Cisco Nexus 5000 シリーズ スイッチ Fabric Manager ソフトウェア コンフィギュレーション ガイド

Software Release 4.0

June 2008

Text Part Number: OL-16598-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。米国サイト掲載ドキュメントとの差異が生じる場合があるため、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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。シスコシステムズ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、シスコシステムズ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システムズ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。

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0809R)

このマニュアルで使用している IP アドレスは、実際のアドレス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、および図は、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 Nexus 5000 シリーズ スイッチ Fabric Manager ソフトウェア コンフィギュレーション ガイド
Copyright © 2008 Cisco Systems, Inc.
All rights reserved

Copyright © 2009, シスコシステムズ合同会社 .
All rights reserved.

CONTENTS

はじめに xix

対象読者 xix

マニュアルの構成 xx

表記法 xxii

関連資料 xxiii

マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン xxiv

シスコのテクニカル サポート xxiv

Service Request ツールの使用 xxiv

その他の情報の入手方法 xxv

CHAPTER 1

製品概要 1-1

Nexus 5000 シリーズの新しいテクノロジー 1-2

FCoE 1-2

IOC 1-2

仮想インターフェイス 1-3

Nexus 5000 シリーズ スイッチ ハードウェア 1-4

シャーシ 1-4

拡張モジュール 1-4

イーサネット インターフェイス 1-4

ファイバ チャネル インターフェイス 1-4

管理インターフェイス 1-4

Nexus 5000 シリーズ スイッチ ソフトウェア 1-5

イーサネット スイッチング 1-5

FCoE およびファイバ チャネル スイッチング 1-5

ライセンス 1-5

QoS 1-6

サービサビリティ 1-6

SPAN 1-6

Ethanalyzer 1-6

Call Home 1-6

オンライン診断 1-7

EEM 1-7

スイッチ管理 1-7
SNMP 1-7
構成の検証とロールバック 1-7
RBAC 1-7
コンフィギュレーション方式 1-7
ネットワーク セキュリティ機能 1-8
VDC 1-8
典型的な展開トポロジ 1-9
イーサネット TOR スイッチ トポロジ 1-9
IOC トポロジ 1-10
サポートされる規格 1-11

CHAPTER 2
Cisco Fabric Manager のインストール 2-1
Cisco Fabric Manager の概要 2-2
Fabric Manager Server 2-2
Fabric Manager Client 2-2
Fabric Manager Server プロキシ サービス 2-3
Device Manager 2-4
Performance Manager 2-4
Fabric Manager Web Server 2-4
スイッチ管理の概要 2-5
mgmt0 2-6
IPFC 2-6
管理ソフトウェアのインストール 2-7
インストールを開始する前に 2-7
サポート対象のソフトウェア 2-7
最小限のハードウェア要件 2-8
データベースのインストール 2-8
Oracle のインストール 2-9
Fabric Manager のインストール 2-10
Device Manager のインストール 2-18
管理ソフトウェアのアップグレード 2-21
Cisco Fabric Manager とその他の管理ツールとの統合 2-21
ファイアウォールの背後での Fabric Manager の稼働 2-22
管理ソフトウェアのアンインストール 2-23

CHAPTER 3
Fabric Manager Server 3-1
Fabric Manager Server の概要 3-2
Fabric Manager Server のインストールおよび設定 3-3

Fabric Manager Server のインストール 3-3
Fabric Manager Server のライセンスの有無 3-4
Fabric Manager Web Sever のインストール 3-4
Performance Manager の収集機能の確認 3-4
Fabric Manager Server ファブリックの管理 3-5
継続的管理対象のファブリックの選択 3-5
Fabric Manager Server プロパティ ファイル 3-6
Fabric Manager Server の変更 3-7
Fabric Manager Server ユーザの追加または削除 3-7
Fabric Manager Server のユーザ名およびパスワードの変更 3-8
ポーリング時間とファブリック再検出時間の変更 3-8
デバイス エイリアスまたは FC エイリアスの使用 3-9
スイッチへのデバイス エイリアスの保存 3-9

CHAPTER 4
Fabric Manager の認証 4-1
Fabric Manager 認証の概要 4-2
ファブリックの検出 4-4
ファブリック検出の設定 4-4
Performance Manager の認証 4-5
Fabric Manager Web Server の認証 4-7

CHAPTER 5
Fabric Manager Client 5-1
Fabric Manager Client の概要 5-2
Fabric Manager の拡張モード 5-2
Fabric Manager Client の起動 5-3
Fabric Manager Client の概観 5-8
メニューバー 5-9
ツールバー 5-10
Logical Domains ペイン 5-12
フィルタリング 5-12
Physical Attributes ペイン 5-12
Information ペイン 5-13
分離可能なテーブル 5-14
Fabric ペイン 5-14
コンテキスト メニュー 5-16
マップの保存 5-17
要素の消去 5-17
複数のファブリックの表示 5-18
グループによるフィルタリング 5-19

ステータス バー 5-20
Fabric Manager のプリファレンスの設定 5-21
ネットワーク ファブリック検出 5-22
デバイス グループの変更 5-23
ラックへのエイリアス名の使用 5-24
ユーザおよびロールによる管理者アクセスの制御 5-25
Fabric Manager ウィザードの使用 5-25
Fabric Manager のトラブルシューティング ツール 5-26

CHAPTER 6
Device Manager 6-1
Device Manager の概要 6-2
Device Manager の起動 6-2
Device Manager の使用法 6-3
メニューバー 6-3
ツールバー アイコン 6-4
ダイアログボックス 6-5
タブ 6-5
凡例 6-5
スーパーバイザおよびスイッチング モジュール 6-6
コンテキスト メニュー 6-7
Quick Configuration Tool の使用 6-8
Device Manager のプリファレンスの設定 6-10

CHAPTER 7
CFS の使用 7-1
CFS の概要 7-2
CFS 配信 7-3
CFS 配信のモード 7-3
非協調型配信 7-3
協調型配信 7-3
無制限の非協調型配信 7-3
スイッチの CFS 配信のイネーブル化およびディセーブル化 7-4
IP を介した CFS 配信 7-5
ファイバ チャネルを介した CFS 配信 7-6
CFS 配信のスコープ 7-7
CFS マージのサポート 7-7
アプリケーションの CFS サポート 7-8
CFS アプリケーション要件 7-8
アプリケーションの CFS のイネーブル化 7-8
ネットワークのロック 7-10

変更のコミット 7-10
変更の廃棄 7-11
コンフィギュレーションの保存 7-11
ロック済みセッションのクリア 7-12
CFS リージョン 7-13
CFS リージョンの概要 7-13
シナリオの例 7-13
Fabric Manager を使用した CFS リージョンの管理 7-14
CFS リージョンの作成 7-14
CFS リージョンへの機能の割り当て 7-15
別のリージョンへの機能の移動 7-16
リージョンからの機能の削除 7-17
CFS リージョンの削除 7-17
CFS 配信情報の表示 7-18
Fabric Manager を使用した CFS の例 7-19
Device Manager を使用した CFS の例 7-22
デフォルト設定 7-23

CHAPTER 8 イーサネット インターフェイスの設定 8-1
イーサネット インターフェイスの概要 8-2
イーサネット インターフェイスの設定 8-2
インターフェイス情報の表示 8-3
物理イーサネットのデフォルト設定値 8-4

CHAPTER 9 仮想インターフェイスの設定 9-1
仮想インターフェイスの概要 9-1
仮想インターフェイスの設定 9-2
VIG の作成 9-2
VIG ウィザードの使用 9-4
物理イーサネット インターフェイスへの VIG のバインド 9-4
VIG の削除 9-5
VI ウィザードの使用 9-5
仮想イーサネット インターフェイスの作成 9-6
仮想イーサネット インターフェイスの削除 9-7
仮想ファイバ チャネル インターフェイスの作成 9-8
仮想ファイバ チャネル インターフェイスの削除 9-8

CHAPTER 10 ファイバ チャネル インターフェイスの設定 10-1
ファイバ チャネル インターフェイスの概要 10-2

ライセンスの要件 10-2
物理ファイバ チャネル インターフェイス 10-2
仮想ファイバ チャネル インターフェイス 10-2
インターフェイス モード 10-3
E ポート 10-4
F ポート 10-4
NP ポート 10-4
TE ポート 10-4
SD ポート 10-5
Auto モード 10-5
インターフェイス ステート 10-5
管理ステート 10-6
動作ステート 10-6
原因コード 10-6
BB_credit 10-8
ファイバ チャネル インターフェイスの設定 10-9
ファイバ チャネル インターフェイスの設定 10-9
インターフェイスの管理ステートの設定 10-10
インターフェイス モードの設定 10-10
インターフェイスの説明の設定 10-11
管理速度の設定 10-11
自動検知 10-12
SD ポートのフレーム カプセル化の設定 10-12
受信データ フィールド サイズの設定 10-12
ビット エラーしきい値の概要 10-13
BB_credit の設定 10-13
ファイバ チャネル インターフェイスの確認 10-14
SFP トランスミッタ タイプの確認 10-14
インターフェイスの統計情報の収集 10-14
デフォルト設定 10-16

CHAPTER 11
ドメイン パラメータの設定 11-1
ファイバ チャネル ドメインの概要 11-2
ドメインの再起動の概要 11-3
ドメインの再起動 11-4
スイッチ プライオリティの概要 11-5
スイッチ プライオリティの設定 11-5
fcdomain の初期化の概要 11-5
fcdomain のイネーブル化またはディセーブル化 11-6

ファブリック名の設定 11-6
着信 RCF の概要 11-7
着信 RCF の拒否 11-7
結合ファブリックの自動再構成の概要 11-8
自動再構成のイネーブル化 11-8
ドメイン ID 11-9
ドメイン ID の概要 11-9
スタティック ドメイン ID または優先ドメイン ID の指定 11-11
許可ドメイン ID リストの概要 11-12
許可ドメイン ID リストの設定 11-12
許可ドメイン ID リストの CFS 配信の概要 11-13
配信のイネーブル化 11-14
ファブリックのロック 11-14
変更のコミット 11-14
変更の廃棄 11-15
ファブリックのロックのクリア 11-15
保留中の変更の表示 11-16
セッション ステータスの表示 11-16
連続ドメイン ID 割り当ての概要 11-16
連続ドメイン ID 割り当てのイネーブル化 11-17
FC ID 11-18
固定的 FC ID の概要 11-18
固定的 FC ID 機能のイネーブル化 11-19
固定的 FC ID 設定の注意事項 11-19
固定的 FC ID の設定 11-20
HBA の固有エリア FC ID の概要 11-21
HBA の固有エリア FC ID の設定 11-21
固定的 FC ID の選択消去の概要 11-23
固定的 FC ID の消去 11-23
fcdomain の統計情報の表示 11-24
デフォルト設定 11-24

CHAPTER 12 N ポート バーチャライゼーションの設定 12-1
NPV の概要 12-2
NP ポート 12-2
NP リンク 12-3
FLOGI 動作 12-3
注意事項および制限事項 12-5
NPV の設定 12-6

Device Manager による NPV の設定 12-6

CHAPTER 13 VSAN トランキングの設定 13-1
VSAN トランキングの概要 13-2
VSAN トランキングの不一致 13-2
VSAN トランキング プロトコル 13-3
VSAN トランキングの設定 13-4
注意事項および制約事項 13-4
トランク モードの概要 13-4
トランク モードの設定 13-5
トランク許可 VSAN リストの概要 13-6
VSAN の許可アクティブ リストの設定 13-7
デフォルト設定 13-8

CHAPTER 14 SAN ポート チャネルの設定 14-1
SAN ポート チャネルの概要 14-2
ポート チャネルおよび VSAN トランキングの概要 14-3
ロード バランシングの概要 14-4
SAN ポート チャネルの設定 14-6
SAN ポート チャネル設定の注意事項 14-7
SAN ポート チャネルの設定 14-7
SAN ポート チャネル モードの概要 14-10
SAN ポート チャネル削除の概要 14-11
SAN ポート チャネルの削除 14-12
SAN ポート チャネルのインターフェイス 14-13
SAN ポート チャネルへのインターフェイス追加の概要 14-13
互換性チェック 14-13
一時停止状態および分離状態 14-14
SAN ポート チャネルへのインターフェイスの追加 14-14
インターフェイスの強制追加 14-15
SAN ポート チャネルからのインターフェイス削除の概要 14-15
SAN ポート チャネルからのインターフェイスの削除 14-16
ポート チャネル プロトコル 14-17
チャネル グループの作成の概要 14-17
自動作成の注意事項 14-19
自動作成のイネーブル化および設定 14-19
手動設定チャネル グループの概要 14-20
手動設定チャネル グループへの変換 14-20
SAN ポート チャネル設定の確認 14-21

デフォルト設定 14-21

CHAPTER 15 VSAN の設定と管理 15-1
VSAN の概要 15-2
VSAN トポロジ 15-2
VSAN の利点 15-4
VSAN とゾーン 15-4
VSAN の設定 15-6
VSAN 作成の概要 15-6
VSAN の静的な作成 15-7
ポート VSAN メンバシップの概要 15-8
スタティック ポート VSAN メンバシップの概要 15-8
デフォルト VSAN の概要 15-9
分離された VSAN の概要 15-9
分離された VSAN メンバシップの概要 15-9
VSAN の動作ステート 15-10
スタティック VSAN の削除の概要 15-10
スタティック VSAN の削除 15-11
ロード バランシングの概要 15-11
ロード バランシングの設定 15-12
Interop モードの概要 15-12
デフォルト設定 15-12

CHAPTER 16 ゾーンの設定と管理 16-1
ゾーン分割の概要 16-2
ゾーン分割機能 16-2
ゾーン分割の例 16-3
ゾーン実装 16-4
アクティブおよびフル ゾーン セット設定時の注意事項 16-5
ゾーンの設定 16-7
ゾーン設定ツールの概要 16-7
ゾーン設定ツールを使用したゾーンの設定 16-8
ゾーン メンバーの追加 16-10
デフォルト ゾーン ポリシーの設定 16-12
ゾーン セット 16-13
ゾーン セットの作成の概要 16-13
ゾーン セットのアクティブ化 16-14
ゾーン メンバシップ情報の表示 16-16
デフォルト ゾーンの概要 16-16

デフォルト ゾーンの設定 16-17
FC エイリアスの作成の概要 16-18
FC エイリアスの作成 16-18
エイリアスへのメンバーの追加 16-20
ゾーンメンバーの pWWN ベースメンバーへの変換 16-22
ゾーンの実行 16-23
ゾーン セット配信 16-24
フル ゾーン セット配信のイネーブル化 16-24
ワンタイム配信のイネーブル化 16-25
リンクの分離からの回復の概要 16-26
ゾーン セットのインポートおよびエクスポート 16-27
ゾーン セット配信 16-28
ゾーン セットのコピー 16-29
ゾーンのバックアップおよび復元の概要 16-29
ゾーンのバックアップおよび復元 16-30
ゾーン、ゾーン セット、およびエイリアスの名前の変更 16-31
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 16-32
MDS 以外のデータベースの移行 16-32
ゾーン サーバ データベースの削除 16-33
ゾーン情報の確認 16-33
拡張ゾーン分割 16-34
拡張ゾーン分割の概要 16-34
基本ゾーン分割から拡張ゾーン分割への変更 16-35
拡張ゾーン分割から基本ゾーン分割への変更 16-36
拡張ゾーン分割のイネーブル化 16-36
データベースのマージ 16-37
ゾーン マージの分析 16-38
ゾーン マージ制御ポリシーの設定 16-38
ゾーン データベースのコンパクト化 16-39
デフォルト設定 16-39

CHAPTER 17 Distributing Device Alias Service 17-1
デバイス エイリアスの概要 17-2
デバイス エイリアスの機能 17-2
デバイス エイリアスの前提条件 17-2
ゾーン エイリアスとデバイス エイリアスの比較 17-3
デバイス エイリアス データベース 17-4
デバイス エイリアス モード 17-4

デバイス エイリアス モードの変更に関する注意事項 17-5
デバイス エイリアス モードの設定 17-5
デバイス エイリアス配信の概要 17-6
デバイス エイリアス データベースの配信 17-6
デバイス エイリアスの作成の概要 17-7
デバイス エイリアスの作成 17-7
変更のコミット 17-8
変更の廃棄 17-8
レガシー ゾーン エイリアスの変換 17-9
デバイス エイリアスまたは FC エイリアスの使用法 17-9
データベース マージの注意事項 17-10
デフォルト設定 17-10

CHAPTER 18 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 18-1
FSPF の概要 18-2
FSPF の例 18-2
フォールトトレラント ファブリックの例 18-2
冗長リンクの例 18-3
FSPF のグローバル設定 18-4
SPF 計算ホールド タイムの概要 18-4
LSR の概要 18-4
VSAN での FSPF の設定 18-5
FSPF のデフォルト設定へのリセット 18-5
FSPF のイネーブル化またはディセーブル化 18-6
FSPF インターフェイスの設定 18-7
FSPF リンク コストの概要 18-7
FSPF リンク コストの設定 18-7
ハロー タイム インターバルの概要 18-8
ハロー タイム インターバルの設定 18-8
デッド タイム インターバルの概要 18-9
デッド タイム インターバルの設定 18-9
再送信インターバルの概要 18-9
再送信インターバルの設定 18-9
特定のインターフェイスに対する FSPF のディセーブル化の概要 18-10
特定のインターフェイスに対する FSPF のディセーブル化 18-10
FSPF データベースの表示 18-10
FSPF 統計情報の表示 18-12
FSPF ルート 18-13
ファイバ チャネル ルートの概要 18-13

ファイバ チャネル ルートの設定 18-13
順序どおりの配信 18-15
ネットワーク フレーム順序の再設定の概要 18-15
SAN ポート チャネル フレーム順序の再設定の概要 18-16
順序どおりの配信のイネーブル化の概要 18-16
順序どおりの配信のグローバルなイネーブル化 18-17
特定の VSAN に対する順序どおりの配信のイネーブル化 18-17
ドロップ遅延時間の設定 18-18
デフォルト設定 18-19

CHAPTER 19 FLOGI、ネーム サーバ、FDMI、および RSCN データベースの管理 19-1
FLOGI の概要 19-2
ネーム サーバ プロキシ 19-3
ネーム サーバ プロキシ登録の概要 19-3
ネーム サーバ プロキシの登録 19-4
重複 pWWN の拒否の概要 19-4
重複 pWWN 拒否 19-4
ネーム サーバ データベース エントリの概要 19-5
ネーム サーバ データベース エントリの表示 19-5
FDMI 19-6
FDMI の表示 19-6
RSCN 19-7
RSCN 情報の概要 19-7
RSCN 情報の表示 19-8
multi-pid オプションの概要 19-8
multi-pid オプションの設定 19-9
RSCN 統計情報のクリア 19-9
CFS を使用した RSCN タイマー設定の配信 19-10
CFS による RSCN タイマーの設定 19-11
デフォルト設定 19-11

CHAPTER 20 SPAN の設定 20-1
SPAN 送信元の概要 20-2
送信元ポートの特性 20-2
SPAN 宛先の概要 20-3
宛先ポートの特性 20-3
SPAN の設定 20-4
Device Manager を使用した SPAN の設定 20-4
Device Manager を使用した SPAN セッションの作成 20-5

Device Manager を使用した SPAN 送信元の編集 20-6
Device Manager を使用した SPAN セッションの削除 20-7
SPAN のデフォルト設定値 20-7

CHAPTER 21
SCSI ターゲットの検出 21-1
SCSI LUN 検出の概要 21-2
SCSI LUN 検出開始の概要 21-2
SCSI LUN 検出の開始 21-3
カスタマイズ検出開始の概要 21-3
カスタマイズ検出の開始 21-4
SCSI LUN 情報の表示 21-4

CHAPTER 22
高度な機能および概念 22-1
ファイバ チャネルの TOV 22-2
すべての VSAN のタイマー設定 22-2
VSAN ごとのタイマー設定 22-4
fctimer 配信の概要 22-4
fctimer 配信のイネーブル化またはディセーブル化 22-5
データベース マージの注意事項 22-5
WWN 22-6
WWN 情報の確認 22-6
リンク初期化 WWN の使用法 22-6
セカンダリ MAC アドレスの設定 22-7
HBA の FC ID 割り当て 22-8
デフォルトの企業 ID リスト 22-8
企業 ID の設定の確認 22-9
スイッチの相互運用性 22-10
Interop モードの概要 22-10
interop モード 1 の設定 22-12
相互運用性ステータスの確認 22-13
デフォルト設定 22-14

CHAPTER 23
FC-SP および DHCHAP の設定 23-1
ファブリック認証の概要 23-2
DHCHAP 23-3
ファイバ チャネル機能との DHCHAP の互換性 23-4
DHCHAP イネーブル化の概要 23-4
DHCHAP のイネーブル化 23-4
DHCHAP 認証モードの概要 23-5

DHCHAP モードの設定 23-6
DHCHAP ハッシュ アルゴリズムの概要 23-6
DHCHAP ハッシュ アルゴリズムの設定 23-7
DHCHAP グループ設定の概要 23-7
DHCHAP グループの設定 23-7
DHCHAP パスワードの概要 23-8
ローカル スイッチの DHCHAP パスワードの設定 23-8
リモート デバイスのパスワード設定の概要 23-9
リモート デバイスの DHCHAP パスワードの設定 23-9
DHCHAP タイムアウト値の概要 23-9
DHCHAP タイムアウト値の設定 23-10
DHCHAP AAA 認証の設定 23-10
ISL 上での FC-SP のイネーブル化 23-10
デフォルト設定 23-11

CHAPTER 24
ポート セキュリティの設定 24-1
ポート セキュリティの概要 24-2
ポート セキュリティの実行 24-2
自動学習の概要 24-3
ポート セキュリティのアクティブ化 24-3
ポート セキュリティの設定 24-4
自動学習と CFS 配信を使用するポート セキュリティの設定 24-4
自動学習を使用し、CFS 配信を使用しないポート セキュリティの設定 24-5
手動データベース設定によるポート セキュリティの設定 24-6
ポート セキュリティのイネーブル化 24-7
ポート セキュリティのアクティブ化 24-9
ポート セキュリティのアクティブ化 24-9
データベースのアクティブ化の拒否 24-10
ポート セキュリティの強制的なアクティブ化 24-10
データベースの再アクティブ化 24-11
コンフィギュレーション データベースへのアクティブ データベースのコピー 24-11
アクティブなポート セキュリティ設定の表示 24-12
ポート セキュリティ統計情報の表示 24-12
ポート セキュリティ違反の表示 24-12
自動学習 24-13
自動学習のイネーブル化の概要 24-13
自動学習のイネーブル化 24-13

自動学習のディセーブル化 24-14
自動学習デバイスの許可 24-15
許可の例 24-15
ポート セキュリティの手動設定 24-17
WWN の識別の注意事項 24-17
許可済みのポート ペアの追加 24-18
ポート セキュリティ設定の削除 24-19
ポート セキュリティ設定の配信 24-20
配信のイネーブル化 24-20
ファブリックのロック 24-21
変更のコミット 24-21
アクティブ化および自動学習の設定の配信 24-21
データベース マージの注意事項 24-22
データベースの相互作用 24-23
データベースのシナリオ 24-23
ポート セキュリティ データベースのコピー 24-24
ポート セキュリティ データベースの削除 24-25
ポート セキュリティ データベースのクリア 24-25
デフォルト設定 24-26

CHAPTER 25
ファブリック バインディングの設定 25-1
ファブリック バインディングの概要 25-2
ライセンスの要件 25-2
ポート セキュリティとファブリック バインディングの比較 25-2
ファブリック バインディングの実行 25-3
ファブリック バインディングの設定 25-4
ファブリック バインディングの設定 25-4
ファブリック バインディングのイネーブル化 25-5
スイッチ WWN リストの概要 25-5
スイッチ WWN リストの設定 25-6
ファブリック バインディングのアクティブ化と非アクティブ化の概要 25-7
ファブリック バインディングのアクティブ化 25-7
ファブリック バインディングの強制的なアクティブ化 25-8
ファブリック バインディング設定のコピー 25-8
ファブリック バインディング設定の作成 25-9
ファブリック バインディング設定の削除 25-9
コンフィギュレーション ファイルへのファブリック バインディングのコピー 25-10

EFMD 統計情報の表示 25-10
ファブリック バインディング違反の表示 25-11
ファブリック バインディングのアクティブ データベースの表示 25-11
ファブリック バインディング設定の保存 25-12
ファブリック バインディング統計情報のクリア 25-12
ファブリック バインディング データベースの削除 25-13
デフォルト設定 25-13

CHAPTER 26
FCS の設定 26-1
FCS の概要 26-2
FCS の特性 26-3
FCS 検出情報の表示 26-4
FCS 要素の表示 26-5
FCS プラットフォームの作成 26-6
FCS Fabric Port の表示 26-7
デフォルト設定 26-8

CHAPTER 27
ポート トラッキングの設定 27-1
ポート トラッキングの概要 27-2
ポート トラッキングの設定 27-3
ポート トラッキングのイネーブル化 27-4
リンク対象ポート設定の概要 27-4
トラッキング対象ポートの動作バインディング 27-5
複数ポート トラッキングの概要 27-7
複数ポートのトラッキング 27-7
VSAN 内のポートの監視の概要 27-7
VSAN 内のポートの監視 27-8
強制シャットダウンの概要 27-8
トラッキング対象ポートの強制シャットダウン 27-8
ポート トラッキングのデフォルト設定値 27-8

CHAPTER 28
ネットワーク モニタリング 28-1
SAN 検出およびトポロジ マッピングの概要 28-2
デバイスの検出 28-2
トポロジ マッピング 28-2
トポロジ マップの使用方法 28-2
カスタマイズしたトポロジ マップ レイアウトの保存 28-3
Fabric Manager トポロジ マップでのラックの使用 28-4
複数ファブリックのマッピング 28-4

コンポーネント管理 28-4
Fabric Manager Web Server からの Inventory タブの使用方法 28-4
Device Manager からのログの表示 28-5
ヘルスおよびイベント モニタリング 28-5
Fabric Manager Events タブ 28-5
Fabric Manager Web Server Report のイベント情報 28-5
Device Manager のイベント 28-5

CHAPTER 29
Performance Manager 29-1
Performance Manager の概要 29-2
データ補間 29-3
データ収集 29-3
パフォーマンスしきい値の使用方法 29-3
フロー セットアップ ウィザード 29-4
フロー統計情報の設定 29-5
フロー統計の概要 29-5
フロー統計のカウント 29-5

CHAPTER 30
Nexus 5000 管理ソフトウェアの FAQ 30-1
Nexus 5000 シリーズの問題 30-2
Display FCoE モードについて 30-2
Display FCoE モードへのスイッチング 30-2
Fabric Manager の一般的な問題 30-2

CHAPTER 31
ファブリックのトラブルシューティング 31-1
トラブルシューティングのツールおよび技術 31-2
Cisco Traffic Analyzer 31-3
Cisco Protocol Analyzer 31-3
スイッチ デバイス状態の分析 31-4
スイッチ ファブリック設定の分析 31-5
エンドツーエンド接続の分析 31-7
ping ツールの使い方（fcping） 31-9
Trace Route（fctrace）などのトラブルシューティング ツールの使い方 31-10
ゾーン マージ結果の分析 31-11
show tech support コマンドの使用 31-12
CLI コマンドの実行 31-14
夏時間の調整 31-15
その他のスイッチの検索 31-16
ファイバ チャネルの TOV 31-18

VSAN ごとのタイマー設定 31-19
ファブリック アナライザの設定 31-21
Cisco Fabric Analyzer の概要 31-21
ローカル テキストベース キャプチャ 31-22
リモート キャプチャ デーモン 31-22
GUI ベース クライアント 31-23
Cisco Fabric Analyzer の設定 31-23
リモート IP アドレスへのキャプチャの送信 31-24
キャプチャされたフレームの表示 31-24
ディスプレイ フィルタの定義 31-25
キャプチャ フィルタ 31-25
使用可能なキャプチャ フィルタ 31-26
WWN の設定 31-27
リンク初期化 WWN の使用法 31-27
セカンダリ MAC アドレスの設定 31-28
WWN 情報の表示 31-28
HBA の FC ID 割り当て 31-29
デフォルト設定 31-29

INDEX 索引

はじめに

ここでは、『*Nexus 5000 シリーズ Fabric Manager コンフィギュレーション ガイド*』の対象読者、構成、および表記法について説明します。さらに、関連資料の入手方法についても説明します。

対象読者

このマニュアルは、Nexus 5000 シリーズ スイッチ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

このマニュアルは、次の章で構成されています。

章	タイトル	説明
第 1 章	製品概要	Nexus 5000 シリーズ スイッチの概要について説明します。
第 2 章	Cisco Fabric Manager のインストール	Fabric Manager コンポーネントと機能の概要、およびアプリケーションのインストールと起動に関する情報を示します。
第 3 章	Fabric Manager Server	Fabric Manager Server の GUI（グラフィカル ユーザ インターフェイス）および機能について詳細に説明します。
第 4 章	Fabric Manager の認証	Fabric Manager コンポーネントとファブリック スイッチ間の認証方式について説明します。
第 5 章	Fabric Manager Client	Fabric Manager Client の GUI および機能について詳細に説明します。
第 6 章	Device Manager	Device Manager の GUI および機能について詳細に説明します。
第 7 章	CFS の使用	Cisco Fabric Services（CFS）の GUI および機能について説明します。
第 8 章	イーサネット インターフェイスの設定	Fabric Manager を使用してイーサネット インターフェイスを設定する方法について説明します。
第 9 章	仮想インターフェイスの設定	Fabric Manager を使用して仮想インターフェイスを設定する方法について説明します。
第 10 章	ファイバ チャネル インターフェイスの設定	Fabric Manager を使用してファイバ チャネル インターフェイスを設定する方法について説明します。
第 11 章	ドメイン パラメータの設定	Fabric Manager を使用してファイバ チャネル ドメインを設定する方法について説明します。
第 12 章	N ポート バーチャライゼーションの設定	SAN 内の過剰なファイバ チャネル ドメイン ID を減らすための NPV デバイスの設定方法を説明します。
第 13 章	VSAN トランキングの設定	Fabric Manager を使用して VSAN トランクを設定する方法について説明します。
第 14 章	SAN ポート チャネルの設定	SAN ポート チャネルおよびロード バランシングの概念について説明し、SAN ポート チャネルの設定方法、ポート チャネルにポートを追加する方法、および SAN ポート チャネルからポートを削除する方法について詳細に説明します。
第 15 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 16 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 17 章	Distributing Device Alias Service	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。

章	タイトル	説明
第 18 章	ファイバ チャネル ルーティング サービスおよびプロトコルの設定	ファイバ チャネル ルーティング サービスおよびプロトコルの詳細情報と設定情報を示します。
第 19 章	FLOGI、ネーム サーバ、FDMI、および RSCN データベースの管理	ストレージ デバイスの管理および Registered State Change Notification（RSCN）データベースの表示に必要となる、ネーム サーバおよびファブリックのログインについて詳述します。
第 20 章	SPAN の設定	Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）、SPAN 送信元、フィルタ、SPAN セッション、SD ポート特性、および設定について説明します。
第 21 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 14 章	SAN ポート チャネルの設定	SAN ポート チャネルおよびロード バランシングの概念について説明し、SAN ポート チャネルの設定方法、ポート チャネルにポートを追加する方法、および SAN ポート チャネルからポートを削除する方法について詳細に説明します。
第 22 章	高度な機能および概念	高度な設定機能（タイムアウト値、fctrace ツール、およびシスコ製以外のスイッチとの相互運用）について説明します。
第 23 章	FC-SP および DHCHAP の設定	DHCHAP プロトコルについて説明します。DHCHAP は、Nexus 5000 シリーズ スイッチと他のデバイスの間で認証を提供する FC-SP プロトコルです。
第 24 章	ポート セキュリティの設定	Nexus 5000 シリーズ スイッチのポートへの不正アクセスを防止するポート セキュリティ機能について詳細に説明します。
第 25 章	ファブリック バインディングの設定	Fabric Manager を使用してファブリック バインディング機能を設定する方法について説明します。
第 26 章	FCS の設定	Fabric Manager を使用して Fabric Configuration Server（FCS）を設定する方法について説明します。
第 27 章	ポート トラッキングの設定	リンク障害の迅速な復旧を可能にするポート トラッキング機能について説明します。
第 28 章	ネットワーク モニタリング	Fabric Manager のモニタリング機能の使用方法を説明します。
第 29 章	Performance Manager	Performance Manager の使用方法について詳述します。
第 30 章	Nexus 5000 管理ソフトウェアの FAQ	FAQ の回答を示します。
第 31 章	ファブリックのトラブルシューティング	Fabric Manager のトラブルシューティングについて詳述します。

表記法

コマンドの説明では、次の表記法を使用しています。

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

出力例では、次の表記法を使用しています。

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

このマニュアルでは、次の表記法を使用しています。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

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

関連資料

Nexus 5000 シリーズのマニュアルは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

次に、Cisco Nexus 5000 シリーズに関連するマニュアルを示します。

『*Cisco Nexus 5000 Series Release Notes*』

『*Cisco Nexus 5000 Series CLI Software Configuration Guide*』Release 4.0

『*Cisco Nexus 5000 Series Fabric Manager Software Configuration Guide*』Release 4.0

『*Cisco Nexus 5000 Series System Messages Reference*』

『*Cisco Nexus 5000 Series Command Reference*』Release 4.0

『*Cisco Nexus 5000 Series Hardware Installation Guide*』Release 4.0

『*Cisco Nexus 5000 Series MIBs Reference*』Release 4.0

マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン

マニュアルの入手方法、テクニカル サポート、マニュアルに関するフィードバックの提供、セキュリティ ガイドライン、および推奨エイリアスや一般的なシスコのマニュアルについては、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

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

シスコのテクニカル サポート

次の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。

http://www.cisco.com/en/US/support/index.html

以下を含むさまざまな作業にこの Web サイトが役立ちます。

- テクニカル サポートを受ける
- ソフトウェアをダウンロードする
- セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける
- ツールおよびリソースへアクセスする
  - Product Alert の受信登録
  - Field Notice の受信登録
  - Bug Toolkit を使用した既知の問題の検索
- Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する
- トレーニング リソースへアクセスする
- TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する

Japan テクニカル サポート Web サイトでは、Technical Support Web サイト（http://www.cisco.com/techsupport）の、利用頻度の高いドキュメントを日本語で提供しています。

Japan テクニカル サポート Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

Service Request ツールの使用

Service Request ツールには、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

日本語版の Service Request ツールは次の URL からアクセスできます。

http://www.cisco.com/jp/go/tac/sr/

シスコの世界各国の連絡先一覧は、次の URL で参照できます。

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

その他の情報の入手方法

シスコの製品、サービス、テクノロジー、ネットワーキング ソリューションに関する情報について、さまざまな資料をオンラインで入手できます。

- シスコの E メール ニュースレターなどの配信申し込みについては、Cisco Subscription Center にアクセスしてください。

  http://www.cisco.com/offer/subscribe

- 日本語の月刊 Email ニュースレター「Cisco Customer Bridge」については、下記にアクセスください。

  http://www.cisco.com/web/JP/news/cisco_news_letter/ccb/

- シスコ製品に関する変更やアップデートの情報を受信するには、Product Alert Tool にアクセスし、プロファイルを作成して情報の配信を希望する製品を選択してください。Product Alert Tool には、次の URL からアクセスできます。

  http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

- 『*Cisco Product Quick Reference Guide*』はリファレンス ツールで、パートナーを通じて販売されている多くのシスコ製品に関する製品概要、主な機能、製品番号、および簡単な技術仕様が記載されています。『*Cisco Product Quick Reference Guide*』を発注するには、次の URL にアクセスしてください。

  http://www.cisco.com/go/guide

- ネットワークの運用面の信頼性を向上させることのできる最新の専門的サービス、高度なサービス、リモート サービスに関する情報については、Cisco Services Web サイトを参照してください。Cisco Services Web サイトには、次の URL からアクセスできます。

  http://www.cisco.com/go/services

- Cisco Marketplace では、さまざまなシスコの書籍、参考資料、マニュアル、ロゴ入り商品を提供しています。Cisco Marketplace には、次の URL からアクセスできます。

  http://www.cisco.com/go/marketplace/

- DVD に収録されたシスコの技術マニュアル（Cisco Product Documentation DVD）は、Product Documentation Store で発注できます。Product Documentation Store には、次の URL からアクセスできます。

  http://www.cisco.com/go/marketplace/docstore

- 日本語マニュアルの DVD は、マニュアルセンターから発注できます。マニュアルセンターには下記よりアクセスください。

  http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/manual_center/index.shtml

- Cisco Press では、ネットワーク、トレーニング、認定関連の出版物を発行しています。Cisco Press には、次の URL からアクセスできます。

  http://www.ciscopress.com

- 日本語のシスコプレスの情報は以下にアクセスください。

  http://www.seshop.com/se/ciscopress/default.asp

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスできます。

  http://www.cisco.com/ipj

- 『*What's New in Cisco Product Documentation*』は、シスコ製品の最新マニュアル リリースに関する情報を提供するオンライン資料です。毎月更新されるこの資料は、製品カテゴリ別にまとめられているため、目的の製品マニュアルを見つけることができます。

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

- シスコの Web サイトの各国語版へは、次の URL からアクセスしてください。

  http://www.cisco.com/public/countries_languages.shtml

CHAPTER 1

製品概要

Nexus 5000 シリーズは、データセンター向けの Top-of-Rack（TOR; トップオブラック）スイッチのファミリです。Nexus 5020 スイッチは、1.04 Tbps スイッチング スループットを備えた、10 ギガビット イーサネットおよび Fibre Channel over Ethernet（FCoE）スイッチです。Nexus 5020 は、最大 52 個の 10 ギガビット イーサネット ポートに低遅延ワイヤ スピードのスイッチングを提供します。

Nexus 5020 スイッチは FCoE をサポートし、データセンターの I/O Consolidation（IOC）を提供します。オプションのファイバ チャネル対応拡張モジュールは、4 個または 8 個のネイティブ ファイバ チャネル SAN インターフェイスを提供します。

この章では、Nexus 5000 シリーズ スイッチ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。

- Nexus 5000 シリーズの新しいテクノロジー（p.1-2）
- Nexus 5000 シリーズ スイッチ ハードウェア（p.1-4）
- Nexus 5000 シリーズ スイッチ ソフトウェア（p.1-5）
- 典型的な展開トポロジ（p.1-9）
- サポートされる規格（p.1-11）

Nexus 5000 シリーズの新しいテクノロジー

Nexus 5000 シリーズ スイッチはいくつかの新しいテクノロジーを導入しています。ここで説明する内容は、次のとおりです。

- FCoE（p.1-2）
- IOC（p.1-2）
- 仮想インターフェイス（p.1-3）

FCoE

FCoE は、物理イーサネット リンク上のファイバ チャネル トラフィックのカプセル化方式を提供します。FCoE フレームは一意の Ethertype を使用するので、FCoE トラフィックおよび標準イーサネット トラフィックを同一のリンクで伝送できます。

ファイバ チャネル トラフィックでは、ロスレス（無損失）トランスポート レイヤが必要です。ネイティブ ファイバ チャネルは、バッファ間クレジット システムを使用してロスレス サービスを実装します。イーサネット リンクは、FCoE トラフィックに対してロスレス サービスを提供する必要があります。

Nexus 5000 シリーズ スイッチのイーサネット リンクは、2 つのメカニズム（リンクレベル フロー制御とプライオリティ フロー制御）を提供して、FCoE トラフィックのロスレス転送を確保します。

IEEE 802.3x リンクレベル フロー制御では、輻輳している受信者が遠端に短期間データの転送を一時停止するように信号を送ることができます。ポーズ機能は、リンク上のすべてのトラフィックに適用されます。

Priority Flow Control（PFC; プライオリティ フロー制御）機能は、イーサネット リンク上の特定のトラフィック クラスにポーズ機能を適用します。たとえば、PFC は FCoE トラフィックにロスレス サービス、標準イーサネット トラフィックにベストエフォート サービスを提供できます。PFC は、IEEE 802.1p トラフィック クラスを使用してイーサネット トラフィックの特定のクラスに異なるサービス レベルを提供できます。

IOC

IOC により、単一のネットワーク テクノロジーで IP、SAN、および IPC トラフィックを伝送できます。

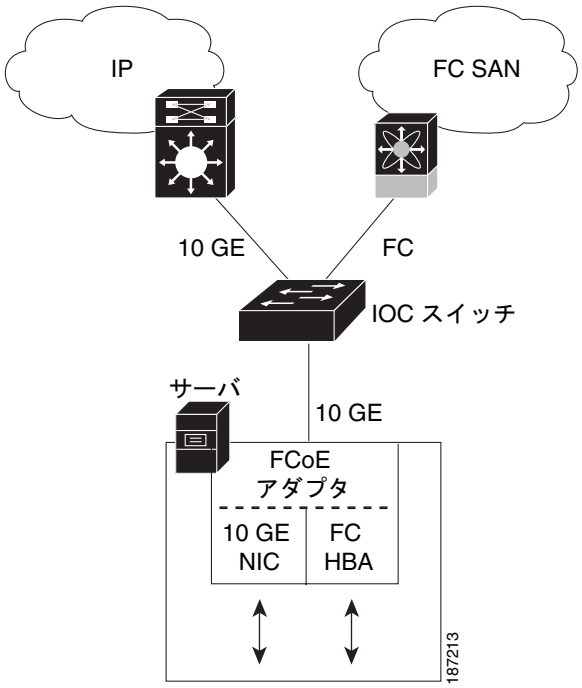
FCoE により、IOC の進化的手法を実現できます。上位のファイバ チャネル レイヤは変更されないので、ファイバ チャネルの運用モデルが維持されます。FCoE ネットワーク管理および設定は、ネイティブ ファイバ チャネル ネットワークに類似しています。

Nexus 5000 シリーズ スイッチは、FCoE を使用してスイッチとサーバ間の同一の物理イーサネット接続でファイバ チャネルおよびイーサネット トラフィックを伝送します。サーバでは、接続は Converged Network Adapter（CNA）で終端します。アダプタは、2 つのインターフェイス（イーサネット NIC インターフェイスとファイバ チャネル HBA インターフェイス）をサーバの Operating System（OS; オペレーティング システム）に提供します。サーバの OS は、FCoE のカプセル化を認識しません（図 1-1 を参照）。

スイッチ側では、着信イーサネット ポートは Ethertype を使用してフレームを区別し、イーサネット トラフィックとファイバ チャネル トラフィックを分離します。イーサネット フレームとファイバ チャネル フレームは、それぞれのネットワーク側のインターフェイスにスイッチングされます。

Nexus 5000 シリーズ スイッチは QoS（Quality Of Service）機能を提供して、スイッチ間のファイバ チャネル トラフィックに対してロスレス サービスを確保します。ベストエフォート サービスは、すべてのイーサネット トラフィックに適用できます。または、イーサネット トラフィックの特定のクラスに異なる QoS レベルを設定することもできます。

図 1-1　IOC



仮想インターフェイス

FCoE がイネーブルの場合、物理イーサネット ケーブルは論理イーサネット接続および論理ファイバ チャネル接続のトラフィックを伝送します。

Nexus 5000 シリーズ スイッチは仮想インターフェイスを使用して、同一物理イーサネットで伝送される論理接続を表します。Nexus 5000 シリーズ スイッチは、仮想イーサネットおよび仮想ファイバ チャネル インターフェイスをサポートします。

設定の目的で、仮想イーサネットおよび仮想ファイバ チャネル インターフェイスは、物理イーサネット インターフェイスのレイヤ 2 サブインターフェイスとして実装されます。

リンクレベル機能（リンク デバウンス タイマーおよび CDP など）は、物理イーサネット インターフェイスに設定されています。論理レイヤ 2 イーサネット機能（VLAN メンバシップおよび ACL など）は、仮想イーサネット インターフェイスに設定されています。論理ファイバ チャネル機能（VSAN メンバシップなど）は、仮想ファイバ チャネル インターフェイスに設定されています。

Nexus 5000 シリーズ スイッチ ハードウェア

Nexus 5020 スイッチは、Nexus 5000 シリーズの製品です。ここでは、Nexus 5020 スイッチ ハードウェアについて次の内容を説明します。

- シャーシ（p.1-4）
- 拡張モジュール（p.1-4）
- イーサネット インターフェイス（p.1-4）
- ファイバ チャネル インターフェイス（p.1-4）
- 管理インターフェイス（p.1-4）

シャーシ

Nexus 5020 スイッチは、ラック マウント用に設計された 2 RU シャーシです。このシャーシは、冗長ファンと冗長電源をサポートしています。

Nexus 5020 スイッチング ファブリックは低遅延、ノンブロッキングで、64 ～ 9216 バイトのイーサネット フレーム サイズをサポートしています。

拡張モジュール

Nexus 5020 スイッチには、オプションの拡張モジュールとして 2 つのスロットがあります。次の拡張モジュールを使用できます。

- N5K-M1404。4 個の 10 ギガビット イーサネット ポート、4 個の 1/2/4 Gb ファイバ チャネル ポートを提供。
- N5K-M1600。6 個の 10 ギガビット イーサネット ポートを提供。

拡張モジュールは、活性挿抜（Online Insertion and Removal; OIR）をサポートする Field-Replaceable Unit（FRU; 現場交換可能ユニット）です。

イーサネット インターフェイス

Nexus 5020 スイッチには、SFP+ インターフェイス アダプタを搭載した 40 個の固定 10 ギガビット イーサネット ポートを装備しています。拡張モジュールにより、さらに最大 12 個の 10 ギガビット イーサネット ポートを使用できます。

すべての 10 ギガビット イーサネット ポートが FCoE をサポートしています。各ポートをダウンリンク（サーバに接続）またはアップリンク（データセンター LAN に接続）として使用できます。

ファイバ チャネル インターフェイス

ファイバ チャネル ポートは、Nexus 5020 スイッチではオプションです。拡張モジュールを使用すると、最大 8 個のファイバ チャネル ポートを使用できます。

各ファイバ チャネル ポートをダウンリンク（サーバに接続）またはアップリンク（データセンター SAN ファブリックに接続）として使用できます。

管理インターフェイス

Nexus 5020 スイッチには、2 つの専用管理インターフェイス（シリアル コンソール ポートと 10/100/1000 イーサネット インターフェイス）があります。

Nexus 5000 シリーズ スイッチ ソフトウェア

Nexus 5000 シリーズ スイッチは Cisco Nexus Operating System（NX-OS）を実行するレイヤ 2 デバイスです。ここでは、Nexus 5000 シリーズ スイッチ ソフトウェアについて次の内容を説明します。

- イーサネット スイッチング（p.1-5）
- FCoE およびファイバ チャネル スイッチング（p.1-5）
- ライセンス（p.1-5）
- QoS（p.1-6）
- サービサビリティ（p.1-6）
- スイッチ管理（p.1-7）
- ネットワーク セキュリティ機能（p.1-8）
- VDC（p.1-8）

イーサネット スイッチング

Nexus 5000 シリーズ スイッチは、高密度および高性能なイーサネット システムをサポートするように設計されており、次のイーサネット スイッチング機能を提供します。

- IEEE 802.1D-2004 Rapid Spanning Tree Protocol（RSTP）および Multiple Spanning Tree Protocol（MSTP）（802.1w および 802.1s）
- IEEE 802.1Q VLAN およびトランク
- IEEE 802.3ad リンク集約
- プライベート VLAN
- トラフィック抑制（ユニキャスト、マルチキャスト、およびブロードキャスト）

FCoE およびファイバ チャネル スイッチング

Nexus 5000 シリーズ スイッチは、FCoE インターフェイス（サーバ側へ）およびネイティブ ファイバ チャネル インターフェイス（SAN 側へ）に提供することによって、データセンター IOC をサポートしています。

FCoE およびファイバ チャネル スイッチングには、次の機能が含まれます。

- Cisco Fabric Service
- N ポート バーチャライゼーション（NPV）
- VSAN および VSAN トランキング
- ゾーニング
- Distributed Device Alias Service
- SAN ポート チャネル

ライセンス

Cisco Nexus 5000 シリーズ スイッチには、出荷時にライセンスがインストールされています。スイッチは、ライセンスを管理するコマンド、および追加のライセンスをインストールするコマンドを提供します。

QoS

Nexus 5000 シリーズ スイッチは、トラフィックの優先順位付けおよび出力インターフェイスの帯域割り当てなどの QoS 機能を提供します。

スイッチのデフォルトの QoS 設定は、ファイバ チャネルおよび FCoE トラフィックに対してロスレス サービスを提供します。QoS は、イーサネット トラフィックに追加のサービス クラスを提供するように設定できます。

サービサビリティ

Nexus 5000 シリーズ スイッチのサービサビリティ機能は、ネットワーク プランに対してデータを提供し、問題解決の時間の短縮に役立ちます。

ここで説明する内容は、次のとおりです。

- SPAN（p.1-6）
- Ethanalyzer（p.1-6）
- Call Home（p.1-6）
- オンライン診断（p.1-7）
- EEM（p.1-7）

SPAN

Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能を使用すると、管理者は外部アナライザが取り付けられた SPAN 宛先ポートに、セッションに影響を及ぼすことなく SPAN セッション トラフィックを転送して、ポート間のすべてのトラフィックを分析できます。

Ethanalyzer

Ethanalyzer は、Wireshark（旧称 Ethereal）オープン ソース コードに基づく Cisco NX-OS プロトコル アナライザ ツールです。Ethanalyzer は、パケットのキャプチャとデコード用の Wireshark のコマンドライン バージョンです。Ethanalyzer を使用して、ネットワークのトラブルシューティングや、コントロールプレーン トラフィックの分析ができます。Ethanalyzer の詳細については、『*Cisco NX-OS Troubleshooting Guide, Release 4.0*』を参照してください。

Call Home

Call Home は、ハードウェア コンポーネントとソフトウェア コンポーネントを継続的に監視し、重要なシステム イベントを E メールで通知する機能です。多様なメッセージ形式を使用できるため、ポケベル サービス、標準 E メール、および XML ベースの自動解析アプリケーションと最適な互換性を保つことができます。アラートのグループ化や、宛先プロファイルのカスタマイズも可能です。この機能を利用すると、たとえばネットワーク サポート技術者を直接ポケットベルで呼び出したり、E メール メッセージを Network Operations Center（NOC; ネットワークオペレーションセンター）に送信したり、Cisco AutoNotify サービスを使用して直接 Cisco Technical Assistance Center（TAC）でケースを作成することができます。この機能は自律システム運用のために開発され、問題発生時にネットワーキング デバイスから IT スタッフへの通知を可能にし、問題の迅速な解決に役立ちます。

オンライン診断

Cisco Generic Online Diagnostics（GOLD; 汎用オンライン診断）は、ハードウェアおよび内部データパスが設計どおりに稼働していることを確認する診断ファシリティのスイートです。Cisco GOLD には、起動時診断、継続的監視、オンデマンドおよびスケジュールによるテストなどのフィーチャセットがあります。GOLD を使用することで、障害の迅速な分離と継続的なシステム監視が可能になります。

EEM

Cisco Embedded Event Manager（EEM）は、Cisco NX-OS に組み込まれているデバイスおよびシステム管理テクノロジーです。Cisco EEM を使用すると、ユーザは特定のネットワーク イベントがトリガーであるスクリプトを作成できます。

スイッチ管理

ここで説明する内容は、次のとおりです。

- SNMP（p.1-7）
- 構成の検証とロールバック（p.1-7）
- RBAC（p.1-7）
- コンフィギュレーション方式（p.1-7）

SNMP

Cisco NX-OS は、SNMP（簡易ネットワーク管理プロトコル）バージョン 1、2、および 3 に準拠しています。一連の MIB（Management Information Base; 管理情報ベース）がサポートされます。

構成の検証とロールバック

Nexus 5000 シリーズ スイッチでは、構成をコミットする前に構成の整合性や、必要なハードウェアリソースが使用可能かどうかを検証することができます。デバイスをあらかじめ構成しておいて、検証済みの構成をあとで適用することができます。また、構成にはチェックポイントが組み込まれるため、スイッチ オペレータは必要に応じて、問題がないことが分かっている構成に戻すことができます。

RBAC

Role-Based Access Control（RBAC; ロールベース アクセス コントロール）では、ユーザにロールを割り当てることで、スイッチ操作へのアクセスを制限できます。管理者はアクセスが必要なユーザだけにアクセスを許可するように、カスタマイズできます。

コンフィギュレーション方式

Nexus 5000 シリーズ スイッチは、ダイレクト ネットワーク コンフィギュレーション方式、または Fabric Manager サーバでホストされる Web サービスを使用して設定できます。

ここで説明する内容は、次のとおりです。

- CLI、XML 管理インターフェイス、または SNMP を使用した設定（p.1-8）
- Cisco MDS Fabric Manager を使用した設定（p.1-8）

CLI、XML 管理インターフェイス、または SNMP を使用した設定

次に示すように、CLI（コマンドライン インターフェイス）、Secure Shell（SSH; セキュア シェル）上の管理インターフェイス、または SNMP を使用して Nexus 5000 シリーズ スイッチを設定できます。

- CLI ― SSH セッション、Telnet セッション、またはコンソール ポートから CLI を使用してスイッチを設定できます。SSH では、デバイスへのセキュアな接続が提供されます。
- SSH 上の XML 管理インターフェイス ― XML 管理インターフェイスを使用してスイッチを設定できます。XML 管理インターフェイスは、CLI 機能を補完する NETCONF プロトコルに基づくプログラミング インターフェイスです。詳細については、『*Cisco NX-OS XML Management Interface User Guide, Release 4.0*』を参照してください。
- SNMP ― SNMP を使用すると、MIB を使用してスイッチを設定できます。

Cisco MDS Fabric Manager を使用した設定

Nexus 5000 シリーズ スイッチは、ローカル PC で稼働し Fabric Manager サーバを使用する Fabric Manager クライアントを使用して設定することもできます。

ネットワーク セキュリティ機能

Cisco NX-OS Release 4.0 は、次のセキュリティ機能を備えています。

- Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）および TACACS+
- IEEE 802.1x 認証および RADIUS
- SSH プロトコル バージョン 2
- Simple Network Management Protocol Version 3（SNMPv3）
- ポート セキュリティ
- DHCP スヌーピング
- Port-Based ACL（PACL）および VLAN-Based ACL（VACL）を含む、MAC ACL および IP ACL

VDC

Cisco NX-OS には、オペレーティング システムおよびハードウェア リソースを、仮想デバイスをエミュレートする Virtual Device Context（VDC; 仮想デバイス コンテキスト）にセグメント化する機能があります。Nexus 5000 シリーズ スイッチは、複数の VDC はサポートしていません。すべてのスイッチ リソースは、デフォルトの VDC で管理されます。

典型的な展開トポロジ

このリリースの、Nexus 5020 スイッチは、通常次のトポロジで展開されます。

- イーサネット TOR スイッチ トポロジ（p.1-9）
- IOC トポロジ（p.1-10）

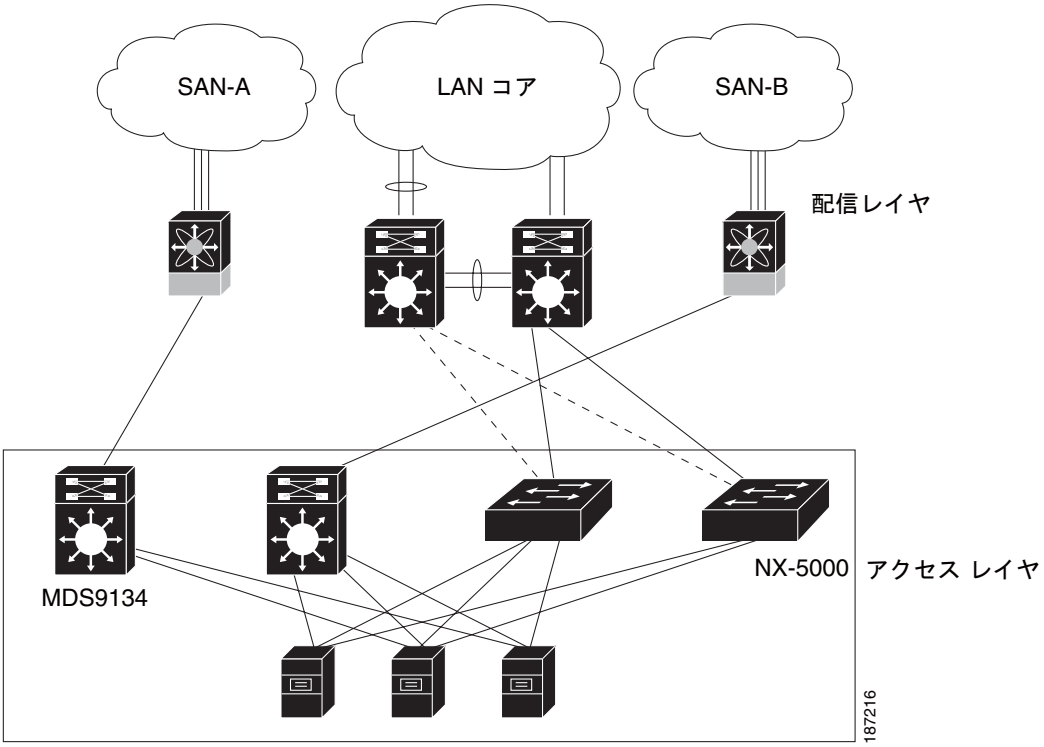
イーサネット TOR スイッチ トポロジ

Nexus 5020 スイッチは、データセンター LAN ディストリビューション レイヤ スイッチへのアップリンクを備えた、10 ギガビット イーサネット TOR スイッチとして展開できます。図 1-2 に構成例を示します。

この例では、ブレード サーバ ラックが Nexus 5020 スイッチへの 10 ギガビット イーサネット アップリンクをサポートするブレード スイッチを内蔵しています。ブレード スイッチは FCoE をサポートしていないので、Nexus 5020 スイッチには FCoE トラフィックおよびファイバ チャネル ポートがありません。

この構成例では、Nexus 5020 スイッチは 2 つの Catalyst スイッチへのイーサネット アップリンクを備えています。STP がデータセンター LAN でイネーブルにされている場合、一方のスイッチへのリンクは STP がアクティブになり、他のスイッチへのリンクでは STP がブロックされます。

図 1-2　イーサネット TOR スイッチ トポロジ



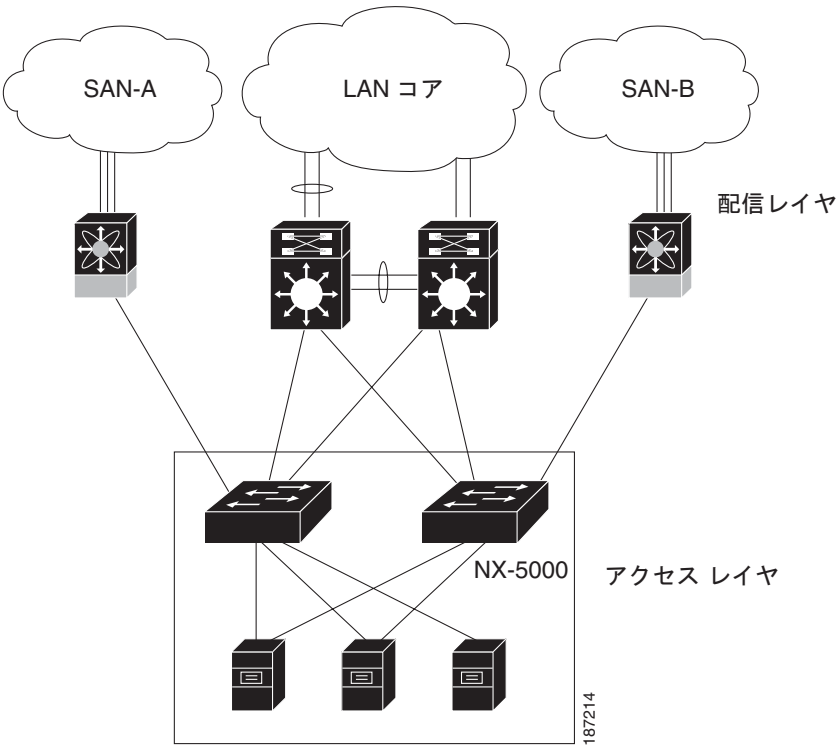
Nexus 5020 スイッチのすべてのサーバ側のポートは、標準のイーサネットを使用しています。FCoE は必要ではないので、10 ギガビット イーサネット NIC を使用してサーバ ポートが接続されます。

サーバは、MDS 9134 SAN スイッチを介してデータセンター SAN に接続されます。サーバのファイバ チャネル ポートには、標準ファイバ チャネル HBA が必要です。

IOC トポロジ

図 1-3 に、Nexus 5020 スイッチの典型的な IOC シナリオを示します。

図 1-3　IOC トポロジ



Nexus 5020 スイッチは、FCoE を使用してサーバ ポートに接続されます。サーバのポートには、CNA が必要です。冗長構成の場合、各サーバが両方の Nexus 5020 スイッチに接続されます。これには、デュアルポート CNA アダプタを使用できます。CNA はアクティブ / パッシブ モードで設定できます。サーバは、サーバベースのフェールオーバーをサポートしている必要があります。

Nexus 5020 スイッチでは、イーサネットのネットワーク側ポートは 2 つの Catalyst 6500 スイッチに接続されます。必要なアップリンク トラフィック量に応じて、各 Catalyst スイッチに複数のポートが接続され、ポート チャネルとして設定される場合があります。STP がデータセンター LAN でイネーブルにされている場合、一方のスイッチへのリンクは STP がアクティブになり、他方のスイッチへのリンクでは STP がブロックされます。

Nexus 5020 SAN のネットワーク側ポートは、Cisco MDS 9000 ファミリ スイッチに接続されます。必要なトラフィック量に応じて、各 MDS 9000 ファミリ スイッチに複数のファイバ チャネル ポートが接続され、SAN ポート チャネルとして設定される場合があります。

サポートされる規格

表 1-1 に、Nexus 5000 シリーズ スイッチでサポートされる規格を示します。

表 1-1　IEEE 準拠

規格	説明
802.1D	MAC ブリッジ
802.1s	MSTP
802.1w	RSTP
802.1AE	MAC セキュリティ（リンク層暗号化）
802.3ad	LACP によるリンク集約
802.3ae	10 ギガビット イーサネット
802.1Q	VLAN タギング
802.1p	イーサネット フレームのサービス クラス タギング
802.1x	ポートベースのネットワーク アクセス コントロール

CHAPTER 2

Cisco Fabric Manager のインストール

Cisco Fabric Manager を使用すると、CLI（コマンドライン インターフェイス）を使用しなくても、一般的なスイッチ設定作業を実行できます。Fabric Manager は、ファイバ チャネル ファブリックをリアルタイムに表示する GUI を備え、シスコおよびサードパーティ製 SAN スイッチの設定を管理できます。

この章の内容は、次のとおりです。

- Cisco Fabric Manager の概要（p.2-2）
- スイッチ管理の概要（p.2-5）
- 管理ソフトウェアのインストール（p.2-7）
- 管理ソフトウェアのアップグレード（p.2-21）
- Cisco Fabric Manager とその他の管理ツールとの統合（p.2-21）
- ファイアウォールの背後での Fabric Manager の稼働（p.2-22）
- 管理ソフトウェアのアンインストール（p.2-23）

Cisco Fabric Manager の概要

Cisco Fabric Manager を使用すると、CLI を使用しなくても、多くのスイッチ コンフィギュレーション コマンドを実行できます。CLI を使用した Nexus 5000 シリーズ スイッチの設定方法の詳細については、『*Cisco Nexus 5000 Series CLI Configuration Guide*』を参照してください。

Fabric Manager は、完全な設定機能およびステータス モニタリング機能のほかに、ファイバ チャネル ping や traceroute などの強力なファイバ チャネル トラブルシューティング ツールを備えています。

Cisco Fabric Manager は次に示す管理アプリケーションで構成されます。

- Fabric Manager Server（p.2-2）
- Fabric Manager Client（p.2-2）
- Fabric Manager Server プロキシ サービス（p.2-3）
- Device Manager（p.2-4）
- Performance Manager（p.2-4）
- Fabric Manager Web Server（p.2-4）

Fabric Manager Server

Fabric Manager Server ソフトウェアは、Fabric Manager を実行する前にインストールしておく必要があります。Windows PC では、Fabric Manager Server はサービスとしてインストールされ、Windows Services コントロール パネルを使用して管理されます。Fabric Manager Server は物理および論理ファブリックの検出や、SNMP（簡易ネットワーク管理プロトコル）トラップ、Syslog メッセージ、および Performance Manager しきい値イベントを受信します。詳細については、第 3 章「Fabric Manager Server」を参照してください。

Fabric Manager Client

Fabric Manager Client コンポーネントでは、シスコ スイッチ、サードパーティ製スイッチ、ホスト、ストレージ デバイスなど、ファイバ チャネル ネットワーク ファブリックのマップが表示されます。Fabric Manager Client には、Fabric Manager Server の機能にアクセスするためのメニューが複数用意されています。詳細については、第 5 章「Fabric Manager Client」を参照してください。

Fabric Manager Server プロキシ サービス

Fabric Manager Client および Device Manager は、SNMP を使用して Fabric Manager Server と通信します。通常の設定では、Fabric Manager Server がファイアウォールの背後にインストールされることがあります。Cisco Fabric Manager で使用可能な SNMP プロキシ サービスは、これらの SNMP 要求に対して、TCP ベースのトランスポート プロキシを提供します。SNMP プロキシ サービスを使用すると、ファイアウォールで UDP トラフィックをすべてブロックしたり、設定された TCP ポートを介して通信するように Fabric Manager Client を設定することができます。

Fabric Manager は、スイッチの一部の機能の管理に CLI を使用します。これらの管理作業は、Fabric Manager で使用され、プロキシ サービスは使用されません。次の CLI 機能にアクセスするには、使用中のファイアウォールが Fabric Manager に対してオープンである必要があります。

- 外部および内部のループバック テスト
- フラッシュ ファイルへのアクセス
- CLI ユーザの作成
- **Show image version** コマンド
- **Show tech** コマンド
- スイッチ保管レポート（Syslog、アカウンティング）
- ゾーンの移行
- **Show cores** コマンド

SNMP プロキシ サービスを使用していて、サーバ上の別のアプリケーションがポート 9198 を使用している場合は、ワークステーションの設定値を変更する必要があります。

（注） スイッチは、CLI とは異なり、常に、リモート AAA ユーザよりもローカル SNMP ユーザを先に確認します。

プロキシ サービスを使用するために Windows ワークステーションを変更する手順は、次のとおりです。

ステップ 1　Internet Explorer を開き、［**ツール**］>［**インターネット オプション**］を選択します。

［インターネット オプション］ダイアログボックスが表示されます。

ステップ 2　［**接続**］タブをクリックし、［**LAN の設定**］を選択します。

［LAN の設定］ダイアログボックスが表示されます。

ステップ 3　［**LAN にプロキシ サーバーを使用する**］チェックボックスをオンにして、［**詳細設定**］をクリックします。

ステップ 4　［例外］セクションに、サーバ IP アドレスまたはローカル ホストを追加します。

ステップ 5　［**OK**］をクリックして、変更を保存します。

詳細については、「ファイアウォールの背後での Fabric Manager の稼働」（p.2-22）を参照してください。

Device Manager

Device Manager は、1 台のスイッチに対し 2 つのビューを表示します。

- Device View — スイッチ コンフィギュレーションがグラフィック表示され、統計情報および設定情報にアクセスできます。
- Summary View には、スイッチの xE ポート（ISL［スイッチ間リンク］）、Fx ポート（ファブリック ポート）、Nx ポート（接続先ホストおよびストレージ）、スイッチの SAN ポート チャネルや、ファイバ チャネルおよび IP ネイバー デバイスのサマリーが表示されます。Summary View は、動作可能なすべての仮想インターフェイス（ファイバ チャネルおよびイーサネット）も表示します。サマリーまたは詳細統計情報は図示したり、印刷したり、タブ区切りフォーマットでファイルに保存したりできます。詳細については、第 6 章「Device Manager」を参照してください。

Performance Manager

Performance Manager は SNMP を使用してデータを取り込み、詳細なトラフィック分析を行います。このデータはさまざまなグラフおよびチャートに変換され、あらゆる Web ブラウザで表示できます。詳細については、第 29 章「Performance Manager」を参照してください。

Fabric Manager Web Server

Fabric Manager Web Server を使用すると、オペレータは Web ブラウザを使用して、離れた場所からイベント、パフォーマンス、およびコンポーネントを監視したり、レポートを取得したりできます。

スイッチ管理の概要

Cisco Nexus 5000 シリーズ スイッチは、標準管理プロトコルを使用してアクセスおよび設定されます。表 2-1 に、Cisco Nexus 5000 シリーズ スイッチに対するアクセス、モニタ、および設定用に Fabric Manager がサポートしている管理プロトコルを示します。

表 2-1　サポート対象の管理プロトコル

管理プロトコル	目的
Telnet/SSH	Cisco Nexus 5000 シリーズ スイッチの CLI へのリモート アクセスを実現します。
FTP/SFTP/TFTP、SCP	コンフィギュレーション イメージおよびソフトウェア イメージをデバイス間でコピーします。
SNMPv1、v2c、および v3	80 個を超える異なる MIB（管理情報ベース）を含みます。Cisco Nexus 5000 シリーズ スイッチは SNMP バージョン 1、2、3、および RMON V1、V2 をサポートします。RMON は、デバイスまたはネットワーク動作の変化に基づいて、しきい値の設定や通知の送信を含む、高度なアラームおよびイベント管理を行います。 デフォルトでは、Cisco Fabric Manager は Cisco Nexus 5000 シリーズ スイッチとの通信に SNMPv3 を使用します。SNMPv3 は暗号化されたユーザ名およびパスワードを使用して、安全な認証を実現します。SNMPv3 にはすべての管理トラフィックを暗号化する機能もあります。
HTTP/HTTPS	Fabric Manager Web Server との通信や、Cisco Fabric Manager ソフトウェアの配布およびインストールに使用される Web ブラウザの HTTP および HTTPS を含みます。HTTP は、Cisco Fabric Manager Server と Cisco Nexus 5000 シリーズ スイッチ間の通信には使用されません。
XML/CIM over HTTP/HTTPS	Cisco NX-OS で稼働する Storage Area Network（SAN; ストレージ エリア ネットワーク）管理アプリケーションの設計に対する CIM サーバのサポートを含みます。
ANSI T11 FC-GS-3	Fabric Configuration Server（FCS）で管理サーバを定義する際に、Fibre Channel-Generic Services（FC-GS-3）を提供します。Fabric Manager はネーム サーバ データベースおよび Fibre Channel Shortest Path First（FSPF）トポロジ データベースに格納された情報の上部に位置する、FCS が提供する情報を使用して、詳細なトポロジ ビューを作成し、ファブリックのすべてのデバイスの情報を収集します。

Fabric Manager は、帯域内または帯域外管理接続を使用してスイッチに接続されます。ここでは、接続方法について説明します。

- mgmt0（p.2-6）
- IPFC（p.2-6）

mgmt0

帯域外管理接続は、スーパーバイザ モジュールの 10/100 Mbps イーサネット インターフェイス（mgmt0 のラベル）です。mgmt0 インターフェイスを管理ネットワークに接続すると、イーサネット上で IP を介してスイッチにアクセスできます。そのためには、ファブリック内の少なくとも 1 台の Cisco MDS 9000 ファミリ スイッチ、または Nexus 5000 シリーズ スイッチに、イーサネット管理ポートを通して接続する必要があります。その後は、この接続を使用して、帯域内（ファイバ チャネル）接続によるその他のスイッチの管理を実行できます。この接続を使用しない場合は、各スイッチの mgmt0 ポートをイーサネット ネットワークに接続する必要があります。

IPFC

帯域内 IP 接続を使用して、ファイバ チャネル ネットワーク上のスイッチを管理することもできます。Cisco MDS 9000 ファミリは、IPFC ネットワークをトランスポートするためのカプセル化方式を定義する RFC 2625 IPFC をサポートします。

IPFC は IP パケットをファイバ チャネル フレームにカプセル化します。これにより、スイッチごとに専用のイーサネット接続を確立しなくても、ファイバ チャネル ネットワーク上で管理情報を伝達できるようになります。この機能を使用すると、帯域内管理ソリューションを完全に構築できます。

（注） Fabric Manager を使用するには、少なくとも 1 つの Cisco MDS 9000 ファミリ、または Nexus 5000 シリーズ スイッチに帯域外（イーサネット）接続を行う必要があります。

管理ソフトウェアのインストール

ここでは、Fabric Manager および Device Manager をインストールする方法について説明します。ここでは、次の内容について説明します。

- インストールを開始する前に（p.2-7）
- サポート対象のソフトウェア（p.2-7）
- データベースのインストール（p.2-8）
- Fabric Manager のインストール（p.2-10）
- Device Manager のインストール（p.2-18）

インストールを開始する前に

Cisco Fabric Manager にアクセスする前に、次の作業を実行する必要があります。

ステップ 1　スーパーバイザ モジュールには、セットアップ ルーチンまたは CLI を使用して次の値を設定します。

- mgmt0 インターフェイスに割り当てられる IP アドレス
- SNMP クレデンシャル（v3 ユーザ名およびパスワードまたは v1/v2 コミュニティ）— ファブリック内のすべてのスイッチに対して同じユーザ名およびパスワードを維持します。

