0
Merge requests received: 0
Merge request rejects sent: 0
Merge responses received: 2
Merge response rejects sent: 0
Activation requests received: 0
Activation request rejects sent: 0
Activation requests sent: 2
Activation request rejects received: 0
```

デフォルト設定

表 5-2 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 5-2 デフォルトのデバイス エイリアス パラメータ

パラメータ(Parameters)	デフォルト
使用中のデータベース	有効なデータベース
変更を受け入れるデータベース	保留中のデータベース
デバイス エイリアス ファブリック ロックの状態	最初のデバイス エイリアス作業でロックされる



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。特殊な考慮事項を必要とする設定を除き、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。同等な 2 つのパスが使用可能な場合は、推奨ルートが提供されます。

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について説明します。内容は次のとおりです。

- [FSPF の概要 \(6-1 ページ\)](#)
- [FSPF のグローバル設定 \(6-4 ページ\)](#)
- [FSPF のインターフェイスでの設定 \(6-6 ページ\)](#)
- [FSPF ルート \(6-10 ページ\)](#)
- [順序どおりの配信 \(6-12 ページ\)](#)
- [フロー統計情報の設定 \(6-16 ページ\)](#)
- [デフォルト設定 \(6-21 ページ\)](#)

FSPF の概要

FSPF は、ファイバチャネル ネットワーク内でのルーティング用として、T11 委員会によって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、次の特性および特徴があります。

- 複数パスの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、ホップ単位ルーティングを行います。
- FSPF が稼働するポートは 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 単位で稼働します。ファブリック内の各 VSAN では、この VSAN に設定されたスイッチとの接続が保証されます。
- 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 ステータスを追跡し、各リンクにコストを対応付けます。
- 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。ただし、より強固で、効率的な差分ダイクストラ アルゴリズムを静的に、あるいは動的に選択することができます。VSAN 単位でルートが計算されるため、再コンバージェンス タイムは高速かつ効率的です。

FSPF の例

ここでは、FSPF の利点を示すトポロジおよびアプリケーション例について説明します。

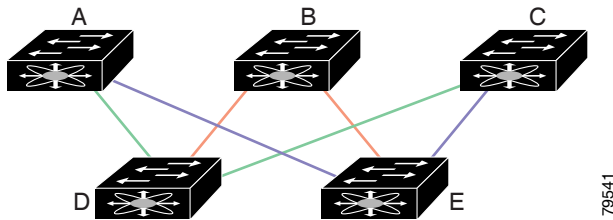


(注) FSPF 機能は任意のトポロジで使用できます。

フォールトトレラント ファブリック

図 6-1 に、部分的メッシュ 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。ファブリック内のどの部分でリンク ダウンが発生しても、各スイッチはファブリック内の他のすべてのスイッチと通信できます。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 6-1 フォールトトレラント ファブリック



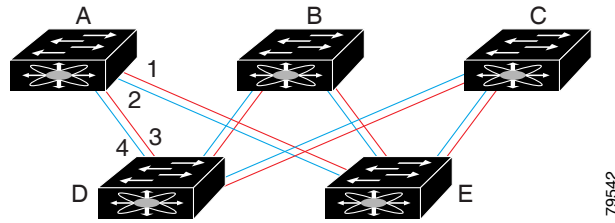
たとえば、すべてのリンク速度が等しい場合、FSPF は A ~ C 2 つの同等なパス (A-D-C [グリーン] と A-E-C [ブルー]) を計算します。

冗長リンク

図 6-1 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 6-2 に、この配置例を示します。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。この設定により、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 6-2 冗長リンクを持つ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、PortChannel 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。PortChannel が存在する場合は、これらのパスが 2 つに削減されます。

PortChannel 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 6-3 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無効にする (表 6-1 を参照)。
- スイッチ 1 またはスイッチ 2 のどちらか一方のリンクをシャットダウンする (表 6-2 を参照)。

図 6-3 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

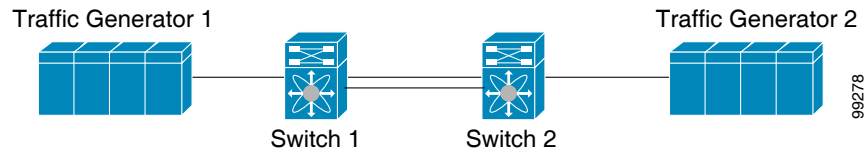


表 6-1 SmartBits ケーブルの物理的取り外しのシナリオ

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 6-2 SmartBits スイッチでのリンク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、タイプミスや、その他の軽微な設定エラーが発生する可能性も低減されます。



(注)

FSPF はデフォルトでイネーブルになっています。通常、これらの高度な機能は設定する必要がありません。



注意

バックボーン リージョンのデフォルトは 0 (ゼロ) です。この設定を変更する必要があるのは、デフォルト以外のリージョンを使用する場合だけです。バックボーン リージョンを使用して別のベンダー製品と併用する場合は、これらの製品の設定と互換性が保たれるようにこのデフォルトを変更できます。

この項では、次のトピックについて取り上げます。

- [SPF 計算ホールド タイムの概要 \(6-4 ページ\)](#)
- [Link State Record のデフォルトの概要 \(6-4 ページ\)](#)
- [VSAN での FSPF の設定 \(6-5 ページ\)](#)
- [FSPF のデフォルト設定へのリセット \(6-5 ページ\)](#)
- [FSPF の有効化または無効化 \(6-6 ページ\)](#)
- [VSAN の FSPF カウンタのクリア \(6-6 ページ\)](#)

SPF 計算ホールド タイムの概要

SPF 計算のホールド タイムは、VSAN での 2 つの連続した SPF 計算間の最小時間に設定されます。これを小さい値に設定すると、VSAN 上のパスの再計算によるファブリックの変更に対して、FSPF の処理が速くなります。SPF 計算のホールド タイムが短いと、スイッチの CPU 時間は長くなります。

Link State Record のデフォルトの概要

ファブリックに新しいスイッチが追加されるたびに、Link State Record (LSR) が近接スイッチに送信されて、ファブリック全体にフラッドイングされます。表 6-3 に、スイッチ応答に関するデフォルト設定を示します。

表 6-3 LSR のデフォルト設定

LSR のオプション	デフォルト	説明
ACK インターバル (RxmtInterval)	5 秒	再送信するまで、スイッチが LSR からの ACK を待機する期間

表 6-3 LSR のデフォルト設定(続き)

LSR のオプション	デフォルト	説明
リフレッシュ タイム (LSRefreshTime)	30 分	LSR リフレッシュを送信するまで、スイッチが待機する期間
最大エージング (MaxAge)	60 分	データベースから LSR を削除するまで、スイッチが待機する期間

LSR の最小着信時間は、この VSAN の LSR アップデートの受信間隔です。LSR の最小着信時間よりも前に着信した LSR アップデートは廃棄されます。

LSR 最小間隔は、このスイッチが VSAN 上の LSR アップデートを送信する頻度です。

VSAN での FSPF の設定

VSAN 全体に FSPF 機能を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# fspf config vsan 1	指定された VSAN に対して FSPF グローバル コンフィギュレーション モードを開始します。
ステップ 3	switch-config-(fspf-config)# spf static	ダイナミック(デフォルト)差分 VSAN に対してスタティック SPF 計算を強制実行します。
ステップ 4	switch-config-(fspf-config)# spf hold-time 10	VSAN 全体に対して、2 つのルート計算間のホールド タイムをミリ秒(msec)単位で設定します。デフォルト値は 0 です (注) 指定期間が短いほど、ルーティングは高速化されます。ただし、それに応じて、プロセッサ消費量が増大します。
ステップ 5	switch-config-(fspf-config)# region 7	現在の VSAN に自律リージョンを設定し、リージョン ID(7)を指定します。

FSPF のデフォルト設定へのリセット

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には、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# no fspf config vsan 3	VSAN 3 の FSPF 設定を削除します。

FSPF の有効化または無効化

FSPF ルーティング プロトコルを有効または無効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# fspf enable vsan 7	VSAN 7 内で FSPF ルーティング プロトコルを有効にします。
	switch(config)# no fspf enable vsan 5	VSAN 5 内で FSPF ルーティング プロトコルを無効にします。

VSAN の FSPF カウンタのクリア

VSAN 全体の FSPF 統計情報カウンタをクリアするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# clear fspf counters vsan 1	指定された VSAN の FSPF 統計情報カウンタをクリアします。インターフェイス参照番号を指定しない場合は、すべてのカウンタがクリアされます。

FSPF のインターフェイスでの設定

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。次に示す設定手順は、特定の VSAN 内の 1 つのインターフェイスに適用されます。

この項では、次のトピックについて取り上げます。

- [FSPF リンク コストの概要 \(6-7 ページ\)](#)
- [FSPF リンク コストの設定 \(6-7 ページ\)](#)
- [hello タイム インターバルの概要 \(6-7 ページ\)](#)
- [hello タイム インターバルの設定 \(6-7 ページ\)](#)
- [デッド タイム インターバルの概要 \(6-8 ページ\)](#)
- [デッド タイム インターバルの設定 \(6-8 ページ\)](#)
- [再送信インターバルの概要 \(6-8 ページ\)](#)
- [再送信インターバルの設定 \(6-9 ページ\)](#)
- [インターフェイス単位での FSPF のディセーブル化 \(6-9 ページ\)](#)
- [特定のインターフェイスに対する FSPF のディセーブル化 \(6-9 ページ\)](#)
- [インターフェイスの FSPF カウンタのクリア \(6-10 ページ\)](#)

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 ステータスを追跡し、データベース内の各リンクにコストを対応付け、コストが最小なパスを選択します。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。コストは、1 ~ 65,535 の整数値で指定できます。1 Gbps のデフォルト コストは 1000 であり、2 Gbps では 500 です。

FSPF リンク コストの設定

FSPF リンク コストを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# interface fc1/4 switch(config-if)#	指定されたインターフェイスを設定します。すでに設定されている場合は、指定されたインターフェイスに対してコンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# fspf cost 5 vsan 90	VSAN 90 の選択されたインターフェイスのコストを設定します。

hello タイム インターバルの概要

FSPF hello タイム インターバルを設定すると、リンク状態を確認するために送信される定期的な hello メッセージの間隔を指定できます。指定できる整数値は 1 ~ 65,535 秒です。



(注) この値は、ISL の両端のポートで同じでなければなりません。

hello タイム インターバルの設定

FSPF の hello タイム インターバルを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# interface fc1/4 switch(config-if)#	指定されたインターフェイスを設定します。すでに設定されている場合は、指定されたインターフェイスに対してコンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# fspf hello-interval 15 vsan 175 switch(config-if)#	VSAN 175 のリンクのヘルスを確認するために、hello メッセージ インターバル (15 秒) を指定します。デフォルトは 20 秒です。

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すると、hello メッセージを受信しなければならない最大間隔を指定できます。この期間が経過すると、ネイバーは消失したと見なされ、データベースから削除されます。指定できる整数値は 1 ~ 65,535 秒です。



(注)

- この値は、ISL の両端のポートで同じでなければなりません。
- 設定したデッド タイム インターバルが hello タイム インターバルより短い場合、コマンドプロンプトでエラーが報告されます。
- ソフトウェア アップグレード中に、fspf デッド インターバルが ISSU ダウンタイム(80 秒)よりも長いことを確認します。fspf デッド インターバルが ISSU ダウンタイムよりも短いと、ソフトウェア アップグレードが失敗し、次のエラー メッセージが表示されます。

エラーメッセージ Service "fspf" returned error: Dead interval for interface is less than ISSU upgrade time.

デッド タイム インターバルの設定

FSPF のデッド タイム インターバルを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# interface fc1/4 switch(config-if)#	指定されたインターフェイスを設定します。すでに設定されている場合は、指定されたインターフェイスに対してコンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# fspf dead-interval 25 vsan 7 switch(config-if)#	VSAN 7 に、選択されたインターフェイスで hello メッセージを受信しなければならない最大間隔を指定します。この期間が経過すると、ネイバーは消失したと見なされます。デフォルトは 80 秒です。

再送信インターバルの概要

インターフェイス上で未確認応答リンク ステート アップデートを送信するまでの期間を指定します。再送信インターバルを指定する整数値の有効範囲は、1 ~ 65,535 秒です。



(注)

この値は、インターフェイスの両端のスイッチで同じでなければなりません。

再送信インターバルの設定

FSPF の再送信タイム インターバルを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# interface fc1/4 switch(config-if)#	指定されたインターフェイスを設定します。すでに設定されている場合は、指定されたインターフェイスに対してコンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# fspf retransmit-interval 15 vsan 12 switch(config-if)#	VSAN 12 における未確認応答リンク状態アップデートの再送信間隔を指定します。デフォルトは 5 秒です。

インターフェイス単位での FSPF のディセーブル化

選択したインターフェイスで FSPF プロトコルをディセーブルにできます。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。このデフォルト設定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) 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で FSPF プロトコルをディセーブルにできます。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。このデフォルト設定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。

特定のインターフェイスに対して FSPF を無効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# interface fc1/4 switch(config-if)#	指定されたインターフェイスを設定します。すでに設定されている場合は、指定されたインターフェイスに対してコンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# fspf passive vsan 1 switch(config-if)#	指定された VSAN 内の特定の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します。
	switch(config-if)# no fspf passive vsan 1 switch(config-if)#	指定された VSAN 内の特定のインターフェイスに対して FSPF プロトコルを再度イネーブルにします。

選択したインターフェイスで FSPF プロトコルをディセーブルにできます。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。このデフォルト設定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。

インターフェイスの FSPF カウンタのクリア

インターフェイスの FSPF 統計情報カウンタをクリアするには、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>switch# clear fspf counters vsan 200 interface fc1/1</code>	VSAN 200 内の指定インターフェイスの FSPF 統計情報カウンタをクリアします。

FSPF ルート

FSPF は、FSPF データベース内のエントリに基づいて、ファブリックを経由する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させるか、または静的に設定することもできます。

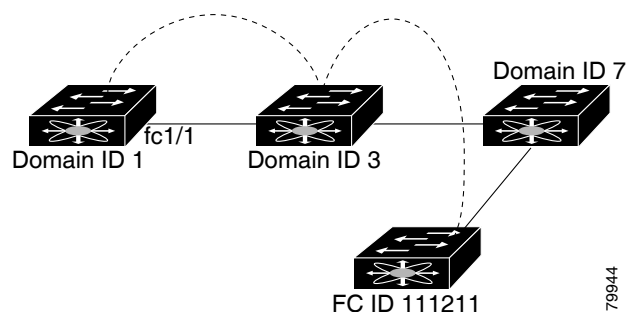
この項では、次のトピックについて取り上げます。

- [ファイバチャネルのルートの概要 \(6-10 ページ\)](#)
- [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 \(6-11 ページ\)](#)
- [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 \(6-11 ページ\)](#)
- [マルチキャスト ルート スイッチの概要 \(6-11 ページ\)](#)
- [マルチキャスト ルート スイッチの設定 \(6-11 ページ\)](#)

ファイバチャネルのルートの概要

各ポートは、FC ID に基づいてフレームを転送する転送ロジックを実行します。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 6-4 を参照)。

図 6-4 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。

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。

主要スイッチから最も小さなドメインスイッチにマルチキャストルートを変更するには、**mcast root lowest vsan** コマンドを使用します。

マルチキャスト ルート スイッチの設定

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には、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# mcast root lowest vsan 1	最も小さなドメイン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。
	switch(config)# mcast root principal vsan 1	デフォルトでは、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。

設定されており稼働しているマルチキャスト モードと選択されたルート ドメインを表示するには、**show mcast** コマンドを使用します。

```
switch# show mcast vsan 1
Multicast root for VSAN 1
    Configured root mode : Principal switch
    Operational root mode : Principal switch
    Root Domain ID : 0xef(239)
```

順序どおりの配信

データ フレームの順序どおりの配信 (IOD) 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、順序外のフレーム配信を処理できません。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 を使用するのには、順序外のフレーム配信をサポートできない環境の場合だけにしてください。



ヒント

順序どおりの配信機能をイネーブルにすると、グレースフル シャットダウン機能は実行されません。

この項では、次のトピックについて取り上げます。

- [ネットワーク フレーム順序の再設定の概要 \(6-13 ページ\)](#)
- [ポート チャネル フレーム順序の再設定の概要 \(6-13 ページ\)](#)
- [順序どおりの配信の有効化の概要 \(6-14 ページ\)](#)
- [順序どおりの配信のグローバルなイネーブル化 \(6-14 ページ\)](#)
- [特定の VSAN に対する順序どおりの配信のイネーブル化 \(6-15 ページ\)](#)
- [順序どおりの配信のステータスの表示 \(6-15 ページ\)](#)
- [ドロップ遅延時間の設定 \(6-15 ページ\)](#)
- [遅延情報の表示 \(6-16 ページ\)](#)

ネットワーク フレーム順序の再設定の概要

ネットワーク内でルートが変更されると、新しく選択されたパスが元のルートよりも高速になったり、輻輳が軽減されたりすることがあります。

図 6-5 ルート変更の配信

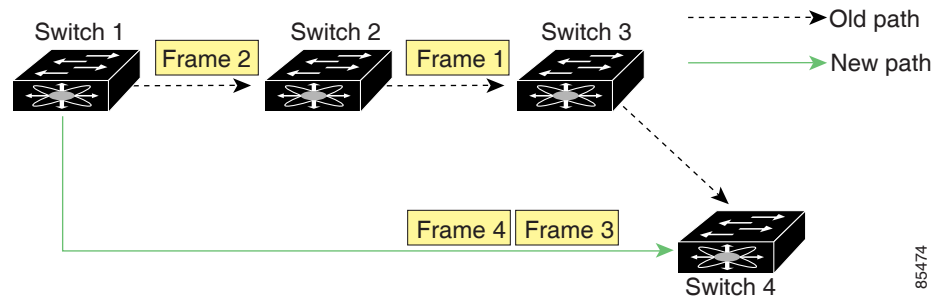


図 6-5 では、スイッチ 1 からスイッチ 4 への新しいパスの方が高速です。したがって、フレーム 3 およびフレーム 4 は、フレーム 1 およびフレーム 2 よりも先に配信されることがあります。

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された順番で配信されます。
- ネットワーク遅延ドロップ期間内に順番どおりに配信できないフレームは、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 6-6 リンクが輻輳している場合の配信

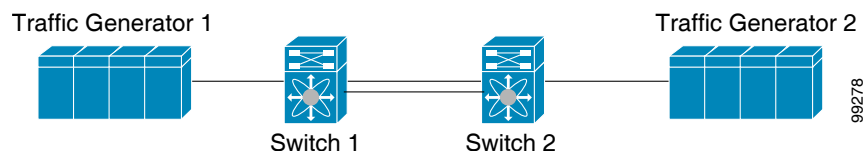


図 6-6 では、元のパス (赤い点線) のポートが輻輳しています。したがって、フレーム 3 およびフレーム 4 は、フレーム 1 およびフレーム 2 よりも先に配信されることがあります。

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) が稼働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が配信されてから、新しいフレームが許可されます。
- 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](#)」セクション(6-15 ページ)を参照してください。

順序どおりの配信の有効化の概要

順序どおりの配信機能は、特定の VSAN またはスイッチ全体に対してイネーブルにできます。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

この機能をイネーブルにするのは、順序に従わないフレームを処理できないデバイスがスイッチに搭載されている場合に限定してください。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、および交換 ID に基づくロードバランシング アルゴリズムをハードウェアで実行しても、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にするのは、ファブリック全体にこの機能が必要な場合だけにしてください。そうでない場合は、この機能を必要とする VSAN に対してだけ IOD をイネーブルにします。



(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。

スイッチで順序どおりの配信を有効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# in-order-guarantee	スイッチ内で順序どおりの配信をイネーブルにします。
	switch(config)# no in-order-guarantee	スイッチを出荷時の設定に戻し、順序どおりの配信機能をディセーブルにします。

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。

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には、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>switch# config t</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>switch(config)# in-order-guarantee vsan 3452</code>	VSAN 3452 の順序どおりの配信を有効にします。
	<code>switch(config)# no in-order-guarantee vsan 101</code>	スイッチを出荷時の設定に戻し、VSAN 101 の順序どおりの配信機能をディセーブルにします。

順序どおりの配信のステータスの表示

現在の設定ステータスを表示するには、`show in-order-guarantee` コマンドを使用します。

```
switch# show in-order-guarantee
global inorder delivery configuration:guaranteed

VSAN specific settings
vsan 1 inorder delivery:guaranteed
vsan 101 inorder delivery:not guaranteed
vsan 1000 inorder delivery:guaranteed
vsan 1001 inorder delivery:guaranteed
vsan 1682 inorder delivery:guaranteed
vsan 2001 inorder delivery:guaranteed
vsan 2009 inorder delivery:guaranteed
vsan 2456 inorder delivery:guaranteed
vsan 3277 inorder delivery:guaranteed
vsan 3451 inorder delivery:guaranteed
vsan 3452 inorder delivery:guaranteed
```

ドロップ遅延時間の設定

ネットワーク、ネットワーク内の指定された VSAN、またはスイッチ全体のデフォルトの遅延時間を変更できます。

ネットワークおよび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。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# fcdroplateny network 5000	ネットワークのネットワークドロップ遅延時間を 5000 ミリ秒に設定します。有効値は 0 ~ 60000 ミリ秒です。デフォルトは 2000 ミリ秒です。 (注) ネットワークのドロップ遅延時間は、ネットワーク内の最長パスのすべてのスイッチ遅延の合計として計算する必要があります。
	switch(config)# fcdroplateny network 6000 vsan 3	VSAN 3 のネットワークドロップ遅延時間を 6000 ミリ秒に設定します。
	switch(config)# no fcdroplateny network 4500	現在の fcdroplateny ネットワーク設定 (4500) を削除し、出荷時の初期状態に戻します。

遅延情報の表示

設定された遅延パラメータを表示するには、**show fcdroplateny** コマンドを使用できます(例 6-1 を参照)。

例 6-1 アドミニストレーティブ ディスタンスの表示

```
switch# show fcdroplateny
switch latency value:500 milliseconds
global network latency value:2000 milliseconds

VSAN specific network latency settings
vsan 1 network latency:5000 milliseconds
vsan 2 network latency:2000 milliseconds
vsan 103 network latency:2000 milliseconds
vsan 460 network latency:500 milliseconds
```

フロー統計情報の設定

フロー統計情報は、集約統計情報テーブル内の入力トラフィックをカウントします。次の 2 種類の統計情報を収集できます。

- 集約フロー統計 (VSAN のトラフィックをカウント)。
- VSAN 内の送信元/宛先 ID ペアに対応するトラフィックをカウントするフロー統計情報。

この項では、次のトピックについて取り上げます。

- [フロー統計の概要 \(6-17 ページ\)](#)
- [集約フロー統計情報のカウント \(6-17 ページ\)](#)
- [個々のフロー統計情報のカウント \(6-17 ページ\)](#)
- [FIB 統計情報のクリア \(6-18 ページ\)](#)
- [フロー統計情報の表示 \(6-18 ページ\)](#)

フロー統計の概要

フローカウンタを有効にすると、第1世代のモジュールの集約フロー統計とフロー統計に最大1000のエントリ、第2世代のモジュールでは最大2000のエントリが使用可能になります。各新フローのモジュールに必ず未使用のフローインデックスを割り当ててください。フローインデックスはモジュール全体で繰り返し使用できます。フローインデックスの番号の間は、集約フロー統計情報とフロー統計情報間で共有します。

第1世代のモジュールは、モジュールあたり最大1024のフローステートメントを許容します。第2世代のモジュールは、モジュールあたり最大2048～128のフローステートメントを許容します。



(注) 各セッションでは、ローカル接続デバイスでのみ fcflow カウンタが増加します。このカウンタは、イニシエータが接続しているスイッチで設定する必要があります。

集約フロー統計情報のカウント

VSAN の集約フロー統計情報をカウントするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <code>config t</code> switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <code>fcflow stats aggregated module 1 index 1005 vsan 1</code> switch(config)#	集約フローカウンタをイネーブルにします。
	switch(config)# <code>no fcflow stats aggregated module 1 index 1005 vsan 1</code> switch(config)#	集約フローカウンタをディセーブルにします。

個々のフロー統計情報のカウント

VSAN 内の送信元および宛先 FC ID のフロー統計情報をカウントするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <code>config t</code> switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <code>fcflow stats module 1 index 1 0x145601 0x5601ff 0xffffffff vsan 1</code> switch(config)#	フローカウンタをイネーブルにします。 (注) ソース ID および宛先 ID は、16進形式の FC ID (0x123aff など) で指定します。使用できるマスクは、0xff0000 または 0xffffffff のどちらかです。
	switch(config)# <code>no fcflow stats aggregated module 2 index 1001 vsan 2</code> switch(config)#	フローカウンタをディセーブルにします。

FIB 統計情報のクリア

集約フローカウンタをクリアするには、`clear fcflow stats` コマンドを使用します(例 6-2 と 6-3 を参照)。

例 6-2 集約フローカウンタのクリア