（注）　Nexus 5000 シリーズ スイッチは、RADIUS、TACACS、またはローカル SNMP ユーザを使用した AAA 認証をサポートします。

ステップ 2　Fabric Manager ソフトウェアを入手します。Cisco.com の次の URL からダウンロードできます。

http://cisco.com/cgi-bin/tablebuild.pl/mds-fm

ステップ 3　Fabric Manager および Device Manager のインスタンスをすべてシャットダウンします。

（注）　最新バージョンの Fabric Manager アプリケーションをインストールすることを推奨します。Fabric Manager は、Nexus 5000 シリーズ スイッチで稼働する NX-OS ソフトウェアと下位互換性があります。スイッチをアップグレードする場合、まず Fabric Manager ソフトウェアをアップグレードしてから、スイッチの Cisco NX-OS ソフトウェアをアップグレードします。

サポート対象のソフトウェア

（注）　ソフトウェア サポートに関する最新情報は、『*Cisco Nexus 5000 Series Release Notes for Cisco NX-OS Release 4.0*』を参照してください。

Cisco Fabric Manager は、次のソフトウェアをサポートしています。

- OS（オペレーティング システム）
  - Windows 2000 SP4、2003 SP2、XP SP2
  - Redhat Linux（2.6 Kernel）
  - Solaris（SPARC）8 および 10
  - VMWare Server 1.0

- Java
  - Sun JRE および JDK 1.5(x) がサポートされています。
  - Java Web Start 1.2、1.0.1 および 1.5
- ブラウザ
  - Internet Explorer 6.x および 7.0

（注） Internet Explorer 7.0 は Windows 2000 SP4 ではサポートされていません。

  - Firefox 1.5 および 2.0
- データベース
  - Oracle Database 10g Express
  - PostgreSQL 8.2（Windows）
  - PostgreSQL 8.1（Solaris および Linux）
- セキュリティ
  - Cisco ACS 3.1 および 4.0
  - PIX Firewall
  - IP テーブル
  - SSH v2
  - Global Enforce SNMP Privacy Encryption
  - HTTPS

最小限のハードウェア要件

大規模ファブリック（1000 以上のエンド デバイス）で Fabric Manager Server が稼働している PC では、2 GB の RAM および 10 GB の空きディスク容量を備えた Dual Core/Dual CPU 高速システムの使用を推奨します。

データベースのインストール

Fabric Manager では、Oracle Database 10g Express または PostgreSQL データベースが必要です。

Fabric Manager インストレーション ウィザードには、PostgreSQL データベースを自動的にインストールするオプションがあります。このオプションを選択しない場合、Fabric Manager をインストールする前にデータベースをインストールする必要があります。

（注） 大規模ファブリック（1000 以上のエンド デバイス）で Performance Manager を稼働しているユーザの場合は、Oracle Database 10g Express オプションを推奨します。

Oracle のインストール

（注） Oracle Database 10g Express を使用する場合は、Fabric Manager のインストールを続行する前に、データベースをインストールして、ユーザ名とパスワードを作成する必要があります。

Oracle データベースのインストール手順は、次のとおりです。

ステップ 1　次の URL にアクセスし、Oracle Database 10g Express をインストールします。

http://www.oracle.com/technology/software/products/database/xe/index.html

（注） PC にすでに別の Oracle インスタンスがインストールされている場合は、同じ PC に Oracle データベースをインストールしないことを推奨します。このような場合、Fabric Manager が使用できるのは PostgreSQL データベースのみです。

ステップ 2　OracleXE.exe を実行して Oracle データベースをインストールし、システム ユーザのパスワードを設定します。

Oracle インストーラによって Oracle Database 10g Express サーバがインストールされ、データベース管理者がこのサーバを管理する際は、パスワードを使用します。

ステップ 3　インストールを完了し、Services ウィンドウで両方のサービス（OracleServiceXE および OracleXETNSListener）が稼働していることを確認します。

ステップ 4　次のスクリプトを実行してデフォルトの Oracle admin ポートを変更し、データベース アカウントを作成します。

```
C:\> cd c:\oraclexe\app\oracle\product\10.2.0\server\bin
C:\oraclexe\app\oracle\product\10.2.0\server\bin>sqlplus / as sysdba
SQL> exec dbms_xdb.sethttpport(8082);
SQL> GRANT CONNECT,RESOURCE,UNLIMITED TABLESPACE TO SCOTT IDENTIFIED BY
TIGER;
SQL> EXIT;
```

（注） Oracle Database 10g Express オプションを使用できるのは、Microsoft Windows の場合だけです。UNIX システムでは使用できません。

Oracle データベースのバックアップについては、次の URL にアクセスしてください。

http://download.oracle.com/docs/cd/B25329_01/doc/admin.102/b25107/backrest.htm#i1004902

または次の URL の exp/imp ユーティリティを使用してください。

http://download.oracle.com/docs/cd/B25329_01/doc/admin.102/b25107/impexp.htm#BCEEDCIB

（注） PostgreSQL データベースのバックアップの詳細については、pg_dump ユーティリティを実行してください。ユーティリティを実行するには、次の URL にアクセスしてください。
http://www.postgresql.org/docs/8.1/static/app-pgdump.html

Fabric Manager のインストール

CD-ROM または Cisco.com から Fabric Manager をインストールする必要があります。

（注） Fabric Manager をインストールするユーザには、ユーザ アカウントを作成し、サービスを起動するためのすべての管理権限が必要です。また、すべてのポートへのアクセス権も必要です。Fabric Manager Server と PostgreSQL データベースが使用するポートは次のとおりです。
1098、1099、4444、4445、8009、8083、8090、8092、8093、514、5432

Cisco.com からソフトウェアをダウンロードする場合は、次の Web サイト にアクセスしてください。

http://cisco.com/cgi-bin/tablebuild.pl/mds-fm

Solaris に Fabric Manager をインストールする手順は次のとおりです。

ステップ 1　Fabric Manager のインストールに使用するパスに Java 1.5 を設定します。

ステップ 2　「データベースのインストール」（p.2-8）の手順に従って、Fabric Manager に使用するデータベースをインストールします。

ステップ 3　Fabric Manager の jar ファイル、m9000-fm-3.3.0.*xx*.jar を、CD-ROM から Solaris ワークステーション上のフォルダにコピーします。

（注） CD-ROM のファイル名には、ステップ 3 で示した「*xx*」の箇所に番号が含まれます。ステップ 4 の **java** コマンドにも、「*xx*」と同じ番号を使用してください。

ステップ 4　次のコマンドを使用して、インストーラを起動します。

```
java -Xmx256m -jar m9000-fm-3.3.0.xx.jar
```

ステップ 5　Fabric Manager 管理ソフトウェア セットアップ ウィザードの画面に表示される指示に従います。

サーバの初回の接続時に、ワークステーションにインストールされている Sun Java Virtual Machine バージョンが正しいかどうか、Fabric Manager から確認を求められます。Fabric Manager はインストール中にバージョン 1.5(x) を検索します。必要な場合は、Sun Java Virtual Machine ソフトウェアをインストールします。

（注） Java 要件が異なっている場合でも、Fabric Manager と同じ PC 上で CiscoWorks を実行できます。Fabric Manager 用に新しい Java バージョンをインストールする場合は、CiscoWorks に必要な古い Java バージョンを上書きしないようにしてください。両方の Java バージョンは PC 上 で共存できます。

（注） Windows の場合、Fabric Manager のインストールやアップグレードは、リモート デスクトップではなく、VNC を使用してコンソールから実行する必要があります。

Windows に Fabric Manager をインストールする手順は次のとおりです。

ステップ 1　**Install Management Software** リンクをクリックします。

ステップ 2　**Management Software** > **Cisco Fabric Manager** を選択します。

ステップ 3　**Installing Fabric Manager** リンクをクリックします。

ステップ 4　**FM Installer** リンクをクリックします。

Cisco Fabric Manager Installer ウィンドウに、管理ソフトウェア セットアップ ウィザードへのウェルカム メッセージが表示されます（図 2-1 を参照）。

図 2-1　管理ソフトウェア セットアップ ウィザードのウェルカム メッセージ

ステップ 5　**Next** をクリックするとインストールが開始されます。

ステップ 6　**I accept the terms of the License Agreement** チェックボックスにチェックを入れ、**Next** をクリックします。

Install Options ダイアログボックスが表示されます（図 2-2 を参照）。

図 2-2　Install Options ダイアログボックス

ステップ 7　いずれかのオプション ボタンをクリックします。

- Fabric Manager Server (Licensed) ― Fabric Manager Server のサーバ コンポーネントをインストールします。
- Fabric Manager Standalone ― Fabric Manager のスタンドアロン バージョンをインストールします。

（注）　Fabric Manager Standalone は、Fabric Manager Client と、これにバンドルされているローカル バージョンの Fabric Manager Server からなる単一アプリケーションです。Fabric Manager Standalone では、隣接したファブリックの検出と監視を行うことができます。

ステップ 8　Fabric Manager のインストール用にワークステーション上のフォルダを選択します。

- Windows では、デフォルトのロケーションは C:\Program Files\Cisco Systems\MDS 9000 です。
- UNIX（Solaris または Linux）マシンでは、インストール パス名は、インストールを実行するユーザの権限に応じて、/usr/local/cisco_mds9000 または $HOME/cisco_mds9000 になります。

ステップ 9　**Next** をクリックします。

Database Options ダイアログボックスが表示されます（図 2-3 を参照）。

図 2-3　Database Options ダイアログボックス

ステップ 10　**Install PostgreSQL** オプション ボタンをクリックして、Postgre SQL データベースをインストールします。**Use existing DB** をクリックして、使用するデータベースを指定します。

Install PostgreSQL を選択した場合は、デフォルトを受け入れ、パスワードを入力します。PostgreSQL データベースがインストールされます。

（注）　PostgreSQL のインストールを選択した場合は、稼働中のすべてのセキュリティ ソフトウェアをディセーブルにする必要があります。そうしないと、一部のフォルダやユーザがインストールされないことがあります。

（注）　ご使用のシステムで Cygwin が稼働している場合は、PostgreSQL をインストールする前に、環境変数パスから **cygwin/bin** を削除してください。

ステップ 11　**Use existing DB** を選択する場合は、**PostgreSQL 8.1/8.2** オプション ボタンまたは **Oracle10g** オプション ボタンをクリックします。

ステップ 12 Database Options ダイアログボックスで、**Next** をクリックします（図 2-3 を参照）。

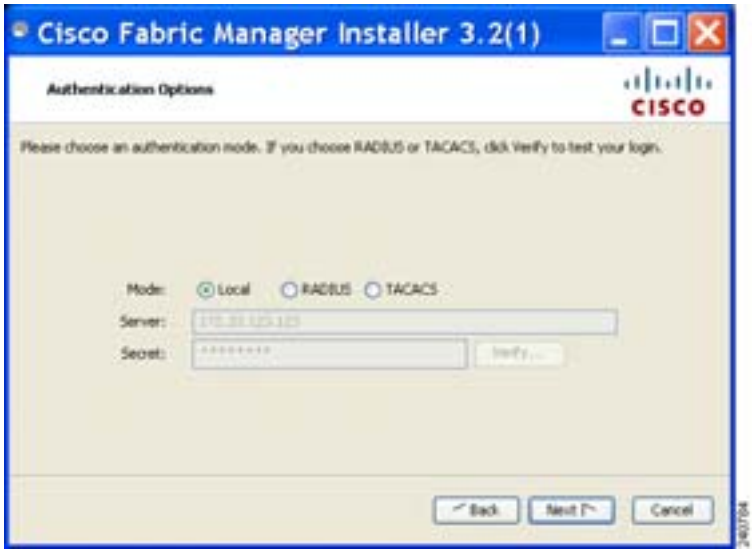
User Options ダイアログボックスが表示されます（図 2-4 を参照）。

図 2-4　User Options ダイアログボックス

ステップ 13 ユーザ名およびパスワードを入力し、**Next** をクリックします。

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

図 2-5　Authentication Options ダイアログボックス



ステップ 14 認証モード（Local、RADIUS、または TACACS）を選択して、**Next** をクリックします。**Verify** をクリックして、ログインをテストします。

Fabric Manager Standalone の場合は、Configuration Options ダイアログボックスが表示されます（図 2-6 を参照）。

図 2-6　Fabric Manager Standalone の Configuration Options ダイアログボックス

ステップ 15 Fabric Manager Standalone をインストールする場合は、必要に応じて、**FC Alias** および **SNMPv3** のチェックボックスをオンにしてから、**Install** をクリックします。

Fabric Manager Server の場合は、Configuration Options ダイアログボックスが表示されます（図 2-7 を参照）。

図 2-7　Fabric Manager Server の Configuration Options ダイアログボックス

ステップ 16 Fabric Manager Server をインストールする場合は、必要に応じて、ローカル インターフェイスと Web サーバ ポートを選択するか、**FC Alias** および **SNMPv3** のチェックボックスをオンにして、**Install** をクリックします。

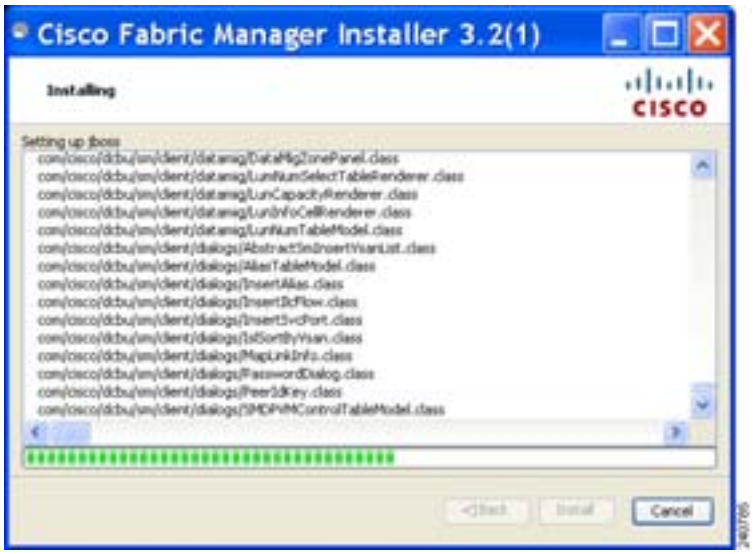
（注） **Use HTTPS Web Server** チェックボックスをオンにした場合、Web Server Port フィールドはグレー表示になり、デフォルト ポートは 443 になります。

（注） インストール中に特定の IP アドレスを指定し、サーバ ホストの IP アドレスを変更した場合は、次の 2 つのファイル（どちらも $INSTALL/conf ディレクトリにあります）を修正する必要があります。server.properties ファイルの **server.bindaddrs** を新しい IP アドレスに変更し、FMServer.conf ファイルの **wrapper.app.parameter.4** を新しい IP アドレスに変更します。

ステップ 17 インストールを中止する場合は、**Cancel** をクリックします。

インストールの進行状況が Cisco Fabric Manager Installer ウィンドウに表示されます（図 2-8 を参照）。

図 2-8　インストールの進行状況



インストールが完了すると、インストール完了メッセージが Cisco Fabric Manager Installer ウィンドウに表示されます（図 2-9 を参照）。

図 2-9　インストール完了メッセージ

（注） Fabric Manager Standalone をインストールした場合は、**Launch Fabric Manager** または **Launch Device Manager** のチェックボックスをオンにすることによって、Fabric Manager または Device Manager の起動を選択できます。Fabric Manager および Device Manager のアイコンがデスクトップに自動的に作成されます。

ステップ 18 **Finish** をクリックすると、Cisco Fabric Manager Installer ウィンドウが閉じます。

Fabric Manager Server をインストールした場合、Fabric Manager Client を起動するまで、Fabric Manager と Device Manager のアイコンはデスクトップに作成されません。「Fabric Manager Client の起動」（p.5-3）の手順に従って、Fabric Manager Client を起動します。

Create shortcuts チェックボックスをオンにした場合は、Windows の［**スタート**］>［**プログラム**］に Cisco MDS 9000 プログラム グループが作成されます。このプログラム グループには、インストール ディレクトリ内のバッチ ファイルへのショートカットが格納されます。Fabric Manager Server、データベース、および Web Server の 3 つのサービスが起動します。Performance Manager サーバがインストールされますが、最初に特定の設定手順を完了する必要があるため、インストール時にはこのサービスは起動しません。

UNIX（Solaris または Linux）マシンでは、インストール ディレクトリ内にシェル スクリプトが作成されます。Windows サービスと同等のプログラムを実行するシェル スクリプトは、FMServer.sh、FMPersist.sh、PMCollector.sh および FMWebClient.sh です。サーバ側のデータおよび Performance Manager データはすべてインストール ディレクトリに格納されます。

Fabric Manager Client は、Fabric Manager Server がないと実行できません。このサーバ コンポーネントは、Fabric Manager をダウンロードしてインストールするときに、同時にダウンロードおよびインストールされます。Windows マシンでは、Fabric Manager Server はサービスとしてインストールされます。このサービスを管理するには、Microsoft Windows のコントロール パネルのサービスを使用します。Fabric Manager Server サービスは、デフォルト設定では、マシンを再起動するときに自動起動されます。この設定を変更するには、サービスのプロパティを変更します。

Device Manager のインストール

Device Manager ソフトウェアの実行ファイルは、スイッチ スーパーバイザ モジュールに存在します。Device Manager ソフトウェアをインストールまたはアップグレードするには、Web ブラウザでスーパーバイザ モジュールにアクセスして、表示される Web ページで **Install** リンクをクリックします。ワークステーションで稼働しているソフトウェアが、最新バージョンの Device Manager であるかどうかが確認されます。最新バージョンでない場合は、最新バージョンがダウンロードされ、ワークステーションにインストールされます。

ワークステーションに Device Manager をインストールする手順は次のとおりです。

ステップ 1　ブラウザの Address フィールドにスイッチの IP アドレスを入力します。

Device Manager の Installation ウィンドウが表示されます（図 2-10 を参照）。

図 2-10　Device Manager の Installation ウィンドウ

ステップ 2　**Cisco Device Manager** リンクをクリックします。

Cisco Device Manager Installer ウィンドウに、管理ソフトウェア セットアップ ウィザードのウェルカム メッセージが表示されます（図 2-11 を参照）。

図 2-11　管理ソフトウェア セットアップ ウィザードのウェルカム メッセージ

ステップ 3　**Next** をクリックするとインストールが開始されます。

ステップ 4　**I accept the terms of the License Agreement** チェックボックスにチェックを入れ、**Next** をクリックします。

ステップ 5　Device Manager のインストール用としてワークステーション上のフォルダを選択します。

- Windows では、デフォルトのロケーションは C:\Program Files\Cisco Systems\MDS 9000 です。
- UNIX（Solaris または Linux）マシンでは、インストール パス名は、インストールを実行するユーザの権限に応じて、/usr/local/cisco_mds9000 または $HOME/cisco_mds9000 になります。

ステップ 6　**Install** をクリックします。

インストールの進行状況が Cisco Device Manager Installer ウィンドウに表示されます（図 2-12 を参照）。

図 2-12　インストールの進行状況

インストールが完了すると、インストール完了メッセージが Cisco Device Manager Installer ウィンドウに表示されます（図 2-13 を参照）。

図 2-13　インストール完了メッセージ

ステップ 7　**Finish** をクリックすると、Cisco Device Manager Installer ウィンドウが閉じます。

管理ソフトウェアのアップグレード

Device Manager が稼働しているスイッチにログインし、そのスイッチの方が Device Manager ソフトウェアのバージョンが高い場合は、上位バージョンをインストールするように要求されます。Device Manager は任意のタイミングでアップグレードすることもできます。その場合は、ブラウザのアドレス フィールドに、上位バージョンのソフトウェアがインストールされたスーパーバイザ モジュールの IP アドレスまたはホスト名を入力します。

（注） インストーラでは、ダウングレードがサポートされていません。Device Manager を旧リリースにダウングレードするには、手動でアンインストールしてから、前のバージョンの Device Manager をインストールする必要があります。

Cisco Fabric Manager ソフトウェアをアップグレードする場合は、「管理ソフトウェアのインストール」（p.2-7）に記載された手順に従ってください。インストーラは、Fabric Manager アプリケーションのソフトウェア アップグレードをサポートしています。

Cisco Fabric Manager とその他の管理ツールとの統合

Fabric Manager、Device Manager、および Performance Manager は次の管理ツールと併用することができます。

- Cisco Traffic Analyzer — VSAN およびプロトコル別にトラフィックを分類して、Logical Unit Number（LUN）レベルで SCSI トラフィックを調査することができます。
- Cisco Protocol Analyzer — ファイバ チャネルおよび Ethereal 用にシスコが開発した SCSI デコーダを使用して、ファイバ チャネル フレームの実際のシーケンスを簡単に調査できます。
- Cisco Port Analyzer Adapter 2 — SPAN（スイッチド ポート アナライザ）トラフィック（ファイバ チャネル制御とデータ プレーン トラフィックの両方）をイーサネット ヘッダーにカプセル化して、分析のために Windows PC またはワークステーションにトランスポートすることができます。Cisco Traffic Analyzer および Cisco Protocol Analyzer では、SPAN トラフィックを Windows PC またはワークステーションにトランスポートするために PAA が必要です。

これらのツールの詳細、および Cisco Fabric Manager 管理アプリケーションとの連携方法については、第 31 章「ファブリックのトラブルシューティング」を参照してください。

ファイアウォールの背後での Fabric Manager の稼働

Fabric Manager、Device Manager、および Performance Manager が稼働している Windows PC がファイアウォールの背後に置かれている場合は、特定のポートが使用可能でなければなりません。

デフォルトでは、Fabric Manager Client および Device Manager は、使用可能な最初の UDP ポートを使用して、SNMP 応答を送受信します。UDP SNMP トラップ ローカル ポートは、Fabric Manager の場合は 1162、Device Manager の場合は 1163 または 1164 です。Fabric Manager Server は TCP RMI ポート 9099 も開きます。

次のステートメントのアンコメントによって、Fabric Manager Client または Device Manager が SNMP 応答に使用する UDP ポートを選択できます。

- Windows デスクトップでは、C:\Program Files\Cisco Systems\MDS9000\bin ディレクトリの FabricManager.bat ファイルまたは DeviceManager.bat ファイル内の次のステートメントをアンコメントします。

  ```
  rem JVMARGS=%JVMARGS% -Dsnmp.localport=9001
  ```

- UNIX デスクトップでは、$HOME/.cisco_mds9000/bin ディレクトリの FabricManager.sh ファイルまたは DeviceManager.sh ファイル内の次のステートメントをアンコメントします。

  ```
  # JVMARGS=$JVMARGS -Dsnmp.localport=9001
  ```

Fabric Manager Server プロキシ サービスは、Fabric Manager Client または Device Manager と Fabric Manager Server の間の SNMP 通信に設定可能な TCP ポート（デフォルトは 9198）を使用します。

Fabric Manager Server コンポーネントの場合は、着信接続用に、ファイアウォール上で予測可能な 2 つの TCP ポートを開く必要があります。

- server.port = 9099
- server.data.port = 9100

これらの 2 つのポートがオープンであるかぎり、Fabric Manager Client はサーバに接続できます。Fabric Manager Client に接続されているその他の TCP ポートは、ファイアウォールの背後にあるサーバによって開始されます。

表 2-2 に、Fabric Manager アプリケーションが使用するすべてのポートを示します。

表 2-2　Fabric Manager のポートの使用

通信タイプ	使用ポート
すべてのアプリケーションが使用するポート	
SSH	ポート 22（TCP）
Telnet	ポート 23（TCP）
HTTP	ポート 80（TCP）
TFTP	ポート 69（UDP）
Syslog	ポート 514（UDP）
Fabric Manager Server および Performance Manager が使用するポート	
SNMP_TRAP	ポート 2162（UDP）
SNMP	SNMP プロキシが使用可能な場合は空いているローカル ポート（UDP）または 9198（TCP）をランダムに選択。ポートは、server.properties で変更可能。
Java RMI	ポート 9099、9100（TCP）
Fabric Manager Client が使用するポート	

表 2-2　Fabric Manager のポートの使用

通信タイプ	使用ポート
SNMP	SNMP プロキシが使用可能な場合は空いているローカル ポート（UDP）をランダムに選択。ポートは、client -Dsnmp.localport オプションで変更可能。
Java RMI	19199 ～ 19399（TCP）の空いているローカル ポートを選択。ポートは、client -Dclient.portStart および -Dclient.portEnd オプションで変更可能。たとえば、-Dclient.portStart = 19199 -Dclient.portEnd = 19399。
Device Manager が使用	
SNMP_TRAP	1163 ～ 1170（UDP）の空いているローカル ポートを選択。
SNMP	SNMP プロキシが使用可能な場合は空いているローカル ポート（UDP）または 9198（TCP）をランダムに選択。ポートは、server.properties で変更可能。

管理ソフトウェアのアンインストール

Windows PC の Fabric Manager アプリケーションをアンインストールする手順は、次のとおりです。

ステップ 1　稼働中の Fabric Manager および Device Manager のインスタンスをすべて閉じます。

ステップ 2　［スタート］>［**プログラム**］>［**Cisco MDS 9000**］>［**Uninstall**］を選択して、uninstall.bat スクリプトを実行します。

コマンドラインからバッチ ファイル（デフォルトでは C:\Program Files\Cisco Systems\MDS 9000 フォルダ内）を直接実行することもできます。

UNIX マシンの Fabric Manager アプリケーションをアンインストールする手順は、次のとおりです。

ステップ 1　Fabric Manager のインストール場所に応じて次のシェル スクリプトを実行します。
$HOME/cisco_mds9000/Uninstall.sh または **/usr/local/cisco_mds9000/uninstall.sh**

（注）　今後のアップグレードのインストールが妨げられる可能性があるため、MDS 9000 フォルダは削除しないでください。

CHAPTER 3

Fabric Manager Server

Fabric Manager Server は高度な SAN モニタリング機能、トラブルシューティング機能、および設定機能のためのプラットフォームです。Fabric Manager Server 機能は Cisco Fabric Manager アプリケーションに統合されています。

この章の内容は、次のとおりです。

- Fabric Manager Server の概要（p.3-2）
- Fabric Manager Server のインストールおよび設定（p.3-3）
- Fabric Manager Server ファブリックの管理（p.3-5）
- Fabric Manager Server プロパティ ファイル（p.3-6）
- Fabric Manager Server の変更（p.3-7）

Fabric Manager Server の概要

Cisco Fabric Manager Server をコンピュータにインストールすると、集中管理サービスおよびパフォーマンス モニタリングが可能になります。SNMP 操作を使用して、ファブリックの情報を効率的に収集できます。サーバ コンポーネントを含む Cisco Fabric Manager ソフトウェアを使用するためには、ワークステーションに約 60 MB のハードディスク スペースが必要です。Cisco Fabric Manager Server は Windows 2000、Windows 2003、Windows XP、Solaris 8.x 以降、および Red Hat Linux で稼働します。

Cisco Fabric Manager Server として設定された各コンピュータは、複数のファイバ チャネル Storage Area Network（SAN; ストレージ エリア ネットワーク）を監視できます。1 台の Cisco Fabric Manager Server に最大 16 台のクライアント（デフォルト）を同時に接続できます。Cisco Fabric Manager Server で監視されないファブリック内のシスコ製スイッチに、Cisco Fabric Manager Client を直接接続することもできます。こうすると、1 台のコンソールから任意のシスコ製スイッチを管理できます。

Cisco Fabric Manager Server には次の機能があります。

- 複数のファブリックの管理 — Fabric Manager Server は同じユーザ インターフェイスで複数の物理ファブリックを監視します。この機能により、冗長ファブリックの管理が容易になります。ライセンスが付与された Fabric Manager Server では、すべての設定済みファブリックに関する最新の検出情報が維持されるため、Fabric Manager Client を開くと、デバイス ステータスおよび相互接続をすぐに使用できます。

（注） ライセンスが付与されていない Cisco Fabric Manager で監視や設定ができるのは、一度に 1 つのファブリックだけです。新規ファブリックに切り替えるには、Open メニューを使用する必要があります。これにより、アプリケーションは元のファブリックの監視を停止し、新規ファブリックを再検出します。

- 継続的なヘルス モニタリング — スイッチの状態が継続的に監視されるため、前回 Fabric Manager Client を開いたあとに発生したすべてのイベントが取り込まれます。
- ユーザ プロファイルのローミング — ライセンスが付与された Fabric Manager Server は、ローミング ユーザ プロファイル機能を使用して、プリファレンスおよびトポロジ マップ レイアウトをサーバに格納します。これにより、ストレージ ネットワークの管理に使用するコンピュータに関係なく、ユーザ インターフェイスの一貫性を保ちます。

（注） Fabric Manager Client および Fabric Manager Server では、同じリリースを使用する必要があります。

Fabric Manager Server のインストールおよび設定

ここでは、Fabric Manager Server のインストールおよび設定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。

- Fabric Manager Server のインストール（p.3-3）
- Fabric Manager Server のライセンスの有無（p.3-4）
- Fabric Manager Web Sever のインストール（p.3-4）
- Performance Manager の収集機能の確認（p.3-4）

Fabric Manager Server のインストール

Fabric Manager をインストールすると、基本バージョンの Fabric Manager Server（ライセンスなし）も一緒にインストールされます。Fabric Manager アイコンをクリックすると、Fabric Manager Server コンポーネントが稼働しているコンピュータの IP アドレスを入力するダイアログが開きます。Fabric Manager Server の IP アドレスを入力するテキスト ボックスが表示されない場合は、**Options** をクリックして、設定オプション リストを展開します。Fabric Manager Server コンポーネントがローカル マシン上で稼働している場合は、このフィールドを **localhost** のままにします。有効なサーバを指定せずに Fabric Manager を実行しようとすると、Fabric Manager Server をローカルで起動するように求めるプロンプトが表示されます。

Windows PC では、Fabric Manager Server はサービスとしてインストールします。このサービスを管理するには、Microsoft Windows の管理ツールのサービスを使用します。Fabric Manager Server サービスは、デフォルト設定では、Windows PC を再起動するときに自動起動されます。この設定を変更するには、サービスのプロパティを変更します。

（注） Fabric Manager Server を実行する前に、ファブリック内の各スイッチ、またはリモート Authentication, Authorization, Accounting（AAA; 認証、認可、アカウンティング）サーバ上に、専用の Fabric Manager 管理ユーザを作成する必要があります。このユーザを使用して、ファブリック トポロジを検出します。「ファブリックの検出」（p.4-4）を参照してください。

Fabric Manager Server をインストールして、初期設定を行う手順は、次のとおりです。

ステップ 1　ワークステーションに Fabric Manager および Fabric Manager Server をインストールします。「Fabric Manager Server のインストール」（p.3-3）を参照してください。

ステップ 2　Fabric Manager にログインします。「Fabric Manager Client の起動」（p.5-3）を参照してください。

ステップ 3　（任意）Performance Manager のフローを作成して、ファブリックを監視します。「フロー統計のカウント」（p.29-5）を参照してください。

ステップ 4　ファブリックを継続的に監視するように、Fabric Manager Server を設定します。「Fabric Manager Server ファブリックの管理」（p.3-5）を参照してください。

ステップ 5　Fabric Manager Server を介して管理するファブリックごとに、ステップ 2 ～ 4 を繰り返します。

ステップ 6　Fabric Manager Web Sever をインストールします。「Fabric Manager Web Sever のインストール」（p.3-4）を参照してください。

ステップ 7　Performance Manager がデータを収集していることを確認します。「Performance Manager の収集機能の確認」（p.3-4）を参照してください。

Fabric Manager Server のライセンスの有無

Fabric Manager をインストールすると、基本バージョンの Fabric Manager Server（ライセンスなし）も一緒にインストールされます。Performance Manager、リモート クライアント サポート、およびファブリックの継続的なモニタリングなどのライセンス機能を取得するには、Fabric Manager Server パッケージを購入して、インストールする必要があります。

ただし、これらのライセンス機能のトライアル バージョンを使用できます。機能のトライアル バージョンをイネーブルにするには、ライセンスを購入した場合と同様に各機能を実行します。この機能が一定期間のみ有効なデモ バージョンであることを示すダイアログボックスが表示されます。

いずれかの Fabric Manager Server 機能を評価していて、その機能の評価期間を終了するには、Device Manager を使用します。

Fabric Manager Web Sever のインストール

Web ブラウザを通じて Performance Manager レポートを表示するには、Fabric Manager Web Server をインストールする必要があります。CD-ROM から Fabric Manager Web Server をインストールする方法については、『*Cisco MDS 9000 Family Fabric Manager Configuration Guide*』を参照してください

Performance Manager の収集機能の確認

Performance Manager の収集機能を 5 分以上実行したあとに、データが収集されたかどうかを確認するには、Fabric Manager で **Performance Manager** > **Reports** を選択します。収集された最初の数個のデータ ポイントが、グラフおよび表形式で表示されます。

（注）　レポートを表示するには、Fabric Manager Web Server をインストールする必要があります。『*Cisco MDS 9000 Family Fabric Manager Configuration Guide*』を参照してください。

Fabric Manager Server ファブリックの管理

Fabric Manager Server ファブリックは、クライアントでそのファブリックが開かれているかどうかにかかわらず、継続的に管理できます。継続的管理の対象であるファブリックは、Fabric Manager Server を起動すると自動的にリロードされ、管理されます。

継続的管理対象のファブリックの選択

Fabric Manager Client を終了すると、そのファブリックを Fabric Manager Server で継続的に管理するかどうかを選択するプロンプトが表示されます。Fabric Manager Client を使用して、管理するファブリックを選択することもできます。

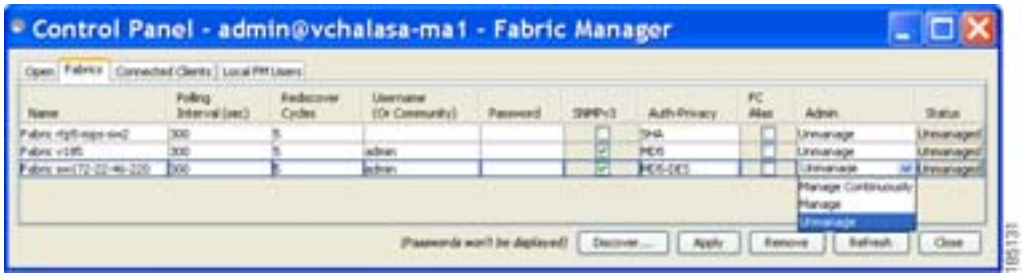
Fabric Manager を使用してファブリックを継続的に管理する手順は、次のとおりです。

ステップ 1　**Server** > **Admin** を選択します。

Control Panel ダイアログボックスの Fabrics タブが開きます（図 3-1 を参照）。

（注）　Fabrics タブにアクセスできるのは、ネットワーク管理者だけです。

図 3-1　Control Panel ダイアログボックスの Fabrics タブ



（注）　ファブリック管理用のユーザ名とパスワードは事前に設定できます。このインスタンスでは、TACACS+ サーバではなく、ローカル スイッチのアカウントを使用する必要があります。

ステップ 2　次のいずれかの Admin オプションを選択します。

- **Manage Continuously** ― Fabric Manager Server が起動すると自動的にこのファブリックが管理対象となり、このオプションが Unmanage に変更されるまで継続して管理されます。
- **Manage** ― このファブリックを表示する Fabric Manager インスタンスがなくなるまで、Fabric Manager Server によって管理されます。
- **Unmanage** ― Fabric Manager Server はこのファブリックの管理を停止します。

ステップ 3　**Apply** をクリックします。

（注）Performance Manager 使用してこれらのファブリックに関するデータを収集する場合は、ここでフローを設定し、データ収集を定義する必要があります。これらの手順については、第 29 章「Performance Manager」を参照してください。

Fabric Manager Server プロパティ ファイル

Fabric Manager Server プロパティ ファイル（MDS 9000\server.properties）には、Fabric Manager Server の機能方法を決定するプロパティ リストが格納されています。このファイルの編集にはテキスト エディタを使用します。プロパティを設定するには、Admin タブにある Fabric Manager Web Services GUI（グラフィカル ユーザ インターフェイス）を使用します。

（注）server.properties ファイルおよび AAA.properties ファイルのパスワードを任意で暗号化できます。

Fabric Manager Server プロパティ ファイルには、次に示す 6 つの一般セクションが含まれています。

- GENERAL — サーバの全般的な設定が格納されます。
- SNMP SPECIFIC — SNMP 要求、応答、およびトラップの各設定が格納されます。
- SNMP PROXY SERVER SPECIFIC — SNMP プロキシ サーバ コンフィギュレーションの設定および TCP ポート指定の設定が格納されます。
- GLOBAL FABRIC — 検出やロードなどのファブリックの設定が格納されます。
- CLIENT SESSION — サーバにログインできる Fabric Manager Client の設定が格納されます。
- EVENTS — Syslog メッセージの設定が格納されます。
- Performance Chart — Performance Manager のチャート生成の終了時間を定義する設定値が格納されます。
- EMC CALL HOME — EMS の指定に基づいて、E メールで XML データとしてトラップを転送するための設定が格納されます。
- EVENT FORWARD SETUP — Cisco Fabric Manager Server が記録したイベントを E メールで転送するための設定が格納されます。

次に、Cisco MDS SAN-OS Release 3.4 の新規、または変更されたサーバ プロパティを示します。

- Display FCoE — ユーザはツリー ノード、メニュー アイテム、ツールバー ボタン、および Fibre Channel over Ethernet（FCoE）に関連するトポロジ ノード / リンクを表示できます。ファブリックに Nexus 5000 シリーズ スイッチが含まれる場合、**displayFCoE** プロパティを true に設定します。

（注）Display FCoE プロパティを設定した場合、Fabric Server の再起動が必要です。

Fabric Manager Server の変更

Fabric Manager では、サーバを停止したり再起動することなく、Fabric Manager Server の一部の設定値を変更できます。このような変更が可能な設定値は、次のとおりです。

- Fabric Manager Server ユーザの追加または削除（p.3-7）
- Fabric Manager Server のユーザ名およびパスワードの変更（p.3-8）
- ポーリング時間とファブリック再検出時間の変更（p.3-8）

Fabric Manager Server ユーザの追加または削除

Fabric Manager Server ユーザの追加や既存ユーザのパスワードの変更は、Fabric Manager を使用して、次の手順を実行します。

ステップ 1　Control Panel ダイアログボックスで、**Local FM Users** タブをクリックします（図 3-1 を参照）。Fabric Manager ユーザのリストが表示されます。

（注）　ユーザを管理できるのは、ネットワーク管理者だけです。

ステップ 2　ユーザを追加する場合は **New** をクリックします。既存のユーザのパスワードを変更する場合は **Edit** をクリックします。

図 3-2 のように、FM User ダイアログボックスが表示されます。

図 3-2　FM User ダイアログボックス

ステップ 3　新規ユーザのユーザ名とパスワードを設定し、**Apply** をクリックします。

Fabric Manager を使用して Fabric Manager Server ユーザを削除する手順は、次のとおりです。

ステップ 1　Control Panel ダイアログボックスで、**Local FM Users** タブをクリックします（図 3-1 を参照）。

Fabric Manager ユーザのリストが表示されます。

ステップ 2　削除するユーザ名をクリックします。

ステップ 3　そのユーザを削除する場合 **Remove** をクリックします。

ステップ 4　削除を確認する場合は **Yes** をクリックし、削除を取り消す場合は **No** をクリックします。

Fabric Manager Server のユーザ名およびパスワードの変更

Fabric Manager Client からファブリックへのアクセスに使用するユーザ名とパスワードは、Fabric Manager Server を再起動せずに変更できます。

Fabric Manager Server で使用されるユーザ名またはパスワードの変更手順は、次のとおりです。

ステップ 1　**Server** > **Admin** を選択します。

Control Panel ダイアログボックスの Fabrics タブが開きます（図 3-1 を参照）。

ステップ 2　Fabric Manager Server で監視する各ファブリックの名前またはパスワードを設定します。

ステップ 3　**Apply** をクリックして、変更を保存します。

ポーリング時間とファブリック再検出時間の変更

Fabric Manager Server は、定期的に監視対象のファブリックをポーリングし、一定間隔で（デフォルトは 5 サイクル）フル ファブリックを再検出します。これらの設定値は、Fabric Manager Server を再起動せずに、Fabric Manager Client から変更できます。

Fabric Manager を使用して、Fabric Manager Server が使用するポーリング時間、またはフル ファブリック再検出の設定を変更する手順は次のとおりです。

ステップ 1　**Server** > **Admin** を選択します。

Control Panel ダイアログボックスの Fabrics タブが開きます（図 3-1 を参照）。

ステップ 2　Fabric Manager Server で監視する各ファブリックに対して、Polling Interval を設定し、Fabric Manager Server がそのファブリックの要素をポーリングし、そのステータスと統計情報を取得する頻度を指定します。

ステップ 3　Fabric Manager Server で監視する各ファブリックに対して、Rediscover Cycles を設定し、Fabric Manager Server がフル ファブリックを再検出する頻度を指定します。

ステップ 4　**Apply** をクリックして、変更を保存します。

デバイス エイリアスまたは FC エイリアスの使用

Fabric Manager で FC エイリアスとグローバル デバイス エイリアスのどちらを使用するかを、Fabric Manager Server を再起動せずに Fabric Manager Client から変更できます。

Fabric Manager を使用して、Fabric Manager が FC エイリアスまたはグローバル デバイス エイリアスを使用するように変更する手順は、次のとおりです。

ステップ 1　**Server** > **Admin** を選択します。

Control Panel ダイアログボックスの Fabrics タブが開きます（図 3-1 を参照）。

ステップ 2　グローバル デバイス エイリアスを使用する場合は Fabric Manager Server で監視する各ファブリックに対して、**Device Alias** チェックボックスをオンにし、FC エイリアスを使用する場合はオフにします。

ステップ 3　**Apply** をクリックして、変更を保存します。

スイッチへのデバイス エイリアスの保存

Fabric Manager Server でグローバル デバイス エイリアスを使用する場合、これらの変更はローカル スイッチには反映されません。スイッチにデバイス エイリアスを保存するまで、そのスイッチは FC エイリアスを使用します。

Fabric Manager を使用してスイッチにグローバル デバイス エイリアスを保存する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches** > **End Devices** を展開し、**Hosts** または **Storage** を選択します。

Information ペインにエンド デバイスが表示されます。

ステップ 2　スイッチに認識させたい各デバイス エイリアスを強調表示にして、デバイスの **Device Alias** アイコンを右クリックし、**Save Selected Device Aliases** を選択します。

CHAPTER 4

Fabric Manager の認証

Fabric Manager には、ファブリック内のスイッチと通信する相互依存ソフトウェア コンポーネントが含まれています。これらのコンポーネントはさまざまな方法を使用して、ほかのコンポーネントおよびスイッチに対する認証を行います。この章では、これらの認証ステップ、ファブリックおよびコンポーネントの推奨される認証設定について説明します。

この章の内容は、次のとおりです。

- Fabric Manager 認証の概要（p.4-2）
- ファブリックの検出（p.4-4）
- Performance Manager の認証（p.4-5）
- Fabric Manager Web Server の認証（p.4-7）

Fabric Manager 認証の概要

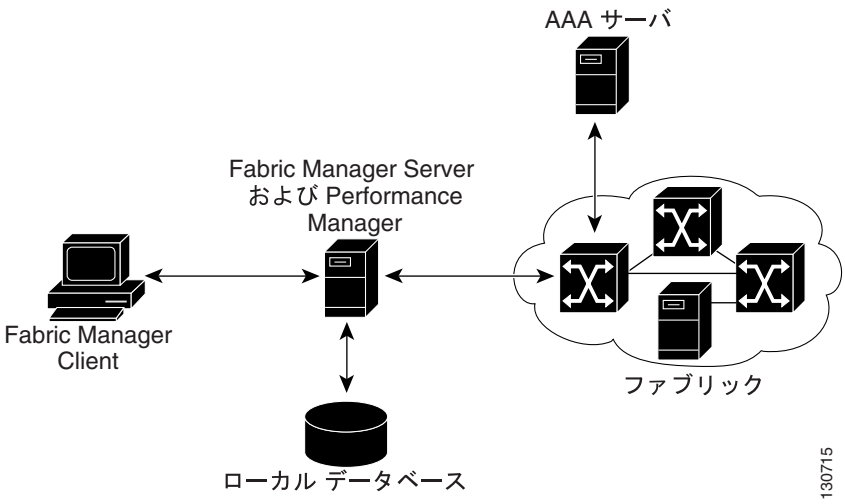
Fabric Manager には、ファブリックを管理するために相互作用する複数のコンポーネントが含まれています。

この章の内容は、次のとおりです。

- Fabric Manager Client
- Fabric Manager Server
- Performance Manager
- Cisco SAN スイッチおよびストレージ デバイスが内部接続されたファブリック
- AAA サーバ（オプション）

図 4-1 に、これらのコンポーネントの構成例を示します。

図 4-1　Fabric Manager の認証例



管理者は Fabric Manager Client を起動して、ファブリックの検出に使用されるシード スイッチを選択します。使用するユーザ名およびパスワードが Fabric Manager Server に渡され、シード スイッチの認証アクセスに使用されます。このユーザ名およびパスワードが、認識された SNMP（簡易ネットワーク管理プロトコル）ユーザ名およびパスワードと異なる場合、Fabric Manager Client か Fabric Manager Server が、スイッチに対する CLI（コマンドライン インターフェイス）セッションを開き（Secure Shell［SSH; セキュア シェル］または Telnet）、ユーザ名およびパスワードのペアを再試行します。ローカル スイッチ認証データベースまたはリモート Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバで、スイッチがユーザ名とパスワードを認識した場合、スイッチは Fabric Manager Client および Server で使用される一時的な SNMP ユーザ名を作成します。

（注） リモート AAA サーバ認証を使用して Fabric Manager または Device Manager を認証する場合は、認証が遅くなることがあります。

（注）CLI セッションが、Fabric Manager Client と Fabric Manager Server 間のファイアウォールを経由できるようにする必要があります。「ファイアウォールの背後での Fabric Manager の稼働」（p.2-22）を参照してください。

（注）SNMPv3 ユーザ名認証のパスワードとプライバシ パスワード、および CLI ユーザ名とパスワードの照合には、同じパスワードを使用することを推奨します。

ファブリックの検出

Fabric Manager Server は同じユーザ インターフェイスで複数の物理ファブリックを監視します。この機能により、冗長ファブリックの管理が容易になります。ライセンスが付与された Fabric Manager Server では、すべての設定済みファブリックに関する最新の検出情報が維持されるため、Fabric Manager Client を起動すると、デバイス ステータスおよび相互接続をすぐに使用できます。

注意　Fabric Manager Server の CPU 利用率が 50 パーセントを超える場合は、より高クラスの CPU システムに交換することを推奨します。詳細および推奨ハードウェアについては、「インストールを開始する前に」（p.2-7）を参照してください。

ネットワークの検出および Performance Manager の設定は、次の項目で説明する方法で行うことを推奨します。この手順に従えば、Fabric Manager Server はファブリックを詳細に表示できます。以降の Fabric Manager Client セッションでは、クライアントのログイン権限に基づいてこの詳細ビューをフィルタリングできます。たとえば、ファブリック内に複数の VSAN（仮想 SAN）があり、これらの VSAN のサブセットに制限されているユーザが作成されています。Fabric Manager Server でファブリック内のすべての VSAN を表示するために、ネットワーク管理者ロール、またはネットワーク オペレータ ロールを使用して Fabric Manager Server でファブリック検出を開始するとします。VSAN 制限のあるユーザが Fabric Manager Client を起動すると、管理が許可されている VSAN だけが表示されます。

（注）　Fabric Manager Server は、常にローカル スイッチ アカウントを使用してファブリックを監視します。AAA（RADIUS または TACACS+）サーバは使用しません。ファブリック サービスのプロビジョニングを目的としたクライアントへのログインには AAA ユーザ アカウントを使用できます。Fabric Manager Server ファブリックのモニタリングに関する詳細は、「Fabric Manager Server ファブリックの管理」（p.3-5）を参照してください。

ファブリック検出の設定

Fabric Manager Server がファブリック全体を検出するように設定する手順は、次のとおりです。

ステップ 1　ネットワーク管理者ロールまたはネットワーク オペレータ ロールを使用して、ファブリックのスイッチごとに専用の Fabric Manager 管理ユーザ名を作成します。

または AAA サーバ内に専用の Fabric Manager 管理ユーザ名を作成し、この AAA サーバを使用して認証するように、ファブリック内のすべてのスイッチを設定します。

ステップ 2　この Fabric Manager 管理ユーザ名に使用されるロール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、このロールにすべての VSAN へのアクセス権が含まれていることを確認します。

ステップ 3　Fabric Manager 管理ユーザを使用して、Fabric Manager Client を起動します。

この手順により、すべての VSAN がファブリック検出の対象になります。

ステップ 4　ファブリックを継続的に監視するように、Fabric Manager Server を設定します。

「Fabric Manager Server ファブリックの管理」（p.3-5）を参照してください。

ステップ 5　Fabric Manager Server を介して管理するファブリックごとに、ステップ 4 を繰り返します。

Performance Manager の認証

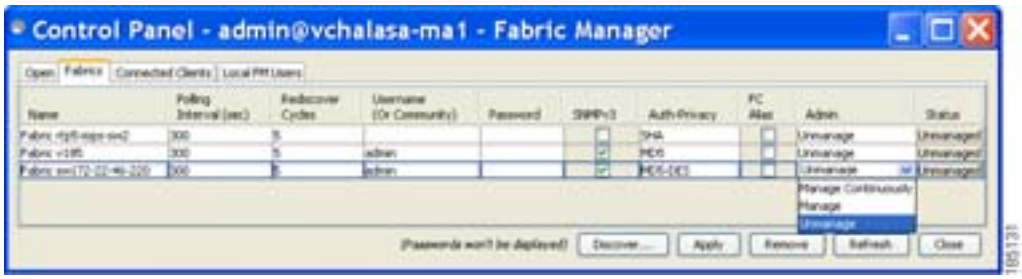
Performance Manager は Fabric Manager Server データベースに格納されたユーザ名およびパスワード情報を使用します。Performance Manager の動作中にファブリック内のスイッチでこの情報が変更された場合は、Fabric Manager Server データベースを更新して、Performance Manager を再起動する必要があります。Fabric Manager Server データベースを更新するには、Fabric Manager Server からファブリックを削除して、ファブリックを再検出する必要があります。

Performance Manager で使用されるユーザ名およびパスワード情報を更新する手順は、次のとおりです。

ステップ 1　Fabric Manager で **Server** > **Admin** をクリックします。

Control Panel ダイアログボックスの Fabrics タブが開きます（図 4-2 を参照）。

図 4-2　Control Panel ダイアログボックスの Fabrics タブ



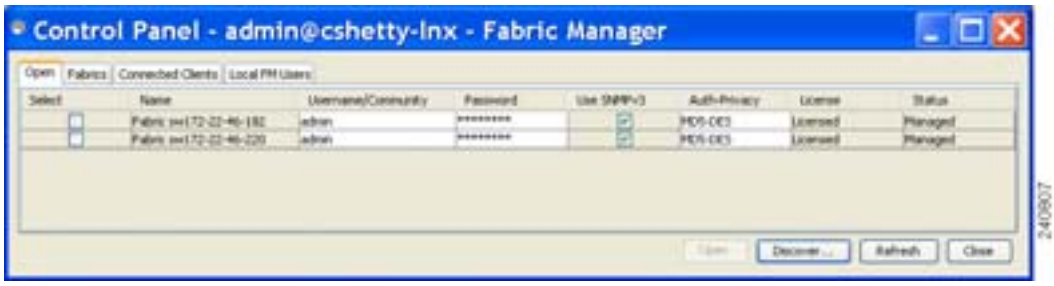
ステップ 2　ユーザ名およびパスワード情報を更新したファブリックをクリックします。

ステップ 3　**Remove** をクリックして、Fabric Manager Server からこれらのファブリックを削除します。

ステップ 4　**File** > **Open Fabric** を選択します。

Control Panel ダイアログボックスは 図 4-3 のように表示されます。

図 4-3　Control Panel ダイアログボックス



ステップ 5　ファブリックを再検出するための適切なユーザ名とパスワードを入力し、Select カラムで開きたいファブリックの隣のチェックボックスにチェックを入れます。

ステップ 6　**Open** をクリックして、ファブリックを再検出します。

Fabric Manager Server がユーザ名およびパスワードの情報を更新します。

ステップ 7　再検出する必要があるファブリックごとに、ステップ 4 ～ 6 を繰り返します。

ステップ 8　**Performance** > **Collector** > **Restart** を選択して、Performance Manager を再起動し、新しいユーザ名およびパスワードを使用します。

Fabric Manager Web Server の認証

Fabric Manager Web Server は、ファブリック内のスイッチと直接通信しません。Fabric Manager Web Server は、ローカルに格納される、あるいは AAA サーバにリモートに格納される、独自のユーザ名およびパスワードの組み合わせを使用します。

Fabric Manager Web Server でのユーザ認証には、RADIUS または TACACS+ サーバを使用することを推奨します。

RADIUS 認証を使用するように Fabric Manager Web Server を設定する手順は、次のとおりです。

ステップ 1　Fabric Manager Web Server を起動します。

ステップ 2　**Admin** タブ > **Web Users** を選択して、Fabric Manager Web Server で使用される認証を更新します。

ステップ 3　**AAA** をクリックします。

ステップ 4　認証モード属性を **radius** に設定します。

ステップ 5　最大 3 つの RADIUS サーバの RADIUS サーバ名、共有秘密、認証方法、使用ポートを設定します。

ステップ 6　**Modify** をクリックして、この情報を保存します。

TACACS+ 認証を使用するように Fabric Manager Web Server を設定する手順は、次のとおりです。

ステップ 1　Fabric Manager Web Server を起動します。

ステップ 2　**Admin** > **Web Users** を選択して、Fabric Manager Web Server で使用される認証を更新します。

ステップ 3　**AAA** をクリックします。

ステップ 4　authenticationmode 属性を **tacacs** に設定します。

ステップ 5　最大 3 つの TACACS+ サーバの TACACS+ サーバ名、共有秘密、認証方法、使用ポートを設定します。

ステップ 6　**Modify** をクリックして、この情報を保存します。

CHAPTER 5

Fabric Manager Client

Cisco Fabric Manager Client は、リモート ワークステーションから Fabric Manager アプリケーションへのアクセスを可能にする、Java ベースの GUI（グラフィカル ユーザ インターフェイス）アプリケーションです。

この章の内容は、次のとおりです。

- Fabric Manager Client の概要（p.5-2）
- Fabric Manager Client の起動（p.5-3）
- Fabric Manager Client の概観（p.5-8）
- Fabric Manager のプリファレンスの設定（p.5-21）
- ネットワーク ファブリック検出（p.5-22）
- デバイス グループの変更（p.5-23）
- ユーザおよびロールによる管理者アクセスの制御（p.5-25）
- Fabric Manager ウィザードの使用（p.5-25）
- Fabric Manager のトラブルシューティング ツール（p.5-26）

Fabric Manager Client の概要

Cisco Fabric Manager は Java および SNMP（簡易ネットワーク管理プロトコル）ベースのネットワーク ファブリックおよびデバイス管理ツールです。GUI を通じて、シスコやサードパーティ製スイッチ、ホスト、およびストレージ デバイスを含むネットワーク ファブリックをリアルタイムで表示できます。

Fabric Manager Client には、シスコ スイッチの完全な設定機能およびステータス モニタリング機能のほかに、ファイバ チャネル トラブルシューティング ツールもあります。これらのヘルス分析ツールおよび設定分析ツールには、ファイバ チャネル ping および traceroute など、シスコ スイッチの機能が使用されています。

（注） Fabric Manager Client と Fabric Manager Server は、同じリリースを使用する必要があります。

Fabric Manager の拡張モード

拡張モードはデフォルトでイネーブルであり、Fabric Manager 機能の完全なスイートを提供します。ユーザ インターフェイスを簡略化するには、Fabric Manager Client の右上にある **Advanced** チェックボックスをオフにします。このモードでは、VSAN（仮想 SAN）、ゾーン分割、インターフェイス設定など、基本的なスイッチ機能にアクセスできます。

Fabric Manager Client の起動

（注） ネットワーク管理者は、最初に Fabric Manager Web Server を使用し、次に示す手順で Fabric Manager Client を起動する必要があります。管理者がユーザのデスクトップに Fabric Manager Client のアイコンをインストールすれば、ユーザはそのアイコンをダブルクリックして Fabric Manager Client を起動できるようになります。

Fabric Manager Client の起動手順は、次のとおりです。

ステップ 1　ブラウザを開き、Fabric Manager Server をインストールした IP アドレスを入力するか、または、ローカル ワークステーションに Fabric Manager Server をインストールした場合は、ローカル ホストを入力します。

図 5-1 のように、Fabric Manager Web Server Login ダイアログボックスが表示されます。

図 5-1　Fabric Manager Web Server のログイン ダイアログボックス

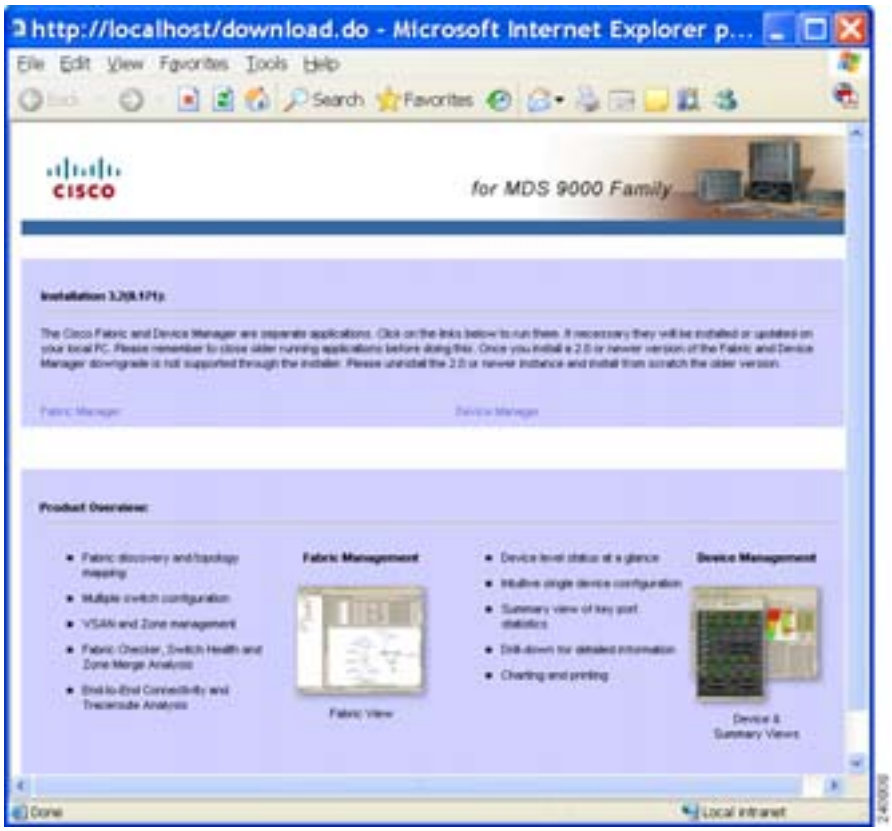
ステップ 2　ユーザ名およびパスワードを入力し、**Login** をクリックします。

Fabric Manager Web Server Summary ページが表示されます。

ステップ 3　このページの右上にある **Download** リンクをクリックします。

Fabric Manager および Device Manager の Download ページが表示されます（図 5-2 を参照）。

図 5-2　Fabric Manager および Device Manager のダウンロード ページ



ステップ 4　**Fabric Manager** と **Device Manager** のいずれかのリンクをクリックします。

Fabric Manager Client 初回起動時には、Fabric Manager のショートカットを作成するかどうかを問うメッセージが表示されます（図 5-3 を参照）。

図 5-3　Fabric Manager のショートカット作成メッセージ

ステップ 5　Fabric Manager のショートカットを作成する場合は、**Yes** をクリックします。

（注）　このメッセージが表示されるのは、Fabric Manager Client の初回起動時だけです。

ステップ 6　ソフトウェアがインストールされ、デスクトップにアイコンが作成されたら、Fabric Manager アイコンをダブルクリックして、Fabric Manager を起動します。

図 5-4 に示すように、Fabric Manager Login ダイアログボックスが表示されます。

図 5-4　Fabric Manager のログイン ダイアログボックス

ステップ 7　Fabric Manager Server のユーザ名とパスワードを入力します。

ステップ 8　Fabric Manager Client が TCP ベース プロキシ サーバを介して Fabric Manager Server と通信するように設定する場合は、**Use SNMP Proxy** チェックボックスをオンにします。

ステップ 9　**Login** をクリックします。Fabric Manager Server に正しくログインしたら、シード スイッチを設定してアクセス権があるファブリックを開きます。

（注）　Fabric Manager Client の初回起動時、または使用可能なファブリックがない場合には、Discover New Fabric ダイアログボックスが表示されます。

図 5-5 に示すように、Discover New Fabric ダイアログボックスが表示されます。

図 5-5　Discover New Fabric ダイアログボックス

（注） 新しいファブリックを検出できるのは、ネットワーク管理者だけです。

ステップ 10 ファブリック シード スイッチを、Fabric Manager を使用するシスコ スイッチに設定します。

（注） NPV モードで稼働しているシスコ スイッチを、ファブリック シード スイッチにはできません。

ステップ 11 スイッチのユーザ名とパスワードを入力します。

ステップ 12 スイッチに設定したプライバシ プロトコルに応じて、Auth-Privacy オプションを選択します。

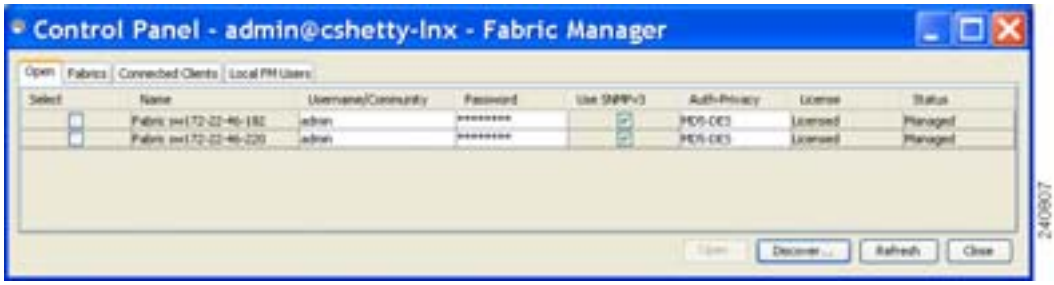
- スイッチにまだプライバシ プロトコルを設定していない場合は、MD 5（プライバシなし）の Auth-Privacy オプションを選択します。
- スイッチにプライバシ プロトコルを設定している場合は、設定に適した Auth-Privacy オプションを選択してください。

（注） クリーン検出を実行する場合は、ファブリックを削除してから再検出します。

ステップ 13 **Discover** をクリックします。

図 5-6 のように、Control Panel ダイアログボックスが表示されます。

図 5-6　Control Panel ダイアログボックス



（注） サーバとクライアントが同じワークステーションで稼働していて、データベース内にライセンスのないファブリックがあると、ダイアログボックスにメッセージが表示されます。管理対象外のファブリック（ライセンスの状態は unknown）がある場合もメッセージが表示されます。

ステップ 14 Select カラムで、開きたいファブリックの隣のチェックボックスをオンにするか、**Discover** をクリックして、新しいファブリックを追加します。

（注） ファブリックを継続管理または非管理にできるのはネットワーク管理者だけです。詳細については、「継続的管理対象のファブリックの選択」（p.3-5）を参照してください。

ステップ 15 **Open** をクリックして、選択したファブリックを開きます。

（注） ファブリックの表示が不完全な場合は、VSAN 制限のないユーザとしてファブリックを再検出します。

稼働中の Fabric Manager インスタンスから Fabric Manager Client を起動する手順は、次のとおりです。

ステップ 1 **File** > **Open Fabric** を選択するか、または Fabric Manager ツールバーの **Open Switch Fabric** アイコンをクリックします。

Control Panel ダイアログボックスは、図 5-6 のように表示されます。

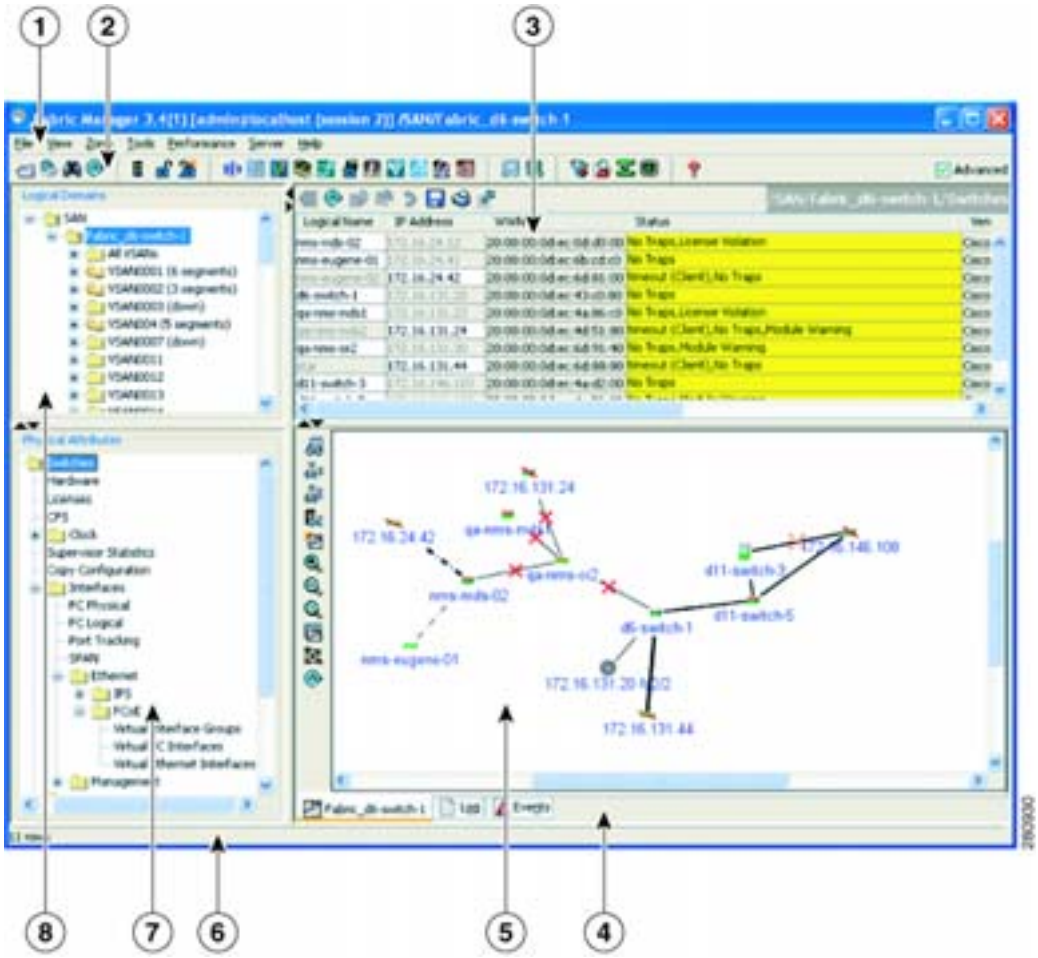
ステップ 2 Select カラムで、開きたいファブリックの隣のチェックボックスをオンにして、**Open** をクリックします。

（注） Fabric Manager を使用して行われた変更は、管理対象スイッチの実行コンフィギュレーションに適用されます。コンフィギュレーションの変更や、ゾーンのアクティブ化などの操作を行うと、終了する前に変更を保存するように求めるプロンプトが表示されます。

Fabric Manager Client の概観

ここでは、Fabric Manager Client のインターフェイスについて説明します（図 5-7 を参照）。

図 5-7　Fabric Manager のメイン ウィンドウ



1	メニューバー — メニュー別に編成されたオプションにアクセスできます。
2	ツールバー — File、Tools、および Help メニュー内で最も一般的に使用されるオプションに直接アクセスするためのアイコンが配置されています。
3	Information ペイン — メニュー ツリーで選択されたオプションに関する情報が表示されます。
4	ステータス バー（右側）— 検出プロセスで表示された最後のエントリ、および有効なエラーメッセージが表示されます。
5	Fabric ペイン — スイッチ、ホスト、ストレージなどのネットワーク ファブリックのマップが表示されます。また、ログおよびイベント データを表示するためのタブも配置されています。
6	ステータス バー（左側）— テーブルに表示される行数などの一時的なメッセージが短期間表示されます。
7	Logical Domains ペイン — 設定済みの SAN、ファブリック、VSAN およびゾーンが表示され、ユーザ定義グループにアクセスできます。
8	Physical Attributes ペイン — 上記で選択されたファブリック、VSAN、またはゾーンに応じて、使用可能な設定作業がツリー表示されます。論理的に選択されたスイッチおよびエンド デバイスが一覧表示されます。

（注）各ペインのサイズを変更するには、各領域の境界をドラッグするか、**Minimize**（最小化）または **Maximize**（最大化）コントロールをクリックします。

メニューバー

Fabric Manager メイン ウィンドウの上部にあるメニューバーには、現在のファブリックの管理やトラブルシューティング、および Fabric ペインに表示される情報の制御を行うためのオプションが配置されています。メニューバーには、次のメニューがあります。

- File — 新しいファブリックのオープン、現在のファブリックの再検出、スイッチの位置の特定、プリファレンスの設定、マップの印刷、Fabric ペイン ログの消去（ログの右クリック）やエクスポートを行います。
- View — マップの外観を変更します（Fabric ペイン ツールバーにもこれらのオプションと同じ機能が配置されています）。
- Zone — ゾーン、ゾーン セット、および Inter-VSAN Routing（IVR）を管理します。
- Tools — 接続や設定の確認およびトラブルシューティングを行います（「Fabric Manager のトラブルシューティング ツール」[p.5-26] を参照）。
- Performance — Performance Manager および Cisco Traffic Analyzer を実行および設定し、レポートを生成します。
- Server — クライアントおよびファブリックの管理作業を実行します。Fabric Manager Server の管理コマンドや **purge** コマンドが用意されています。管理対象スイッチが表示されます。
- Help — Information ペインに、特定のダイアログボックスに関するオンライン ヘルプ トピックが表示されます。

ツールバー

Fabric Manager のメイン ツールバーには、最も一般的に使用されるメニューバー オプションにアクセスするためのアイコンが配置されています（表 5-1 を参照）。

表 5-1　Fabric Manager Client のメイン ツールバー

アイコン	説明
	スイッチ ファブリックを開きます。
	現在のファブリックを再検出します。
	マップを検索します。
	VSAN を作成します。
	DPVM ウィザードを起動します。
	フル ゾーン データベースを編集します。
	IVR ゾーン ウィザードを起動します。
	SAN ポート チャネル ウィザードを起動します。
	Virtual Interface Group（VIG）ウィザードを起動します。
	Virtual Interface（VI）ウィザードを起動します。
	FCIP ウィザードを起動します。
	iSCSI ウィザードを起動します。
	QoS ウィザードを起動します。
	ユーザおよびロールを設定します。

表 5-1　Fabric Manager Client のメイン ツールバー（続き）

アイコン	説明
	IP-ACL ウィザードを起動します。
	License Install ウィザードを起動します。
	Software Install ウィザードを起動します。
	スイッチ ヘルス分析を実行します。
	ファブリック設定分析を実行します。
	エンドツーエンド接続分析を実行します。
	ISL パフォーマンスを監視します。Information ペインに、ファブリック内のすべてのインターフェイスのリアルタイム ISL パフォーマンス情報が表示されます。
	オンライン ヘルプが表示されます。

Logical Domains ペイン

Logical Domains ペインでは、ファブリック、VSAN、およびゾーンの属性を管理したり、ユーザ定義グループにアクセスしたりできます。ツリー内のいずれかのフォルダを右クリックして、ポップアップ メニューのメニュー項目をクリックします。該当する設定ダイアログボックスが表示されます。

ファブリックのデフォルト名は、VSAN 1 内の主要スイッチの名前、IP アドレス、または World Wide Name（WWN）です。VSAN 1 が分割されている場合は、最も小さな WWN を持つ主要スイッチのデフォルト名が選択されます。表示されるファブリック名の順序は、次のようになります。

- Fabric <sysName>
- Fabric <ipAddress>
- Fabric <sWWN>

Fabric Manager でファブリック名を変更する手順は、次のとおりです。

ステップ 1　**Server** > **Admin** を選択します。

Control Panel ダイアログボックスが表示されます。

ステップ 2　ファブリックの名前をダブルクリックし、そのファブリックの新しい名前を入力します。

ステップ 3　**Apply** をクリックすると、名前が変更されます。

フィルタリング

Fabric Manager には、目的のデータのみを表示するためのフィルタリング メカニズムがあります。フィルタリングを実行するには、最初に Logical Domains ペインでファブリックおよび VSAN を選択します。これにより、Fabric ペインの表示範囲が絞られます。選択した項目に属さない情報はすべて薄く表示されます。選択した項目に属さない情報は、Information ペインの表にも表示されません。選択したフィルタは Fabric Manager ウィンドウの右上に表示されます（図 5-8 を参照）。

さらに範囲を絞り込むには、Physical Attributes で属性を選択します。選択内容に応じて、Fabric Manager のテーブル、表示、およびフィルタ基準が変更されます。

Physical Attributes ペイン

現在選択されているファブリック、VSAN、またはゾーン内のスイッチの管理に使用できるオプションをツリー表示するには、Physical Attributes ペインを使用します。

オプションを選択するには、フォルダをクリックして使用可能なオプションを表示し、オプションをクリックします。Information ペインに、選択したオプションに関する情報が表形式で表示されます。Physical Attributes ペインには次のメイン フォルダが配置されています。

- Switches — ハードウェア、システム、ライセンス、およびコンフィギュレーション ファイルの表示および設定を行います。
- Interfaces — 物理ファイバ チャネル、仮想ファイバ チャネル、イーサネット、SVC、および SAN ポート チャネル インターフェイスの表示および設定を行います。
- Fibre Channel Services — ファイバ チャネル ネットワーク設定の表示および設定を行います。

- Events — イベント、アラーム、しきい値、通知、およびインフォームの表示および設定を行います。
- Security — スイッチ管理および FC-SP セキュリティの表示および設定を行います。
- End Devices — エンド デバイスの表示および設定を行います。

Information ペイン

Information ペインには、Logical Domains ペインまたは Physical Attributes ペインのメニュー ツリーで選択されたオプションに対応する情報テーブルが表示されます。Information ペインのツールバーには、表 5-2 に示された処理を 1 つまたは複数実行するためのボタンが配置されています。

表 5-2　Information ペインのツールバー

アイコン		説明
	Apply Changes	コンフィギュレーションの変更を適用します。
	Refresh Values	テーブルの値を更新します。
	Create Row	テーブル内に新しい行を作成するためのダイアログボックスを開きます。
	Delete Row	現在強調表示されている行をテーブルから削除します。
	Copy/Ctrl+C	行のデータを他の行にコピーします。
	Paste/Ctrl +V	行のデータを他の行に貼り付けます。
	Undo Changes/Ctrl-Z	直前の変更を元に戻します。
	Export	情報をファイルにエクスポートし、保存します。
	Print Table	Information ペインの内容を出力します。
	Detach Table	Information ペイン内のテーブルの編集不可能なコピーを作成し、画面上で移動可能な独自のウィンドウに表示します。

(注) 変更を加えた場合はコンフィギュレーションを保存する必要があります。保存しないとデバイスの再起動後に変更が失われます。

（注）ツールバーに配置されるボタンは、選択したオプションによって変わります。Information ペインで選択されたフィールドなどのオブジェクトに応じて、ボタンがアクティブまたは非アクティブ（薄い表示）になります。

分離可能なテーブル

Fabric Manager 内の分離可能なテーブルを使用することにより、テーブルを分離し、デスクトップ上の別のエリアに移動して、各 VSAN の類似テーブルを比較することができます。あるビューで情報テーブルを開いたまま、Fabric Manager 内の別のエリアを調べることができます。テーブルを分離するには、Fabric Manager の Information ペインで **Detach Table** アイコンをクリックします。

Fabric ペイン

Fabric ペインにはファブリックがグラフィック表示されます。表 5-3 に、ファブリック内のデバイスに応じて表示されるグラフィックの説明を示します。

表 5-3　Fabric Manager のグラフィック

アイコンまたはグラフィック	説明
	ディレクタ クラスの Cisco MDS 9000
	ディレクタ クラス以外のスイッチ
	一般的なファイバ チャネル スイッチ
	Cisco SN5428
	Cisco Nexus 5000 シリーズ スイッチ
	デバイス内にオレンジの直線が引かれている場合、このデバイスは管理できますが、動作時に問題が発生します。
	デバイスまたはリンク内にオレンジの「X」が示されている場合、そのデバイスまたは ISL は正常に動作していません。
	デバイス内にレッドの直線が引かれている場合は、このデバイスを管理できません。
	デバイスまたはリンク内にレッドの「X」が示されている場合は、デバイスがダウンしているか、または ISL がダウンしています。

表 5-3　Fabric Manager のグラフィック（続き）

アイコンまたはグラフィック	説明
	ファイバ チャネル HBA（またはラック）
	ファイバ チャネル ターゲット（またはラック）
	iSCSI ホスト
	ファイバ チャネル ISL およびエッジ接続
	ファイバ チャネル SAN ポート チャネル
	Fibre Channel over Ethernet（FCoE）接続
	IP ISL およびエッジ接続
	IP ポート チャネル
	NPV 接続
	ファイバ チャネル ループ（ストレージ）
	IP クラウド（ホスト）。このアイコンは、Fabric Manager の Fabric ペインに SAN（複数のファブリック）を表示する場合に、ファブリックを表現するために使用します。
	ボックスで囲まれているデバイス、クラウド、またはループには、非表示リンクが接続されています。

スイッチまたはディレクタがグレー表示されている場合、Fabric Manager はこれらと通信できません。

Fabric ペインの下部には、次のタブがあります。

- Fabric — 複数のファブリックを表示した場合は、ファブリックごとに独自のタブが表示されます。各タブをクリックして、ファブリックを切り替えることができます。
- Log — ファブリック検出などの Fabric Manager の動作について説明するメッセージを表示します。
- Events — 管理ステーションで受信された SNMP トラップに関する情報を表示します。検出されたイベントと、ライセンス、SNMP などの重要なトラップが組み合わされて表示されます。

次の手順を実行すると、Fabric ペインに大きいファブリックが見やすく表示されます。

- エンド デバイス ラベルをオフにします。
- ループを折りたたみます。
- 展開された複数のリンクを折りたたみます（折りたたまれた複数のリンクは、太い一重線で表示されます）。
- VSAN でファブリックの一部を薄い表示にするか非表示にします。

（注）VSAN ツリーで VSAN、ゾーン、またはゾーン メンバーを選択すると、マップの強調表示機能が変更され、選択されたオブジェクトが識別されます。強調表示を解除するには、Fabric ペイン ツールバーの **Clear Highlight** ボタンをクリックするか、またはポップアップ メニューで **Clear Highlight** を選択します。

コンテキスト メニュー

Fabric ペインのアイコンを右クリックすると、ポップアップ メニューが開き、選択されたアイコンのタイプに応じて異なるオプションが表示されます。オブジェクトに応じて、次の機能を持つオプションが表示されます。

- 選択されたスイッチに対して Device Manager のインスタンスを開きます。
- 選択されたスイッチの CLI（コマンドライン インターフェイス）セッションを開きます。
- 選択されたオブジェクトの表示名をコピーします。
- デバイスに **ping** または **traceroute** コマンドを実行します。
- エンド デバイスを表示または非表示にします。
- 属性を表示します。
- SAN ポート チャネルのメンバーを停止して、ディセーブルにします。
- ISL のトランキング モードを設定します。
- 選択された ISL に SAN ポート チャネルを作成または追加します。

Fabric ペインには、マップの外観を保存、出力、および変更するためのオプションが配置されたツールバーがあります。マップを右クリックすると、ポップアップ メニューが開き、マップの外観を変更するためのオプション（ツールバーと同じ機能）が表示されます。

（注）Fabric ペインから Web ベース アプリケーションまたは Web ベースでないアプリケーションを起動できます。これを実行するには、ストレージ ポートまたはラックに IP アドレスを割り当てます。次に、右クリックしてポップアップ メニューを開き、**Device Manager** を選択します。

マップの保存

Fabric ペインのマップは、イメージとして、または編集可能な Visio 図として保存できます。また、リンク ラベル付きで保存することも、リンク ラベルなしで保存することも可能です。作成された Visio 図は編集が可能で、次の 2 つのレイヤに保存できます。

- デフォルト レイヤには、ファブリック内のすべてのスイッチおよびリンクが含まれます。
- エンド デバイス レイヤには、エンド デバイスが含まれ、これをオフにすることにより、Visio 図からエンド デバイスを削除できます。

Visio 図としてマップを保存するには、**Files > Export > Visio** を選択し、**Map** または **Map with link labels** を選択します。保存された Visio 図には、Fabric ペインで選択した表示オプションが保持されます。たとえば、マップ内の複数のリンクを折りたたんで、そのリンクを Visio 図としてエクスポートすると、その Visio 図にはこれらの複数のリンクが 1 つの太いリンクとして表示されます。

Tools メニューの Show Tech Support オプションでも、マップを Visio 図として保存できます。

要素の消去

Fabric ペインでは、**Refresh Map** アイコンをクリックすることによって、いつでもマップをリフレッシュできます。**Refresh Map** アイコンを使用すると、マップは再描画されますが、停止している要素は消去されません。要素を消去するには、次のいずれかの操作を実行します。

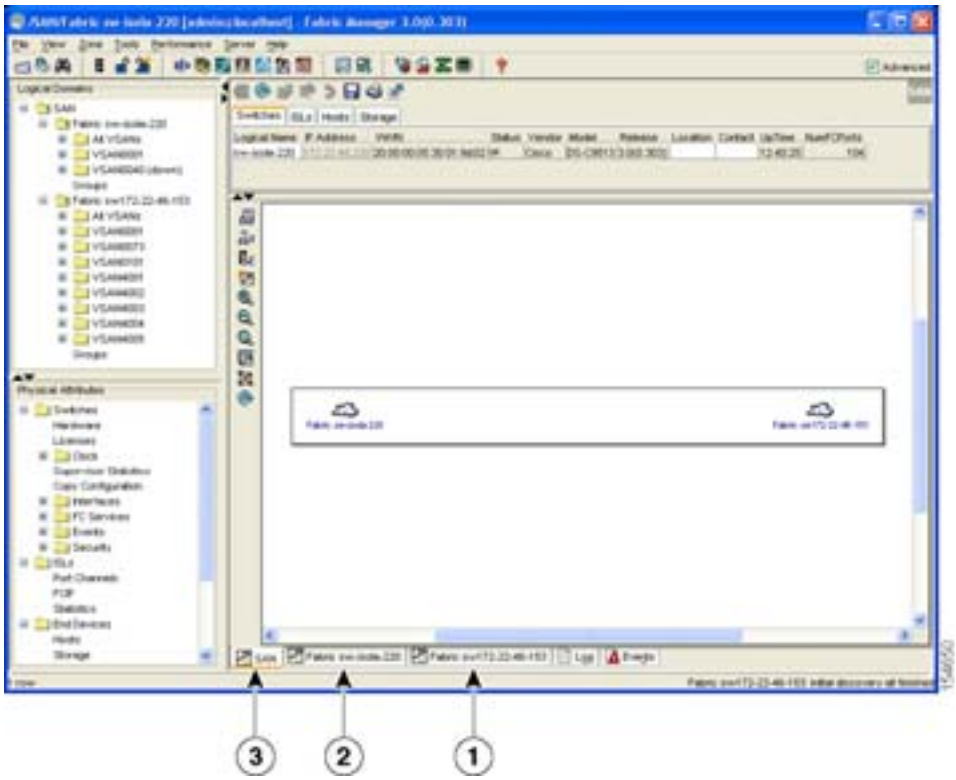
- **Server > Purge Down Elements** をクリックします。これによって、ファブリック内の停止している要素がすべて消去されます。
- **Fabric** ペインを右クリックし、**Purge Down Elements** を選択します。
- 停止している要素を右クリックし、**Purge** を選択します。この操作によって消去されるのは、ファブリック内の要素のうち、選択したものだけです。

（注） 停止していない要素を選択して消去した場合、その要素は次回のファブリック検出サイクルで再表示されます。

複数のファブリックの表示

Fabric Manager は、同じペイン上に複数のファブリックを表示できます（図 5-8 を参照）。

図 5-8　Fabric Manager の複数ファブリック表示ウィンドウ



1	ファブリック 172.23.46.152 の Fabric ビュー タブこれを選択すると、Fabric ビューにファブリック 172.23.46.152 が表示されます。
2	ファブリック 172.23.46.153 の Fabric ビュー タブこれを選択すると、Fabric ビューにファブリック 172.23.46.153 が表示されます。
3	SAN タブ（選択済み）— 両方のファブリックが表示されます。

（注） 複数のファブリックにログインするには、同じユーザ名およびパスワードを使用する必要があります。

シード スイッチを選択しなくても、両方のファブリックの情報が表示されます。ファブリックの詳細を表示するには、Fabric ペインの下部にあるそのファブリックのタブをクリックするか、または SAN タブでそのファブリックの **Cloud** アイコンをダブルクリックします。

（注） ラックの名前は一意でなければなりません。各ポートに同じラック名を使用すると、Fabric Manager は両方のファブリックに接続されているホスト / ターゲット ラックを表示します。auto-creation をディセーブルにするか、または一意のラック名を作成することによって、この問題を回避できます。

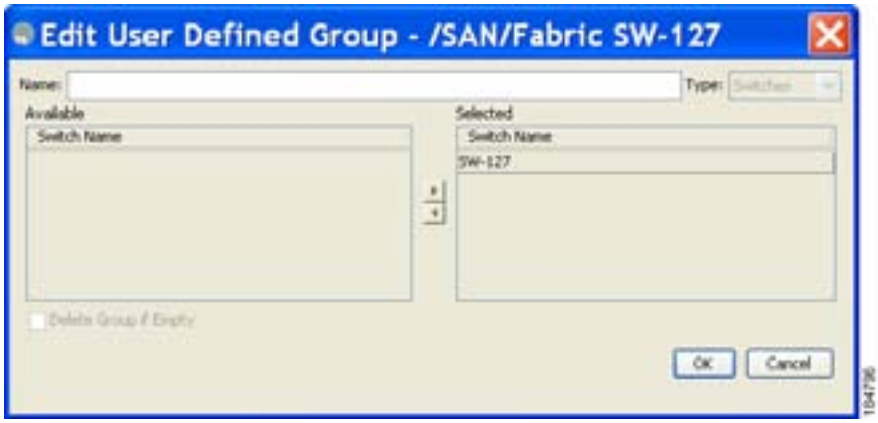
グループによるフィルタリング

スイッチまたはエンド ポートのグループを作成することによって、Fabric ペインの表示をフィルタリングできます。Fabric Manager でグループを作成する手順は、次のとおりです。

ステップ 1　Fabric ペインのマップでスイッチまたはエンド ポートを右クリックし、**Group** > **Create** を選択します。

図 5-9 のように、Edit User Defined Group ダイアログボックスが表示されます。

図 5-9　Edit User Defined Group ダイアログボックス



ステップ 2　**Name** フィールドにグループ名を入力します。

ステップ 3　矢印を使用して、Available カラムから Selected カラムに、追加するスイッチまたはエンド ポートを移動します。

ステップ 4　**OK** をクリックして、グループを保存します。

Fabric Manager の既存のグループにスイッチまたはエンド ポートを追加する手順は、次のとおりです。

ステップ 1　スイッチまたはエンド ポートを右クリックして、**Group** > **Add To** > ***YourGroupName*** を選択します。

図 5-9 のように、Edit User Defined Group ダイアログボックスが表示されます。

ステップ 2　追加するスイッチまたはエンド ポートを、矢印を使用して、Available カラムから Selected カラムに移動します。

ステップ 3　**OK** をクリックして、更新されたグループを保存します。

作成したグループによって表示をフィルタリングする手順は、次のとおりです。

ステップ 1　Logical Domains ペインの **Groups** フォルダを展開します。

図 5-10 のように、作成したグループのリストが表示されます。

図 5-10　Fabric ペインのマップで強調表示されたグループ

ステップ 2　フィルタリングするグループ名をクリックします。

Fabric ペインで、グループ内のスイッチまたはエンド デバイスは通常どおりに表示され、その他のスイッチおよびエンド デバイスはすべてグレーに表示されます。

ステップ 3　Logical Domains ペインで **Groups** フォルダをクリックすると、通常の表示に戻ります。

（注）　すべての CFS メンバー スイッチが表示される場合、誤設定を避けるため、ユーザ定義グループのテーブルは、CFS 制御機能がイネーブルに設定されているスイッチを除くグループ内のスイッチに基づいてフィルタリングされます。

ステータス バー

Fabric Manager ウィンドウの下部にあるステータス バーの右側には、検出プロセスで表示された最後のエントリ、および有効なエラー メッセージが表示されます。ファブリックに変更が行われた場合は、新規検出が必要であることを示すメッセージが表示されます。ステータス バーには、一時的なメッセージ（テーブルに表示される行数など）が短期間表示されたり、検出時の問題点が長期間表示されたりします。

Fabric Manager のプリファレンスの設定

Fabric Manager の動作に関するプリファレンスを設定するには、Fabric Manager メニューバーで **File > Preferences** を選択します。Preferences ダイアログボックスが表示され、アプリケーションの各コンポーネントを設定するための次のタブが表示されます。

- General
- SNMP
- Map

Fabric Manager の General タブのデフォルト設定は次のとおりです。

- Show Switch Name by — IP アドレス、DNS 名、または論理名別に Fabric ペインにスイッチを表示します。デフォルト設定は Logical Name です。
- Show WorldWideName (WWN) Vendor — Fabric Manager によって表示された任意のテーブルまたはリスト内で、WWN ベンダー名を表示します。スイッチの IP アドレスの前に名前を表示するには、**Prepend Name** チェックボックスをオンにします。IP アドレスの代わりに名前を表示するには、**Replacing Vendor Bytes** チェックボックスをオンにします。デフォルトは Prepend Name オプションです。
- Show End Device Using — エイリアスまたは pWWN エイリアスを使用して Fabric ペインにエンド デバイスを表示します。デフォルト設定は Alias です。
- Show Shortened iSCSI Names — デフォルト設定は OFF です。
- Show Timestamps as Date/Time — タイムスタンプを日付 / 時刻フォーマットで表示します。この設定がオフの場合、タイムスタンプは経過時間で表示されます。デフォルト設定はイネーブル（ON）です。
- Telnet Path — システムの telnet.exe ファイルのパスを設定します。デフォルトは telnet.exe ですが、正しい場所を参照する必要があります。

（注） パスを参照するか、パスを入力した場合に、パス名にスペースが入っていると（c:\program files\telnet.exe など）、パスは無効になります。パスを有効にするには、手動でパスを引用符で囲む必要があります（“c:\program files\telnet.exe” など）。

- Use Secure Shell instead of Telnet — CLI を使用してスイッチと通信する場合に、SSH または Telnet のどちらを使用するかを指定します。イネーブルの場合は、SSH アプリケーションのパスを指定する必要があります。デフォルト設定は、ディセーブルです。
- Confirm Deletion — Fabric Manager を使用して設定の一部を削除する場合に、確認用ポップアップ ウィンドウを表示します。デフォルト設定はイネーブル（ON）です。
- Export Tables with Format — Device Manager を使用してテーブルをエクスポートした場合に作成されるファイルのタイプを指定します。Tab-Delimited（タブ区切り）、または XML から選択できます。デフォルト設定は Tab-Delimited です。
- Show CFS Warnings — 選択した機能に関してすべてのスイッチで CFS がイネーブルでない場合に警告メッセージを表示します。

Fabric Manager の SNMP のデフォルト設定は次のとおりです。

- Retry request 1 time(s) after 5 sec timeout — 再試行値を 0 ～ 5、タイムアウト値を 3 ～ 30 に設定できます。
- Trace SNMP packets in Log — デフォルト設定は OFF です。
- Enable Audible Alert when Event Received — デフォルト設定は OFF です。

Fabric Manager の マップのデフォルト設定は次のとおりです。

- Display Unselected VSAN Members ― Fabric ペインに選択されていない VSAN メンバーを表示します。デフォルト設定は ON です。
- Display End Devices ― Fabric ペインにファブリックのエンド デバイスを表示します。デフォルト設定は ON です。
- Display End Device Labels ― Fabric ペインにファブリックのエンド デバイス ラベルを表示します。デフォルト設定は ON です。
- Expand Loops ― Fabric ペインに、ファブリックのループを個別の接続として表示します。デフォルト設定は OFF です。
- Expand Multiple Links ― Fabric ペインに、複数のリンクを 1 本の太い線でなく、個別の線として表示します。デフォルト設定は ON です。
- Open New Device Manager Each Time ― ファブリック内のスイッチから Device Manager を起動するたびに、新しいインスタンスをオープンします。デフォルト値は OFF です。つまり、一度にオープンされる Device Manager のインスタンスは 1 つのみです。
- Select Switch or Link from Table ― Fabric ペイン内のスイッチまたはリンクを、Information ペイン内のテーブルのスイッチまたはリンクをクリックして選択できます。デフォルト設定はディセーブル（OFF）です。つまり、テーブル内のスイッチまたはリンクをクリックしても、Fabric ペイン内のスイッチまたはリンクの選択は変更されません。
- Layout New Devices Automatically ― Fabric ペインに追加された新規デバイスを、最適な位置に自動的に配置します。デフォルト設定は OFF です。このモードで新規デバイスを追加した場合、最初の位置が要求を満たさないときは、手動で位置を変更する必要があります。
- Use Quick Layout when Switch has 30 or more End Devices ― この値のデフォルト設定値（30）を表示します。このフィールドに任意の番号を入力できます。Quick Layout をディセーブルにするには、**0** を入力します。
- Override Preferences for Non-default Layout ― この値のデフォルト設定値を（ON）を表示します。
- Automatically Save Layout ― このオプションがイネーブルの場合、レイアウトに関するすべての変更が自動的に保存されます。デフォルト設定は ON です。
- Detach Overview Window ― 表示するファブリック エリアの中央に Fabric ペインを簡単に移動できるようになります（この機能は、Fabric ペイン内に全体を表示できない大規模なファブリックの場合に役立ちます）。概要ウィンドウを起動するには、**Show/Hide Overview Window** ボタンをクリックします。**Show/Hide Overview Window** ボタンを再びクリックしないかぎり、概要ウィンドウはファブリック ウィンドウ上にオーバーレイされたままになります。この設定がイネーブルの場合は、概要ウィンドウを切り離して片側に移動し、その間に Fabric ペインにアクセスできます。デフォルト設定はディセーブル（OFF）です。

ネットワーク ファブリック検出

Cisco Fabric Manager は Fabric Manager に接続されたスイッチへの SNMP クエリを通して、ファブリック トポロジに関する情報を収集します。スイッチは、ファブリックに接続されたすべてのデバイスを検出したあとに応答します。デバイスの検出には、FSPF テクノロジー データベースおよび Name Server データベース内の情報や、FC-GS-3/4 標準で定義された Fabric Configuration Server の要求 / 応答メカニズムによって収集された情報が使用されます。Fabric Manager を起動する場合は、検索のためにシード スイッチの IP アドレス（またはホスト名）を入力します。

Fabric Manager を起動し、検出が完了すると、検出されたすべてのスイッチ、ホスト、ストレージ デバイスを含むネットワーク ファブリックのビューが表示されます。

デバイス グループの変更

FC-GS-3 要求に応答できないデバイスがある場合は、Fabric Manager マップの各エンド デバイスとして、1 台のサーバまたはストレージ サブシステムの複数のポートが表示されることがあります。

エンド デバイスを 1 つのラックにグループ化して、Fabric Manager のマップ上で 1 つのアイコンとして表示する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**End Devices** を展開し、**Storage** または **Hosts** を選択します。

Information ペインにエンド デバイスが表示されます。

ステップ 2　Fabric ペインのデバイスの 1 つをクリックするか、または Information ペインの **Enclosures** タブをクリックして、ラックに入れたいデバイスの名前（Name フィールド内）をクリックします。

ステップ 3　Fabric ペインのマップに新しいラックの名前を入力します。

ステップ 4　Name フィールドのデバイス名を 1 回クリックします。複数の名前を選択する場合は、**Shift** キーを押しながらその他の名前をそれぞれクリックします。

ステップ 5　**Ctrl-C** を押して、選択された名前をコピーします。

ステップ 6　**Ctrl-V** を押して、Name フィールドにデバイス名を貼り付けます。

（注）　ラックからデバイスを削除するには、目的のデバイスの名前をトリプル クリックし、**Delete** キーを押します。ラックを削除するには、ラック内のデバイスごとにこのステップを繰り返します。

ラックへのエイリアス名の使用

Fabric Manager を使用し、エイリアス名をラック名として使用するラックを作成する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**End Devices** を展開し、**Hosts** または **Storage** を選択します。

Information ペインに デバイスのリストが表示されます。NxPorts タブがデフォルトです。

ステップ 2　エイリアス名に変換するラック名を右クリックし、**Alias > Enclosure** を選択します（図 5-11 を参照）。

図 5-11　エイリアス ラック

ステップ 3　**Apply Changes** アイコンをクリックして、これらの変更を保存します。

ユーザおよびロールによる管理者アクセスの制御

シスコ スイッチは、CLI を使用しているか、または Cisco Fabric Manager を使用しているかに関係なく、ロール ベースの管理アクセスをサポートします。ロール ベースの管理アクセスを使用すると、特定のロールに特定の管理権限を割り当てたあと、各ロールに 1 つまたは複数のユーザを割り当てることができます。

デフォルト ロールには、ユーザが GUI（Fabric Manager および Device Manager）にアクセスするのに必要なアクセス権限が含まれます。これらのアクセス権限は、ユーザが GUI を使用できるようにするために、すべてのユーザに自動的に付与されます。

Cisco Fabric Manager は SNMPv3 を使用して、ロール ベースの管理アクセスを確立します。セットアップ ルーチンを完了すると、単一のロール、ユーザ名、およびパスワードが確立されます。このユーザに割り当てられたロールを使用すると、ユーザおよびロールの作成を含む、最高レベルの権限が使用可能になります。Cisco Fabric Manager を使用すると、ロールやユーザを作成したり、ネットワーク内のセキュア管理アクセスの必要性に応じてパスワードを割り当てることができます。

Fabric Manager ウィザードの使用

Fabric Manager Client には、一般的な設定作業を実行するために、次のウィザードが用意されています。

- VSAN — ファブリック内の複数のスイッチに VSAN を作成し、interop モード、ロードバランス、FICON などの VSAN 属性を設定します。
- Zone Edit Tool — ゾーン セット、ゾーン、およびエイリアスを作成します。ゾーンにメンバーを追加し、ゾーン データベースを編集します。
- SAN Port Channel — 選択した ISL から SAN ポート チャネルを手動でまたは自動的に作成します。チャネル ID やトランキング モードなどの SAN ポート チャネル属性を設定します。
- IP ACL — 順序付きの IP Access Control List（ACL; アクセス コントロール リスト）を作成し、ファブリック内の選択したスイッチに配布します。
- License Install — ファブリック内の選択したスイッチで、ライセンスのダウンロードおよびインストールを容易に実行できるようにします。
- Software Install — ファブリック内の選択したスイッチでイメージの互換性を確認し、ソフトウェア イメージをインストールします。
- Virtual Interface Group — VIG を作成します。
- Virtual Interfaces — 仮想イーサネット インターフェイスおよび仮想ファイバ チャネル インターフェイスを作成します。

Fabric Manager のトラブルシューティング ツール

Fabric Manager には、ツールバーまたは Tools メニューから使用可能なトラブルシューティング ツールがいくつかあります。ツールの使用手順については、第 31 章「ファブリックのトラブルシューティング」を参照してください。ここで、各ツールについて簡単に説明します。

- Zone Merge Analysis — ゾーン マージ分析ツール（Zone メニューから使用可能）を使用すると、2 つのシスコ スイッチが相互接続されている場合に、ゾーンが正常にマージされるかどうかを判別できます。相互接続されたスイッチ ポートで同じ名前の VSAN を使用できる場合、またはこれらのポートに同じ名前のゾーンが含まれている場合、Fabric Manager はこのゾーン内のメンバーが同じであるか確認します。マージ分析ツールは、マージの実行前、またはファブリックを相互接続してゾーン マージ障害原因を判別したあとに実行できます。
- End-to-End Connectivity — Fabric Manager のエンドツーエンド接続分析ツールはファイバ チャネル ping を使用して、特定の VSAN 内のシスコ スイッチとエンド デバイス（HBA およびストレージ デバイス）間の相互接続を検証します。エンド デバイスがアクティブな帯域内または帯域外管理パスを経由して管理可能なスイッチに接続されている Fabric Manager は基本接続のほかに、次の内容を検証することもできます。
  - パスが冗長である
  - ゾーンに 2 つ以上のメンバーが含まれる

エンド デバイスが管理可能なスイッチに接続されている（帯域内または帯域外管理パスで現在アクティブである）

- Switch Health Analysis — Fabric Manager を使用して詳細なスイッチ ヘルス分析を実行できます。重要なシスコ スイッチ、モジュール、ポート、およびファイバ チャネル サービスのステータスがすべて検証されます。40 を超える条件がチェックされます。このツールを使用すると、シスコ スイッチの状態にすばやく、容易に、かつ完全にアクセスできます。
- Fabric Configuration Analysis — Fabric Manager にはファブリック設定分析ツールがあります。ファブリック内のすべてのシスコ スイッチの設定が、参照スイッチまたはポリシー ファイルと比較されます。チェックする機能、および実行するチェック タイプを定義することができます。分析では一致しない値、失われた値、または余分な値を検索できます。すべての機能に対してすべての設定チェックを行った場合、シスコ スイッチにつき 200 以上のチェックが実行されます。

分析を実行すると、検出された問題点の詳細とともに結果が表示されます。設定が異なっている場合は、この設定を選択し **Resolve** ボタンをクリックして、自動的に解決することができます。参照スイッチまたはポリシー ファイルに合わせて、設定が自動的に変更されます。

CHAPTER 6

Device Manager

この章では、Cisco Device Manager の説明と、使用手順を示します。この章の内容は、次のとおりです。

- Device Manager の概要（p.6-2）
- Device Manager の起動（p.6-2）
- Device Manager の使用法（p.6-3）
- Quick Configuration Tool の使用（p.6-8）
- Device Manager のプリファレンスの設定（p.6-10）

Device Manager の概要

Device Manager を使用すると、搭載された拡張モジュール、各ポートのステータス、電源モジュール、およびファン アセンブリを含めて、Cisco Nexus 5000 シリーズ スイッチ シャーシをグラフィック表示できます。

Fabric Manager の Information ペイン内のテーブルは、基本的に、Device Manager で表示されるダイアログボックスに対応しています。ただし、Fabric Manager のテーブルには 1 つまたは複数のスイッチの値が表示されますが、Device Manager ダイアログボックスに表示されるのは 1 つのスイッチの値です。また、デバイス固有の設定の確認や、トラブルシューティング用の情報は、Fabric Manager よりも Device Manager の方が詳細です。

Device Manager は、Device View と Summary View の 2 つのビューを提供します。Summary View では、スイッチのインターフェイスを監視できます。Device View では、次のようなスイッチ レベルの設定を実行できます。

- 複数の VSAN のゾーンの設定
- ポート、SAN ポート チャネル、およびトランキングの管理
- スイッチへの SNMPv3 セキュリティ アクセスの管理
- スイッチへの CLI（コマンドライン インターフェイス）セキュリティ アクセスの管理
- アラーム、イベント、および通知の管理
- コンフィギュレーション ファイルおよびソフトウェア イメージの保存とコピー
- ハードウェア構成の表示
- シャーシ、モジュール、およびポートのステータスや統計情報の表示

Device Manager の起動

Device Manager は、デスクトップまたは Fabric Manager から起動できます。

デスクトップから Device Manager を起動するには、**Device Manager** アイコンをダブルクリックし、「Cisco Fabric Manager とその他の管理ツールとの統合」（p.2-21）に記載された手順に従います。

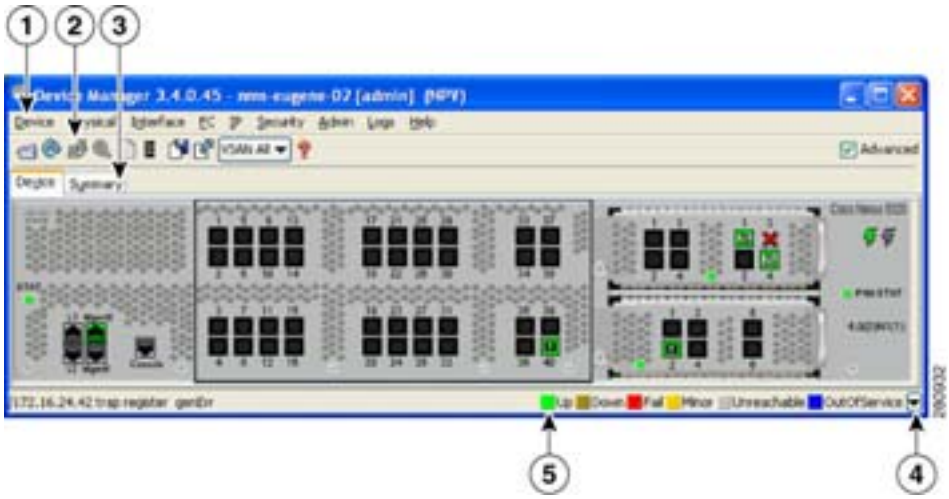
Fabric Manager から Device Manager を起動するには、次のいずれかの作業を実行します。

- Fabric ペインのマップで、管理するスイッチを右クリックし、表示されたメニューで **Device Manager** を選択します。
- Fabric ペインのマップでスイッチをダブルクリックします。
- Fabric ペインのマップでスイッチを選択し、**Tools** > **Device Manager** を選択します。

Device Manager の使用法

ここでは、Device Manager インターフェイスについて説明します（図 6-1 を参照）。

図 6-1　Device Manager の Device タブ



1	メニューバー	4	凡例
2	ツールバー	5	ステータス
3	タブ		

メニューバー

Device Manager メイン ウィンドウの上部にあるメニューバーでは、1 台のスイッチの管理およびトラブルシューティングを行うことができます。メニューバーには、次のオプションがあります。

- Device — Device Manager のインスタンスのオープン、管理プリファレンスの設定、ページ レイアウトの設定、現在のスイッチとの Telnet/Secure Shell（SSH; セキュア シェル）セッションのオープン、デバイス イメージのエクスポート、および Device Manager アプリケーションのクローズを行います。
- Physical — コンポーネント、モジュール、温度センサ、電源モジュール、ファン、およびシステム全体を表示し、管理できます。
- Interface — SAN ポート チャネル、およびファイバ チャネル、イーサネット ポートを設定して管理できます。診断、管理、モニタリング機能、および Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）とポートのトラッキング機能も提供します。
- FC — VSAN（仮想 SAN）、ドメイン、およびネーム サーバの特性を設定して管理できます。高度な設定機能も提供します。
- Security — FCSP、ポート セキュリティ、SNMP（簡易ネットワーク管理プロトコル）セキュリティ、共通のロール、SSH、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）、および IP Access Control List（ACL; アクセス コントロール リスト）を設定して管理できます。
- Admin — スイッチ設定の保存、コピー、編集、および消去、イベントのモニタ、フラッシュ ファイルの操作、ライセンスの管理、NTP の設定、CFS の使用、およびスイッチのリセットを実行できます。**show tech support**、**show cores**、および **show image** コマンドを使用することもできます。

- Logs — メッセージ、ハードウェア、イベント、およびアカウンティングの各ログを表示します。Syslog セットアップも設定できます。
- Help — Information ペインに、特定のダイアログボックスに関するオンライン ヘルプ トピックが表示されます。

ツールバー アイコン

Device Manager ツールバーを使用すると、多くの Device Manager 機能にすばやくアクセスできます。アイコンを選択すると、機能を設定するためのダイアログボックスが開くことがあります。ツールバーには、主な Device View アイコンおよび Summary View アイコンが配置されています（表 6-1 を参照）。

表 6-1　Device Manager のメイン ツールバー

アイコン		説明
	Open Device	他のスイッチの Device Manager ビューを開きます。このビューを別のウィンドウで開くオプションがあります。
	Refresh Display	スイッチと通信し、Device Manager ビューに情報を表示します。
	Command-Line Interface	スイッチに対する CLI コマンド ウィンドウを別個に開きます。
	Configure Selected	選択されたコンポーネント（ライン カードまたはポート）の設定ダイアログボックスを開きます。
	SysLog	スイッチに発生した最新のシステム メッセージのリストを表示するウィンドウを開きます。
	VSANs	スイッチの VSAN 設定を行う VSAN ダイアログボックスを開きます。
	Save Configuration	現在の実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。
	Copy	サーバとスイッチ間でコンフィギュレーション ファイルをコピーします。
	Toggle FICON/Interface Port Labels	FICON およびインターフェイス ポート ラベルを切り替えます。
VSAN All	Select VSAN	ポートの表示をフィルタリングして、選択された VSAN に属すポートだけを表示します。
	Help	Device Manager のオンライン ヘルプにアクセスします。

ダイアログボックス

ツールバー アイコンを選択すると、選択された機能を設定するためのダイアログボックスが開くことがあります。このダイアログボックスには、テーブル操作用アイコンが配置されている場合があります。これらのアイコンの詳細については、「Information ペイン」（p.5-13）を参照してください。

タブ

タブは、次の機能を提供します。

- Device — スイッチ シャーシおよびコンポーネントのグラフィック表示を提供します。
- Summary — 1 台のスイッチ、ファイバ チャネルおよび IP 近接デバイスにおけるアクティブなインターフェイスを表示します。Summary View にはポート速度、リンク利用率、およびその他のトラフィック統計情報も表示されます。Summary View タブの左上に、トラフィック監視用のボタンが 2 つあります。選択されたオブジェクトのトラフィックを監視するには、**Monitor Selected Interface Traffic Util%** ボタンをクリックします。選択されたオブジェクトの詳細な統計情報を表示するには、**Monitor Selected Interface Traffic Details** ボタンをクリックします。ポーリング インターバル、タイプまたは Rx/Tx 表示、およびしきい値を設定できます。

凡例

Device Manager の右下にある凡例は、次のようにポート ステータスを示します。

- カラー
  - グリーン — ポートが起動しています。
  - ブラウン — ポートは管理上のダウン状態です。
  - レッド — ポートはダウンしているか、または障害があります。
  - オレンジ — ポートにマイナー障害が発生しています。
  - グレー — ポートに到達できません。
  - ブルー — ポートはアウト オブ サービス状態です。
- ラベル
  - X — リンク障害
  - E — ISL（スイッチ間リンク）
  - TE — Multi-VSAN ISL
  - F — ホスト / ストレージ
  - FL — F ループ
  - I — iSCSI
  - SD — スパンの終点
  - CH — チャネル
  - CU — 制御ユニット
  - NP — プロキシ N ポート（NPV モード）
  - f — 仮想ファイバ チャネル インターフェイスが存在
  - e — 仮想イーサネット インターフェイスが存在

スーパーバイザおよびスイッチング モジュール

Device View でオブジェクトを右クリックして、その情報を取得したり、設定することができます。モジュールを右クリックすると、メニューにモジュール番号が表示され、モジュールの設定やリセットを実行できます。ポートを右クリックすると、メニューにポート番号が表示され、そのポートに関する設定、監視、イネーブル化、ディセーブル化、ビーコン モードの設定、または診断を実行できます。

ヒント　Device Manager では複数のポートを選択し、選択したすべてのポートにオプションを一度に適用できます。ポートを選択するには、マウスをクリックしたまま、選択するポートを囲むようにドラッグするか、**Ctrl** キーを押したまま各ポートをクリックします。

ポートをイネーブルまたはディセーブルにするには、ポートを右クリックし、ポップアップ メニューで **Enable** または **Disable** をクリックします。複数のポートをイネーブルまたはディセーブルにするには、マウスをドラッグしてポートを選択し、選択されたポートを右クリックします。ポップアップ メニューで **Enable** または **Disable** をクリックします。

（注）　Device Manager では、ファイバ チャネル ポートでのみ Enable および Disable を使用できます（イーサネット ポートでは使用できません）。

1 つまたは複数のポートのトランキングを管理するには、選択されたポートを右クリックし、**Configure** をクリックします。表示されたダイアログボックスの Trunk カラムの現在の値を右クリックし、プルダウン リストで **nonTrunk**、**trunk**、または **auto** をクリックします。

Device Manager を使用して SAN ポート チャネルを作成するには、Interface メニューで **PortChannels** をクリックします。詳細な手順については、第 14 章「SAN ポート チャネルの設定」を参照してください。Fabric Manager を使用して SAN ポート チャネルを簡単に作成することもできます。

（注）　SAN ポート チャネルを作成するには、リンク両端のすべてのポートでポート速度、トランキング タイプ、および管理ステートを同じにする必要があります。

コンテキスト メニュー

両方の Device Manager ビューでコンテキスト メニューを使用可能にするには、デバイスまたはテーブルを右クリックします。

Device View メニュー

- Device — システム、モジュール、または電源モジュールを右クリックするとメニューが表示され、デバイスの設定に関するオプションを選択できます。
- Port — ポートを右クリックすると、クリックしたポートの番号を示すメニューが起動し、そのポートに関する設定、モニタリング、イネーブル化、またはディセーブル化を実行できます。

（注） イーサネット ポートのコンテキスト メニューでは物理イーサネット ポートだけではなく、物理イーサネットに存在する任意の仮想インターフェイスの設定およびモニタリングも実行します。

Summary View メニュー

- Table — テーブルのヘッダーを右クリックすると、そのテーブルに表示されるカラムのリストが表示されます（Interface、Description、VSANs、Mode、Connected To、Speed (Gb)、Rx、Tx、Errors、Discards、および Log）。ポート タイプに該当する設定ダイアログボックスを起動するには、Description フィールドをクリックします。

Quick Configuration Tool の使用

Device Manager は、スイッチにイーサネット インターフェイスを設定するツールを提供します。Quick Configuration Tool では、各イーサネット インターフェイスの次のいずれかの設定を選択できます。

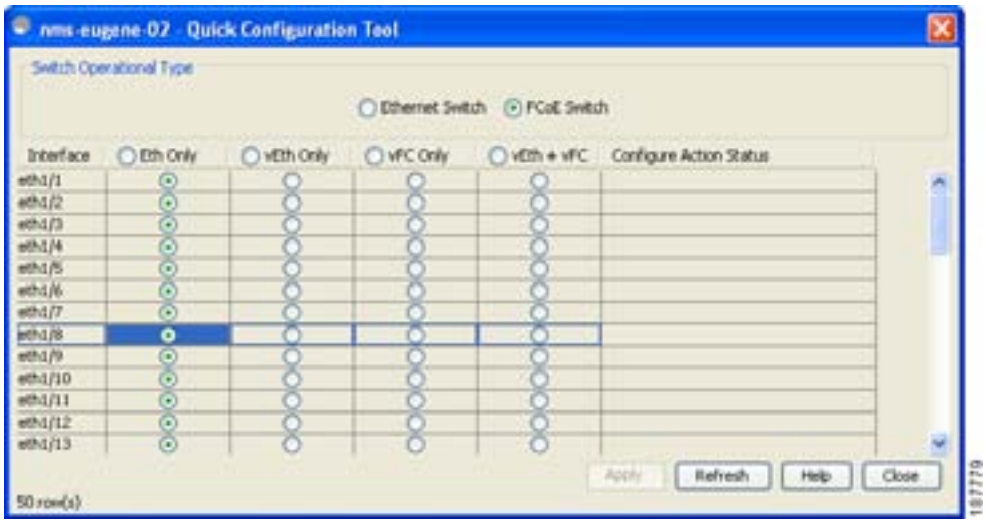
- Eth Only — 仮想インターフェイスなしで物理イーサネットを設定します。
- vEth Only — 物理イーサネットを、仮想イーサネット インターフェイスに関連する VIG を持つように設定します。
- vFC Only — 物理イーサネットを、仮想ファイバ チャネル インターフェイスに関連する VIG を持つように設定します。
- vEth + vFC — 物理イーサネットを、仮想イーサネット インターフェイスおよび仮想ファイバ チャネル インターフェイスに関連する VIG を持つように設定します。

Quick Configuration Tool を使用してイーサネット インターフェイスを設定する手順は、次のとおりです。

ステップ 1　ツール メニューで、Quick Config Wizard を選択します。

Quick Configuration Tool ウィンドウが表示されます（図 6-2 を参照）。

図 6-2　Quick Configuration Tool



ステップ 2　スイッチをイーサネット スイッチとして設定する場合は、Switch Operational Type ペインで、**Ethernet Switch** オプション ボタンをクリックします。スイッチをファイバ チャネルおよび FCoE インターフェイスとの I/O Consolidation（IOC）として設定する場合は、**FCoE Switch** オプション ボタンをクリックします。

ステップ 3　（任意）すべてのインターフェイスを選択したカラムの値に設定するには、カラムのヘッダーのオプション ボタンをクリックします。

ステップ 4　各行で、インターフェイスに適用する設定のオプション ボタンをクリックします。

ステップ 5　**Apply** ボタンをクリックして、設定変更を適用します。

Configure Action Status フィールドに、要求された設定変更の現在のステータスが表示されます。

ステップ 6　（任意）Configure Action Status フィールドをクリアするには、**Refresh** ボタンをクリックします。Device Manager は、スイッチからの最新のステータスでフィールドを更新します。

Device Manager のプリファレンスの設定

Device Manager アプリケーションのプリファレンスを設定するには、Device メニューで **Device** > **Preferences** を選択します。設定できるプリファレンスは次のとおりです。

- Retry Requests x Time(s) After x sec Timeout ― 再試行要求値を設定できます。デフォルト設定は、5 秒間のタイムアウト後に 1 回です。
- Enable Status Polling Every x secs ― ステータス ポーリング値を設定できます。デフォルト設定はイネーブル（オン）で、期間は 40 秒です。
- Trace SNMP Packets in Message Log ― Device Manager が SNMP パケットをトレースし、トレースを記録するかどうかを設定できます。デフォルト設定は、ディセーブル（オフ）です。
- Register for Events After Open, Listen on Port 1163 ― Device Manager を開いたあとにイベントが記録されるように、現在のスイッチを登録できます。デフォルト設定はイネーブル（オン）です。
- Confirm Deletion ― Device Manager を使用して設定の一部を削除する場合に、確認用ポップアップを表示します。デフォルト設定はイネーブル（オン）です。
- Show WorldWideName (WWN) Vendor ― Device Manager によって表示された任意のテーブルまたはリスト内で、WWN ベンダー名を表示します。**Prepend** がオンの場合は、スイッチの IP アドレスの前に名前が表示されます。**Replace** がオンの場合は、IP アドレスの代わりに名前が表示されます。デフォルト設定では、**Prepend** オプションがイネーブル（オン）です。
- Show Timestamps as Date/Time ― タイムスタンプを日付 / 時刻フォーマットで表示します。この設定がオフの場合、タイムスタンプは経過時間で表示されます。デフォルト設定はイネーブル（オン）です。
- Telnet Path ― システムの telnet.exe ファイルのパスを設定します。デフォルトは telnet.exe ですが、正しい場所を参照する必要があります。

（注） パスを参照するか、パスを入力した場合に、パス名にスペースが入っていると（c:\program files\telnet.exe など）、パスは無効になります。パスを有効にするには、手動でパスを引用符で囲みます（“c:\program files\telnet.exe” など）。

- Use Secure Shell Instead of Telnet ― CLI を使用してスイッチと通信する場合に、SSH と Telnet のどちらを使用するかを指定します。イネーブルの場合は、SSH アプリケーションのパスを指定する必要があります。デフォルト設定は、ディセーブルです。
- CLI Session Timeout x secs (0= disable) ― CLI セッションのタイムアウト インターバルを指定します。ディセーブル（タイムアウト値なし）にするには、0 を入力します。デフォルト設定は 30 秒です。
- Show Tooltips in Physical View ― Physical（Device）View にツールチップを表示するかどうかを決定します。デフォルト設定はイネーブル（オン）です。
- Label Physical View Ports With: ― Physical（Device）View を使用している場合に、ポートに割り当てるラベル タイプを指定します。FICON および Interface を選択できます。デフォルト設定は Interface です。
- Export Table ― Device Manager を使用してテーブルをエクスポートした場合に作成されるファイルのタイプを指定します。Tab-Delimited（タブ区切り）、または XML から選択できます。デフォルト設定は Tab-Delimited です。

CHAPTER 7

CFS の使用

Nexus 5000 シリーズ スイッチは、Cisco Fabric Services（CFS）機能を提供します。この機能は、ネットワーク内のすべてのスイッチに設定情報を自動配信することでプロビジョニングを簡易化します。

スイッチ機能は、CFS インフラストラクチャを使用して、機能で必要な機能データまたは設定データを配信できます。

この章の内容は、次のとおりです。

- CFS の概要（p.7-2）
- CFS 配信（p.7-3）
- アプリケーションの CFS サポート（p.7-8）
- CFS リージョン（p.7-13）
- CFS 配信情報の表示（p.7-18）
- Fabric Manager を使用した CFS の例（p.7-19）
- Device Manager を使用した CFS の例（p.7-22）
- デフォルト設定（p.7-23）

CFS の概要

Nexus 5000 シリーズ スイッチの一部の機能は、正しく機能するために、ネットワーク内の他のスイッチと設定を同期させる必要があります。ネットワーク内の各スイッチで手動により同期化を行う方法は、単調でエラーの元となる作業です。

CFS はネットワーク内の自動設定同期化に対して共通のインフラストラクチャを提供します。また、機能に対して転送機能および共通サービスのセットを提供します。CFS はネットワーク内の CFS 対応スイッチを検出したり、すべての CFS 対応スイッチの機能を検出できます。

Nexus 5000 シリーズ スイッチは、ファイバ チャネル、IPv4、または IPv6 ネットワークを介した CFS メッセージの配信をサポートしています。スイッチがファイバ チャネル ポートでプロビジョニングされている場合、デフォルトではファイバ チャネルを介した CFS がイネーブルです。IP を介した CFS を明示的にイネーブルにする必要があります。

CFS には次の機能があります。

- CFS レイヤでクライアント / サーバ関係を持たないピア間のプロトコル
- ファイバ チャネル、IPv4、または IPv6 ネットワークを介した CFS メッセージの配信
- 3 つの配信モード
  - 協調型配信：常時、ネットワーク内で 1 つの配信のみが許可されます。
  - 非協調型配信：協調型配信が進行中である場合を除いて、ネットワーク内で複数の同時配信を実行できます。
  - 無制限の非協調型配信：既存の協調型配信がある場合に、ネットワーク内で複数の同時配信が許可されます。無制限の非協調型配信は、他のすべての配信タイプの配信と同時に実行できます。

次の機能は、IP を介した CFS 配信でサポートされています。

- IP ネットワークを介した配信の 1 つのスコープ：
  - 物理スコープ：配信は、IP ネットワーク全体に及びます。

次の機能は、ファイバ チャネル SAN を介した CFS 配信でサポートされています。

- SAN ファブリックを介した配信の 3 つのスコープ
  - 論理スコープ：配信は、VSAN のスコープ内で発生します。
  - 物理スコープ：配信は、物理トポロジ全体に及びます。
  - 選択した VSAN セットを超える場合：一部の機能は一部の特定の VSAN を介した設定配信を必要とします。これらの機能は、配信を制限する VSAN セットを CFS に指定できます。
- ファブリック マージ イベント中（2 つの独立した SAN ファブリックのマージ中）に、機能設定のマージを実行するマージ プロトコルをサポートします。

CFS 配信

CFS 配信機能は、下位層の転送には依存しません。Nexus 5000 シリーズ スイッチは、IP を介した CFS 配信およびファイバ チャネルを介した CFS 配信をサポートしています。CFS を使用する機能は、下位層の転送を認識しません。

ここでは、さらに詳しい内容について説明します。

- CFS 配信のモード（p.7-3）
- スイッチの CFS 配信のイネーブル化およびディセーブル化（p.7-4）
- IP を介した CFS 配信（p.7-5）
- ファイバ チャネルを介した CFS 配信（p.7-6）
- CFS 配信のスコープ（p.7-7）
- CFS マージのサポート（p.7-7）

CFS 配信のモード

CFS は、異なる機能の要件に対応するために 3 つの配信のモードをサポートしています。常時 1 つのモードだけを適用できます。ここでは、CFS 配信のモードについて説明します。

- 非協調型配信（p.7-3）
- 協調型配信（p.7-3）
- 無制限の非協調型配信（p.7-3）

非協調型配信

非協調型配信は、ピアからの情報と競合しないと思われる情報を配信する場合に使用されます。1 つの機能に対して非協調型の同時配信を適用できます。

協調型配信

協調型配信は、常時 1 つの機能配信だけに適用できます。CFS はロックを使用してこの機能を実行します。ネットワーク内のどこかの機能でロックが取得されていれば、協調型配信を開始することはできません。協調型配信は、3 つの段階に分かれます。

1. ネットワーク ロックが取得されます。
2. 設定が配信され、コミットされます。
3. ネットワーク ロックが解放されます。

協調型配信には 2 種類あります。

- CFS によるもの — 機能が介在することなく、機能要求に応じて CFS が各段階を実行します。
- 機能によるもの — 各段階が機能によって完全に管理されます。

  協調型配信は、ポート セキュリティの設定などの、複数のスイッチで操作および配信が可能な情報の配信に使用されます。

無制限の非協調型配信

無制限の非協調型配信では、既存の協調型配信がある場合にネットワーク内で複数の同時配信が許可されます。無制限の非協調型配信は、他のすべての配信タイプの配信と同時に実行できます。

スイッチの CFS 配信のイネーブル化およびディセーブル化

スイッチがファイバ チャネル ポートでプロビジョニングされている場合、デフォルトではファイバ チャネルを介した CFS がイネーブルです。IP を介した CFS を明示的にイネーブルにする必要があります。

物理接続を維持したまま、スイッチで CFS をグローバルにディセーブル化し、CFS を使用する機能からネットワーク全体への配信を隔離することができます。スイッチで CFS がグローバルにディセーブルにされている場合、CFS 動作はスイッチに制限されます。

Fabric Manager を使用して特定のスイッチ上で CFS 配信をグローバルにディセーブル化またはイネーブル化する手順は、次のとおりです。

ステップ 1　CFS 機能を選択します。たとえば、Physical Attributes ペインで **Switches** > **Events** を展開してから、**CallHome** を選択します。

Information ペインの CFS タブに該当する機能が表示されます。

ステップ 2　**CFS** タブをクリックして、ネットワーク内のスイッチごとに、該当機能の CFS ステートを表示します。

ステップ 3　**Global State** カラムの値をクリックします。値がドロップダウン メニューに変わります。

ステップ 4　ドロップダウン メニューから、**disable** または **enable** を選択します。

ステップ 5　CFS をディセーブルまたはイネーブルにするすべてのスイッチで、ステップ 3 および 4 を繰り返します。

ステップ 6　Config Action カラムを **commit** に設定します。

ステップ 7　**Apply Changes** アイコンをクリックして、その機能の設定変更をコミットし、CFS を通じて変更内容を配信します。

Device Manager を使用して、特定のスイッチ上で CFS 配信をグローバルにディセーブル化またはイネーブル化する手順は、次のとおりです。

ステップ 1　**Admin** > **CFS (Cisco Fabric Services)** を選択します。

そのスイッチのすべての機能の CFS ステータスを示す CFS ダイアログボックスが表示されます。

ステップ 2　現在のスイッチで CFS 配信をディセーブル化またはイネーブル化するには、**Globally Enabled** チェックボックスをオフまたはオンにします。

ステップ 3　**Apply** をクリックして、このスイッチの CFS をディセーブルにします。

IP を介した CFS 配信

IP を介した CFS 配信は次の機能をサポートしています。

- IP ネットワーク全体での物理的配信
- ファイバ チャネルまたは IP を介して到達可能なすべてのスイッチに配信が到達する、ハイブリッド ファイバ チャネルおよび IP ネットワークでの物理的配信

（注） スイッチはまずファイバ チャネルを介して情報を配信し、ファイバ チャネルでの最初の試みが失敗すると IP ネットワークを介して配信します。IP およびファイバ チャネルの両方を介した配信がイネーブルの場合、CFS が重複メッセージを送信することはありません。

- IP バージョン 4（IPv4）または IP バージョン 6（IPv6）を介した配信

（注） CFS は同じスイッチから IPv4 と IPv6 の両方を介して配信することはできません。

- 設定可能なマルチキャスト アドレスを使用してネットワーク トポロジの変更を検出するキープアライブ メカニズム
- リリース 2.x 以上が稼働している Cisco MDS 9000 ファミリ スイッチとの互換性

図 7-1 はファイバ チャンネル接続と IP 接続の両方を持つネットワークを示します。ノード A はファイバ チャネルを介してノード B にイベントを転送します。ノード B はユニキャスト IP を使用してノード C とノード D にイベントを転送します。ノード C はファイバ チャネルを介してノード E にイベントを転送します。

図 7-1　ファイバ チャネル接続と IP 接続を持つネットワーク例 1

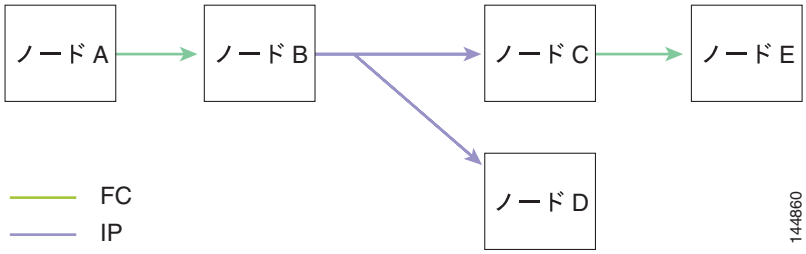


図 7-2 は、ノード C とノード D がファイバ チャネルを使用して接続されていることを除き、図 7-1 と同じです。ノード B にはノード C とノード D の IP 用配布リストがあるので、この例のすべてのプロセスは同じです。ノード D はすでにノード B からの配布リストに入っているため、ノード C はノード D に転送しません。

図 7-2　ファイバ チャネル接続と IP 接続を持つネットワーク例 2

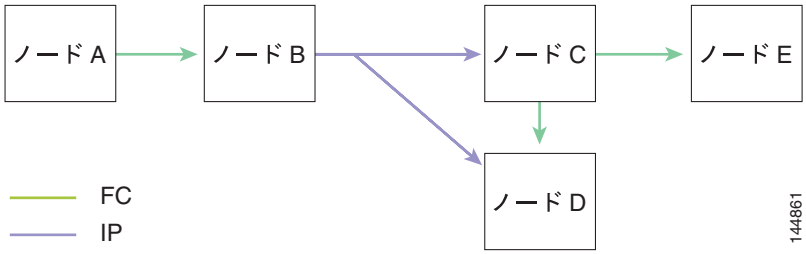
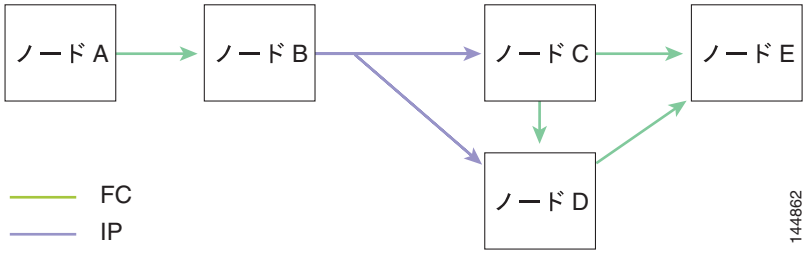


図 7-3 は、ノード D とノード E が IP を使用して接続されていることを除き、図 7-2 と同じです。ノード E はノード B からの配布リストに入っていないため、ノード C およびノード D は両方ともイベントをノード E に転送します。

図 7-3　ファイバ チャネル接続と IP 接続を持つネットワーク例 3



ファイバ チャネルを介した CFS 配信

ファイバ チャネルを介した FCS 配信の場合、CFS プロトコル層が FC2 層の上位に存在します。CFS は FC2 転送サービスを使用して、他のスイッチに情報を送信します。CFS はすべての CFS パケットに対して独自の SW_ILS（0x77434653）プロトコルを使用します。CFS パケットはスイッチ ドメイン コントローラ アドレスで送受信されます。

CFS 配信のスコープ

Nexus 5000 シリーズ スイッチのそれぞれ異なるアプリケーションは、次の各種のレベルで設定を配信する必要があります。ファイバ チャネルを介した CFS 配信を使用する場合、次のレベルを使用できます。

- VSAN レベル（論理スコープ）

  VSAN のスコープ内で動作するアプリケーションは、設定の配信が VSAN に限定されます。アプリケーション例は、VSAN 内でのみコンフィギュレーション データベースを適用可能なポート セキュリティです。

（注） 論理スコープは、IP を介した FCS 配信ではサポートされていません。

- 物理トポロジ レベル（物理スコープ）

  一部のアプリケーション（NTP など）は、物理トポロジ全体に設定を配信する必要があります。
- 選択した 2 つのスイッチ間

  一部のアプリケーションは、ネットワーク内の選択したスイッチ間でのみ動作します。

CFS マージのサポート

CFS マージは、ファイバ チャネルを介した CFS 配信でサポートされています。

アプリケーションは CFS を通して、設定を SAN ファブリック内で継続的に同期します。このような 2 つのファブリック間で ISL（スイッチ間リンク）を起動すると、これらのファブリックがマージされることがあります。これらの 2 つのファブリック内の構成情報セットが異なっているために、マージ イベント中に調整が必要になることがあります。CFS はアプリケーション ピアがオンラインになるたびに通知します。M のアプリケーション ピアを持つファブリックが N のアプリケーション ピアを持つ別のファブリックとマージし、アプリケーションが通知のたびにマージ アクションを行う場合は、リンク アップ イベントがファブリック内の M*N マージをトリガーします。

CFS がサポートするプロトコルは、CFS レイヤで複雑なマージを処理することにより、必要なマージ数を 1 に削減します。このプロトコルはスコープ単位でアプリケーションごとに動作します。このプロトコルでは、ファブリック内の 1 つのスイッチがそのファブリックのマージ マネージャとして選択されます。その他のスイッチでは、マージ プロセスにロールがありません。

2 つのファブリック内のマージ マネージャは、マージ中にコンフィギュレーション データベースを相互に交換します。一方のデータベースのアプリケーションが情報をマージし、マージに成功したかどうかを判別して、結合されたファブリック内のすべてのスイッチにマージ ステータスを通知します。

マージに成功した場合は、マージされたデータベースが結合されたファブリック内のすべてのスイッチに配信され、新規ファブリック全体が一貫したステートになります。マージ障害から回復するには、新規ファブリック内の任意のスイッチから配信を開始します。この配信により、ファブリック内のすべてのピアが同じコンフィギュレーション データベースに復元されます。

アプリケーションの CFS サポート

ここでは、アプリケーションをサポートする CFS 機能について説明します。

- CFS アプリケーション要件（p.7-8）
- アプリケーションの CFS のイネーブル化（p.7-8）
- ネットワークのロック（p.7-10）
- 変更のコミット（p.7-10）
- 変更の廃棄（p.7-11）
- コンフィギュレーションの保存（p.7-11）
- ロック済みセッションのクリア（p.7-12）

CFS アプリケーション要件

ネットワーク内のすべてのスイッチは CFS に対応している必要があります。CFS に対応していないスイッチは配信を受信できず、ネットワークの一部が目的の配信を受信できなくなります。

CFS には次の要件があります。

- 暗黙的な CFS の使用 — CFS 対応アプリケーションに CFS タスクを初めて発行した場合は、設定変更プロセスが開始し、アプリケーションによってネットワークがロックされます。
- 保留データベース — 保留データベースはコミットされていない情報を保持する一時的なバッファです。データベースがネットワーク内のほかのスイッチのデータベースと同期するように、コミットされていない変更はすぐに適用されません。変更をコミットする場合、保留データベースはコンフィギュレーション データベース（別名、アクティブ データベースまたは有効なデータベース）を上書きします。
- アプリケーション単位でイネーブル化またはディセーブル化した CFS 配信 — CFS 配信ステートのデフォルト（イネーブルまたはディセーブル）は、アプリケーション間で異なります。CFS 配信がディセーブル化されたアプリケーションは、設定を配信せず、ネットワーク内の他のスイッチからの配信も受信しません。
- 明示的な CFS コミット — 大半のアプリケーションでは、新しいデータベースをネットワークに配信したりネットワーク ロックを解放するために一時的なバッファ内の変更をアプリケーション データベースにコピーする明示的なコミット動作が必要です。一時バッファ内の変更はコミット操作を実行しなければ適用されません。

アプリケーションの CFS のイネーブル化

すべての CFS ベース アプリケーションは、配信機能をイネーブルまたはディセーブルにすることができます。

デフォルトでは、アプリケーションの配信はイネーブルです。

アプリケーションの配信を明示的にイネーブルにしないかぎり、CFS はアプリケーション設定を配信しません。

Fabric Manager を使用して機能に対する CFS をイネーブルにする手順は、次のとおりです。

ステップ 1　CFS をイネーブルにする機能を選択します。

たとえば、Physical Attributes ペインで **Switches** > **Events** を展開してから、**CallHome** を選択します。Information ペインに、該当する機能および CFS タブが表示されます。**CFS** タブをクリックして、ネットワーク内のスイッチごとに、該当機能の CFS ステートを表示します。

ステップ 2　CFS をイネーブルにするスイッチを決定します。CFS をイネーブルにする場合は Feature Admin カラムを **enable** に、CFS をディセーブルにする場合は **disable** に設定します。

（注）　CFS を使用する機能に対応したネットワーク内のすべてのスイッチ、または VSAN 内のすべてのスイッチに対して、CFS をイネーブルにします。

ステップ 3　変更した行を右クリックして、ポップアップ メニューを表示します。**Apply Changes** を選択して、CFS の設定変更を適用します。CFS の変更が有効になると、CFS タブが更新されます。

Fabric Manager が CFS の変更ステータスを受信すると、Last Result カラムを更新します。

Device Manager を使用して機能に対する CFS をイネーブルにする手順は、次のとおりです。

ステップ 1　**Admin** > **CFS**（**Cisco Fabric Services**）を選択します。

そのスイッチのすべての機能の CFS ステータスを示す CFS ダイアログボックスが表示されます。

ステップ 2　CFS が必要な機能を決定します。CFS をイネーブルにする場合は Command カラムを **enable** に、CFS をディセーブルにする場合は **disable** に設定します。

（注）　ネットワーク内のすべてのスイッチ、または CFS を使用する機能に対応した VSAN 内のすべてのスイッチに対して、CFS をイネーブルまたはディセーブルにします。

ステップ 3　**Pending Differences** をクリックして、現在のスイッチの機能の設定を、ネットワーク内の他のスイッチ、またはこの機能に対して CFS がイネーブル化されている VSAN 内の他のスイッチと比較します。Show Pending Diff ダイアログボックスを閉じます。

ステップ 4　**Apply** をクリックして、CFS 設定変更を適用します。

Device Manager は CFS の変更ステータスを取り込んで、Last Command カラムおよび Result カラムを更新します。

ネットワークのロック

CFS インフラストラクチャを使用する機能（またはアプリケーション）を初めて設定する場合、この機能は CFS セッションを開始して、ネットワークをロックします。ネットワークがロックされると、スイッチ ソフトウェアはロックを保持しているスイッチからのこの機能に対する設定変更だけを許可します。他のスイッチからこの機能に設定変更を加えると、そのスイッチはユーザにロックされたステータスににあることを通知するメッセージを発行します。設定変更は、該当アプリケーションによって保留データベースに保持されます。

ネットワークのロックが必要な CFS セッションを開始したあとに、セッションが終了されなかった場合、管理者はセッションをクリアできます。ネットワークをロックしたユーザの名前は、再起動およびスイッチオーバーを行っても保持されます。（同じマシン上で）別のユーザが設定作業を実行しようとしても、拒否されます。

変更のコミット

コミット動作はすべてのアプリケーション ピアの保留データベースを保存し、すべてのスイッチのロックを解放します。

一般に、コミット機能はセッションを開始しません。セッションを開始するのは、ロック機能のみです。ただし、設定が変更されていない場合は、空のコミットを使用できます。この場合は、コミット動作によりロックを取得し、現在のデータベースを配信するセッションが開始されます。

CFS インフラストラクチャを使用して機能に対する設定変更をコミットした場合は、次のいずれかの応答に関する通知を受信します。

- 1 つまたは複数の外部スイッチが成功ステータスを報告 — アプリケーションは変更をローカルに適用し、ネットワーク ロックを解放します。
- どの外部スイッチも成功ステートを報告しない — アプリケーションはこのステートを失敗として認識し、ネットワーク内のすべてのスイッチに変更を適用しません。ネットワーク ロックは解放されません。

指定した機能について、その機能に対する変更をコミットできます。

Fabric Manager を使用して CFS 対応機能に変更をコミットする手順は、次のとおりです。

ステップ 1　CFS をイネーブルにする機能を選択します。

たとえば、Physical Attributes ペインで **Switches** を開き、**Events** を開いてから、**CallHome** を選択します。

Information ペインに、該当する機能および CFS タブが表示されます。

ステップ 2　**CFS** タブをクリックして、ネットワーク内のスイッチごとに、該当機能の CFS ステートを表示します。

ステップ 3　任意のスイッチの Config Action カラムの値を右クリックして、ドロップダウン メニューからオプション（Copy、Paste、Export to File、Print Table、Detach Table）を選択します。

ステップ 4　**Apply Changes** アイコンをクリックして、その機能の設定変更をコミットし、CFS を通じて変更内容を配信します。

Fabric Manager は CFS の変更ステータスを取り込んで、機能または VSAN の Last Command カラムおよび Result カラムを更新します。

Device Manager を使用して CFS 対応機能に変更をコミットする手順は、次のとおりです。

ステップ 1　**Admin** > **CFS**（**Cisco Fabric Services**）を選択します。

そのスイッチのすべての機能の CFS ステータスを示す CFS ダイアログボックスが表示されます。

ステップ 2　該当機能の設定変更をコミットし、CFS を通して変更を配信する場合は、適用可能な機能ごとに、Command カラムを **commit** に設定します。該当機能に対する変更を廃棄して、この機能の CFS のネットワーク ロックを解放する場合は、Command カラムを **abort** に設定します。

ステップ 3　（任意）この情報を必要とする CFS 機能の CFS 配信基準として、**Type** または **VsanID** を提供できます。

ステップ 4　**Pending Differences** をクリックして、現在のスイッチの機能の設定を、ネットワーク内の他のスイッチ、またはこの機能に対して CFS がイネーブル化されている VSAN 内の他のスイッチと比較します。

ステップ 5　**Apply** をクリックして、CFS 設定変更を適用します。

Device Manager は CFS の変更ステータスを取り込んで、Last Command カラムおよび Result カラムを更新します。

注意　変更をコミットしない場合、変更は実行コンフィギュレーションに保存されません。

変更の廃棄

設定変更を廃棄する場合、アプリケーションは保留データベースを一度に消去し、ネットワーク内のロックを解放します。中断とコミット機能の両方を使用できるのは、ネットワーク ロックが取得されたスイッチだけです。

その機能の Command カラム値を **disable** に設定してから、**Apply** をクリックすると、指定した機能の変更を廃棄できます。

コンフィギュレーションの保存

（保留データベースにまだ存在していて）適用されていない変更内容は、実行コンフィギュレーションには表示されません。変更をコミットすると、保留データベース内の設定変更が有効なデータベースのコンフィギュレーションを上書きします。

注意　変更をコミットしない場合、変更は実行コンフィギュレーションに保存されません。

CISCO-CFS-MIB には CFS 関連機能の SNMP（簡易ネットワーク管理プロトコル）設定情報が含まれます。この MIB（管理情報ベース）の詳細については、『*Cisco Nexus 5000 Series MIB Quick Reference*』を参照してください。

ロック済みセッションのクリア

アプリケーションによって保持されているロックは、ロックが取得されたにもかかわらず解放されていない状態からネットワークを復旧するために、ネットワークの任意のスイッチから解放できます。この機能には Admin 権限が必要です。

Fabric Manager を使用してロックをクリアする手順は、次のとおりです。

ステップ 1　**CFS** タブをクリックします。

ステップ 2　ロックをクリアする各スイッチの Config Action ドロップダウン リストから **clearLock** を選択します（図 7-4 を参照）。

ステップ 3　**Apply Changes** アイコンをクリックして、変更を保存します。

図 7-4　ロックのクリア

注意　この機能を使用してネットワーク内のロックを解放する場合は、注意が必要です。ネットワーク内の全スイッチのすべての保留データベースの内容は、一度に消去されて失われます。

CFS リージョン

ここでは、次の内容について説明します。

- CFS リージョンの概要（p.7-13）
- シナリオの例（p.7-13）
- Fabric Manager を使用した CFS リージョンの管理（p.7-14）
- CFS リージョンの作成（p.7-14）
- CFS リージョンへの機能の割り当て（p.7-15）
- 別のリージョンへの機能の移動（p.7-16）
- リージョンからの機能の削除（p.7-17）
- CFS リージョンの削除（p.7-17）

CFS リージョンの概要

CFS リージョンは、物理配信スコープにおける所定の機能またはアプリケーションに対するスイッチのユーザ定義のサブセットです。ネットワークが広い範囲に及ぶ場合、物理プロキシミティに基づいてスイッチ セット間で特定のプロファイルの配信をローカライズまたは制限する必要がある場合があります。CFS リージョンを使用すると、所定の CFS 機能またはアプリケーションに対するネットワーク内の複数の配信アイランドを作成できます。CFS リージョンは、機能の設定の配信をネットワークにおけるスイッチの特定のセットまたはグループに制限するように設計されています。