```
switch# clear fcflow stats aggregated module 2 index 1
```

例 6-3 送信元 FC ID と宛先 FC ID のフローカウンタのクリア

```
switch# clear fcflow stats module 2 index 1
```

フロー統計情報の表示

フロー統計情報を表示するには、`show fcflow stats` コマンドを使用します(例 6-4 ~ 6-6 を参照)。

例 6-4 指定されたモジュールの集約フロー詳細情報の表示

```
switch# show fcflow stats aggregated module 6
Idx  VSAN  frames  bytes
-----
1    800   20185860 1211151600
```

例 6-5 指定されたモジュールのフロー詳細情報の表示

```
switch# show fcflow stats module 6

Idx  VSAN  DID          SID          Mask          frames  bytes
-----
2    800   0x520400    0x530260    0xffffffff    20337793 1220267580
```

例 6-6 指定されたモジュールのフロー インデックス使用状況の表示

```
switch# show fcflow stats usage module 6
Configured flows for module 6: 1-2
```

グローバル FSPF 情報の表示

例 6-7 に、特定の VSAN に対するグローバルな FSPF 情報を表示します。

- スイッチのドメイン番号。
- スイッチの自律リージョン。
- Min_LS_arrival: スイッチが LSR 更新を受け入れるまでに経過する必要がある最小時間。
- Min_LS_interval: スイッチが LSR を送信できるまでに経過する必要がある最小時間。

**ヒント**

Min_LS_interval が 10 秒よりも長い場合、グレースフル シャットダウン機能が実装されません。

- LS_refresh_time: 更新 LSR 送信間の時間間隔。
- Max_age: LSR が削除されるまでの LSR の最大維持期間。

例 6-7 指定した VSAN の FSPF 情報の表示

```
switch# show fspf vsan 1
FSPF routing for VSAN 1
FSPF routing administration status is enabled
FSPF routing operational status is UP
It is an intra-domain router
Autonomous region is 0
SPF hold time is 0 msec
MinLsArrival = 1000 msec , MinLsInterval = 5000 msec
Local Domain is 0x65(101)
Number of LSRs = 3, Total Checksum = 0x0001288b

Protocol constants :
  LS_REFRESH_TIME = 1800 sec
  MAX_AGE          = 3600 sec

Statistics counters :
  Number of LSR that reached MaxAge = 0
  Number of SPF computations         = 7
  Number of Checksum Errors          = 0
  Number of Transmitted packets :   LSU 65 LSA 55 Hello 474 Retranmsitted LSU 0
  Number of received packets :     LSU 55 LSA 60 Hello 464 Error packets 10
```

FSPF データベースの表示

例 6-8 に、指定された VSAN の FSPF データベースの要約を示します。その他のパラメータを指定しない場合、データベース内のすべての LSR が表示されます。

- 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

LSR 所有者のドメイン ID の追加パラメータを発行して、特定の情報を取得するために表示を絞り込むことができます。各インターフェイスについて、次の情報も確認できます。

- 隣接スイッチのドメイン ID
- E ポート インデックス
- 近接スイッチのポート インデックス
- リンク タイプとコスト

例 6-8 FSPF データベース情報の表示

```
switch# show fspf database vsan 1

FSPF Link State Database for VSAN 1 Domain 0x0c(12)
LSR Type = 1
Advertising domain ID = 0x0c(12)
LSR Age = 1686
LSR Incarnation number = 0x80000024
LSR Checksum = 0x3caf
Number of links = 2
  NbrDomainId      IfIndex  NbrIfIndex  Link Type      Cost
-----
    0x65(101) 0x0000100e    0x00001081         1         500
    0x65(101) 0x0000100f    0x00001080         1         500

FSPF Link State Database for VSAN 1 Domain 0x65(101)
LSR Type = 1
Advertising domain ID = 0x65(101)
LSR Age = 1685
LSR Incarnation number = 0x80000028
LSR Checksum = 0x8443
Number of links = 6
  NbrDomainId      IfIndex  NbrIfIndex  Link Type      Cost
-----
    0xc3(195) 0x00001085    0x00001095         1         500
    0xc3(195) 0x00001086    0x00001096         1         500
    0xc3(195) 0x00001087    0x00001097         1         500
    0xc3(195) 0x00001084    0x00001094         1         500
    0x0c(12) 0x00001081    0x0000100e         1         500
    0x0c(12) 0x00001080    0x0000100f         1         500

FSPF Link State Database for VSAN 1 Domain 0xc3(195)
LSR Type = 1
Advertising domain ID = 0xc3(195)
LSR Age = 1686
LSR Incarnation number = 0x80000033
LSR Checksum = 0x6799
Number of links = 4
  NbrDomainId      IfIndex  NbrIfIndex  Link Type      Cost
-----
    0x65(101) 0x00001095    0x00001085         1         500
    0x65(101) 0x00001096    0x00001086         1         500
    0x65(101) 0x00001097    0x00001087         1         500
    0x65(101) 0x00001094    0x00001084         1         500
```

FSPF インターフェイスの表示

例 6-9 に、選択された各インターフェイスの次の情報を表示します。

- リンク コスト
- タイマー値
- ネイバーのドメイン ID(既知の場合)
- ローカル インターフェイス番号
- リモート インターフェイス番号(既知の場合)
- インターフェイスの FSPF 状態。
- インターフェイス カウンタ

例 6-9 FSPF インターフェイスの情報の表示

```

switch# show fspf vsan 1 interface fc1/1
FSPF interface fc1/1 in VSAN 1
FSPF routing administrative state is active
Interface cost is 500
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is FULL
Neighbor Domain Id is 0x0c(12), Neighbor Interface index is 0x0f100000
Statistics counters :
  Number of packets received : LSU 8 LSA 8 Hello 118 Error packets 0
  Number of packets transmitted : LSU 8 LSA 8 Hello 119 Retransmitted LSU 0
  Number of times inactivity timer expired for the interface = 0

```

デフォルト設定

表 6-4 に、FSPF 機能のデフォルト設定を示します。

表 6-4 FSPF のデフォルト設定値

パラメータ (Parameters)	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です。
SPF 計算	ダイナミック
SPF ホールド タイム	0.
バックボーン リージョン	0.
ACK インターバル (RxmtInterval)	5 秒
リフレッシュ タイム (LSRefreshTime)	30 分
最大エージング (MaxAge)	60 分
hello 間隔	20 秒
デッド間隔	80 秒
配信ツリー情報	主要スイッチ(ルート ノード)から取得します。
Routing table	FSPF は指定された宛先への等コスト パスを 16 まで格納します。
ロード バランシング	複数の等コスト パスの宛先 ID およびソース 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)を指定しない場合、デフォルトは 10 です。
リモート宛先スイッチ	リモート宛先スイッチを指定しない場合、デフォルトは、direct 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。

■ デフォルト設定



DWDM の設定

この章では、次の事項について説明します。

- [DWDM の概要 \(7-1 ページ\)](#)
- [X2 DWDM トランシーバ周波数の設定 \(7-1 ページ\)](#)

DWDM の概要

高密度波長分割多重 (DWDM) 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) 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。

X2 DWDM トランシーバ周波数の設定

モジュールの X2 DWDM トランシーバ周波数を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>switch# config t</code>	コンフィギュレーションモードに入ります。
ステップ 2	<code>switch(config)# module 1 transceiver-frequency x2-eth</code>	リンクが X2 イーサネットとして機能するように設定します。
	<code>switch(config)# module 1 transceiver-frequency x2-fc</code>	リンクが X2 FC として機能するように設定します (デフォルト)。



(注)

この機能は、MDS 9134 モジュール以外ではサポートされていません。MDS 9134 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。



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ファブリック ログイン (FLOGI) 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。内容は次のとおりです。

- [FLOGIの概要\(8-1 ページ\)](#)
- [FLOGI の詳細の表示\(8-1 ページ\)](#)
- [ネームサーバ\(8-3 ページ\)](#)
- [FDMI\(8-8 ページ\)](#)
- [FDMI の表示\(8-8 ページ\)](#)
- [RSCN\(8-10 ページ\)](#)
- [デフォルト設定\(8-19 ページ\)](#)
- [ポート ペーシングの有効化\(8-19 ページ\)](#)

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ファイバチャネル ID が必要です。FLOGI テーブルにストレージ デバイスが表示されるかどうかを確認するには、次の項で説明するように **show flogi** コマンドを使用します。必要なデバイスが FLOGI テーブルに表示されていれば、FLOGI が正常に行われます。ホスト Host Bus Adapter (HBA) および接続ポートに直接接続されているスイッチ上の FLOGI データベースを検査します。

FLOGI の詳細の表示

FLOGI データベースの詳細を表示するには、**show flogi database** コマンドを使用します。例 8-1 ~ 8-4 を参照してください。

例 8-1 FLOGI データベースの詳細の表示

```
switch# show flogi database
-----
INTERFACE  VSAN      FCID          PORT NAME          NODE NAME
-----
sup-fc0    2         0xb30100     10:00:00:05:30:00:49:63  20:00:00:05:30:00:49:5e
```

```

fc9/13      1      0xb200e2  21:00:00:04:cf:27:25:2c  20:00:00:04:cf:27:25:2c
fc9/13      1      0xb200e1  21:00:00:04:cf:4c:18:61  20:00:00:04:cf:4c:18:61
fc9/13      1      0xb200d1  21:00:00:04:cf:4c:18:64  20:00:00:04:cf:4c:18:64
fc9/13      1      0xb200ce  21:00:00:04:cf:4c:16:fb  20:00:00:04:cf:4c:16:fb
fc9/13      1      0xb200cd  21:00:00:04:cf:4c:18:f7  20:00:00:04:cf:4c:18:f7

```

Total number of flogi = 6.

例 8-2 インターフェイス別の FLOGI データベースの表示

```

switch# show flogi database interface fc1/11
-----
INTERFACE  VSAN    FCID          PORT NAME          NODE NAME
-----
fc1/11     1       0xa002ef     21:00:00:20:37:18:17:d2  20:00:00:20:37:18:17:d2
fc1/11     1       0xa002e8     21:00:00:20:37:38:a7:c1  20:00:00:20:37:38:a7:c1
fc1/11     1       0xa002e4     21:00:00:20:37:6b:d7:18  20:00:00:20:37:6b:d7:18
fc1/11     1       0xa002e2     21:00:00:20:37:18:d2:45  20:00:00:20:37:18:d2:45
fc1/11     1       0xa002e1     21:00:00:20:37:39:90:6a  20:00:00:20:37:39:90:6a
fc1/11     1       0xa002e0     21:00:00:20:37:36:0b:4d  20:00:00:20:37:36:0b:4d
fc1/11     1       0xa002dc     21:00:00:20:37:5a:5b:27  20:00:00:20:37:5a:5b:27
fc1/11     1       0xa002da     21:00:00:20:37:18:6f:90  20:00:00:20:37:18:6f:90
fc1/11     1       0xa002d9     21:00:00:20:37:5b:cf:b9  20:00:00:20:37:5b:cf:b9
fc1/11     1       0xa002d6     21:00:00:20:37:46:78:97  0:00:00:20:37:46:78:97

```

Total number of flogi = 10.

例 8-3 VSAN 別の FLOGI データベースの表示

```

switch# show flogi database vsan 1
-----
INTERFACE  VSAN    FCID          PORT NAME          NODE NAME
-----
fc1/3      1       0xef02ef     22:00:00:20:37:18:17:d2  20:00:00:20:37:18:17:d2
fc1/3      1       0xef02e8     22:00:00:20:37:38:a7:c1  20:00:00:20:37:38:a7:c1
fc1/3      1       0xef02e4     22:00:00:20:37:6b:d7:18  20:00:00:20:37:6b:d7:18
fc1/3      1       0xef02e2     22:00:00:20:37:18:d2:45  20:00:00:20:37:18:d2:45
fc1/3      1       0xef02e1     22:00:00:20:37:39:90:6a  20:00:00:20:37:39:90:6a
fc1/3      1       0xef02e0     22:00:00:20:37:36:0b:4d  20:00:00:20:37:36:0b:4d
fc1/3      1       0xef02dc     22:00:00:20:37:5a:5b:27  20:00:00:20:37:5a:5b:27
fc1/3      1       0xef02da     22:00:00:20:37:18:6f:90  20:00:00:20:37:18:6f:90
fc1/3      1       0xef02d9     22:00:00:20:37:5b:cf:b9  20:00:00:20:37:5b:cf:b9
fc1/3      1       0xef02d6     22:00:00:20:37:46:78:97  20:00:00:20:37:46:78:97

```

Total number of flogi = 10.

例 8-4 FC ID 別の FLOGI データベースの表示

```

switch# show flogi database fcid 0xef02e2
-----
INTERFACE  VSAN    FCID          PORT NAME          NODE NAME
-----
fc1/3      1       0xef02e2     22:00:00:20:37:18:d2:45  20:00:00:20:37:18:d2:45

```

Total number of flogi = 1.

詳細については、「[デフォルトの企業 ID リスト](#)」セクション(11-9 ページ)と『Cisco MDS 9000 Family Troubleshooting Guide』の「Loop Monitoring」の項を参照してください。

ネーム サーバ

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 サーバでは、情報を最初に登録したデバイスによるデータベース エントリの変更が認められます。

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。

この項では、次のトピックについて取り上げます。

- [ネーム サーバから送信される一括通知 \(8-3 ページ\)](#)
- [ネーム サーバの一括通知の有効化 \(8-3 ページ\)](#)
- [ネーム サーバの一括通知の無効化 \(8-4 ページ\)](#)
- [ネーム サーバプロキシの登録 \(8-5 ページ\)](#)
- [重複 pWWN の拒否の概要 \(8-5 ページ\)](#)
- [重複 pWWN の拒否 \(8-5 ページ\)](#)
- [ネーム サーバ データベース エントリ \(8-6 ページ\)](#)
- [ネーム サーバのデータベース同期の最適化 \(8-6 ページ\)](#)
- [ネーム サーバ データベースのエントリ数の確認 \(8-6 ページ\)](#)
- [ネーム サーバ データベースのエントリの表示 \(8-7 ページ\)](#)

ネーム サーバから送信される一括通知

Cisco MDS 9000 スイッチでのファイバ チャネル プロトコルのパフォーマンスを向上させるため、ネーム サーバは 1 つの MTS ペイロードで複数の通知を送信することで、リモート エントリ 変更通知を最適化します。この MTS 通知を受け取るその他の約 10 個のコンポーネントは、複数の通知ではなく 1 つの一括通知を処理する必要があります。

ネーム サーバの一括通知の有効化

NX-OS Release 6.2(1) ~ 6.2(7) では、一括通知はデフォルトでは無効です。1 つのスイッチでこの機能を有効にしても、同じファブリック内のその他のスイッチには影響しません。



(注) NX-OS Release 6.2(9) 以降では、一括送信はデフォルトで有効です。

機能制限

- DMM、IOA、SME などのインテリジェント アプリケーションが有効な場合は常に、一括通知機能はサポートされません。
- FC リダイレクトの設定は、一括通知機能と常に競合します。



(注) 前述の制約はリリース 6.2.7 のみに適用されます。

手順の詳細

ネーム サーバの一括通知を有効にするには、NX-OS Release 6.2(1) ~ 6.2(7) で次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# fcns bulk-notify switch(config)#	1 つの Messaging and Transaction Services (MTS) ペイロードでの複数ネーム サーバ エントリ変更通知の送信を有効にします。

ネーム サーバの一括通知の無効化

手順の詳細

ネーム サーバの一括通知を無効にするには、NX-OS Release 6.2(1) ~ 6.2(7) で次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# no fcns bulk-notify switch(config)#	1 つの Messaging and Transaction Services (MTS) ペイロードでの複数ネーム サーバ エントリ変更通知の送信を無効にします。

ネーム サーバの一括通知を無効にするには、NX-OS Release 6.2(9) 以降で次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# fcns no-bulk-notify switch(config)#	1 つの Messaging and Transaction Services (MTS) ペイロードでの複数ネーム サーバ エントリ変更通知の送信を無効にします。

NX-OS Release 6.2(9) 以降ですでに無効にした設定を再度有効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# no fcns no-bulk-notify switch(config)#	1 つの Messaging and Transaction Services (MTS) ペイロードでの複数ネーム サーバ エントリ変更通知の送信を再び有効にします。

ネーム サーバ プロキシ 登録

ネーム サーバ 登録要求はすべて、パラメータが登録または変更されたポートと同じポートから送信されます。そのポートにパラメータがないと、要求は拒否されます。

この許可を使用すると、WWN が他のノードに代わって特定のパラメータを登録できるようになります。

ネーム サーバ プロキシ の 登録

ネーム サーバ プロキシ を登録するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# fcns proxy-port 21:00:00:e0:8b:00:26:d0 vsan 2	指定した VSAN のプロキシ ポートを設定します。

重複 pWWN の拒否の概要

FC 標準では、NX-OS は同一スイッチ、同一 VSAN、および同一 FC ドメインですでにログインしている pWWN の任意のインターフェイスでのログインを受け入れます。同じ pWWN が、異なるインターフェイスで同じスイッチにログインしないようにするには、ポート セキュリティ機能を使用します。

デフォルトでは、同一 VSAN の異なるスイッチでの(重複する pWWN による)今後の FLOGI はすべて拒否され、以前の FLOGI が維持されます。これは FC 標準に準拠していません。このオプションを無効にすると、以前の FCNS エントリを削除することで、同一 VSAN の異なるスイッチでの(重複する pWWN による)今後の FLOGI はすべて許可されます。

重複 pWWN の拒否

重複 pWWN を拒否するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# configure terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# fcns reject-duplicate-pwwn vsan 1	異なるスイッチでの(重複する pWWN による)今後の FLOGI はすべて拒否され、以前の FLOGI が維持されます。(デフォルト)
	switch(config)# no fcns reject-duplicate-pwwn vsan 1	以前の FLOGI エントリを削除することで、異なるスイッチでの(重複する pWWN による)今後の FLOGI はすべて許可されます。 ただし、他のスイッチの FLOGI データベースには以前のエントリがまだ含まれています。

ネームサーバデータベースエントリ

ネームサーバはすべてのホストのネームエントリを FCNS データベースに保管しています。ネームサーバを使用すると、Nx ポートで(ネームサーバへの)PLOGI 中に属性を登録し、その他のホストの属性を取得できます。Nx ポートが明示的または暗黙的にログアウトする時点で、これらの属性は登録解除されます。

マルチスイッチファブリック構成では、各スイッチ上で稼働するネームサーバインスタンスが分散型データベースで情報を共有します。スイッチごとに1つのネームサーバプロセスのインスタンスが実行されます。

ネームサーバのデータベース同期の最適化

エンドデバイスが FC4 機能をネームサーバデータベースに登録しない場合、VHBA (scsi-target と呼ばれる)コンポーネントがエンドデバイスに対して PRLI を実行し、FC4 機能を検出し、エンドデバイスの代理でネームサーバに登録します。VHBA からのこの検出は、ローカル接続デバイスと

リモート接続デバイスの両方に対して実行されています。リモート接続デバイスに対してこの検出を実行する必要はありません。これは、ネームサーバは標準ネームサーバ同期プロトコルを使用してリモート接続デバイスの FC4 機能を取得するためです。したがって、ローカル接続デバイスだけを検出するように、VHBA コンポーネントのデフォルトの動作が変更されました。この動作を変更するには、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>switch(config)# scsi-target discovery</code>	スイッチが、リモート デバイスの fc-4 機能も検出できるようにします。ただしこれは、ユーザがスイッチをリロードするか、またはスイッチをスイッチオーバーする場合のデフォルトの動作ではありません。
ステップ 2	<code>switch(config)# scsi-target discovery local-only</code>	デフォルトの動作に戻ります。

ネームサーバデータベースのエントリ数の確認

ネームサーバデータベースのエントリ数を確認するには、次の手順に従います。:

	コマンド	目的
ステップ 1	<code>switch# show fcns internal info global</code>	ネームサーバデータベースのデバイスエントリの数を表示します。
ステップ 2	<code>switch# show fcns internal info</code>	出力の終わりに、ネームサーバデータベースのデバイスの数を表示します。

ネーム サーバ データベースのエントリの表示

指定した VSAN またはすべての VSAN のネーム サーバのデータベースおよび統計情報を表示するには、**show fcns** コマンドを使用します(例 8-5 ~ 8-8 を参照)。

例 8-5 ネーム サーバ データベースの表示

```
switch# show fcns database
-----
FCID          TYPE  PWWN                               (VENDOR)          FC4-TYPE:FEATURE
-----
0x010000      N     50:06:0b:00:00:10:a7:80             (Cisco)            scsi-fcp fc-gs
0x010001      N     10:00:00:05:30:00:24:63             (Cisco)            ipfc
0x010002      N     50:06:04:82:c3:a0:98:52             (Company 1)        scsi-fcp 250
0x010100      N     21:00:00:e0:8b:02:99:36             (Company A)        scsi-fcp
0x020000      N     21:00:00:e0:8b:08:4b:20             (Company A)
0x020100      N     10:00:00:05:30:00:24:23             (Cisco)            ipfc
0x020200      N     21:01:00:e0:8b:22:99:36             (Company A)        scsi-fcp
```

例 8-6 指定した VSAN のネーム サーバ データベースの表示

```
switch# show fcns database vsan 1
VSAN 1:
-----
FCID          TYPE  PWWN                               (VENDOR)          FC4-TYPE:FEATURE
-----
0x030001      N     10:00:00:05:30:00:25:a3             (Cisco)            ipfc
0x030101      NL    10:00:00:00:77:99:60:2c             (Interphase)
0x030200      N     10:00:00:49:c9:28:c7:01
0xec0001      NL    21:00:00:20:37:a6:be:14             (Seagate)          scsi-fcp

Total number of entries = 4
```

例 8-7 ネーム サーバ データベースの詳細の表示

```
switch# show fcns database detail
-----
VSAN:1      FCID:0x030001
-----
port-wnn (vendor)      :10:00:00:05:30:00:25:a3 (Cisco)
node-wnn                :20:00:00:05:30:00:25:9e
class                   :2,3
node-ip-addr            :0.0.0.0
ipa                     :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:ipfc
symbolic-port-name      :
symbolic-node-name      :
port-type                :N
port-ip-addr            :0.0.0.0
fabric-port-wnn         :00:00:00:00:00:00:00:00
hard-addr                :0x000000
-----
VSAN:1      FCID:0xec0200
-----
port-wnn (vendor)      :10:00:00:5a:c9:28:c7:01
node-wnn                :10:00:00:5a:c9:28:c7:01
class                   :3
node-ip-addr            :0.0.0.0
ipa                     :ff ff ff ff ff ff ff ff
```

```
fc4-types:fc4_features:
symbolic-port-name      :
symbolic-node-name     :
port-type               :N
port-ip-addr           :0.0.0.0
fabric-port-wwn        :22:0a:00:05:30:00:26:1e
hard-addr               :0x000000
Total number of entries = 2
```

例 8-8 ネームサーバ統計情報の表示

```
switch# show fcns statistics
registration requests received = 27
deregistration requests received = 0
queries received = 57
queries sent = 10
reject responses sent = 14
RSCNs received = 0
RSCNs sent = 0
```

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によって管理できます。この機能を追加することにより、既存のファイバチャネル ネームサーバおよび管理サーバの機能を補完します。

FDMI 機能を使用すると、独自のホスト エージェントをインストールしなくても、Cisco 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のバージョン
- ホスト オペレーティング システム (OS) の名前およびバージョン番号

FDMI エントリはすべて永続ストレージに保存され、FDMI プロセスを起動した時点で取り出されます。

FDMI の表示

FDMI データベース情報を表示するには、`show fdmi` コマンドを使用します (例 8-9 ~ 8-11 を参照)。

例 8-9 すべての HBA 管理サーバの表示

```
switch# show fdmi database
Registered HBA List for VSAN 1
  10:00:00:00:c9:32:8d:77
  21:01:00:e0:8b:2a:f6:54
switch# show fdmi database detail
Registered HBA List for VSAN 1
```

```

-----
HBA-ID: 10:00:00:00:c9:32:8d:77
-----
Node Name           :20:00:00:00:c9:32:8d:77
Manufacturer        :Emulex Corporation
Serial Num          :0000c9328d77
Model               :LP9002
Model Description:Emulex LightPulse LP9002 2 Gigabit PCI Fibre Channel Adapter
Hardware Ver        :2002606D
Driver Ver          :SLI-2 SW_DATE:Feb 27 2003, v5-2.20a12
ROM Ver             :3.11A0
Firmware Ver        :3.90A7
OS Name/Ver         :Window 2000
CT Payload Len      :1300000
  Port-id: 10:00:00:00:c9:32:8d:77
-----
HBA-ID: 21:01:00:e0:8b:2a:f6:54
-----
Node Name           :20:01:00:e0:8b:2a:f6:54
Manufacturer        :QLogic Corporation
Serial Num          :\74262
Model               :QLA2342
Model Description:QLogic QLA2342 PCI Fibre Channel Adapter
Hardware Ver        :FC5010409-10
Driver Ver          :8.2.3.10 Beta 2 Test 1 DBG (W2K VI)
ROM Ver             :1.24
Firmware Ver        :03.02.13.
OS Name/Ver         :500
CT Payload Len      :2040
  Port-id: 21:01:00:e0:8b:2a:f6:54

```

例 8-10 指定された VSAN の HBA の詳細の表示

```

switch# show fdbi database detail vsan 1
Registered HBA List for VSAN 1
-----
HBA-ID: 10:00:00:00:c9:32:8d:77
-----
Node Name           :20:00:00:00:c9:32:8d:77
Manufacturer        :Emulex Corporation
Serial Num          :0000c9328d77
Model               :LP9002
Model Description:Emulex LightPulse LP9002 2 Gigabit PCI Fibre Channel Adapter
Hardware Ver        :2002606D
Driver Ver          :SLI-2 SW_DATE:Feb 27 2003, v5-2.20a12
ROM Ver             :3.11A0
Firmware Ver        :3.90A7
OS Name/Ver         :Window 2000
CT Payload Len      :1300000
  Port-id: 10:00:00:00:c9:32:8d:77
-----
HBA-ID: 21:01:00:e0:8b:2a:f6:54
-----
Node Name           :20:01:00:e0:8b:2a:f6:54
Manufacturer        :QLogic Corporation
Serial Num          :\74262
Model               :QLA2342
Model Description:QLogic QLA2342 PCI Fibre Channel Adapter
Hardware Ver        :FC5010409-10
Driver Ver          :8.2.3.10 Beta 2 Test 1 DBG (W2K VI)
ROM Ver             :1.24
Firmware Ver        :03.02.13.

```

```
OS Name/Ver      :500
CT Payload Len   :2040
  Port-id: 21:01:00:e0:8b:2a:f6:54
```

例 8-11 指定された HBA エントリの詳細の表示

```
switch# show fDMI database detail hba-id 21:01:00:e0:8b:2a:f6:54 vsan 1

Node Name          :20:01:00:e0:8b:2a:f6:54
Manufacturer       :QLogic Corporation
Serial Num         :\74262
Model              :QLA2342
Model Description  :QLogic QLA2342 PCI Fibre Channel Adapter
Hardware Ver       :FC5010409-10
Driver Ver         :8.2.3.10 Beta 2 Test 1 DBG (W2K VI)
ROM Ver            :1.24
Firmware Ver       :03.02.13.
OS Name/Ver        :500
CT Payload Len     :2040
  Port-id: 21:01:00:e0:8b:2a:f6:54
```

RSCN

Registered State Change Notification (RSCN) は、ファブリック内で行われた変更について各ホストに通知するためのファイバチャネルサービスです。ホストは (SCR を通じて) ファブリックコントローラに登録することにより、この情報を受信できます。次のいずれかのイベントが発生した場合、適宜通知されます。

- ファブリックへのディスクの追加または削除
- 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

この項では、次のトピックについて取り上げます。

- [RSCN 情報について \(8-11 ページ\)](#)
- [RSCN 情報の表示 \(8-11 ページ\)](#)
- [multi-pid オプション \(8-12 ページ\)](#)
- [ドメイン フォーマット SW-RSCN の抑制 \(8-12 ページ\)](#)
- [結合 SW-RSCN \(8-13 ページ\)](#)
- [結合 SW RSCN の有効化 \(8-13 ページ\)](#)
- [結合 SW-RSCN の無効化 \(8-14 ページ\)](#)
- [RSCN 統計情報のクリア \(8-14 ページ\)](#)
- [CFS を使用した RSCN タイマー設定の配布 \(8-15 ページ\)](#)
- [RSCN タイマー設定の確認 \(8-16 ページ\)](#)
- [RSCN タイマー設定の配信 \(8-16 ページ\)](#)

RSCN 情報について

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、登録済みのノードに変更が発生したことを通知します。ネームサーバに再度クエリを発行して新しい情報を取得するのは、各ノードの責任範囲です。スイッチが各ノードに送信する RSCN には、変更に関する詳細情報は含まれていません。

RSCN 情報の表示

RSCN 情報を表示するには、`show rscn` コマンドを使用します(例 8-12 および 8-13 を参照)。

例 8-12 登録デバイス情報の表示

```
switch# show rscn scr-table vsan 1
SCR table for VSAN: 1
-----
FC-ID          REGISTERED FOR
-----
0x1b0300      fabric detected rscns
Total number of entries = 1
```



(注) SCR テーブルは設定不可能です。ホストが RSCN 情報と一緒に SCR フレームを送信する場合にかぎり、入力されます。ホストが RSCN 情報を受信しない場合、`show rscn scr-table` コマンドはエントリを返しません。

例 8-13 RSCN のカウンタ情報の表示

```
switch(config)# show rscn statistics vsan 106

Statistics for VSAN: 106
-----
Number of SCR received           = 0
Number of SCR ACC sent           = 0
Number of SCR RJT sent           = 0
Number of RSCN received          = 0
Number of RSCN sent              = 0
Number of RSCN ACC received      = 0
Number of RSCN ACC sent          = 0
Number of RSCN RJT received      = 0
Number of RSCN RJT sent          = 0
Number of SW-RSCN received       = 0
Number of SW-RSCN sent           = 0
Number of SW-RSCN ACC received   = 0
Number of SW-RSCN ACC sent       = 0
Number of SW-RSCN RJT received   = 0
Number of SW-RSCN RJT sent       = 0
Number of CSWR received          = 3137
Number of CSWR sent              = 0
Number of CSWR ACC received      = 0
Number of CSWR ACC sent          = 3137
```

```
Number of CSWR RJT received = 0
Number of CSWR RJT sent     = 0
Number of CSWR RJT not sent  = 0
```

multi-pid オプション

RSCN の **multi-pid** オプションをイネーブルに設定すると、登録済み Nx ポートに対して生成される RSCN に、影響を受けた複数のポート ID が含まれる場合があります。この場合、ゾーン分割ルールを適用してから、影響を受けた複数のポート ID が 1 つの RSCN にまとめられます。このオプションをイネーブルにすることによって、RSCN の数を減らすことができます。たとえば、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済みです。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] オプションを無効にしてください。

multi-pid オプションの設定

multi-pid オプションを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# rscn multi-pid vsan 105	VSAN 105 の RSCN を multi-pid フォーマットで送信します。

ドメインフォーマット SW-RSCN の抑制

ドメインフォーマット SW-RSCN は、ローカル スイッチ名またはローカル スイッチ管理 IP アドレスが変更されるとすぐに送信されます。この SW-RSCN は、ISL を介して、他のすべてのドメインおよびスイッチに送信されます。リモート スイッチから、ドメインフォーマット SW-RSCN を開始したスイッチに対して GMAL コマンドおよび GIELN コマンドを発行すると、変更内容を判別できます。ドメインフォーマット SW-RSCN によって、一部の非 Cisco MDS スイッチで問題が発生することがあります (『[Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide](#)』を参照)。

これらの SW-RSCN の ISL を介した送信を抑制するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# rscn suppress domain-swrrscn vsan 105	VSAN 105 のドメイン フォーマット SW-RSCN の送信を抑制します。



(注) ポート アドレス フォーマット RSCN またはエリア アドレス フォーマット RSCN の送信は抑制できません。

結合 SW-RSCN

Cisco MDS 9000 スイッチでのファイバチャネルプロトコルのパフォーマンス向上のため、SW-RSCN は遅延され、収集され、1 つの結合 SW-RSCN として単一ファイバチャネル交換でファブリック内のすべてのスイッチに送信されます。

結合 SW RSCN の有効化

[Restrictions(機能制限)]

- ファブリック内のすべてのスイッチで Cisco MDS 6.2(7) 以降が実行されている必要があります。
- この機能には、Cisco MDS 以外のスイッチとの相互運用性はありません。

手順の詳細

結合 SW-RSCN を有効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# rscn coalesce swrrscn vsan 1 switch(config)#	VSAN 1 の Switch Registered State Change Notification (SWRSCN) の結合を有効にします。デフォルト遅延は 500 ミリ秒です。
ステップ 3	switch(config)# rscn coalesce swrrscn vsan 1 delay 800 switch(config)#	VSAN 1 の Switch Registered State Change Notification (SWRSCN) の結合を有効にします。SW-RSCN を最大で 800 ミリ秒遅延します。



(注) 6.2(7) 以降が稼働しているすべてのスイッチでは、デフォルトで結合 SW-RSCN を処理できますが、結合 SW-RSCN の送信は CLI で有効にした後でのみ可能です。

結合 SW-RSCN の無効化

手順の詳細

結合 SW-RSCN を無効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>switch# config t</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>switch(config)# no rscn coalesce</code> <code>swrscn vsan 1</code> <code>switch(config)#</code>	VSAN 1 の Switch Registered State Change Notification (SWRSCN) の結合を無効にします。

RSCN 統計情報のクリア

カウンタをクリアしたあとに、それらのカウンタを別のイベントに関して表示することができます。たとえば、特定のイベント (ONLINE または OFFLINE イベントなど) で生成された RSCN または SW-RSCN の個数を追跡できます。このような統計情報を利用して、VSAN 内で発生する各イベントへの応答を監視できます。

指定された VSAN の RSCN 統計情報をクリアするには、`clear rscn statistics` コマンドを使用します。

```
switch# clear rscn statistics vsan 1
```

RSCN 統計情報をクリアした後に `show rscn` コマンドを実行すると、クリアされたカウンタを表示できます。

```
switch# show rscn statistics vsan 1
Statistics for VSAN: 1
-----
Number of SCR received           = 0
Number of SCR ACC sent           = 0
Number of SCR RJT sent           = 0
Number of RSCN received          = 0
Number of RSCN sent              = 0
Number of RSCN ACC received      = 0
Number of RSCN ACC sent          = 0
Number of RSCN RJT received      = 0
Number of RSCN RJT sent          = 0
Number of SW-RSCN received       = 0
Number of SW-RSCN sent           = 0
Number of SW-RSCN ACC received   = 0
Number of SW-RSCN ACC sent       = 0
Number of SW-RSCN RJT received   = 0
Number of SW-RSCN RJT sent       = 0
Number of CSWR received          = 0
Number of CSWR sent              = 0
Number of CSWR ACC received      = 0
Number of CSWR ACC sent          = 0
Number of CSWR RJT received      = 0
Number of CSWR RJT sent          = 0
Number of CSWR RJT not sent      = 0
```

CFS を使用した RSCN タイマー設定の配布

各スイッチのタイムアウト値は、手動で設定されるため、異なるスイッチが別々の時間にタイムアウトになると、誤設定が生じます。つまり、ネットワーク内の異なる N ポートが別々の時間に RSCN を受信してしまふことがあります。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 の数も削減します。

RSCN は、配布と非配布の 2 つのモードをサポートしています。配布モードでは、RSCN は CFS を使用して、ファブリック内のすべてのスイッチに設定を配布します。非配布モードでは、影響を受けるのはローカル スイッチに対するコンフィギュレーション コマンドだけです。



(注) すべてのコンフィギュレーション コマンドが配布されるわけではありません。配信されるのは、**rscn event-tov tov vsan vsan** コマンドのみです。

RSCN タイマーは、初期化およびスイッチオーバーの実行時に CFS に登録されます。ハイアベイラビリティを実現するため、RSCN タイマー配布がクラッシュし再起動する場合、またはスイッチオーバーが発生した場合には、クラッシュまたはスイッチオーバーが発生する前の状態から、通常の機能が再開されます。



(注) ダウングレードを実行する場合は、事前に、ネットワーク内の RSCN タイマー値をデフォルト値に戻してください。デフォルト値に戻しておかないと、VSAN およびその他のデバイスを経由するリンクがディセーブルになります。

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、**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。

RSCN タイマーの設定

RSCN は、VSAN 単位のイベント リスト キューを維持します。RSCN イベントは、生成されると、このキューに入れられます。最初の RSCN イベントがキューに入ると、VSAN 単位のタイマーが始動します。タイムアウトになると、すべてのイベントがキューから出され、結合 RSCN が登録済みユーザに送信されます。デフォルトのタイマー値の場合に、登録済みユーザに送信される結合 RSCN の数が最小になります。配置によっては、ファブリック内の変更を追跡するために、イベント タイマー値をさらに小さくする必要があります。



(注) RSCN タイマー値は、VSAN 内のすべてのスイッチで同一にする必要があります。「[RSCN タイマー設定の配信](#)」セクション(8-16 ページ)を参照してください。



(注) ダウングレードを実行する場合は、事前に、ネットワーク内の RSCN タイマー値をデフォルト値に戻してください。デフォルト値に戻しておかないと、VSAN およびその他のデバイスを経由するリンクがディセーブルになります。

RSCN タイマーを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# rscn distribute	RSCN タイマーの設定の配布をイネーブルにします。
ステップ 3	switch(config)# rscn event-tov 300 vsan 10	選択した VSAN のイベント タイムアウト値 (ミリ秒) を設定します。この例では、VSAN 12 のイベント タイムアウト値は 300 ミリ秒に設定されます。有効値は 0 ~ 2000 ミリ秒です。値をゼロ (0) に設定すると、タイマーはディセーブルになります。
	switch(config)# no rscn event-tov 300 vsan 10	デフォルト値 (ファイバチャネル VSAN の場合は 2000 ミリ秒、FICON VSAN の場合は 1000 ミリ秒) に戻ります。
ステップ 4	switch(config)# rscn commit vsan 10	配信する RSCN タイマー設定を VSAN 10 内のスイッチにコミットします。

RSCN タイマー設定の確認

RSCN タイマー設定を確認するには、**show rscn event-tov vsan** コマンドを使用します。

```
switch# show rscn event-tov vsan 10
Event TOV : 1000 ms
```

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、異なるスイッチが別々の時間にタイムアウトになると、誤設定が生じます。つまり、ネットワーク内の異なる N ポートが別々の時間に RSCN を受信してしまうことがあります。Cisco Fabric Service (CFS) インフラストラクチャでは、RSCN タイマー設定情報をファブリック内のすべてのスイッチに自動的に配布することで、この状況を解消します。また、SW-RSCN の数も削減します。『Cisco MDS 9000 Family NX-OS System Management Configuration Guide』を参照してください。

RSCN は、配布と非配布の 2 つのモードをサポートしています。配布モードでは、RSCN は CFS を使用して、ファブリック内のすべてのスイッチに設定を配布します。非配布モードでは、影響を受けるのはローカル スイッチに対するコンフィギュレーション コマンドだけです。



(注) すべてのコンフィギュレーション コマンドが配布されるわけではありません。配信されるのは、**rscn event-tov tov vsan vsan** コマンドのみです。



(注) RSCN タイマー設定だけが配布されます。

RSCN タイマーは、初期化およびスイッチオーバーの実行時に CFS に登録されます。ハイアベイラビリティを実現するため、RSCN タイマー配布がクラッシュし再起動する場合、またはスイッチオーバーが発生した場合には、クラッシュまたはスイッチオーバーが発生する前の状態から、通常の機能が再開されます。



(注) **show incompatibility system** コマンドを使用して以前の Cisco MDS NX-OS リリースにダウングレードする場合に、互換性を指定できます。以前のリリースへのダウングレードの前に、RSCN タイマー配信サポートを無効にする必要があります。



(注) デフォルトでは、RSCN タイマー配信機能は無効になっているため、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。



(注) RSCN タイマー設定で CFS 配信が正しく行われるようにするには、ファブリック内のすべてのスイッチで Cisco SAN-OS Release 3.0(1) 以降または Cisco NX-OS 4.1(1b) が稼働している必要があります。

この項では、次のトピックについて取り上げます。

- [RSCN タイマー設定の配布のイネーブル化\(8-17 ページ\)](#)
- [ファブリックのロック\(8-17 ページ\)](#)
- [RSCN タイマー設定の変更のコミット\(8-18 ページ\)](#)
- [RSCN タイマー設定の変更の廃棄\(8-18 ページ\)](#)
- [ロック済みセッションのクリア\(8-18 ページ\)](#)
- [RSCN 設定の配布情報の表示\(8-18 ページ\)](#)

RSCN タイマー設定の配布のイネーブル化

RSCN タイマー設定の配布を有効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# rscn distribute	RSCN タイマーの設定の配布をイネーブルにします。
	switch(config)# no rscn distribute	RSCN タイマーの配布をディセーブル(デフォルト)にします。

ファブリックのロック

データベースを変更するときの最初のアクションによって、保留中のデータベースが作成され、VSAN 内の機能がロックされます。ファブリックがロックされると、次のような状況になります。

- 他のユーザがこの機能の設定に変更を加えることができなくなります。
- コンフィギュレーション データベースのコピーが、最初のアクティブ変更と同時に保留中のデータベースになります。

RSCN タイマー設定の変更のコミット

アクティブ データベースに加えられた変更をコミットする場合、ファブリック内のすべてのスイッチに設定がコミットされます。コミットが正常に行われると、設定の変更がファブリック全体に適用され、ロックが解除されます。

RSCN タイマー設定の変更をコミットするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# rscn commit vsan 10	RSCN タイマーの変更をコミットします。

RSCN タイマー設定の変更の廃棄

保留中のデータベースに加えられた変更を廃棄(中断)する場合、コンフィギュレーション データベースは影響を受けないまま、ロックが解除されます。

RSCN タイマー設定の変更を廃棄するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# rscn abort vsan 10	RSCN タイマーの変更を廃棄し、保留中のコンフィギュレーション データベースをクリアします。

ロック済みセッションのクリア

RSCN タイマー設定を変更したが、変更をコミットまたは廃棄してロックを解除するのを忘れた場合、管理者はファブリック内の任意のスイッチからロックを解除できます。管理者がこの操作を行うと、ユーザによる保留データベースの変更は廃棄され、ファブリックのロックは解除されます。



ヒント

保留中のデータベースは揮発性ディレクトリでだけ有効で、スイッチが再起動されると廃棄されます。

管理者の特権を使用して、ロックされた RSCN セッションを解除するには、EXECモードで **clear rscn session** コマンドを使用します。

```
switch# clear rscn session vsan 10
```

RSCN 設定の配布情報の表示

RSCN 設定の配信の登録ステータスを表示するには、**show cfs application name rscn** コマンドを使用します。

```
switch# show cfs application name rscn

Enabled           : Yes
Timeout           : 5s
Merge Capable     : Yes
Scope              : Logical
```

RSCN 設定の配信のセッション ステータス情報を表示するには、**show rscn session status vsan** コマンドを使用します。



(注) 結合対象のファブリックの RSCN タイマー値が異なる場合、結合は失敗します。

```
switch# show rscn session status vsan 1
Session Parameters for VSAN: 1
-----
Last Action           : Commit
Last Action Result    : Success
Last Action Failure Reason : None
```

設定をコミットした際に有効になる一連のコンフィギュレーション コマンドを表示するには、**show rscn pending** コマンドを使用します。



(注) 保留中のデータベースには、既存設定と変更された設定の両方が含まれます。

```
switch# show rscn pending
rscn event-tov 2000 ms vsan 1
rscn event-tov 2000 ms vsan 2
rscn event-tov 300 ms vsan 10
```

保留中の設定とアクティブな設定の違いを表示するには、**show rscn pending-diff** コマンドを使用します。次の例では、VSAN 10 のタイムアウト値が 2000 ミリ秒(デフォルト)から 300 ミリ秒に変更されています。

```
switch# show rscn pending-diff
- rscn event-tov 2000 ms vsan 10
+ rscn event-tov 300 ms vsan 10
```

デフォルト設定

表 8-1 に、RSCN のデフォルト設定を示します。

表 8-1 デフォルトの RSCN 設定値

パラメータ (Parameters)	デフォルト
RSCN タイマー値	2000 ミリ秒(ファイバ チャネル VSAN) 1000 ミリ秒(FICON VSAN)
RSCN タイマー設定の配布	ディセーブル

ポート ページングの有効化

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

■ ポート ペーシングの有効化



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。内容は次のとおりです。

- [SCSI LUN 検出の概要 \(9-1 ページ\)](#)
- [SCSI LUN 情報の表示 \(9-3 ページ\)](#)

SCSI LUN 検出の概要

Small Computer System Interface (SCSI) ターゲットにはディスク、テープ、およびその他のストレージデバイスが含まれます。これらのターゲットの 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
- デバイスのキャパシティ、シリアル番号、およびデバイス ID 情報を表示するため。
- ネーム サーバにイニシエータおよびターゲット機能を登録するため。

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

SCSI LUN 検出機能は、CLI (コマンドライン インターフェイス) または SNMP (簡易ネットワーク管理プロトコル) を通じて、オンデマンドで開始されます。隣接スイッチが Cisco MDS 9000 ファミリーに含まれる場合、この情報は隣接スイッチとも同期されます。

この項では、次のトピックについて取り上げます。

- [SCSI LUN 検出の開始の概要 \(9-2 ページ\)](#)
- [SCSI LUN 検出の開始 \(9-2 ページ\)](#)
- [カスタマイズ検出開始の概要 \(9-2 ページ\)](#)
- [カスタマイズ検出の開始 \(9-2 ページ\)](#)

SCSI LUN 検出の開始の概要

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内の Nx ポートのうち、FC4 Type = SCSI_FCP として登録されたものだけが検出されます。

SCSI LUN 検出の開始

SCSI LUN 検出を開始するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# discover scsi-target local os all discovery started	すべてのオペレーティング システム (OS) のローカル SCSI ターゲットを検出します。オペレーティング システム のオプションは aix 、 all 、 hpux 、 linux 、 solaris 、または windows です。
	switch# discover scsi-target remote os aix discovery started	AIX OS に割り当てられたリモート SCSI ターゲットを検出します。
	switch# discover scsi-target vsan 1 fcid 0x9c03d6 discover scsi-target vsan 1 fcid 0x9c03d6 VSAN: 1 FCID: 0x9c03d6 PWWN: 00:00:00:00:00:00:00:00 PRLI RSP: 0x01 SPARM: 0x0012 SCSI TYPE: 0 NLUNS: 1 Vendor: Company 4 Model: ST318203FC Rev: 0004 Other: 00:00:02:32:8b:00:50:0a	指定された VSAN(1)および FC ID (0x9c03d6)の SCSI ターゲットを検出します。
	switch# discover scsi-target custom-list os linux discovery started	Linux OS に割り当てられたカスタマイズ リストから SCSI ターゲットを検出します。

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 とドメインのペア リストによって行われます。ドメイン ID は 0 ~ 255 の数値 (10 進数)、または 0x0 ~ 0xFF の数値 (16 進数) です。

この検出を開始するには、**custom-list** オプションを使用します。

カスタマイズ検出の開始

カスタマイズ検出を開始するには、次のいずれかの手順を実行します。

	コマンド	目的
ステップ 1	switch# discover custom-list add vsan 1 domain 0X123456	指定されたエントリをカスタム リストに追加します。
	switch# discover custom-list delete vsan 1 domain 0X123456	指定されたドメイン ID をカスタム リストから削除します。

SCSI LUN 情報の表示

検出結果を表示するには、**show scsi-target** および **show fcns database** コマンドを使用します。例 9-1 ~ 9-8 を参照してください。

例 9-1 検出ターゲットの表示

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



(注)

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

例 9-2 FCNS データベースの表示