（注） CFS リージョンは、物理スイッチにのみに基づいて設定できます。VSAN 内に CFS リージョンを設定することはできません。

シナリオの例

Call Home アプリケーションは、特別な状況や異常が発生したときにネットワーク管理者にアラートをトリガーするアプリケーションです。ネットワークが広い範囲に及び、ネットワーク内のスイッチのサブセットを担当するネットワーク管理者が複数存在する場合、Call Home アプリケーションは、管理者のいる場所にかかわらずすべてのネットワーク管理者にアラートを送信します。Call Home アプリケーションは、メッセージ アラートを選択してネットワーク管理者に送信するために、CFS リージョンを実装してアプリケーションの物理スコープを調整するか絞り込む必要があります。

CFS リージョンは、0 ～ 200 の範囲の番号で識別されます。リージョン 0 はデフォルトのリージョンとして予約されており、ファブリック内のすべてのスイッチを含みます。1 ～ 200 のリージョンを設定できます。デフォルトのリージョンは、下位互換性を維持します。

機能が移動され、新しいリージョンに割り当てられて、そのスコープがそのリージョンに制限される場合、配信またはマージの目的で他のすべてのリージョンを無視します。機能へのリージョンの割り当てには、初期物理スコープの配信に優先順位があります。

CFS リージョンを設定すると、複数の機能に設定を配信できます。ただし、所定のスイッチで所定の機能の設定を配信することができるのは、一度に 1 つの CFS リージョンのみです。一旦機能を割り当てた CFS リージョンは、その設定を別の CFS リージョン内に配信できなくなります。

Fabric Manager を使用した CFS リージョンの管理

ここでは、Fabric Manager を使用して、CFS リージョンを管理する方法について説明します。Fabric Manager は、すべてのスイッチ、リージョン、およびトポロジの各リージョンに関連付けられた機能の総合的ビューを提供します。次のタスクを完了するには、All Regions タブおよび Feature by Region タブの下のテーブルを使用します。

- CFS リージョンの作成（p.7-14）
- CFS リージョンへの機能の割り当て（p.7-15）
- 別のリージョンへの機能の移動（p.7-16）
- リージョンからの機能の削除（p.7-17）

CFS リージョンの作成

Fabric Manager を使用して CFS リージョンを作成する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches** を展開して、**CFS** を選択します。

Information ペインに、Global、IP Multicast、Feature by Region、および All Regions タブが表示されます。

ステップ 2　**All Regions** タブをクリックします。

タブに Switches and RegionIds のリストが表示されます。

ステップ 3　ツールバーの **Create Row** ボタンをクリックします。

図 7-5 に、Create a Region ダイアログボックスを示します。

図 7-5　Create a Region ダイアログボックス

ステップ 4　ドロップダウン リストからスイッチを選択して、範囲から RegionId を選択します。

ステップ 5　**Create** をクリックします。

リージョンが正常に作成されると、ダイアログボックスの下部に Success と表示されます。

CFS リージョンへの機能の割り当て

Fabric Manager を使用してリージョンに機能を割り当てる手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches** を展開して、**CFS** を選択します。

Information ペインに、Global、IP Multicast、Feature by Region、および All Regions タブが表示されます。

ステップ 2　**Feature by Region** タブをクリックします。

このタブは、すべてのスイッチを、対応する Feature および RegionId とともに表示します。

ステップ 3　ツールバーの **Create Row** ボタンをクリックします。

図 7-6 に、Assign a Feature ダイアログボックスを示します。

図 7-6　Assign a Feature ダイアログボックス

ステップ 4　ドロップダウン ボックスでスイッチを選択します。

選択したスイッチで実行されている機能が、Feature ドロップダウン ボックスに表示されます。

ステップ 5　そのスイッチの機能を選択して、リージョンに関連付けます。

ステップ 6　リストからリージョン番号を選択して、選択した機能に RegionId を関連付けます。

ステップ 7　**Create** をクリックすると、リージョンへのスイッチ機能の割り当てが完了します。

機能が正常に割り当てられると、ダイアログボックスの下部に Success と表示されます。

Feature by Region タブを使用して新しいリージョンに機能が割り当てられると、All Regions タブの下のテーブルに、新しいリージョンが示された新しい行が自動的に作成されます。また、All Regions タブを使用してリージョンを作成することもできます。

（注）　Feature by Region タブでは、**Create Row** をクリックしてスイッチの機能を別のリージョンに再割り当てを実行しようとすると、操作が失敗したことを示すメッセージが表示されます。このエラーメッセージは、エントリがすでに存在することを示します。別のリージョンへの機能の移動は、次のセクションで説明する別のタスクで実行できます。

別のリージョンへの機能の移動

機能を新しいリージョンに移動するには、まず All Regions タブに新しいリージョンを作成します。つまり、All Regions タブに、新しい Region ID の新しい行が追加される必要があります。

Fabric Manager を使用して別のリージョンに機能を移動する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches** を展開して、**CFS** を選択します。

Information ペインに、Global、IP Multicast、Feature by Region、および All Regions タブが表示されます。

ステップ 2　**Feature by Region** タブをクリックします。

図 7-7 は、Feature by Region タブを表示します。このタブは、機能とリージョンの詳細とともにすべてのスイッチを表示します。

図 7-7　Feature by Region タブ

ステップ 3　必要な行の RegionId セルをダブルクリックします。

値の変更をプロンプトで表示するセルでカーソルが点滅します。

ステップ 4　RegionId 値を必要なリージョンに変更します。

ステップ 5　ツールバーで **Apply Changes** ボタンをクリックして、変更をコミットします。

リージョンからの機能の削除

Fabric Manager を使用してリージョンから機能を削除する手順は、次のとおりです。

ステップ 1　**Feature by Region** タブをクリックして、必要な行をクリックします。

ステップ 2　ツールバーで **Delete Row** ボタンをクリックします。

図 7-8 に、確認ダイアログボックスを示します。

図 7-8　リージョンからの機能の削除

ステップ 3　**Yes** をクリックして、ビューのテーブルから行を削除することを確認します。

CFS リージョンの削除

リージョン全体を削除する手順は、次のとおりです。

ステップ 1　**All Regions** タブをクリックして、必要な行をクリックします。

ステップ 2　**Delete Row** をクリックします。

このアクションは、そのスイッチおよびリージョンに関連するすべてのエントリを Feature by Region タブのテーブルから削除します。

図 7-9 に、確認ダイアログボックスを示します。

図 7-9　CFS リージョンの削除

ステップ 3　**Yes** をクリックして、リージョンの削除を確認します。

（注）　CFS は同じスイッチから IPv4 と IPv6 の両方を介して配信することはできません。

CFS 配信情報の表示

Device Manager を使用してスイッチの CFS 配信のステータスを表示する手順は、次のとおりです。

ステップ 1　**Admin > CFS**（**Cisco Fabric Services**）を選択します。

CFS ダイアログボックスが表示されます。このダイアログボックスは、CFS を使用する各機能の配信ステータス（現在登録されているアプリケーションが CFS を使用しているかどうか、最後に成功したマージの結果）を表示します。

ステップ 2　行を選択し、**Details** をクリックして、機能の詳細を表示します。

Fabric Manager を使用した CFS の例

この手順は、Fabric Manager を使用して CFS を使用する機能を設定した場合に表示される内容を示した例です。

ステップ 1　設定する CFS 対応機能を選択します。

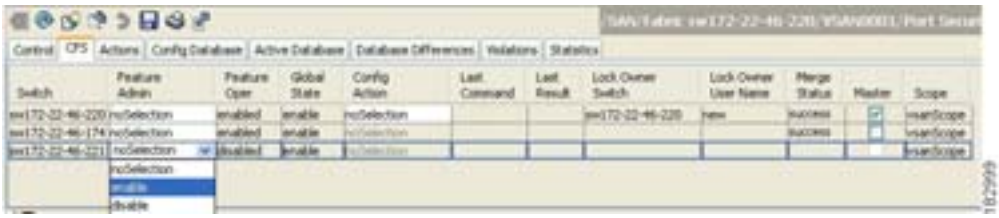
たとえば、Logical Domains ペインで **VSAN** を展開してから、**Port Security** を選択します。

Information ペインに、その VSAN のポート セキュリティ設定が表示されます。

ステップ 2　**CFS** タブをクリックします。

各スイッチの CFS の設定およびステータスが表示されます（図 7-10 を参照）。

図 7-10　CFS 設定



ステップ 3　Feature Admin ドロップダウン リストから各スイッチに対して **enable** を選択します。

ステップ 4　ネットワーク内のすべてのスイッチに対して、ステップ 3 を繰り返します。

（注）　ネットワーク内のすべてのスイッチで、現在の機能に対して CFS をイネーブルにしない場合は、警告が表示されます。

ステップ 5　この機能のマージ マスターとして機能させるスイッチの **Master** チェックボックスをオンにします。

ステップ 6　CFS をイネーブルにするスイッチごとに、Config Action ドロップダウン リストで **commit Changes** を選択します。

ステップ 7　Information ペインで、**Servers** タブをクリックします。

マスター スイッチに基づいて、この機能の設定が表示されます（図 7-11 を参照）。

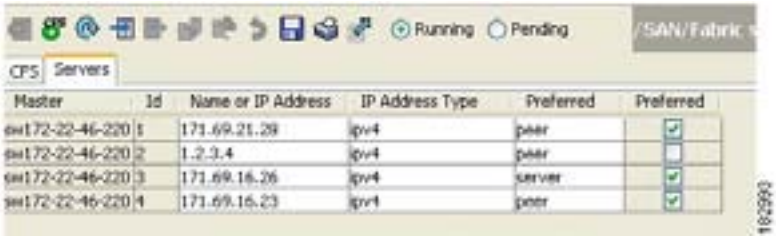
ステップ 8　機能の設定を変更します。たとえば、Master カラムの名前を右クリックし、**Create Row** を選択して、NTP 用のサーバを作成します。

a.　NTP サーバの ID および Name or IP Address を入力します。

b.　**Mode** オプション ボタンを設定し、オプションで **Preferred** チェックボックスをオンにします。

c.　**Create** をクリックして、サーバを追加します。

図 7-11　Servers タブ



ステップ 9　**Delete Row** アイコンをクリックして、行を削除します。

変更内容を加えると、ステータスが自動的に **Pending** に変わります（図 7-12 を参照）。

図 7-12　Pending へのステータス変更

ステップ 10　**Commit CFS Pending Changes** アイコンをクリックして、変更内容を保存します（図 7-13 を参照）。

図 7-13　Commit CFS Pending Changes

ステップ 11　ステータスが Running に変わります（図 7-14 を参照）。

図 7-14　Running へのステータス変更

ステップ 12 CFS をイネーブルにするスイッチごとに、Config Action ドロップダウン リストで **abortChanges** を選択します（図 7-15 を参照）。

図 7-15　設定変更のコミット

（注） **enable** を選択した場合は、Fabric Manager はステータスを pending に変更しません。最初の変更が実際に行われるまで、pending ステータスは適用されないためです。

ステップ 13 **Apply Changes** アイコンをクリックして、その機能の設定変更をコミットし、CFS を通じて変更内容を配信します。

（注） デバイス エイリアスなどの機能と CFS を併用する場合は、各設定の終了時に **commit** を選択する必要があります。セッションがロックされている場合は、**abort** を選択して、機能を終了する必要があります。

Fabric Manager を使用して機能ごとに配信用にマスターまたはシード スイッチを設定する手順は、次のとおりです。

ステップ 1 CFS に対してマージ マスターが必要な機能を選択します。

たとえば、Physical Attributes ペインで **Switches** > **Events** を展開してから、**CallHome** を選択します。

Information ペインに、CFS タブを含む該当する機能が表示されます。

ステップ 2 **CFS** タブをクリックして、ネットワーク内のスイッチごとに、該当機能の CFS ステートを表示します。

ステップ 3 この機能のマージ マスターとして機能させるスイッチの **Master column** チェックボックスをオンにします。

ステップ 4 **Apply Changes** アイコンをクリックして、今後の CFS 配信用にこのスイッチをマスターとして選択します。

Device Manager を使用した CFS の例

この手順は、Device Manager を使用して CFS を使用する機能を設定した場合に表示される内容を示した例です。CFS を使用する機能の具体的な手順については、該当する機能のマニュアルを参照してください。

Device Manager を使用して CFS を使用する機能を設定する手順は、次のとおりです。

ステップ 1　任意の CFS 対応機能のダイアログボックスを開きます。

Device Manager が CFS 対応であるかどうかを調べます。また、Owner テーブル内のエントリを最低 1 つ調べて、機能がロックされているかどうかも調べます。CFS がイネーブル化されていて、機能がロックされている場合、Device Manager はその機能のステータスを pending に設定します。ロック情報を示すダイアログボックスが表示されます。

ステップ 2　プロンプトが表示されたら、**Continue** または **Cancel** をクリックします。継続した場合は、CFS ステータスが復元されます。

ステップ 3　**Admin > CFS (Cisco Fabric Services)** を選択して、CFS ロック ホルダーのユーザ名を表示します。

ステップ 4　ロックされた機能をクリックして、**Details** をクリックします。

ステップ 5　**Owners** タブをクリックし、UserName カラムを参照します。

（注）　**Refresh** をクリックしないかぎり、Device Manager はネットワーク全体で機能のステータスをモニタしません。別の CFS 対応スイッチ上のユーザが同じ機能を設定しようとしても、pending ステータスは表示されません。ただし、そのユーザのスイッチで設定変更が拒否されます。

ステップ 6　CFS がイネーブル化されていて、機能がロックされていない場合、Device Manager はその機能のステータスを running に設定します。

その後、この機能に関するダイアログボックスが表示されます。作成、削除、または変更を実行するとすぐに、Device Manager はステータスを pending に変更して、保留データベース内の更新済み情報を表示します。

ステップ 7　機能の CFS テーブルを表示します。Device Manager がステータスを running に変更するのは、**commit**、**clear**、または **abort** を選択して、適用した場合のみです。**enable** を選択した場合は、Device Manager はステータスを pending に変更しません。最初の変更が実際に行われるまで、pending ステータスは適用されないためです。

直前のコマンドが **noOp** の場合、Last Command および Result フィールドはブランクです。

（注）　デバイス エイリアスなどの機能と CFS を併用する場合は、各設定の終了時に **commit** を選択する必要があります。セッションがロックされている場合は、**abort** を選択して、機能を終了する必要があります。

デフォルト設定

表 7-1 に、CFS 設定のデフォルト設定値を示します。

表 7-1　デフォルトの CFS パラメータ

パラメータ	デフォルト
スイッチでの CFS 配信	イネーブル
データベース変更	最初の設定変更によって暗黙的にイネーブルにされる
アプリケーションの配信	アプリケーションごとに異なる
コミット	明示的な設定が必要
IP を介した CFS	ディセーブル
IPv4 マルチキャスト アドレス	239.255.70.83
IPv6 マルチキャスト アドレス	ff15::efff:4653

CHAPTER 8

イーサネット インターフェイスの設定

ここでは、Nexus 5000 シリーズ スイッチのイーサネット インターフェイス設定について説明します。この章の内容は、次のとおりです。

- イーサネット インターフェイスの概要（p.8-2）
- イーサネット インターフェイスの設定（p.8-2）
- インターフェイス情報の表示（p.8-3）

イーサネット インターフェイスの概要

イーサネット ポートは、サーバまたは LAN に接続された標準イーサネット インターフェイスとして動作します。

イーサネット インターフェイスは、Fibre Channel over Ethernet（FCoE）もサポートします。FCoE を使用すると、物理イーサネット リンクがイーサネットとファイバ チャネル トラフィックの両方を伝送できます。

Nexus 5000 シリーズ スイッチでは、イーサネット インターフェイスがデフォルトでイネーブルです。

イーサネット インターフェイスの設定

Fabric Manager および Device Manager は、Nexus 5000 シリーズ スイッチ上の物理イーサネット インターフェイスの設定値とステータス情報を表示します。ただし、Fabric Manager または Device Manager を使用して物理イーサネット インターフェイスの設定を変更することはできません。

インターフェイス情報の表示

Fabric Manager および Device Manager は、Nexus 5000 シリーズ スイッチ上の物理イーサネット インターフェイスの設定値とステータス情報を表示します。

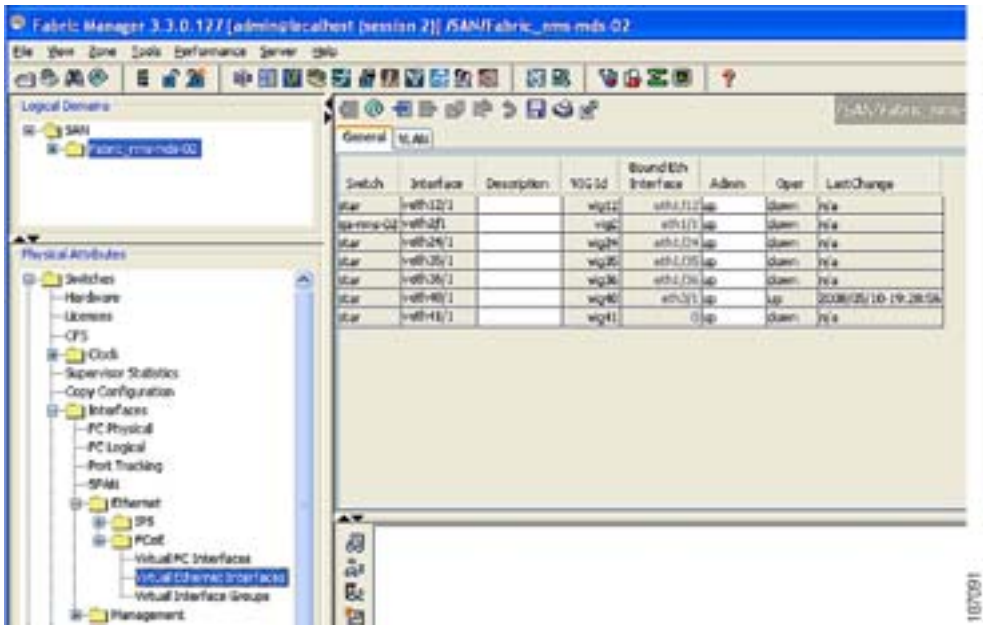
Fabric Manager を使用してイーサネット インターフェイスを表示する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches** > **Interfaces** を展開して、**Ethernet** を選択します。

Ethernet interface Information ペインが表示されます（図 8-1 を参照）。

General タブは、各インターフェイスの説明、速度、MAC アドレス、およびステータスを表示します。

図 8-1　Ethernet Information ペイン



ステップ 2　各インターフェイスに割り当てられた VLAN を表示するには、**VLAN** タブを選択します。

ステップ 3　各インターフェイスに割り当てられた CDP ネイバを表示するには、**CDP Neighbors** タブを選択します。

物理イーサネットのデフォルト設定値

次の表に、すべての物理イーサネット インターフェイスのデフォルト設定値を示します。

パラメータ	デフォルト設定値
デバウンス	イネーブル、100 ミリ秒
デュプレックス	Auto（全二重）
カプセル化	ARPA
MTU[1]	1500 バイト
ポート モード	Access
速度	Auto（10000）

1. MTU は、物理イーサネット インターフェイス単位では変更できません。MTU を変更する際は、QoS クラスのマップを選択します。

CHAPTER 9

仮想インターフェイスの設定

ここでは、Nexus 5000 シリーズ スイッチの仮想インターフェイス設定について説明します。この章の内容は、次のとおりです。

- 仮想インターフェイスの概要（p.9-1）
- 仮想インターフェイスの設定（p.9-2）

仮想インターフェイスの概要

Nexus 5000 シリーズ スイッチは、I/O Consolidation（IOC）をサポートしています。IOC では、スイッチとサーバ間の同一の物理イーサネット接続でファイバ チャネルおよびイーサネット トラフィックを伝送できます。IOC の詳細については、第 1 章「製品概要」を参照してください。

仮想インターフェイスの概念は、同一物理イーサネットで伝送される論理接続のエミュレートに使用されます。Nexus 5000 シリーズ スイッチは、仮想イーサネットおよび仮想ファイバ チャネル インターフェイスをサポートしています。

設定の目的で、仮想イーサネットまたは仮想ファイバ チャネル インターフェイスが物理イーサネット インターフェイスのレイヤ 2 サブインターフェイスとして実装されます。イーサネット インターフェイスに設定できる論理機能（VLAN や ACL など）は、それぞれの仮想イーサネット インターフェイスに設定できます。論理ファイバ チャネル機能（VSAN など）は、仮想ファイバ チャネル インターフェイスに設定できます。

（注） 仮想インターフェイスは、管理ステートが down に設定されている状態で作成されます。仮想インターフェイスを作動させるには、管理ステートを明示的に設定する必要があります。

仮想インターフェイスの設定

ここでは、仮想インターフェイスの設定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。

- VIG の作成（p.9-2）
- VIG ウィザードの使用（p.9-4）
- 物理イーサネット インターフェイスへの VIG のバインド（p.9-4）
- VIG の削除（p.9-5）
- VI ウィザードの使用（p.9-5）
- 仮想イーサネット インターフェイスの作成（p.9-6）
- 仮想イーサネット インターフェイスの削除（p.9-7）
- 仮想ファイバ チャネル インターフェイスの作成（p.9-8）
- 仮想ファイバ チャネル インターフェイスの削除（p.9-8）

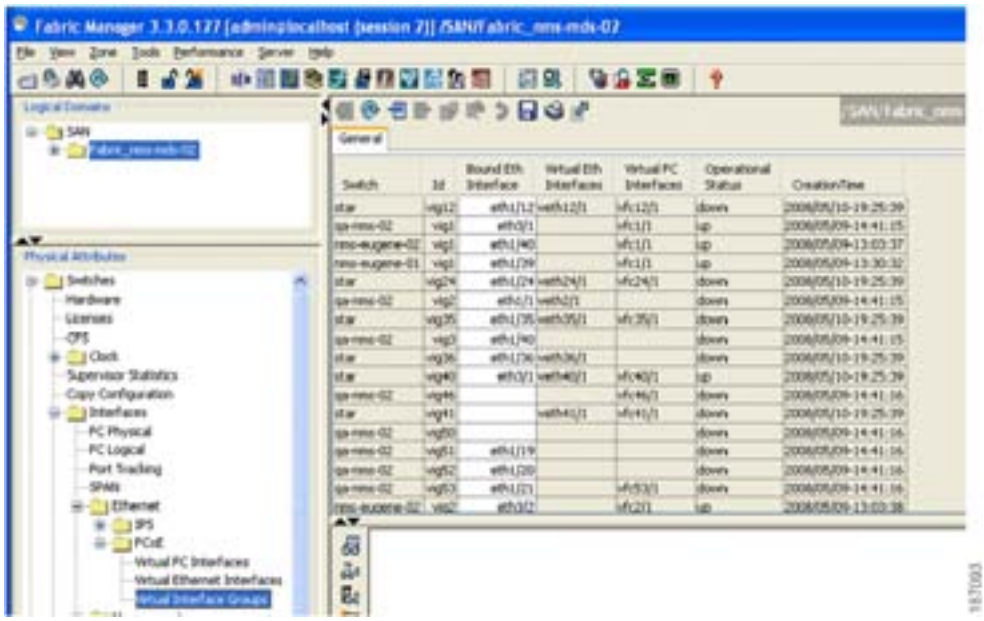
VIG の作成

Virtual Interface Group（VIG）を作成する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches** > **Interfaces** > **Ethernet** > **FCoE** を展開して、**Virtual Interface Groups** を選択します。

Information ペインに Virtual Interface Groups が表示されます（図 9-1 を参照）。

図 9-1　Virtual Interface Group Information ペイン



ステップ 2　Virtual Interface Group Information ペイン ツールバーで、**Create Row** アイコンをクリックします。

Create VIG ダイアログボックスが表示されます（図 9-2 を参照）。

図 9-2　Create VIG ダイアログボックス

ステップ 3　Switch プルダウン メニューからスイッチを選択します。

ステップ 4　Id フィールドに、VIG 番号を入力します。

ステップ 5　（任意）VIG にバインドする物理イーサネット インターフェイスを選択します。

Virtual Interface Groups テーブルに、新しく作成した VIG が表示されます。Create Virtual Interface Group ダイアログボックスの Id フィールドが 1 ずつ増加します。

ステップ 6　（任意）さらに VIG を作成するには、ステップ 3 ～ 6 を繰り返します。

ステップ 7　**Close** をクリックして、終了します。

VIG ウィザードの使用

VIG ウィザードを使用して VIG を作成する手順は、次のとおりです。

ステップ 1　ツールバーで **Virtual Interface Group** ボタンをクリックします。

Virtual Interface Group ウィザード ダイアログボックスが表示されます（図 9-3 を参照）。

図 9-3　Virtual Interface Group ウィザード

ステップ 2　Virtual Interface Group ウィザード の指示に従います。VIG が作成されるスイッチ、VIG に関連付けられる物理イーサネット ポート、および VIG ID を選択します。

ステップ 3　**Finish** をクリックして、その変更をコミットして配信します。

物理イーサネット インターフェイスへの VIG のバインド

物理イーサネット ポートに VIG をバインドする手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches** > **Interfaces** > **Ethernet** > **FCoE** を展開して、**Virtual Interface Groups** を選択します。

Information ペインに Virtual Interface Groups が表示されます（図 9-1 を参照）。

ステップ 2　変更する必要がある VIG の **Bound Eth Interface** エントリをクリックします。物理インターフェイスを入力します。

ステップ 3　**Apply Changes** をクリックして、その変更をコミットして配信します。

VIG の削除

VIG を削除する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches** > **Interfaces** > **Ethernet** > **FCoE** を展開して、**Virtual Interface Groups** を選択します。

Information ペインに Virtual Interface Groups が表示されます（図 9-1 を参照）。

ステップ 2　削除する VIG を選択します。

ステップ 3　**Delete Row** アイコンをクリックします。

削除を確認するダイアログボックスが表示されます。

ステップ 4　削除するには、**Yes** をクリックします。

ステップ 5　**Apply** アイコンをクリックして、変更を適用します。

.

VI ウィザードの使用

ステップ 1　ツールバーで **Virtual Interface** ボタンをクリックします。

Virtual Interface Wizard ダイアログボックスが表示されます（図 9-4 を参照）。

図 9-4　Virtual Interface ウィザード

ステップ 2　Virtual Interface ウィザード の指示に従います。Virtual Interface（VI）が作成されるスイッチ、VI を含める VIG を選択し、VI タイプ（イーサネットまたはファイバ チャネル）を指定します。ウィザードは、VI ID を 1 に設定します。

ステップ 3　**Finish** をクリックして、その変更をコミットして配信します。

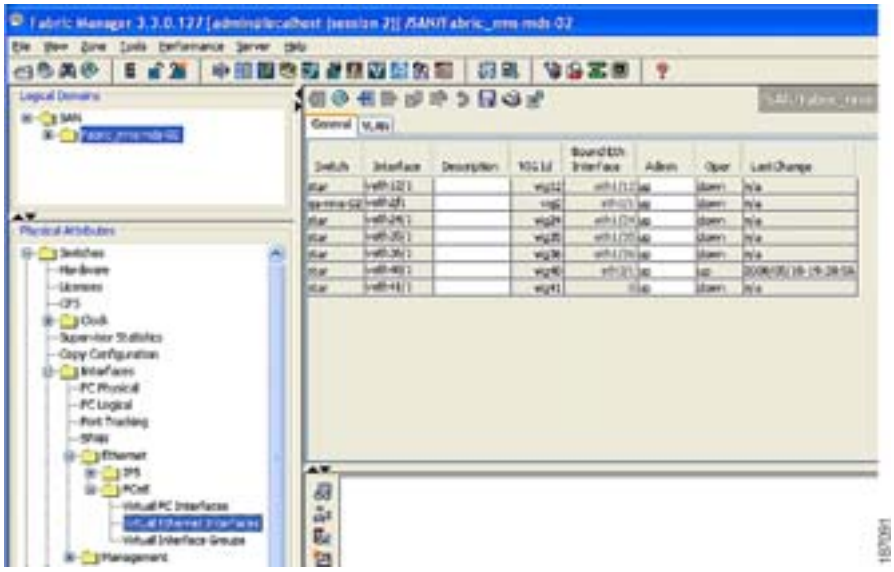
仮想イーサネット インターフェイスの作成

仮想イーサネット インターフェイスを作成する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches**、**Interfaces**、**Ethernet**、**FCoE**、**Virtual Interfaces** の順に展開して、**Ethernet** を選択します。

Virtual Ethernet Information ペインが表示されます（図 9-5 を参照）。

図 9-5　Virtual Ethernet



ステップ 2　Information ペイン ツールバーで、**Create Row** アイコンをクリックします。

Virtual Ethernet ダイアログボックスが表示されます（図 9-6 を参照）。

図 9-6　仮想イーサネットの作成

ステップ 3　Switch プルダウン メニューからスイッチを選択します。

ステップ 4　VIG ID フィールドに、VIG ID を入力します。VI ID は、1 に設定されます。

ステップ 5　**Create** をクリックします。

ステップ 6　Apply アイコンをクリックして、変更を適用します。

仮想イーサネット インターフェイスの削除

仮想イーサネット インターフェイスを削除する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches** > **Interfaces** > **Ethernet** > **FCoE** を展開して、**Virtual Ethernet Interfaces** を選択します。

Virtual Ethernet Information ペインが表示されます（図 9-5 を参照）。

ステップ 2　Information ペインの Virtual Ethernet の行を選択します。

ステップ 3　Information ペイン ツールバーで、**Delete Row** アイコンをクリックします。

ステップ 4　ダイアログボックスで削除を確認します。

仮想ファイバ チャネル インターフェイスの作成

仮想ファイバ チャネル インターフェイスを作成する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches** > **Interfaces** > **Ethernet** > **FCoE** を展開して、**Virtual FC Interfaces** を選択します。

ステップ 2　Information ペイン ツールバーで、**Create Row** アイコンをクリックします。

Virtual Ethernet ダイアログボックスが表示されます（図 9-7 を参照）。

図 9-7　仮想ファイバ チャネルの作成

ステップ 3　Switch プルダウン メニューからスイッチを選択します。

ステップ 4　VIG ID フィールドに、VIG ID を入力します。インターフェイス ID は、1 の値に設定されています。

ステップ 5　**Create** をクリックします。

仮想ファイバ チャネル インターフェイスの削除

仮想ファイバ チャネル インターフェイスを削除する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches** > **Interfaces** > **Ethernet** > **FCoE** を展開して、**Virtual FC Interfaces** を選択します。

Virtual Fibre Channel Information ペインが表示されます。

ステップ 2　Information ペインの仮想ファイバ チャネルの行を選択します。

ステップ 3　Information ペイン ツールバーで、**Delete Row** アイコンをクリックします。

ステップ 4　ダイアログボックスで削除を確認します。

CHAPTER 10

ファイバ チャネル インターフェイスの設定

この章では、ファイバ チャネル インターフェイスおよび仮想ファイバ チャネル インターフェイスの設定について説明します。この章の内容は、次のとおりです。

- ファイバ チャネル インターフェイスの概要（p.10-2）
- ファイバ チャネル インターフェイスの設定（p.10-9）
- ファイバ チャネル インターフェイスの確認（p.10-14）
- デフォルト設定（p.10-16）

ファイバ チャネル インターフェイスの概要

ここでは、ファイバ チャネル インターフェイスおよび仮想ファイバ チャネル インターフェイス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。

- ライセンスの要件（p.10-2）
- 物理ファイバ チャネル インターフェイス（p.10-2）
- 仮想ファイバ チャネル インターフェイス（p.10-2）
- インターフェイス モード（p.10-3）
- インターフェイス ステート（p.10-5）
- BB_credit（p.10-8）

ライセンスの要件

Nexus 5000 シリーズ スイッチでは、ファイバ チャネルの機能がストレージ プロトコル サービス ライセンスに含まれています。

ファイバ チャネル インターフェイスおよびその機能を使用する前に、正しいライセンス（N5010SS または N5020SS）がインストールされていることを確認してください。

物理ファイバ チャネル インターフェイス

Nexus 5000 シリーズ スイッチは、最大 8 つの物理ファイバ チャネル アップリンクを提供します。ファイバ チャネル インターフェイスは、オプションの拡張モジュールでサポートされています。Fibre Channel plus Ethernet 拡張モジュールには、4 つのファイバ チャネル インターフェイスが含まれています。

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

仮想ファイバ チャネル インターフェイス

Fibre Channel over Ethernet（FCoE）カプセル化を使用すると、物理イーサネット ケーブルでファイバ チャネルおよび Classic Ethernet（CE）トラフィックを同時に伝送できます。Nexus 5000 シリーズ スイッチでは、FCoE 対応物理イーサネット インターフェイスは、1 つの論理 CE インターフェイスおよび 1 つの論理ファイバ チャネル インターフェイスのトラフィックを伝送できます。Nexus 5000 シリーズ スイッチでは、論理インターフェイスが仮想インターフェイスとして設定されています。仮想ファイバ チャネル インターフェイスは、論理ファイバ チャネル インターフェイスを表します。

仮想ファイバ チャネルは、Virtual Interface Group（VIG）のサブインターフェイスとして設定されます。

仮想ファイバ チャネル インターフェイスは F モードのみをサポートし、物理ファイバ チャネル インターフェイスでサポートされている機能のサブセットを提供します。

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

- SAN ポート チャネル
- VSAN トランキング。仮想ファイバ チャネルは、1 つの VSAN に関連付けられます。
- SPAN 宛先を仮想ファイバ チャネル インターフェイスにすることはできません。
- Buffer-to-Buffer credit（BB_credit）

- Exchange Link Parameter（ELP）または Fabric Shortest Path First（FSPF）プロトコル
- Physical Attributes（速度、レート、モード、トランスミッタ情報、MTU サイズ）の設定
- ポート トラッキング

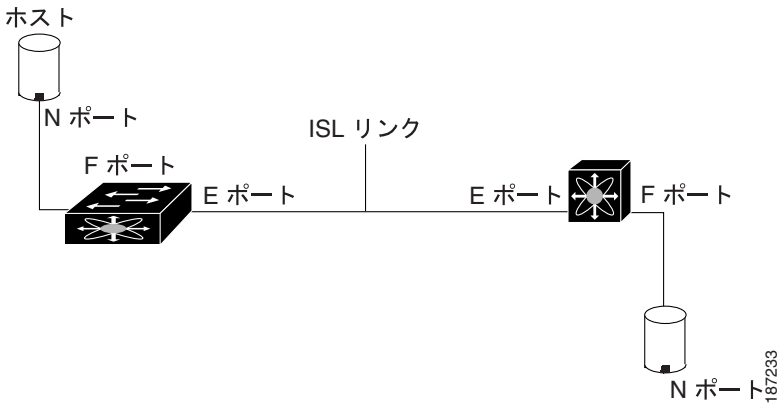
インターフェイス モード

スイッチ内の各物理ファイバ チャネル インターフェイスは、E ポート、TE ポート、F ポート、および SD ポートのいずれか 1 つで動作することができます（図 10-1 を参照）。物理ファイバ チャネルインターフェイスは、E ポート、F ポート、または SD ポートとして設定できます。インターフェイスは、Auto モードにも設定できます。ポート タイプは、インターフェイスの初期化中に判別されます。

NPV モードでは、ファイバ チャネル インターフェイスは NP モード、F モード、または SD モードとして動作できます。NPV モードの詳細については、第 12 章「N ポート バーチャライゼーションの設定」を参照してください。

仮想ファイバ チャネル インターフェイスは、F モードにのみ設定できます。

図 10-1　スイッチ ポートのモード



（注） インターフェイスには、デフォルトで VSAN 1 が自動的に割り当てられます。第 15 章「VSAN の設定と管理」を参照してください。

各インターフェイスには、管理設定と動作ステータスが対応付けられています。

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

ここでは、各インターフェイス モードについて簡単に説明します。

- E ポート（p.10-4）
- F ポート（p.10-4）
- NP ポート（p.10-4）

- TE ポート（p.10-4）
- SD ポート（p.10-5）
- Auto モード（p.10-5）

E ポート

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

別のスイッチに接続された E ポートも、SAN ポート チャネルを形成するように設定できます（第 14 章「SAN ポート チャネルの設定」を参照）。

F ポート

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

NP ポート

NP ポートは、NPV モードになっているデバイスのポートであり、F ポートでコア NVP スイッチに接続されます。NP ポートは、複数の物理 N ポートのプロキシとして機能する N ポートのように動作します。

NP ポートおよび NPV の詳細については、第 12 章「N ポート バーチャライゼーションの設定」を参照してください。

TE ポート

トランキング E ポート（TE ポート）モードでは、インターフェイスがトランキング拡張ポートとして機能します。別の TE ポートに接続し、2 つのスイッチ間で Extended ISL（EISL）を作成することができます。TE ポートは別の Nexus 5000 シリーズ スイッチまたは Cisco MDS 9000 ファミリ スイッチに接続されます。TE ポートは E ポートの機能を拡張して、次の内容をサポートします。

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

TE ポート モードでは、すべてのフレームが VSAN 情報を含む EISL フレーム形式で送信されます。相互接続されたスイッチは VSAN ID を使用して、1 つまたは複数の VSAN からのトラフィックを同一の物理リンク上で多重化します。この機能を Nexus 5000 シリーズでは VSAN トランキングと呼びます（第 13 章「VSAN トランキングの設定」を参照）。TE ポートは、クラス 3 とクラス F サービスをサポートします。

SD ポート

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

Auto モード

Auto モードに設定されたインターフェイスは、F ポート、E ポート、および TE ポートのいずれかのモードで動作できます。ポート モードは、インターフェイスの初期化中に判別されます。たとえば、インターフェイスがノード（ホストまたはディスク）に接続されている場合は、F ポート モードで動作します。インターフェイスがサードパーティ製のスイッチに接続されている場合、E ポート モードで動作します。インターフェイスが Nexus 5000 シリーズ または Cisco MDS 9000 ファミリの別のスイッチに接続されている場合、TE ポート モードとして動作します（第 13 章「VSAN トランキングの設定」を参照）。

SD ポートは初期化中に判別されず、管理上設定されます。

インターフェイス ステート

インターフェイス ステートは、インターフェイスの管理設定および物理リンクのダイナミック ステートによって異なります。ここでは、ステートおよびステートに影響する設定について説明します。

- 管理ステート（p.10-6）
- 動作ステート（p.10-6）
- 原因コード（p.10-6）

管理ステート

管理ステートは、インターフェイスの管理設定を表します。表 10-1 で、管理ステートについて説明します。

表 10-1　管理ステート

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

動作ステート

動作ステートは、インターフェイスの現在の動作ステートを示します。表 10-2 で、動作ステートについて説明します。

表 10-2　動作ステート

動作ステート	説明
Up	インターフェイスは、要求に沿ってトラフィックを送受信しています。このステートにするためには、インターフェイスが管理上アップの状態、インターフェイス リンク レイヤ ステートがアップの状態で、インターフェイスの初期化が完了している必要があります。
Down	インターフェイスが（データ）トラフィックを送信または受信することができません。
トランキング	インターフェイスが TE ポートで正常に動作しています。

原因コード

原因コードは、インターフェイスの動作ステートによって異なります。表 10-3 で、動作ステートの原因コードについて説明します。

表 10-3　インターフェイスのステートの原因コード

管理設定	動作ステート	原因コード
Up	Up	なし
Down	Down	管理上のダウン。管理のためにインターフェイスをダウンとして設定すると、インターフェイスはディセーブルになります。トラフィックは送受信されません。
Up	Down	表 10-4 を参照してください。

（注） 表 10-4 には一部の原因コードのみが記載されています。

管理ステートが Up、動作ステートが Down の場合、原因コードは非動作原因コードによって異なります。表 10-4 に、非動作の原因コードの説明を示します。

表 10-4　非動作ステートの原因コード

原因コード（長いバージョン）	説明	適用可能なモード
Link failure or not connected	物理層リンクが正常に動作していません。	すべて
SFP not present	Small Form-Factor Pluggable（SFP; 着脱可能小型フォーム ファクタ）ハードウェアが接続されていません。	
Initializing	物理層リンクが正常に動作しており、プロトコル初期化が進行中です。	
Reconfigure fabric in progress	ファブリックが現在再設定されています。	
Offline	スイッチ ソフトウェアは指定された R_A_TOV 時間だけ待機してから、初期化を再試行します。	
Inactive	インターフェイスの VSAN が削除されているか、suspended ステートです。 インターフェイスを正常に動作させるには、設定済みのアクティブな VSAN にポートを割り当てます。	
Hardware failure	ハードウェア障害が検出されました。	
Error disabled	エラー条件は、管理上の注意を必要とします。さまざまな理由でインターフェイスがエラーディセーブルになります。たとえば、 • 設定障害 • 互換性のない BB_credit 設定 インターフェイスを動作させるには、最初にこのステートの原因となるエラー条件を修正してから、インターフェイスを管理上のシャット ダウン状態またはイネーブル状態にします。	
Isolation because limit of active port channels is exceeded.	スイッチがすでにアクティブ SAN ポート チャネルの最大数で設定されているため、インターフェイスが分離されています。	
Isolation due to ELP failure	ポートのネゴシエーションに失敗しました。	E ポートおよび TE ポートのみ
Isolation due to ESC failure	ポートのネゴシエーションに失敗しました。	
Isolation due to domain overlap	Fibre Channel Domain（fcdomain）が重複しています。	
Isolation due to domain ID assignment failure	割り当てられたドメイン ID が無効です。	
Isolation due to the other side of the link E port isolated	リンクの他端の E ポートが分離されています。	
Isolation due to invalid fabric reconfiguration	ファブリックの再設定によりポートが分離されました。	
Isolation due to domain manager disabled	fcdomain 機能がディセーブルです。	
Isolation due to zone merge failure	ゾーン結合に失敗しました。	
Isolation due to VSAN mismatch	ISL の両端で VSAN が異なります。	

表 10-4　非動作ステートの原因コード（続き）

原因コード（長いバージョン）	説明	適用可能なモード
port channel administratively down	SAN ポート チャネルに所属するインターフェイスがダウンの状態です。	SAN ポート チャネル インターフェイスのみ
Suspended due to incompatible speed	SAN ポート チャネルに所属するインターフェイスに互換性のない速度が存在します。	
Suspended due to incompatible mode	SAN ポート チャネルに所属するインターフェイスに互換性のないモードが存在します。	
Suspended due to incompatible remote switch WWN	不適切な接続が検出されました。SAN ポート チャネルのすべてのインターフェイスが同じスイッチ ペアに接続されている必要があります。	

BB_credit

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

Nexus 5000 シリーズ スイッチでは、ファイバ チャネル インターフェイスで BB_credit メカニズムが使用されますが、仮想ファイバ チャネル インターフェイスでは使用されません。仮想ファイバ チャネル インターフェイスは、基盤となる物理イーサネット インターフェイスの機能に基づいたフロー制御を提供します。

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

（注） receive BB_credit 値は、ポート モードによって次のように決まります。

- 物理ファイバ チャネル インターフェイスの場合、デフォルト値は F モードおよび E モードのインターフェイスで 16 です。この値は必要に応じて変更できます。最大値は、64 です。
- 仮想ファイバ チャネル インターフェイスの場合、BB_credits は使用されません。

ファイバ チャネル インターフェイスの設定

ここでは、ファイバ チャネル インターフェイスの設定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。

- ファイバ チャネル インターフェイスの設定（p.10-9）
- インターフェイスの管理ステートの設定（p.10-10）
- インターフェイス モードの設定（p.10-10）
- インターフェイスの説明の設定（p.10-11）
- 管理速度の設定（p.10-11）
- SD ポートのフレーム カプセル化の設定（p.10-12）
- 受信データ フィールド サイズの設定（p.10-12）
- ビット エラーしきい値の概要（p.10-13）
- BB_credit の設定（p.10-13）

ファイバ チャネル インターフェイスの設定

ネイティブ ファイバ チャネル インターフェイスは、Fabric Manager を使用して、Physical Attributes ペインから **Switches** > **Interfaces** > **FC Physical** を展開して設定します。

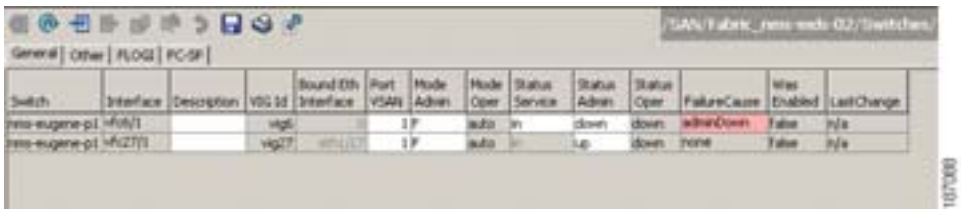
図 10-2 に、ファイバ チャネル インターフェイスの Information ペインの例を示します。

図 10-2　ネイティブ ファイバ チャネル インターフェイスの設定

仮想ファイバ チャネル インターフェイスは、Fabric Manager を使用して、Physical Attributes ペインから **Switches** > **Interfaces** > **Ethernet** > **FCoE** > **Virtual FC Interfaces** を展開して設定します。

図 10-3 に、仮想ファイバ チャネル インターフェイスの Information ペインの例を示します。

図 10-3　仮想ファイバ チャネル インターフェイスの設定



インターフェイスの管理ステートの設定

Fabric Manager を使用してインターフェイス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。

ステップ 1　Physical Attributes ペインで、**Switches > Interfaces** を展開して、**FC Physical** を選択します。仮想ファイバ チャネル インターフェイスで、**Switches > Interfaces > Ethernet > FCoE** > **Virtual FC Interfaces** を展開します。

Information ペインにインターフェイス設定が表示されます。

ステップ 2　**General** タブをクリックします。

ステップ 3　**Status Admin** をクリックします。

ドロップダウン ボックスでアップまたはダウンの選択肢を確認します。

ステップ 4　ステータスをダウン（ディセーブル）またはアップ（イネーブル）に設定します。

ステップ 5　**Apply Changes** をクリックします。

インターフェイス モードの設定

Fabric Manager を使用してインターフェイス モードを設定する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches > Interfaces** を展開して、**FC Physical** を選択します。仮想ファイバ チャネル インターフェイスで、**Switches > Interfaces > Ethernet** > **FCoE** > **Virtual FC Interfaces** を展開します。

Information ペインにインターフェイス設定が表示されます。

ステップ 2　**General** タブをクリックします。

ステップ 3　**Mode Admin** をクリックします。目的のモードをプルダウン リストから選択します。

ステップ 4　**Apply Changes** アイコンをクリックします。

インターフェイスの説明の設定

インターフェイスの説明により、トラフィック、またはインターフェイスの使用を識別できるようになります。インターフェイスの説明は、任意の英数字の文字列にすることができます。

Fabric Manager を使用してインターフェイスを設定する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches > Interfaces** を展開して、**FC Physical** を選択します。仮想ファイバ チャネル インターフェイスで、**Switches > Interfaces > Ethernet > FCoE** > **Virtual FC Interfaces** を展開します。

Information ペインにインターフェイス設定が表示されます。

ステップ 2　**General** タブをクリックします。

ステップ 3　**Description** をクリックします。目的のテキストを入力します。

ステップ 4　（任意）その他のタブを使用して、その他の設定パラメータを設定します。

ステップ 5　**Apply Changes** アイコンをクリックします。

管理速度の設定

管理速度を、物理ファイバ チャネル インターフェイスに設定できます（仮想ファイバ チャネル インターフェイスには設定できません）。デフォルトの場合、インターフェイスの管理速度はスイッチによって自動的に計算されます。

注意　管理 速度の変更は、混乱が生じる操作です。

Fabric Manager を使用してインターフェイスの管理速度を設定する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches > Interfaces** を展開して、**FC Physical** を選択します。

Information ペインにインターフェイス設定が表示されます。

ステップ 2　**General** タブをクリックします。

ステップ 3　**Speed Admin** をクリックします。目的の速度をドロップダウン リストから設定します。

数値は、1 秒あたりのメガビット（Mbps）単位の速度を示しています。速度は、1 Gbps、2 Gbps、4 Gbps、**auto**（デフォルト）のうちいずれかに設定できます。

ステップ 4　**Apply Changes** をクリックします。

自動検知

速度の自動検知は、すべての 4 Gbps インターフェイスにおいてデフォルトでイネーブルです。インターフェイスは、この設定により、4 Gbps ポートにおいて、1 Gbps、2 Gbps、4 Gbps のいずれかの速度で動作できるようになります。専用レート モードで動作するインターフェイスで自動検知をイネーブルにすると、ポートが 1 Gbps または 2 Gbps の動作速度でネゴシエーションしていても、4 Gbps の帯域幅が予約されます。

SD ポートのフレーム カプセル化の設定

SD ポート モードのインターフェイスで送信されるすべてのフレームには、フレーム形式を EISL に設定できます。フレームのカプセル化を EISL に設定すると、すべての発信フレームは、すべての SPAN ソースに EISL フレーム形式で送信されます。

インターフェイスにおけるフレームのカプセル化の設定については、『*Cisco Nexus 5000 Series Family CLI Configuration Guide*』を参照してください。

受信データ フィールド サイズの設定

ネイティブ ファイバ チャネル インターフェイスに受信データ フィールド サイズを設定することもできます（仮想ファイバ チャネル インターフェイスには設定できません）。デフォルト データ フィールド サイズが 2112 バイトである場合、フレームの長さは 2148 バイトになります。

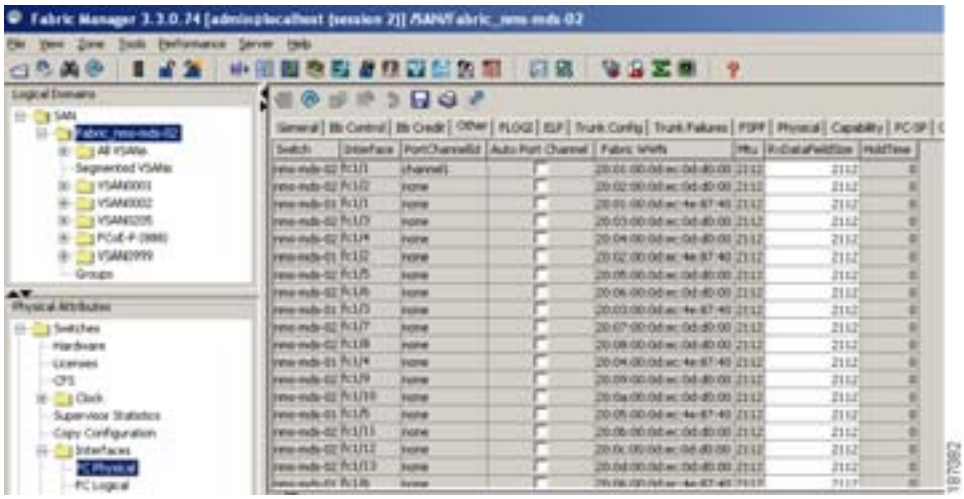
Fabric Manager を使用して受信データ フィールド サイズを設定する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches** > **Interfaces** を展開して、**FC Physical** を選択します。

Information ペインにインターフェイス設定が表示されます。

ステップ 2　**Other** タブをクリックし、**RxDataFieldSize** フィールドを設定します（図 10-4 を参照）。

図 10-4　Rx データ サイズの変更



ステップ 3　**Apply Changes** をクリックします。

ビット エラーしきい値の概要

スイッチはビット エラー レートしきい値を使用し、パフォーマンスの低下がトラフィックに深刻に影響する前に、エラー レートの上昇を検出します。

ビット エラーは、次の理由で発生することがあります。

- ケーブル不良。
- GBIC または SFP の不良。
- 1 Gbps で動作するように GBIC または SFP が指定されているが、2 Gbps で使用されている。
- 2 Gbps で動作するように GBIC または SFP が指定されているが、4 Gbps で使用されている。
- 長距離に短距離ケーブルが使用されているか、短距離に長距離ケーブルが使用されている。
- 一時的な同期の喪失。
- 片側または両側でケーブルの接続が緩んでいる。
- 片側または両側で GBIC または SFP の接続が不適切である。

5 分間に 15 のエラー バーストが発生すると、ビット エラー レートしきい値が検出されます。デフォルトの場合、しきい値に達すると、インターフェイスはスイッチによってディセーブルになります。インターフェイスは再びイネーブルにすることができます。

しきい値を超えてもインターフェイスをディセーブルにしないように、スイッチを設定できます。

インターフェイスのビット エラーしきい値のディセーブル化については、『*Cisco Nexus 5000 Series CLI Configuration Guide*』を参照してください。

（注） インターフェイスがビットエラーしきい値イベントでディセーブル化されないように設定されていても、スイッチはビットエラーしきい値イベントを検出すると、Syslog メッセージを生成します。

BB_credit の設定

BB_credit スキームは、仮想ファイバ チャネル インターフェイスでは使用されていません。Fabric Manager を使用してネイティブ ファイバ チャネル インターフェイス用に BB_credit を設定する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches > Interfaces** を展開して、**FC Physical** を選択します。

Information ペインにインターフェイス設定が表示されます。

ステップ 2　**Bb Credit** タブを選択します。

バッファ クレジットが表示されます。

ステップ 3　インターフェイスに BB_credit を設定します。

ステップ 4　**Apply Changes** をクリックします。

ファイバ チャネル インターフェイスの確認

ここでは、ファイバ チャネル インターフェイスを表示するコマンドについて説明します。

- SFP トランスミッタ タイプの確認（p.10-14）
- インターフェイスの統計情報の収集（p.10-14）

SFP トランスミッタ タイプの確認

SPF トランスミッタ タイプを物理ファイバ チャネル インターフェイスで表示できます（仮想ファイバ チャネルでは表示できません）。

SFP ハードウェア トランスミッタは略語で表示されます。

Fabric Manager を使用してインターフェイスの SFP タイプを表示する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches** > **Interfaces** を展開して、**FC Physical** を選択します。

Information ペインにインターフェイス設定が表示されます。

ステップ 2　**Physical** タブをクリックして、選択したインターフェイスの送信タイプを設定します。

インターフェイスの統計情報の収集

Fabric Manager または Device Manager を使用し、任意のスイッチでインターフェイスの統計情報を収集できます。この統計情報を収集する間隔はユーザによる設定が可能です。

（注）　Fabric Manager では、**Switches** > **ISLs** と展開して Physical Attributes ペインから **Statistics** を選択し、インターフェイスの統計情報を収集できます。

Device Manager を使用してインターフェイス カウンタを収集して表示する手順は、次のとおりです。

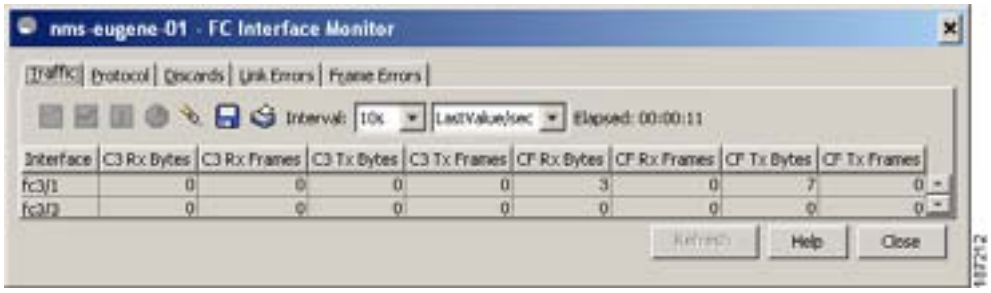
ステップ 1　Interface メニューでインターフェイスを右クリックして、**Monitor** を選択し、**Ethernet Enabled** または **FC Enabled** を選択します。

Interface Monitor ダイアログボックスが表示されます。

ステップ 2　インターフェイスの統計情報を収集する秒数、およびデータの表現方法を Interval ドロップダウンメニューで設定します。たとえば、**10s** と **LastValue/sec** をクリックします。

ステップ 3　関連統計情報を表示するには、図 10-5 に示す任意のタブをクリックします。

図 10-5　Device Manager FC Interface Monitor ダイアログボックス



ステップ 4　（任意）累積カウンタをリセットするには、**Pencil** アイコンをクリックします。

ステップ 5　（任意）収集された統計情報をファイルに保存するには、**Save** アイコンをクリックします。統計情報を印刷するには、**Print** アイコンをクリックします。

ステップ 6　統計情報の収集と表示が終わったら、**Close** をクリックします。

デフォルト設定

表 10-5 に、ネイティブ ファイバ チャネル インターフェイス パラメータのデフォルト設定の一覧を示します。

表 10-5　ファイバ チャネル インターフェイス パラメータのデフォルト

パラメータ	デフォルト
インターフェイス モード	Auto
インターフェイス速度	Auto
管理ステート	シャットダウン（初期設定中に変更しない場合）
トランク モード	オン（初期設定中に変更しない場合）
トランク許可 VSAN	1 ～ 4093
インターフェイス VSAN	デフォルト VSAN（1）
ビーコン モード	オフ（ディセーブル）
EISL カプセル化	ディセーブル
データ フィールド サイズ	2112 バイト

表 10-6 に、仮想ファイバ チャネル インターフェイス パラメータのデフォルト設定の一覧を示します。

表 10-6　仮想ファイバ チャネル インターフェイス パラメータのデフォルト

パラメータ	デフォルト
インターフェイス モード	Auto
インターフェイス速度	なし
管理ステート	シャットダウン（初期設定中に変更しない場合）
トランク モード	なし
トランク許可 VSAN	なし
インターフェイス VSAN	デフォルト VSAN（1）
EISL カプセル化	なし
データ フィールド サイズ	なし

CHAPTER 11

ドメイン パラメータの設定

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

注意 fcdomain パラメータを毎日変更しないでください。このような変更は、管理者や、スイッチの動作に精通した担当者が実行してください。

ヒント 設定の変更時には、実行コンフィギュレーションを保存してください。次回スイッチをリブートすると、保存した設定が使用されます。設定を保存しないと、以前保存したスタートアップ コンフィギュレーションが使用されます。

この章の内容は、次のとおりです。

- ファイバ チャネル ドメインの概要（p.11-2）
- ドメイン ID（p.11-9）
- FC ID（p.11-18）
- fcdomain の統計情報の表示（p.11-24）
- デフォルト設定（p.11-24）

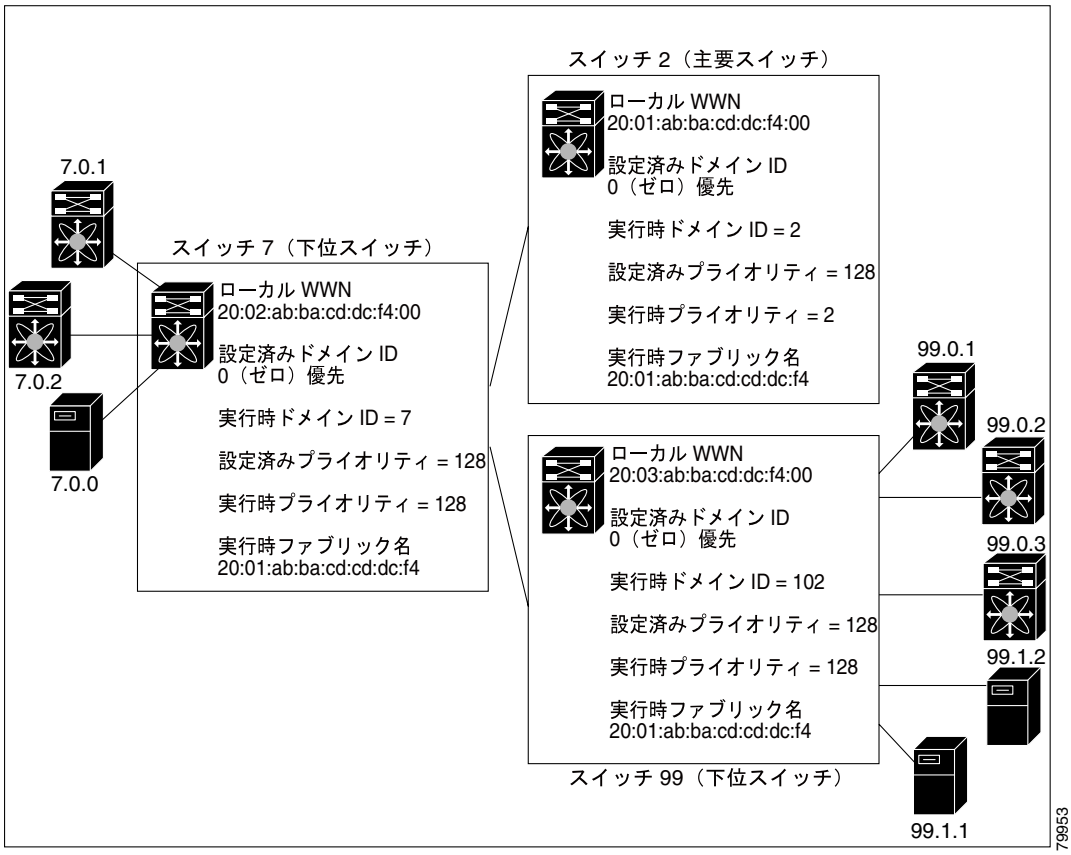
ファイバ チャネル ドメインの概要

ここでは、fcdomain の各フェーズについて説明します。

- 主要スイッチ選択 — このフェーズでは、ファブリックで一意の主要スイッチが選択されます。
- ドメイン ID 配信 — このフェーズでは、ファブリックの各スイッチが一意のドメイン ID を取得します。
- FC ID 割り当て — このフェーズでは、ファブリックで対応するスイッチに接続されている各デバイスに、一意の FC ID が割り当てられます。
- ファブリック再設定 — このフェーズでは、ファブリックのすべてのスイッチが再同期され、すべてのスイッチが新しいスイッチ選択フェーズを同時に再開します。

fcdomain の設定例については、図 11-1 を参照してください。

図 11-1　fcdomain の設定例



（注） すべての手順で使用するドメイン ID および VSAN の値は例にすぎません。設定に合った ID および値を使用してください。

ここでは、fcdomain の機能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。

- ドメインの再起動の概要（p.11-3）
- ドメインの再起動（p.11-4）
- スイッチ プライオリティの概要（p.11-5）
- スイッチ プライオリティの設定（p.11-5）
- fcdomain の初期化の概要（p.11-5）
- fcdomain のイネーブル化またはディセーブル化（p.11-6）
- ファブリック名の設定（p.11-6）
- 着信 RCF の概要（p.11-7）
- 着信 RCF の拒否（p.11-7）
- 結合ファブリックの自動再構成の概要（p.11-8）
- 自動再構成のイネーブル化（p.11-8）

ドメインの再起動の概要

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

ドメイン ID の矛盾を解決するためには、ドメイン ID を手動で割り当てる必要があります。ドメイン ID の手動割り当ても含む多くの設定変更を適用するには、中断を伴う再起動が必要です。中断を伴わないドメインの再起動は、優先ドメイン ID をスタティック ID に変更する（実際のドメイン ID は変更されない）ときに限って許容されます。

（注） ユーザがスタティック ドメインを具体的に設定しますが、スタティック ドメインはランタイム ドメインと異なることがあります。ドメイン ID が異なる場合は、次の中断を伴う再起動または中断を伴わない再起動のあとで、ランタイム ドメイン ID がスタティック ドメイン ID に変更されます。

ヒント VSAN が INTEROP モードである場合は、その VSAN の fcdomain で中断を伴う再起動を実行できません。

対応するランタイム値に設定の多くを適用できます。後続の各セクションで、fcdomain パラメータをランタイム値に適用する方法について詳しく説明します。

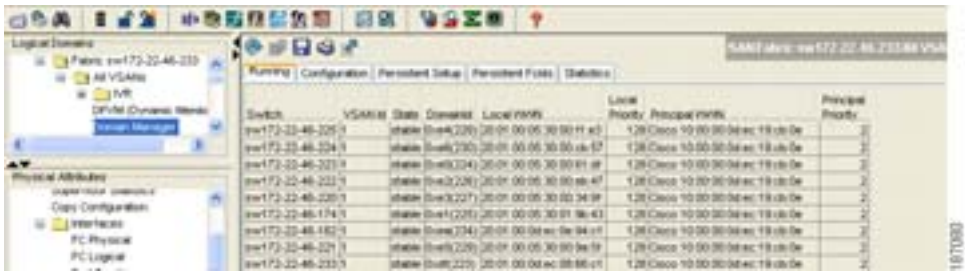
ドメインの再起動

Fabric Manager を使用して中断を伴うファブリックの再起動、または中断を伴わない再起動を行う手順は次のとおりです。

ステップ 1　**Fabric*xx*** > **VSAN*xx*** と展開し、再起動するファブリックおよび VSAN の Logical Domains ペインで **Domain Manager** を選択します。

Information ペインにドメインの Running タブ設定が表示されます（図 11-2 を参照）。

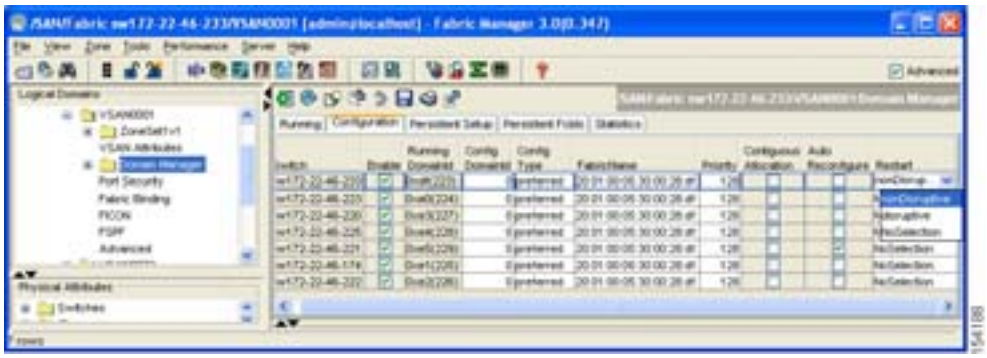
図 11-2　実行中ドメインの設定



ステップ 2　**Configuration** タブをクリックします。

図 11-3 に示すスイッチ設定が表示されます。

図 11-3　ドメインの設定



ステップ 3　fcdomain を再起動するファブリックのスイッチ用に、Restart ドロップダウン リストで **disruptive** または **nonDisruptive** を選択します。

ステップ 4　**Apply Changes** アイコンをクリックし、この fcdomain の再起動を開始します。

スイッチ プライオリティの概要

デフォルトで設定されているプライオリティは 128 です。プライオリティ設定の有効範囲は 1 から 254 までです。プライオリティ 1 が最高プライオリティです。値 255 は別のスイッチから受け入れられますが、ローカルに設定することはできません。

新しいスイッチは、安定したファブリックに参加する場合、主要スイッチにならないことがあります。主要スイッチ選択フェーズ中に、プライオリティが最高のスイッチが主要スイッチになります。2 つのスイッチが同じプライオリティで設定されている場合は、World-Wide Name（WWN）が低いスイッチが主要スイッチになります。

プライオリティ設定は、fcdomain の再起動時にランタイムに適用されます（「ドメインの再起動の概要」[p.11-3] を参照）。この設定は、中断を伴う再起動および中断を伴わない再起動の両方に適用可能です。

スイッチ プライオリティの設定

Fabric Manager を使用して主要スイッチの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　**Fabric*xx* > VSAN*xx*** と展開し、主要スイッチのプライオリティを設定するファブリックおよび VSAN の Logical Domains ペインで **Domain Manager** を選択します。

図 11-4 のように、Information ペインにドメインの実行コンフィギュレーションが表示されます。

図 11-4　実行中ドメインの設定

ステップ 2　**Configuration** タブをクリックします。

図 11-3 に示すスイッチ設定が表示されます。

ステップ 3　ファブリック内で主要スイッチにするスイッチの Priority を高い値に設定します。

ステップ 4　**Apply Changes** アイコンをクリックして、これらの変更を保存します。

fcdomain の初期化の概要

fcdomain 機能はデフォルトで各スイッチでイネーブルになっています。あるスイッチで fcdomain 機能をディセーブルにすると、そのスイッチはファブリックのその他のスイッチに加わらなくなります。fcdomain 設定は、中断を伴う再起動でランタイムに適用されます。

fcdomain のイネーブル化またはディセーブル化

Fabric Manager を使用して、単一の VSAN またはある範囲の VSAN で fcdomain をディセーブルにするには、次の手順を実行します。

ステップ 1　**Fabric*xx* > VSAN*xx*** と展開し、fcdomain をディセーブルにするファブリックおよび VSAN の Logical Domains ペインで **Domain Manager** を選択します。

Information ペインにドメインの実行コンフィギュレーションが表示されます。

ステップ 2　**Configuration** タブをクリックし、fcdomain をディセーブルにするファブリックのスイッチごとに、**Enable** チェックボックスをオフにします（図 11-5 を参照）。

図 11-5　ドメインの設定

ステップ 3　**Apply Changes** アイコンをクリックして、これらの変更を保存します。

ファブリック名の設定

Fabric Manager を使用して、ディセーブルになっている fcdomain のファブリック名の値を設定するには、次の手順を実行します。

ステップ 1　**Fabric*xx* > VSAN*xx*** と展開し、ファブリック名を設定するファブリックおよび VSAN の Logical Domains ペインで **Domain Manager** を選択します。

Information ペインにドメインの実行コンフィギュレーションが表示されます。

ステップ 2　**Configuration** タブをクリックし、ファブリックのスイッチごとにファブリック名を設定します。

ステップ 3　**Apply Changes** アイコンをクリックして、これらの変更を保存します。

着信 RCF の概要

インターフェイスや VSAN ごとに、RCF 要求フレームの拒否を選択できます。RCF 拒否オプションはデフォルトでディセーブルです（つまり、RCF 要求フレームは自動的には拒否されません）。

RCF 拒否 オプションは、すぐに有効になります。

fcdomain の再起動は必要ありません。（「ドメインの再起動の概要」[p.11-3] を参照）。

（注） 仮想ファイバ チャネル インターフェイスは F ポート モードでのみ動作するため、仮想ファイバ チャネル インターフェイスに RFC 拒否オプションを設定する必要はありません。

着信 RCF の拒否

Fabric Manager を使用して着信 RCF 要求フレームを拒否する手順は、次のとおりです。

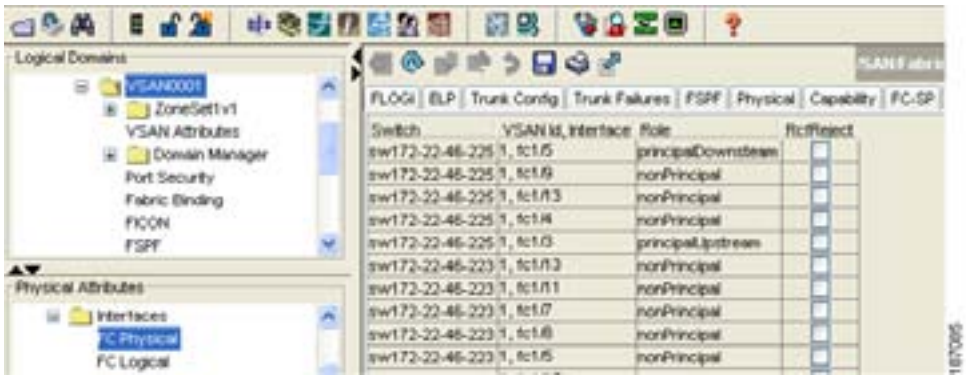
ステップ 1　Physical Attributes ペインで、**Switches** > **Interfaces** を展開して、**FC Physical** を選択します。

Information ペインにファイバ チャネル設定が表示されます。

ステップ 2　**Domain Mgr** タブをクリックします。

図 11-6 の情報が表示されます。

図 11-6　着信 RCF 要求フレームの拒否



ステップ 3　RCF 要求フレームを拒否するインターフェイスごとに、**RcfReject** チェックボックスをオンにします。

ステップ 4　**Apply Changes** アイコンをクリックして、これらの変更を保存します。

結合ファブリックの自動再構成の概要

自動再構成オプションはデフォルトでディセーブルになっています。ドメインが重なる別々の安定ファブリックに属す 2 つのスイッチを結合する場合は、次のような状況になる可能性があります。

- 自動再構成が両方のスイッチでイネーブルである場合は、中断を伴う再構成フェーズが始まります。
- 片方のスイッチまたは両方のスイッチで自動再構成がディセーブルである場合、2 つのスイッチ間のリンクは分離されます。

自動再構成オプションはランタイムですぐに有効になります。fcdomain を再起動する必要はありません。ドメインのオーバーラップのためにドメインが現在分離されており、あとで両方のスイッチで自動再構成オプションをイネーブルにすると、ファブリックは引き続き分離されます。両方のスイッチで自動再構成オプションをイネーブルにしてからファブリックを接続すると、中断を伴う再構成（RCF）が行われます。中断を伴う再構成では、データ トラフィックが影響されることがあります。重複リンクで構成されているドメインを変更して、ドメインのオーバーラップを解消することにより、中断を伴わない fcdomain の再構成を実行できます。

自動再構成のイネーブル化

Fabric Manager を使用して特定 VSAN（またはある範囲の VSAN）で自動再構成をイネーブルにするには、次の手順を実行します。

ステップ 1　**Fabric*xx*** > **VSAN*xx*** と展開し、自動再構成をイネーブルにするファブリックおよび VSAN の Logical Domains ペインで **Domain Manager** を選択します。