```
switch# show fcns database
```

VSAN 1:

```
-----
FCID          TYPE  PWWN                                (VENDOR)          FC4-TYPE:FEATURE
-----
0xeb0000      N     21:01:00:e0:8b:2a:f6:54 (Qlogic)          scsi-fcp:init
0xeb0201      NL    10:00:00:00:c9:32:8d:76 (Emulex)          scsi-fcp:init
```

Total number of entries = 2

VSAN 7:

```
-----
FCID          TYPE  PWWN                                (VENDOR)          FC4-TYPE:FEATURE
-----
0xed0001      NL    21:00:00:04:cf:fb:42:f8 (Seagate)         scsi-fcp:target
```

Total number of entries = 1

VSAN 2002:

```
-----
FCID          TYPE  PWWN                                (VENDOR)          FC4-TYPE:FEATURE
-----
0xcafe00      N     20:03:00:05:30:00:2a:20 (Cisco)           FICON:CUP
```

Total number of entries = 1

例 9-3 検出されたターゲット ディスクの表示

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

```
-----
VSAN          FCID          PWWN                                VENDOR            MODEL              REV
-----
1             0x9c03d6     21:00:00:20:37:46:78:97             Company 4         ST318203FC         0004
1             0x9c03d9     21:00:00:20:37:5b:cf:b9             Company 4         ST318203FC         0004
1             0x9c03da     21:00:00:20:37:18:6f:90             Company 4         ST318203FC         0004
1             0x9c03dc     21:00:00:20:37:5a:5b:27             Company 4         ST318203FC         0004
1             0x9c03e0     21:00:00:20:37:36:0b:4d             Company 4         ST318203FC         0004
1             0x9c03e1     21:00:00:20:37:39:90:6a             Company 4         ST318203 CLAR18    3844
1             0x9c03e2     21:00:00:20:37:18:d2:45             Company 4         ST318203 CLAR18    3844
1             0x9c03e4     21:00:00:20:37:6b:d7:18             Company 4         ST318203 CLAR18    3844
1             0x9c03e8     21:00:00:20:37:38:a7:c1             Company 4         ST318203FC         0004
1             0x9c03ef     21:00:00:20:37:18:17:d2             Company 4         ST318203FC         0004
```

例 9-4 すべてのオペレーティングシステムで検出された LUN の表示

```
switch# show scsi-target lun os all
ST336607FC from SEAGATE (Rev 0006)
FCID is 0xed0001 in VSAN 7, PWWN is 21:00:00:04:cf:fb:42:f8
-----
OS   LUN   Capacity Status   Serial Number   Device-Id
      (MB)
-----
WIN 0x0   36704   Online   3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
AIX 0x0   36704   Online   3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
SOL 0x0   36704   Online   3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
LIN 0x0   36704   Online   3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
HP  0x0   36704   Online   3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
```

例 9-5 Solaris OS で検出された LUN の表示

```
switch# show scsi-target lun os solaris
ST336607FC from SEAGATE (Rev 0006)
FCID is 0xed0001 in VSAN 7, PWWN is 21:00:00:04:cf:fb:42:f8
-----
OS   LUN   Capacity Status   Serial Number   Device-Id
      (MB)
-----
SOL 0x0   36704   Online   3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
```

次のコマンドを実行すると、各 OS (Windows、AIX、Solaris、Linux、または HPUX) に割り当てられたポート WWN が表示されます。

例 9-6 各 OS の pWWN の表示

```
switch# show scsi-target pwwn
-----
OS      PWWN
-----
WIN     24:91:00:05:30:00:2a:1e
AIX     24:92:00:05:30:00:2a:1e
SOL     24:93:00:05:30:00:2a:1e
LIN     24:94:00:05:30:00:2a:1e
HP      24:95:00:05:30:00:2a:1e
```

例 9-7 カスタマイズされた検出ターゲットの表示

```
switch# show scsi-target custom-list
-----
VSAN    DOMAIN
-----
1       56
```

オンラインになった SCSI ターゲットの自動検出を確認するには、**show scsi-target auto-poll** コマンドを使用します。内部 UUID 番号は、シャーシに CSM または IPS モジュールが装着されていることを示します。

例 9-8 自動検出されたターゲットの表示

```
switch(config)# show scsi-target auto-poll
name server polling is enabled
auto-polling is disabled, poll_start:0 poll_count:0 poll_type:0
USERS OF AUTO POLLING
-----
```




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) をサポートしたことで、FICON プロセッサからスイッチのインバンド管理ができるようになりました。

この章は、次の項で構成されています。

- [FICON の概要 \(10-1 ページ\)](#)
- [FICON ポート番号の設定 \(10-8 ページ\)](#)
- [FICON の設定 \(10-16 ページ\)](#)
- [FICON ポートの設定 \(10-25 ページ\)](#)
- [FICON コンフィギュレーション ファイル \(10-34 ページ\)](#)
- [ポート スワッピング \(10-38 ページ\)](#)
- [FICON テープ アクセラレーション \(10-40 ページ\)](#)
- [XRC アクセラレーションの設定 \(10-44 ページ\)](#)
- [FICON VSAN のオフライン状態への移行 \(10-44 ページ\)](#)
- [CUP インバンド管理 \(10-45 ページ\)](#)
- [FICON 情報の表示 \(10-46 ページ\)](#)
- [デフォルト設定 \(10-54 ページ\)](#)

FICON の概要

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 (図 10-1 を参照)。

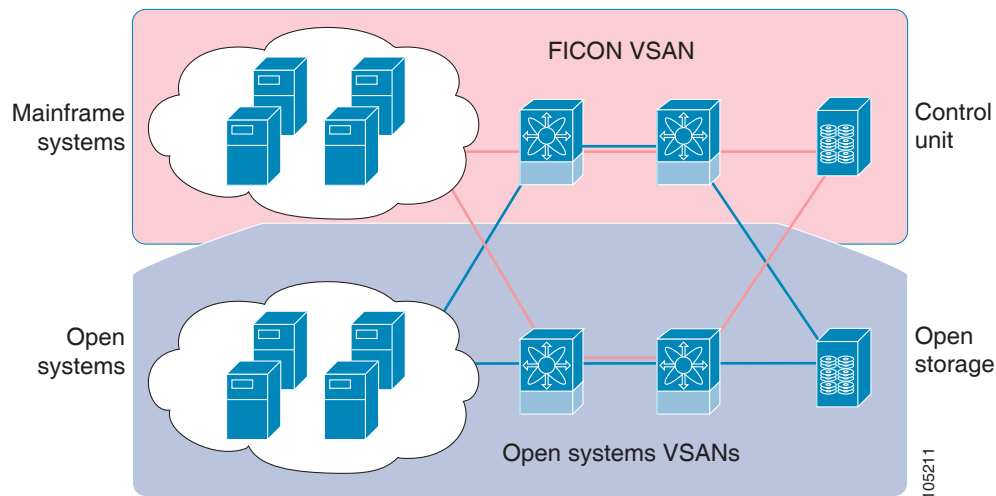
FICON 機能は、以下ではサポートされていません。

- 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

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。

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。

図 10-1 共有システムストレージネットワーク



この項では、次のトピックについて取り上げます。

- [FICON の要件 \(10-2 ページ\)](#)
- [MDS 固有 FICON のメリット \(10-3 ページ\)](#)
- [FICON のカスケード化 \(10-7 ページ\)](#)
- [FICON VSAN の前提条件 \(10-7 ページ\)](#)

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。

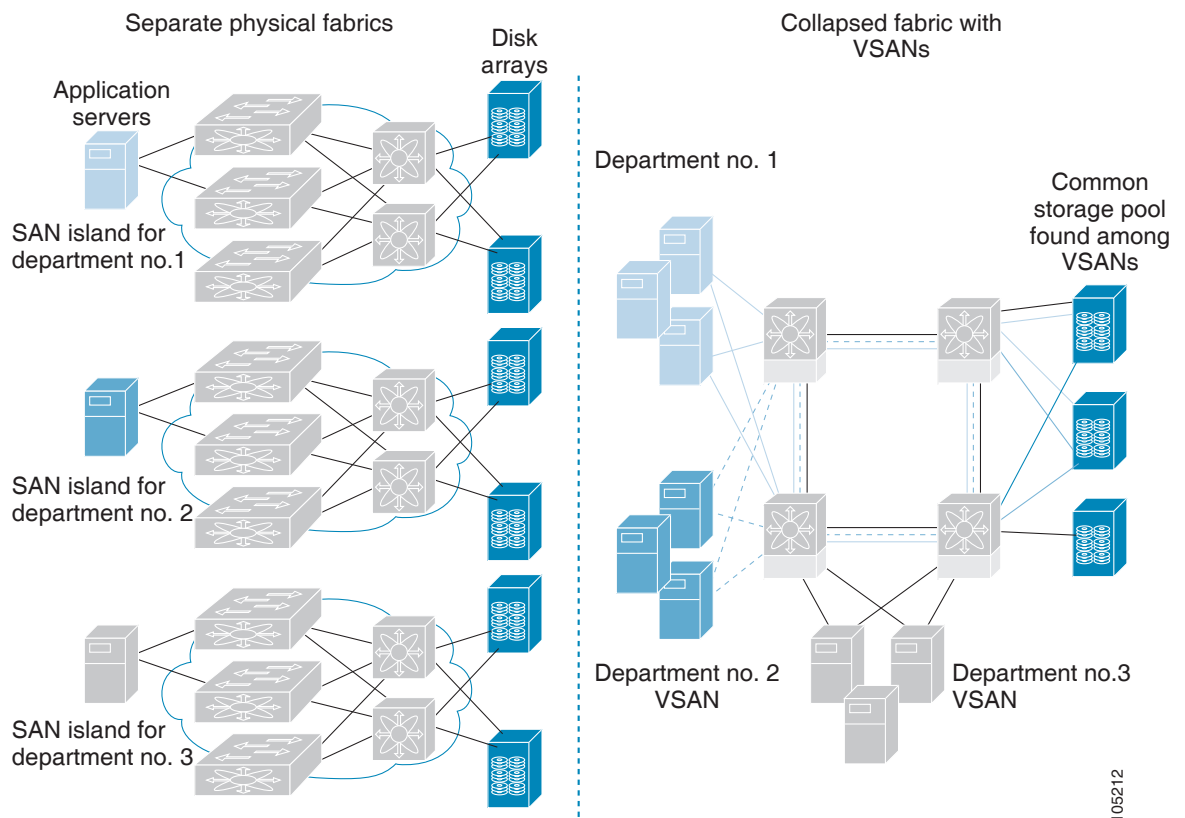
- [VSAN によるファブリックの最適化\(10-3 ページ\)](#)
- [FCIP のサポート\(10-4 ページ\)](#)
- [ポートチャネルのサポート\(10-4 ページ\)](#)
- [VSAN による、FICON と FCP の混在への対応\(10-5 ページ\)](#)
- [Cisco MDS でサポートされている FICON 機能\(10-5 ページ\)](#)

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 10-2 を参照)。

図 10-2 VSAN 固有ファブリックの最適化



105212

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 を有効にできる 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。

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 CUP、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公正さがあるため、「すべてのポートは等しく作成」されます。これにより、他のベンダー製プラットフォームで発生する「ローカル スイッチング」問題を除去して、プロビジョニングを簡素化することができます。

FICON LPAR にポートを追加する処理プロセスは、中断なしに実行されます。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スイッチ間リンク (ISL) 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、PortChannel 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 にはハードウェア独立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のが可能です。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 ポートを切り離します。



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 ファミリー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働中のソフトウェア 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わせを最大 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 ファミリーには、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独立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4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、簡易ネットワーク管理プロトコルバージョン3 (SNMPv3)、ロールベース アクセス コントロール、セキュア シェル プロトコル (SSH)、セキュア ファイル転送プロトコル (SFTP)、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。



(注) LUN ゾーン分割および読み取り専用ゾーンは、Cisco MDS NX-OS Release 5.x 以降ではサポートされていません。

- 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 インバンド管理」セクション(10-45 ページ)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、ブロック状態またはブロック解除状態を設定します。また、接続制限属性をポートに設定できます。「FICON ポートの設定」セクション(10-25 ページ)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
- 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」セクション(10-34 ページ)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」セクション(10-5 ページ)を参照してください。
- 拡張カスケード サポート: 「CUP インバンド管理」セクション(10-45 ページ)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」セクション(10-22 ページ)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」セクション(10-23 ページ)を参照。
- Call Home 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。

- 詳細な SPAN (スイッチド ポート アナライザ) 診断: Cisco MDS 9000 ファミリには、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、および統合された Call Home 機能が組み込まれているため、信頼性の向上、迅速な問題解決、およびサービスコストの削減が実現します。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」セクション(11-2 ページ)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。
- ポート レベルのインシデント アラート: ポート レベルのインシデント アラートを表示およびクリアします。「RLIR 情報のクリア」セクション(10-34 ページ)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 バインディングを有効にし、設定する必要があります(『Cisco MDS 9000 Family NX-OS Security Configuration Guide』を参照)。

FICON VSAN の前提条件

FICON VSAN を稼働状態にするには、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。「ヒントアクティブなゾーン セットを保存するために、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピー copy running-config startup-config コマンドを実行する必要はありません。ただし、フルゾーン セットを明示的に保存するには、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピー copy running-config startup-config コマンドを実行する必要があります。ファブリックに複数のスイッチが含まれている場合は、copy running-config startup-config fabric コマンドを実行する必要があります。キーワード fabric を指定すると、copy running-config startup-config コマンドがファブリック内のすべてのスイッチで実行され、フルゾーン情報がファブリック内のすべてのスイッチのスタートアップ コンフィギュレーションに保存されます。これは、スイッチのリロードおよび電源再投入時に重要です。」セクション(4-23 ページ)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 6 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)。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 インバンド管理」セクション(10-45 ページ)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

この項では、次のトピックについて取り上げます。

- デフォルトの FICON ポート番号設定方式(10-9 ページ)
- ポートアドレス(10-11 ページ)
- 実装ポートおよび非実装ポートのアドレス(10-11 ページ)
- 予約済み FICON ポート番号設定方式の概要(10-11 ページ)
- 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(10-12 ページ)
- FICON ポート番号設定に関するガイドライン(10-12 ページ)
- スロットへの FICON ポート番号の割り当て(10-13 ページ)
- FICON ポート番号割り当ての表示(10-13 ページ)
- FCIP およびポートチャネルのポート番号の概要(10-14 ページ)
- 予約済み FICON ポート番号設定方式の概要(10-11 ページ)
- FC ID の割り当て(10-15 ページ)

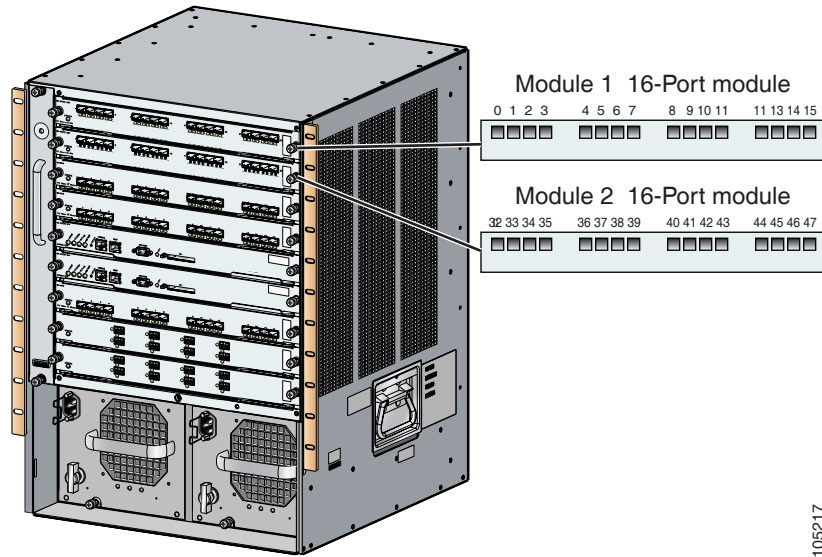


(注) FICON ポート番号を予約する前に、スイッチ上で FICON をイネーブルにしておく必要があります(「VSAN の FICON を有効にする操作の概要」セクション(10-16 ページ)を参照)。

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 10-3 を参照)。

図 10-3 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、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)

スロットにポート番号を手動で割り当てて超過分のポートを使用するには、**ficon slot assign port-numbers** コマンドを使用できます。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 10-3 (10-54 ページ) 表 10-1)を確認し、「予約済み FICON ポート番号設定方式の概要」セクション(10-11 ページ)セクション、「FICON ポート番号設定に関するガイドライン」セクション(10-12 ページ)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」セクション(10-13 ページ)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。

FICON ポート番号の設定

表 10-3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 10-1 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
		割り当て先ポート	割り当て先ポートチャンネル/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	
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			
	スロット 8	160 ~ 191			
	スロット 9	192 ~ 223			
					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。

表 10-1 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
		割り当て先ポート	割り当て先ポートチャネル/FCIP		
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			
	スロット 8	なし			
	スロット 9	96 ~ 111			
	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](#)」セクション(10-38 ページ)を参照)。

ポートアドレスをスワッピングするには、`ficon swap portnumber` コマンドを実行します。

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 10-3 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 10-3 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 10-3 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、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 10-3 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。ポートチャンネルまたは 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 およびポートチャンネルのポート番号の概要」セクション(10-14 ページ)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

使用するポート番号を決定するには、**show ficon port-number assign** コマンドおよび **show ficon first-available port-number** コマンドを使用します。



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。

FICON ポート番号をスロットに割り当てる手順は、次のとおりです。

	コマンド	目的
ステップ 1	<code>switch# config t</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>switch(config)# ficon slot 3 assign</code> <code>port-numbers 0-15, 48-63</code>	スロット 3 の最大 32 のインターフェイス用に FICON ポート番号 0 ~ 15 と 48 ~ 63 を予約します。
	<code>switch(config)# ficon slot 3 assign</code> <code>port-numbers 0-15, 17-32</code>	スロット 3 の最初の 16 インターフェイス用に FICON ポート番号 0 ~ 15 を予約し、次の 16 のインターフェイス用に 17 ~ 32 を予約します。
	<code>switch(config)# ficon slot 3 assign</code> <code>port-numbers 0-63</code>	スロット 3 の最大 64 のインターフェイス用に FICON ポート番号 0 ~ 63 を予約します。
	<code>switch(config)# ficon slot 3 assign</code> <code>port-numbers 0-15, 56-63</code>	スロット 3 の最大 24 のインターフェイス用に予約されている FICON ポート番号を変更します。
	<code>switch(config)# no ficon slot 3 assign</code> <code>port-numbers 0-15, 56-63</code>	FICON ポート番号を解放します。

FICON ポート番号割り当ての表示

スイッチに割り当てられているポート番号を表示するには、**show ficon port-numbers assign** コマンドを使用します。

```
switch# show ficon port-numbers assign
ficon slot 1 assign port-numbers 0-31
ficon slot 2 assign port-numbers 32-63
ficon slot 3 assign port-numbers 64-95
ficon slot 4 assign port-numbers 96-127
ficon logical-port assign port-numbers 128-153
```

特定のスロットに割り当てられているポート番号を表示するには、**show ficon port-numbers assign slot** コマンドを使用します。

```
switch# show ficon port-numbers assign slot 2
ficon slot 2 assign port-numbers 32-63
```

論理ポート用に予約されているポート番号を表示するには、**show ficon port-numbers assign** コマンドを使用します。

```
switch# show ficon port-numbers assign logical-port
ficon logical-port assign port-numbers 128-153
```

FCIP およびポートチャネルのポート番号の概要

FCIP および PortChannel 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」セクション(10-25 ページ)、「FICON ポートの設定」セクション(10-25 ページ)、「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」セクション(10-14 ページ)、および「FCIP インターフェイスへのポート番号のバインド」セクション(10-26 ページ)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 10-1(10-10 ページ)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(「予約済み FICON ポート番号設定方式の概要」セクション(10-11 ページ))を参照、デフォルト ポート番号を使用できます。

FCIP または PortChannel インターフェイスのバインドに最初に使用できるポート番号を確認するには、**show ficon first-available port-number** コマンドを使用します(例 10-12(10-48 ページ)を参照)。



ヒント

マッピングのインターフェイスとなるポート番号を表示するには、**show ficon vsan portaddress brief** コマンドを使用します。ポートチャネル/FCIP 範囲内で、PortChannel または FCIP インターフェイスに割り当てられていないポート番号を割り当てることができます(例 10-13(10-48 ページ))を参照)。

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。

FICON ポート番号を論理インターフェイス用に予約するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# ficon logical-port assign port-numbers 230-249	FCIP および PortChannel インターフェイス用にポート番号 230 ~ 249 を予約します。

	コマンド	目的
ステップ 3	<code>switch(config)# ficon logical-port assign port-numbers 0xe6-0xf9</code>	<p>FCIP および PortChannel インターフェイス用にポート番号 0xe6 ~ 0xf9 を予約します。</p> <p>(注) アクティブなポート番号は変更できません。shutdown コマンドを使用してインターフェイスを無効にし、no ficon portnumber コマンドを使用してポート番号をアンバインドする必要があります。「FICON ポートの設定」セクション(10-25 ページ)を参照してください。</p>
ステップ 4	<code>switch(config)# no ficon logical-port assign port-numbers 230-249</code>	<p>ポート番号を解放します。</p> <p>(注) アクティブなインターフェイスのポート番号は解放できません。shutdown コマンドを使用してインターフェイスを無効にし、no ficon portnumber コマンドを使用してポート番号をアンバインドする必要があります。「FICON ポートの設定」セクション(10-25 ページ)を参照してください。</p>

FC ID の割り当て

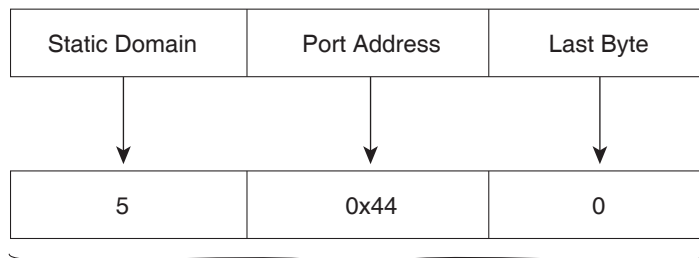
FICON には予測可能なスタティック FC ID 割り当て方式が必要です。FICON がイネーブルのときは、接続先ポートのポートアドレスに応じた FC ID がデバイスに割り当てられます。ポートアドレスは、ファブリックアドレスの中央バイトを構成しています。また、ファブリック内のデバイスはすべて、ファブリックアドレスの最終バイトが同一である必要があります。最終バイト値はデフォルトでは 0 ですが、他の値を設定することも可能です。



(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 を有効または無効にすると、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 10-4 を参照)。

図 10-4 FICON 用スタティック FC ID の割り当て



Static FC ID allocation for interface fc3/5 includes the static domain ID (5), the port address (0x44), and the last byte value (0).

113134

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。

この項では、次のトピックについて取り上げます。

- [VSAN の FICON を有効にする操作の概要 \(10-16 ページ\)](#)
- [スイッチでの FICON の有効化 \(10-17 ページ\)](#)
- [VSAN での手動での FICON のイネーブル化 \(10-20 ページ\)](#)
- [\[code-page\] オプションの設定 \(10-21 ページ\)](#)
- [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 \(10-22 ページ\)](#)
- [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 \(10-22 ページ\)](#)
- [ホストでタイムスタンプを制御できるようにする \(10-22 ページ\)](#)
- [タイムスタンプのクリア \(10-23 ページ\)](#)
- [FICON パラメータの SNMP 制御の設定 \(10-23 ページ\)](#)
- [FICON デバイスの従属関係の概要 \(10-23 ページ\)](#)
- [FICON デバイスの従属関係のクリア \(10-24 ページ\)](#)
- [実行コンフィギュレーションの自動保存 \(10-24 ページ\)](#)

VSAN の FICON を有効にする操作の概要

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。

- 自動 **setup ficon** コマンドを使用します。
「[基本 FICON 設定のセットアップ](#)」セクション (10-17 ページ) を参照してください。
- 各前提条件を手動でアドレッシングします。
「[FICON の概要](#)」セクション (10-1 ページ) 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](#)」セクション (10-35 ページ) を参照してください。

スイッチでの FICON の有効化

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。VSAN で FICON を有効にすることで、スイッチで FICON を明示的または暗黙的に有効にできます。ただし、すべての VSAN で FICON を無効にしても、スイッチの FICON は無効になりません。FICON を明示的に無効にする必要があります。

スイッチの FICON をグローバルに有効または無効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# feature ficon	スイッチの FICON をグローバルにイネーブルにします。
ステップ 3	switch(config)# no feature ficon	スイッチで FICON をグローバルに無効化し、すべての FICON 設定を削除します。

基本 FICON 設定のセットアップ

ここでは、Cisco MDS 9000 ファミリー 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。



(注)

任意のプロンプトで Ctrl+C キーを押すと、残りの設定オプションを飛ばして、設定手順を先に進めることができます。



ヒント

事前に設定された質問に回答しない場合、または任意の質問の回答を省略する場合は、Enter を押します。デフォルトの回答が見つからない場合(たとえば、スイッチ名)、スイッチは以前の設定を使用して、次の質問にスキップします。

FICON を有効にして設定するには、次の手順を実行します。

ステップ 1 EXEC コマンド モードで **setup ficon** コマンドを入力します。

```
switch# setup ficon
--- Ficon Configuration Dialog ---
```

This setup utility will guide you through basic Ficon Configuration on the system.

Press Enter if you want to skip any dialog. Use ctrl-c at anytime to skip all remaining dialogs.

ステップ 2 **yes** と入力して(デフォルトは **yes**)、基本 FICON 設定セットアップを開始します。

```
Would you like to enter the basic configuration dialog (yes/no) [yes]: yes
```

FICON セットアップユーティリティでは、手順に従って、基本的な設定プロセスを完了できます。どのプロンプトでも、Ctrl を押した状態で C を押すと、設定プロセスが終了します。

ステップ 3 FICON を有効にする必要がある VSAN の番号を入力します。

```
Enter vsan [1-4093]: 2
```

ステップ 4 VSAN を作成するには、**yes** と入力します(デフォルトは **yes**)。

```
vsan 2 does not exist, create it? (yes/no) [yes]: yes
```

ステップ 5 VSAN の選択を確定するには、**yes** と入力します(デフォルトは **yes**)。

```
Enable ficon on this vsan? (yes/no) [yes]: yes
```



(注) この時点で VSAN がまだ作成されていない場合は、ソフトウェアにより作成されます。

ステップ 6 指定された FICON VSAN のドメイン ID 番号を入力します。

```
Configure domain-id for this ficon vsan (1-239): 2
```

ステップ 7 カスケード モードで FICON を設定するには、**yes** と入力します(デフォルトは **no**)。 **no** と入力すると、**ステップ 8** にスキップします(「[CUP インバンド管理](#)」[セクション\(10-45 ページ\)](#) を参照)。

```
Would you like to configure ficon in cascaded mode: (yes/no) [no]: yes
```

a. FICON: CUP のピア WWN の割り当て

```
Configure peer wwn (hh:hh:hh:hh:hh:hh:hh:hh): 11:00:02:01:aa:bb:cc:00
```

b. FICON: CUP のピアドメイン ID の割り当て

```
Configure peer domain (1-239) : 4
```

c. 追加のピアを設定する場合は **yes** と入力します(ステップ **7a** と **7b** を繰り返します)。追加のピアを設定しない場合は **no** と入力します。

```
Would you like to configure additional peers: (yes/no) [no]: no
```

ステップ 8 SNMP に対し既存のポート接続パラメータの変更を許可するには、**yes** と入力します(デフォルトは **yes**) (「[FICON パラメータの SNMP 制御の設定](#)」[セクション\(10-23 ページ\)](#) を参照)。

```
Enable SNMP to modify port connectivity parameters? (yes/no) [yes]: yes
```

ステップ 9 必要に応じて、ホスト(メインフレーム)がポート接続パラメータを変更できるようにするには、**no** と入力します(デフォルトは **no**) (「[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](#)」[セクション\(10-22 ページ\)](#) を参照)。

```
Disable Host from modifying port connectivity parameters? (yes/no) [no]: no
```

ステップ 10 **yes** と入力し(デフォルトは **yes**)、**active equals saved** 機能を有効にします(「[実行コンフィギュレーションの自動保存](#)」[セクション\(10-24 ページ\)](#) を参照)。

```
Enable active=saved? (yes/no) [yes]: yes
```

ステップ 11 追加の FICON VSAN を設定するには、**yes** と入力します(デフォルトは **yes**)。

```
Would you like to configure additional ficon vsans (yes/no) [yes]: yes
```

ステップ 12 ここまでに入力した設定を確認して修正します。

ステップ 13 設定に問題がなければ、**no** と入力します(デフォルトは **no**)。



(注) 説明のため、次の設定では異なる FICON 設定の VSAN を 3 つ示しています。次に、さまざまな FICON シナリオでのこれらの設定による出力の例を示します。

The following configuration will be applied:

```
fcdomain domain 2 static vsan 1
fcdomain restart disruptive vsan 1
fabric-binding database vsan 1
swwn 11:00:02:01:aa:bb:cc:00 domain 4
fabric-binding activate vsan 1
zone default-zone permit vsan 1
ficon vsan 1
no host port control
```

```
fcdomain domain 3 static vsan 2
fcdomain restart disruptive vsan 2
fabric-binding activate vsan 2 force
zone default-zone permit vsan 2
ficon vsan 2
no host port control
no active equals saved
```

```
vsan database
vsan 3
fcdomain domain 5 static vsan 3
fcdomain restart disruptive vsan 3
fabric-binding activate vsan 3 force
zone default-zone permit vsan 3
ficon vsan 3
no snmp port control
no active equals saved
```

Would you like to edit the configuration? (yes/no) [no]: **no**

ステップ 14 この設定を使用および保存する場合は、**yes** と入力します (デフォルトは **yes**)。実装されたコマンドが表示されます。指定された **VSAN** で **FICON** が有効になった後で、**EXEC** モード スイッチ プロンプトが再び表示されます。

Use this configuration and apply it? (yes/no) [yes]: **yes**

```
`fcdomain domain 2 static vsan 1`
`fcdomain restart disruptive vsan 1`
`fabric-binding database vsan 1`
`swwn 11:00:02:01:aa:bb:cc:00 domain 4`
`fabric-binding activate vsan 1`
`zone default-zone permit vsan 1`
`ficon vsan 1`
`no host port control`

`fcdomain domain 3 static vsan 2`
`fcdomain restart disruptive vsan 2`
`fabric-binding activate vsan 2 force`
`zone default-zone permit vsan 2`
`ficon vsan 2`
`no host port control`
`no active equals saved`
```



(注) 新しい **VSAN** が作成された場合、2 つの追加コマンド (**vsan database** と **vsan number**) が表示されます。

```

`vsan database`
`vsan 3`
`in-order-guarantee vsan 3`
`fcdomain domain 2 static vsan 3`
`fcdomain restart disruptive vsan 3`
`fabric-binding activate vsan 3 force`
`zone default-zone permit vsan 3`
`ficon vsan 3`
`no snmp port control`
Performing fast copy config...done.
switch#

```

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](#)」セクション(10-24 ページ)に進んでください。

VSAN 上で FICON を手動で有効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# vsan database switch(config-vsan-db)# vsan 5 switch(config-vsan-db)# do show vsan usage 4 vsan configured configured vsans:1-2,5,26 vsans available for configuration:3-4,6-25,27-4093 switch(config-vsan-db)# exit	VSAN 5 を有効にします。
ステップ 3	switch(config)# in-order-guarantee vsan 5	VSAN 5 の順序どおりの配信をアクティブにします。 第6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。
ステップ 4	switch(config)# fcdomain domain 2 static vsan 2	VSAN 2 のドメイン ID を設定します。 ドメインパラメータの設定の詳細については、『 <i>Cisco MDS 9000 Family NX-OS System Management Configuration Guide</i> 』を参照してください。
ステップ 5	switch(config)# fabric-binding activate vsan 2 force	VSAN 2 のファブリック バインディングをアクティブにします。 『 <i>Cisco MDS 9000 Family NX-OS Security Configuration Guide</i> 』を参照してください。

	コマンド	目的
ステップ 6	<code>switch(config)# zone default-zone permit vsan 2</code>	VSAN 2 に許可するデフォルトゾーンを設定します。 「CUP インバンド管理」セクション (10-45 ページ) を参照してください。
ステップ 7	<code>switch(config)# ficon vsan 2</code> <code>switch(config-ficon)#</code>	VSAN 2 で FICON を有効にします。
	<code>switch(config)# no ficon vsan 6</code>	VSAN 6 で FICON 機能を無効にします。
ステップ 8	<code>switch(config-ficon)# no host port control</code>	メインフレーム ユーザに対し、スイッチをオフライン状態に移行することを禁止します。 「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」セクション (10-22 ページ) を参照してください。

[code-page] オプションの設定

FICON スtring は、拡張 2 進化 10 進コード (EBCDIC) 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、オプションです。使用する EBCDIC フォーマットが不明な場合は、**us-canada** (デフォルト) オプションを引き続き使用することを推奨します。

VSAN で [code-page] オプションを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>switch# config t</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>switch(config)# ficon vsan 2</code> <code>switch(config-ficon)#</code>	VSAN 2 で FICON を有効にします。
ステップ 3	<code>switch(config-ficon)# code-page italy</code>	italy EBCDIC フォーマットを設定します。
	<code>switch(config-ficon)# no code-page</code>	us-canada EBCDIC フォーマットを使用する出荷時デフォルトに戻します。

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。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 CUP に送信します。

ホストでスイッチをオフライン状態に移行できるようにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# ficon vsan 2 switch(config-ficon)#	VSAN 2 で FICON を有効にします。
ステップ 3	switch(config-ficon)# no host control switch offline	メインフレーム ユーザに対し、スイッチをオフライン状態に移行することを禁止します。
	switch(config-ficon)# host control switch offline	ホストでスイッチをオフライン状態(デフォルト)に移行できるようにし、ポートをシャットダウンします。

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。

メインフレーム ユーザが FICON パラメータを設定できるようにするには、**host port control** コマンドを使用します。

ホスト(メインフレーム)で Cisco MDS スイッチの FICON パラメータの設定を許可するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# ficon vsan 2 switch(config-ficon)#	VSAN 2 で FICON を有効にします。
ステップ 3	switch(config-ficon)# no host port control	メインフレーム ユーザに対し、Cisco MDS スイッチで FICON パラメータの設定を禁止します。
	switch(config-ficon)# host port control	メインフレーム ユーザに対し、Cisco MDS スイッチで FICON パラメータの設定を許可します(デフォルト)。

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 ファミリー 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。

VSAN クロックの現行時刻は、`show ficon vsan vsan-id`、`show ficon` および `show accounting log` コマンドの出力に示されます。

タイムスタンプのホスト制御を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>switch# config t</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>switch(config)# ficon vsan 2</code> <code>switch(config-ficon)#</code>	VSAN 2 で FICON を有効にします。
ステップ 3	<code>switch(config-ficon)# no host set-timestamp</code>	メインフレーム ユーザに対し、VSAN 固有のクロックを変更することを禁止します。
	<code>switch(config-ficon)# host set-timestamp</code>	ホストでこのスイッチのクロックを設定できるようにします(デフォルト)。

タイムスタンプのクリア



(注) タイムスタンプは、メインフレームではなく Cisco MDS スイッチでのみクリアできます。

VSAN クロックをクリアするには、EXEC モードで `clear ficon vsan vsan-id timestamp` コマンドを使用します。

```
switch# clear ficon vsan 20 timestamp
```

FICON パラメータの SNMP 制御の設定

FICON パラメータの SNMP 制御を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>switch# config t</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>switch(config)# ficon vsan 2</code> <code>switch(config-ficon)#</code>	VSAN 2 で FICON を有効にします。
ステップ 3	<code>switch(config-ficon)# no snmp port control</code>	SNMP ユーザに対し FICON パラメータの設定を禁止します。
	<code>switch(config-ficon)# snmp port control</code>	SNMP ユーザに対し FICON パラメータの設定を許可します(デフォルト)。

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。

FICON デバイスの従属関係のクリア

現在のデバイス従属関係をクリアするには、EXEC モードで **clear ficon vsan vsan-id allegiance** コマンドを実行します。

```
switch# clear ficon vsan 1 allegiance
```

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、スイッチのリポート後も、新しい設定が消去されずに済みます。デフォルトでは、**active equals saved** オプションがすべての FICON VSAN で自動的に有効になっています。

表 10-2 は、さまざまなシナリオでの Active = Saved オプション **active equals saved** コマンドの結果と、実行コンフィギュレーションからスタートアップ コンフィギュレーションに暗黙的にコピーした結果 (**copy running start**) **copy running-config startup-config** コマンドを示したものです。

active equals saved コマンドがファブリック内のどの FICON 対応 VSAN でも有効になっている場合は、次の保存方式が適用されます(表 10-2 の番号 1 と 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」セクション(10-34 ページ)を参照)。

active equals saved コマンドがファブリック内のすべての FICON 対応 VSAN でも有効になっていない場合、FICON 固有の設定変更が IPL ファイルに保存されず、暗黙の **copy running startup** コマンドが実行されないため、**copy running start** コマンドを明示的に実行する必要があります(表 10-2 の 3 を参照)。

表 10-2 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 ¹ copy running start が発行されたかどうか	注
1	はい	(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	はい	(1 つの FICON VSAN で) イネーブル	暗黙的	active equals saved オプションがイネーブルな VSAN でだけ、FICON の変更は 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。

表 10-2 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 ¹ copy running start が発行されたかどうか	注
3	はい	(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	いいえ	N/A		

1. Cisco NX-OS ソフトウェアが、Cisco MDS スイッチで **copy running-config startup-config** コマンドを暗黙的に実行する場合、バイナリ設定だけが生成され、ASCII 設定は生成されません(例 10-24(10-53 ページ)を参照)。この段階で追加の ASCII 設定を生成する場合は、**copy running-config startup-config** コマンドを明示的に再度発行する必要があります。



(注)

active equals saved が有効な場合、Cisco NX-OS ソフトウェアでは、FICON 設定で **copy running startup** コマンドを実行する必要がありません。スイッチまたはファブリックが複数の FICON 対応 VSAN で構成されており、これらの VSAN の 1 つで **active equals saved** が有効な場合、FICON 以外の設定を変更すると、すべての設定がスタートアップ コンフィギュレーションに保存されます。

実行コンフィギュレーションを自動的に保存するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# ficon vsan 2 switch(config-ficon)#	VSAN 2 で FICON を有効にします。
ステップ 3	switch(config-ficon)# active equals saved switch(config-ficon)# no active equals saved	スイッチまたはファブリック内のすべての VSAN の自動保存機能をイネーブルにします。 この VSAN の自動保存を無効にします。

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。

この項では、次のトピックについて取り上げます。

- [PortChannel へのポート番号のバインド \(10-26 ページ\)](#)
- [FCIP インターフェイスへのポート番号のバインド \(10-26 ページ\)](#)
- [ポートブロックの設定 \(10-26 ページ\)](#)
- [ポートの禁止 \(10-27 ページ\)](#)
- [ポート アドレス名の割り当て \(10-29 ページ\)](#)

- [RLIR の概要 \(10-29 ページ\)](#)
- [RLIR 優先ホストの指定 \(10-29 ページ\)](#)
- [RLIR 情報の表示 \(10-30 ページ\)](#)
- [RLIR 情報のクリア \(10-34 ページ\)](#)

PortChannel へのポート番号のバインド



注意

FICON がすべての VSAN で無効になっていると、PortChannel または FCIP インターフェイスへのポート番号割り当てがすべて失われます(復元できません)。

PortChannel を FICON ポート番号にバインドする(関連付ける)と、そのインターフェイスを起動できます。

FICON ポート番号に PortChannel をバインドするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# interface Port-channel 1 switch(config-if)#	PortChannel インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# ficon portnumber 234	選択された PortChannel ポートに FICON ポート番号を割り当てます。

FCIP インターフェイスへのポート番号のバインド

FICON ポート番号に FCIP インターフェイスをバインドする(関連付ける)ことで、そのインターフェイスを起動できます。

FICON ポート番号に FCIP インターフェイスをバインドするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch1(config)# interface fcip 51 switch1(config-if)#	FCIP インターフェイス (51) を作成します。
ステップ 3	switch(config-if)# ficon portnumber 208	選択された FCIP インターフェイスに FICON ポート番号を割り当てます。

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) FICON VSAN 内のゾーン分割デバイスは、現在禁止されている FICON ポートと競合する可能性があるため、使用しないでください。ゾーン分割とポート禁止を同一 VSAN 内で使用することは推奨されません。



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。

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には、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# ficon vsan 2 switch(config-ficon)#	VSAN 2 で FICON を有効にします。
ステップ 3	switch(config-ficon)# portaddress 1 - 5 switch(config-ficon-portaddr)#	詳細な設定を行うため、ポート アドレス 1 ~ 5 を選択します。
ステップ 4	switch(config-ficon-portaddr)# block	一連のポート アドレスを無効にし、運用停止状態で維持します。
	switch(config-ficon-portaddr)# no block	選択されたポート アドレスを有効にし、工場出荷時デフォルト (ポート アドレスがブロックされていない状態) に戻します。

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、非稼働状態のポートは、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。

ポート禁止のデフォルト状態の設定

デフォルトでは、スイッチに実装されるインターフェイスではポート禁止が無効になっています。Cisco MDS SAN-OS Release 3.0(2) の時点では、各自が作成した VSAN でデフォルトのポート禁止状態を有効に変更し、実装されるポートで必要に応じてポート禁止を無効にすることを選択できます。また、デフォルトの変更後に作成された FICON コンフィギュレーションファイルでのみ、新しいデフォルト設定が反映されます(「[FICON コンフィギュレーションファイル](#)」セクション(10-34 ページ)を参照)。

スイッチに実装されているすべてのインターフェイスでデフォルトのポート禁止設定を変更するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# ficon port default-state prohibit-all	スイッチで実装されているすべてのインターフェイスのデフォルトとして、ポート禁止を有効にします。
	switch(config)# no ficon port default-state prohibit-all	スイッチで実装されているすべてのインターフェイスのデフォルトとして、ポート禁止を無効にします(デフォルト)。

ポート禁止のデフォルト状態の設定を表示するには、**show ficon port default-state** コマンドを使用します。

```
switch# show ficon port default-state
Port default state is prohibit-all
```

ポート禁止の設定

VSAN のポート アドレスを禁止する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# ficon vsan 2 switch(config-ficon)#	VSAN 2 で FICON を有効にします。
ステップ 3	switch(config-ficon)# portaddress 7 switch(config-ficon-portaddr)#	詳細な設定を行うため、ポート アドレス 7 を選択します。
ステップ 4	switch(config-ficon-portaddr)# prohibit portaddress 3-5	VSAN 2 のポート アドレス 7 に対し、ポート 3、4、および 5 に対する通信を禁止します。
	switch(config-ficon-portaddr)# no prohibit portaddress 5	以前の禁止状態からポート アドレス 5 を解除します。

ポート アドレス名の割り当て

ポート アドレス名を割り当てるには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# ficon vsan 2 switch(config-ficon)#	VSAN 2 で FICON を有効にします。
ステップ 3	switch(config-ficon)# portaddress 7 switch(config-ficon-portaddr)#	詳細な設定を行うため、ポート アドレス 7 を選択します。
ステップ 4	switch(config-ficon-portaddr)# name SampleName	ポート アドレスに名前を割り当てます。 (注) ポート アドレス名は、24 文字までの英数字に制限されています。
	switch(config-ficon-portaddr)# no name SampleName	以前に設定されたポート アドレス名を削除します。

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。

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。

copy running-config startup-config コマンドを入力すると、RLIR データが永続ストレージに書き込まれます。

RLIR 優先ホストの指定

Cisco MDS SAN-OS Release 3.0(3) では、RLIR フレームを受信する優先ホストを指定できます。MDS スイッチが優先ホストに RLIR フレームを送信するのは、次の条件が満たされた場合だけです。

- VSAN 内に、登録機能が「always receive」に設定され、RLIR に登録されているホストがない。VSAN に「always receive」として登録されているホストが 1 つ以上ある場合、RLIR はそれらのホストにのみ送信され、設定された優先ホストには送信されません。
- 優先ホストが、登録機能が「conditionally receive」に設定されて登録されている。



(注) 登録されているすべてのホストの登録機能が「conditionally receive」に設定されている場合は優先ホストが RLIR フレームを受信します。

指定できる RLIR 優先ホストは、VSAN ごとに 1 つだけです。デフォルトでは、登録機能が「always receive」に設定されているホストがない場合、スイッチは登録機能が「conditionally receive」に設定されている VSAN のホストの 1 つに RLIR フレームを送信します。

VSAN の RLIR 優先ホストを指定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# rlir preferred-cond fcid 0x772c00 vsan 5	VSAN 5 の RLIR 優先ホストとして FC ID 0x772c00 を指定します。(FC ID 0x772c00 は一例です。)
	switch(config)# no rlir preferred-cond fcid 0x654321 vsan 2	VSAN 5 の RLIR 優先ホストとして FC ID 0x772c00 を削除します。

RLIR 優先ホスト設定を表示するには、**show rlir erl** コマンドを使用します。

```
switch# show rlir erl
Established Registration List for VSAN: 5
-----
FC-ID LIRR FORMAT REGISTERED FOR
-----
0x772c00 0x18 conditional receive(*)
0x779600 0x18 conditional receive
0x779700 0x18 conditional receive
0x779800 0x18 conditional receive
Total number of entries = 4
(*) - Denotes the preferred host
```

RLIR 情報の表示

show rlir statistics コマンドは、LIRR、RLIR、および DRLIR フレームの完全な統計情報を表示します。受信フレーム数、送信フレーム数、および拒否フレーム数が表示されます。特定の VSAN の VSAN 統計情報を取得するため、VSAN ID を指定します。VSAN ID を指定しないと、アクティブなすべての VSAN の統計情報が表示されます(例 10-1 および 10-2 を参照)。

例 10-1 すべての VSAN の RLIR 統計情報の表示

```
switch# show rlir statistics

Statistics for VSAN: 1
-----

Number of LIRR received      = 0
Number of LIRR ACC sent     = 0
Number of LIRR RJT sent     = 0
Number of RLIR sent         = 0
Number of RLIR ACC received = 0
Number of RLIR RJT received = 0
Number of DRLIR received   = 0
Number of DRLIR ACC sent   = 0
Number of DRLIR RJT sent   = 0
Number of DRLIR sent       = 0
Number of DRLIR ACC received = 0
Number of DRLIR RJT received = 0
```

```

Statistics for VSAN: 100
-----
Number of LIRR received      = 26
Number of LIRR ACC sent     = 26
Number of LIRR RJT sent     = 0
Number of RLIR sent         = 815
Number of RLIR ACC received = 815
Number of RLIR RJT received = 0
Number of DRLIR received   = 417
Number of DRLIR ACC sent   = 417
Number of DRLIR RJT sent   = 0
Number of DRLIR sent       = 914
Number of DRLIR ACC received = 828
Number of DRLIR RJT received = 0

```

例 10-2 指定した VSAN の RLIR 統計情報の表示