Information ペインにドメインの実行コンフィギュレーションが表示されます。

ステップ 2　**Configuration** タブをクリックし、自動的に再構成するファブリックのスイッチごとに **Auto Reconfigure** チェックボックスをオンにします。

ステップ 3　**Apply Changes** アイコンをクリックして、これらの変更を保存します。

ドメイン ID

ドメイン ID により、VSAN でスイッチが一意に識別されます。スイッチには、さまざまな VSAN で異なるドメイン ID が付いていることがあります。ドメイン ID は FC ID 全体の一部分です。

ここでは、ドメイン ID の設定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。

- ドメイン ID の概要（p.11-9）
- スタティック ドメイン ID または優先ドメイン ID の指定（p.11-11）
- 許可ドメイン ID リストの概要（p.11-12）
- 許可ドメイン ID リストの設定（p.11-12）
- 許可ドメイン ID リストの CFS 配信の概要（p.11-13）
- 配信のイネーブル化（p.11-14）
- ファブリックのロック（p.11-14）
- 変更のコミット（p.11-14）
- 変更の廃棄（p.11-15）
- ファブリックのロックのクリア（p.11-15）
- 保留中の変更の表示（p.11-16）
- セッション ステータスの表示（p.11-16）
- 連続ドメイン ID 割り当ての概要（p.11-16）
- 連続ドメイン ID 割り当てのイネーブル化（p.11-17）

ドメイン ID の概要

設定したドメイン ID は、優先またはスタティックにすることができます。デフォルトでは、設定されているドメイン ID は 0（ゼロ）であり、設定タイプは優先です。

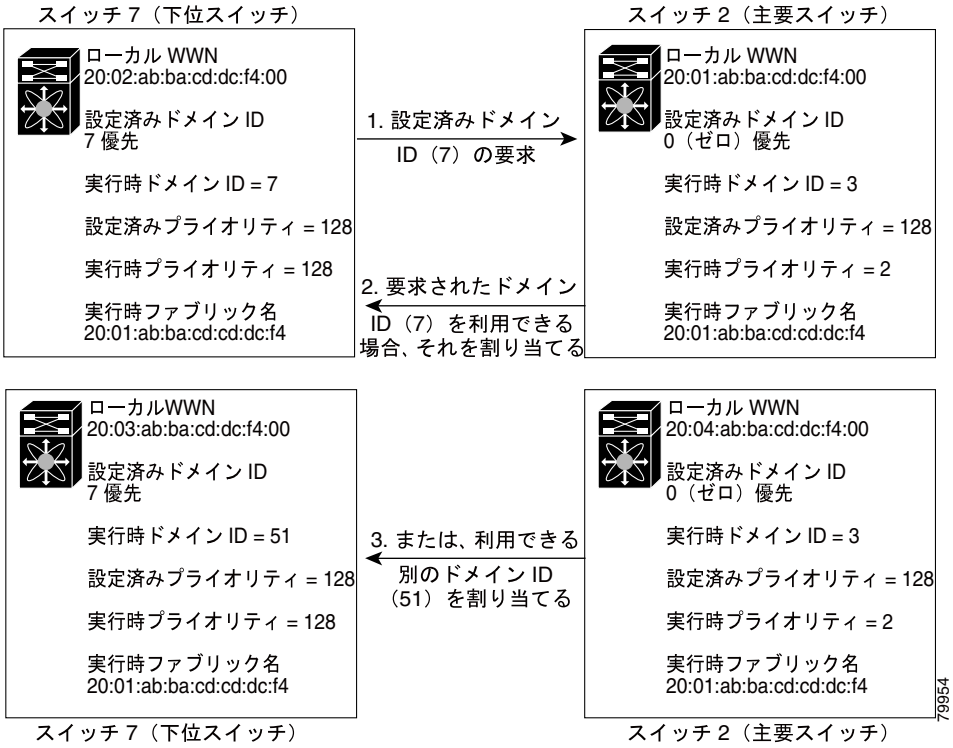
（注） 値 0（ゼロ）は、優先オプションを使用している場合に限り設定できます。

ドメイン ID を設定しない場合、ローカル スイッチはランダムな ID を要求で送信します。スタティックなドメイン ID を使用してください。

下位スイッチがドメインを要求すると、次のプロセスが行われます（図 11-7 を参照）。

1. ローカル スイッチが、設定済みドメイン ID 要求を主要スイッチに送信します。
2. 要求されたドメイン ID が使用可能である場合、主要スイッチはそのドメイン ID を割り当てます。要求されたドメイン ID が使用可能でない場合は、別の使用可能なドメイン ID を割り当てます。

図 11-7　優先オプションを使用した設定プロセス



下位スイッチの動作は、次の要因によって変化します。

- 許可されているドメイン ID リスト
- 設定されているドメイン ID
- 主要スイッチが要求スイッチに割り当てたドメイン ID

特定の状況では次のように変化します。

- 受信したドメイン ID が許可リスト内に収まっていない場合は、要求ドメイン ID がランタイム ドメイン ID になり、その VSAN のインターフェイスはすべて分離されます。
- 割り当てられたドメイン ID および要求したドメイン ID が同一である場合、優先オプションとスタティック オプションは関係なく、割り当てられたドメイン ID がランタイム ドメイン ID になります。
- 割り当てられたドメイン ID および要求したドメイン ID が異なる場合は、次のケースが当てはまります。
  - 設定されているタイプがスタティックである場合、割り当てられたドメイン ID は廃棄され、すべてのローカル インターフェイスは分離されて、ローカル スイッチが設定済みドメイン ID を自分自身に割り当て、そのドメイン ID がランタイム ドメイン ID になります。
  - 設定されているタイプが優先の場合、ローカル スイッチは主要スイッチによって割り当てられたドメイン ID を受け入れて、割り当てられたドメイン ID がランタイム ドメイン ID になります。

設定されたドメイン ID を変更すると、VSAN で現在設定されているすべての許可ドメイン ID リストに新しいドメイン ID が含まれる場合に限り、変更内容は受け入れられます。ゼロ優先ドメイン ID を設定することもできます。

注意　設定したドメインの変更をランタイム ドメインに適用する場合は、**fcdomain** を再起動する必要があります。

（注）　許可ドメイン ID リストを設定した場合、追加するドメイン ID は VSAN でその範囲に収まっている必要があります。「許可ドメイン ID リストの概要」（p.11-12）を参照してください。

スタティック ドメイン ID または優先ドメイン ID の指定

スタティック ドメイン ID タイプを割り当てるということは、特定のドメイン ID を要求するということです。スイッチは、要求したアドレスを取得しなかった場合、自分自身をファブリックから分離します。優先ドメイン ID を指定するということも、特定のドメイン ID を要求するということですが、要求したドメイン ID が使用不可である場合、スイッチは別のドメイン ID を受け入れます。

中断を伴う再起動、または中断を伴わない再起動のあとでスタティック オプションをランタイムに適用できる間は、中断を伴う再起動のあとに限って優先オプションがランタイムに適用されます（「ドメインの再起動の概要」[p.11-3] を参照）。

（注）　VSAN 内では、すべてのスイッチでドメイン ID タイプが同一である必要があります（スタティックまたは優先）。あるスイッチがスタティック ドメイン タイプで、別のスイッチが優先ドメイン タイプであるというように、設定が混在している場合は、リンクが分離されることがあります。

Fabric Manager を使用してスタティックまたは優先のドメイン ID を指定する手順は、次のとおりです。

ステップ 1　**Fabric***xx* > **VSAN***xx* と展開し、ドメイン ID を設定するファブリックおよび VSAN の Logical Domains ペインで **Domain Manager** を選択します。

Information ペインにドメインの実行コンフィギュレーションが表示されます。

ステップ 2　Config DomainID に値を入力して Config Type ドロップダウン リストから **static** または **preferred** をクリックし、ファブリックのスイッチにドメイン ID を設定します。

ステップ 3　**Apply Changes** アイコンをクリックして、これらの変更を保存します。

許可ドメイン ID リストの概要

デフォルトの場合、割り当てるドメイン ID リストの有効範囲は 1 から 239 までです。許可ドメイン ID リストに含める範囲のリストを指定し、それぞれの範囲をカンマで区切ることができます。主要スイッチは、ローカルに設定されている許可ドメイン リストで使用可能なドメイン ID を割り当てます。

重複しないドメイン ID で VSAN を設計するには、許可ドメイン ID リストを使用します。今後、NAT 機能がない IVR を実装する必要がある場合は、これが役立ちます。

ヒント　ファブリックの 1 つのスイッチで許可リストを設定する場合は、ファブリックの他の全スイッチで同じリストを設定して一貫性を保つか、Cisco Fabric Service（CFS）を使用して設定を配信することを推奨します。

許可ドメイン ID リストでは、次の条件を満たす必要があります。

- このスイッチが主要スイッチである場合は、現在割り当てられているすべてのドメイン ID を許可リストに含める必要があります。
- このスイッチが下位スイッチである場合は、ローカル ランタイム ドメイン ID を許可リストに含める必要があります。
- スイッチのローカルで設定されているドメイン ID を許可リストに含める必要があります。
- 割り当てられているドメイン ID、およびその他のすでに設定されているドメイン ID リストの共通部分を空にすることはできません。

許可ドメイン ID リストの設定

Fabric Manager を使用して許可ドメイン ID リストを設定する手順は、次のとおりです。

ステップ 1　**Fabric*xx* > VSAN*xx* > Domain Manager** と展開し、許可ドメイン ID リストを設定するファブリックおよび VSAN の Logical Domains ペインで **Allowed** を選択します。

Information ペインに CFS 設定が表示されます（図 11-8 を参照）。

図 11-8　許可 CFS 設定情報

ステップ 2　Admin ドロップダウン リストを **enable** に設定し、Global ドロップダウン リストを **enable** に設定します。

ステップ 3　**Apply Changes** をクリックし、CFS による許可ドメイン ID リストの配信をイネーブルにします。

ステップ 4　**Allowed DomainIds** タブをクリックします。

図 11-9 に示す Allowed Domain ID 画面が表示されます。

図 11-9　許可ドメイン ID リスト

ステップ 5　このドメインの許可ドメイン ID リストに list を設定します。

ステップ 6　**CFS** タブをクリックし、Config Action を **commit** に設定します。

ステップ 7　**Apply Changes** アイコンをクリックしてこの許可ドメイン ID リストを確定し、VSAN で配信します。

許可ドメイン ID リストの CFS 配信の概要

CFS インフラストラクチャを使用し、ファブリックのすべての Cisco SAN スイッチに許可ドメイン ID リストの設定情報を配信することをイネーブルにすることができます。この機能により、1 つのスイッチのコンソールからファブリック内の設定を同期できます。同じ設定が VSAN 全体に配信されるので、発生する可能性がある設定ミスや、同一 VSAN の 2 つのスイッチで互換性がない許可ドメインを設定する可能性を回避できます。

VSAN のすべてのスイッチで許可ドメイン ID リストの一貫性を保つには、CFS を使用して許可ドメイン ID リストを配信します。

（注）　許可ドメイン ID リストを設定し、主要スイッチで確定することを推奨します。

CFS の詳細については、第 7 章「CFS の使用」を参照してください。

配信のイネーブル化

許可ドメイン ID リストの CFS 配信は、デフォルトでディセーブルです。許可ドメイン ID リストの配信先となるすべてのスイッチで配信をイネーブルにする必要があります。

Fabric Manager を使用して許可ドメイン ID リスト設定の配信をイネーブルにする（またはディセーブルにする）手順は、次のとおりです。

ステップ 1　**Fabric*xx* > VSAN*xx* > Domain Manager** と展開し、許可ドメイン ID リストを設定するファブリックおよび VSAN の Logical Domains ペインで **Allowed** を選択します。

Information ペインに CFS 設定が表示されます。

ステップ 2　許可ドメイン ID リストの CFS 配信をイネーブルにするには、Admin ドロップダウン リストを **enable** に、Global ドロップダウン リストを **enable** に設定します。

ステップ 3　**Apply Changes** アイコンをクリックし、CFS による許可ドメイン ID リストの配信をイネーブルにします。

ファブリックのロック

既存設定を変更する最初の処理により、保留設定が作成されてファブリックの機能がロックされます。ファブリックをロックすると、次の条件が成立します。

- 他のユーザは、この機能の設定を変更できなくなります。
- アクティブな設定をコピーすると、保留設定が作成されます。これ以後の変更は保留中のコンフィギュレーションに対して行われ、アクティブなコンフィギュレーション（およびファブリック内の他のスイッチ）に変更をコミットするか、または変更を廃棄するまで、保留中のコンフィギュレーションにとどまります。

変更のコミット

保留されているドメイン設定の変更を VSAN のその他の SAN スイッチに適用するには、変更を確定する必要があります。保留中の設定変更は配信され、正常に確定された時点で、設定変更は VSAN 全体の SAN スイッチでアクティブな設定に適用されて、ファブリックのロックは解除されます。

Fabric Manager を使用して保留中のドメイン設定変更を確定し、ロックを解除する手順は次のとおりです。

ステップ 1　**Fabric*xx* > VSAN*xx* > Domain Manager** と展開し、許可ドメイン ID リストを設定するファブリックおよび VSAN の Logical Domains ペインで **Allowed** を選択します。

Information ペインに CFS 設定が表示されます。

ステップ 2　Config Action ドロップダウン リストを **commit** に設定します。

ステップ 3　**Apply Changes** アイコンをクリックしてこの許可ドメイン ID リストを確定し、VSAN で配信します。

変更の廃棄

ドメイン設定に対する保留中の変更をいつでも廃棄し、ファブリックのロックを解除できます。保留中の変更を廃棄する（打ち切る）と、設定は影響されずにロックが解除されます。

Fabric Manager を使用して保留中のドメイン設定変更を廃棄し、ロックを解除する手順は次のとおりです。

ステップ 1　**Fabric*xx* > VSAN*xx* > Domain Manager** と展開し、許可ドメイン ID リストを設定するファブリックおよび VSAN の Logical Domains ペインで **Allowed** を選択します。

Information ペインに CFS 設定が表示されます。

ステップ 2　Config Action ドロップダウン リストを **abort** に設定します。

ステップ 3　**Apply Changes** アイコンをクリックし、許可ドメイン ID リストに対する保留中の変更を廃棄します。

ファブリックのロックのクリア

ドメイン設定タスクを実行し、変更の確定か廃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すると、保留中の変更は廃棄され、ファブリックのロックは解除されます。

ヒント　保留中の変更は一時的なディレクトリのみで使用可能であり、スイッチが再起動されると廃棄されます。

Fabric Manager を使用してファブリックのロックを解除する手順は、次のとおりです。

ステップ 1　**Fabric*xx* > VSAN*xx* > Domain Manager** と展開し、許可ドメイン ID リストが必要なファブリックおよび VSAN の Logical Domains ペインで **Allowed** を選択します。

Information ペインに CFS 設定が表示されます。

ステップ 2　Config Action ドロップダウン リストを **clear** に設定します。

ステップ 3　**Apply Changes** アイコンをクリックし、ファブリックのロックをクリアします。

保留中の変更の表示

Fabric Manager を使用して保留中の設定変更を表示する手順は、次のとおりです。

ステップ 1　許可ドメイン ID リストを設定するファブリックおよび VSAN の Logical Domains ペインで、**Fabric*xx* > VSAN*xx* > Domain Manager** > **Allowed** と展開します。

Information ペインに CFS 設定が表示されます。

ステップ 2　Config View As ドロップダウン リストを **pending** に設定します。

ステップ 3　**Apply Changes** アイコンをクリックし、ファブリックのロックをクリアします。

ステップ 4　**AllowedDomainIds** タブをクリックします。

許可ドメイン ID リストの保留中の設定が表示されます。

セッション ステータスの表示

Fabric Manager を使用して配信セッションのステータスを表示する手順は、次のとおりです。

ステップ 1　**Fabric*xx* > VSAN*xx* > Domain Manager** と展開し、許可ドメイン ID リストを設定するファブリックおよび VSAN の Logical Domains ペインで **Allowed** を選択します。

ステップ 2　CFS 設定およびセッション ステータスが Information ペインに表示されます。

連続ドメイン ID 割り当ての概要

連続ドメイン割り当てはデフォルトではディセーブルです。下位スイッチが複数のドメインを主要スイッチに要求し、ドメインが連続していない場合は、次のような状況になる可能性があります。

- 連続ドメイン割り当てが主要スイッチでイネーブルになっている場合、主要スイッチは連続ドメインを特定して下位スイッチに割り当てます。連続ドメインが使用不可である場合、スイッチ ソフトウェアはこの要求を却下します。
- 連続ドメイン割り当てが主要スイッチでディセーブルになっている場合、主要スイッチは使用可能ドメインを下位スイッチに割り当てます。

連続ドメイン ID 割り当てのイネーブル化

Fabric Manager を使用して特定 VSAN（またはある範囲の VSAN）で連続ドメインをイネーブルにするには、次の手順を実行します。

ステップ 1　**Fabric*xx* > VSAN*xx*** と展開し、連続ドメインをイネーブルにするファブリックおよび VSAN の Logical Domains ペインで **Domain Manager** を選択します。

Information ペインにドメインの実行コンフィギュレーションが表示されます。

ステップ 2　**Configuration** タブをクリックし、連続割り当てをイネーブルにするファブリックのスイッチごとに **Contiguous Allocation** チェックボックスをオンにします。

ステップ 3　**Apply Changes** アイコンをクリックして、これらの変更を保存します。

FC ID

N ポートが Nexus 5000 シリーズ スイッチにログインすると、そのポートには FC ID が割り当てられます。デフォルトでは、固定的 FC ID 機能がイネーブルです。この機能をディセーブルにすると、次のような状況になる可能性があります。

- N ポートが Nexus 5000 シリーズ スイッチにログインします。N の要求側ポートの WWN、および割り当てられた FC ID は保持され、揮発性キャッシュに保存されます。この揮発性キャッシュの内容は、リブートすると失われます。
- スイッチは、最善の方法でバインディング FC ID を WWN に保持するように設計されています。たとえば 1 つの N ポートがスイッチから切断し、別のデバイスがその FC ID を要求した場合、この要求は許可され、最初に FC ID に関連していた WWN が解放されます。
- 揮発性キャッシュには、WWN と FC ID のバインディングのエントリが 4000 個まで保存されます。このキャッシュがいっぱいになると、新しい（最新）エントリによってキャッシュの最も古いエントリが上書きされます。この場合、最も古いエントリに対応する WWN と FC ID の関連は失われます。
- スイッチが同一 VSAN に属す限り、切断してから同一スイッチ内の任意のポートに再接続した場合、N ポートは同一 FC ID を受け取ります。

ここでは、FC ID の設定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。

- 固定的 FC ID の概要（p.11-18）
- 固定的 FC ID 機能のイネーブル化（p.11-19）
- 固定的 FC ID 設定の注意事項（p.11-19）
- 固定的 FC ID の設定（p.11-20）
- HBA の固有エリア FC ID の概要（p.11-21）
- HBA の固有エリア FC ID の設定（p.11-21）
- 固定的 FC ID の選択消去の概要（p.11-23）
- 固定的 FC ID の消去（p.11-23）

固定的 FC ID の概要

固定的 FC ID がイネーブルである場合は、次のようになります。

- fcdomain で現在使用中の FC ID は、リブートしても保存されます。
- fcdomain は、デバイス（ホストまたはディスク）がポート インターフェイスに接続されたあとでスイッチが学習したダイナミック エントリをデータベースに自動的に入力します。

（注） AIX または HP-UX ホストからスイッチに接続している場合は、これらのホストを接続している VSAN 内で固定的な FC ID 機能をイネーブルにしてください。

（注） 固定的 FC ID がイネーブルの場合、リブート後は FC ID を変更できません。FC ID はデフォルトでイネーブルですが、各 VSAN でディセーブルにできます。

F ポートに割り当てられた固定的 FC ID はインターフェイス間で移動でき、引き続き同一の固定的 FC ID を維持できます。

固定的 FC ID 機能のイネーブル化

Fabric Manager を使用して固定的 FC ID 機能をイネーブルにする手順は、次のとおりです。

ステップ 1　**Fabric*xx*** > **VSAN*xx*** と展開し、固定的 FC ID 機能をイネーブルにするファブリックおよび VSAN の Logical Domains ペインで **Domain Manager** を選択します。

Information ペインにドメインの実行コンフィギュレーションが表示されます。

ステップ 2　**Persistent Setup** タブをクリックし、固定的 FC ID をイネーブルにするファブリックのスイッチごとに **enable** チェックボックスをオンにします。

ステップ 3　**Apply Changes** アイコンをクリックして、これらの変更を保存します。

固定的 FC ID 設定の注意事項

固定的 FC ID 機能をイネーブルにしたら、固定的 FC ID サブモードを開始し、スタティック エントリまたはダイナミック エントリを FC ID データベースに追加できます。デフォルトの場合、すべての追加エントリはスタティックになります。固定的 FC ID は VSAN 単位で設定します。

固定的 FC ID を手動で設定する場合は、次の要件に従ってください。

- 必要な VSAN で固定的 FC ID 機能をイネーブルにしてください。
- 必要な VSAN がアクティブな VSAN であることを確認してください。固定的 FC ID は、アクティブな VSAN のみで設定可能です。
- FC ID のドメイン部分が、必要な VSAN のランタイム ドメイン ID と同じであることを確認してください。ソフトウェアがドメインの不一致を検出すると、コマンドは拒否されます。
- 領域の設定時には、FC ID のポートフィールドが 0（ゼロ）であることを確認します。

固定的 FC ID の設定

Fabric Manager を使用して固定的 FC ID を設定する手順は、次のとおりです。

ステップ 1　**Fabric*xx*** > **VSAN*xx*** と展開し、固定的 FC ID リストを設定するファブリックおよび VSAN の Logical Domains ペインで **Domain Manager** を選択します。

Information ペインにドメインの実行コンフィギュレーションが表示されます。

ステップ 2　**Persistent FcIds** タブをクリックし、**Create Row** をクリックします。

図 11-10 に示す Create Persistent FC ID ダイアログボックスが表示されます。

図 11-10　Create Persistent FC ID ダイアログボックス

ステップ 3　スイッチ、WWN、固定にする FC ID を選択します。

ステップ 4　Mask フィールドの **single** または **area** オプション ボタンをクリックします。

ステップ 5　Assignment フィールドの **static** または **dynamic** オプション ボタンをクリックします。

ステップ 6　**Apply Changes** アイコンをクリックして、これらの変更を保存します。

HBA の固有エリア FC ID の概要

（注） Host Bus Adapter（HBA）ポートおよびストレージ ポートを同一スイッチに接続している場合に限り、このセクションを読んでください。

HBA ポートとストレージ ポートを両方とも同一スイッチに接続している場合、一部の HBA ポートにはストレージ ポートとは別のエリア ID が必要となります。たとえば、ストレージ ポートの FC ID が 0x6f7704 である場合、このポートのエリアは 77 です。この場合、HBA ポートのエリアは 77 以外にすることができます。HBA ポートの FC ID は手動で設定し、ストレージ ポートの FC ID とは別にする必要があります。

Nexus 5000 シリーズ スイッチでは、FC ID の固定機能により、この要件を容易に満たすことができます。この機能を使用し、ストレージ ポートまたは HBA ポートのいずれかに、エリアが異なる FC ID を事前に割り当てることができます。

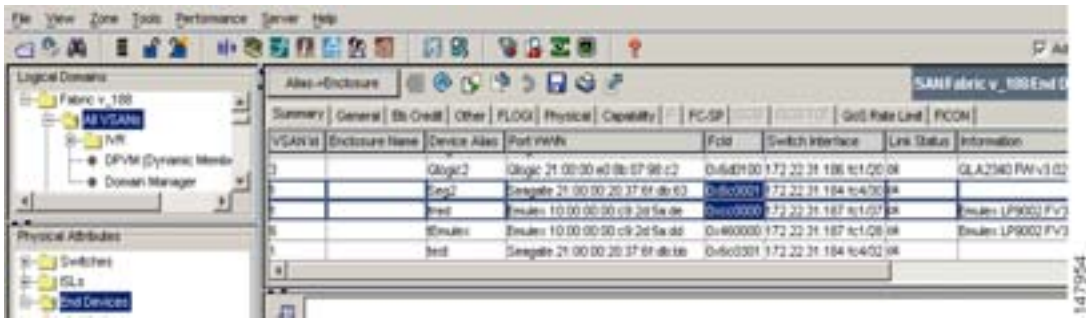
HBA の固有エリア FC ID の設定

この作業では、スイッチ ドメイン 111（16 進法では 6f）による設定例を使用します。サーバは、FCoE を介してスイッチに接続されます。HBA ポートはインターフェイス vfc20/1 に、ストレージ ポートは同一スイッチのインターフェイス fc2/3 に接続します。

Fabric Manager を使用して HBA ポートに別のエリア ID を設定する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインの **End Device** を展開し、**Summary** タブを選択して、HBA のポート WWN（Port Name フィールド）を取得します（図 11-11 を参照）。

図 11-11　Fabric Manager の FLOGI データベース情報



（注） この設定では、両方の FC ID に同じエリア 00 が割り当てられています。

ステップ 2　Physical Attributes ペインで、**Switches** > **Interfaces** を展開して、**FC Physical** を選択します。

Fibre Channel Interfaces Information ペインが表示されます。

ステップ 3　HBA が接続されているインターフェイスで、Status Admin ドロップダウン リストを **down** に設定します。

MDS スイッチで HBA インターフェイスがシャットダウンされます。

ステップ 4　**Fabricxx > VSANxx** と展開し、**Domain Manager** を選択します。

ステップ 5　Information ペインの **Persistent Setup** タブをクリックし、FC ID 機能がイネーブルであることを確認します（図 11-12 を参照）。

図 11-12　Fabric Manager の固定的 FC ID 情報

この機能がディセーブルである場合は、この手順を続けて固定的 FC ID をイネーブルにします。

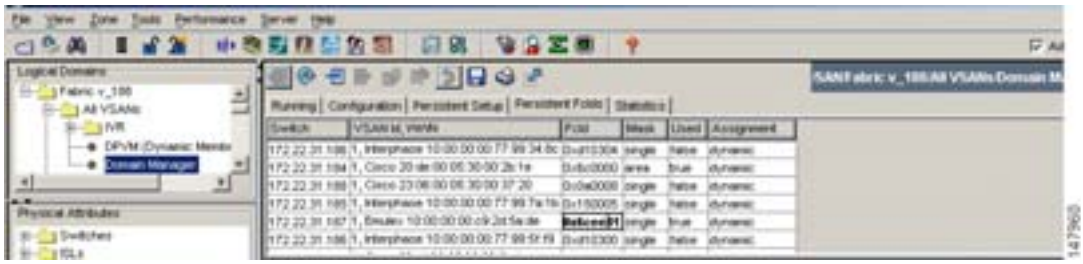
この機能がすでにイネーブルになっている場合は、ステップ 7 に進みます。

ステップ 6　スイッチで固定的 FC ID 機能をイネーブルにするには、**Enable** チェックボックスをオンにします（図 11-13 を参照）。

ステップ 7　**Persistent FcIds** タブをクリックし、エリア割り当てが異なる新しい FC ID を FcId フィールドで割り当てます。

たとえば、図 11-13 では、*00* が *ee* に置き換わります。

図 11-13　Fabric Manager での FC ID の設定



ステップ 8　**Apply Changes** をクリックし、新しい FC ID を保存します。

ステップ 9　FC ID の値を比較し、HBA の FC ID を確認します。

（注）　両方の FC ID でエリア割り当てが異なっています。

ステップ 10　Physical Attributes ペインで、**Switches** > **Interfaces** を展開して、**FC Physical** を選択します。HBA が接続されているインターフェイスで、Status Admin ドロップダウン リストを **up** に設定します。

Nexus 5000 シリーズ スイッチで HBA インターフェイスがイネーブルになります。

固定的 FC ID の選択消去の概要

固定的 FC ID は選択的に消去できます。現在使用中のスタティック エントリと FC ID は削除できません。表 11-1 は、固定的 FC ID の消去時に削除される FC ID エントリと維持される FC ID エントリを示しています。

表 11-1　消去される FC ID

固定的 FC ID の状態	固定使用状態	処理
スタティック	使用中	削除されない
スタティック	未使用	削除されない
ダイナミック	使用中	削除されない
ダイナミック	未使用	削除される

固定的 FC ID の消去

Fabric Manager を使用して固定的 FC ID を削除する手順は、次のとおりです。

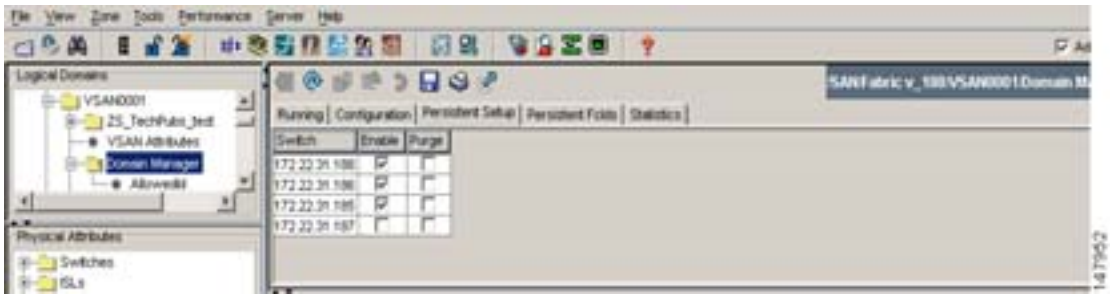
ステップ 1　固定的 FC ID を消去するファブリックの Logical Domains ペインで、**Fabric*xx*** > **All VSANs** > **Domain Manager** と展開します。

Information ペインにドメインの実行コンフィギュレーションが表示されます。

ステップ 2　**Persistent Setup** タブをクリックします。

図 11-14 のように、Information ペインに固定的 FC ID 設定が表示されます。

図 11-14　Fabric Manager の固定的 FC ID 情報



ステップ 3　固定的 FC ID を消去するスイッチの **Purge** チェックボックスをオンにします（図 11-14 を参照）。

ステップ 4　**Apply Changes** アイコンをクリックして、これらの変更を保存します。

fcdomain の統計情報の表示

Fabric Manager は fcdomain の統計情報を収集し、Information ペインに表示します。

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

ステップ 1　**Fabric*xx* > All VSANs** と展開し、統計情報を表示するファブリックの Logical Domains ペインで **Domain Manager** を選択します。

Information ペインにドメインの実行コンフィギュレーションが表示されます。

ステップ 2　**Statistics** タブをクリックします。

Information ペインに FC ID の統計情報が表示されます。

デフォルト設定

表 11-2 に、すべての fcdomain パラメータのデフォルト設定一覧を示します。

表 11-2　デフォルトの fcdomain パラメータ

パラメータ	デフォルト
fcdomain 機能	イネーブル
設定済みドメイン ID	0（ゼロ）
設定済みドメイン	優先
自動再構成オプション	無効
連続割り当てオプション	無効
プライオリティ	128
許可リスト	1 ～ 239
ファブリック名	20:01:00:05:30:00:28:df
RCF 拒否	ディセーブル
固定的 FC ID	イネーブル
許可ドメイン ID リスト設定の配信	ディセーブル

CHAPTER 12

N ポート バーチャライゼーションの設定

N Port Virtualization（NPV; N ポート バーチャライゼーション）では、SAN ファブリックで使用されるファイバ チャネル ドメイン ID 数が減少します。NPV モードで動作するエッジ スイッチはファブリックに加入せず、NPV コア スイッチとエンド デバイスの間でトラフィックを渡します。これによって、各エッジ スイッチ一意のドメイン ID が必要なくなります。

この章の内容は、次のとおりです。

- NPV の概要（p.12-2）
- 注意事項および制限事項（p.12-5）
- NPV の設定（p.12-6）

NPV の概要

一般的にファイバ チャネル ネットワークは、コアエッジ モデルを使用して、多くのファブリック スイッチをコア デバイスに接続して展開します。しかし、ファブリックのポート数が増えると、展開するスイッチ数も増えて、ドメイン ID の数が劇的に増加します（1 つの SAN でサポートされている最大数は 239）。ファイバ チャネル ネットワークで多くのブレード スイッチを展開すると、これはさらに難しい課題になります。

NPV では、複数の NPV スイッチ間で NPV コア スイッチのドメイン ID を共有することで、ドメイン ID の数の増加を解決します。

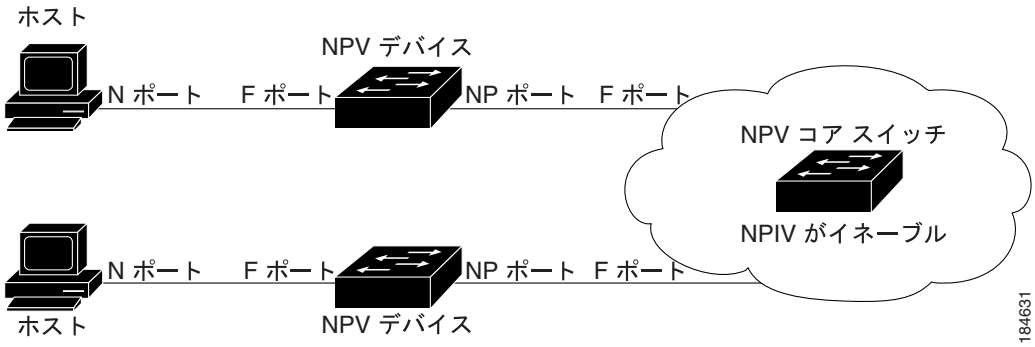
NPV エッジ スイッチは、複数のローカル接続 N ポートを 1 つまたは複数の外部 NP リンクに集約します。エッジ スイッチはコア ファイバ チャネル スイッチのホスト、およびファブリック スイッチまたはブレード スイッチのサーバのファイバ チャネル スイッチのように見えます。

NPV では、NPV コア スイッチの同一ポートに複数のデバイスが接続されるので、コア スイッチに必要になる追加のポートを削減できます。

図 12-1 に、NPV 設定のインターフェイスレベルのビューを示します。

Nexus 5000 シリーズ スイッチでは、物理ファイバ チャネル インターフェイスを NP ポートまたは F ポートにすることができます。仮想ファイバ チャネル インターフェイスは F ポートにすることができます。

図 12-1　インターフェイス レベルの Cisco NPV 設定



（注） 2 つのエンド デバイス間におけるやり取りでは NPV デバイスからコアへの同じアップリンクが使用されるので、NPV モードでは順序どおりのデータ配信が必要ありません。NPV デバイスを超えるトラフィックでは、コア スイッチは、設定されている場合、順序どおりの配信を実行します。

ここでは、NPV モードのスイッチの動作について説明します。

- NP ポート（p.12-2）
- NP リンク（p.12-3）
- FLOGI 動作（p.12-3）

NP ポート

NP ポート（プロキシ N ポート）は、NPV モードになっているスイッチのポートであり、F ポートでコア NPV スイッチに接続されます。NP ポートは、複数の物理 N ポートのプロキシとして機能する N ポートのように動作します。

NP リンク

NP リンクは、基本的に特定エンド デバイスへの NPIV アップリンクです。NP リンクは、NPV コア スイッチへのアップリンクがアップしたときに確立します。アップリンクがダウンすると、NP リンクは終了します。アップリンクが確立すると、NPV スイッチは内部 FLOGI を NPV コア スイッチに対して実行し、FLOGI が正常に実行された場合は、NPV コア スイッチのネーム サーバに自分自身を登録します。この NP リンクにおけるエンド スイッチからのその後の FLOGI は FDISC に変換されます。

サーバ リンクは、NP リンク間で均等に分散されます。サーバ リンクの背後にあるすべてのエンド デバイスは、1 つの NP リンクのみにマッピングされます。

FLOGI 動作

NP ポートがアップすると、Nexus 5000 シリーズ スイッチがまず NPV コア スイッチに自分自身をログインし、次のパラメータを含む GLOGI 要求を送信します。

- 内部ログインで pWWN として使用される NP ポートのファブリック ポート WWN（fWWN）
- 内部 FLOGI でノード WWN（nWWN）として使用される Nexus 5000 シリーズ スイッチの VSAN ベースのスイッチ WWN（sWWN）

Nexus 5000 シリーズ スイッチは、FLOGI 要求が完了すると、次のパラメータをさらに使用して、ファブリック ネーム サーバに自分自身を登録します。

- NPV デバイス自体のネーム サーバ登録のシンボリック ポート名に、NP ポートのスイッチ名とインターフェイス名（fc2/4 など）が埋め込まれています。
- Nexus 5000 シリーズ スイッチの IP アドレスは、NPV デバイスのネーム サーバ登録で IP アドレスとして登録されます。

（注） NP ポートにおける内部 FLOGI の BB_SCN は、常にゼロに設定されます。BB_SCN は NPV デバイスの F ポートでサポートされます。

図 12-2 は、NPV コア スイッチと NPV デバイスの間における内部 FLOGI のフローを示しています。

図 12-2　内部 FLOGI フロー

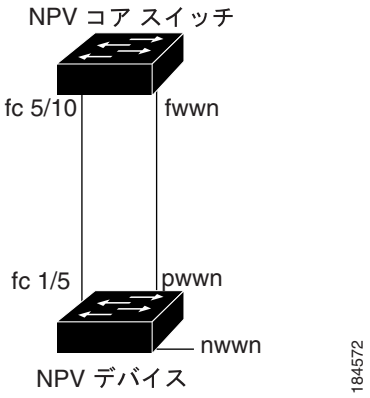


表 12-1 に、図 12-2 に示した内部 FLOGI パラメータを示します。

表 12-1　内部 FLOGI パラメータ

パラメータ	派生元
pWWN	NP ポートの fWWN
nWWN	NPV デバイスの VSAN ベース sWWN
fWWN	NPV コア スイッチの F ポートの fWWN
シンボリック ポート名	スイッチ名および NP ポート インターフェイス文字列 **（注）** スイッチ名が得られない場合、出力は「switch」になり、たとえば、switch: fc2/3 となります。
IP アドレス	NPV デバイスの IP アドレス
シンボリック ノード名	NPV スイッチ名

fWWN ベースのゾーン分割が NPV デバイスでサポートされますが、次のような理由のために推奨できません。

- ゾーン分割は NPV デバイスでは実施されない（NPV コア スイッチで実施される）。
- NPV デバイスに接続されている複数のデバイスは、コアで同じ F ポートによってログインするので、別々のゾーンに分割できない。
- 同一デバイスが、コア スイッチで（使用する NPV リンクによって）別の fWWN を使用してログインすることがあり、別々の fWWN を使用してゾーン分割しなければならないことがある。

注意事項および制限事項

次に、NPV 展開時の注意事項および要件を示します。

- NPV コア スイッチで使用可能なすべてのメンバー タイプを使用し、NPV デバイスに接続されているエンド デバイスにゾーン分割を設定できます。fWWN、sWWN、ドメイン、ポートベースのうちいずれかのゾーン分割を使用する場合は、NPV コア スイッチの fWWN、sWWN、ドメインまたはポートを使用する必要があります。
- NPV モードで、ポート トラッキングがサポートされています。「ポート トラッキングの概要」（p.27-2）を参照してください。
- NPV スイッチでは、NPV スイッチでログインするデバイス用にポート セキュリティがサポートされます。NPV コア スイッチでは、ポート セキュリティがインターフェイスごとにイネーブルになります。NPV スイッチでログインするデバイス用に NPV コア スイッチでポート セキュリティをイネーブルにするには、次の要件に従う必要があります。
  - 内部 FLOGI をポート セキュリティ データベースに含める必要があります。これにより、NPV コア スイッチのポートで通信およびリンクが許可されます。
  - すべてのエンド デバイスの pWWN も、ポート セキュリティ データベースに含める必要があります。

  VSAN に基づいて別々の NPV セッションにデバイスをグループ化すると、複数の VSAN を NPV 対応スイッチでサポートできます。アップリンクが伝送できる VSAN に基づいて、正しいアップリンクを選択する必要があります。
- NPV ではロード バランシング アルゴリズムが使用され、VSAN のエンド デバイスが最初のログイン時にいずれかの NPV コア スイッチ リンク（同一 VSAN）に自動的に割り当てられます。同一 VSAN に複数の NPV コア スイッチ リンクがある場合は、特定のコア スイッチ リンクにエンド デバイスを割り当てることはできません。
- サーバ インターフェイスがダウンしてからサービスに復帰する場合、インターフェイスが同じコア スイッチ リンクに割り当てられない場合があります。
- 割り当てられているコア スイッチ リンクが動作している場合にだけ、サーバ インターフェイスが動作します。
- NPV モードの場合、サーバとターゲットの両方をスイッチに接続できます。
- ローカル スイッチングはサポートされません。すべてのトラフィックは NPV コア スイッチを使用してスイッチングされます。
- NPV デバイスは複数の NPV コア スイッチに接続できます。言い換えると、さまざまな NP ポートをさまざまな NPV コア スイッチに接続できます。
- NPV では NPIV 対応モジュール サーバ（ネスト NPIV）がサポートされます。
- F ポート、NP ポート、SD ポートのみが NPV モードでサポートされます。

NPV の設定

NPV をイネーブルにすると、システム設定は消去され、システムは NPV モードがイネーブルの状態でリブートされます。

（注） 設定をあとで使用する必要がある場合、NPV の前にブート フラッシュ メモリまたは TFTP サーバに現在の設定を保存することを推奨します。

Device Manager による NPV の設定

Device Manager を使用して NPV を設定する手順は、次のとおりです。

ステップ 1　Nexus 5000 シリーズ スイッチから Device Manager を起動して、NPV をイネーブルにします。

ステップ 2　Admin ドロップダウン メニューから **Feature Control** を選択します。**Action** フィールドで、NPV 機能の **enable** を選択して、**Apply** をクリックします。

ステップ 3　NPV デバイスで外部インターフェイスを設定するには、Interface ドロップダウン リストから **FC All** を選択します。

ステップ 4　Mode Admin カラムで、各外部インターフェイスの **NP** ポート モードを選択して、**Apply** をクリックします。

ステップ 5　Nexus 5000 シリーズ スイッチでサーバ インターフェイスを設定するには、Interface ドロップダウン リストから **FC All** を選択します。

ステップ 6　Mode Admin カラムで、各外部サーバ インターフェイスの **F** ポート モードを選択して、**Apply** をクリックします。

ステップ 7　デフォルトの Admin ステータスは **down** です。ポート モードの設定後、Admin ステータスに **up** を選択し、リンクをアップにする必要があります。

CHAPTER 13

VSAN トランキングの設定

この章では、Nexus 5000 シリーズ スイッチで提供される VSAN トランキング機能について説明します。

この章の内容は、次のとおりです。

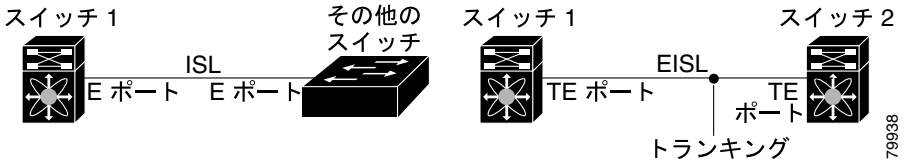
- VSAN トランキングの概要（p.13-2）
- VSAN トランキングの設定（p.13-4）
- デフォルト設定（p.13-8）

VSAN トランキングの概要

VSAN トランキングでは、相互接続ポートが Enhanced ISL（EISL; 拡張 ISL）フレーム形式を使用して、同一物理リンクによって複数の VSAN でフレームを送受信できます（図 13-1 を参照）。

VSAN トランキングはネイティブ ファイバ チャネル インターフェイスでサポートされていますが、仮想ファイバ チャネル インターフェイスではサポートされていません。

図 13-1　VSAN トランキング



VSAN トランキング機能には次の制約事項があります。

- トランキング設定は E ポートのみに適用可能です。トランク モードを E ポートでイネーブルにして、そのポートがトランキング E ポートとして動作すると、そのポートは TE ポートと呼ばれます。
- TE ポート用に設定したトランク許可 VSAN は、フレームの送受信ができる許可アクティブ VSAN を判別するため、トランキング プロトコルに使用されます。
- トランキングがイネーブルの E ポートをサードパーティ製スイッチに接続した場合も、トランキング プロトコルによって E ポートとしてのシームレスな動作が保証されます。

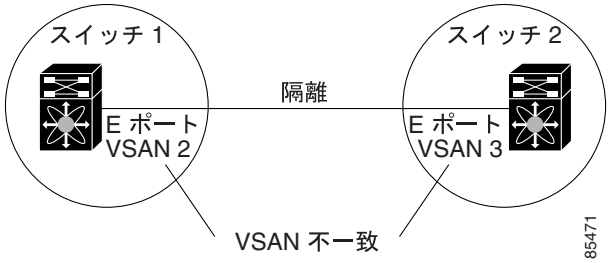
ここでは、SAN トランキングの詳細について説明します。内容は次のとおりです。

- VSAN トランキングの不一致（p.13-2）
- VSAN トランキング プロトコル（p.13-3）

VSAN トランキングの不一致

E ポート間で VSAN を誤って設定すると、2 つの VSAN でトラフィックがマージされる（そのために両方の VSAN が一致しなくなる）などの問題につながることがあります。VSAN トランキング プロトコルでは ISL の両側で VSAN インターフェイスが確認され、VSAN のマージが回避されます（図 13-2 を参照）。

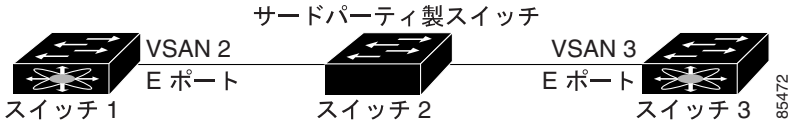
図 13-2　VSAN の不一致



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

2 つの Nexus 5000 シリーズ スイッチの間にサードパーティ製スイッチが配置されている場合、トランキング プロトコルは VSAN のマージを検出できません（図 13-3 を参照）。

図 13-3　サードパーティ製スイッチの VSAN 不一致



VSAN 2 および VSAN 3 は、ネーム サーバおよびゾーン アプリケーションにおいて重複エントリで事実上マージされます。Cisco MDS 9000 Fabric Manager は、このようなトポロジの検出に役立ちます。

VSAN トランキング プロトコル

トランキング プロトコルは、E ポートおよび TE ポートの動作において重要です。トランキング プロトコルは次の機能をサポートします。

- 動作トランク モードの動的ネゴシエーション。
- トランク許可 VSAN の共通セットの選択。
- ISL 間における VSAN 不一致の検出。

VSAN トランキング プロトコルはデフォルトでイネーブルです。トランキング プロトコルをスイッチでディセーブルにすると、そのスイッチのポートには新しいトランク設定を適用できません。既存のトランク設定は影響されません。TE ポートは引き続きトランク モードで機能しますが、以前（トランキング プロトコルがイネーブルたったときに）ネゴシエーションした VSAN のみでトラフィックをサポートします。このスイッチに直接接続されているその他のスイッチは、接続インターフェイスで同じように影響されます。トランキング以外の ISL 間で、さまざまなポート VSAN からのトラフィックをマージしなければならない場合は、トランキング プロトコルをディセーブルにします。

VSAN トランキングの設定

ここでは、VSAN トランキングの設定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。

- 注意事項および制約事項（p.13-4）
- トランク モードの概要（p.13-4）
- トランク モードの設定（p.13-5）
- トランク許可 VSAN リストの概要（p.13-6）
- VSAN の許可アクティブ リストの設定（p.13-7）

注意事項および制約事項

VSAN トランキングを設定する場合、次の点に注意してください。

- VSAN トランキング ISL の両側が同じポート VSAN に属すようにすることを推奨します。ポート VSAN が異なるプラットフォームまたはファブリック スイッチでは、片側がエラーを返し、反対側は接続されません。
- 矛盾した設定を避けるには、すべての E ポートをシャットダウンしてから VSAN トランキング プロトコルのイネーブル化またはディセーブル化を行います。

トランク モードの概要

デフォルトでは、トランク モードはすべてのファイバ チャネル インターフェイスでイネーブルです。ただし、トランク モード設定は E ポート モードのみで有効です。トランク モードは、on（イネーブル）、off（ディセーブル）、auto（自動）のうちいずれかに設定できます。デフォルトのトランク モードは on です。リンクの両端のトランク モード設定により、リンクのトランキング状態および両端のポート モードが決まります（表 13-1 を参照）。

表 13-1　スイッチ間のトランク モード ステータス

トランク モード設定		状態およびポート モードの結果	
スイッチ 1	**スイッチ 2**	**トランキング状態**	**ポート モード**
on	auto または on	トランキング（EISL）	TE ポート
off	auto、on、off のいずれか	トランキングなし（ISL）	E ポート
auto	auto	トランキングなし（ISL）	E ポート

ヒント　Nexus 5000 シリーズ スイッチでの推奨設定は、トランクの片側が auto、反対側が on です。

（注）　サードパーティ製スイッチに接続した場合、トランク モード設定は作用しません。ISL は常にトランキングがディセーブルの状態です。

トランク モードの設定

Fabric Manager を使用してトランク モードを設定する手順は、次のとおりです。

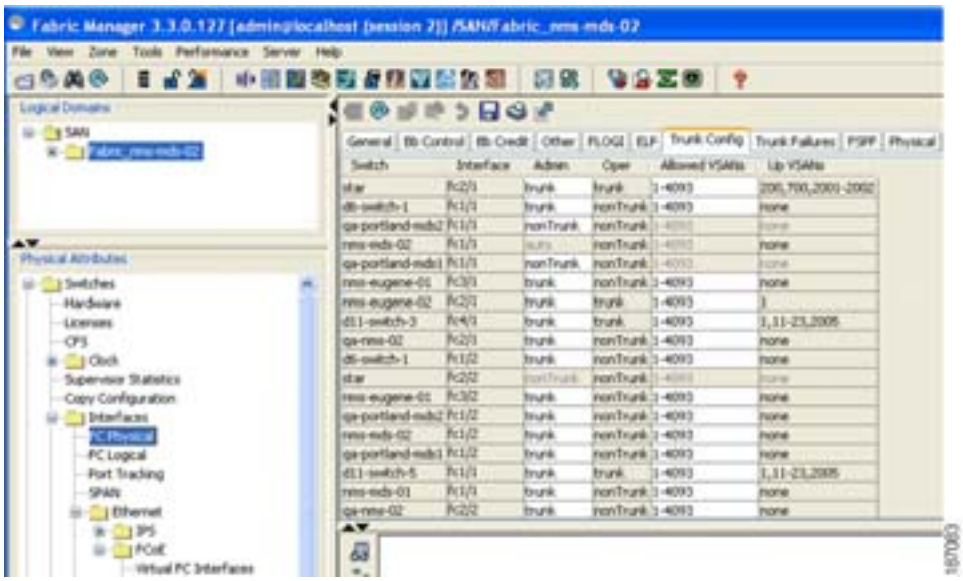
ステップ 1　Physical Attributes ペインで、**Switches > Interfaces** を展開して、**FC Physical** を選択します。

Information ペインにインターフェイス設定が表示されます。

ステップ 2　**Trunk Config** タブをクリックして、選択したインターフェイスのトランキング モードを変更します。

図 13-4 に示す情報が表示されます。

図 13-4　トランキングの設定



ステップ 3　Admin および Allowed VSANs の値を変更します。

ステップ 4　**Trunk Failures** タブをクリックして、ISL の障害状態をチェックします。

FailureCause カラムに理由が表示されます（図 13-5 を参照）。

図 13-5　Trunk Failures タブ

ステップ 5　**Apply Changes** アイコンをクリックします。

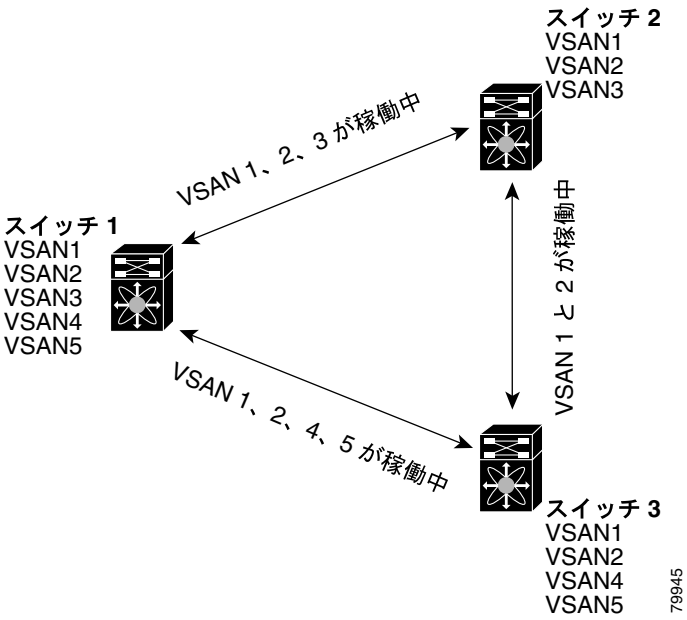
トランク許可 VSAN リストの概要

各ファイバ チャネル インターフェイスには、トランク許可 VSAN リストが関連付けられています。TE ポート モードの場合、フレームはこのリストで指定されている 1 つ以上の VSAN で送受信されます。デフォルトでは、VSAN 範囲全体（1 ～ 4093）がトランク許可リストに組み込まれています。

スイッチで設定されてアクティブになっている VSAN の共通セットは、インターフェイスのトランク許可 VSAN リストに組み込まれ、これは*許可アクティブ VSAN* と呼ばれます。トランキング プロトコルでは許可アクティブ VSAN のリストが ISL の 2 つの端で使用され、トラフィックが許可される動作 VSAN のリストが判断されます。

図 13-6 では、トランク許可 VSAN のデフォルト設定で、スイッチ 1 に VSAN 1 ～ 5、スイッチ 2 に VSAN 1 ～ 3、スイッチ 3 に VSAN 1、2、4、5 が含まれています。3 つのスイッチすべてで設定されているすべての VSAN は許可アクティブです。ただし、図 13-6 のように、ISL の端での許可アクティブ VSAN の共通セットのみが、動作状態になります。

図 13-6　デフォルトの許可アクティブ VSAN 設定



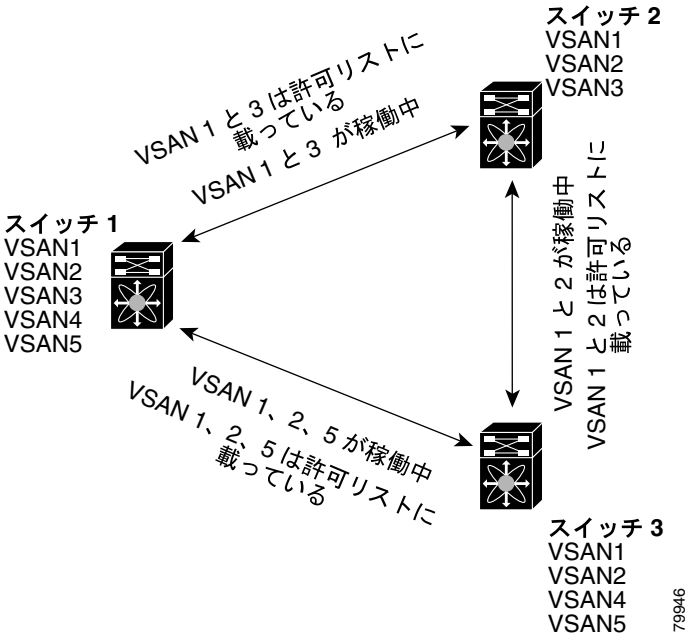
許可アクティブ リストから VSAN の選択セットを設定し、トランキング ISL で指定されている VSAN へのアクセスを制御できます。

図 13-6 を例として使用し、インターフェイスごとに許可 VSAN のリストを設定できます（図 13-7 を参照）。たとえば、スイッチ 1 に接続されている ISL の許可 VSAN リストから VSAN 2 および 4 を削除すると、ISL ごとの VSAN の動作許可リストは次のようになります。

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

その結果、VSAN 2 は、スイッチ 1 からスイッチ 3 を通ってスイッチ 2 にルーティングされます。

図 13-7　動作および許可の VSAN 設定



VSAN の許可アクティブ リストの設定

Fabric Manager を使用して VSAN の許可アクティブ リストをインターフェイスに設定する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Interfaces** を展開して、**FC Physical** を選択します。

Information ペインにインターフェイス設定が表示されます。

ステップ 2　**Trunk Config** タブをクリックします。

現在のトランク設定が表示されます。

ステップ 3　設定するインターフェイスごとに、Allowed VSANs を許可 VSAN のリストに設定します。

ステップ 4　これらの変更を保存する場合は **Apply Changes** をクリックします。保存されていない変更を廃棄する場合は **Undo Changes** を クリックします。

デフォルト設定

表 13-2 に、トランキング パラメータのデフォルト設定を示します。

表 13-2　デフォルトのトランク設定パラメータ

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

CHAPTER 14

SAN ポート チャネルの設定

SAN ポート チャネルは、複数の物理インターフェイスを 1 つの論理インターフェイスに集約し、より高い集約帯域幅、ロード バランシング、リンク冗長性を提供するものです。

Nexus 5000 シリーズ スイッチでは、SAN ポート チャネルに物理ファイバ チャネル インターフェイスを含めることができますが、仮想ファイバ チャネル インターフェイスを含めることはできません。SAN ポート チャネルには、最大 8 つのファイバ チャネル インターフェイスを含めることができます。

この章では、スイッチで提供される SAN ポート チャネル機能について説明します。この章の内容は次のとおりです。

- SAN ポート チャネルの概要（p.14-2）
- SAN ポート チャネルの設定（p.14-6）
- SAN ポート チャネルのインターフェイス（p.14-13）
- ポート チャネル プロトコル（p.14-17）
- SAN ポート チャネル設定の確認（p.14-21）
- デフォルト設定（p.14-21）

SAN ポート チャネルの概要

SAN ポート チャネルには、次の機能があります。

- ISL（スイッチ間リンク）（E ポート）または EISL（TE ポート）を介してポイントツーポイント接続を提供します。複数のリンクを SAN ポート チャネルに結合することができます。
- チャネルで機能しているすべてのリンクにトラフィックを配信することによって、ISL 上の集約帯域幅を増加させます。
- 複数のリンク間で負荷を分散し、最適な帯域利用を維持します。ロード バランシングは、送信元 ID、宛先 ID、および Exchange ID（OX ID）に基づきます。
- ISL にハイ アベイラビリティをもたらします。1 つのリンクに障害が発生した場合、そのリンクで伝送されていたトラフィックは残りのリンクに切り替えられます。SAN ポート チャネルでリンクが 1 つダウンしても、上位層プロトコルでは認識されません。上位層プロトコルから見れば、帯域幅が減っていても引き続きリンクは存在しています。ルーティング テーブルはリンク障害の影響を受けません。

Nexus 5000 シリーズ スイッチは、最大 4 つの SAN ポート チャネルをサポートします（各ポート チャネルに 8 つのインターフェイス）。ポート チャネル番号は各チャネル グループに関連付けられた、（各スイッチ内で）一意の識別番号です。この番号の範囲は 1 ～ 256 です。

ここでは SAN について、次の内容を説明します。

- ポート チャネルおよび VSAN トランキングの概要（p.14-3）
- ロード バランシングの概要（p.14-4）

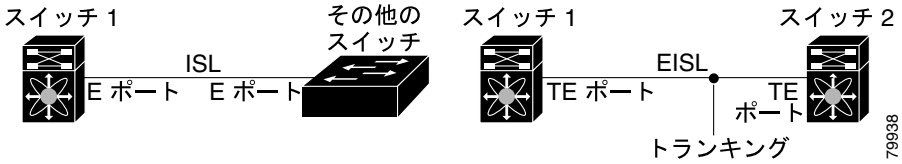
ポート チャネルおよび VSAN トランキングの概要

Nexus 5000 シリーズ のスイッチは、VSAN トランキングおよびポート チャネルを次のように実装します。

- SAN ポート チャネルは、複数の物理リンクを 1 つの集約論理リンクに統合できます。
- 業界標準の E ポートは、他のベンダー スイッチにリンクでき、図 14-1 の左側に示されているように ISL と呼ばれます。
- VSAN トランキングは、EISL 形式フレームを送信するリンクが、複数の VSAN にトラフィックを伝送できるようにします。E ポートでトランキングを動作させると、その E ポートは TE ポートになります。EISL はシスコ スイッチのみを接続できます（図 14-1 の右側を参照）。

トランク インターフェイスの詳細については、第 13 章「VSAN トランキングの設定」を参照してください。

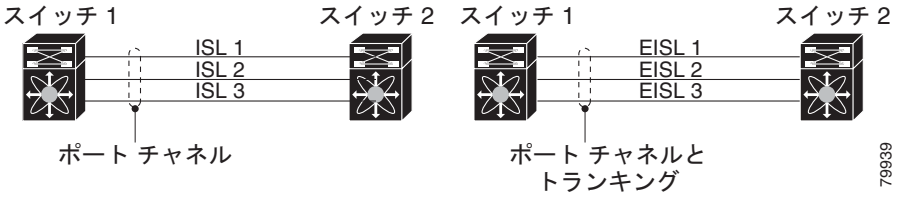
図 14-1　VSAN トランキングのみの場合



E ポートであるメンバーで SAN ポート チャネルを作成できます（図 14-2 の左側を参照）。この設定では、ポート チャネルが論理 ISL を実装します（1 つの VSAN のトラフィックを伝送）。

TE ポートであるメンバーで SAN ポート チャネルを作成できます（図 14-2 の右側を参照）。この設定では、ポート チャネルが論理 EISL を実装します（複数の VSAN のトラフィックを伝送）。

図 14-2　ポート チャネルおよび VSAN トランキングの場合



ロード バランシングの概要

ロード バランシング機能は、次の方法により提供されます。

- フロー ベース — 送信元から送信先へのすべてのフレームが、特定フロー用の同一リンクを流れます。つまり、最初のフローの交換に選択されたリンクが、その後すべての交換に使用されます。
- エクスチェンジ ベース — 交換の最初のフレームがリンクに割り当てられ、その後の交換のフレームは同じリンクを流れます。ただし、後続の交換で別のリンクが使用されることがあります。この方法により、交換ごとにフレームの順序を維持しながら、より細かいロード バランシングが可能になります。

図 14-3 は、フローベースのロード バランシングの動作を示しています。フローの最初のフレームが転送用にインターフェイスで受信されるときは、リンク 1 が選択されます。そのフローの各後続フレームは同じリンクで送信されます。SID1 および DID1 のフレームではリンク 2 は使用されません。

図 14-3　SID1、DID1、およびフロー ベースのロード バランシング

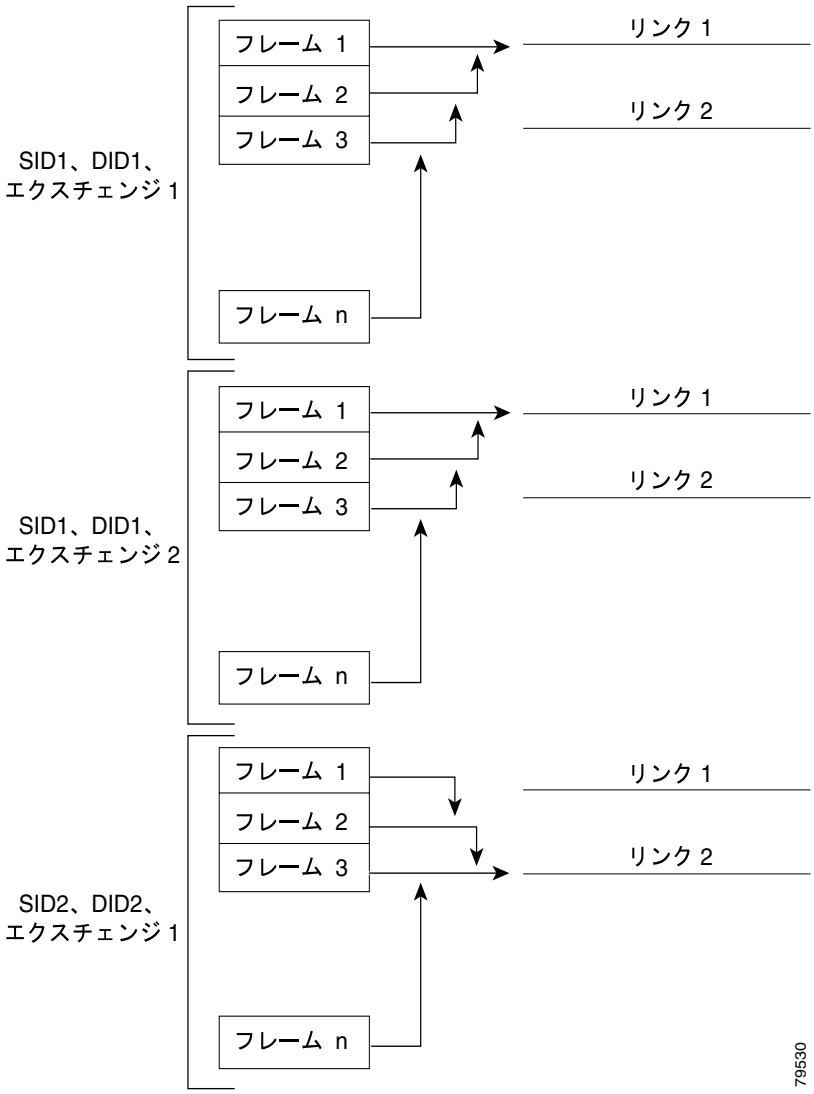
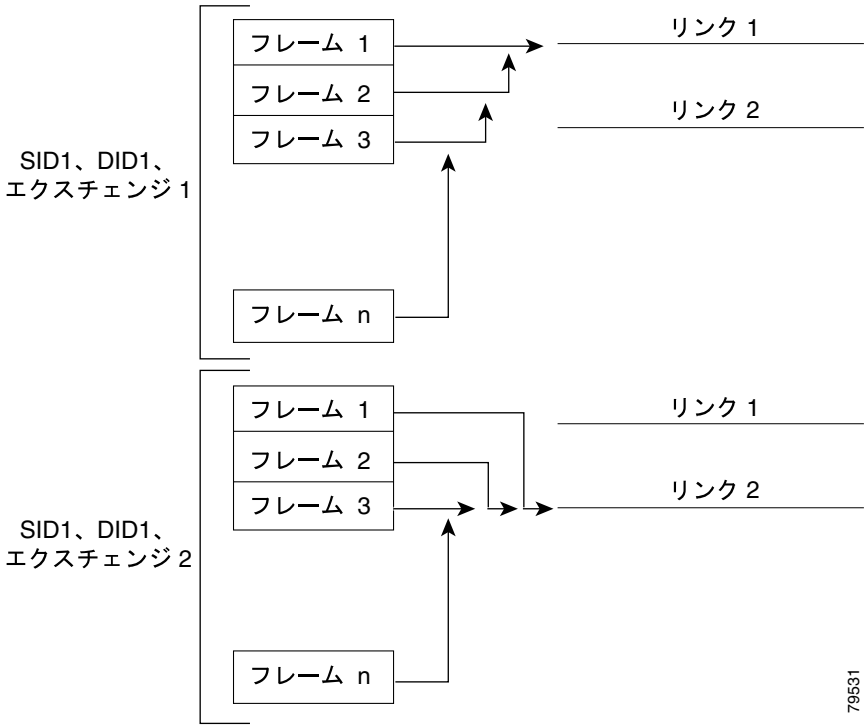


図 14-4 は、エクスチェンジ ベースのロード バランシングの動作を示しています。交換の最初のフレームが転送用にインターフェイスで受信されるときは、リンク 1 がハッシュ アルゴリズムで選択されます。その交換の残りの全フレームは、同じリンクで送信されます。エクスチェンジ 1 では、フレームはリンク 2 を使用しません。次のエクスチェンジでは、リンク 2 がハッシュ アルゴリズムで選択されます。これで、エクスチェンジ 2 のすべてのフレームでリンク 2 が使用されます。

図 14-4　SID1、DID1、およびエクスチェンジ ベースのロード バランシング



SAN ポート チャネルの設定

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

図 14-5 は、有効な SAN ポート チャネル設定の例です。

図 14-5　有効な SAN ポート チャネル設定

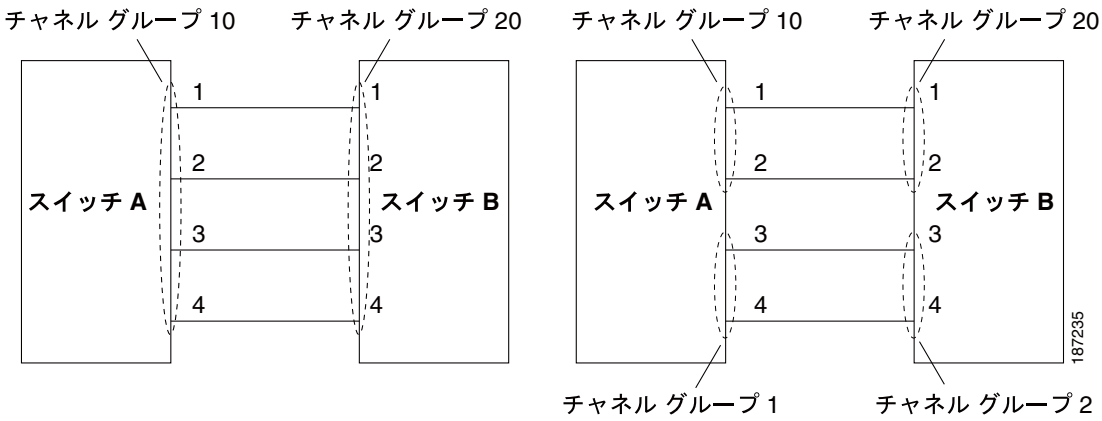
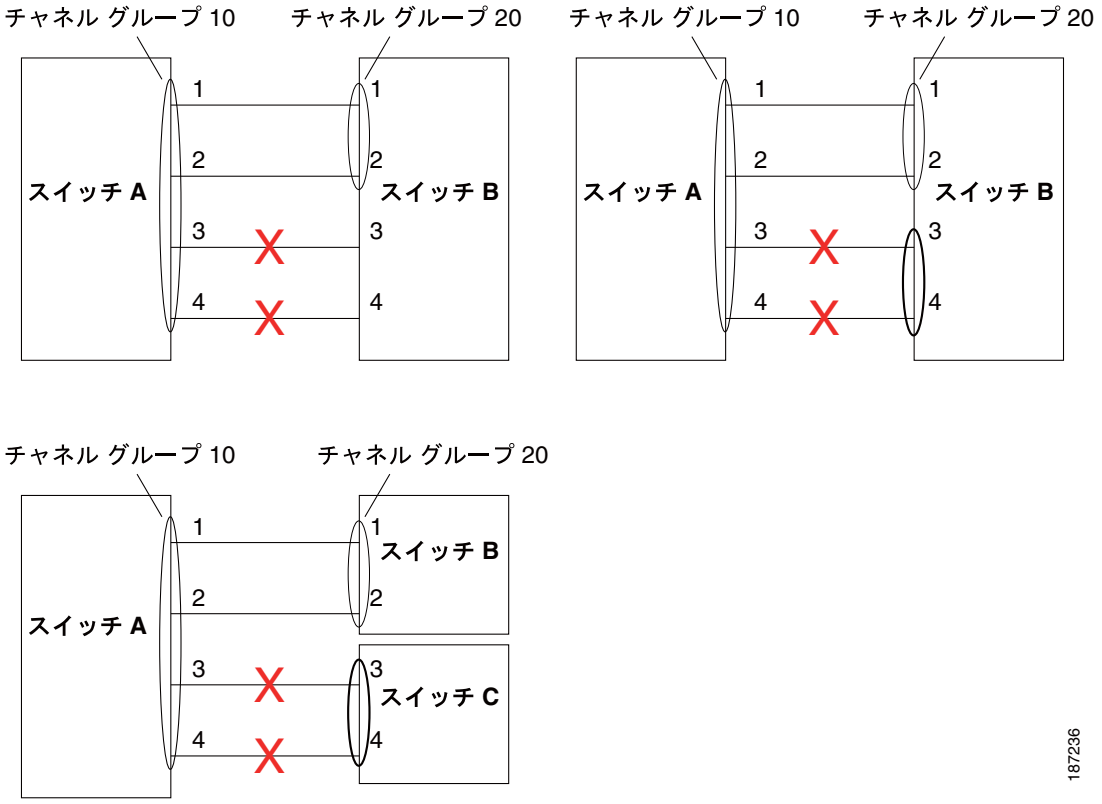


図 14-6 に、無効な設定例を示します。1、2、3、4 の順序でリンクがアップする場合、ファブリックの設定が誤っているので、リンク 3 および 4 は動作上のダウンになります。

図 14-6　誤った設定



ここでは、SAN ポート チャネルの設定方法および変更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。

- SAN ポート チャネル設定の注意事項（p.14-7）
- SAN ポート チャネルの設定（p.14-7）
- SAN ポート チャネル モードの概要（p.14-10）
- SAN ポート チャネル削除の概要（p.14-11）
- SAN ポート チャネルの削除（p.14-12）

SAN ポート チャネル設定の注意事項

SAN ポート チャネルを設定する前に、次の注意事項について検討してください。

- SAN ポート チャネルを、両方に拡張モジュールを使用したファイバ チャネル ポートを使用して設定します（拡張モジュールのうち 1 つに障害が発生した場合の可用性を向上させるため）。
- 1 つの SAN ポート チャネルを、別のセットのスイッチに接続しないようにします。SAN ポート チャネルでは、同一セットのスイッチ間におけるポイントツーポイント接続が必要です。