```

switch# show rlir statistics vsan 4

Statistics for VSAN: 4
-----
Number of LIRR received      = 0
Number of LIRR ACC sent     = 0
Number of LIRR RJT sent     = 0
Number of RLIR sent         = 0
Number of RLIR ACC received = 0
Number of RLIR RJT received = 0
Number of DRLIR received   = 0
Number of DRLIR ACC sent   = 0
Number of DRLIR RJT sent   = 0
Number of DRLIR sent       = 0
Number of DRLIR ACC received = 0
Number of DRLIR RJT received = 0

```

show rlir erl コマンドは、スイッチで RLIR 受信のために登録されている Nx ポートのリストを表示します。VSAN ID を指定しない場合は、すべてのアクティブ VSAN の詳細が表示されます(例 10-3 および 10-4 を参照)。

例 10-3 すべての ERL の表示

```

switch# show rlir erl

Established Registration List for VSAN: 2
-----
FC-ID      LIRR FORMAT  REGISTERED FOR
-----
0x0b0200   0x18         always receive
Total number of entries = 1

Established Registration List for VSAN: 100
-----
FC-ID      LIRR FORMAT  REGISTERED FOR
-----
0x0b0500   0x18         conditional receive
0x0b0600   0x18         conditional receive
Total number of entries = 2

```

例 10-3 では [Registered For] 列に FC ID が conditional receive であると示されている場合に、後続の RLIR の有効な受信者として送信元ポートが登録されます。他の ERL の受信者が選択されない場合にのみ、この送信元ポートが RLIR の受信者として選択されます。

例 10-3 では [Registered For] 列に FC ID が always receive であると示されている場合に、後続の RLIR の有効な受信者として送信元ポートが登録されます。この送信元ポートは LIR の受信者として常に選択されます。



(注) どの N ポートにも always receive RLIR が登録されていない場合、または RLIR の配信がいずれかのポートで失敗する場合は、conditional receive RLIR に登録されているポートに RLIR が送信されます。

例 10-4 指定された VSAN の ERL の表示

```
switch# show rllr erl vsan 100
Established Registration List for VSAN: 100
-----
FC-ID          LIRR FORMAT    REGISTERED FOR
-----
0x0b0500      0x18           conditional receive
0x0b0600      0x18           conditional receive

Total number of entries = 2
```



(注) 例 10-5 から 例 10-7 では、ホストのタイムスタンプ(*で示す)が使用可能な場合、スイッチのタイムスタンプと共に出力されます。ホストのタイムスタンプが使用可能ではない場合は、スイッチのタイムスタンプだけが出力されます。

例 10-5 LIR 履歴の表示

```
switch# show rllr history

Link incident history
-----
*Host Time Stamp
Switch Time Stamp          Port   Interface  Link Incident
-----
*Sun Nov 30 21:47:28 2003
Sun Nov 30 13:47:55 2003      2      fc1/2      Implicit Incident
*Sun Nov 30 22:00:47 2003
Sun Nov 30 14:01:14 2003      2      fc1/2      NOS Received
*Sun Nov 30 22:00:55 2003
Sun Nov 30 14:01:22 2003      2      fc1/2      Implicit Incident
*Mon Dec 1 20:14:26 2003
Mon Dec 1 12:14:53 2003      4      fc1/4      Implicit Incident
*Mon Dec 1 20:14:26 2003
Mon Dec 1 12:14:53 2003      4      fc1/4      Implicit Incident
*Thu Dec 4 04:43:32 2003
Wed Dec 3 20:43:59 2003      2      fc1/2      NOS Received
*Thu Dec 4 4:43:41 2003
Wed Dec 3 20:44:08 2003      2      fc1/2      Implicit Incident
*Thu Dec 4 4:46:53 2003
Wed Dec 3 20:47:20 2003      2      fc1/2      NOS Received
*Thu Dec 4 4:47:05 2003
Wed Dec 3 20:47:32 2003      2      fc1/2      Implicit Incident
*Thu Dec 4 4:48:07 2003
Wed Dec 3 20:48:34 2003      2      fc1/2      NOS Received
```

```
*Thu Dec 4 04:48:39 2003
Wed Dec 3 20:49:06 2003      2      fc1/2  Implicit Incident
*Thu Dec 4 5:02:20 2003
Wed Dec 3 21:02:47 2003      2      fc1/2  NOS Received
...
```

例 10-6 指定されたインターフェイスの最近の LIR の表示

```
switch# show rlir recent interface fc1/1-4

Recent link incident records
-----
Host Time Stamp          Switch Time Stamp          Port Intf  Link Incident
-----
Thu Dec 4 05:02:29 2003  Wed Dec 3 21:02:56 2003  2    fc1/2  Implicit Incident
Thu Dec 4 05:02:54 2003  Wed Dec 3 21:03:21 2003  4    fc1/4  Implicit Incident
```

例 10-7 指定されたポート番号の最近の LIR の表示

```
switch# show rlir recent portnumber 1-4

Recent link incident records
-----
Host Time Stamp          Switch Time Stamp          Port Intf  Link Incident
-----
Thu Dec 4 05:02:29 2003  Wed Dec 3 21:02:56 2003  2    fc1/2  Implicit Incident
Thu Dec 4 05:02:54 2003  Wed Dec 3 21:03:21 2003  4    fc1/4  Implicit Incident
```

Cisco SAN-OS Release 3.0(3) 以降、**show rlir history** コマンド出力には、他のスイッチから DRLIR として受信したリモート リンク インシデントが示されます。RLIR は、以前の Cisco NX-OS リリースと同様に DRLIR の結果として生成されます(例 10-8 を参照)。

例 10-8 Cisco SAN-OS Release 3.0(3) の LIR 履歴の表示

```
switch# show rlir history

Link incident history
-----
Host Time Stamp          Switch Time Stamp          VSAN  Domain  Port  Intf  Link Incident  Loc/Rem
-----
Sep 20 12:42:44 2006     Sep 20 12:42:44 2006     ****  ****   0x0b  fc1/12  Loss of sig/sync  LOC
Reported Successfully to: [0x640001] [0x640201]
Sep 20 12:42:48 2006     Sep 20 12:42:48 2006     ****  ****   0x0b  fc1/12  Loss of sig/sync  LOC
Reported Successfully to: [0x640001] [0x640201]
*** ** *:*:** ****     Sep 20 12:42:51 2006     1001  230    0x12  ****   Loss of sig/sync  REM
Reported Successfully to: [0x640001] [0x640201]
Sep 20 12:42:55 2006     Sep 20 12:42:55 2006     ****  ****   0x0b  fc1/12  Loss of sig/sync  LOC
Reported Successfully to: None [No Registrations]
*** ** *:*:** ****     Sep 20 12:45:56 2006     1001  230    0x12  ****   Loss of sig/sync  REM
Reported Successfully to: None [No Registrations]
*** ** *:*:** ****     Sep 20 12:45:56 2006     1001  230    0x12  ****   Loss of sig/sync  REM
Reported Successfully to: None [No Registrations]
Sep 20 12:52:45 2006     Sep 20 12:52:45 2006     ****  ****   0x0b  fc1/12  Loss of sig/sync  LOC
Reported Successfully to: None [No Registrations]

**** - Info not required/unavailable
```

RLIR 情報のクリア

指定された VSAN の既存の統計情報をすべてクリアするには、**clear rlr statistics** コマンドを使用します。

```
switch# clear rlr statistics vsan 1
```

すべてのインターフェイスのすべてのリンク インシデント レコードが記録されている RLIR 履歴をクリアするには、**clear rlr history** コマンドを使用します。

```
switch# clear rlr history
```

指定したインターフェイスの最近の RLIR 情報をクリアするには、**clear rlr recent interface** コマンドを使用します。

```
switch# clear rlr recent interface fc 1/2
```

指定したポート番号の最近の RLIR 情報をクリアするには、**clear rlr recent portnumber** コマンドを使用します。

```
switch# clear rlr recent portnumber 16
```

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 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。

この項では、次のトピックについて取り上げます。

- [FICON コンフィギュレーション ファイルの概要 \(10-35 ページ\)](#)
- [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 \(10-35 ページ\)](#)
- [FICON コンフィギュレーション ファイルの編集 \(10-36 ページ\)](#)
- [FICON コンフィギュレーション ファイルの表示 \(10-36 ページ\)](#)
- [FICON コンフィギュレーション ファイルのコピー \(10-38 ページ\)](#)

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

保存されているファイルの設定を実行コンフィギュレーションに適用するには、`ficon vsan number apply file filename` コマンドを使用します。

```
switch# ficon vsan 2 apply file SampleFile
```

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。

指定された FICON コンフィギュレーションファイルの内容を編集するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# ficon vsan 2 switch(config-ficon)#	VSAN 2 で FICON を有効にします。
ステップ 3	switch(config-ficon)# file IplFile1 switch(config-ficon-file)#	VSAN 2 の FICON コンフィギュレーションファイル IplFile1 にアクセスします。このファイルが存在しない場合は、作成されます。 (注) すべての FICON ファイル名は、最大 8 文字の英数字に制限されています。
	switch(config-ficon)# no file IplFileA	以前に作成された 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 4	switch(config-ficon-file)# portaddress 3 switch(config-ficon-file-portaddr)#	ポート アドレス 3 のサブモードを開始して、IplFile1 という名前のコンフィギュレーションファイルの内容を編集します。 (注) 実行コンフィギュレーションは現在の設定に適用されません。設定が適用されるのは、 ficon vsan number apply file filename コマンドが実行される場合だけです。
ステップ 5	switch(config-ficon-file-portaddr)# prohibit portaddress 5	コンフィギュレーションファイル IplFile1 の内容を編集し、ポート アドレス 5 に対してポート アドレス 3 へのアクセスを禁止します。
ステップ 6	switch(config-ficon-file-portaddr)# block	コンフィギュレーションファイル IplFile1 の内容を編集し、特定のポート アドレス範囲をブロックし、運用停止状態で維持します。
ステップ 7	switch(config-ficon-file-portaddr)# name P3	コンフィギュレーションファイル IplFile1 の内容を編集し、P3 という名前をポート アドレス 3 に割り当てます。この名前が存在しない場合は、作成されます。存在する場合は上書きされます。

FICON コンフィギュレーションファイルの表示

すべての FICON コンフィギュレーションファイルの内容を表示するには、**show ficon vsan vsan-id file all** コマンドを使用します。

```
switch# show ficon vsan 2 file all
File IPL      is locked
FICON configuration file IPLFILEA in vsan 2
```

```

Description:
  Port address 0(0)
    Port name is
    Port is not blocked
    Prohibited port addresses are 250-253,255(0xfa-0xfd,0xff)

  Port address 1(0x1)
    Port name is
    Port is not blocked
    Prohibited port addresses are 250-253,255(0xfa-0xfd,0xff)
Port address 2(0x2)
  Port name is
  Port is not blocked
  Prohibited port addresses are 250-253,255(0xfa-0xfd,0xff)

  Port address 3(0x3)
    Port name is P3
    Port is blocked
    Prohibited port addresses are 5,250-253,255(0x5,0xfa-0xfd,0xff)
..

```

特定の FICON コンフィギュレーション ファイルの内容を表示するには、**show ficon vsan vsan-id file name** コマンドを使用します。

```

switch# show ficon vsan 2 file name IPLfilea
FICON configuration file IPLFILEA in vsan 2
Description:
  Port address 0(0)
    Port name is
    Port is not blocked
    Prohibited port addresses are 250-253,255(0xfa-0xfd,0xff)

  Port address 1(0x1)
    Port name is
    Port is not blocked
    Prohibited port addresses are 250-253,255(0xfa-0xfd,0xff)

  Port address 2(0x2)
    Port name is
    Port is not blocked
    Prohibited port addresses are 250-253,255(0xfa-0xfd,0xff)

  Port address 3(0x3)
    Port name is P3
    Port is blocked
    Prohibited port addresses are 5,250-253,255(0x5,0xfa-0xfd,0xff)

```

特定の FICON ポートの FICON コンフィギュレーション ファイルの情報を表示するには、**show ficon vsan vsan-id file name filename portaddress** コマンドを使用します。

```

switch# show ficon vsan 2 file name IPLfilea portaddress 3
FICON configuration file IPLFILEA in vsan 2
Description:
  Port address 3(0x3)
    Port name is P3
    Port is blocked
    Prohibited port addresses are 5,250-253,255(0x5,0xfa-0xfd,0xff)

```

FICON コンフィギュレーション ファイルのコピー

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には、EXEC モードで **ficon vsan vsan-id copy file existing-file-name save-as-file-name** コマンドを使用します。

```
switch# ficon vsan 20 copy file IPL IPL3
```

既存のコンフィギュレーション ファイルのリストを表示するには、**show ficon vsan vsan-id** コマンドを実行します。

```
switch# show ficon vsan 20
Ficon information for VSAN 20
  Ficon is online
  VSAN is active
  Host port control is Enabled
  Host offline control is Enabled
  User alert mode is Disabled
  SNMP port control is Enabled
  Host set director timestamp is Enabled
  Active=Saved is Enabled
  Number of implemented ports are 250
  Key Counter is 5
  FCID last byte is 0
  Date/Time is same as system time (Wed Dec 3 20:10:45.924591 2003)
  Device Allegiance not locked
  Codepage is us-canada
Saved configuration files
  IPL
  IPL3
```

ポートスワッピング

FICON ポートスワッピング機能は、メンテナンス専用を提供されています。

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

[Active=Saved] チェックボックスをオンにすると、任意の FICON VSAN 上で **active equals saved** が有効になり、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。それ以外の場合は、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わると、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。

ポートを稼働状態にする際は、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。

ficon swap portnumber コマンドは、対象の2つのポートにのみ関連します。この VSAN に依存しないコマンドを EXEC モードで実行する必要があります。Cisco MDS NX-OS は、ポート スワップを実行する前に VSAN でポート番号の重複を調べます。

ficon swap portnumber old-port-number new-port-number after swap noshut コマンドを指定してポートを起動する場合は、**no shutdown** コマンドを明示的に実行してトラフィックを再開する必要があります。

この項では、次のトピックについて取り上げます。

- [ポート スワッピングの概要 \(10-39 ページ\)](#)
- [ポート スワッピング \(10-40 ページ\)](#)

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 ガイドラインは、ポート スワップ設定にも適用されます (『Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide』を参照)。

ポート スワッピング

スイッチ上に重複するポート番号がない場合は、物理ファイバ チャンネル ポート (ポート番号を除く) を次の手順でスワップできます。

ステップ 1 EXEC モードで **fiction swap portnumber old-port-number new-port-number** コマンドを発行します。



(注) MDS スイッチで、コマンドに指定されている *old-port-number* または *new-port-number* と同じポート番号のインターフェイスが複数ある場合、**fiction swap portnumber** コマンドは失敗する可能性があります。

指定したポートはシャットダウンされます。

ステップ 2 2つのポート間の前面パネル ポート ケーブルを物理的に交換できます。

ステップ 3 各ポートで **no shutdown** コマンドを実行し、トラフィック フローを許可します。



(注) **fiction swap portnumber old-port-number new-port-number after swap noshut** コマンドを指定すると、ポートは自動的に初期化されます。

スイッチで重複するポート番号がある場合は、物理ファイバ チャンネル ポート (重複するポート番号を含む) を次の手順でスワップできます。

ステップ 1 EXEC モードで **fiction swap interface old-interface new-interface** コマンドを実行します。

指定したインターフェイスはシャットダウンされます。

ステップ 2 2つのポート間の前面パネル ポート ケーブルを物理的に交換できます。

ステップ 3 各ポートで **no shutdown** コマンドを実行し、トラフィック フローを許可します。



(注) **fiction swap interface old-interface new-interface after swap noshut** コマンドを指定すると、ポートは自動的に初期化されます。

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 ヘッドの操作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 テープ読み取りアクセラレーションは、Cisco MDS NX-OS Release 5.0(1) 以降でサポートされています。詳細については、「[FICON テープ読み取りアクセラレーション設定](#)」セクション (10-43 ページ) を参照してください。

図 10-5 図 10-8 に、サポートされている設定を示します。

図 10-5 IBM/StorageTek (STK) ライブラリに直接アクセスするホスト



図 10-6 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

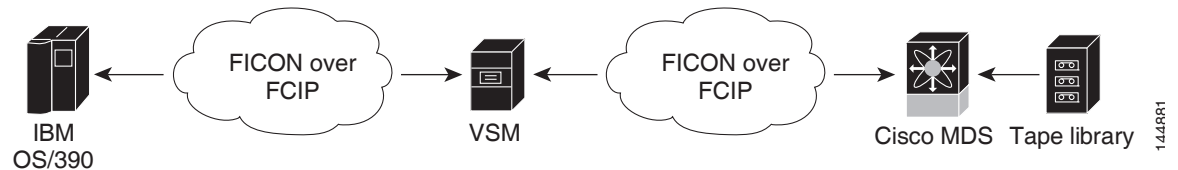
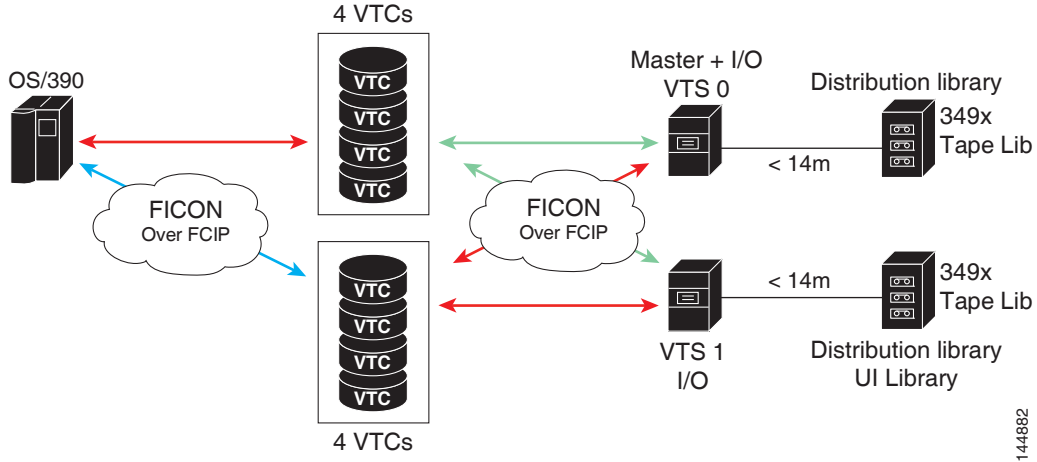
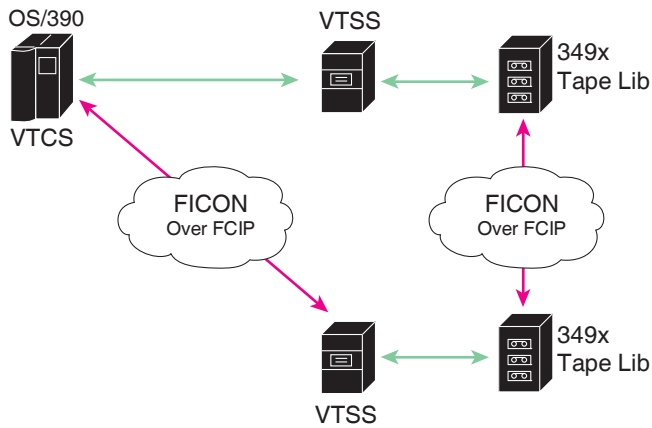


図 10-7 ピアツーピア Virtual Tape Server (VTS) にアクセスするホスト



144882

図 10-8 ピアツーピア Virtual Tape Server (VTS) にアクセスするホスト



144883



(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。

FICON テープ アクセラレーションを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# interface fcip 2 switch(config-if)#	FCIP インターフェイスを指定し、インターフェイス コンフィギュレーション サブモードを開始します。
ステップ 3	switch(config-if)# ficon-tape-accelerator vsan 100 This configuration change will disrupt all traffic on the FCIP interface in all VSANs.Do you wish to continue? [no] y	FCIP インターフェイスを介した FICON テープ アクセラレーションをイネーブルにします。
	switch(config-if)# no ficon-tape-accelerator vsan 100 This configuration change will disrupt all traffic on the FCIP interface in all VSANs.Do you wish to continue? [no] y	FCIP インターフェイスを介した FICON テープ アクセラレーションをディセーブルにします(デフォルト)。

show running-config コマンドを使用して、FCIP 設定で FICON テープ アクセラレーションを確認します。

```
switch# show running-config | begin "interface fcip"
interface fcip2
  ficon-tape-accelerator vsan 100
  no shutdown
...
```

FICON テープ読み取りアクセラレーション設定

FICON テープ アクセラレーションに適用される設定のガイドラインと制限はすべて、FICON テープ読み取りアクセラレーションにも適用されます。FICON テープ アクセラレーションと FICON テープ読み取りアクセラレーションは共存可能です。

FICON テープ読み取りアクセラレーションを有効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# interface fcip 2 switch(config-if)#	FCIP インターフェイスを指定し、インターフェイス コンフィギュレーション サブモードを開始します。

	コマンド	目的
ステップ 3	switch(config-if)# ficon-tape-read-accelerator This configuration change will disrupt all traffic on the FCIP interface in all VSANs.Do you wish to continue? [no] y	FCIP インターフェイスを介した FICON テープ読み取りアクセラレーションを有効にします。
	switch(config-if)# no ficon-tape-read-accelerator This configuration change will disrupt all traffic on the FCIP interface in all VSANs.Do you wish to continue? [no] y	FCIP インターフェイスを介した FICON テープ読み取りアクセラレーションを無効にします(デフォルト)。

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。

XRC テープ アクセラレーションを有効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface fcip 2 switch(config)#	FCIP トンネル インターフェイスを指定し、インターフェイス コンフィギュレーション サブモードを開始します。
ステップ 3	switch(config-if)# ficon-xrc-emulator switch(config)#	FCIP インターフェイスを介した XRC アクセラレーションを有効にします。
	switch(config-if)# no ficon-xrc-emulator switch(config)#	FCIP トンネル インターフェイスを介した XRC アクセラレーションを無効にします(デフォルト)。



(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有効にできないため、同一の VSAN 上には存在できません。

FICON VSAN のオフライン状態への移行

VSAN で停止する必要があるすべてのポートをログアウトするには、EXEC モードで **ficon vsan vsan-id offline** コマンドを実行します。

オフライン状態を解除し、ポートが再びログオンできるようにするには、EXEC モードで EXEC レベルの **ficon vsan vsan-id online** コマンドを実行します。



(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」セクション(10-22 ページ)を参照)。

CUP インバンド管理

CUP プロトコルを介して、アクセス コントロールの設定が行われ、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。

この項では、次のトピックについて取り上げます。

- [ゾーンへの CUP の配置\(10-45 ページ\)](#)
- [制御ユニットの情報の表示\(10-46 ページ\)](#)

ゾーンへの CUP の配置

ゾーンに CUP を配置するには、次の手順を実行します。

ステップ 1 必要な VSAN に許可するデフォルト ゾーンを設定します。

```
switch# config t
switch(config)# zone default-zone permit vsan 20
```

ステップ 2 必要な VSAN に対して **show fcns database** コマンドを発行し、必須 FICON CUP WWN を取得します。

```
switch# show fcns database vsan 20
```

VSAN 20:

FCID	TYPE	PWWN	(VENDOR)	FC4-TYPE:FEATURE
0x0d0d00	N	50:06:04:88:00:1d:60:83	(EMC)	FICON:CU
0x0dfe00	N	25:00:00:0c:ce:5c:5e:c2	(Cisco)	FICON:CUP
0x200400	N	50:05:07:63:00:c2:82:d3	(IBM)	scsi-fcp FICON:CU f..
0x200800	N	50:05:07:64:01:40:15:0f	(IBM)	FICON:CH
0x20fe00	N	20:00:00:0c:30:ac:9e:82	(Cisco)	FICON:CUP

Total number of entries = 5



(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 WWN の pWWN をすべて追加する必要があります。前述の出力例には複数の FICON:CUP が含まれており、これはカスケード設定を示しています。

ステップ 3 示されている FICON:CUP WWN をゾーン データベースに追加します。