SAN ポート チャネルの設定を誤った場合は、誤設定メッセージを受信することがあります。このメッセージを受信した場合、エラーが検出されたため、ポート チャネルの物理リンクはディセーブルになります。

次の要件が満たされない場合、SAN ポート チャネルのエラーが検出されます。

- SAN ポート チャネルのいずれかの側の各スイッチに、同じ数のインターフェイスが接続されている必要があります。
- 各インターフェイスは、反対側の対応するインターフェイスに接続する必要があります（無効な設定の例については、図 14-6 を参照）。
- ポート チャネルの設定後は、SAN ポート チャネルのリンクを変更できません。ポート チャネルの設定後にリンクを変更する場合は、ポート チャネル内のインターフェイスにリンクを再接続してリンクを再びイネーブルにします。

3 つすべての条件を満たしていない場合、エラー リンクはディセーブルになります。

SAN ポート チャネルの設定

Fabric Manager の Port Channel Wizard を使用して SAN ポート チャネルを作成する手順は、次のとおりです。

ステップ 1　ツールバーで **Port Channel Wizard** アイコンをクリックします（図 14-7 を参照）。

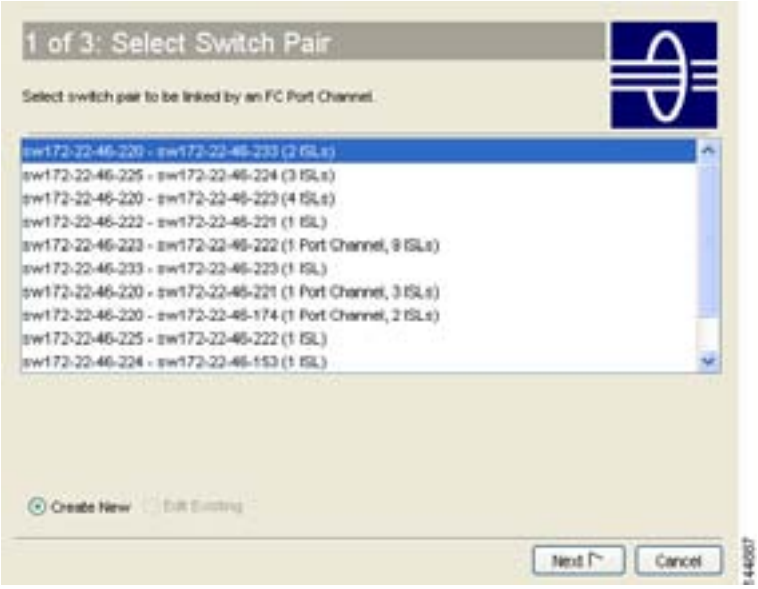
図 14-7　Port Channel Wizard アイコン

Port Channel Wizard の最初の画面が表示されます。

ステップ 2　スイッチ ペアを選択します。

図 14-8 に、スイッチ ペアのリストを表示します。

図 14-8　スイッチ ペアの選択

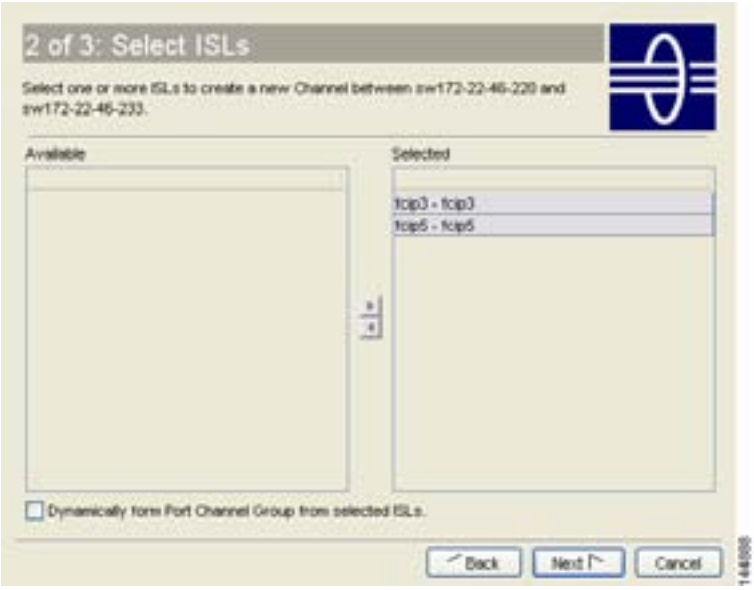


ステップ 3　**Next** をクリックします。

ステップ 4　ISL を選択します。

図 14-9 に、ISL のリストを示します。

図 14-9　ISL の選択

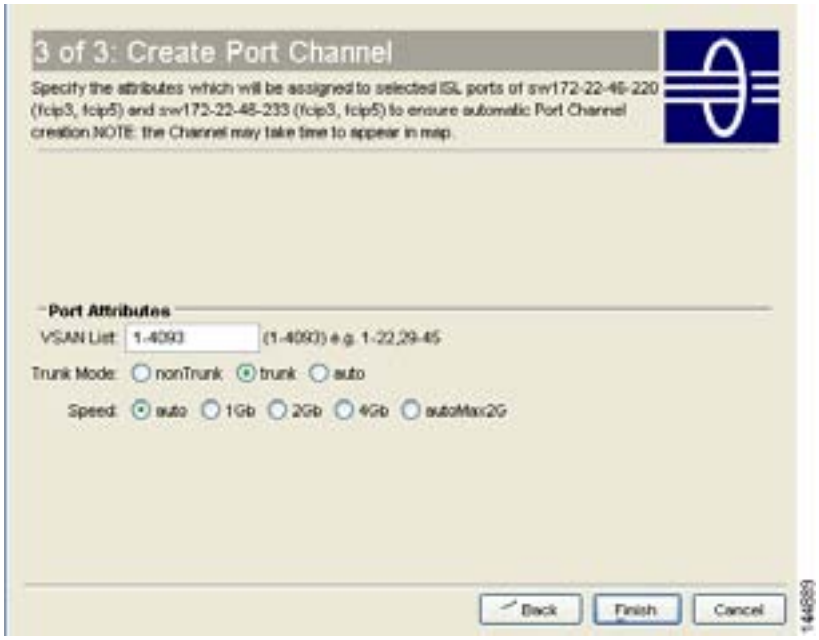


ステップ 5　（任意）SAN ポート チャネルを動的に作成し、ISL プロパティの Admin、Trunk、Speed、および VSAN 属性で同一にする場合は、**Dynamically form Port Channel Group from selected ISLs** チェックボックスをオンにします。

ステップ 6　**Next** をクリックします。

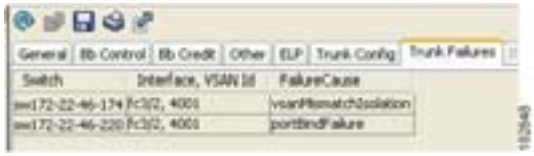
ステップ 7　選択した ISL から SAN ポート チャネルを動的に形成した場合は、最後の Port Channel Wizard 画面が表示されます（図 14-10 を参照）。VSAN List、Trunk Mode、Speed を設定して、ステップ 11 に進みます。

図 14-10　ポート チャネルの動的な形成



ステップ 8　SAN ポート チャネルを動的な形成を選択しなかった場合は、3 番めの Port Channel Wizard ダイアログボックスが表示されます （図 14-11 を参照）。

図 14-11　ポート チャネルの作成



ステップ 9　必要に応じて、各スイッチのチャネル ID または説明を変更します。

ステップ 10 画面下部に表示される属性を調べ、必要に応じて設定します。

図 14-11 には次の属性が示されています。

- VSAN List — ISL が属する VSAN のリスト。
- Trunk Mode — SAN ポート チャネル内のリンク上でトランキングをイネーブルにすることができます。TE ポート間にリンクが存在する場合は、**trunking** を選択します。E ポート間にリンクが存在する場合は、**nontrunking** を選択します。不明な場合は、**auto** を選択します。
- Force Admin, Trunk, Speed, and VSAN attributes to be identical — チャネル内のすべての物理ポートで同じパラメータ設定が使用されるようにします。これらの設定が同じでない場合、ポートは SAN ポート チャネルに属することができません。
- Speed — ポートの速度値は、**auto**、**1Gb**、**2Gb**、**4Gb**、**autoMax2G** のうちいずれかにします。

ステップ 11 **OK** をクリックします。

SAN ポート チャネルが作成されます。Fabric ペインに新しいポート チャネルが表示されるまでに、数分間かかることがあります。

SAN ポート チャネル モードの概要

チャネル グループのモード パラメータで各 SAN ポート チャネルを設定し、このチャネル グループのすべてのメンバー ポートでポート チャネル プロトコル動作を決めることができます。チャネル グループ モードに可能な値は次のとおりです。

- On（デフォルト）— メンバー ポートは SAN ポート チャネルの一部として動作するか、非アクティブのままになります。このモードでは、ポート チャネル プロトコルが始まりません。しかしポート チャネル プロトコル フレームをピア ポートから受信した場合、ソフトウェアはネゴシエーション不能ステータスを示します。On モードで設定されたポート チャネルでは、ポート チャネル設定でポートの追加または削除を行う場合、片側のポート チャネル メンバー ポートのイネーブル化およびディセーブル化を明示的に行う必要があります。ローカルとリモートのポートが相互に接続されていることを物理的に確認します。
- Active — ピア ポートのチャネル グループ モードに関係なく、メンバー ポートはピア ポートとポート チャネル プロトコル ネゴシエーションを始めます。ピア ポートがチャネル グループ内で設定されていて、ポート チャネル プロトコルをサポートしないか、ネゴシエーション不能ステータスで応答した場合は、デフォルトで On モードの動作となります。Active ポート チャネル モードでは、片側でポート チャネル メンバー ポートのイネーブル化およびディセーブル化を明示的に行わなくても、自動回復が可能です。

表 14-1 に、On モードと Active モードの比較を示します。

表 14-1　チャネル グループ設定の違い

On モード	Active モード
プロトコルは交換されません。	ピア ポートとポート チャネル プロトコル ネゴシエーションを行います。
動作値に SAN ポート チャネルとの互換性がない場合、インターフェイスは一時停止状態になります。	動作値に SAN ポート チャネルとの互換性がない場合、インターフェイスは分離状態になります。

表 14-1　チャネル グループ設定の違い

On モード	Active モード
ポート チャネル メンバー ポート設定の追加または変更を行うとき、片側のポート チャネル メンバー ポートのディセーブル化（shut）およびイネーブル化（no shut）を明示的に行う必要があります。	ポート チャネル インターフェイスの追加または変更を行うと、SAN ポート チャネルは自動的に回復します。
ポートの初期化は同期されません。	ピア スイッチ間でチャネルのすべのポートの起動が同期されます。
プロトコルが交換されないため、誤設定が検出されないことがあります。	ポート チャネル プロトコルが使用され、誤設定が確実に検出されます。
設定を誤ったポートは一時停止状態に移行します。片側でメンバー ポートのディセーブル化（shut）およびイネーブル化（no shut）を明示的に行う必要があります。	誤設定の訂正のため、設定を誤ったポートは分離状態に移行します。設定の誤りを訂正したら、プロトコルによって自動的に回復されます。
これは、デフォルトのモードです。	このモードは明示的に設定する必要があります。

Fabric Manager を使用して Active モードを設定する手順は、次のとおりです。

ステップ 1　**ISL** を展開して、Physical Attributes ペインで **Port Channels** を選択します。

Information ペインに設定したポート チャネルが表示されます。

ステップ 2　**Protocols** タブをクリックします。Mode ドロップダウン リストから、ポート チャネルに適したモードを選択します。

ステップ 3　**Apply Changes** アイコンをクリックし、変更内容を保存します。

SAN ポート チャネル削除の概要

SAN ポート チャネルを削除すると、対応するチャネル メンバシップも削除されます。削除した SAN ポート チャネルのすべてのインターフェイスは、個別の物理リンクに変換されます。SAN ポート チャネルの削除後、使用するモード（Active および On）に関係なく、片側のポートは正常にダウンします。これは、インターフェイスがダウンしてもフレームが失われないことを示します（「インターフェイスの管理ステートの設定」[p.10-10] を参照）。

あるポートの SAN ポート チャネルを削除すると、削除した SAN ポート チャネル内の各ポートは互換性のあるパラメータ設定（速度、モード、ポート VSAN、許可されている VSAN、ポート セキュリティ）を維持します。この設定は必要に応じて明示的に変更できます。

- スイッチ全体の矛盾状態を避けて、スイッチ全体の一貫性を維持するために、デフォルトの On モードを使用する場合、ポートはシャットダウンします。このポートは明示的に再びイネーブルにする必要があります。
- Active モードを使用すると、ポート チャネル ポートは削除から自動的に回復します。

SAN ポート チャネルの削除

Fabric Manager の Port Channel Wizard を使用してポート チャネルを削除する手順は、次のとおりです。

ステップ 1　ツールバーで **Port Channel Wizard** アイコンをクリックします（図 14-12 を参照）。

図 14-12　Port Channel Wizard アイコン

Port Channel Wizard の最初の画面が表示されます。

ステップ 2　削除する既存ポート チャネルを選択して、**Next** を選択します。

このポート チャネルに現在関連している ISL のリストが表示されます。

ステップ 3　**Next** をクリックします。

関連 ISL およびこのポート チャネルに使用可能な ISL の編集可能リストが表示されます。

ステップ 4　各関連 ISL をクリックして左矢印をクリックします。ポート チャネルからすべての ISL が削除されます。

ステップ 5　このポート チャネルを削除するには、**Delete Port Channel If Empty** チェックボックスをオンにします。

ステップ 6　この変更を保存する場合は、**Finish** をクリックします。変更を廃棄する場合は、**Cancel** をクリックします。

SAN ポート チャネルのインターフェイス

既存 SAN ポート チャネルで物理ファイバ チャネル インターフェイス（またはある範囲のインターフェイス）の追加または削除を行うことができます。設定で互換性があるパラメータは SAN ポート チャネルにマッピングされます。SAN ポート チャネルにインターフェイスを追加すると、SAN ポート チャネルのチャネル サイズおよび帯域幅が増加します。SAN ポート チャネルからインターフェイスを削除すると、SAN ポート チャネルのチャネル サイズおよび帯域幅は減少します。

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

ここでは、SAN ポート チャネルのインターフェイス設定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。

- SAN ポート チャネルへのインターフェイス追加の概要（p.14-13）
- SAN ポート チャネルへのインターフェイスの追加（p.14-14）
- インターフェイスの強制追加（p.14-15）
- SAN ポート チャネルからのインターフェイス削除の概要（p.14-15）
- SAN ポート チャネルからのインターフェイスの削除（p.14-16）

SAN ポート チャネルへのインターフェイス追加の概要

既存 SAN ポート チャネルに物理インターフェイス（またはある範囲のインターフェイス）を追加できます。設定で互換性があるパラメータは SAN ポート チャネルにマッピングされます。SAN ポート チャネルにインターフェイスを追加すると、SAN ポート チャネルのチャネル サイズおよび帯域幅が増加します。

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

互換性チェック

互換性チェックにより、チャネルのすべての物理ポートで同じパラメータ設定が使用されていることを確認します。同じパラメータ設定が使用されていないと、SAN ポート チャネルの一部にはなれません。互換性チェックは、SAN ポート チャネルにポートを追加する前に実行します。

このチェックにより、次のパラメータおよび設定が SAN ポート チャネルの両端で一致することを確認します。

- 機能パラメータ（インターフェイスのタイプ、両端のファイバ チャネル）。
- 管理上の互換性のパラメータ（速度、モード、ポート VSAN、許可されている VSAN、ポート セキュリティ）。
- 動作パラメータ（速度およびリモート スイッチの WWN）。

リモート スイッチの互換性パラメータおよび管理上のパラメータに、ローカル スイッチの機能パラメータと管理パラメータとの互換性がない場合、ポートを追加する手順はエラーになります。互換性チェックに問題がない場合、インターフェイスは動作し、対応する互換性パラメータ設定がこのインターフェイスに適用されます。

一時停止状態および分離状態

動作パラメータに互換性がない場合、互換性チェックはエラーになり、インターフェイスは設定モードに基づいて一時停止状態か分離状態になります。

- インターフェイスは、On モードに設定されている場合、一時停止状態になります。
- インターフェイスは、Active モードに設定されている場合、分離状態になります。

「原因コード」（p.10-6）を参照してください。

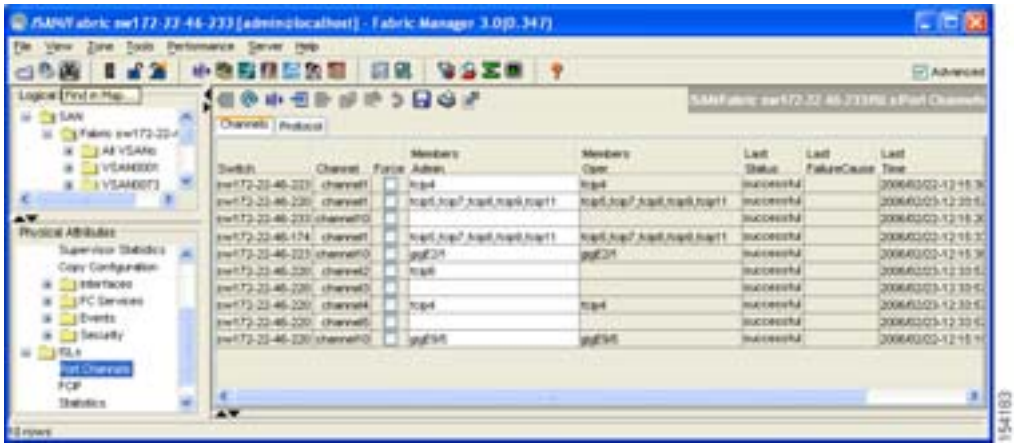
SAN ポート チャネルへのインターフェイスの追加

Fabric Manager を使用してインターフェイスまたはある範囲のインターフェイスを SAN ポート チャネルに追加する手順は、次のとおりです。

ステップ 1　**ISL** を展開して、Physical Attributes ペインで **Port Channels** を選択します。

Information ペインに設定した SAN ポート チャネルが表示されます（図 14-13 を参照）。

図 14-13　ポート チャネル



ステップ 2　**Channels** タブをクリックし、編集するスイッチおよび SAN ポート チャネルを探します。

ステップ 3　SAN ポート チャネルに追加するインターフェイスまたはインターフェイスのリストに、Members Admin を設定します。

ステップ 4　変更を保存する場合は、**Apply Changes** をクリックします。変更を廃棄する場合は、**Undo Changes** をクリックします。

インターフェイスの強制追加

SAN ポート チャネルにより、ポート設定の上書きを強制することができます。この場合、インターフェイスは SAN ポート チャネルに追加されます。

- デフォルトの ON モードを使用してスイッチ間で矛盾状態を避けて、スイッチ間の一貫性を維持する場合、ポートはシャットダウンします。このポートは明示的に再びイネーブルにする必要があります。
- Active モードを使用すると、ポート チャネル ポートは追加から自動的に回復します。

（注） インターフェイス内から SAN ポート チャネルを作成するときは、**Force** オプションを使用できません。

メンバーの強制追加後、使用するモード（Active および On）に関係なく、片側のポートは正常にダウンします。これは、インターフェイスがダウンしてもフレームが失われないことを示します（「インターフェイスの管理ステートの設定」[p.10-10] を参照）。

Fabric Manager を使用して SAN ポート チャネルにポートを強制追加する手順は、次のとおりです。

ステップ 1　**ISL** を展開して、Physical Attributes ペインで **Port Channels** を選択します。

Information ペインに設定したポート チャネルが表示されます。

ステップ 2　**Channels** タブをクリックし、編集するスイッチおよび SAN ポート チャネルを探します。

ステップ 3　SAN ポート チャネルに追加するインターフェイスまたはインターフェイスのリストに、Members Admin を設定します。

ステップ 4　このインターフェイスの追加を強制するには、**Force** チェックボックスをオンにします。

ステップ 5　**Apply Changes** アイコンをクリックし、変更内容を保存します。

SAN ポート チャネルからのインターフェイス削除の概要

物理インターフェイスを SAN ポート チャネルから削除すると、チャネルのメンバシップは自動的に更新されます。削除したインターフェイスが最後の動作インターフェイスである場合、ポート チャネルのステータスはダウン状態に変更されます。SAN ポート チャネルからインターフェイスを削除すると、SAN ポート チャネルのチャネル サイズおよび帯域幅は減少します。

- デフォルトの ON モードを使用してスイッチ間で矛盾状態を避けて、スイッチ間の一貫性を維持する場合、ポートはシャットダウンします。このポートは明示的に再びイネーブルにする必要があります。
- Active モードを使用すると、ポート チャネル ポートは削除から自動的に回復します。

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

SAN ポート チャネルからのインターフェイスの削除

Fabric Manager を使用して物理インターフェイスまたはある範囲の物理インターフェイスを SAN ポート チャネルから削除する手順は、次のとおりです。

ステップ 1　**ISL** を展開して、Physical Attributes ペインで **Port Channels** を選択します。

Information ペインに設定した SAN ポート チャネルが表示されます。

ステップ 2　**Channels** タブをクリックし、編集するスイッチおよび SAN ポート チャネルを探します。

ステップ 3　Members the Admin カラムで、削除するインターフェイスまたはインターフェイスのリストを削除します。

ステップ 4　**Apply Changes** アイコンをクリックし、変更内容を保存します。

ポート チャネル プロトコル

スイッチ ソフトウェアには、強力なエラー検出機能および同期機能があります。チャネル グループを手動で設定できますが、自動的に作成することもできます。どちらの場合でも、チャネル グループの機能と設定パラメータは同じです。関連ポート チャネル インターフェイスに適用される設定を変更すると、その変更はチャネル グループのすべてのメンバーに伝わります。

Cisco SAN スイッチは、ポート チャネル設定を交換するプロトコルをサポートします。これにより、非互換 ISL でのポート チャネル管理が簡単になります。さらに自動作成モードでは、互換性があるパラメータを含む ISL により、手動操作なしでチャネル グループが自動的に作成されます。

ポート チャネル プロトコルは、デフォルトでイネーブルです。

ポート チャネル プロトコルにより、Cisco SAN スイッチにおけるポート チャネル機能モデルが拡張されます。ISL のピア ポート間の通信には、Exchange Peer Parameter（EPP）サービスが使用されます。各スイッチは、ピア ポートから受信した情報、およびローカル設定と動作値を使用し、それが SAN ポート チャネルの一部であるかどうかを判断します。このプロトコルでは、一連のポートが確実に同一 SAN ポート チャネルの一部になります。一連のポートが同一ポート チャネルの一部となるのは、互換性があるパートナーがすべてのポートに存在する場合のみです。

ポート チャネル プロトコルでは、次の 2 つのサブプロトコルが使用されます。

- 始動プロトコル — 誤った設定が自動的に検出され、訂正できるようになります。このプロトコルでは両側で SAN ポート チャネルが同期されるので、特定フローのすべてのフレーム（送信元 FC ID、宛先 FC ID、OX_ID によって識別）は両方向で同一の物理リンクによって伝送されます。これにより、書き込みアクセラレーションのようなアプリケーションが、FCIP リンクで SAN ポート チャネル用に動作するようになります。
- 自動作成プロトコル — 互換性があるポートが SAN ポート チャネルに自動的に集約されます。

ここでは、ポート チャネル プロトコルの設定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。

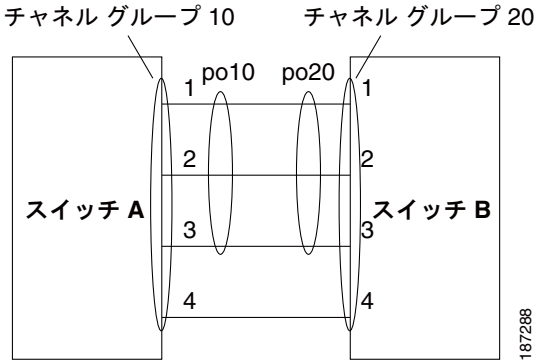
- チャネル グループの作成の概要（p.14-17）
- 自動作成の注意事項（p.14-19）
- 自動作成のイネーブル化および設定（p.14-19）
- 手動設定チャネル グループの概要（p.14-20）
- 手動設定チャネル グループへの変換（p.14-20）

チャネル グループの作成の概要

チャネル グループの自動作成がイネーブルの場合、手動操作なしで ISL をチャネル グループに自動的に設定できます。図 14-14 に、チャネル グループ自動作成の例を示します。

個別リンクとして最初の ISL がアップします。図 14-14 の例では、リンク A1-B1 がこれに該当します。次のリンク（この例では A2-B2）がアップすると、ポート チャネル プロトコルはこのリンクにリンク A1-B1 との互換性があるかどうかを識別し、それぞれのスイッチにチャネル グループ 10 および 20 を自動的に作成します。それぞれのポートに互換性の設定がある場合、リンク A3-B3 がチャネル グループ（およびポート チャネル）に参加できます。リンク A4-B4 が個別リンクとして動作するということは、このチャネル グループのその他のメンバー ポートとの互換性がないということです。

図 14-14　チャネル グループの自動作成



チャネル グループが形成されるときに、チャネル グループ番号が動的に割り当てられます。

ポートが初期化される順序に基づいて、チャネル グループ番号が同一セットのポート チャネルでもリブートすると変更されることがあります。

表 14-2 は、ユーザ設定チャネル グループと自動設定チャネル グループの違いを示しています。

表 14-2　チャネル グループ設定の違い

ユーザ設定チャネル グループ	自動作成チャネル グループ
ユーザが手動で設定します。	チャネル グループの自動作成が両側のすべてのポートでイネーブルである場合、互換性のある 2 つのスイッチ間で、互換性のあるリンクがアップしたときに自動的に作成されます。
メンバー ポートは、チャネル グループの自動作成に参加できません。自動作成機能は設定できません。	どのポートも、ユーザ設定チャネル グループのメンバーになりません。
チャネル グループのポートのサブセットで SAN ポート チャネルを形成できます。互換性がないポートは、On モード設定または Active モード設定により、一時停止状態か分離状態になります。	チャネル グループに組み込まれるすべてのポートが SAN ポート チャネルに参加します。メンバー ポートが分離状態や一時停止状態になることはありませんが、リンクに互換性がないことが判明した場合は、そのメンバー ポートはチャネル グループから削除されます。
SAN ポート チャネルで行った管理上の設定はチャネル グループのすべてのポートに適用され、ポート チャネル インターフェイスの設定は保存できます。	SAN ポート チャネルで行った管理上の設定はチャネル グループのすべてのポートに適用されますが、メンバー ポートの設定は保存され、ポート チャネル インターフェイスの設定は保存されません。このチャネル グループは、必要に応じて明示的に変換できます。
任意のチャネル グループを削除でき、チャネル グループにメンバーを追加できます。	チャネル グループは削除できません。チャネル グループへのメンバーの追加や削除もできません。チャネル グループは、メンバー ポートが存在しなくなると削除されます。

自動作成の注意事項

自動作成プロトコルを使用する場合には、次の事項に注意してください。

- 自動作成機能をイネーブルにした場合、SAN ポート チャネルの一部としてポートを設定することはできません。この 2 つの設定は相互に排他的です。
- 自動作成は、SAN ポート チャネルをネゴシエーションするため、ローカル ポートとピア ポートの両方でイネーブルにする必要があります。
- 集約は次の 2 つのいずれかの方法で行われます。
  - 互換性のある自動作成 SAN ポート チャネルにポートが集約されます。
  - 互換性がある別のポートにポートが集約され、新しい SAN ポート チャネルが形成されます。
- 新しく作成された SAN ポート チャネルは、アベイラビリティに基づいて大きいものから順に最大のポート チャネル番号から割り当てられます。ポート チャネルの番号すべてが使用されている場合、集約は行われません。
- メンバシップを変更したり、自動作成された SAN ポート チャネルを削除したりすることはできません。
- 自動作成をディセーブルにすると、すべてのメンバー ポートは自動作成 SAN ポート チャネルから削除されます。
- 最後のメンバーが自動作成 SAN ポート チャネルから削除されると、チャネルは自動的に削除され、番号は解放されて再利用されます。
- 自動作成 SAN ポート チャネルは、リブート後は固定されません。自動作成 SAN ポート チャネルは、固定的ポート チャネルと同一になるように手動で設定できます。SAN ポート チャネルを固定させた場合、自動作成機能はすべてのメンバー ポートでディセーブルになります。
- 自動作成機能のイネーブル化とディセーブル化は、ポートごとに、またはスイッチのすべてのポートで実行できます。この設定をイネーブルにすると、チャネル グループ モードはアクティブになります。このタスクのデフォルトはディセーブルです。
- チャネル グループの自動作成がインターフェイスでイネーブルになっている場合は、自動作成をディセーブルにしてから、ソフトウェアの前バージョンにダウングレードしたり、手動設定チャネル グループでインターフェイスを設定したりする必要があります。

ヒント　Nexus 5000 シリーズの任意のスイッチで自動作成をイネーブルにする場合は、スイッチ間の最低 1 つの相互接続ポートで自動作成を設定しないままにしておくことを推奨します。2 つのスイッチ間のすべてのポートを自動作成機能で同時に設定すると、自動作成 SAN ポート チャネルにポートが追加されるとき、ポートが自動的にディセーブルになって再度イネーブルになるので、この 2 つのスイッチ間でトラフィックが混乱することがあります。

自動作成のイネーブル化および設定

ポート チャネルの自動作成を設定するには、Port Channel Wizard で **Dynamically form Port Channel Group from selected ISLs** オプションをチェックします。「SAN ポート チャネルの設定」（p.14-7）を参照してください。

手動設定チャネル グループの概要

ユーザ設定チャネル グループは、自動作成チャネル グループに変換できません。しかし、自動作成チャネル グループを手動チャネル グループに変換することはできます。このタスクは、元に戻すことはできません。チャネル グループ番号は変化しませんが、メンバー ポートは手動設定チャネル グループのプロパティに従って動作し、チャネル グループの自動作成はすべてのメンバー ポートで暗黙的にディセーブルになります。

ヒント　固定をイネーブルにする場合は、SAN ポート チャネルの両側でイネーブルにしてください。

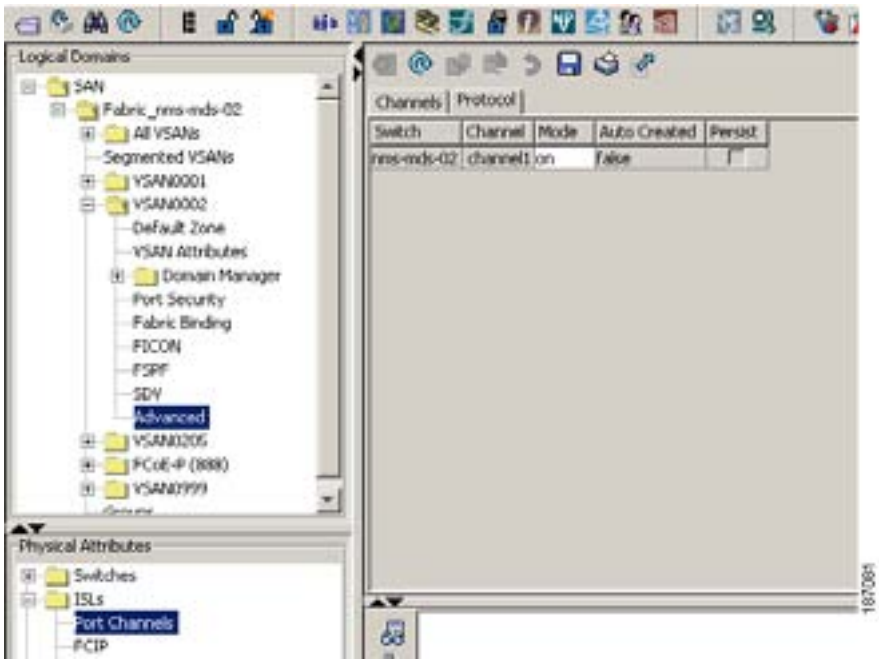
手動設定チャネル グループへの変換

Fabric Manager を使用して自動作成チャネル グループをユーザ設定チャネル グループに変換する手順は、次のとおりです。

ステップ 1　**ISL** を展開して、Physical Attributes ペインで **Port Channels** を選択します。**Protocol** タブをクリックします。

図 14-15 に示すスイッチ プロトコルが表示されます。

図 14-15　スイッチ プロトコル



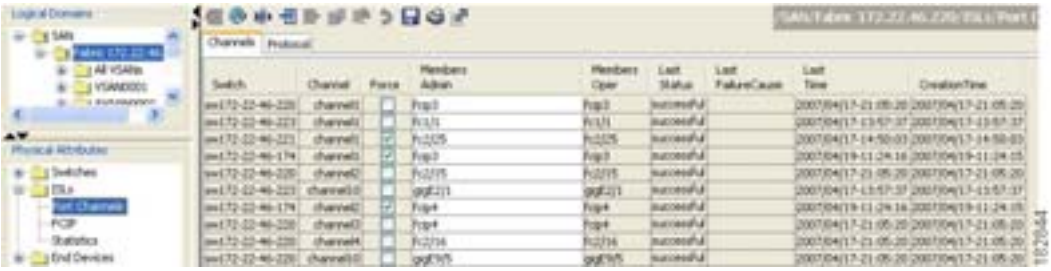
ステップ 2　手動設定チャネル グループに変換するチャネルごとに、**Persist** チェックボックスをオンにします。

ステップ 3　**Apply Changes** アイコンをクリックし、変更内容を保存します。

SAN ポート チャネル設定の確認

ポート チャネル設定を確認するには、Fabric Manager の Information ペインを使用します（図 14-16 を参照）。

図 14-16　Fabric Manager のポート チャネルのサマリー



デフォルト設定

表 14-3 に、SAN ポート チャネルのデフォルト設定値を示します。

表 14-3　デフォルトの SAN ポート チャネル パラメータ

パラメータ	デフォルト
ポート チャネル	デフォルトで FSPF がイネーブルです。
ポート チャネルの作成	管理上のアップ
デフォルトのポート チャネル モード	On
自動作成	ディセーブル

CHAPTER 15

VSAN の設定と管理

VSAN（仮想 SAN）を使用することによって、ファイバ チャネル ファブリックでより高度なセキュリティと安定性を得ることができます。VSAN は同じファブリックに物理的に接続されたデバイスを分離します。VSAN では、一般の物理インフラストラクチャで複数の論理 SAN を作成することができます。各 VSAN には最大 239 のスイッチを含めることができ、それぞれが独立したアドレス領域を持っているため、複数の VSAN で同時に同じ FC ID（ファイバ チャネル ID）を使用できます。この章の内容は、次のとおりです。

- VSAN の概要（p.15-2）
- VSAN の設定（p.15-6）
- デフォルト設定（p.15-12）

VSAN の概要

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

ここでは VSAN について、次の内容を説明します。

- VSAN トポロジ（p.15-2）
- VSAN の利点（p.15-4）
- VSAN とゾーン（p.15-4）

VSAN トポロジ

VSAN を導入すると、ネットワーク管理者はスイッチ、リンク、および 1 つまたは複数の VSAN を含む単一のトポロジを構築できます。このトポロジの各 VSAN では、SAN の動作およびプロパティが同じです。VSAN には次の特性もあります。

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

図 15-1 に、各階にスイッチが 1 つある合計 3 つのスイッチによるファブリックを示します。スイッチと接続されたデバイスの地理的な配置は、論理 VSAN のセグメンテーションには依存しません。VSAN 間では、通信が行えません。各 VSAN 内で、すべてのメンバーが相互に対話できます。

図 15-1　論理 VSAN のセグメンテーション

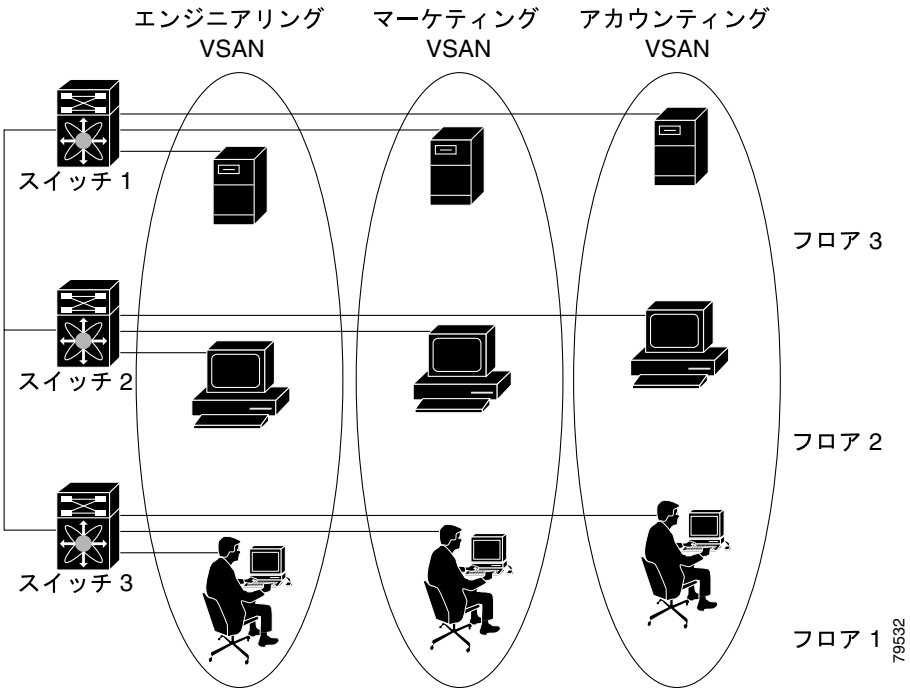
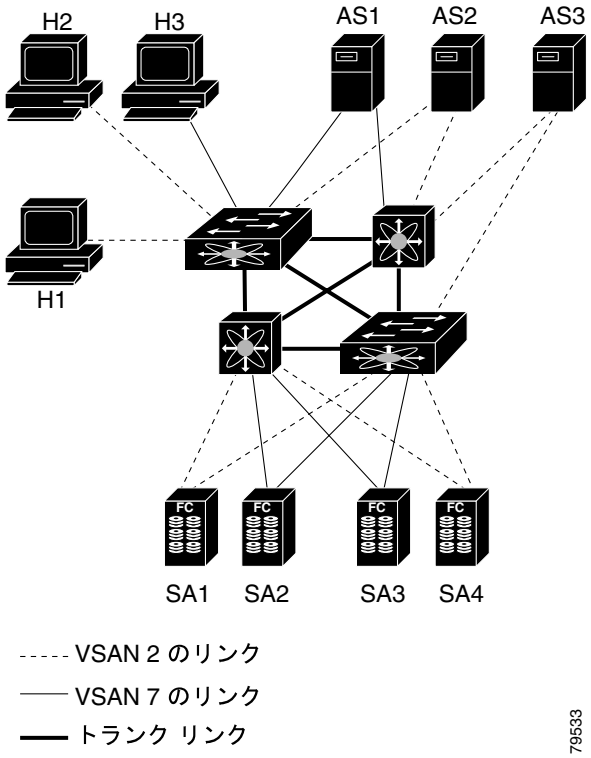


図 15-2 に、VSAN 2（点線）と VSAN 7（実線）の 2 つの定義された VSAN による物理ファイバ チャネル スイッチングのインフラストラクチャを示します。VSAN 2 には、ホスト H1 および H2、アプリケーション サーバ AS2 および AS3、およびストレージ アレイ SA1 および SA4 が含まれます。VSAN 7 は、H3、AS1、SA2、および SA3 と接続します。

アプリケーション サーバまたはストレージ アレイは、ファイバ チャネルまたは仮想ファイバ チャネル インターフェイスを使用するスイッチに接続できます。VSAN にはファイバ チャネルおよび仮想ファイバ チャネル インターフェイスを混在させることができます。

図 15-2　2 つの VSAN の例



このネットワーク内の 4 つのスイッチは、VSAN 2 と VSAN 7 の両方のトラフィックを伝送する VSAN トランク リンクによって相互接続されます。各 VSAN に異なるスイッチ間トポロジを設定できます。図 15-2 では、VSAN 2 および VSAN 7 のスイッチ間トポロジは同じです。

VSAN がなければ、ネットワーク管理者は、別個の SAN に対して別個のスイッチとリンクが必要になります。VSAN をイネーブルにすることによって、同一のスイッチとリンクが複数の VSAN で共有できます。VSAN では、スイッチ精度ではなく、ポート精度で SAN を作成できます。図 15-2 に、VSAN が物理 SAN で定義された仮想トポロジを使用して相互に通信を行うホストまたはストレージ デバイスのグループであることを示します。

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

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

VSAN の利点

VSAN には、次のような利点があります。

- トラフィックの分離 — 必要に応じて、トラフィックを VSAN 境界内に含み、1 つの VSAN 内だけにデバイスを常駐させることによって、ユーザ グループ間での絶対的な分離を確保します。
- スケーラビリティ — VSAN は、1 つの物理ファブリックの上でオーバーレイされます。複数の論理 VSAN 層を作成することによって、SAN のスケーラビリティが拡張します。
- VSAN 単位のファブリック サービス — VSAN 単位のファブリック 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。
- 冗長性 — 同一の物理 SAN で作成された複数の VSAN は、冗長性を保証します。1 つの VSAN に障害が発生した場合、ホストとデバイスの間にあるバックアップ パスによって（同一の物理 SAN の別の VSAN）に冗長保護が設定されます。
- 設定の容易さ — SAN の物理構造を変更することなく、VSAN 間でユーザを追加、移動、または変更できます。ある VSAN から別の VSAN へデバイスを移動する場合は、物理的な設定ではなく、ポート レベルの設定だけが必要となります。

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

VSAN とゾーン

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

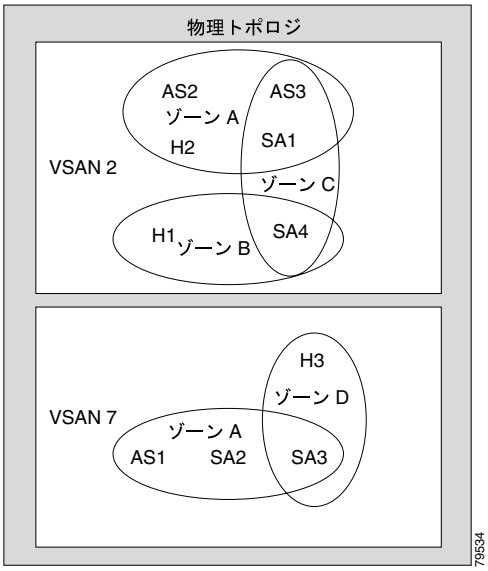
2 つの VSAN は未接続の 2 つの SAN に相当するので、VSAN 1 のゾーン A は、VSAN 2 のゾーン A とは異なり、別個のものです。表 15-1 に、VSAN とゾーンとの相違点を示します。

表 15-1　VSAN とゾーンの比較

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

図 15-3 に、VSAN とゾーンの可能な組み合わせを示します。VSAN 2 では、ゾーン A、ゾーン B、ゾーン C の 3 つのゾーンが定義されます。ゾーン C は、ファイバ チャネル標準に準拠してゾーン A とゾーン B にオーバーラップします。VSAN 7 では、ゾーン A とゾーン D の 2 つのゾーンが定義されます。VSAN 境界を越えるゾーンはありません。VSAN 2 に定義されたゾーン A は、VSAN 7 に定義されたゾーン A と異なり、別個のものです。

図 15-3　VSAN とゾーン分割



VSAN の設定

VSAN には次の属性があります。

- VSAN ID — VSAN ID は、デフォルト VSAN（VSAN 1）、ユーザ定義の VSAN（VSAN 2 ～ 4093）、および分離された VSAN（VSAN 4094）で VSAN を識別します。
- ステート — VSAN の管理ステートを active （デフォルト）または suspended ステートに設定できます。VSAN が作成されると、VSAN はさまざまな条件またはステートに置かれます。
  - VSAN の active ステートは、VSAN が設定され、イネーブルであることを示します。VSAN をイネーブルにすることによって、VSAN のサービスをアクティブにします。
  - VSAN の suspended ステートは、VSAN が設定されていて、イネーブルにされていないことを示します。この VSAN にポートが設定されている場合、ポートはディセーブルの状態です。このステートを使用して、VSAN の設定を失うことなく VSAN を非アクティブにします。suspended ステートの VSAN のすべてのポートは、ディセーブルの状態です。VSAN を suspended ステートにすることによって、ファブリック全体のすべての VSAN パラメータを事前設定し、VSAN をただちにアクティブにできます。
- VSAN 名 — このテキスト ストリングは、管理目的で VSAN を識別します。名前は、1 ～ 32 までの文字が可能で、すべての VSAN で一意である必要があります。デフォルトでは、VSAN 名は VSAN と 4 桁ストリングの連結で VSAN ID を表します。たとえば、VSAN 3 のデフォルト名は VSAN0003 です。

（注） VSAN 名は一意のものである必要があります。

- ロード バランシング属性 — これらの属性は、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 ID（OX ID）（デフォルトでは、src-dst-ox-id）の使用を示します。

ここでは、VSAN の作成および設定方法について、次の内容を説明します。

- VSAN 作成の概要（p.15-6）
- VSAN の静的な作成（p.15-7）
- ポート VSAN メンバシップの概要（p.15-8）
- スタティック ポート VSAN メンバシップの概要（p.15-8）
- デフォルト VSAN の概要（p.15-9）
- 分離された VSAN の概要（p.15-9）
- 分離された VSAN メンバシップの概要（p.15-9）
- VSAN の動作ステート（p.15-10）
- スタティック VSAN の削除の概要（p.15-10）
- スタティック VSAN の削除（p.15-11）
- ロード バランシングの概要（p.15-11）
- ロード バランシングの設定（p.15-12）
- Interop モードの概要（p.15-12）

VSAN 作成の概要

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

VSAN の静的な作成

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

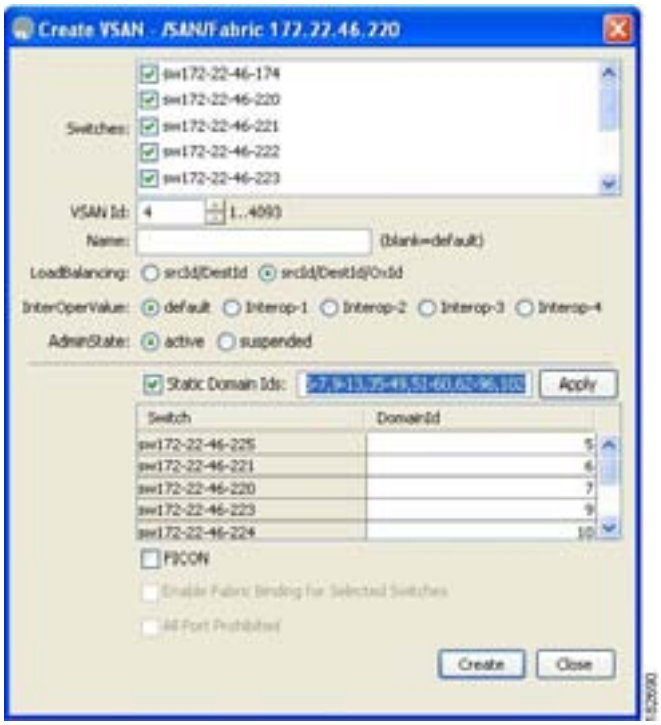
Fabric Manager を使用して VSAN を作成して設定する手順は、次のとおりです。

ステップ 1　**Create VSAN** アイコンをクリックします（図 15-4 を参照）。

図 15-4　Create VSAN アイコン

Create VSAN ダイアログボックスが表示されます（図 15-5 を参照）。

図 15-5　Create VSAN ダイアログボックス



（注）　Static Domain Ids チェックボックスをオンにすると Fabric Manager が中断モードの VSAN を作成し、自動的に VSAN をアクティブにします。

ステップ 2　この VSAN で必要なスイッチをオンにします。

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

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

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

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

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

詳細については第 25 章「ファブリック バインディングの設定」を参照してください。

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

ポート VSAN メンバシップの概要

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

- スタティック — ポートに VSAN を割り当てます。
  「スタティック ポート VSAN メンバシップの概要」（p.15-8）を参照してください。
- ダイナミック — デバイス WWN に基づいて VSAN を割り当てます。この方法は Dynamic Port VSAN Membership（DPVM）機能といいます。Nexus 5000 シリーズ スイッチは DPVM をサポートしていません。

VSAN トランキング ポートは、許可リストの一部である VSAN の対応リストを持ちます（第 13 章「VSAN トランキングの設定」を参照）。

スタティック ポート VSAN メンバシップの概要

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

ステップ 1　Physical Attributes ペインで、**Switches** > **Interfaces** を展開して、**FC Physical** を選択します。

Information ペインにインターフェイス設定が表示されます。

ステップ 2　**General** タブを選択します。

ファイバ チャネルの一般的物理情報が表示されます。PortVSAN フィールドに新しい VSAN を入力します。

ステップ 3　これらの変更を保存する場合は **Apply Changes** をクリックします。保存されていない変更を廃棄する場合は **Undo Changes** をクリックします。

デフォルト VSAN の概要

Nexus 5000 シリーズ スイッチの出荷時の設定値では、デフォルト VSAN 1 だけがイネーブルにされています。製造環境 VSAN として VSAN 1 を使用しないことを推奨します。VSAN が設定されていない場合、ファブリック内のすべてのデバイスはデフォルト VSAN に含まれているとみなされます。デフォルトでは、デフォルト VSAN にすべてのポートが割り当てられています。

（注） VSAN 1 は削除できませんが、中断できます。

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

分離された VSAN の概要

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

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

注意 分離された VSAN を使用してポートを設定しないでください。

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

分離された VSAN メンバシップの概要

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

ステップ 1　**Fabric*xx*** を展開し、Logical Domains ペインで **All VSANs** を選択します。

Information ペインに VSAN 設定が表示されます。

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

分離された VSAN のインターフェイスが表示されます。

VSAN の動作ステート

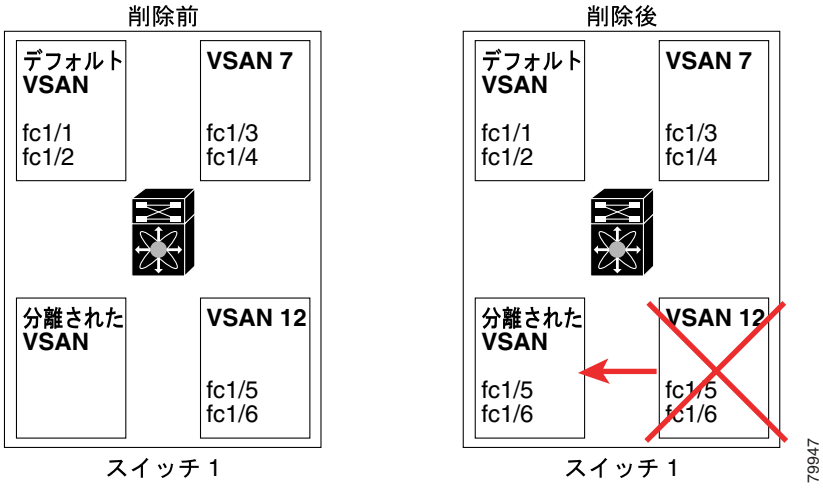
VSAN がアクティブで、最低 1 つのポートが起動していれば、VSAN は動作ステートにあります。このステートは、トラフィックがこの VSAN を通過できることを示します。このステートを設定することはできません。

スタティック VSAN の削除の概要

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

- VSAN 属性およびポート メンバシップの詳細は、VSAN マネージャによって保持されます。コンフィギュレーションから VSAN を削除すると、この機能が影響を受けます。VSAN が削除されると、VSAN 内のすべてのポートが非アクティブになり、ポートは分離された VSAN に移動されます。同一の VSAN が再作成されると、ポートはその VSAN に自動的に割り当てられません。明示的にポート VSAN メンバシップを再設定する必要があります（図 15-6 を参照）。

図 15-6　VSAN ポート メンバシップの詳細



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

（注） 許可 VSAN リストは、VSAN が削除されても影響を受けません（第 13 章「VSAN トランキングの設定」を参照）。

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

スタティック VSAN の削除

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

ステップ 1　Logical Domains ペインで **All VSANs** をクリックします。

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

ステップ 2　削除する VSAN を右クリックしてから、ドロップダウン メニューで **Delete Row** をクリックします（図 15-7 を参照）。

図 15-7　VSAN の削除

確認ダイアログボックスが表示されます。

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

ロード バランシングの概要

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

ロード バランシングの設定

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

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

Information ペインに VSAN 設定が表示されます（図 15-8 を参照）。

図 15-8　すべての VSAN の属性

ステップ 2　VSAN をクリックして、LoadBalancing フィールドに入力します。

ステップ 3　これらの変更を保存する場合は、**Apply Changes** をクリックします。保存されていない変更を廃棄する場合は、**Undo Changes** をクリックします。

Interop モードの概要

相互運用性を使用すると、複数ベンダーによる製品の間で相互に接続することができます。ファイバ チャネル標準規格では、ベンダーに対して共通の外部ファイバ チャネル インターフェイスを作成することを推奨しています。詳細については、「スイッチの相互運用性」（p.22-10）を参照してください。

デフォルト設定

表 15-2 に設定されたすべての VSAN のデフォルト設定値を示します。

表 15-2　デフォルトの VSAN パラメータ

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

CHAPTER 16

ゾーンの設定と管理

ゾーン分割は、ストレージ デバイスまたはユーザ グループ間のアクセス制御の設定を可能にします。ファブリックで管理者権限を持つユーザは、ゾーンを作成して、ネットワーク セキュリティを強化し、データ損失またはデータ破壊を防止することができます。ゾーン分割は、発信元 / 宛先 ID フィールドを検証することによって実行されます。

FC-GS-4 および FC-SW-3 標準で指定された高度なゾーン分割機能がサポートされています。既存の基本ゾーン分割機能を使用したり、高度な標準準拠のゾーン分割機能を使用できます。

この章の内容は、次のとおりです。

- ゾーン分割の概要（p.16-2）
- ゾーンの設定（p.16-7）
- ゾーン セット（p.16-13）
- ゾーン セット配信（p.16-24）
- ゾーン セット配信（p.16-28）
- ゾーン情報の確認（p.16-33）
- 拡張ゾーン分割（p.16-34）
- ゾーン データベースのコンパクト化（p.16-39）
- デフォルト設定（p.16-39）

（注） 表 15-1（p.15-4）に、ゾーンと VSAN の主な相違点を示します。

ゾーン分割の概要

ここでは、ゾーン分割について説明します。

- ゾーン分割機能（p.16-2）
- ゾーン分割の例（p.16-3）
- ゾーン実装（p.16-4）
- アクティブおよびフル ゾーン セット設定時の注意事項（p.16-5）

ゾーン分割機能

ゾーン分割には、次の機能があります。

- 1 つの ゾーン は複数のゾーン メンバーから構成されます。
  - ゾーンのメンバー同士はアクセスできますが、異なるゾーンのメンバー同士はアクセスできません。
  - ゾーン分割がアクティブでない場合、すべてのデバイスがデフォルト ゾーンのメンバーとなります。
  - ゾーン分割がアクティブの場合、アクティブ ゾーン（アクティブ ゾーン セットに含まれるゾーン）にないデバイスがデフォルト ゾーンのメンバーとなります。
  - ゾーンのサイズを変更できます。
  - 2 つ以上のゾーンにデバイスが所属することができます。
  - 物理ファブリックには、最大 16,000 の メンバー を設定できます。これには、ファブリック内のすべての VSAN が含まれます。
- ゾーン セットは、1 つまたは複数のゾーンで構成されます。
  - ゾーン セットは、単一エンティティとしてファブリックのすべてのスイッチでアクティブまたは非アクティブにできます。
  - アクティブにできるのは、常に 1 つのゾーン セットだけです。
  - ゾーンを 2 つ以上のゾーン セットのメンバーにすることができます。
  - ゾーン スイッチあたりの最大ゾーン セット数は 500 です。
- ゾーン分割は、ファブリックの任意のスイッチから管理できます。
  - 任意のスイッチからゾーンをアクティブにする場合、ファブリックのすべてのスイッチがアクティブ ゾーン セットを受信します。また、ファブリック内のすべてのスイッチにフル ゾーン セットが配信されます（この機能が発信元スイッチでイネーブルである場合）。
  - 既存のファブリックに新しいスイッチが追加されると、新しいスイッチによってゾーン セットが取得されます。
- ゾーンの変更を中断せずに設定できます。
  - 影響を受けないポートまたはデバイスのトラフィックを中断させることなく、新しいゾーンおよびゾーン セットをアクティブにできます。
- ゾーン メンバシップは、次の ID を使用して指定できます。
  - Port World Wide Name（pWWN）— スイッチに接続された N ポートの pWWN をゾーンのメンバーとして指定します。
  - ファブリック pWWN — ファブリック ポート（スイッチ ポートの WWN）の WWN を指定します。このメンバシップは、ポートベース ゾーン分割ともいいます。
  - FC ID — スイッチに接続された N ポートの FC ID をゾーンのメンバーとして指定します。
  - インターフェイスおよび Switch WWN（sWWN）— sWWN によって識別されたスイッチのインターフェイスを指定します。このメンバシップは、インターフェイスベース ゾーン分割ともいいます。

— インターフェイスおよびドメイン ID — ドメイン ID によって識別されたスイッチのインターフェイスを指定します。

— ドメイン ID およびポート番号 — シスコ スイッチのドメイン ID を指定し、さらに他社製スイッチに所属するポートを指定します。

（注） 仮想ファイバ チャネル インターフェイスを介してスイッチに接続される N ポートの場合、N ポートの pWWN、N ポートの FC ID、または 仮想ファイバ チャネル インターフェイスのファブリック pWWN を使用してゾーン メンバシップを指定できます。

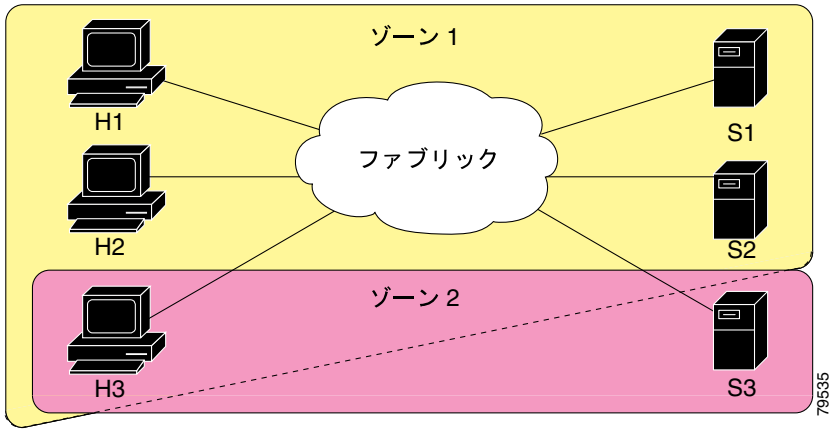
- デフォルト ゾーン メンバシップには、特定のメンバシップとの関係を持たないすべてのポートまたは WWN が含まれます。デフォルト ゾーン メンバー間のアクセスは、デフォルト ゾーン ポリシーによって制御されます。
- VSAN あたり最大 8000 ゾーン、さらにスイッチ上のすべての VSAN 合計で最大 8000 までのゾーンを設定できます。

（注） インターフェイスベース ゾーン分割は、Cisco SAN スイッチでのみ機能します。インターフェイスベース ゾーン分割は、interop モードに設定された VSAN でのみ機能します。

ゾーン分割の例

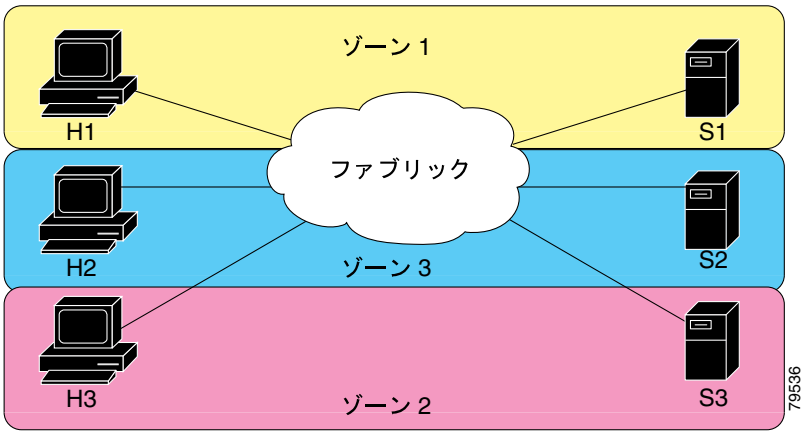
図 16-1 に、ファブリックの 2 つのゾーン（ゾーン 1 およびゾーン 2）で構成されるゾーン セットを示します。ゾーン 1 は、3 つすべてのホスト（H1、H2、H3）からストレージ システム S1 と S2 に常駐するデータへのアクセスを提供します。ゾーン 2 は、S3 のデータを H3 からのアクセスだけに限定します。H3 は、両方のゾーンに存在します。

図 16-1　2 つのゾーンを持つファブリック



他の方法を使用して、このファブリックをゾーンに分割できます。図 16-2 に、別の可能性を示します。新しいソフトウェアをテストする目的で、ストレージ システム S2 を分離する必要があると想定します。これを実行するために、ホスト H2 とストレージ S2 だけを含むゾーン 3 が設定されます。ゾーン 3 ではアクセスを H2 と S2 だけに限定し、ゾーン 1 ではアクセスを H1 と S1 だけに限定できます。

図 16-2　3 つのゾーンを持つファブリック



ゾーン実装

Nexus 5000 シリーズ スイッチは、自動的に次の基本的なゾーン機能をサポートします（追加の設定を行う必要はありません）。

- ゾーンが VSAN（仮想 SAN）に含まれます。
- ハード ゾーン分割をディセーブルにすることはできません。
- ネーム サーバ クエリがソフト ゾーン分割されます。
- アクティブ ゾーン セットだけが配信されます。
- ゾーンが分割できないデバイスは、相互にアクセスできません。
- 各 VSAN に同一名のゾーンまたはゾーン セットを含めることができます。
- 各 VSAN は、フル データベースとアクティブ データベースを持ちます。
- アクティブ ゾーン セットを変更するには、フル ゾーン データベースをアクティブ化する必要があります。
- アクティブ ゾーン セットは、スイッチを再起動しても維持されます。
- フル データベースへの変更は、明示的に保存する必要があります。
- ゾーンの再アクティブ化（ゾーン セットがアクティブの状態で、別のゾーン セットをアクティブ化する場合）は、既存のトラフィックに干渉しません。

必要に応じて、さらに次のゾーン機能を設定できます。

- VSAN 単位ですべてのスイッチにフル ゾーン セットを伝播します。
- ゾーンに属さないメンバーのデフォルト ポリシーを変更します。
- VSAN を interop モードに設定して、他のベンダーと相互運用します。相互に干渉することなく、同じスイッチ内の 1 つの VSAN を interop モードに、別の VSAN を基本モードに設定することもできます。
- E ポートの分離を解除します。

アクティブおよびフル ゾーン セット設定時の注意事項

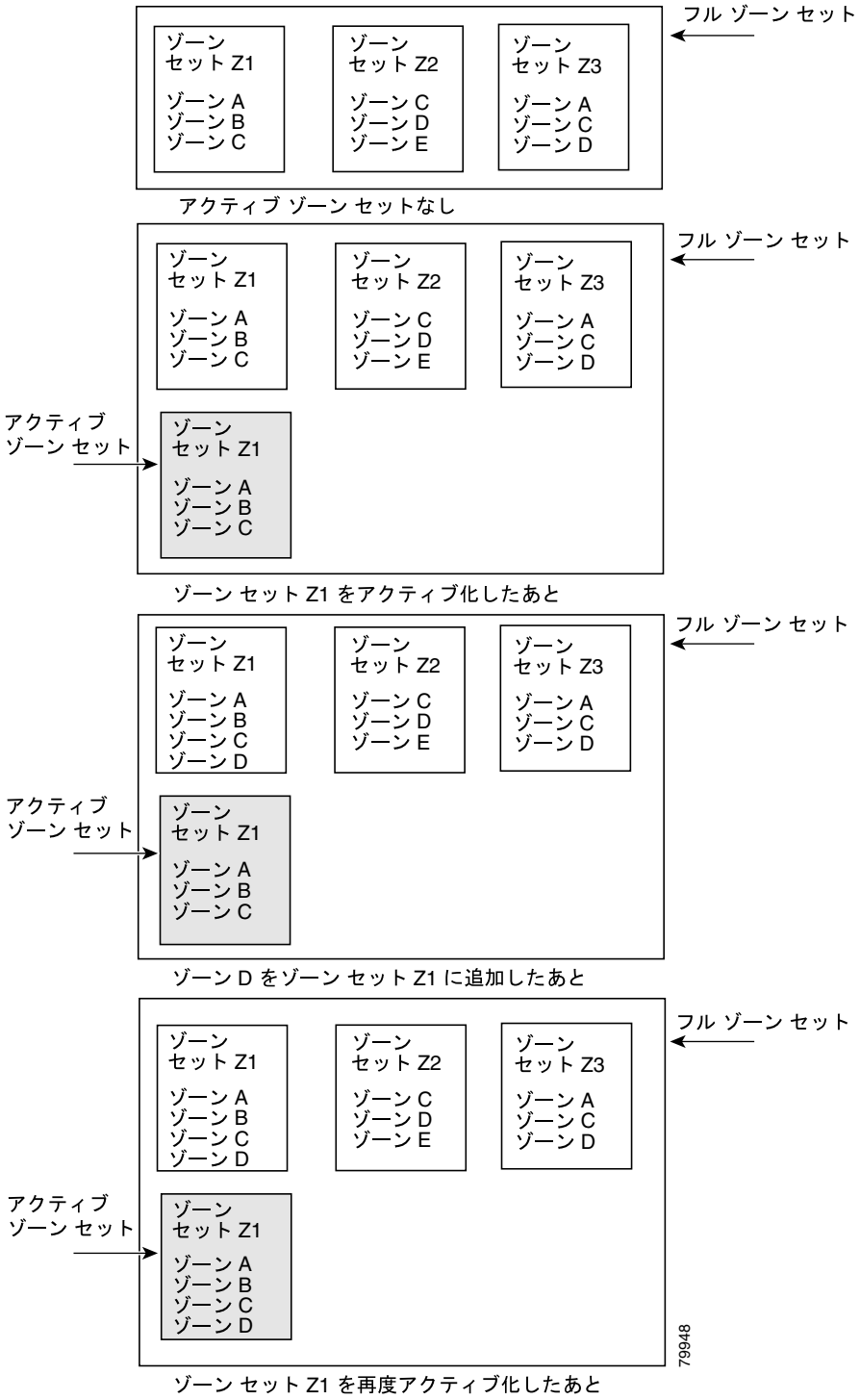
ゾーン セットを設定する前に、次の注意事項について検討してください。

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

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

図 16-3 に、アクティブ化されたゾーン セットに追加されるゾーンを示します。

図 16-3　アクティブおよびフル ゾーン セット



ゾーンの設定

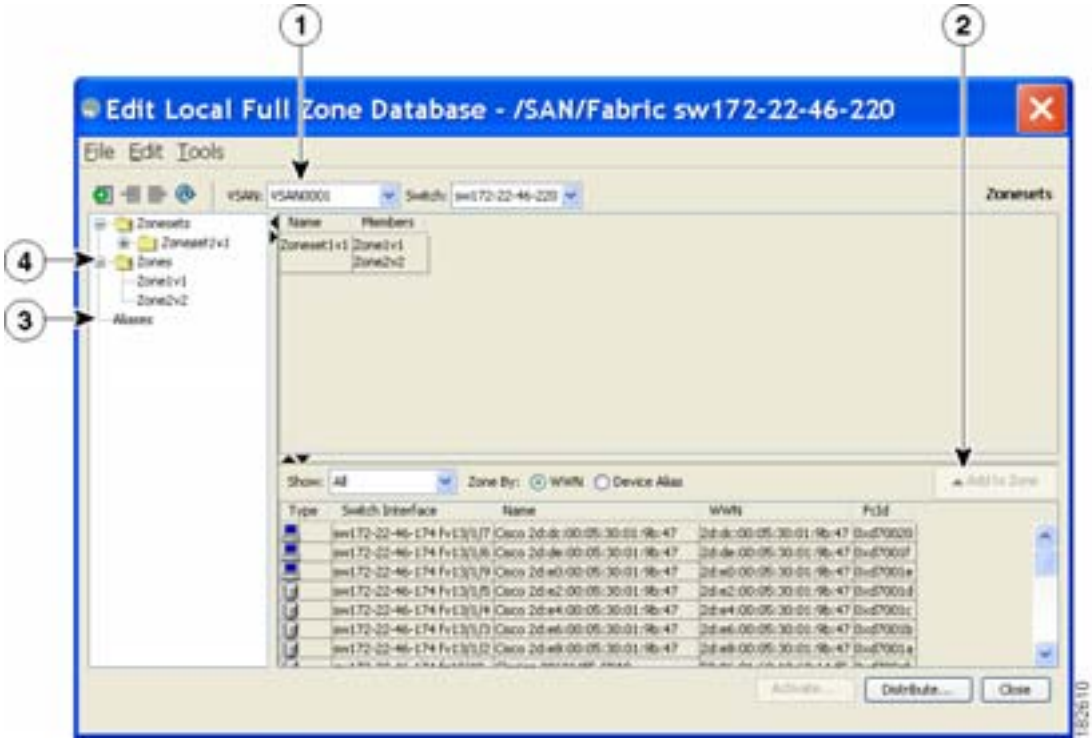
ここではゾーンの設定方法について、次の内容を説明します。

- ゾーン設定ツールの概要（p.16-7）
- ゾーン設定ツールを使用したゾーンの設定（p.16-8）
- ゾーン メンバーの追加（p.16-10）
- デフォルト ゾーン ポリシーの設定（p.16-12）

ゾーン設定ツールの概要

ゾーン設定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 16-4 を参照）。

図 16-4　Edit Local Full Zone Database ダイアログボックス



1	ドロップダウン メニューの VSAN を選択してから、**Enter** キーを押すと 、特定の VSAN 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 モードの設定」（p.17-5）を参照してください。

ヒント　Physical Attributes ペインから **Switches** を展開して、sWWN を取得します。sWWN を指定しない場合は、自動的にローカル sWWN が使用されます。

ゾーン設定ツール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 16-5 を参照）。

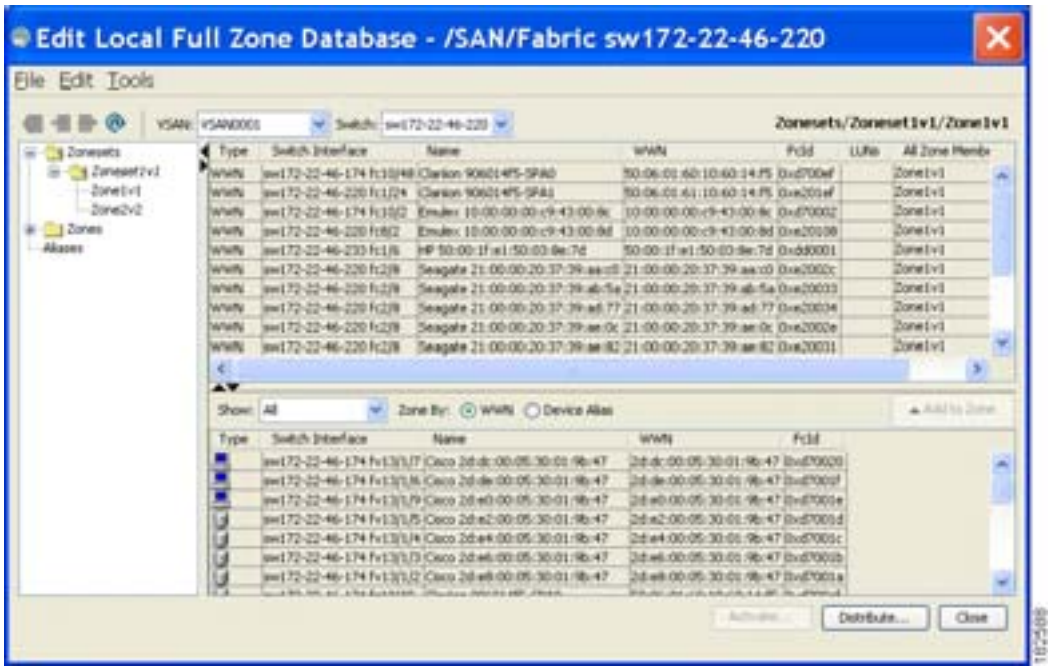
図 16-5　Zone アイコン

Select VSAN ダイアログボックスが表示されます。

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

図 16-6 に示す Edit Local Full Zone Database ダイアログボックスが表示されます。

図 16-6　Edit Local Full Zone Database ダイアログボックス

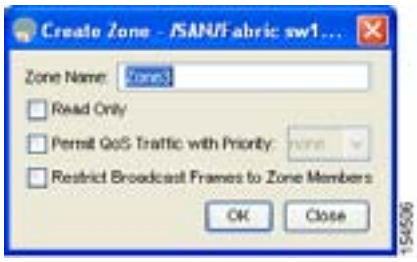


ゾーン メンバシップ情報を表示する場合は、**All Zone Membership(s)** カラムを右クリックして、ポップアップ メニューで現在の行またはすべての行の **Show Details** を選択します。

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

Create Zone ダイアログボックスが表示されます（図 16-7 を参照）。

図 16-7　Create Zone ダイアログボックス



ステップ 4　ゾーン名を入力します。

ステップ 5　次のチェックボックスのうち 1 つをオンにします。

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

b. **Permit QoS traffic with Priority（プライオリティで QoS トラフィックを許可）**— ドロップダウン リストでプライオリティを設定します。

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

ステップ 6　**OK** をクリックしてゾーンを作成します。

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

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

Zoneset Name ダイアログボックスが表示されます（図 16-8 を参照）。

図 16-8　Zoneset Name ダイアログボックス

ステップ 8　ゾーン セット名を入力し、**OK** をクリックします。

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

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

Select Zone ダイアログボックスが表示されます（図 16-9 を参照）。

図 16-9　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。

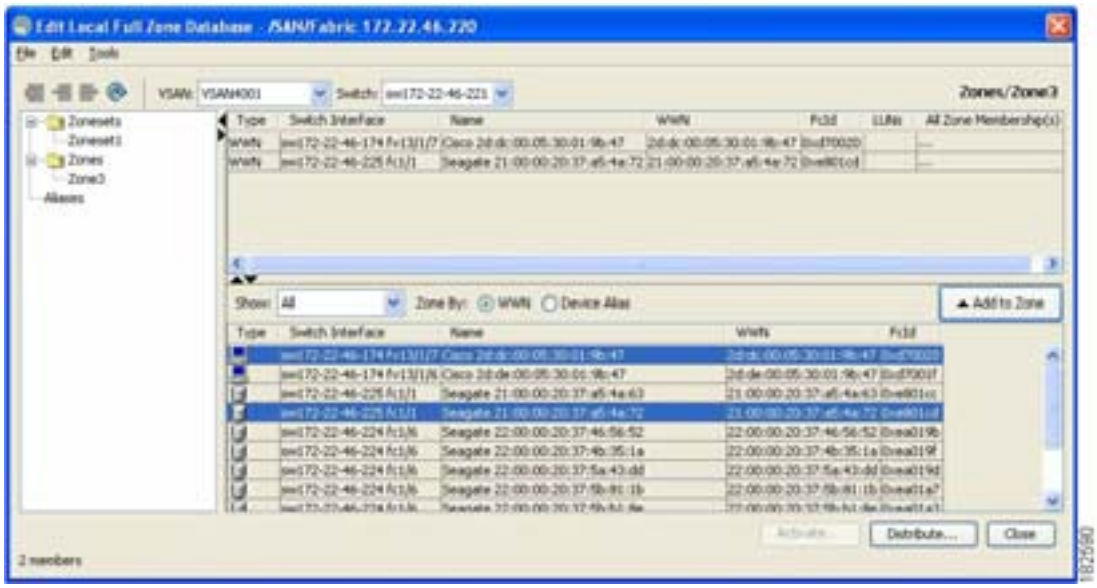
ステップ 1　**Zone** > **Edit Local Full Zone Database** を選択します。

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（図 16-10 を参照）が表示されます。

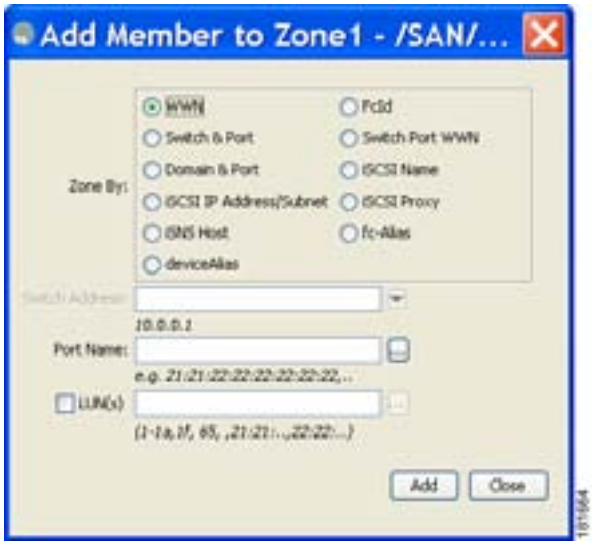
図 16-10　Edit Local Full Zone Database ダイアログボックス



ステップ 3　Fabric ペインから追加するメンバーを選択し、**Add to Zone** をクリックするか、メンバーを追加するゾーンをクリックし、**Insert** アイコンをクリックします。

図 16-11 に示す Add Member to Zone ダイアログボックスが表示されます。

図 16-11　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 モードの設定」（p.17-5）を参照してください。

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

ステップ 5　**Add** をクリックして、ゾーンにメンバーを追加します。

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

デフォルト ゾーン ポリシーの設定

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

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

Select VSAN ダイアログボックスが表示されます。

ステップ 2　VSAN を選択して、**OK** をクリックします。

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

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

図 16-12 に示す Modify Default Zone Properties ダイアログボックスが表示されます。

図 16-12　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 リストを **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。

ゾーン セット

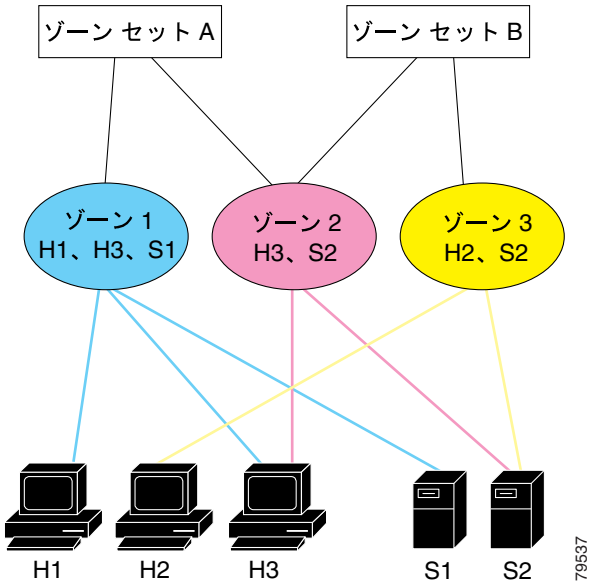
ここではゾーン セットについて、次の内容を説明します。

- ゾーン セットの作成の概要（p.16-13）
- ゾーン セットのアクティブ化（p.16-14）
- ゾーン メンバシップ情報の表示（p.16-16）
- デフォルト ゾーンの概要（p.16-16）
- デフォルト ゾーンの設定（p.16-17）
- FC エイリアスの作成の概要（p.16-18）
- FC エイリアスの作成（p.16-18）
- エイリアスへのメンバーの追加（p.16-20）
- ゾーンメンバーの pWWN ベースメンバーへの変換（p.16-22）
- ゾーンの実行（p.16-23）

ゾーン セットの作成の概要

図 16-13 では、それぞれ独自のメンバシップ階層とゾーン メンバーを持つ別個の 2 つのセットが作成されています。

図 16-13　ゾーン セット、ゾーン、ゾーン メンバーの階層



ゾーンは、アクセス制御を指定するための方法を提供し、ゾーン セットは、ファブリックでアクセス制御を実行するためにゾーンをグループ化します。ゾーン セット A またはゾーン セット B のいずれか（両方でなく）をアクティブにすることができます。

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

ゾーン セットのアクティブ化

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

Fabric Manager を使用して既存のゾーン セット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。

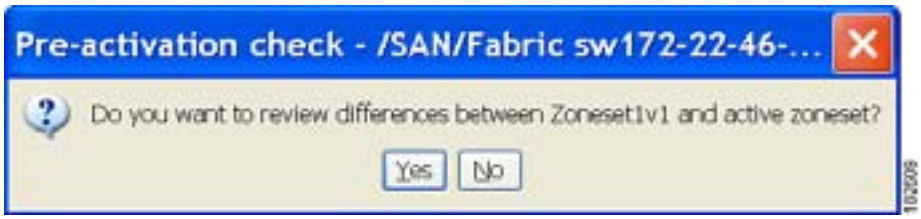
ステップ 2　VSAN を選択して、**OK** をクリックします。

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 16-14 を参照）。

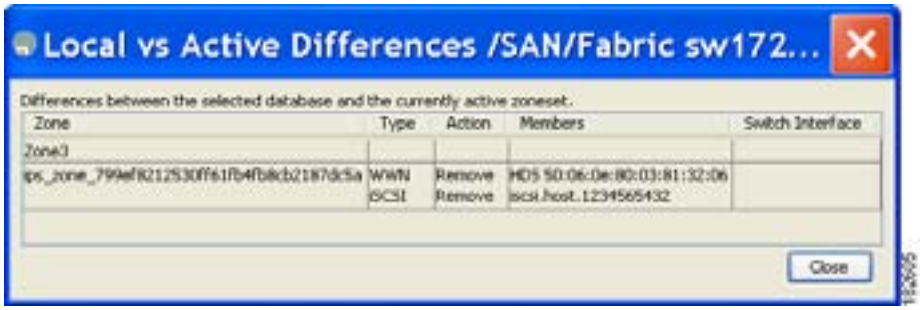
図 16-14　Pre-Activation Check ダイアログボックス



ステップ 4　**Yes** をクリックして、相違を確認します。

図 16-15 に示す Local vs. Active Differences ダイアログボックスが表示されます。

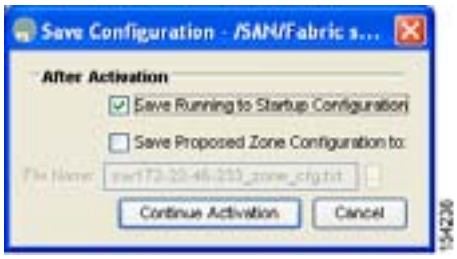
図 16-15　Local vs. Active Differences ダイアログボックス



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 16-16 を参照）。

図 16-16　Save Configuration ダイアログボックス

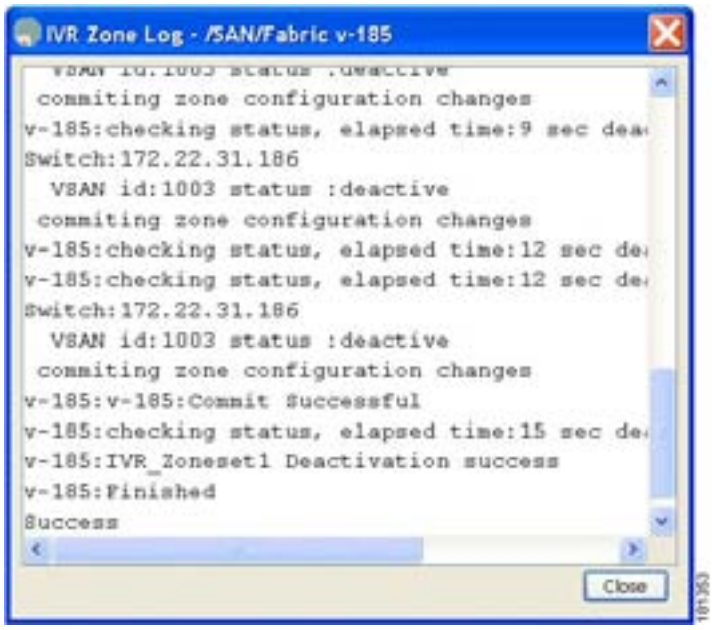


ステップ 6　すべての変更をスタートアップ コンフィギュレーションに保存するには、**Save Running to Startup Configuration** チェックボックスをオンにします。

ステップ 7　ゾーン セットをアクティブにするには **Continue Activation** をクリックします。ダイアログボックスを閉じて、保存されていない変更を廃棄するには、**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 16-17 を参照）。

図 16-17　Zone Log ダイアログボックス



既存のゾーン セット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。

ステップ 2　確認ダイアログボックスで **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。

ゾーン メンバシップ情報の表示

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

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

Select VSAN ダイアログボックスが表示されます。

ステップ 2　VSAN を選択して、**OK** をクリックします。

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

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

（注）　デフォルト ゾーン メンバーが明示的に表示されるのは、デフォルト ゾーン ポリシーが **permit** に設定されている場合のみです。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。「ゾーン情報の確認」（p.16-33）を参照してください。

デフォルト ゾーンの概要

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

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

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

（注）スイッチが初めて初期化される場合、ゾーンは設定されておらず、すべてのメンバーがデフォルト ゾーンに所属するものとみなされます。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を変更できます。

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

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

デフォルト ゾーンの設定

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

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

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

Information ペインにゾーン ポリシー情報が表示されます（図 16-18 を参照）。

図 16-18　デフォルト ゾーン ポリシー

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

ステップ 3　Default Zone Behavior フィールドで、ドロップダウン リストから **permit** または **deny** を選択します。

FC エイリアスの作成の概要

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

- pWWN ― N ポートの WWN は、16 進形式です（10:00:00:23:45:67:89:ab など）。
- fWWN ― ファブリック ポート名の WWN は 16 進形式です（10:00:00:23:45:67:89:ab など）。
- FC ID ― N ポート ID は、0xhhhhhh 形式です（0xce00d1 など）。
- ドメイン ID ― ドメイン ID は 1 ～ 239 の整数です。このメンバシップ設定を完了するには、他社製スイッチの必須ポート番号が必要です。
- インターフェイス ― インターフェイスベース ゾーン分割はポートベース ゾーン分割と同様に、ゾーン設定にスイッチ インターフェイスが使用されます。ローカルおよびリモート スイッチの両方で、スイッチ インターフェイスをゾーン メンバーとして指定できます。リモート スイッチを指定するには、特定の VSAN 内のリモート sWWN またはドメイン ID を入力します。

ヒント　スイッチは、VSAN ごとに最大 2048 個のエイリアスをサポートします。

FC エイリアスの作成

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

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

Select VSAN ダイアログボックスが表示されます。

ステップ 2　VSAN を選択して、**OK** をクリックします。

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

ステップ 3　左下のペインで、**Aliases** をクリックします（図 16-19 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 16-19　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 16-20 を参照）。

図 16-20　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。

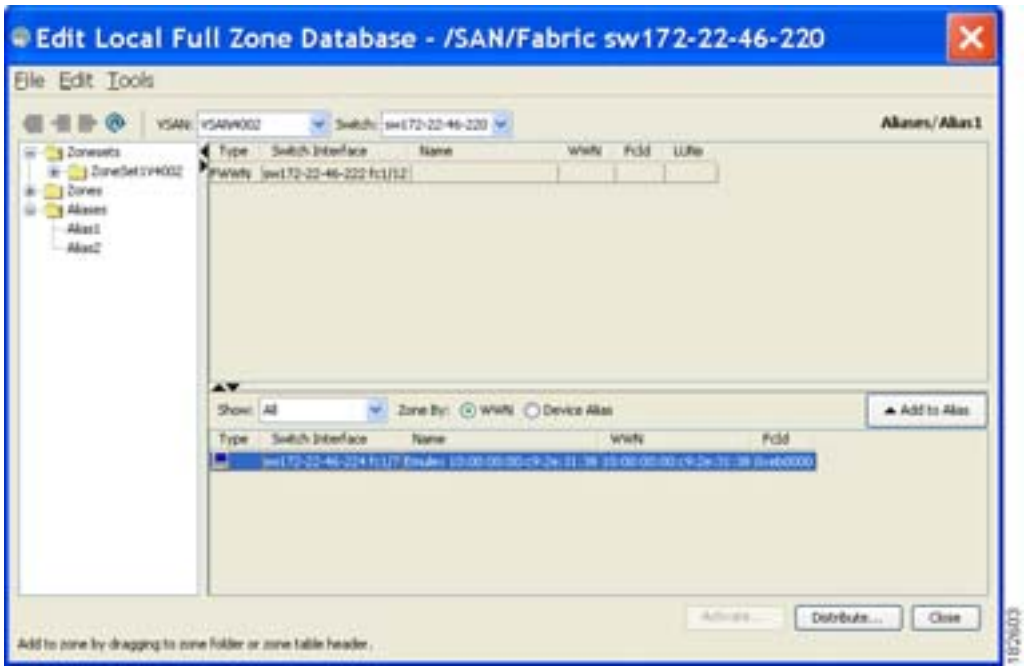
ステップ 1　**Zone** > **Edit Local Full Zone Database** を選択します。

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 16-21 を参照）。

図 16-21　Edit Local Full Zone Database ダイアログボックス



ステップ 3　メンバーを追加するエイリアス（FC-Aliases フォルダ内）をクリックします。

ステップ 4　Fabric ペインから追加するメンバーを選択し（図 16-21 を参照）、**Add to Alias** をクリックします。

Fabric Manager を使用して、エイリアスにメンバーを追加する別の方法もあります。ステップ 4 の代わりに、ステップ 5 ～ 7 を実行します。

ステップ 5　メンバーを追加するエイリアスをクリックし、**Insert** アイコンをクリックします。

図 16-22 に示す Add Member to Alias ダイアログボックスが表示されます。

図 16-22　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 モードの設定」（p.17-5）を参照してください。

ステップ 6　Browse ボタンをクリックしてポート名を選択するか、**LUN** チェックボックスをクリックしてから Browse ボタンをクリックして LUN を設定します。

ステップ 7　**Add** をクリックして、エイリアスにメンバーを追加します。

ゾーンメンバーの pWWN ベースメンバーへの変換

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

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

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

Select VSAN ダイアログボックスが表示されます。

ステップ 2　VSAN を選択して、**OK** をクリックします。

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

ステップ 3　変換するゾーンをクリックします。

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

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

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

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

ヒント　実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーしてアクティブ ゾーン セットを保存する必要はありません。ただし、明示的にフル ゾーン セットを保存するには、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーする必要があります。

（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 enhanced モードの場合、仮想デバイス名は Fabric Manager の Zoning ウィンドウの Device Alias Database に表示されます。この場合、デバイス エイリアス名を選択するか、Add Member to Zone ダイアログボックスで pWWN を入力することができます。詳細については、「ゾーン メンバーの追加」（p.16-10）を参照してください。

（注）　デバイス エイリアス モードをイネーブルにする前に、デバイス エイリアス モードがどのように動作するのかを確認してください。デバイス エイリアス モードの詳細と要件については、第 17 章「Distributing Device Alias Service」を参照してください。

ゾーンの実行

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

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

ハード ゾーン分割は、N ポートから送信される各フレームでハードウェアによって実行されます。スイッチにフレームが着信した時点で、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。

Nexus 5000 シリーズ スイッチは、ハードおよびソフトの両方のゾーン分割をサポートしています。

ゾーン セット配信

フル ゾーン セットを配信するには、ワンタイム配信またはフル ゾーン セット配信のいずれかの方法を使用します。表 16-1 に相違を示します。

表 16-1　ゾーン セット配信の相違

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

ここではゾーン セット配信について、次の内容を説明します。

- フル ゾーン セット配信のイネーブル化（p.16-24）
- ワンタイム配信のイネーブル化（p.16-25）
- リンクの分離からの回復の概要（p.16-26）
- ゾーン セットのインポートおよびエクスポート（p.16-27）

フル ゾーン セット配信のイネーブル化

Nexus 5000 シリーズのすべてのスイッチは、新しい E ポート リンクが立ち上がったとき、または新しいゾーン セットが VSAN でアクティブ化されたときに、アクティブ ゾーン セットを配信します。ゾーン セットの配信は、隣接スイッチへのマージ要求の送信時、またはゾーン セットのアクティブ化の際に行われます。

Fabric Manager を使用して VSAN ベースですべてのスイッチへのフル ゾーン セットおよびアクティブ ゾーン セットの配信をイネーブルにする手順は、次のとおりです。

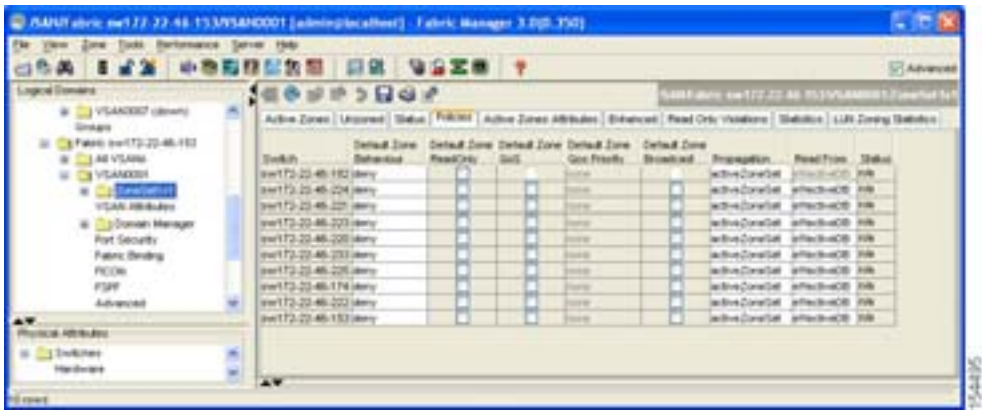
ステップ 1　**VSAN** を開き、Logical Domains ペインで、ゾーン セットを選択します。

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

ステップ 2　**Policies** タブをクリックします。

ゾーンの設定されたポリシーが表示されます（図 16-23 を参照）。

図 16-23　ゾーンに設定されたポリシー



ステップ 3　Propagation カラムで、ドロップダウン リストから **Full Zoneset** を選択します。

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

ワンタイム配信のイネーブル化

ファブリック全体で、非アクティブ、非変更のゾーン セットのワンタイム配信が行えます。

Fabric Manager からフル ゾーン セットのワンタイム配信を伝播する手順は、次のとおりです。

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

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

ステップ 2　左側のペインでリストから適切なゾーンをクリックします。

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

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

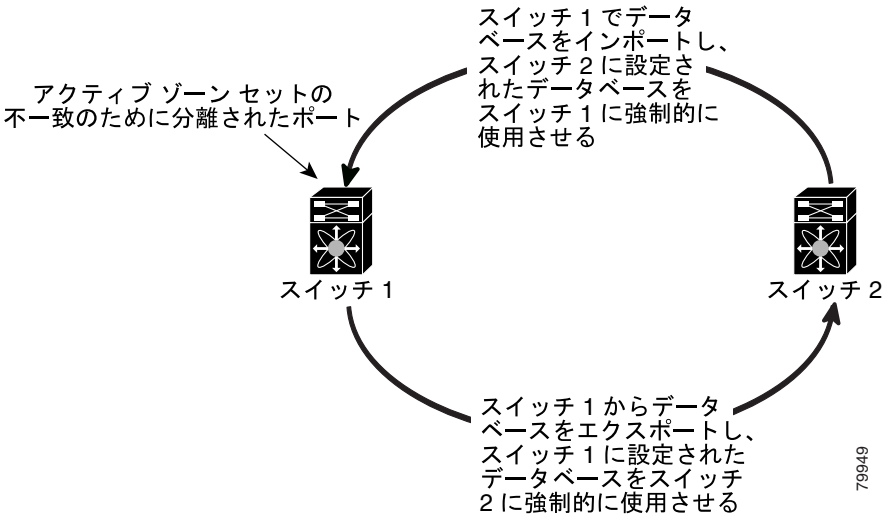
（注）　フル ゾーン セットのワンタイム配信は、interop 2 および interop 3 モードでサポートされていますが、interop 1 モードではサポートされていません。

リンクの分離からの回復の概要

ファブリックの 2 つのスイッチが TE ポートまたは E ポートを使用して結合される場合、アクティブ ゾーン セットのデータベースが 2 つのスイッチまたはファブリック間で異なると、この TE ポートおよび E ポートが分離する可能性があります。TE ポートまたは E ポートが分離した場合、次の 3 つのオプションのいずれかを使用して分離状態からポートを回復できます。

- 近接スイッチのアクティブ ゾーン セットのデータベースをインポートし、現在のアクティブ ゾーン セットと交換します（図 16-24 を参照）。
- 現在のデータベースを近接スイッチにエクスポートします。
- フル ゾーン セットを編集し、修正されたゾーン セットをアクティブにしてから、リンクを立ち上げることにより手動で矛盾を解決します。

図 16-24　データベースのインポートとエクスポート



ゾーン セットのインポートおよびエクスポート

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

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

図 16-25 に示す Zone Merge Failure Recovery ダイアログボックスが表示されます。

図 16-25　Zone Merge Failure Recovery ダイアログボックス

ステップ 3　**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 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スイッチを選択します。

ステップ 5　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 6　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 7　**OK** をクリックして、アクティブ ゾーン セットをインポートまたはエクスポートします。

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

ゾーン セット配信

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

- フル ゾーン セット
- リモート ロケーション（FTP［ファイル転送プロトコル］、SCP、SFTP、または Trivial File Transfer Protocol［TFTP; 簡易ファイル転送プロトコル］を使用）

アクティブ ゾーン セットは、フル ゾーン セットに含まれません。フル ゾーン セットが失われた場合、または伝送されなかった場合に、既存のゾーン セットに変更を加え、アクティブにすることはできません。

注意　アクティブ ゾーン セットをフル ゾーン セットにコピーする際に、同一名のゾーンがフル ゾーン セット データベースにすでに存在する場合は、上書きされる可能性があります。

ここで説明する内容は、次のとおりです。

- ゾーン セットのコピー（p.16-29）
- ゾーンのバックアップおよび復元の概要（p.16-29）
- ゾーンのバックアップおよび復元（p.16-30）
- ゾーン、ゾーン セット、およびエイリアスの名前の変更（p.16-31）
- 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（p.16-32）
- MDS 以外のデータベースの移行（p.16-32）
- ゾーン サーバ データベースの削除（p.16-33）

ゾーン セットのコピー

Nexus 5000 シリーズ スイッチでは、アクティブなゾーン セットを編集できません。ただし、アクティブ ゾーン セットをコピーして新しいゾーン セットを作成し、これを編集することはできます。

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

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

図 16-26 に示す Copy Full Zone Database ダイアログボックスが表示されます。

図 16-26　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。

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および復元

Fabric Manager を使用してフル ゾーン設定をバックアップまたは復元する手順は、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。

ステップ 3　**File** > **Backup** を選択して、TFTP 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。または、**File** > **Restore** を選択して保存されたゾーン設定を復元します。

図 16-27 に示す Restore Zone Configuration ダイアログボックスが表示されます。

図 16-27　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　**Continue Restore** をクリックします。復元しないでダイアログボックスを閉じるには **Close** をクリックします。

ゾーン、ゾーン セット、およびエイリアスの名前の変更

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。

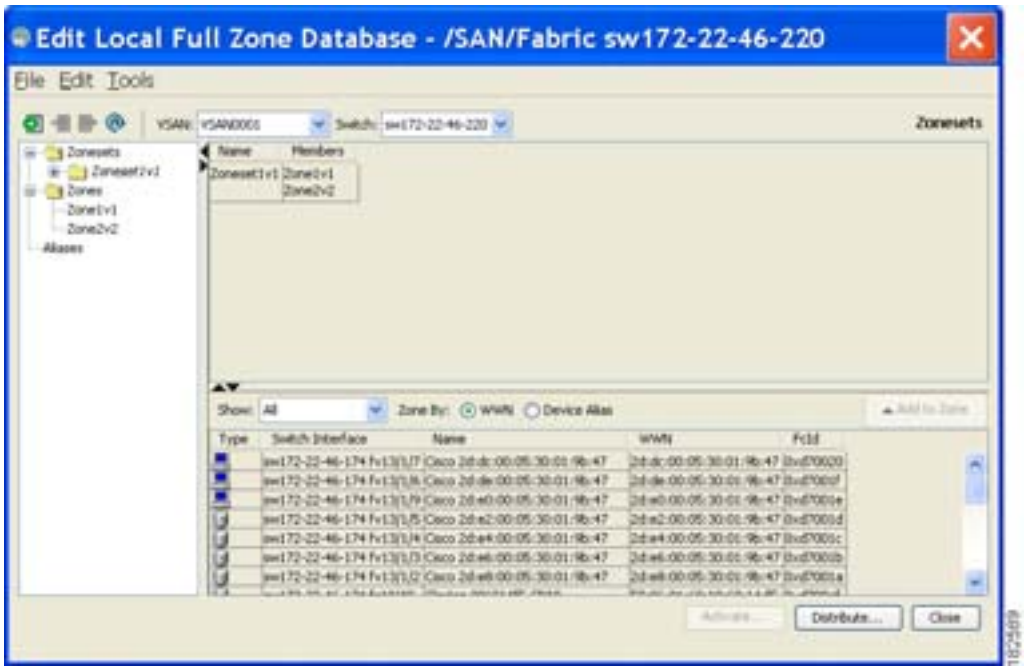
ステップ 1　**Zone** > **Edit Local Full Zone Database** を選択します。

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 16-28 を参照）。

図 16-28　Edit IVR Local Full Zone Database ダイアログボックス



ステップ 3　左側のペインでゾーンまたはゾーン セットをクリックします。

ステップ 4　**Edit** > **Rename** を選択します。

ゾーンまたはゾーン セット名の周囲にエディット ボックスが表示されます。

ステップ 5　新しい名前を入力します。

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

ゾーン、ゾーン セット、FC エイリアス、およびゾーン属性グループのコピー

ゾーン、ゾーン セット、FC エイリアス、またはゾーン属性グループをコピーする手順は、次のとおりです。

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

Select VSAN ダイアログボックスが表示されます。

ステップ 2　VSAN を選択して、**OK** をクリックします。

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

ステップ 3　**Edit** > **Clone** を選択します。

Clone Zoneset ダイアログボックスが表示されます（図 16-29 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 16-29　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、もと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 Wizard 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 Wizard 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 データベースの削除

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削除できます。

ゾーン サーバ データベースを削除するには、『*Cisco Nexus 5000 Series CLI Configuration Guide*』を参照してください。

（注） ゾーン セットを削除するとフル 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 データベースを削除したあとに、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、実行コンフィギュレーションを保存する必要があります。

ゾーン情報の確認

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 セットをクリックします。

Information ペインにゾーンの設定が表示されます。

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

拡張ゾーン分割

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

ここで説明する内容は、次のとおりです。

- 拡張ゾーン分割の概要（p.16-34）
- 基本ゾーン分割から拡張ゾーン分割への変更（p.16-35）
- 拡張ゾーン分割から基本ゾーン分割への変更（p.16-36）
- 拡張ゾーン分割のイネーブル化（p.16-36）
- データベースのマージ（p.16-37）
- ゾーン マージの分析（p.16-38）
- ゾーン マージ制御ポリシーの設定（p.16-38）

拡張ゾーン分割の概要

表 16-2 に、Nexus 5000 シリーズ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 16-2　拡張ゾーン分割の利点

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

表 16-2　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
シスコ固有のゾーン メンバー タイプ（シンボリック ノード名およびその他のタイプ）は他社製スイッチによって使用される場合があります。マージ時に、シスコ固有のタイプは他社製スイッチによって誤って解釈される可能性があります。	メンバー タイプを一意に識別するために、ベンダー固有のタイプ値とベンダー ID が提供されます。	ベンダー タイプが一意です。
fWWN ベースのゾーン メンバシップは、シスコの interop モードでのみサポートされます。	標準 interop モード（interop モード 1）で fWWN ベースのメンバシップをサポートします。	fWWN ベースのメンバー タイプは標準化されています。

基本ゾーン分割から拡張ゾーン分割への変更

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

ステップ 1　ファブリック内のすべてのスイッチが拡張モードで動作できることを確認します。

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

ステップ 2　動作モードを拡張ゾーン分割モードに設定します。

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

Cisco SAN スイッチでは、他の Cisco NX-OS リリースへのダウングレードおよびアップグレードを可能にするために、拡張ゾーン分割から基本ゾーン分割への変更が可能です。

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

ステップ 1　アクティブおよびフル ゾーン セットに拡張ゾーン分割モード固有の設定が含まれていないことを確認します。

このような設定が存在する場合は、この手順を進める前にこれらの設定を削除します。既存の設定を削除しないと、スイッチ ソフトウェアは自動的にこれらの設定を削除します。

ステップ 2　動作モードを基本ゾーン分割モードに設定します。

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。

拡張ゾーン分割のイネーブル化

デフォルトでは、拡張ゾーン分割機能は Nexus 5000 シリーズのすべてのスイッチでディセーブルです。

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

ステップ 1　Logical Domains ペインでは、VSAN を展開して、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 リストで、**enhanced** を選択して、この VSAN で拡張ゾーン分割をイネーブルにします。

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

データベースのマージ

マージの方法は、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 16-3 で指定されたマージ規則を使用してマージされます。

表 16-3　データベースのゾーン マージ ステータス

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

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

マージ プロセスは次のように動作します。

1. ソフトウェアがプロトコル　バージョンを比較します。プロトコル　バージョンが異なる場合、ISL は分離されます。
2. プロトコル バージョンが同じ場合、ゾーン ポリシーが比較されます。ゾーン ポリシーが異なる場合、ISL は分離されます。
3. ゾーン マージ オプションが同じである場合、マージ制御設定に基づいて比較が行われます。
   a. 設定が「制限」の場合、アクティブ ゾーン セットとフル ゾーン セットが同じになる必要があります。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、マージ規則を使用してマージが行われます。

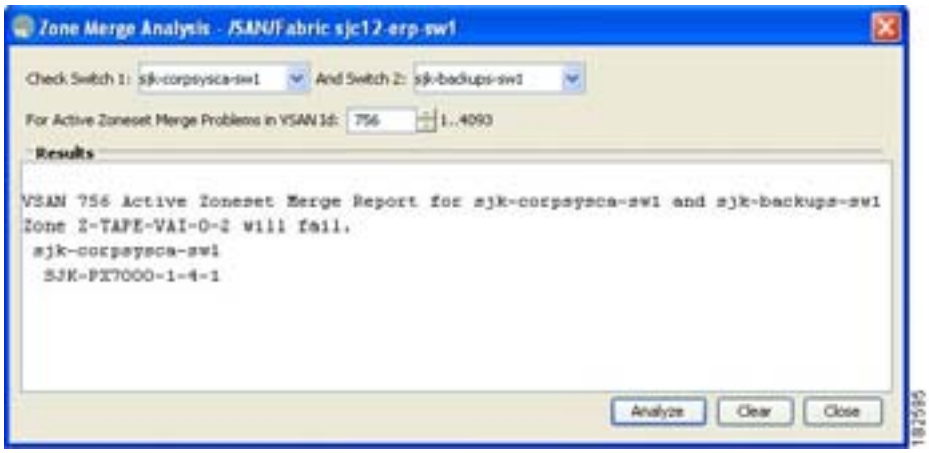
ゾーン マージの分析

Fabric Manager を使用してゾーン マージの分析を行う手順は、次のとおりです。

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

図 16-30 に示す Zone Merge Analysis ダイアログボックスが表示されます。

図 16-30　Zone Merge Analysis ダイアログボックス



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

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

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

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

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

ゾーン マージ制御ポリシーの設定

マージ制御ポリシーを設定するには、『*Cisco Nexus 5000 Series CLI Configuration Guide*』を参照してください。

ゾーン データベースのコンパクト化

過剰なゾーンを削除して、VSAN のゾーン データベースをコンパクトにできます。

（注） スイッチが VSAN あたり 2000 を超えるゾーンをサポートしていても、その隣接スイッチがサポートしていない場合、マージは失敗します。また、スイッチが VSAN あたり 2000 を超えるゾーンをサポートしていても、ファブリック内のすべてのスイッチが VSAN あたり 2000 を超えるゾーンをサポートしていない場合には、ゾーン セットのアクティブ化に失敗することがあります。

ダウングレードのためのゾーン データベースをコンパクト化するには、『*Cisco Nexus 5000 Series CLI Configuration Guide*』を参照してください。

デフォルト設定

表 16-4 に基本ゾーン パラメータのデフォルト設定を示します。

表 16-4　デフォルトの基本ゾーンパラメータ

パラメータ	デフォルト
デフォルト ゾーン ポリシー	すべてのメンバーで拒否
フル ゾーン セット配信	フル ゾーン セットは配信されません。
拡張ゾーン分割	ディセーブル

CHAPTER 17

Distributing Device Alias Service

Nexus 5000 シリーズ スイッチは、ファブリック全体で Distributed Device Alias Service（デバイス エイリアス）をサポートしています。

この章の内容は、次のとおりです。

- デバイス エイリアスの概要（p.17-2）
- デバイス エイリアス データベース（p.17-4）
- レガシー ゾーン エイリアスの変換（p.17-9）
- データベース マージの注意事項（p.17-10）
- デフォルト設定（p.17-10）

デバイス エイリアスの概要

Nexus 5000 シリーズ スイッチで機能（ゾーニング、DPVM、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、予期せぬ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設定コマンドで使用します。この章では、これらのわかりやすい名前を *デバイス エイリアス*と表します。

ここで説明する内容は、次のとおりです。

- デバイス エイリアスの機能（p.17-2）
- デバイス エイリアスの前提条件（p.17-2）
- ゾーン エイリアスとデバイス エイリアスの比較（p.17-3）

デバイス エイリアスの機能

デバイス エイリアスには次の機能があります。

- デバイス エイリアスの情報は、VSAN 構成に依存しません。
- デバイス エイリアスの設定および配信は、ゾーン サーバおよびゾーン サーバ データベースに依存しません。
- データを失うことなく、レガシー ゾーン エイリアス設定をインポートできます。
- デバイス エイリアス アプリケーションでは、Cisco Fabric Services（CFS）インフラストラクチャを使用して、データベースを効率的に管理および配信することができます。デバイス エイリアスでは調整済み配信モードが使用され、配信範囲はファブリック全体に及びます（第 7 章「CFS の使用」を参照）。
- 基本モードおよび拡張モード。「デバイス エイリアス モード」（p.17-4）を参照してください。
- ゾーン、IVR ゾーン、またはポート セキュリティ機能を設定するために使用されるデバイス エイリアスと、対応する pWWN は、**show** コマンド出力に自動的に表示されます。

デバイス エイリアスの前提条件

デバイス エイリアスには次の前提条件があります。

- デバイス エイリアスを割り当てることができるのは、pWWN のみです。
- pWWN と対応するデバイス エイリアスには、1 対 1 の関係がなければなりません。
- デバイス エイリアス名は、次の文字を含む、64 文字の英数字に制限されています。
  - a ～ z および A ～ Z
  - デバイス エイリアス名の先頭は、英数字（a ～ z または A ～ Z）でなければなりません。
  - 1 ～ 9
  - -（ハイフン）および _（下線）
  - $（ドル記号）および ^（キャレット）

ゾーン エイリアスとデバイス エイリアスの比較

表 17-1 に、ゾーンベース エイリアスとデバイス エイリアスの設定の違いを示します。

表 17-1　ゾーン エイリアスとデバイス エイリアスの比較

ゾーンベース エイリアス	デバイス エイリアス
エイリアスは指定された VSAN に限定されます。	VSAN 番号を指定しなくても、デバイス エイリアスを定義できます。また、制限なしに、1 つ以上の VSAN 内で同じ定義を使用することもできます。
ゾーン エイリアスはゾーニング設定の一部です。エイリアス マッピングを使用して、その他の機能を設定することはできません。	デバイス エイリアスは、pWWN を使用する任意の機能と併用できます。
任意のゾーン メンバー タイプを使用して、エンド デバイスを指定できます。	サポートされるのは、pWWN のみです。
設定はゾーン サーバ データベースに格納され、その他の機能に使用することはできません。	デバイス エイリアスはゾーニングに限定されません。デバイス エイリアスの設定は、FCNS、ゾーン、fcping、および traceroute アプリケーションに使用できます。

デバイス エイリアス データベース

デバイス エイリアス機能は 2 つのデータベースを使用して、デバイス エイリアス設定の許可および実装を行います。

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

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

ここで説明する内容は、次のとおりです。

- デバイス エイリアス モード（p.17-4）
- デバイス エイリアス モードの変更に関する注意事項（p.17-5）
- デバイス エイリアス モードの設定（p.17-5）
- デバイス エイリアス配信の概要（p.17-6）
- デバイス エイリアス データベースの配信（p.17-6）
- デバイス エイリアスの作成の概要（p.17-7）
- デバイス エイリアスの作成（p.17-7）
- 変更のコミット（p.17-8）
- 変更の廃棄（p.17-8）

デバイス エイリアス モード

エイリアスが、基本モードおよび拡張モードで動作するように指定できます。

デフォルトの基本モードで動作している場合、デバイス エイリアスは pWWN に即座に拡張されます。たとえば、基本モードの場合に、新しい HBA を示すようにデバイス エイリアスを変更しても、変更内容はゾーン サーバに反映されません。ユーザは以前の HBA の pWWN を削除し、新しい HBA の pWWN を追加してから、ゾーンセットを再びアクティブにする必要があります。

拡張モードで動作しているアプリケーションは、デバイス エイリアス名を「ネイティブ」フォーマットで受け入れます。デバイス エイリアスが pWWN に拡張されることはありません。デバイス エイリアス名は設定に格納され、ネイティブのデバイス エイリアス フォーマットで配信されます。したがって、ゾーン サーバ、PSM、または DPVM などのアプリケーションは、デバイス エイリアス メンバシップの変更を自動的に追跡し、適切に適用することができます。拡張モードで動作させることの主な利点は、変更が 1 回で済むことです。

デバイス エイリアス モードを変更すると、デバイス エイリアス配信がイネーブルな場合に、変更はネットワーク内の別のスイッチに再配信されます。デバイス エイリアス配信がイネーブルでない場合は、ローカル スイッチのモードのみが変更されます。

（注） interop モードの VSAN では、拡張モード、つまりネイティブのデバイス エイリアスベース設定は使用できません。対応するゾーンにネイティブのデバイス エイリアスベース メンバーが存在する場合は、interop モードの VSAN で IVR ゾーンセットをアクティブにすることができません。

デバイス エイリアス モードの変更に関する注意事項

デバイス エイリアス モードを変更する場合、次の点に注意してください。

- 異なるデバイス エイリアス モードで稼働している 2 つのファブリックを連結しても、デバイス エイリアスはマージされません。マージ プロセス中に、モードの自動変換は発生しません。この場合は、一方のモードを選択する必要があります。
- 拡張モードを基本モードに変更する場合は、最初にローカル スイッチおよびリモート スイッチ内のすべてのネイティブ デバイス エイリアスベース設定を明示的に削除するか、すべてのデバイス エイリアスベース設定メンバーを対応する pWWN で置き換える必要があります。
- デバイス エイリアス データベースからデバイス エイリアスを削除すると、すべてのアプリケーションは対応するデバイス エイリアスの適用を自動的に停止します。対応するデバイス エイリアスがアクティブなゾーンセットに含まれる場合は、該当する pWWN に対するすべてのトラフィックが中断されます。
- デバイス エイリアスの名前を変更すると、デバイス エイリアス データベース内のデバイス エイリアス名が変更されるだけでなく、すべてのアプリケーション内の対応するデバイス エイリアス設定も置き換えられます。
- デバイス エイリアス データベースに新しいデバイス エイリアスを追加した場合、アプリケーション設定がこのデバイス エイリアス上にあれば、この設定が自動的に有効になります。たとえば、対応するデバイス エイリアスがアクティブなゾーンセットに含まれていて、デバイスがオンライン状態の場合、ゾーニングは自動的に適用されます。ゾーンセットを再びアクティブにする必要はありません。
- デバイス エイリアス名を新しい HBA の pWWN にマッピングすると、それに応じてアプリケーションの適用方法が変更されます。この場合、ゾーン サーバは新しい HBA の pWWN に基づいて自動的にゾーニングを適用します。

デバイス エイリアス モードの設定

Fabric Manager を使用して拡張モードで動作するようにデバイス エイリアスを設定する手順は、次のとおりです。

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

Information ペインにデバイス エイリアス設定が表示されます（図 17-1 を参照）。

ステップ 2　**Mode** タブをクリックします。

ステップ 3　ConfigMode ドロップダウン リストで **enhanced** を選択します。

図 17-1　モードの設定

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

デバイス エイリアス配信の概要

デフォルトでは、デバイス エイリアス配信がイネーブルです。デバイス エイリアス機能は CFS を使用して、変更内容をファブリック内のすべてのスイッチに配信します。

デバイス エイリアス配信がディセーブルの場合、データベースの変更内容はファブリック内のスイッチに配信されません。デバイス エイリアス データベースを最新状態に維持するには、ファブリック内のすべてのスイッチで同じ変更を手動で実行する必要があります。データベースの変更は即座に有効になるため、保留データベースの処理や、コミットまたは中断処理は発生しません。変更をコミットせずに配信をディセーブルにすると、コミット タスクは失敗します。

次の例に、障害が発生したデバイス エイリアスのステータスを示します。

デバイス エイリアス データベースの配信

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

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

Information ペインにデバイス エイリアス設定が表示されます（図 17-2 を参照）。

図 17-2　Fabric Manager 内のデバイス エイリアス

ステップ 2　**CFS** タブをクリックします。

ステップ 3　Feature Admin カラムから **enable** を選択して、スイッチ エイリアスをイネーブルにします。

ステップ 4　新しくイネーブルにしたスイッチについて、Config Action カラムから **commitChanges** を選択します。

ステップ 5　これらの変更をコミットして配信する場合は **Apply Changes** を、保存されていない変更を廃棄する場合は **Undo Changes** をクリックします。

デバイス エイリアスの作成の概要

任意のデバイス エイリアス設定タスクを実行すると、デバイス エイリアス タスクに関係なく、デバイス エイリアス機能に対してファブリックが自動的にロックされます。ファブリックがロックされると、次のような状況になります。

- 他のユーザは、この機能の設定を変更できなくなります。
- 有効データベースのコピーが取得され、保留データベースとして使用されます。この時点以降の変更は、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、または廃棄（**abort**）するまでは、保留データベースが使用されます。

デバイス エイリアスの作成

Fabric Manager でファブリックをロックする手順は、次のとおりです。

（注） 保留データベース内に、ロックされたファブリックのデバイス エイリアスを作成します。

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

Information ペインにデバイス エイリアスの設定が表示されます。

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

Create Device Alias ダイアログボックスが表示されます（図 17-3 を参照）。

図 17-3　Create Device Alias ダイアログボックス

ステップ 3　Alias および pWWN フィールドに入力します。

ステップ 4　**Create** をクリックして、このエイリアスを作成します。

変更のコミット

保留データベースに対する変更をコミットすると、次のイベントが発生します。

1. 有効データベースの内容が、保留データベースの内容で上書きされます。
2. 保留データベースがファブリック内の各スイッチに配信され、これらのスイッチの有効データベースが新しい変更内容で上書きされます。
3. 保留データベースの内容が空になります。
4. この機能に対するファブリック ロックが解放されます。

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

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

Information ペインにデバイス エイリアスの設定が表示されます。

ステップ 2　**CFS** タブをクリックします。

ステップ 3　Feature Admin カラムから **enable** を選択して、スイッチ エイリアスをイネーブルにします。

ステップ 4　新しくイネーブルにしたスイッチについて、Config Action カラムから **commitChanges** を選択します。

ステップ 5　これらの変更をコミットして配信する場合は **Apply Changes** を、保存されていない変更を廃棄する場合は **Undo Changes** をクリックします。

変更の廃棄

保留データベースに対する変更を廃棄すると、次のイベントが発生します。

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

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

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

Information ペインにデバイス エイリアスの設定が表示されます。

ステップ 2　**CFS** タブをクリックします。

ステップ 3　新しくイネーブルにしたスイッチについて、Config Action カラムから **abort** を選択します。

ステップ 4　**Apply Changes** をクリックして、変更を廃棄します。

レガシー ゾーン エイリアスの変換

レガシー ゾーン エイリアス設定が次の制限事項を満たす場合は、設定をインポートしてこの機能を使用しても、データが失われることはありません。

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

名前または定義に矛盾がある場合、ゾーン エイリアスはインポートされません。

ヒント　ご使用の設定の要件に応じて、必要なゾーン エイリアスをデバイス エイリアス データベースにコピーしてください。

インポート処理が完了したあとに、**commit** 処理を実行すると、変更されたエイリアス データベースが物理ファブリック内のその他のすべてのスイッチに配信されます。ファブリック内のそ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、マージ変更を完全に廃棄することができます。

デバイス エイリアスまたは FC エイリアスの使用法

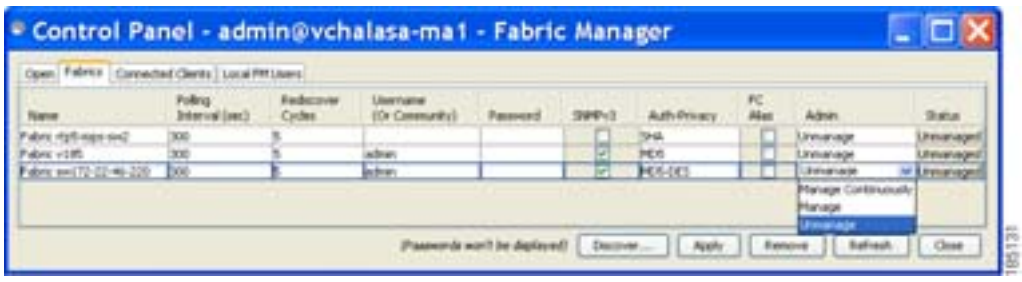
Fabric Manager が FC エイリアスを使用するかグローバル デバイス エイリアスを使用するかは、Fabric Manager Server を再起動せずに、Fabric Manager Client から設定を変更できます。

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

ステップ 1　**Server** > **Admin** をクリックします。

Control Panel ダイアログボックスが表示され、Fabrics タブが開きます（図 17-4 を参照）。

図 17-4　Control Panel ダイアログボックス



ステップ 2　FC エイリアスを使用する場合は、**FC Alias** チェックボックスをオンにします。Fabric Manager Server で管理しているファブリックごとにグローバル デバイス エイリアスを使用する場合は、このチェックボックスをオフにします。

ステップ 3　**Apply** をクリックして、変更を保存します。

データベース マージの注意事項

2 つのデバイス エイリアス データベースをマージする場合は、以下の注意事項に従ってください。

- 名前が異なる 2 つのデバイス エイリアスが同じ pWWN にマッピングされていないことを確認します。
- 同じ 2 つの pWWN が 2 つの異なるデバイス エイリアスにマッピングされていないことを確認します。
- 両方のデータベース内のデバイス エイリアスの総数が、Cisco MDS SAN-OS Release 3.0 (x) 以前が稼働しているファブリックの場合は 8 K（8191 個）、Cisco MDS SAN-OS Release 3.1(x) 以上が稼働しているファブリックの場合は 20 K を超えていないことを確認します。

  両方のデータベース内のデバイス エントリの総数がサポートされている設定上の上限を超えている場合は、マージできません。たとえば、データベース N に 6000 個、データベース M に 2192 個のデバイス エイリアスがあり、SAN-OS 3.0(x) 以前が稼働している場合は、このマージ処理に失敗します。デバイス エイリアス モードが一致していない場合も、マージ処理に失敗します。

詳細については、「CFS マージのサポート」（p.7-7）を参照してください。

デフォルト設定

表 17-2 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 17-2　デバイス エイリアスのデフォルト パラメータ

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

CHAPTER 18

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 Nexus 5000 シリーズ スイッチの E モードおよび TE モードのファイバ チャネル インターフェイスで、デフォルトでイネーブルです。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。FSPF は次の機能を提供します。

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

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

- FSPF の概要（p.18-2）
- FSPF のグローバル設定（p.18-4）
- FSPF インターフェイスの設定（p.18-7）
- FSPF ルート（p.18-13）
- 順序どおりの配信（p.18-15）
- デフォルト設定（p.18-19）

FSPF の概要

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

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

FSPF の例

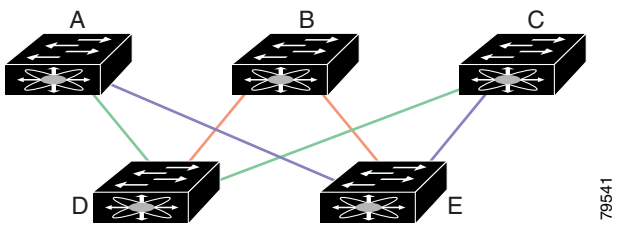
ここではトポロジおよびアプリケーションの例を使用して、FSPF の利点を示します。

（注） FSPF 機能は任意のトポロジで使用できます。

フォールトトレラント ファブリックの例

図 18-1 に、部分メッシュ トポロジを使用するフォールトトレラント ファブリックを示します。ファブリック内のどの場所でリンクが切断されても、各スイッチはファブリック内のその他のすべてのスイッチと通信することができます。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 18-1　フォールトトレラント ファブリック



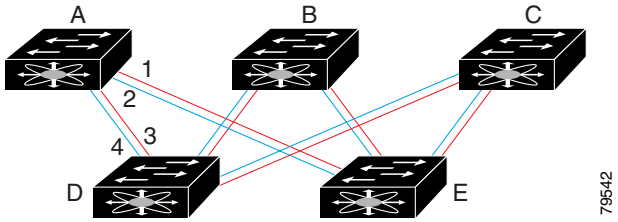
たとえば、すべてのリンクの速度が同じ場合、FSPF は A から C への 2 つの同等パス（A-D-C［グリーン］と A-E-C［ブルー］）を計算します。

冗長リンクの例

図 18-1 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 18-2 に、この配置を示します。Nexus 5000 シリーズ スイッチはポート チャネルをサポートしているため、FSPF プロトコルは物理リンクの各ペアを単一の論理リンクとして認識します。

物理リンク ペアをバンドルすると、データベース サイズの縮小とリンク アップデートの頻度の削減により、FSPF の効率が大幅に向上します。物理リンクを集約すると、障害は単一リンクでなく、SAN ポート チャネル全体に関係するようになります。このような設定は、ネットワークの復元力も向上します。SAN 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 18-2　冗長リンクを備えたフォールトトレラント ファブリック



たとえば、すべてのリンクの速度が同じで、SAN ポート チャネルが存在しない場合、FSPF は A から C への 4 つの同等パス（A1-E-C、A2-E-C、A3-D-C、および A4-D-C）を計算します。SAN ポート チャネルが存在する場合、計算されるパスは 2 つに削減されます。

FSPF のグローバル設定

Nexus 5000 シリーズ スイッチでは、FSPF はデフォルトでイネーブルです。

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

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

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

ここで説明する内容は、次のとおりです。

- SPF 計算ホールド タイムの概要（p.18-4）
- LSR の概要（p.18-4）
- VSAN での FSPF の設定（p.18-5）
- FSPF のデフォルト設定へのリセット（p.18-5）
- FSPF のイネーブル化またはディセーブル化（p.18-6）

SPF 計算ホールド タイムの概要

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

LSR の概要

新しいスイッチをファブリックに追加するたびに、Link State Record（LSR）が隣接スイッチに送信されて、ファブリック全体にフラッディングされます。

表 18-1 に、スイッチ応答に関するデフォルト設定を示します。

表 18-1　LSR のデフォルト設定

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

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

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

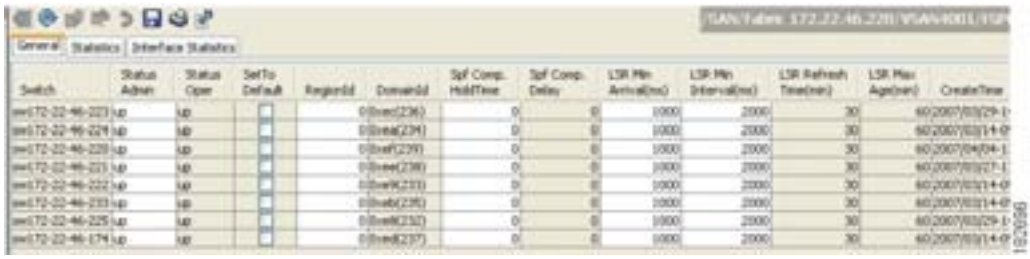
VSAN での FSPF の設定

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

ステップ 1　Fabric を展開し、VSAN を展開してから、FSPF を設定する VSAN に対して **FSPF** を選択します。

Information ペインに FSPF 設定が表示されます（図 18-3 を参照）。

図 18-3　FSPF の一般情報



RegionID、Spf Comp Holdtime、LSR Min Arrival、および LSR Min Interval に値を入力できます。これらの値は、VSAN 上のすべてのインターフェイスに適用されます。

ステップ 2　これらの変更を保存する場合は、**Apply Changes** をクリックします。保存されていない変更を廃棄する場合は、**Undo Changes** をクリックします。

FSPF のデフォルト設定へのリセット

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

ステップ 1　Fabric を展開し、VSAN を展開してから、FSPF を設定する VSAN に対して **FSPF** を選択します。

Information ペインに FSPF 設定が表示されます（図 18-3 を参照）。

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

ステップ 3　これらの変更を保存する場合は、**Apply Changes** をクリックします。保存されていない変更を廃棄する場合は、**Undo Changes** をクリックします。

FSPF のイネーブル化またはディセーブル化

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

ステップ 1　Fabric を展開し、VSAN を展開してから、FSPF を設定する VSAN に対して **FSPF** を選択します。

Information ペインに FSPF 設定が表示されます（図 18-3 を参照）。

ステップ 2　FSPF をイネーブルにする場合は、Status Admin ドロップダウン リストを **up** に設定します。FSPF をディセーブルにする場合は、**down** に設定します。

ステップ 3　これらの変更を保存する場合は、**Apply Changes** をクリックします。保存されていない変更を廃棄する場合は、**Undo Changes** をクリックします。

FSPF インターフェイスの設定

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

ここで説明する内容は、次のとおりです。

- FSPF リンク コストの概要（p.18-7）
- FSPF リンク コストの設定（p.18-7）
- ハロー タイム インターバルの概要（p.18-8）
- ハロー タイム インターバルの設定（p.18-8）
- デッド タイム インターバルの概要（p.18-9）
- デッド タイム インターバルの設定（p.18-9）
- 再送信インターバルの概要（p.18-9）
- 再送信インターバルの設定（p.18-9）
- 特定のインターフェイスに対する FSPF のディセーブル化の概要（p.18-10）
- 特定のインターフェイスに対する FSPF のディセーブル化（p.18-10）
- FSPF データベースの表示（p.18-10）
- FSPF 統計情報の表示（p.18-12）

FSPF リンク コストの概要

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

FSPF リンク コストの設定

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

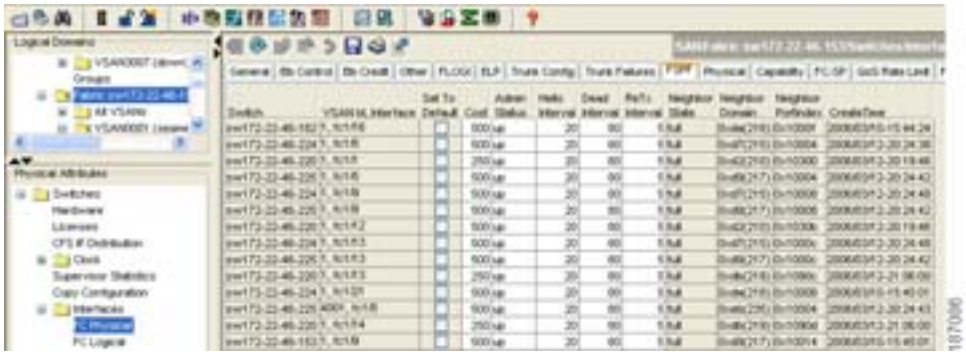
ステップ 1　Physical Attributes ペインで、**Switches** > **Interfaces** を展開して、**FC Physical** を選択します。

Information ペインにインターフェイス設定が表示されます。

ステップ 2　**FSPF** タブをクリックします。

Information ペインに FSPF インターフェイスの設定が表示されます（図 18-4 を参照）。

図 18-4　ファイバ チャネルの物理 FSPF インターフェイス



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

ステップ 4　これらの変更を保存する場合は、**Apply Changes** をクリックします。保存されていない変更を廃棄する場合は、**Undo Changes** をクリックします。

ハロー タイム インターバルの概要

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

（注）　この値は、ISL の両端のポートで同じ値にする必要があります。

ハロー タイム インターバルの設定

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

ステップ 1　Physical Attributes ペインで、**Switches** > **Interfaces** を展開して、**FC Physical** を選択します。

Information ペインにインターフェイス設定が表示されます。

ステップ 2　**FSPF** タブをクリックします。

Information ペインに FSPF インターフェイスの設定が表示されます（図 18-4 を参照）。

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

ステップ 4　これらの変更を保存する場合は、**Apply Changes** をクリックします。保存されていない変更を廃棄する場合は、**Undo Changes** をクリックします。

デッド タイム インターバルの概要

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

（注） この値は、ISL の両端のポートで同じ値にする必要があります。

デッド タイム インターバルの設定

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

ステップ 1　Physical Attributes ペインで、**Switches** > **Interfaces** を展開して、**FC Physical** を選択します。

Information ペインにインターフェイス設定が表示されます。

ステップ 2　**FSPF** タブをクリックします。

Information ペインに FSPF インターフェイスの設定が表示されます（図 18-4 を参照）。

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

ステップ 4　これらの変更を保存する場合は、**Apply Changes** をクリックします。保存されていない変更を廃棄する場合は、**Undo Changes** をクリックします。

再送信インターバルの概要

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

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

再送信インターバルの設定

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

ステップ 1　Physical Attributes ペインで、**Switches** > **Interfaces** を展開して、**FC Physical** を選択します。

Information ペインにインターフェイス設定が表示されます。

ステップ 2　**FSPF** タブをクリックします。

Information ペインに FSPF インターフェイスの設定が表示されます（図 18-4 を参照）。

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

ステップ 4　これらの変更を保存する場合は、**Apply Changes** をクリックします。保存されていない変更を廃棄する場合は、**Undo Changes** をクリックします。

特定のインターフェイスに対する FSPF のディセーブル化の概要

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

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

特定のインターフェイスに対する FSPF のディセーブル化

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

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

ステップ 1　Physical Attributes ペインで、**Switches** > **Interfaces** を展開して、**FC Physical** を選択します。

Information ペインにインターフェイス設定が表示されます。

ステップ 2　**FSPF** タブをクリックします。

Information ペインに FSPF インターフェイスの設定が表示されます（図 18-4 を参照）。

ステップ 3　Admin Status ドロップダウン リストで、**down** を選択します。

ステップ 4　これらの変更を保存する場合は、**Apply Changes** をクリックします。保存されていない変更を廃棄する場合は、**Undo Changes** をクリックします。

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

FSPF データベースの表示

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

- LSR タイプ
- LSR 所有者のドメイン ID
- アドバタイジング ルータのドメイン ID

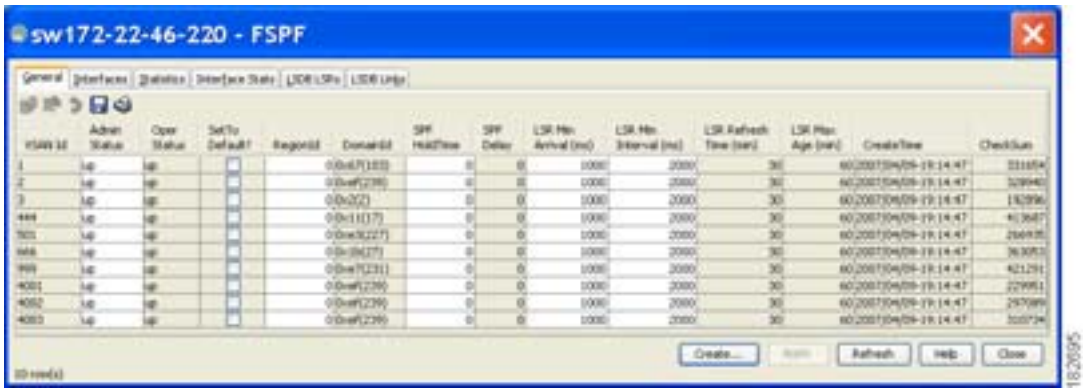
- LSR の経過時間
- LSR を示す番号
- リンク数

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

ステップ 1　**FC > Advanced > FSPF** を選択します。

FSPF ダイアログボックスが表示されます（図 18-5 を参照）。

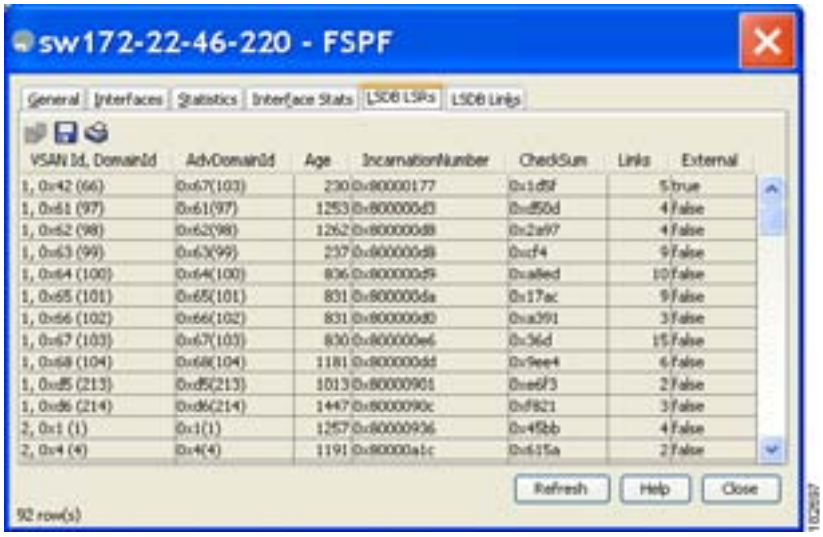
図 18-5　Device Manager の FSPF ダイアログボックス



ステップ 2　**LSDB LSRs** タブをクリックします。

FSPF データベース情報が表示されます（図 18-6 を参照）。

図 18-6　LSDB LSRs タブの FSPF データベース情報



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

FSPF 統計情報の表示

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

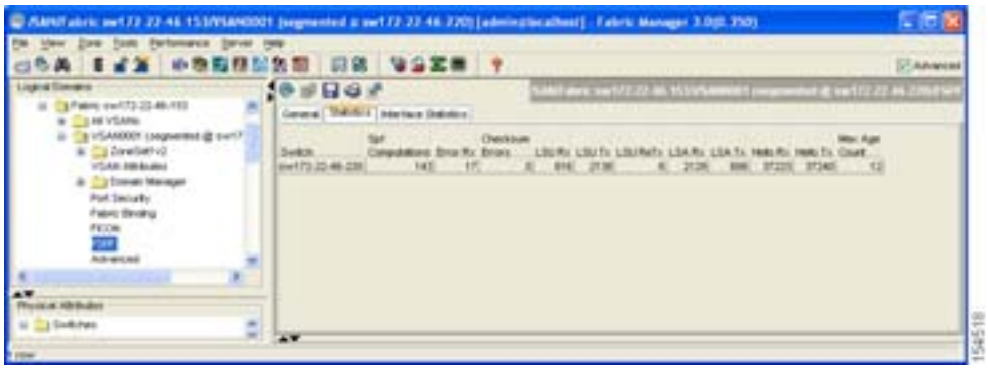
ステップ 1　Fabric を展開し、VSAN を展開してから、Logical Domains ペインで **FSPF** を選択します。

FSPF 設定ダイアログボックスが表示されます。

ステップ 2　**Statistics** タブをクリックします。

Information ペインに FSPF VSAN 統計情報が表示されます（図 18-7 を参照）。

図 18-7　FSPF VSAN 統計情報



ステップ 3　**Interface Statistics** タブをクリックします。

Information ペインに FSPF インターフェイスの統計情報が表示されます。

FSPF ルート

FSPF は FSPF データベースのエントリに基づいて、ファブリック内でトラフィックをルーティングします。これらのルートは動的に学習したり、静的に設定したりできます。

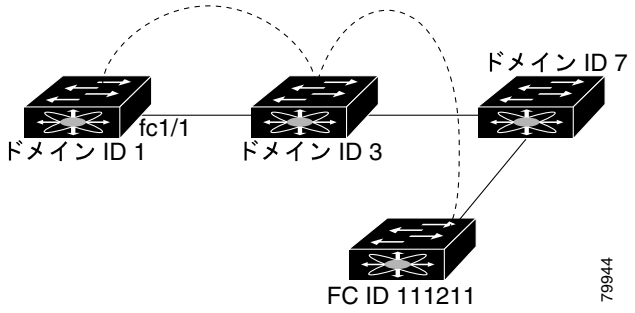
ここで説明する内容は、次のとおりです。

- ファイバ チャネル ルートの概要（p.18-13）
- ファイバ チャネル ルートの設定（p.18-13）

ファイバ チャネル 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。指定されたインターフェイスおよびドメインの FC ID を使用すると、スイッチ内の特定のルート（FC ID 111211 およびドメイン ID 3 など）にドメイン ID 1 を設定することができます（図 18-8 を参照）。

図 18-8　ファイバ チャネルのルート



ファイバ チャネル ルートの設定

FSPF をディセーブルにした場合は、ファイバ チャネル ルートを手動で設定できます。Device Manager を使用してファイバ チャネル ルートを設定する手順は、次のとおりです。

ステップ 1　**FC** > **Advanced** > **Routes** をクリックします。

FC Static Route Configuration ダイアログボックスが表示されます（図 18-9 を参照）。

図 18-9　Fibre Channel Static Route Configuration ダイアログボックス

ステップ 2　**Create** をクリックして、スタティック ルートを作成します。

Create Route ダイアログボックスが表示されます（図 18-10 を参照）。

図 18-10　Create Fibre Channel Route ダイアログボックス

ステップ 3　このルートを設定している VSAN ID を選択します。

ステップ 4　ルートを設定しているデバイスの宛先アドレスおよび宛先マスクを入力します。

ステップ 5　この宛先に到達するために使用するインターフェイスを選択します。

ステップ 6　ネクストホップのドメイン ID およびルート メトリックを選択します。

ステップ 7　**local** または **remote** オプション ボタンを選択します。

ステップ 8　これらの変更を保存するには、**Create** をクリックします。変更を保存せずに終了するには、**Close** をクリックします。

順序どおりの配信

データ フレームの IOD（順序どおりの配信）機能を使用すると、フレームは送信元から送信された場合と同じ順番で宛先に配信されます。

一部のファイバ チャネル プロトコルまたはアプリケーションでは、順序どおりではないフレーム配信は処理できません。このような場合、Nexus 5000 シリーズ 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、特定の出力ポートに送信されるフレームはすべて、受信時と同じ順番で配信されます。

IOD は、使用環境が順序どおりではないフレーム配信をサポートできない場合にのみ使用してください。

ヒント　順序どおりの配信機能がイネーブルな場合、グレースフル シャットダウン機能は実装されません。

ここで説明する内容は、次のとおりです。

- ネットワーク フレーム順序の再設定の概要（p.18-15）
- SAN ポート チャネル フレーム順序の再設定の概要（p.18-16）
- 順序どおりの配信のイネーブル化の概要（p.18-16）
- 順序どおりの配信のグローバルなイネーブル化（p.18-17）
- 特定の VSAN に対する順序どおりの配信のイネーブル化（p.18-17）
- ドロップ遅延時間の設定（p.18-18）

ネットワーク フレーム順序の再設定の概要

ネットワーク内のルートが変更された場合は、新規に選択されたパスが古いルートよりも高速であったり、輻輳がが少なかったりすることがあります。

図 18-11　ルート変更配信

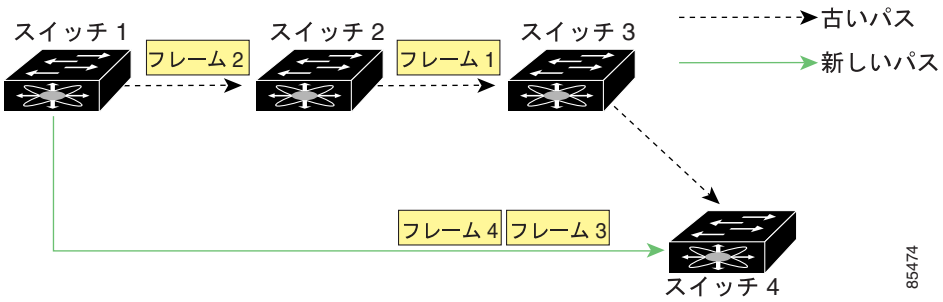


図 18-11 では、スイッチ 1 からスイッチ 4 への新しいパスの方が高速です。このシナリオでは、フレーム 3、フレーム 4 が、フレーム 1、フレーム 2 よりも先に配信されることがあります。

順序保証機能がイネーブルな場合、ネットワーク内のフレームは次のように配信されます。

- ネットワーク内のフレームは、送信時に順序どおりに配信されます。
- ネットワーク遅延ドロップ期間内に順序どおりに配信されなかったフレームは、ネットワーク内でドロップされます。