```
switch(config)# zone name Zone1 vsan 20
switch(config-zone)# member pwwn 25:00:00:0c:ce:5c:5e:c2
```

制御ユニットの情報の表示

例 10-9 に、設定されている制御デバイスの情報を示します。

例 10-9 制御ユニットの情報の表示

```
switch# show ficon control-device sb3
Control Unit Image:0x80b9c2c
VSAN:20 CU:0x20fe00 CUI:0 CUD:0 CURLP:(nil)
ASYNC LP:(nil) MODE:1 STATE:1 CQ LEN:0 MAX:0
PRIMARY LP: VSAN:0 CH:0x0 CHI:0 CU:0x0 CUI:0
ALTERNATE LP: VSAN:0 CH:0x0 CHI:0 CU:0x0 CUI:0
Logical Path:0x80b9fb4
VSAN:20 CH:0x200600 CHI:15 CU:0x20fe00 CUI:0 STATE:1 FLAGS:0x1
LINK: OH:0x0 OC:0x0 IH:0x0 IC:0x0
DEV: OH:0x0 OC:0x0 IH:0x0 IC:0x0
SENSE: 00 00 00 00 00 00 00 00 46
        30 20 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
IUI:0x0 DHF:0x0 CCW:0x0 TOKEN:0x0 PCCW:0x0 FCCW:0x0 PTOKEN:0x0 FTOKEN:0x0
CMD:0x0 CCW_FLAGS:0x0 CCW_COUNT:0 CMD_FLAGS:0x0 PRIO:0x0 DATA_COUNT:0
STATUS:0x0 FLAGS:0x0 PARAM:0x0 QTP:0x0 DTP:0x0
CQ LEN:0 MAX:0 DESTATUS:0x0
```

FICON 情報の表示

この項では、次のトピックについて取り上げます。

- [FICON アラートの受信 \(10-47 ページ\)](#)
- [FICON ポート アドレス情報の表示 \(10-47 ページ\)](#)
- [FICON コンフィギュレーション ファイル情報の表示 \(10-49 ページ\)](#)
- [設定された FICON の状態の表示 \(10-50 ページ\)](#)
- [ポート管理状態の表示 \(10-50 ページ\)](#)
- [バッファ情報の表示 \(10-51 ページ\)](#)
- [実行コンフィギュレーションの FICON 情報の表示 \(10-52 ページ\)](#)
- [スタートアップ コンフィギュレーションの FICON 情報の表示 \(10-53 ページ\)](#)
- [FICON 関連のログ情報の表示 \(10-53 ページ\)](#)

FICON アラートの受信

例 10-10 では、ユーザアラート モードが Enabled であり、FICON 設定の変更を示すアラートを受信することが出力に示されています。

例 10-10 設定された FICON 情報の表示

```
switch# show ficon
Ficon information for VSAN 20
  Ficon is online
  VSAN is active
  Host port control is Enabled
  Host offline control is Enabled
  User alert mode is Enabled
  SNMP port control is Enabled
  Host set director timestamp is Enabled
  Active=Saved is Disabled
  Number of implemented ports are 250
  Key Counter is 73723
  FCID last byte is 0
  Date/Time is set by host to Sun Jun 26 00:04:06.991999 1904
  Device allegiance is locked by Host
  Codepage is us-canada
  Saved configuration files
    IPL
    _TSIRN00
```

FICON ポート アドレス情報の表示

例 10-11 ~ 10-14 では、FICON ポート アドレス情報を表示します。

例 10-11 ポート アドレス情報の表示

```
switch# show ficon vsan 2 portaddress
Port Address 1 is not installed in vsan 2
  Port number is 1, Interface is fc1/1
  Port name is
  Port is not admin blocked
  Prohibited port addresses are 0,241-253,255

Port Address 2 is not installed in vsan 2
  Port number is 2, Interface is fc1/2
  Port name is
  Port is not admin blocked
  Prohibited port addresses are 0,241-253,255
...
Port Address 249 is not installed in vsan 2
  Port name is
  Port is not admin blocked
  Prohibited port addresses are 0,241-253,255

Port Address 250 is not installed in vsan 2
  Port name is
  Port is not admin blocked
  Prohibited port addresses are 0,241-253,255
```

例 10-12 使用可能なポート番号の表示

```
switch# show ficon first-available port-number
Port number 129(0x81) is available
```

例 10-13 では、ポート番号がインストールされている場合、対応するインターフェイスが [Interface] 列に示されています。ポート番号がアンインストールされている場合、この列には何も表示されず、アンバインドされているポート番号であることを示します。たとえば、例 10-13 ではアンバインドされているポート番号は 56 です。

例 10-13 要約形式でのポート番号情報の表示

```
switch# show ficon vsan 2 portaddress 50-55 brief
-----
```

Port Address	Port Number	Interface	Admin Blocked	Status	Oper Mode	FCID
50	50	fc2/18	on	fcotAbsent	--	--
51	51	fc2/19	off	fcotAbsent	--	--
52	52	fc2/20	off	fcotAbsent	--	--
53	53	fc2/21	off	fcotAbsent	--	--
54	54	fc2/22	off	notConnected	--	--
55	55	fc2/23	off	up	FL	0xea0000
56	56		off	up	FL	0xea0000

例 10-14 では、FICON のバージョン形式 1 (32 ビット形式) のカウンタを表示します。

例 10-14 ポート アドレス カウンタ情報の表示

```
switch# show ficon vsan 20 portaddress 8 counters
Port Address 8(0x8) is up in vsan 20
  Port number is 8(0x8), Interface is fc1/8
  Version presented 1, Counter size 32b
  242811 frames input, 9912794 words
    484 class-2 frames, 242302 class-3 frames
    0 link control frames, 0 multicast frames
    0 disparity errors inside frames
    0 disparity errors outside frames
    0 frames too big, 0 frames too small
    0 crc errors, 0 eof errors
    0 invalid ordered sets
    0 frames discarded c3
    0 address id errors
  116620 frames output, 10609188 words
    0 frame pacing time
  0 link failures
  0 loss of sync
  0 loss of signal
  0 primitive seq prot errors
  0 invalid transmission words
  1 lrr input, 0 ols input, 5 ols output
  0 error summary
```

FICON コンフィギュレーション ファイル情報の表示

例 10-15 ~ 10-17 では、FICON コンフィギュレーション ファイル情報を表示します。

例 10-15 指定した FICON コンフィギュレーション ファイルの内容の表示

```
switch# show ficon vsan 3 file IPL
FICON configuration file IPL      in vsan 3
  Port address 1
    Port name is
    Port is not blocked
    Prohibited port addresses are 0,81-253,255

  Port address 2
    Port name is
    Port is not blocked
    Prohibited port addresses are 0,81-253,255

  Port address 3
    Port name is
    Port is not blocked
    Prohibited port addresses are 0,81-253,255

  Port address 4
    Port name is
    Port is not blocked
    Prohibited port addresses are 0,81-253,255

  ...
  Port address 80
    Port name is
    Port is not blocked
    Prohibited port addresses are 0,81-253,255

  Port address 254
    Port name is
    Port is not blocked
    Prohibited port addresses are 0,81-253,255
```

例 10-16 すべての FICON コンフィギュレーション ファイルの表示

```
switch# show ficon vsan 2
Ficon information for VSAN 2
  Ficon is enabled
  VSAN is active
  Host control is Enabled
  Host offline control is Enabled
  Clock alert mode is Disabled
  User alert mode is Disabled
  SNMP control is Disabled
  Active=Saved is Disabled
  Number of implemented ports are 250
  Key Counter is 9
  FCID last byte is 0
  Date/Time is same as system time(Sun Dec 14 01:26:30.273402 1980)
  Device Allegiance not locked
  Codepage is us-canada
Saved configuration files
  IPL
  IPLFILE1
```

例 10-17 FICON コンフィギュレーション ファイルの指定したポート アドレスの表示

```
switch# show ficon vsan 2 file iplfile1 portaddress 1-7
FICON configuration file IPLFILE1 in vsan 2
  Port address 1
    Port name is
    Port is not blocked
    Prohibited port addresses are 0,241-253,255

  Port address 2
    Port name is
    Port is not blocked
    Prohibited port addresses are 0,241-253,255

  Port address 3
    Port name is P3
    Port is not blocked
    Prohibited port addresses are 0,241-253,255
  ...
  Port address 7
    Port name is
    Port is not blocked
    Prohibited port addresses are 0,241-253,255
```

設定された FICON の状態の表示

VSAN で FICON が有効な場合は、その VSAN のポート アドレス情報を表示できます(例 10-18 を参照)。

例 10-18 FICON が有効な場合の指定したポート アドレスの表示

```
switch# show ficon vsan 2 portaddress 55
Port Address 55 is not installed in vsan 2
  Port number is 55, Interface is fc2/23
  Port name is
  Port is not admin blocked
  Prohibited port addresses are 0,241-253,255
  Admin port mode is FL
  Port mode is FL, FCID is 0xea0000
```

ポート管理状態の表示

例 10-19 ~ 10-20 では、FICON ポートの管理状態を表示します。ポートがブロックされた場合、**show ficon vsan number portaddress number** コマンドはポートのブロック ステータスを表示します。特定のポートが禁止されている場合、このコマンドは、禁止されている具体的なポート (3) とデフォルトで禁止されているポート (0,241 ~ 253、および 255) も表示します。名前が割り当てられている場合は、その名前も表示されます。

例 10-19 管理上ブロック解除されたポートの表示

```
switch# show ficon vsan 2 portaddress 2
Port Address 2(0x2) is not installed in vsan 2
  Port number is 2(0x2), Interface is fc1/2
  Port name is
  Port is not admin blocked
```



```
Prohibited port addresses are 0,241-253,255(0,0xf1-0xfd,0xff)
Admin port mode is auto
Peer is Unknown
```

例 10-20 管理上ブロックされたポートの表示

```
switch# show ficon vsan 2 portaddress 1
Port Address 2(0x2) is not installed in vsan 2
Port number is 2(0x2), Interface is fc1/2
Port name is SampleName
Port is admin blocked
Prohibited port addresses are 0,241-253,255(0,0xf1-0xfd,0xff)
Admin port mode is auto
Peer is Unknown
```

バッファ情報の表示

例 10-21 では、[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。チャン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。

例 10-21 指定された VSAN の履歴バッファの表示

```
switch# show ficon vsan 20 director-history
Director History Buffer for vsan 20
```

Key Counter	Ports Address 変更
74556	43
74557	44
74558	45
74559	46
74560	47
74561	48
74562	49
74563	50
74564	51
74565	52
74566	53
74567	54
74568	55
74569	56
74570	57
74571	58
74572	59
74573	60
74574	61
74575	62
74576	63
74577	64

```

74578
74579
74580          1-3,5,10,12,14-16,34-40,43-45,47-54,56-57,59-64
74581          3,5
74582          64
74583
74584          1-3,10,12,14-16,34-40,43-45,47-54,56-57,59-64
74585          1
74586          2
74587          3

```

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。チャン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。

実行コンフィギュレーションの FICON 情報の表示

例 10-22 では、実行コンフィギュレーションの FICON 関連情報を表示します。

例 10-22 実行コンフィギュレーション情報の表示

```

switch# show running-config
Building Configuration ...
in-order-guarantee
vsan database
  vsan 11 name "FICON11" loadbalancing src-dst-id
  vsan 75 name "FICON75" loadbalancing src-dst-id

fcdomain domain 11 static vsan 11
fcdomain domain 119 static vsan 75

fcdroplacency network 100 vsan 11
fcdroplacency network 500 vsan 75

feature fabric-binding
fabric-binding database vsan 11
  swnn 20:00:00:0d:ec:01:20:c0 domain 10
fabric-binding database vsan 75
  swnn 20:00:00:0d:ec:00:d6:40 domain 117
fabric-binding activate vsan 11
fabric-binding activate vsan 75

ficon vsan 75

interface port-channel 1
  ficon portnumber 0x80
  switchport mode E

snmp-server user mblair network-admin auth md5 0x688fa3a2e51ba5538211606e59ac292

```

```

7 priv 0x688fa3a2e51ba5538211606e59ac2927 localizedkey
snmp-server user wwilson network-admin auth md5 0x688fa3a2e51ba5538211606e59ac29
27 priv 0x688fa3a2e51ba5538211606e59ac2927 localizedkey
snmp-server host 171.71.187.101 traps version 2c public udp-port 1163
snmp-server host 172.18.2.247 traps version 2c public udp-port 2162

vsan database
  vsan 75 interface fcl/1
...
interface mgmt0
  ip address 172.18.47.39 255.255.255.128
  switchport speed 100
  switchport duplex full

no system health

ficon vsan 75
  file IPL

```

スタートアップ コンフィギュレーションの FICON 情報の表示

例 10-23 では、スタートアップ コンフィギュレーションの FICON 関連情報を表示します。

例 10-23 スタートアップ コンフィギュレーションの表示

```

switch# show startup-config
...
ficon vsan 2
file IPL

```

例 10-24 では、暗黙的に発行された `copy running start` コマンドに対するスイッチの応答を表示します。この場合、明示的に `copy running start` コマンドを再度発行するまで、バイナリ コンフィギュレーションのみが保存されます(表 10-2 を参照)

例 10-24 スタートアップ コンフィギュレーション ステータスの表示

```

switch# show startup-config
No ASCII config available since configuration was last saved internally
on account of 'active=saved' mode.
Please perform an explicit 'copy running startup` to get ASCII configuration

```

FICON 関連のログ情報の表示

例 10-25 および例 10-26 では、FICON 関連の設定のロギング情報を表示します。

例 10-25 FICON 機能のログレベルの表示

```

switch# show logging level ficon

```

Facility	Default Severity	Current Session Severity
ficon	2	2
0(emergencies)	1(alerts)	2(critical)
3(errors)	4(warnings)	5(notifications)
6(information)	7(debugging)	

例 10-26 FICON 関連ログ ファイルの内容の表示

```
switch# show logging logfile
...
2004 Feb 25 15:38:50 vegas6 %PORT-5-IF_UP: %$VSAN 75: 2004 Wed Feb 25 13:22:04.
131183%$ Interface fc1/8 is up in mode F
2004 Feb 25 15:38:50 vegas6 %PORT-5-IF_UP: %$VSAN 75: 2004 Wed Feb 25 13:22:04.
131217%$ Interface fc1/9 is up in mode F
...
2004 Feb 25 15:39:09 vegas6 %PORT-5-IF_TRUNK_UP: %$VSAN 75: 2004 Wed Feb 25 13:
22:23.131121%$ Interface fc2/1, vsan 75 is up
2004 Feb 25 15:39:09 vegas6 %PORT-5-IF_TRUNK_UP: %$VSAN 75: 2004 Wed Feb 25 13:
22:23.131121%$ Interface fc2/2, vsan 75 is up
2004 Feb 25 15:39:09 vegas6 %PORT-5-IF_TRUNK_UP: %$VSAN 75: 2004 Wed Feb 25 13:
...
2004 Feb 25 23:22:36 vegas6 %PORT-5-IF_UP: %$VSAN 75: 2004 Wed Feb 25 21:05:42.
99916%$ Interface fc3/6 is up in mode F
2004 Feb 25 23:22:37 vegas6 %PORT-5-IF_UP: %$VSAN 75: 2004 Wed Feb 25 21:05:43.
...
```

デフォルト設定

表 10-3 に、FICON 機能のデフォルト設定を示します。

表 10-3 FICON のデフォルト設定

パラメータ (Parameters)	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



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。内容は次のとおりです。

- [共通情報モデル\(CIM\) \(11-1 ページ\)](#)
- [ファイバチャネル タイムアウト値 \(11-2 ページ\)](#)
- [組織固有識別子 \(11-6 ページ\)](#)
- [World Wide Name \(WWN\) \(11-7 ページ\)](#)
- [HBA の FC ID 割り当て \(11-9 ページ\)](#)
- [スイッチの相互運用性 \(11-11 ページ\)](#)
- [デフォルト設定 \(11-18 ページ\)](#)

共通情報モデル(CIM)

共通情報モデル(CIM)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/>



(注)

CIM 機能および SMI-S は現在 Cisco Prime Data Center Network Manager (DCNM) でサポートされています。『Cisco Prime DCNM Installation Guide』および『SMI-S and Web Services Programming Guide, Cisco DCNM for SAN』を参照してください。

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 ~ 4,000 ミリ秒です。デフォルトは 2,000 ミリ秒です。この値は、ポート初期化中に他端と比較されます。
- Resource Allocation TOV (R_A_TOV) : 有効範囲は 5,000 ~ 10,000 ミリ秒です。デフォルトは 10,000 ミリ秒です。この値は、ポート初期化中に他端と比較されます。



(注) Fabric Stability TOV (F_S_TOV) 定数は設定できません。

この項では、次のトピックについて取り上げます。

- [すべての VSAN のタイマー設定\(11-2 ページ\)](#)
- [VSAN ごとのタイマー設定\(11-3 ページ\)](#)
- [fctimer 配信の概要\(11-3 ページ\)](#)
- [fctimer 配信の有効化\(11-4 ページ\)](#)
- [fctimer 設定変更のコミット\(11-4 ページ\)](#)
- [fctimer 設定変更の廃棄\(11-4 ページ\)](#)
- [ファブリックのロックの上書き\(11-4 ページ\)](#)
- [データベース結合に関する注意事項\(11-5 ページ\)](#)
- [設定された fctimer 値の表示\(11-5 ページ\)](#)

すべての VSAN のタイマー設定

ファイバチャネルプロトコルに関連するスイッチのタイマー値を変更できます。



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。

すべての VSAN にファイバチャネル タイマーを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# config t switch(config)	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# fctimer R_A_TOV 6000	すべての VSAN の R_A_TOV 値を 6000 ミリ秒に設定します。このタイプの設定は、すべての VSAN が一時停止されていないかぎり、許可されません。

VSAN ごとのタイマー設定

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。VSAN ごとに異なる `E_D_TOV`、`R_A_TOV`、および `D_S_TOV` 値を設定できます。アクティブ VSAN のタイマー値を変更すると、VSAN は一時停止されてからアクティブになります。



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。

VSAN ごとのファイバチャネル タイマーを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>switch# config t</code> <code>switch(config)</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>switch(config)# fctimer D_S_TOV 6000 vsan 2</code> Warning: The vsan will be temporarily suspended when updating the timer value This configuration would impact whole fabric.Do you want to continue? (y/n) y Since this configuration is not propagated to other switches, please configure the same value in all the switches	VSAN 2 の <code>D_S_TOV</code> 値を 6000 ミリ秒に設定します。VSAN が一時的に停止します。必要に応じて、このコマンドを終了することもできます。

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` の設定を実行して、配布をイネーブルにすると、ファブリック内のすべてのスイッチにその設定が配布されます。

スイッチでの配信をイネーブルにした後で最初のコンフィギュレーション 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、有効データベースと保留データベース モデルを使用し、使用中のコンフィギュレーションに基づいてコマンドを格納またはコミットします。

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 配信の有効化

fctimer ファブリック配信を有効または無効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# fctimer distribute	ファブリック内のすべてのスイッチに対する fctimer 設定の配布をイネーブルにします。ファブリックのロックを取得して、その後の設定変更をすべて保留データベースに格納します。
	switch(config)# no fctimer distribute	ファブリック内のすべてのスイッチに対する fctimer 設定の配布をディセーブル(デフォルト)にします。

fctimer 設定変更のコミット

fctimer の設定変更をコミットすると、有効データベースは保留データベースの設定変更によって上書きされ、ファブリック内のすべてのスイッチが同じ設定を受け取ります。セッション機能を実行せずに fctimer の設定変更をコミットすると、fctimer 設定は物理ファブリック内のすべてのスイッチに配布されます。

fctimer の設定変更をコミットする手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# fctimer commit	ファブリック内のすべてのスイッチに対して fctimer の設定変更を配布し、ロックを解除します。保留データベースに対する変更を有効データベースに上書きします。

fctimer 設定変更の廃棄

設定変更を加えたあと、変更内容をコミットする代わりに廃棄すると、この変更内容を廃棄できます。いずれの場合でも、ロックは解除されます。

fctimer の設定変更を廃棄するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# fctimer abort	保留データベースの fctimer の設定変更を廃棄して、ファブリックのロックを解除します。

ファブリックのロックの上書き

ユーザが fctimer を設定して、変更のコミットや廃棄を行ってロックを解除するのを忘れていた場合、管理者はファブリック内の任意のスイッチからロックを解除できます。管理者がこの操作を行うと、ユーザによる保留データベースの変更は廃棄され、ファブリックのロックは解除されます。



ヒント

変更は `volatile` ディレクトリだけで使用でき、スイッチを再起動すると廃棄されます。

管理者特権を使用して、ロックされた `fctimer` セッションを解除するには、`clear fctimer session` コマンドを使用します。

```
switch# clear fctimer session
```

データベース結合に関する注意事項

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。

- 次の結合条件を確認します。
 - 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` 設定は、変更された `fctimer` 値を持つ VSAN が含まれるスイッチだけに適用される。
 - グローバルな `fctimer` 値は配布されない。
- 配布がイネーブルになっている場合は、グローバル タイマーの値を設定しないでください。



(注)

保留できる `fctimer` 設定操作の回数は 15 回以内です。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。

設定された `fctimer` 値の表示

設定された `fctimer` 値を表示するには、`show fctimer` コマンドを使用します(例 11-1 ~ 11-2 を参照)。

例 11-1 設定されたグローバル TOV の表示

```
switch# show fctimer
F_S_TOV  D_S_TOV  E_D_TOV  R_A_TOV
-----
5000 ms  5000 ms  2000 ms  10000 ms
```



(注)

`show fctimer` コマンドの出力には、(設定されていない場合でも) `F_S_TOV` 定数が表示されます。

例 11-2 指定した VSAN の設定済み TOV の表示

```
switch# show fctimer vsan 10
vsan no.  F_S_TOV  D_S_TOV  E_D_TOV  R_A_TOV
-----
10        5000 ms  5000 ms  3000 ms  10000 ms
```

組織固有識別子

組織固有識別子 (OUI) は、組織をグローバルに識別する一意の 24 ビット数値です。OUI が割り当てられている組織は、その OUI を拡張して 48 ビットまたは 60 ビットの拡張固有識別子 (EUI) を作成します。シスコは IEEE から取得した OUI を使用して EUI を作成しています。これらの識別子が各システムに割り当てられ、保存されています。システムには 1 つ以上の EUI が割り当てられていることがあります。EUI は、MAC アドレス、WWN、SNMP ID などさまざまな形式で使用されます。

Cisco MDS NX-OS ソフトウェアには、使用可能になっている特定のソフトウェア機能に基づく OUI データベースが含まれています。ファブリックに追加される新しいシスコ デバイスの OUI を認識できない場合、一部の機能が影響を受けることがあります。この問題を回避するため、CLI を使用して OUI データベースに OUI を手動で追加できます。

注意事項と制約事項

- **ISSU:** アップグレード後に、デフォルト (組み込み) リストとスタティック (ユーザ定義) リストで OUI が重複することがあります。このような場合には、スタティック OUI とデフォルトリストの OUI を比較し、重複するスタティック OUI を削除することをお勧めします。
- **ISSD:** `wwn oui oui-id` コマンドをサポートしていないリリースにダウングレードする前に、設定されている OUI またはスタティック OUI をすべて削除します。

OUI の削除の詳細については、[OUI の追加および削除 \(11-6 ページ\)](#) を参照してください。

OUI の追加および削除

OUI を OUI データベースに追加するには、グローバル コンフィギュレーション モードで `wwn oui oui-id` コマンドを入力します。OUI データベースから OUI を削除するには、グローバル コンフィギュレーション モードで `no wwn oui oui-id` コマンドを入力します。

`wwn oui` コマンドの詳細については、『*Cisco MDS 9000 Family Command Reference*』を参照してください。

OUI の追加と削除の設定例

例: OUI の追加と削除

```
switch# configure terminal
switch(config)# wwn oui 0x10001c
switch(config)# no wwn oui 0x10001c
switch(config)# end
```

例: OUI の表示

```
switch# show wwn oui
OUI          Vendor          Default/Static
-----
0x0000fc     Cisco           Static
0x00000c     Cisco           Default
0x000196     Cisco           Default
0x000197     Cisco           Default
```

```
0x0001c7 Cisco Default
0x0001c9 Cisco Default
```

World Wide Name (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 11-1 を参照)。

表 11-1 標準化された NAA WWN フォーマット

NAA アドレス	NAA タイプ	WWN フォーマット	
IEEE 48 ビット アドレス	タイプ 1 = 0001b	000 0000 0000b	48 ビット MAC アドレス
IEEE 拡張	タイプ 2 = 0010b	ローカルに割り当て	48 ビット MAC アドレス
IEEE 登録	タイプ 5 = 0101b	IEEE 企業 ID: 24 ビット	VSID: 36 ビット



注意

WWN の変更は、管理者または、スイッチの操作に精通した担当者が実行してください。

この項では、次のトピックについて取り上げます。

- [WWN 情報の表示 \(11-7 ページ\)](#)
- [リンク初期化時の WWN の使用方法 \(11-8 ページ\)](#)
- [セカンダリ MAC アドレスの設定 \(11-8 ページ\)](#)

WWN 情報の表示

WWN 設定のステータスを表示するには、`show wwn` コマンドを使用します。例 11-3 ~ 11-5 を参照してください。

例 11-3 すべての WWN のステータスの表示

```
switch# show wwn status
      Type 1 WWNs: Configured:      64 Available:      48 (75%) Resvd.: 16
      Types 2 & 5 WWNs: Configured: 524288 Available: 450560 (85%) Resvd.: 73728
      NKAU & NKCR WWN Blks: Configured: 1760 Available: 1760 (100%)
      Alarm Status:      Type1:      NONE Types 2&5:      NONE
```

例 11-4 指定したブロック ID 情報の表示

```
switch# show wwn status block-id 51
WWNs in this block: 21:00:ac:16:5e:52:00:03 to 21:ff:ac:16:5e:52:00:03
Num. of WWNs:: Configured: 256 Allocated:    0 Available: 256
Block Allocation Status: FREE
```

例 11-5 特定スイッチの WWN の表示

```
switch# show wwn switch
Switch WWN is 20:00:ac:16:5e:52:00:00
```

リンク初期化時の WWN の使用方法

Exchange Link Protocol (ELP) および Exchange Fabric Protocol (EFP) は、リンク初期化の際に WWN を使用します。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 の使用法はピア スイッチの使用法に応じて変わります。

- ピア スイッチの ELP がスイッチの WWN を使用する場合、ローカル スイッチもスイッチの WWN を使用します。
- ピア スイッチの ELP が VSAN の WWN を使用する場合、ローカル スイッチも VSAN の WWN を使用します。



(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

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。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# wwn secondary-mac 00:99:55:77:55:55 range 64 This command CANNOT be undone. Please enter the BASE MAC ADDRESS again: 00:99:55:77:55:55 Please enter the mac address RANGE again: 64 From now on WWN allocation would be based on new MACs. Are you sure? (yes/no) no You entered: no. Secondary MAC NOT programmed	セカンダリ MAC アドレスを設定します。このコマンドは元に戻せません。

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 ファミリースイッチには特殊な割り当て方式が使用されています。

一部の Host Bus Adapter (HBA) は、ドメインとエリアが同じ FC ID を持つターゲットを検出しません。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 FCID が割り当てられ、残りにはエリア全体が割り当てられます。

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](#)」セクション(11-9 ページ)を参照)。

多数のポートを備えたスイッチのスケ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の間、pWWN で使用される企業 ID (組織固有識別子 (OUI) としても知られる) によって識別されます。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。

この項では、次のトピックについて取り上げます。

- [デフォルトの企業 ID リスト \(11-9 ページ\)](#)
- [企業 ID の設定の確認 \(11-10 ページ\)](#)

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 ファミリー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。この企業 ID を使用すると、設定する永続的 FC ID エントリの数が少なくなります。これらのエントリは、CLI を使用して設定または変更できます。



注意

永続的エントリは、企業 ID の設定よりも優先されます。HBA がターゲットを検出しない場合は、HBA とターゲットが同じスイッチに接続され、FC ID のエリアが同じであることを確認してから、次の手順を実行します。

1. HBA に接続されているポートをシャットダウンします。
2. 永続的 FC ID エントリをクリアします。
3. ポート WWN から企業 ID を取得します。
4. エリア割り当てを必要とするリストに企業 ID を追加します。
5. ポートをアップにします。

企業 ID のリストには、次の特性があります。

- 永続的 FC ID の設定は常に企業 ID リストよりも優先されます。エリアを受け取るように企業 ID が設定されている場合でも、永続的 FC ID の設定によって単一の FC ID が割り当てられます。
- 後続のリリースに追加される新規の企業 ID は、既存の企業 ID に自動的に追加されます。

- 企業 ID のリストは、実行コンフィギュレーションおよび保存されたコンフィギュレーションの一部として保存されます。
- 企業 ID のリストが使用されるのは、`fcinterop` の FC ID 割り当て方式が `auto` モードの場合だけです。変更されないかぎり、`interop` の FC ID 割り当ては、デフォルトで `auto` に設定されています。



ヒント `fcinterop` の FC ID 割り当て方式を `auto` に設定し、企業 ID リストと永続的 FC ID 設定を使用して、FC ID のデバイス割り当てを行うことをお勧めします。

FC ID の割り当てを変更するには、`fcinterop FCID allocation auto` コマンドを使用し、現在割り当てられているモードを表示するには、`show running-config` コマンドを使用します。

- `write erase` を実行すると、リストは該当するリリースに付属している企業 ID のデフォルトリストを継承します。

企業 ID を割り当てる手順は、次のとおりです。

	コマンド	目的
ステップ 1	<code>switch# config t</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>switch(config)# fcid-allocation area</code> <code>company-id 0x003223</code>	デフォルト リストに新しい企業 ID を追加します。
	<code>switch(config)# no fcid-allocation area</code> <code>company-id 0x00E069</code>	デフォルト リストから企業 ID を削除します。
	<code>switch(config)# fcid-allocation area</code> <code>company-id 0x003223</code>	デフォルト リストに新しい企業 ID を追加します。

企業 ID の設定の確認

設定された企業 ID を表示するには、`show fcid-allocation area` コマンドを発行します(例 11-6 を参照)。最初にデフォルト エントリが表示され、次にユーザによって追加されたエントリが表示されます。エントリがデフォルト リストの一部で、あとで削除された場合でも、エントリは表示されます。

例 11-6 デフォルトの企業 ID と設定された企業 ID のリストの表示

```
switch# show fcid-allocation area
FCID area allocation company id info:
  00:50:2E <----- デフォルトのエントリ
  00:50:8B
  00:60:B0
  00:A0:B8
  00:E0:69
  00:30:AE + <----- ユーザが追加したエントリ
  00:32:23 +

  00:E0:8B * <----- (元のデフォルト リストから)明示的に削除されたエントリ
Total company ids: 7
+ - Additional user configured company ids.
* - Explicitly deleted company ids from default list.
```

削除済みエントリの印が付いていない企業 ID のリストを組み合わせると、特定のリリースに付属するデフォルト エントリを暗黙的に導き出すことができます。

また、`show fcid-allocation company-id-from-wwn` コマンドを発行すると、特定の WWN の企業 ID を表示または取得することもできます(例 11-7 を参照)。一部の WWN 形式では、企業 ID がサポートされていません。この場合、FC ID の永続的エントリを設定する必要があります。

例 11-7 指定した WWN の企業 ID の表示

```
switch# show fcid-allocation company-id-from-wwn 20:00:00:05:30:00:21:60
Extracted Company ID: 0x000530
```

スイッチの相互運用性

相互運用性を使用すると、複数ベンダーによる製品の間で相互接続できます。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。



(注) Cisco MDS 9000 ファミリ スイッチでの相互運用性の設定方法に関する詳細は、『*Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*』を参照してください。

この項では、次のトピックについて取り上げます。

- [Interop モードの概要\(11-11 ページ\)](#)
- [interop モード 1 の設定\(11-13 ページ\)](#)

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 11-2 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 11-2 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	相互運用モードがイネーブルの場合の変更点
ドメイン ID	一部のベンダーは、ファブリック内の 239 のドメインを完全には使用できません。 ドメイン ID は 97 ~ 127 の範囲に制限されています。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) を確立するときファイバチャネル タイマー値が E ポートで交換されるので、すべてのスイッチでこれらのタイマーをすべて同じにする必要があります。タイマーには、F_S_TOV、D_S_TOV、E_D_TOV、および R_A_TOV があります。
F_S_TOV	Fabric Stability TOV タイマーが正確に一致するかどうかを確認してください。
D_S_TOV	Distributed Services TOV タイマーが正確に一致するかどうかを確認してください。
E_D_TOV	Error Detect TOV タイマーが正確に一致するかどうかを確認してください。
R_A_TOV	Resource Allocation TOV タイマーが正確に一致するかどうかを確認してください。
トランッキング	2 つの異なるベンダー製のスイッチ間では、トランッ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) を除去することができます。 (注) Brocade では、 <code>cfgsave</code> 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 ファミリー スイッチには影響しません。Cisco MDS 9000 ファミリーの各スイッチに、設定を明示的に保存する必要があります。
ゾーンの伝播	一部のベンダーは、他のスイッチに完全なゾーン設定を受け渡さないで、アクティブ ゾーン セットだけを受け渡します。 ファブリック内の他のスイッチにアクティブ ゾーンセットまたはゾーン設定が正しく伝播されたかどうかを確認してください。
VSAN	interop モードは、指定された VSAN にだけ有効です。 (注) interop モードは、FICON 対応の VSAN でイネーブルにできません。

表 11-2 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	相互運用モードがイネーブルの場合の変更点
TE ポートと PortChannel	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 リンク間でロード バランスします。
ドメインの中断再設定	これは、スイッチ全体に影響するイベントです。Brocade および McData では、ドメイン ID を変更するときにスイッチ全体をオフライン モードにしたり、再起動したりする必要があります。
ドメインの非中断再設定	これは、関連する VSAN に限定されるイベントです。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かを確認してください。
IVRivr	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 ファミリー 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 ファミリー スイッチまたは McData スイッチに接続する前に、Brocade の `msplmgmtdeactivate` コマンドを明示的に実行する必要があります。このコマンドでは、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。

Cisco MDS 9000 ファミリーの任意のスイッチに interop モード 1 を設定するには、次の手順を実行します。

ステップ 1 他ベンダー製スイッチに接続する E ポートの VSAN を相互運用モードにします。

```
switch# config t
switch(config)# vsan database
switch(config-vsan-db)# vsan 1 interop 1
switch(config-vsan-db)# exit
switch(config)#
```



(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 2 97(0x61)～127(0x7F)の範囲でドメイン ID を割り当てます。



(注) これは、McData スイッチに適用される制限です。

```
switch(config)# fcdomain domain 100 preferred vsan 1
```

Cisco MDS 9000 スイッチの場合、デフォルトでは、主要スイッチから ID が要求されます。Preferred オプションを使用した場合、Cisco MDS 9000 スイッチは固有の ID を要求しますが、主要スイッチから別の ID が割り当てられた場合もファブリックに加入します。Static オプションを使用した場合、要求された ID を主要スイッチが承認して、これを割り当てない限り、Cisco MDS 9000 スイッチはファブリックに参加しません。



(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 3 FC タイマーを変更します(システム デフォルトから変更された場合)。



(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。

```
switch(config)# fctimer e_d_tov ?
<1000-4000> E_D_TOV in milliseconds(1000-4000)
switch(config)# fctimer r_a_tov ?
<5000-100000> R_A_TOV in milliseconds(5000-100000)
```

ステップ 4 ドメインを変更するときに、変更された VSAN の Cisco MDS ドメイン マネージャ機能の再起動が必要な場合と、不要な場合があります。

- **disruptive** オプションを使用して、ファブリックを強制的に再設定する場合は次のようになります。

```
switch(config)# fcdomain restart disruptive vsan 1
```

または

- ファブリックを強制的に再設定しない場合は次のようになります。

```
switch(config)# fcdomain restart vsan 1
```

コマンドについて説明します。

Cisco MDS 9000 ファミリのスイッチで相互運用性コマンドを発行した結果の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 **show version** コマンドを使用してバージョンを検証します。

```
switch# show version
Cisco Storage Area Networking Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2003, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
Cisco Systems, Inc. and/or other third parties and are used and
```

```
distributed under license. Some parts of this software are covered
under the GNU Public License. A copy of the license is available
http://www.gnu.org/licenses/gpl.html.
```

```
Software
  BIOS:      version 1.0.8
  loader:    version 1.1(2)
  kickstart: version 2.0(1) [build 2.0(0.6)] [gdb]
  system:    version 2.0(1) [build 2.0(0.6)] [gdb]

  BIOS compile time:      2003/08/07
  kickstart image file is: bootflash:///m9500-sflek9-kickstart-mzg.2.0.0.6.bin
  kickstart compile time: 10/25/2010 12:00:00
  system image file is:   bootflash:///m9500-sflek9-mzg.2.0.0.6.bin
  system compile time:    10/25/2020 12:00:00
```

```
Hardware
  RAM 1024584 kB

  bootflash: 1000944 blocks (block size 512b)
  slot0:      0 blocks (block size 512b)

  172.22.92.181 uptime is 0 days 2 hours 18 minute(s) 1 second(s)

  Last reset at 970069 usecs after Tue Sep 16 22:31:25 1980
  Reason: Reset Requested by CLI command reload
  System version: 2.0(0.6)
  [Service]:
```

ステップ 2 **show interface brief** コマンドを使用して、インターフェイスの状態が設定に必要な状態になっているかどうかを確認します。

```
switch# show int brief
Interface Vsan Admin Admin Status Oper Oper Port-channel
          Mode Trunk Mode Speed
          Mode (Gbps)
-----
fc2/1    1    auto on    up    E    2    --
fc2/2    1    auto on    up    E    2    --
fc2/3    1    auto on    fcotAbsent -- -- --
fc2/4    1    auto on    down -- -- --
fc2/5    1    auto on    down -- -- --
fc2/6    1    auto on    down -- -- --
fc2/7    1    auto on    up    E    1    --
fc2/8    1    auto on    fcotAbsent -- -- --
fc2/9    1    auto on    down -- -- --
fc2/10   1    auto on    down -- -- --
```

ステップ 3 必要な設定を実行しているかどうかを確認するには、**show run** コマンドを使用します。

```
switch# show run
Building Configuration...

  interface fc2/1
no shutdown

  interface fc2/2
no shutdown

  interface fc2/3
interface fc2/4
interface fc2/5
interface fc2/6
```

```

interface fc2/7
no shutdown

interface fc2/8
interface fc2/9
interface fc2/10

<省略>

interface fc2/32

interface mgmt0
ip address 6.1.1.96 255.255.255.0
switchport encap default
no shutdown

vsan database
vsan 1 interop

boot system bootflash:/m9500-system-253e.bin sup-1
boot kickstart bootflash:/m9500-kickstart-253e.bin sup-1
boot system bootflash:/m9500-system-253e.bin sup-2
boot kickstart bootflash:/m9500-kickstart-253e.bin sup-2
callhome

fcdomain domain 100 preferred vsan 1

ip route 6.1.1.0 255.255.255.0 6.1.1.1
ip routing
line console
  databits 5
  speed 110
logging linecard
ssh key rsa 512 force
ssh server enable
switchname MDS9509
username admin password 5 $1$Li8/fBYX$SNc72.xt4nTXpSnR9OUFB/ role network-admin

```

- ステップ 4** 相互運用性モードがアクティブであるかどうかを確認するには、**show vsan** コマンドを使用します。

```

switch# show vsan 1
vsan 1 information
  name:VSAN0001 stalactites
  interoperability mode:yes <----- モードの確認
  loadbalancing:src-id/dst-id/oxid
  operational state:up

```

- ステップ 5** ドメイン ID を確認するには **show fcdomain vsan** コマンドを使用します。

```

switch# show fcdomain vsan 1
The local switch is a Subordinated Switch.

Local switch run time information:
  State: Stable
  Local switch WWN: 20:01:00:05:30:00:51:1f
  Running fabric name: 10:00:00:60:69:22:32:91
  Running priority: 128
  Current domain ID: 0x64(100) <-----ドメイン ID の確認

Local switch configuration information:
  State: Enabled
  Auto-reconfiguration: Disabled
  Contiguous-allocation: Disabled

```

```
Configured fabric name: 41:6e:64:69:61:6d:6f:21
Configured priority: 128
Configured domain ID: 0x64(100) (preferred)
```

```
Principal switch run time information:
Running priority: 2
```

Interface	Role	RCF-reject
fc2/1	Downstream	Disabled
fc2/2	Downstream	Disabled
fc2/7	Upstream	Disabled

ステップ 6 ローカルプリンシパルスイッチステータスを確認するには、**show fcdomain domain-list vsan** コマンドを使用します。

```
switch# show fcdomain domain-list vsan 1
```

```
Number of domains: 5
Domain ID          WWN
-----
0x61(97)          10:00:00:60:69:50:0c:fe
0x62(98)          20:01:00:05:30:00:47:9f
0x63(99)          10:00:00:60:69:c0:0c:1d
0x64(100)         20:01:00:05:30:00:51:1f [Local]
0x65(101)         10:00:00:60:69:22:32:91 [Principal]
-----
```

ステップ 7 スwitchのネクストホップと宛先を確認するには、**show fspf internal route vsan** コマンドを使用します。

```
switch# show fspf internal route vsan 1
```

```
FSPF Unicast Routes
-----
VSAN Number  Dest Domain  Route Cost  Next hops
-----
1            0x61(97)     500         fc2/2
1            0x62(98)     1000        fc2/1
              fc2/2
1            0x63(99)     500         fc2/1
1            0x65(101)    1000        fc2/7
```

ステップ 8 ネームサーバ情報を確認するには、**show fcns data vsan** コマンドを使用します。

```
switch# show fcns data vsan 1
```

```
VSAN 1:
```

FCID	TYPE	PWWN	(VENDOR)	FC4-TYPE:FEATURE
0x610400	N	10:00:00:00:c9:24:3d:90	(Emulex)	scsi-fcp
0x6105dc	NL	21:00:00:20:37:28:31:6d	(Seagate)	scsi-fcp
0x6105e0	NL	21:00:00:20:37:28:24:7b	(Seagate)	scsi-fcp
0x6105e1	NL	21:00:00:20:37:28:22:ea	(Seagate)	scsi-fcp
0x6105e2	NL	21:00:00:20:37:28:2e:65	(Seagate)	scsi-fcp
0x6105e4	NL	21:00:00:20:37:28:26:0d	(Seagate)	scsi-fcp
0x630400	N	10:00:00:00:c9:24:3f:75	(Emulex)	scsi-fcp
0x630500	N	50:06:01:60:88:02:90:cb		scsi-fcp
0x6514e2	NL	21:00:00:20:37:a7:ca:b7	(Seagate)	scsi-fcp
0x6514e4	NL	21:00:00:20:37:a7:c7:e0	(Seagate)	scsi-fcp
0x6514e8	NL	21:00:00:20:37:a7:c7:df	(Seagate)	scsi-fcp
0x651500	N	10:00:00:e0:69:f0:43:9f	(JNI)	

```
Total number of entries = 12
```

デフォルト設定

表 11-3 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 11-3 拡張機能のデフォルト設定値

パラメータ (Parameters)	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 を呼び出すタイムアウト時間	5 秒
fcping 機能によって送信されるフレーム数	5 フレーム
リモート キャプチャ接続プロトコル	TCP
リモート キャプチャ接続モード	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



Fibre Channel Common Transport 管理セキュリティの設定

この章では、Cisco MDS 9000 シリーズ スイッチの Fibre Channel Common Transport (FC-CT) 管理セキュリティ機能について説明します。

Fibre Channel Common Transport の概要

FC-CT 管理セキュリティ機能により、ストレージ管理者またはネットワーク管理者だけが、スイッチに対してクエリーを送信し、情報にアクセスできるようにネットワークを設定できます。このような情報には、ファブリック内のログイン デバイス、ファブリック内のスイッチなどのデバイス、デバイスの接続方法、各スイッチのポートの数、各ポートの接続先、設定済みゾーンの情報、ゾーンまたはゾーン セットの追加と削除の権限、ファブリックに接続するすべてのホストのホスト バス アダプタ (HBA) の詳細などがあります。



(注) Cisco MDS NX-OS Release 6.2(9) では、FC 管理機能はデフォルトで無効です。FC 管理機能を有効にするには、**fc-management enable** コマンドを使用します。

FC-CT 管理クエリーを送信し、管理サーバへの要求を変更できる pWWN を設定できます。いずれかのモジュール (ゾーン サーバ、ゾーン分割されていないファイバ チャネル ネーム サーバ (FCNS)、またはファブリック コンフィギュレーション サーバ (FCS) など) が FC-CT 管理クエリーを受信すると、FC 管理データベースに対する読み取り操作が実行されます。FC 管理データベースでデバイスが検出されると、付与されている権限に基づいて応答が送信されます。デバイスが FC 管理データベースにない場合は、各モジュールが拒否を送信します。FC 管理が無効な場合、各モジュールが各管理クエリーを処理します。

設定時の注意事項

FC 管理セキュリティ機能には、次の設定に関する注意事項があります。

- Cisco MDS スイッチで FC 管理セキュリティ機能が有効な場合、管理クエリーを送信するデバイスのポート ワールドワイド ネーム (pWWN) が FC 管理データベースに追加されていないと、サーバへのすべての管理クエリーが拒否されます。

- FC 管理を有効にすると、N_Port Virtualization (NPV) スイッチから N_Port Identifier Virtualization (NPIV) スイッチへの FC-CT 管理サーバ クエリーが拒否されます。FC 管理セキュリティ機能を有効にした後で、NPV スイッチのスイッチ ワールドワイド ネーム (sWWN) を NPIV スイッチの FC 管理データベースに追加することが推奨されます。

Fibre Channel Common Transport クエリーの設定

FC-CT 管理セキュリティを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config terminal	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# fc-management enable switch(config)#	FC-CT 管理セキュリティを有効にします。
ステップ 3	switch(config)# fc-management database vsan 1	FC-CT 管理セキュリティ データベースを設定します。
ステップ 4	switch(config-fc-mgmt)# pwwn 1:1:1:1:1:1:1:1 feature all operation both	pWWN を FC 管理データベースに追加します。また、 pwwn コマンドを設定するときには次に示すオプションのキーワードも使用できます。 <ul style="list-style-type: none"> fcs: ファブリック コンフィギュレーション サーバに対する FC-CT クエリーを有効または無効にします。 fdmi: FDMI に対する FC-CT クエリーを有効または無効にします。 unzoned-ns: ゾーン分割されていないネーム サーバに対する FC-CT クエリーを有効または無効にします。 zone: ゾーン サーバに対する FC-CT クエリーを有効または無効にします。
ステップ 5	switch# show fc-managment database	設定された FC-CT 管理情報を表示します。

Fibre Channel Common Transport 管理セキュリティの確認

show fc-management database コマンドは、設定されている FC-CT 管理セキュリティ機能の情報を表示します。(例 12-1 を参照)。

例 12-1 Fibre Channel Common Transport クエリーの表示

```
switch# show fc-management database
-----
VSAN PWWN FC-CT Permissions per FC services
-----
1 01:01:01:01:01:01:01:01 Zone (RW), Unzoned-NS (RW), FCS (RW), FDMI (RW)
1 02:02:02:02:02:02:02:02 Zone (R), Unzoned-NS (R), FCS (R), FDMI (R)
1 03:03:03:03:03:03:03:03 Zone (W), Unzoned-NS (W), FCS (W), FDMI (W)
-----
Total 3 entries
switch#
```


FC 管理セキュリティ機能が有効であるかどうかを確認するには、**show fc-management status** コマンドを使用します。

```
switch# show fc-management status
Mgmt Security Disabled
switch#
```

デフォルト設定値

表 12-1 に、Cisco MDS 9000 ファミリ スイッチの FC 管理セキュリティ機能のデフォルト設定を示します。

表 12-1 デフォルトの FC 管理設定

パラメータ (Parameters)	デフォルト
FC-management	ディセーブル

■ デフォルト設定値