SAN ポート チャネル フレーム順序の再設定の概要

SAN 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 18-12　リンク輻輳配信

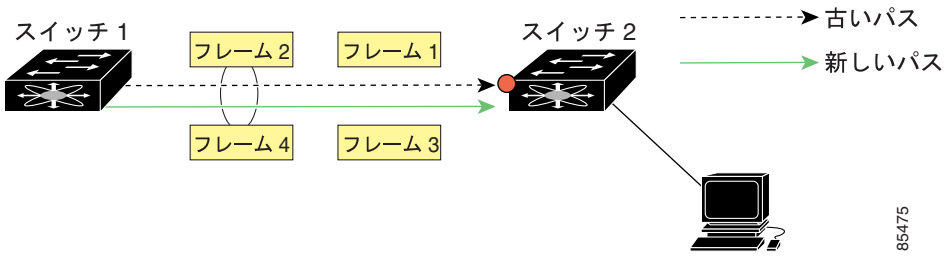


図 18-12 では、古いパスのポート（レッドの点）が輻輳しています。この場合、フレーム 3、フレーム 4 が、フレーム 1 およびフレーム 2 よりも先に配信されることがあります。

順序どおりの配信機能がイネーブルな場合に、ポート チャネル リンクが変更されると、SAN ポート チャネルを経由するフレームは次のように配信されます。

- 古いパスを使用するフレームは、新しいフレームが着信する前に配信されます。
- 新しいフレームは、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一度に削除されたあとに、新しいパスを介して配信されます。

ネットワーク遅延ドロップ期間内に、古いパスを介して順序どおりに配信できなかったフレームはドロップされます。「ドロップ遅延時間の設定」（p.18-18）を参照してください。

順序どおりの配信のイネーブル化の概要

特定の VSAN またはスイッチ全体で、順序どおりの配信機能をイネーブルにすることができます。Nexus 5000 シリーズ 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です。

ヒント　この機能は、順序どおりではないフレームを処理できないデバイスがスイッチ内にある場合に限り、イネーブルにすることを推奨します。通常のファブリック処理中は、Nexus 5000 シリーズ スイッチ内のロード バランシング アルゴリズムによって、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 OX ID に基づくロード バランシング アルゴリズムはハードウェア内で実行され、パフォーマンスは低下しません。ただし、順序どおりの配信機能がイネーブルな場合にファブリックに障害が発生すると、ファブリック転送が意図的に停止し、無秩序に転送された可能性のあるフレームがファブリックから除去されるため、リカバリが遅れます。

順序どおりの配信のグローバルなイネーブル化

順序どおりの配信パラメータがスイッチのすべての VSAN で一様になるように設定するには、順序どおりの配信をグローバルにイネーブル化します。

順序どおりの配信は、ファブリック全体で必要な場合のみグローバルにイネーブル化してください。それ以外の場合は、IOD 機能が必要な VSAN に対してのみ、IOD をイネーブルにしてください。

特定の VSAN に対する順序どおりの配信のイネーブル化

VSAN を作成すると、グローバルな順序保証値が自動的に継承されます。このグローバル値を上書きするには、新しい VSAN の順序保証をイネーブルまたはディセーブルにします。

Fabric Manager を使用して、マルチキャスト ツリー計算に値が最も小さなドメイン スイッチを使用する手順は、次のとおりです。

ステップ 1　ファブリックを展開して、**All VSANS** を選択します。

ステップ 2　**Attributes** タブをクリックします。

Information ペインに一般的な VSAN 属性が表示されます（図 18-13 を参照）。

図 18-13　一般的な VSAN 属性

ステップ 3　**InOrder Delivery** チェックボックスをオンにして、スイッチに対して IOD をイネーブルにします。

ステップ 4　これらの変更を保存する場合は、**Apply Changes** をクリックします。保存されていない変更を廃棄する場合は、**Undo Changes** をクリックします。

ドロップ遅延時間の設定

スイッチ全体またはスイッチ内の特定の VSAN のデフォルトの遅延時間を変更できます。

Fabric Manager を使用して特定のスイッチのドロップ遅延時間を設定する手順は、次のとおりです。

ステップ 1　ファブリックを展開して、**All VSANS** を選択します。

Information ペイン内に VSAN の設定が表示されます。

ステップ 2　**Attributes** タブをクリックします。

Information ペインに一般的な VSAN 属性が表示されます（図 18-14 を参照）。

図 18-14　一般的な VSAN 属性

ステップ 3　Network Latency フィールドをダブルクリックして、値を変更します。

ステップ 4　これらの変更を保存する場合は、**Apply Changes** をクリックします。保存されていない変更を廃棄する場合は、**Undo Changes** をクリックします。

デフォルト設定

表 18-2 に、FSPF 機能のデフォルト設定を示します。

表 18-2　FSPF のデフォルト設定

パラメータ	デフォルト
FSPF	すべての E ポートおよび TE ポートでイネーブル
SPF 計算	ダイナミック
SPF ホールド タイム	0
バックボーン領域	0
確認応答インターバル（RxmtInterval）	5 秒
リフレッシュ時間（LSRefreshTime）	30 分
最大有効期限（MaxAge）	60 分
Hello インターバル	20 秒
デッド インターバル	80 秒
配信ツリーの情報	主要スイッチ（ルート ノード）から取得
ルーティング テーブル	FSPF には指定された宛先への等コスト パスが最大 16 個格納されます。
ロード バランシング	各等コスト パスの宛先 ID および送信元 ID に基づきます。
順序どおりの配信	ディセーブル
ドロップ遅延	ディセーブル
スタティック ルート コスト	ルートのコスト（メトリック）が指定されていない場合、デフォルト コストは 10 です。
リモート宛先スイッチ	リモート宛先スイッチが指定されていない場合、デフォルトはダイレクトです。
マルチキャスト ルーティング	主要スイッチを使用して、マルチキャスト ツリーを計算します。

CHAPTER 19

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、Nexus 5000 シリーズ スイッチが提供する Fabric Login（FLOGI; ファブリック ログイン）データベース、ネーム サーバ機能、Fabric-Device Management Interface（FDMI）、Registered State Change Notification（RSCN）の情報について説明します。この章の内容は、次のとおりです。

- FLOGI の概要（p.19-2）
- ネーム サーバ プロキシ（p.19-3）
- FDMI（p.19-6）
- FDMI の表示（p.19-6）
- RSCN（p.19-7）
- デフォルト設定（p.19-11）

FLOGI の概要

ファイバ チャネル ファブリックでは、ホストまたはディスクごとに FC ID が必要です。必要なデバイスが FLOGI テーブルに表示されている場合は、ファブリック ログインに成功しています。ホスト Host Bus Adapter（HBA）および接続先ポートに直接接続されたスイッチで、FLOGI データベースを調べてください。「デフォルトの企業 ID リスト」（p.22-8）、および「スイッチの相互運用性」（p.22-10）を参照してください。

Fabric Manager を使用して FLOGI テーブル内にストレージ デバイスがあるか確認する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches** > **Interfaces** を展開して、**FC Physical** を選択します。

Information ペインにインターフェイス設定が表示されます。

ステップ 2　**FLOGI** タブをクリックします。

ファブリックにログインしているエンド デバイスがすべて表示されます（図 19-1 を参照）。

図 19-1　FLOGI 物理インターフェイス

ネーム サーバ プロキシ

ネーム サーバ機能は、各 VSAN 内のすべてのホストおよびストレージ デバイスの属性が格納されたデータベースをメンテナンスします。ネーム サーバを使用すると、情報が本来登録されていたデバイスからデータベース エントリを変更することができます。

別のデバイスによって登録済みのデータベース エントリの内容を変更（アップデートまたは削除）する必要がある場合は、プロキシ機能が便利です。

ここで説明する内容は、次のとおりです。

- ネーム サーバ プロキシ登録の概要（p.19-3）
- ネーム サーバ プロキシの登録（p.19-4）
- 重複 pWWN の拒否の概要（p.19-4）
- 重複 pWWN 拒否（p.19-4）
- ネーム サーバ データベース エントリの概要（p.19-5）
- ネーム サーバ データベース エントリの表示（p.19-5）

ネーム サーバ プロキシ登録の概要

すべてのネーム サーバ レジストレーション要求は、パラメータが登録または変更されたポートから送信されます。これ以外のポートから送信された要求は拒否されます。

この認証により、WWN は別のノードに特定のパラメータを登録することができます。

ネーム サーバ プロキシの登録

Fabric Manager を使用してネーム サーバ プロキシを登録する手順は、次のとおりです。

ステップ 1　Fabric を展開し、VSAN を展開してから、**Advanced** を選択します。

Information ペインに VSAN の詳細な設定が表示されます。

ステップ 2　**NS Proxies** タブをクリックします。

選択した VSAN の既存のネーム サーバ プロキシが表示されます（図 19-2 を参照）。

図 19-2　ネーム サーバ プロキシ

ステップ 3　PortName フィールドをダブルクリックて、新しい値を入力して、新しいネーム サーバ プロキシを登録します。

ステップ 4　これらの変更を保存する場合は、**Apply Changes** アイコンをクリックします。保存されていない変更をキャンセルする場合は、**Undo Changes** をクリックします。

重複 pWWN の拒否の概要

別のデバイスの pWWN を使用した悪意のあるログイン、または予期せぬログインを防止することができます。これらの pWWN を使用すると、ファブリックにログインして、ネーム サーバ データベース内の最初のデバイスを置き換えることができます。

重複 pWWN 拒否

重複 pWWN を拒否する方法は、『*Cisco Nexus 5000 Series CLI Configuration Guide*』を参照してください。

ネーム サーバ データベース エントリの概要

ネーム サーバの FCNS データベースには、すべてのホストのネーム エントリが格納されています。ネーム サーバを使用すると、Nx ポートで（ネーム サーバへの）PLOGI 中に属性を登録し、その他のホストの属性を取得できます。Nx ポートが明示的または暗黙的にログアウトすると、これらの属性は登録解除されます。

複数スイッチのファブリック構成の場合、配信されたデータベース内の情報は、各スイッチで稼働している複数のネーム サーバ インスタンスで共有されます。スイッチごとに、ネーム サーバ プロセスのインスタンスが 1 つ実行されます。

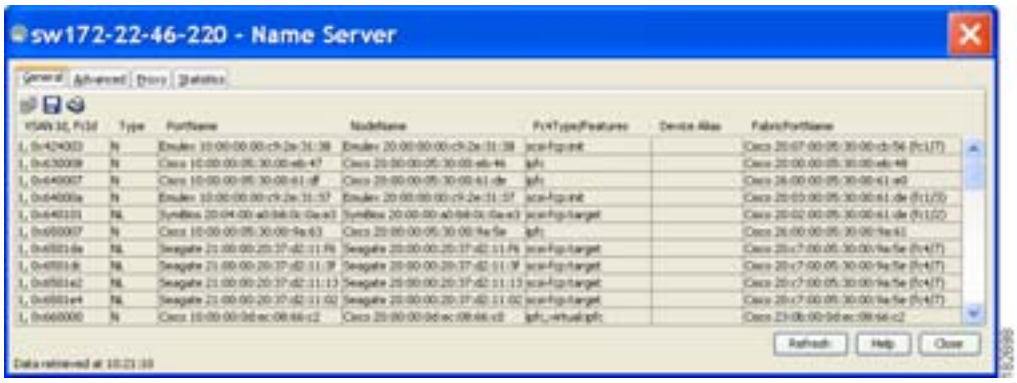
ネーム サーバ データベース エントリの表示

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

ステップ 1　**FC > Name Server** をクリックします。

Name Server ダイアログボックスが表示されます（図 19-3 を参照）。

図 19-3　Name Server ダイアログボックス



デフォルト タブは General タブです。ネーム サーバ データベースが表示されます。

ステップ 2　**Statistics** タブをクリックします。

ネーム サーバの統計情報が表示されます。

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

FDMI

Nexus 5000 シリーズ スイッチでは、FC-GS-4 規格に記述されている FDMI 機能がサポートされます。FDMI を使用すると、ファイバ チャネル HBA などのデバイスをインバンド通信を介して管理できます。この追加機能によって、既存のファイバ チャネル ネーム サーバおよび管理サーバの機能が補完されます。

FDMI 機能を使用すると、独自のホスト エージェントをインストールしなくても、スイッチ ソフトウェアは接続先 HBA およびホスト OS（オペレーティング システム）に関する次の管理情報を抽出できます。

- 製造元、モデル、およびシリアル番号
- ノード名およびノードのシンボリック名
- ハードウェア、ドライバ、およびファームウェア バージョン
- ホスト OS の名前およびバージョン番号

すべての FDMI エントリは永続的ストレージに格納され、FDMI プロセスの起動時に取得されます。

FDMI の表示

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

ステップ 1　**FC** > **Advanced** > **FDMI** をクリックします。

FDMI ダイアログボックスが表示されます。

ステップ 2　**HBA** タブ、**Versions** タブ、または **Targets** タブをクリックします。

RSCN

RSCN は、ファブリック内の変更をホストに通知するファイバ チャネル サービスです。ホストが受信したこの情報は、（SCR を介して）ファブリック コントローラに登録されます。これらの通知により、1 つまたは複数の次のイベントが、適切なタイミングで示されます。

- ファブリックへのディスクの追加または削除
- ネーム サーバの登録内容の変更
- 新しいゾーンの適用
- IP アドレスの変更
- ホストの動作に影響するその他の同様なイベント

ここで説明する内容は、次のとおりです。

- RSCN 情報の概要（p.19-7）
- RSCN 情報の表示（p.19-8）
- multi-pid オプションの概要（p.19-8）
- multi-pid オプションの設定（p.19-9）
- RSCN 統計情報のクリア（p.19-9）
- CFS を使用した RSCN タイマー設定の配信（p.19-10）
- CFS による RSCN タイマーの設定（p.19-11）

RSCN 情報の概要

登録先ホストおよびファブリック内の到達可能なすべてのスイッチに、スイッチ RSCN（SW-RSCN）が送信されます。

（注） スイッチは RSCN を送信して、変更が発生したことを登録先ノードに通知します。ネーム サーバに問い合わせて、新しい情報を取得する作業は、ノードが行います。ノードに送信された RSCN 内のスイッチからは、変更された情報の詳細は配信されません。

RSCN 情報の表示

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

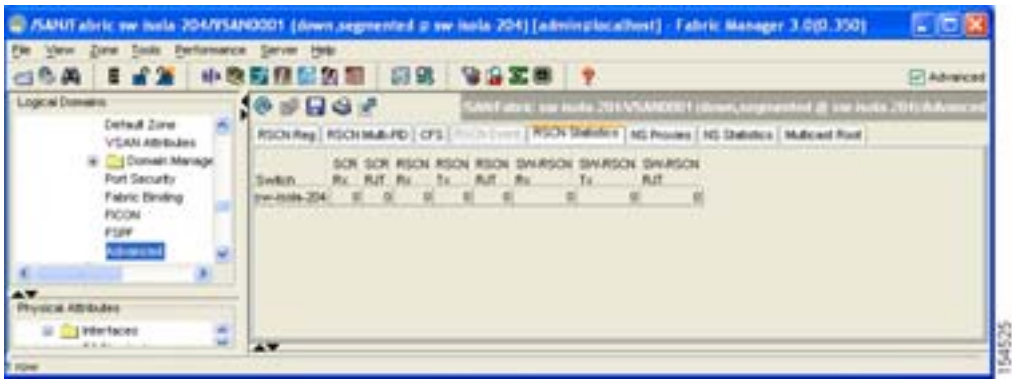
ステップ 1　Fabric を展開し、VSAN を展開してから、**Advanced** を選択します。

Information ペインに VSAN の詳細な設定が表示されます。

ステップ 2　**RSCN Reg** タブまたは **RSCN Statistics** タブをクリックします（図 19-4 を参照）。

RSCN Statistics ペインが表示されます（図 19-4 を参照）。

図 19-4　RSCN 統計情報



multi-pid オプションの概要

RSCN の **multi-pid** オプションがイネーブルな場合、登録済みの Nx ポートに対して生成された RSCN には、関連ポート ID を複数格納できます。この場合、複数の関連ポート ID を単一 RSCN に格納する前に、ゾーン分割ルールが適用されます。このオプションをイネーブルにすると、RSCN 数を削減できます。たとえば、2 つのディスク（D1、D2）およびホスト（H）がスイッチ 1 に接続されているとします。ホスト H は RSCN を受信するように登録されています。D1、D2、および H は同じゾーンに属します。ディスク D1 および D2 が同時にオンラインになると、次のいずれかの処理が適用されます。

- スイッチ 1 で **multi-pid** オプションがディセーブルになります。ホスト H に対して 2 つの RSCN が生成されます（1 つはディスク D1 用、もう 1 つはディスク D2 用）。
- スイッチ 1 で **multi-pid** オプションがイネーブルになります。ホスト H に対して RSCN が 1 つ生成され、RSCN ペイロードによって関連ポート ID がリストされます（この場合は D1 および D2）。

（注）　一部の Nx ポートでは、multi-pid RSCN ペイロードをサポートできないことがあります。その場合は、RSCN の **multi-pid** オプションをディセーブルにしてください。

multi-pid オプションの設定

Fabric Manager を使用して **multi-pid** オプションを設定する手順は、次のとおりです。

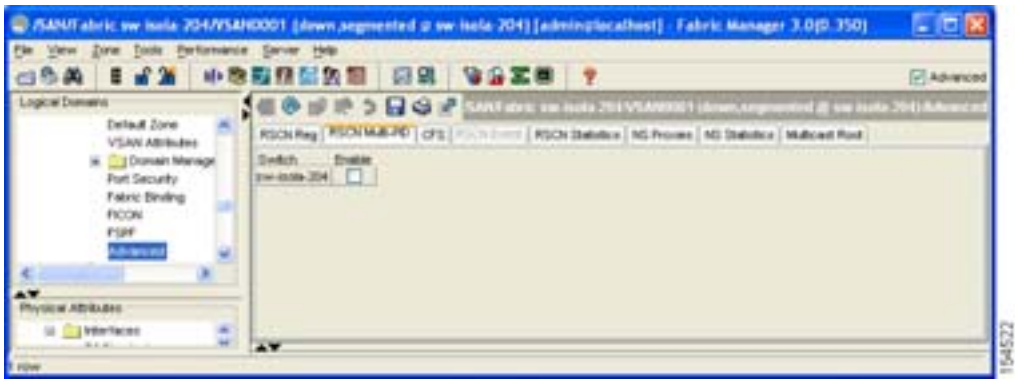
ステップ 1　Fabric を展開し、VSAN を展開してから、**Advanced** を選択します。

Information ペインに VSAN の詳細な設定が表示されます。

ステップ 2　**RSCN Multi-PID** タブをクリックします。

RSCN Multi-PID ペインが表示されます（図 19-5 を参照）。

図 19-5　RSCN Multi-PID



ステップ 3　**Enable** チェックボックスをオンにします。

ステップ 4　これらの変更を保存する場合は、**Apply Changes** アイコンをクリックします。保存されていない変更をキャンセルする場合は、**Undo Changes** をクリックします。

RSCN 統計情報のクリア

カウンタをクリアし、そのあとで、別の一連のイベントに対するカウンタを表示することができます。たとえば、特定のイベント（ONLINE または OFFLINE イベントなど）に対して生成される RSCN 数または SW-RSCN 数を追跡できます。これらの統計情報を使用すると、VSAN 内のイベントごとに応答を監視できます。

指定された VSAN の RSCN 統計情報をクリアする手順については、『*Cisco Nexus 5000 Series CLI Configuration Guide*』を参照してください。

CFS を使用した RSCN タイマー設定の配信

各スイッチのタイムアウト値は手動で設定されるため、複数のスイッチがさまざまな時刻にタイムアウトする場合は設定ミスが生じます。つまり、ネットワーク内の複数の N ポートが異なる時刻に RSCN を受信することがあります。Cisco Fabric Services（CFS）を使用すると、設定情報がファブリック内のすべてのスイッチに自動配信されて、この状況が回避されます。また、SW-RSCN 数も削減されます。

RSCN は配信モードと非配信モードをサポートします。配信モードの場合、RSCN は CFS を使用して、ファブリック内のすべてのスイッチに設定を配信します。非配信モードの場合、ローカル スイッチの設定コマンドのみが影響を受けます。

（注） すべての設定コマンドが配布されるわけではありません。**rscn event-tov** ***tov*** **vsan** ***vsan*** コマンドのみが配信されます。

RSCN タイマーは、初期化およびスイッチオーバー中に CFS に登録されます。ハイ アベイラビリティ構成の場合に、RSCN タイマー配信がクラッシュし、再起動またはスイッチオーバーが発生すると、クラッシュまたはスイッチオーバーの前の状態から標準機能が再開します。

（注） ダウングレードを実行する場合は、ネットワーク内の RCSN タイマー値をデフォルト値に戻しておいてください。そうしないと、VSAN およびその他のデバイス間のリンクがディセーブルになります。

アップグレードまたはダウングレード中の各ソフトウェア 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。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 タイマー配信の機能がディセーブルです。

CFS による RSCN タイマーの設定

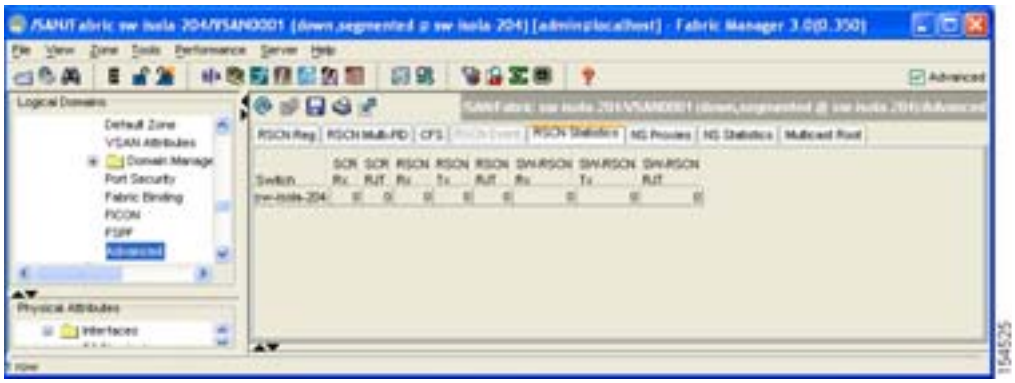
Fabric Manager を使用して CFS に RSCN タイマーを設定する手順は、次のとおりです。

ステップ 1　Fabric を展開し、VSAN を展開してから、Logical Domains ペインで **Advanced** を選択します。

ステップ 2　**RSCN Event** タブをクリックします。

Information ペインに VSAN の詳細な設定が表示されます（図 19-6 を参照）。

図 19-6　VSAN の詳細な設定



ステップ 3　**TimeOut** 値をダブルクリックして、選択した VSAN の値を変更します（ミリ秒）。

ステップ 4　これらの変更を保存する場合は、**Apply Changes** アイコンをクリックします。保存されていない変更をキャンセルする場合は、**Undo Changes** をクリックします。

この例では、イベントのタイムアウト値が VSAN 12 に対して 300 ミリ秒に設定されています。

デフォルト設定

表 19-1 に、RSCN のデフォルト設定を示します。

表 19-1　RSCN のデフォルト設定

パラメータ	デフォルト
RSCN タイマー値	2000 ミリ秒（ファイバ チャネル VSAN の場合）
RSCN タイマー設定の配信	ディセーブル

CHAPTER 20

SPAN の設定

Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能（別名、ポート ミラーリングまたはポート モニタリング）は、ネットワーク アナライザによるネットワーク トラフィックの解析を選択します。ネットワーク アナライザは、Cisco SwitchProbe、Fibre Channel Analyzer、または Remote Monitoring（RMON; リモート モニタリング）プローブにもなります。

ここで説明する内容は、次のとおりです。

- SPAN 送信元の概要（p.20-2）
- SPAN 宛先の概要（p.20-3）
- SPAN の設定（p.20-4）
- SPAN のデフォルト設定値（p.20-7）

SPAN 送信元の概要

SPAN 送信元とは、トラフィックの監視を開始するインターフェイスです。Nexus 5000 シリーズ スイッチは、SPAN 送信元としてイーサネット、仮想イーサネット、ファイバ チャネル、仮想ファイバ チャネル、ポート チャネル、SAN ポート チャネル、VLAN、および VSAN をサポートします。VLAN または VSAN の場合、指定された VLAN または VSAN のすべてのサポート対象のインターフェイスが SPAN 送信元として含まれます。SPAN トラフィックは、イーサネット、仮想イーサネット、ファイバ チャネル、および仮想ファイバ チャネル送信元インターフェイスの入力方向、出力方向、あるいは両方を選択できます。

- 入力送信元（Rx）— この送信元インターフェイスを経由してスイッチに入るトラフィックは、SPAN 宛先ポートにコピーされます。
- 出力送信元（Tx）— この送信元インターフェイスを経由してスイッチから出るトラフィックは、SPAN 宛先ポートにコピーされます。

（注） Device Manager は、送信元ポートとしてイーサネットまたは仮想イーサネット インターフェイスの設定をサポートしていません。

送信元ポートの特性

送信元ポート（別名、モニタ対象ポート）は、ネットワーク トラフィックを解析するために監視するスイッチド インターフェイスです。スイッチは任意の数の入力送信元ポート（スイッチ上で使用できるポートの最大数が限度）および任意の数の送信元 VLAN または VSAN をサポートします。

送信元ポートには、次の特性があります。

- 任意のポート タイプ（イーサネット、仮想イーサネット、ファイバ チャネル、仮想ファイバ チャネル、ポート チャネル、SAN ポート チャネル、VLAN、および VSAN）になることができます。
- 複数の SPAN セッションで監視できます。
- 宛先ポートにはできません。
- 各送信元ポートに監視する方向（入力、出力、または両方）を設定できます。VLAN、VSAN、ポート チャネル、および SAN ポート チャネル送信元の場合、監視する方向は入力だけが可能になり、グループ内のすべての物理ポートに適用されます。
- 送信元ポートは同じ VLAN または VSAN にあっても、異なる VLAN または VSAN にあってもかまいません。
- VLAN または VSAN SPAN 送信元の場合、送信元 VLAN または VSAN のすべてのアクティブ ポートが送信元ポートとして含まれます。
- スイッチは、最大 2 つの出力 SPAN 送信元ポートをサポートします。

SPAN 宛先の概要

SPAN 宛先は、送信元インターフェイスを監視するインターフェイスを意味します。Nexus 5000 シリーズ スイッチは、SPAN 宛先としてイーサネットおよびファイバ チャネル インターフェイスをサポートします。

（注）Device Manager は、宛先ポートとしてのイーサネット インターフェイスの設定をサポートしていません。

送信元 SPAN	宛先 SPAN
イーサネット	イーサネット
ファイバ チャネル	ファイバ チャネル
ファイバ チャネル	イーサネット（FCoE）
仮想イーサネット	イーサネット
仮想ファイバ チャネル	ファイバ チャネル
仮想ファイバ チャネル	イーサネット（FCoE）

宛先ポートの特性

各ローカル SPAN セッションには、送信元ポート、VLAN、または VSAN からのトラフィックのコピーを受信する宛先ポート（別名、モニタ側ポート）が必要です。宛先ポートには、次の特性があります。

- 任意の物理ポート（イーサネット、イーサネット［FCoE］、またはファイバ チャネル）にできます。仮想イーサネットおよび仮想ファイバ チャネル ポートは、宛先ポートにはできません。
- 送信元ポートにはできません。
- ポート チャネルまたは SAN ポート チャネル グループにはできません。
- SPAN セッションがアクティブの間、スパニング ツリーに参加しません。
- 任意の SPAN セッションの送信元 VLAN に属する場合、送信元リストから除外され、監視されません。
- モニタ対象のすべての送信元ポートの送受信トラフィックのコピーを受信します。宛先ポートがオーバーサブスクライブ状態の場合、輻輳を起こす可能性があります。その結果、1 つまたは複数の送信元ポートでトラフィック転送に影響を与える可能性があります。

SPAN の設定

SPAN セッションを設定して、送信元ポートからスイッチ上の指定された宛先ポートにパケットを複製できます。ここで説明する内容は、次のとおりです。

- Device Manager を使用した SPAN の設定（p.20-4）
- Device Manager を使用した SPAN セッションの作成（p.20-5）
- Device Manager を使用した SPAN 送信元の編集（p.20-6）
- Device Manager を使用した SPAN セッションの削除（p.20-7）

Device Manager を使用した SPAN の設定

SD ポートを使ってネットワーク トラフィックを監視する手順は次のとおりです。

ステップ 1　SD ポートを設定します。

ステップ 2　指定した SPAN セッションに SD ポートを接続します。

ステップ 3　セッションに送信元インターフェイスを追加して、ネットワーク トラフィックを監視します。

Device Manager を使用して SPAN モニタリングの SD ポートを設定する手順は、次のとおりです。

ステップ 1　設定するポートを右クリックして **Configure** をクリックします。

通常のポート設定ダイアログボックスが表示されます。

ステップ 2　Mode で **SD** を選択します。

ステップ 3　**Apply** をクリックして変更を適用します。

ステップ 4　ダイアログボックスを閉じます。

Device Manager を使用した SPAN セッションの作成

Device Manager を使用して SPAN セッションを作成する手順は、次のとおりです。

ステップ 1　**Interface** > **SPAN** を選択します。

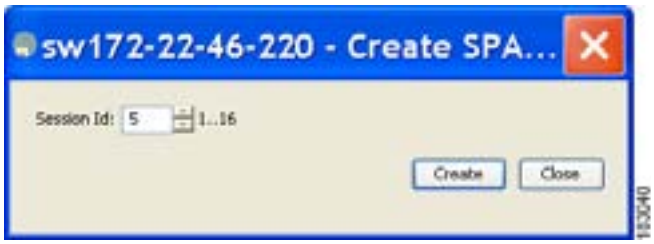
SPAN ダイアログボックスが表示されます。

ステップ 2　**Sessions** タブをクリックします。

ステップ 3　**Create** をクリックします。

Create SPAN Sessions ダイアログボックスが表示されます（図 20-1 を参照）。

図 20-1　Create SPAN Sessions ダイアログボックス



ステップ 4　上向きまたは下向き矢印キーを使用して 1 ～ 16 のセッション ID を選択し、**Create** をクリックします。

ステップ 5　作成するセッションごとにステップ 4 を繰り返します。

ステップ 6　該当するセッションの Dest Interface フィールドに宛先インターフェイスを入力します。

ステップ 7　該当するセッションの Filter VSAN List フィールドにフィルタ VSAN リストを入力します。

ステップ 8　Admin ドロップダウン リストで **active** を選択するか、アクティブな管理ステータスを選択します。

ステップ 9　**Apply** をクリックして変更を保存します。

ステップ 10　2 つのダイアログボックスを閉じます。

Device Manager を使用した SPAN 送信元の編集

Device Manager を使用して SPAN 送信元を編集する手順は、次のとおりです。

ステップ 1　**Interface** > **SPAN** を選択します。

SPAN ダイアログボックスが表示されます。

ステップ 2　**Sources** タブをクリックします。

SPAN Sources ダイアログボックスが表示されます（図 20-2 を参照）。

図 20-2　SPAN Sources タブ

ステップ 3　VSAN List フィールドに VSAN リスト名を入力します。

ステップ 4　**Edit Interface List** をクリックします。

Source Interfaces ダイアログボックスが表示されます。

ステップ 5　**Create** をクリックします。

Source Interfaces Interface Sources ダイアログボックスが表示されます（図 20-3 を参照）。

図 20-3　Source Interfaces Interface Sources ダイアログボックス

ステップ 6　browse ボタンをクリックして、使用できる FC ポートのリストを表示します。

ステップ 7　ポートを選択し、**OK** をクリックします。

ステップ 8　指定する方向をチェックします（**receive** または **transmit**）。

ステップ 9　**Create** をクリックして FC インターフェイス送信元を作成します。

ステップ 10　開いている 3 つのダイアログボックスの **Close** をクリックし、それぞれのダイアログボックスを閉じます。

Device Manager を使用した SPAN セッションの削除

Device Manager を使用して SPAN セッションを削除する手順は、次のとおりです。

ステップ 1　**Interface** > **SPAN** を選択します。

SPAN ダイアログボックスが表示されます。

ステップ 2　**Sessions** タブをクリックします。

ステップ 3　削除する SPAN セッションをクリックします。

ステップ 4　**Delete** をクリックします。

SPAN セッションが削除されます。

ステップ 5　ダイアログボックスを閉じます。

SPAN のデフォルト設定値

表 20-1 に、SPAN パラメータのデフォルト設定値を示します。

表 20-1　SPAN パラメータのデフォルト設定値

パラメータ	デフォルト
SPAN セッション	アクティブ
フィルタが指定されていない場合	SPAN トラフィックには、すべてのアクティブ VSAN から特定のインターフェイスを経由するトラフィックが含まれます。
カプセル化	ディセーブル
SD ポート	出力フレーム形式はファイバ チャネルです。

CHAPTER 21

SCSI ターゲットの検出

この章では、Nexus 5000 シリーズ スイッチが提供する SCSI LUN 検出機能について説明します。この章の内容は、次のとおりです。

- SCSI LUN 検出の概要（p.21-2）
- SCSI LUN 情報の表示（p.21-4）

SCSI LUN 検出の概要

Small Computer System Interface（SCSI）ターゲットは、ディスク、テープ、およびその他のストレージ デバイスなどです。これらのターゲットの Logical Unit Number（LUN）は、ネーム サーバに登録されません。

ネーム サーバに LUN 情報が必要な理由は、次のとおりです。

- LUN ストレージ デバイス情報を表示して、NMS（Network Management System; ネットワーク管理システム）がこの情報にアクセスできるようにするため
- デバイス容量、シリアル番号、およびデバイス ID 情報を報告するため
- ネーム サーバに発信側およびターゲット機能を登録するため

SCSI LUN 検出機能では、ローカル ドメイン コントローラのファイバ チャネル アドレスを使用します。ローカル ドメイン コントローラは送信元 FC ID として使用され、SCSI デバイス上で SCSI INQUIRY、REPORT LUNS、および READ CAPACITY コマンドが実行されます。

SCSI LUN 検出機能は CLI または SNMP を使用して、オンデマンドで開始されます。隣接スイッチが Nexus 5000 シリーズに含まれる場合、この情報は隣接スイッチとも同期されます。

ここで説明する内容は、次のとおりです。

- SCSI LUN 検出開始の概要（p.21-2）
- SCSI LUN 検出の開始（p.21-3）
- カスタマイズ検出開始の概要（p.21-3）
- カスタマイズ検出の開始（p.21-4）

SCSI LUN 検出開始の概要

SCSI LUN 検出はオンデマンドで実行されます。

ネーム サーバ データベースに格納され、FC4 Type = SCSI_FCP として登録された Nx ポートのみが、検出されます。

SCSI LUN 検出の開始

Device Manager を使用して SCSI LUN 検出を開始する手順は、次のとおりです。

ステップ 1　**FC** > **Advanced** > **LUNs** を選択します。

LUN Configuration ダイアログボックスが表示されます（図 21-1 を参照）。

図 21-1　LUN Configuration ダイアログボックス

ステップ 2　StartDiscovery を **local**、**remote**、または **both** に設定します。

ステップ 3　**DiscoveryType** および **OS** を選択します。

ステップ 4　**Apply** をクリックして、検出を開始します。

カスタマイズ検出開始の概要

カスタマイズ検出は、検出を開始するように選択的に設定された VSAN/ ドメイン ペアのリストで構成されます。ドメイン ID は 0 ～ 255 の 10 進数、または 0x0 ～ 0xFF の 16 進数です。

カスタマイズ検出の開始

Device Manager を使用してカスタマイズ検出を開始する手順は、次のとおりです。

ステップ 1　VSAN ドロップダウン メニューをクリックして、カスタマイズ検出を開始する VSAN を選択します。

ステップ 2　**FC** > **Advanced** > **LUNs** を選択します。

LUN Configuration ダイアログボックスが表示されます。

ステップ 3　StartDiscovery を **local**、**remote**、または **both** に設定します。

ステップ 4　DiscoveryType および OS フィールドに入力します。

ステップ 5　**Apply** をクリックして、検出を開始します。

SCSI LUN 情報の表示

Device Manager を使用して検出結果を表示する手順は、次のとおりです。

ステップ 1　**FC** > **Advanced** > **LUNs** を選択します。

LUN Configuration ダイアログボックスが表示されます。

ステップ 2　**LUN** タブまたは **Targets** タブをクリックします。

CHAPTER 22

高度な機能および概念

この章では、Nexus 5000 シリーズ スイッチが提供する高度なファイバ チャネル機能について説明します。この章の内容は、次のとおりです。

- ファイバ チャネルの TOV（p.22-2）
- WWN（p.22-6）
- HBA の FC ID 割り当て（p.22-8）
- スイッチの相互運用性（p.22-10）
- デフォルト設定（p.22-14）

ファイバ チャネルの TOV

スイッチのファイバ チャネル プロトコルに関連するタイマー値を変更するには、次の Timeout Value（TOV; タイムアウト値）を設定します。

- Distributed Services TOV（D_S_TOV）— 有効範囲は 5,000 ～ 10,000 ミリ秒です。デフォルトは 5,000 ミリ秒です。
- Error Detect TOV（E_D_TOV）— 有効範囲は 1,000 ～ 10,000 ミリ秒です。デフォルトは 2,000 ミリ秒です。この値は、ポート初期化中に他端と比較されます。
- Resource Allocation TOV（R_A_TOV）— 有効範囲は 5,000 ～ 10,000 ミリ秒です。デフォルトは 10,000 ミリ秒です。この値は、ポート初期化中に他端と比較されます。

（注） Fabric Stability TOV（F_S_TOV）定数は設定できません。

ここで説明する内容は、次のとおりです。

- すべての VSAN のタイマー設定（p.22-2）
- VSAN ごとのタイマー設定（p.22-4）
- fctimer 配信の概要（p.22-4）
- fctimer 配信のイネーブル化またはディセーブル化（p.22-5）
- データベース マージの注意事項（p.22-5）

すべての VSAN のタイマー設定

スイッチでファイバ チャネル プロトコルに関連するタイマー値を変更できます。

注意 D_S_TOV、E_D_TOV、および R_A_ TOV 値は、スイッチ内のすべての VSAN を一時停止するしないかぎり、グローバルに変更できません。

（注） タイマー値を変更するときに VSAN を指定しない場合は、変更された値がスイッチ内のすべての VSAN に適用されます。

Fabric Manager を使用してタイマーを設定する手順は、次のとおりです。

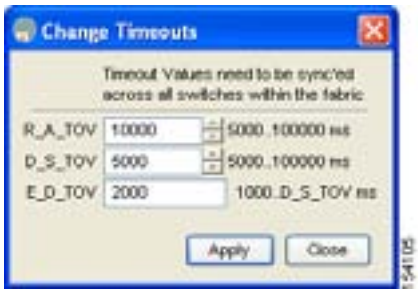
ステップ 1 Physical Attributes ペインで **Switches** > **FC Services** を展開して、**Timers & Policies** を選択します。

Information ペインに複数のスイッチのタイマーが表示されます。

ステップ 2　**Change Timeouts** ボタンをクリックして、タイムアウト値を設定します。

ダイアログボックスが表示されます（図 22-1 を参照）。

図 22-1　Fabric Manager でのタイマーの設定

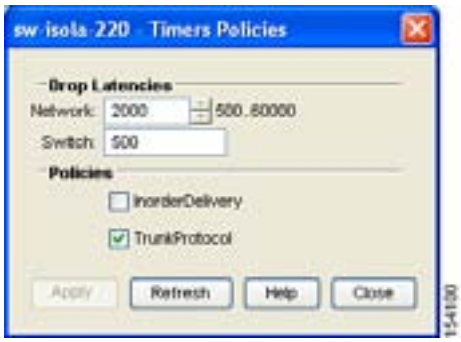


Device Manager を使用してタイマーを設定する手順は、次のとおりです。

ステップ 1　**FC** > **Advanced** > **Timers/Policies** を選択します。

ダイアログボックスに単一スイッチのタイマーが表示されます（図 22-2 を参照）。

図 22-2　Device Manager でのタイマーの設定



VSAN ごとのタイマー設定

特定の VSAN に fctimer を発行し、ファイバ チャネルなど特別なリンクを含む VSAN に異なる TOV 値を設定することもできます。個別の VSAN に、異なる E_D_TOV、R_A_TOV、D_S_TOV 値を設定できます。タイマー値が変更されると、アクティブな VSAN は一時停止してアクティブになります。

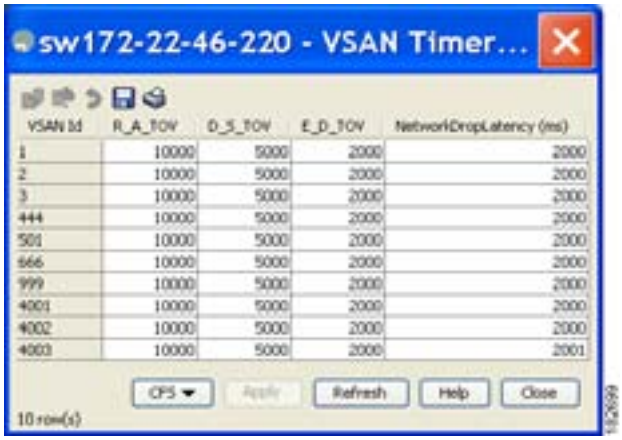
（注） この設定は、ファブリック内のすべてのスイッチに伝播する必要があります。ファブリックのすべてのスイッチで同じ値を設定するようにしてください。

Device Manager を使用して VSAN 単位のファイバ チャネル タイマーを設定する手順は、次のとおりです。

ステップ 1　**FC > Advanced > VSAN Timers** を選択します。

VSANs Timer ダイアログボックスが表示されます（図 22-3 を参照）。

図 22-3　Device Manager の VSAN タイマー



ステップ 2　設定するタイマー値を入力します。

ステップ 3　**Apply** をクリックして、変更を保存します。

fctimer 配信の概要

ファブリック内のすべての Cisco SAN スイッチで、VSAN 単位の fctimer ファブリック配信をイネーブルにできます。fctimer を設定して、配信をイネーブルにすると、この設定がファブリック内のすべてのスイッチに配信されます。

スイッチの配信をイネーブルにしたあとで最初の設定コマンドを入力すると、ファブリック全体のロックが自動的に有効になります。fctimer アプリケーションは有効 / 保留データベース モデルを使用して、ご使用の設定に基づいてコマンドを格納したり、コミットしたりします。

CFS アプリケーションの詳細については、第 7 章「CFS の使用」を参照してください。

fctimer 配信のイネーブル化またはディセーブル化

Device Manager を使用して fctimer 設定変更をイネーブルにして、配信する手順は、次のとおりです。

ステップ 1　**FC** > **Advanced** > **VSAN Timers** を選択します。

VSANs Timer ダイアログボックスが表示されます（図 22-3 を参照）。

ステップ 2　設定するタイマー値を入力します。

ステップ 3　**Apply** をクリックして、変更を保存します。

ステップ 4　これらの変更を配信するには、CFS ドロップダウン リストで **commit** を選択します。変更を保存しないで終了するには、**abort** を選択します。

fctimer 設定の変更をコミットすると、有効データベースが保留データベースの設定変更で上書きされ、ファブリック内のすべてのスイッチが同じ設定になります。セッション機能を実行しないで、fctimer の設定変更をコミットすると、fctimer 設定は物理ファブリック内のすべてのスイッチに配信されます。

データベース マージの注意事項

2 つのファブリックを結合する場合は、次の注意事項に従ってください。

- マージに関する次の条件に注意してください。
  - マージ プロトコルは、fctimer 値の配信に実装されません。ファブリックをマージする場合、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で配信されます。
  - fctimer 設定が適用されるのは、fctimer 値が変更された VSAN を含むスイッチのみです。
  - グローバル fctimer 値は配信されません。
- 配信がイネーブルな場合は、グローバル タイマー値を設定しないでください。

（注）　保留中の fctimer 設定処理の最大数は 15 です。この値に達した場合、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。

詳細については、「CFS マージのサポート」（p.7-7）を参照してください。

WWN

スイッチの WWN は、イーサネット MAC（メディア アクセス制御）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。

Nexus 5000 シリーズ スイッチは、3 つの Network Address Authority（NAA）アドレス フォーマットをサポートします（表 22-1 を参照）。

表 22-1　NAA WWN の標準フォーマット

NAA アドレス	NAA タイプ	WWN フォーマット	
IEEE 48 ビット アドレス	タイプ 1 = 0001b	000 0000 0000b	48 ビット MAC アドレス
IEEE 拡張	タイプ 2 = 0010b	ローカルに割り当て	48 ビット MAC アドレス
IEEE 登録	タイプ 5 = 0101b	IEEE 企業 ID：24 ビット	VSID：36 ビット

注意　WWN の変更は、管理者や、スイッチの動作に精通した担当者が実行してください。

ここで説明する内容は、次のとおりです。

- WWN 情報の確認（p.22-6）
- リンク初期化 WWN の使用法（p.22-6）
- セカンダリ MAC アドレスの設定（p.22-7）

WWN 情報の確認

Device Manager を使用して WWN 情報を表示するには、**FC > Advanced > WWN Manager** を選択します。割り当てられた WWN のリストが表示されます。

リンク初期化 WWN の使用法

Exchange Link Protocol（ELP）および Exchange Fabric Protocol（EFP）は、リンク初期化中に WWN を使用します。ELP と EFP は両方とも、リンク初期化中にデフォルトで VSAN WWN を使用します。ただし、ELP の使用方法はピア スイッチの使用方法に応じて変わります。

- ピア スイッチの ELP が sWWN を使用する場合、ローカル スイッチも sWWN を使用します。
- ピア スイッチの ELP が VSAN WWN を使用する場合、ローカル スイッチも VSAN WWN を使用します。

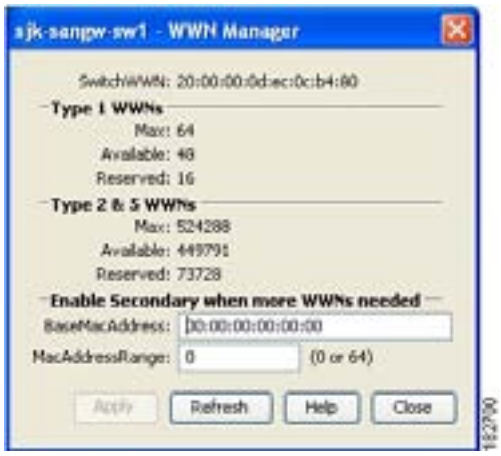
セカンダリ MAC アドレスの設定

Device Manager を使用してセカンダリ MAC アドレスを割り当てる手順は、次のとおりです。

ステップ 1　**FC > Advanced > WWN Manager** を選択します。

割り当てられた WWN のリストが表示されます（図 22-4 を参照）。

図 22-4　Device Manager で割り当てられた WWN



ステップ 2　BaseMacAddress および MacAddressRange フィールドに適切な値を入力します。

ステップ 3　これらの変更を保存するには、**Apply** をクリックします。変更を保存しないで終了するには、**Close** をクリックします。

HBA の FC ID 割り当て

ファイバ チャネル標準では、任意のスイッチの F ポートに接続された N ポートに、固有の FC ID を割り当てる必要があります。使用する FC ID 数を保護するために、Nexus 5000 シリーズ スイッチは特殊な割り当て方式を使用します。

Host Bus Adapter（HBA）で、ドメインと領域が同じ FC ID を持つターゲットを検出しないことがあります。スイッチ ソフトウェアは、この動作をサポートしないテスト対象の企業 ID リストを保持します。これらの HBA には単一の FC ID が割り当てられます。HBA が同じドメインおよび領域内でターゲットを検出できる場合、領域全体が割り当てられます。

多数のポートを備えたスイッチのスケーラビリティを高めるために、スイッチ ソフトウェアは同じドメインおよび領域内でターゲットを検出できる HBA リストを保持します。各 HBA は、ファブリック ログイン中に pWWN で使用される企業 ID（別名、Organizational Unique Identifier［OUI; 組織固有識別子］）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、その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 のタイプ（領域全体または単一）に関係なく、FC ID エントリは保持されます。

ここで説明する内容は、次のとおりです。

- デフォルトの企業 ID リスト（p.22-8）
- 企業 ID の設定の確認（p.22-9）

デフォルトの企業 ID リスト

すべての Nexus 5000 シリーズ スイッチには、領域割り当てが必要な企業 ID のデフォルトリストが格納されています。企業 ID を使用すると、設定される永続的 FC ID エントリ数が削減されます。これらのエントリを設定または変更するには、CLI を使用します。

注意　永続的エントリは、企業 ID 設定よりも優先します。HBA がターゲットの検出に失敗した場合、HBA およびターゲットが同じスイッチに接続されていて、これらの FC ID の領域が同じであることを確認してから、次の手順を実行します。

1. HBA に接続されたポートをシャットダウンします。
2. 永続的 FC ID エントリを消去します。
3. pWWN から 企業 ID を取得します。
4. 領域割り当てを必要とするリストに、この企業 ID を追加します。
5. ポートを起動します。

企業 ID のリストには、次の特性があります。

- 永続的 FC ID 設定は常に企業 ID リストよりも優先します。領域を受信するように企業 ID が設定されている場合でも、永続的 FC ID 設定によって、単一 FC ID が割り当てられます。
- 以降のリリースに追加された新しい企業 ID は、既存の企業 ID に自動的に追加されます。
- 企業 ID のリストは、実行コンフィギュレーションおよび保存されたコンフィギュレーションの一部として保存されます。
- 企業 ID リストが使用されるのは、fcinterop FC ID 割り当て方式が auto モードの場合のみです。interop FC ID 割り当てモードは、変更しないかぎり、デフォルトで auto です。

ヒント　fcinterop FC ID 割り当て方式を auto に設定し、企業 ID リストおよび永続的 FC ID 設定を使用して、FC ID デバイス割り当てを操作することを推奨します。

FC ID 割り当ての変更については、『*Cisco Nexus 5000 Series CLI Configuration Guide*』を参照してください。

次の例では、新しい企業 ID をデフォルト リストに追加します。

```
switch(config)# fcid-allocation area company-id 0x003223
```

企業 ID の設定の確認

Device Manager を使用して、設定された企業 ID を表示するには、**FC** > **Advanced** > **FcId Area Allocation** を選択します。特定のリリースに付属のデフォルト エントリを暗黙的に取得するには、何も指定しない場合に表示された企業 ID リストと、削除されたエントリ リストを結合します。

一部の WWN フォーマットは、企業 ID をサポートしていません。これらの場合は、FC ID の永続的エントリを設定しなければならないことがあります。

スイッチの相互運用性

相互運用性を使用すると、複数ベンダーによる製品の間で相互に作用することができます。ファイバ チャネル標準規格では、ベンダーに対して共通の外部ファイバ チャネル インターフェイスを使用することを推奨しています。

同じ方法で標準に従っていないベンダーもあるため、相互運用性モードが必要になります。ここでは、これらのモードの基本的な概念について簡単に説明します。

各ベンダーには標準モード、および同等の相互運用性モードがあります。相互運用性モードでは拡張機能または独自の機能が無効になり、標準に準拠した実装が可能になります。

ここで説明する内容は、次のとおりです。

- Interop モードの概要（p.22-10）
- interop モード 1 の設定（p.22-12）
- 相互運用性ステータスの確認（p.22-13）

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 22-2 に、相互運用性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 モードの Nexus 5000 シリーズ スイッチに固有の変更点です。

表 22-2　相互運用性がイネーブルの場合のスイッチ動作の変更点

スイッチ機能	相互運用性がイネーブルの場合の変更点
ドメイン ID	ファブリック内の 239 のドメインの一部を使用できないベンダーもあります。 ドメイン ID は 97 ～ 127 の範囲に制限されています。これは、McData の通常の制限をこの範囲に収めるためです。ドメイン ID は、スタティックまたは優先に設定できます。動作内容は次のとおりです。 • スタティック：シスコ スイッチでは 1 つのドメイン ID だけを受け入れます。スイッチがそのドメイン ID を取得できない場合には、ファブリックから隔離します。 • 優先：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 を受け入れます。
タイマー	ISL（スイッチ間リンク）を確立するときにファイバ チャネル タイマー値が E ポートで交換されるため、すべてのスイッチでこれらのタイマーをすべて同じにする必要があります。タイマーは　F_S_TOV、D_S_TOV、E_D_TOV、および R_A_TOV です。
F_S_TOV	Fabric Stability TOV タイマーが正確に一致するか確認します。
D_S_TOV	Distributed Services TOV タイマーが正確に一致するか確認します。

表 22-2　相互運用性がイネーブルの場合のスイッチ動作の変更点（続き）

スイッチ機能	相互運用性がイネーブルの場合の変更点
E_D_TOV	Error Detect TOV タイマーが正確に一致するか確認します。
R_A_TOV	Resource Allocation TOV が正確に一致するか確認します。
トランキング	2 つの異なるベンダー製のスイッチ間では、トランキングはサポートされません。この機能はポート単位、またはスイッチ単位でディセーブルに設定できます。
デフォルト ゾーン	ゾーンのデフォルトの許可動作（すべてのノードから他のすべてのノードを認識可能）または拒否動作（明示的にゾーンに配置されていないすべてのノードが隔離される）は、変更できます。
ゾーン分割属性	ゾーンを pWWN に制限したり、その他の独自のゾーン分割方式（物理ポート番号）を除去できます。 （注）Brocade スイッチでは、**cfgsave** コマンドを使用して、ファブリック全体のゾーン分割設定を保存します。このコマンドは、同じファブリックに属す Nexus 5000 シリーズ スイッチには影響しません。Nexus 5000 シリーズの各スイッチに、必ず設定を保存する必要があります。
ゾーンの伝播	ベンダーによっては、他のスイッチに完全なゾーン設定を渡さず、アクティブ ゾーンセットだけが渡されることがあります。 ファブリック内の他のスイッチにアクティブ ゾーンセットまたはゾーン設定が正しく伝播されたかどうかを確認してください。
VSAN	interop モードが適用されるのは、指定した VSAN だけです。 （注）FICON 対応 VSAN では interop モードをイネーブルにできません。
TE ポートおよび SAN ポート チャネル	シスコ スイッチを Cisco SAN 以外のスイッチに接続する場合には、TE ポートおよび SAN ポート チャネルを使用できません。Cisco SAN 以外のスイッチに接続できるのは、E ポートだけです。interop モードの場合でも、TE ポートおよび SAN ポート チャネルを使用すると、シスコ スイッチをその他の Cisco SAN スイッチに接続できます。
FSPF	interop モードにしても、ファブリック内のフレームのルーティングは変更されません。スイッチは引き続き src-id、dst-id、および ox-id を使用して、複数の ISL リンク間で負荷を分散します。
ドメインの中断再設定	これは、スイッチ全体に影響するイベントです。Brocade および McData では、ドメイン ID を変更するときにスイッチ全体をオフライン モードにしたり、再起動する必要があります。
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。Nexus 5000 シリーズ スイッチには、スイッチ全体ではなく、関連 VSAN の Domain Manager プロセスだけが再起動する機能が組み込まれています。
ネーム サーバ	すべてのベンダーのネームサーバ データベースに正しい値が格納されていることを確認してください。

interop モード 1 の設定

Nexus 5000 シリーズ スイッチでは、interop モード 1 の中断イネーブル化、または非中断イネーブル化を実行できます。

（注） Brocade スイッチから Nexus 5000 シリーズ スイッチまたは McData スイッチに接続する前に、Brocade の **msplmgmtdeactivate** コマンドを確実に実行する必要があります。このコマンドでは、Brocade 独自のフレームを使用して、Nexus 5000 シリーズ スイッチまたは McData スイッチが認識しないプラットフォーム情報を交換します。これらのフレームを拒否すると、一般的な E ポートが隔離されます。

Fabric Manager を使用して VSAN に interop モード 1 を設定する手順は、次のとおりです。

ステップ 1　Logical Domains ペインで **VSAN*xxx* > VSAN Attributes** を選択します。

ステップ 2　Interop ドロップダウン リストで **Interop-1** を選択します。

ステップ 3　**Apply Changes** をクリックして、この interop モードを保存します。

ステップ 4　Logical Domains ペインで **VSAN*xxx*** を展開し、**Domain Manager** を選択します。

Information ペインに Domain Manager の設定が表示されます（図 22-5 を参照）。

図 22-5　Domain Manager の設定

ステップ 5　ドメイン ID を、97（0x61）～ 127（0x7F）の範囲で設定します。

a. **Configuration** タブをクリックします。

b. Configuration タブの Config Domain ID 列をクリックします。

c. **Running** タブをクリックして、変更されたことを確認します。

（注） ドメイン ID 範囲の制限は、McData スイッチに対応します。

（注） ドメイン ID を変更すると、N ポートに割り当てられた FC ID も変更されます。

ステップ 6　ファイバ チャネル タイマーを変更します（システムのデフォルト値以外の場合）。

（注） Cisco、Brocade、McData FC Error Detect（ED_TOV）、および Resource Allocation（RA_TOV）のタイマーは、同じ値にデフォルト設定されています。これらの値は、必要に応じて変更できます。RA_TOV のデフォルト値は 10 秒、ED_TOV のデフォルト値は 2 秒です。FC-SW2 標準に基づく場合、これらの値は、ファブリック内の各スイッチで一致している必要があります。

a. **Switches** > **FC Services** を展開し、**Timers and Policies** を選択します。

Information ペインにタイマーの設定が表示されます。

b. **Change Timeouts** をクリックして、タイムアウト値を変更します。

c. **Apply** をクリックして、新しいタイムアウト値を保存します。

ステップ 7　（任意）**VSAN***xxx* > **Domain Manager** を選択し、**Configuration** タブをクリックし、Restart ドロップダウン リストで **disruptive** または **nonDisruptive** を選択して、ドメインを再起動します。

相互運用性ステータスの確認

ここでは、ファブリックが起動していて、相互運用性モードで稼働しているかを確認する場合に使用する手順について説明します。

Fabric Manager を使用して Cisco Nexus 5000 シリーズ スイッチの相互運用性ステータスを確認する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで **Switches** を選択し、Information ペインでリリース番号を調べて、Cisco SAN-OS リリースを確認します。

ステップ 2　Physical Attributes ペインで、**Switches** > **Interfaces** を展開し、**FC Physical** を選択して、各スイッチのインターフェイス モードを確認します。

ステップ 3　Logical Domains ペインで **Fabric***xx* を展開し、**All VSANs** を選択して、すべての VSAN の interop モードを確認します。

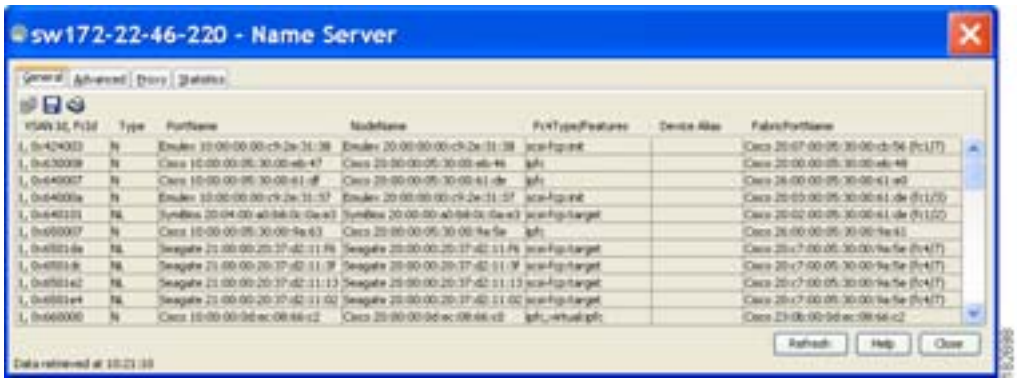
ステップ 4　**Fabric***xx* > **All VSANs** を展開し、**Domain Manager** を選択して、すべての VSAN のドメイン ID、ローカル、および主要 sWWN を確認します（図 22-6 を参照）。

図 22-6　Domain Manager の情報

ステップ 5　Device Manager を使用して、**FC > Name Server** を選択し、ネーム サーバ情報を確認します。

Name Server ダイアログボックスが表示されます（図 22-7 を参照）。

図 22-7　Name Server ダイアログボックス



ステップ 6　**Close** をクリックして、ダイアログボックスを閉じます。

（注）　シスコ スイッチ ネーム サーバには、ローカル エントリとリモート エントリが両方表示され、エントリはタイムアウトしません。

デフォルト設定

表 22-3 に、この章で説明した機能のデフォルト設定値を示します。

表 22-3　拡張機能のデフォルト設定値

パラメータ	デフォルト
CIM サーバ	ディセーブル
CIM サーバ セキュリティ プロトコル	HTTP
D_S_TOV	5,000 ミリ秒
E_D_TOV	2,000 ミリ秒
R_A_TOV	10,000 ミリ秒
fctrace を起動するためのタイムアウト期間	5 秒
fcping 機能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 フレーム制限	10 フレーム
FC ID の割り当てモード	auto モード
ループ モニタリング	ディセーブル
interop モード	ディセーブル

CHAPTER 23

FC-SP および DHCHAP の設定

Fibre Channel Security Protocol（FC-SP）機能は、スイッチ間およびホストとスイッチ間で認証を実行して、企業全体のファブリックに関するセキュリティ問題を解決します。Diffie-Hellman（DH）Challenge Handshake Authentication Protocol（DHCHAP）は、Nexus 5000 シリーズ スイッチとその他のデバイス間で認証を行う FC-SP プロトコルです。DHCHAP は、CHAP プロトコルと DH 交換を組み合わせたものです。

この章の内容は、次のとおりです。

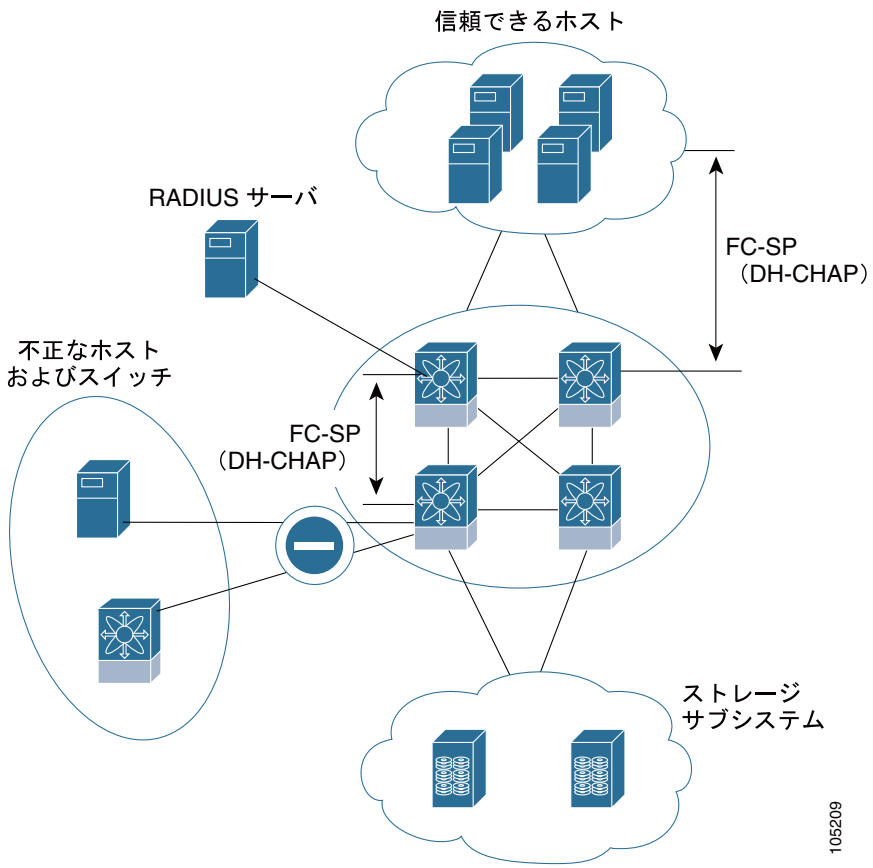
- ファブリック認証の概要（p.23-2）
- DHCHAP（p.23-3）
- デフォルト設定（p.23-11）

ファブリック認証の概要

Nexus 5000 シリーズのスイッチはすべて、スイッチ間またはスイッチとホスト間の認証をファブリック全体で実行できます。これらのスイッチおよびホスト認証は、各ファブリックでローカルに実行することも、リモートで実行することもできます。ストレージ アイランドを企業全体のファブリックに統合して、移行すると、新しいセキュリティ問題が発生します。ストレージ アイランドを保護する方法が、企業全体のファブリックで必ずしも保証されなくなります。たとえば、スイッチが地理的に分散しているキャンパス環境では、他のユーザが故意に、またはユーザ自身が偶然に、互換性のないスイッチに故意に相互接続することにより、ISL（スイッチ間リンク）分離やリンク切断が発生することがあります。

Nexus 5000 シリーズ スイッチでは、認証機能をサポートして物理セキュリティに対応しています（図 23-1 を参照）。

図 23-1　スイッチおよびホストの認証



DHCHAP

DHCHAP は、スイッチに接続されたデバイスを認証する認証プロトコルです。ファイバ チャネル認証を使用すると、信頼できるデバイスだけをファブリックに追加できるので、不正なデバイスのスイッチへのアクセスを防止できます。

（注） この章では、FC-SP および DHCHAP という用語を同じ意味で使用しています。

DHCHAP は、スイッチ間およびホストとスイッチ間の認証をサポートする、必須パスワード ベース鍵交換認証プロトコルです。DHCHAP は、ハッシュ アルゴリズムおよび DH グループとネゴシエートしてから、認証を実行します。また、Message Digest 5（MD5）および Secure Hash Algorithm（SHA-1）アルゴリズムベース認証をサポートします。

ローカル パスワード データベースを使用して DHCHAP 認証を設定する手順は、次のとおりです。

ステップ 1　DHCHAP をイネーブルにします。

ステップ 2　DHCHAP 認証モードを識別して設定します。

ステップ 3　ハッシュ アルゴリズムおよび DH グループを設定します。

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

ステップ 5　再認証用の DHCHAP タイムアウト値を設定します。

ステップ 6　DHCHAP 設定を確認します。

ここで説明する内容は、次のとおりです。

- ファイバ チャネル機能との DHCHAP の互換性（p.23-4）
- DHCHAP イネーブル化の概要（p.23-4）
- DHCHAP のイネーブル化（p.23-4）
- DHCHAP 認証モードの概要（p.23-5）
- DHCHAP モードの設定（p.23-6）
- DHCHAP ハッシュ アルゴリズムの概要（p.23-6）
- DHCHAP ハッシュ アルゴリズムの設定（p.23-7）
- DHCHAP グループ設定の概要（p.23-7）
- DHCHAP グループの設定（p.23-7）
- DHCHAP パスワードの概要（p.23-8）
- ローカル スイッチの DHCHAP パスワードの設定（p.23-8）
- リモート デバイスのパスワード設定の概要（p.23-9）
- リモート デバイスの DHCHAP パスワードの設定（p.23-9）
- DHCHAP タイムアウト値の概要（p.23-9）
- DHCHAP タイムアウト値の設定（p.23-10）
- DHCHAP AAA 認証の設定（p.23-10）
- ISL 上での FC-SP のイネーブル化（p.23-10）

ファイバ チャネル機能との DHCHAP の互換性

ここでは、DHCHAP 機能および既存の Cisco NX-OS 機能の設定の影響について説明します。

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

DHCHAP イネーブル化の概要

デフォルトでは、DHCHAP 機能はすべての Nexus 5000 シリーズ スイッチでディセーブルです。

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

DHCHAP のイネーブル化

Fabric Manager を使用して Cisco MDS スイッチの DHCHAP をイネーブルにする手順は、次のとおりです。

ステップ 1　**Switches** を展開し、**Security** を展開して、**FC-SP** を選択します。

Information ペインに FC-SP（DHCHAP）の設定が表示されます（図 23-2 を参照）。

図 23-2　FC-SP の設定

デフォルトは、**Control** タブです。ファブリック内の全スイッチの FC-SP イネーブル ステートが表示されます。

ステップ 2　Command ドロップダウン リストで、FC-SP をイネーブルするすべてのスイッチについて、**enable** を選択します。

ステップ 3　**Apply Changes** アイコンをクリックし、選択したスイッチ上で FC-SP および DHCHAP をイネーブルにします。

DHCHAP 認証モードの概要

各インターフェイスの DHCHAP 認証ステータスは、設定された DHCHAP ポート モードによって異なります。

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

- on ― 接続元デバイスが DHCHAP 認証をサポートしている場合、スイッチ初期化中に認証シーケンスが実行されます。接続元デバイスが DHCHAP 認証をサポートしていない場合には、リンクが分離状態になります。
- auto-active ― 接続元デバイスが DHCHAP 認証をサポートしている場合、スイッチ初期化中に認証シーケンスが実行されます。接続元デバイスが DHCHAP 認証をサポートしていない場合には、認証シーケンスの残りが継続されます。
- auto-passive（デフォルト）― スイッチは DHCHAP 認証を開始しませんが、接続元デバイスが DHCHAP 認証を開始した場合には、DHCHAP 認証に参加します。
- off ― スイッチは DHCHAP 認証をサポートしません。このモードのポートに認証メッセージが送信された場合、開始元スイッチにエラー メッセージが戻されます。

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

表 23-1 に、さまざまなモードに設定した 2 台のシスコ スイッチ間での認証について説明します。

表 23-1　2 台の MDS スイッチ間の DHCHAP 認証ステータス

<table>
<tr><th rowspan="2">スイッチ N
DHCHAP モード</th><th colspan="4">スイッチ 1 DHCHAP モード</th></tr>
<tr><th>on</th><th>auto-active</th><th>auto-passive</th><th>off</th></tr>
<tr><td>on</td><td rowspan="3">FC-SP 認証が実行されます。</td><td rowspan="3">FC-SP 認証が実行されます。</td><td>FC-SP 認証が実行されます。</td><td>リンクがダウンになります。</td></tr>
<tr><td>auto-active</td><td rowspan="2"></td><td rowspan="2">FC-SP 認証は実行されません。</td></tr>
<tr><td>auto-passive</td><td>FC-SP 認証は実行されません。</td></tr>
<tr><td>off</td><td>リンクがダウンになります。</td><td colspan="3">FC-SP 認証は実行されません。</td></tr>
</table>

DHCHAP モードの設定

Fabric Manager を使用して特定のインターフェイスに DHCHAP モードを設定する手順は、次のとおりです。

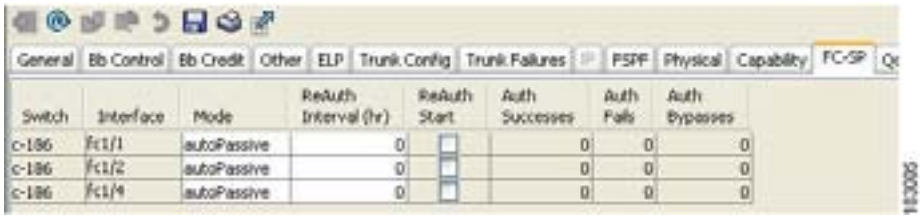
ステップ 1　Physical Attributes ペインで、**Switches**> **Interfaces** を展開して、**FC Physical** を選択します。

Information ペインにインターフェイス設定が表示されます。

ステップ 2　FC-SP タブを選択します。

Information ペインに FC-SP（DHCHAP）の設定が表示されます（図 23-3 を参照）。

図 23-3　FC-SP（DHCHAP）インターフェイス モード



ステップ 3　**Mode** ドロップダウン リストで、FC-SP をサポートする各インターフェイスについて、**DHCP authentication mode** を選択します。

ステップ 4　**Apply Changes** アイコンをクリックして、DHCHAP ポート モードの設定を保存します。

DHCHAP ハッシュ アルゴリズムの概要

Cisco SAN スイッチは、DHCHAP 認証用のデフォルト ハッシュ アルゴリズム プライオリティ リスト（MD5 のあとに SHA-1）をサポートしています。

ヒント　ハッシュ アルゴリズムの設定を変更する場合には、ファブリック内のすべてのスイッチに対してグローバルに変更します。

注意　Remote Access Dial-In User Service（RADIUS）および Terminal Access Controller Access Control System Plus（TACACS+）プロトコルは CHAP 認証に必ず MD5 を使用します。ハッシュ アルゴリズムとして SHA-1 を使用すると、これらの Authentication, Authorization, Accounting（AAA; 認証、認可、アカウンティング）プロトコルが DHCHAP 認証に対してイネーブルに設定されていても、RADIUS および TACACS+ を使用できないことがあります。

DHCHAP ハッシュ アルゴリズムの設定

Fabric Manager を使用してハッシュ アルゴリズムを設定する手順は、次のとおりです。

ステップ 1　**Switches** > **Security** を選択し、**FC-SP** を選択します。

ステップ 2　**General/Password** タブを選択します。

各スイッチの DHCHAP 一般設定モードが表示されます（図 23-4 を参照）。

図 23-4　General/Password タブ

ステップ 3　ファブリック内の各スイッチの DHCHAP HashList を変更します。

ステップ 4　**Apply Changes** アイコンをクリックして、更新したハッシュ アルゴリズム プライオリティ リストを保存します。

DHCHAP グループ設定の概要

すべての Nexus 5000 シリーズ スイッチは、標準で指定されたすべての DHCHAP グループをサポートします。これらのグループは、0（DH 交換を実行しないヌル DH グループ）、1、2、3、または 4 です。

ヒント　DH グループの設定を変更する場合には、ファブリック内の全スイッチに対してグローバルに変更してください。

DHCHAP グループの設定

Fabric Manager を使用して DH グループ設定を変更する手順は、次のとおりです。

ステップ 1　**Switches** > **Security** を展開し、**FC-SP** を選択します。

ステップ 2　**General/Password** タブを選択します。

ステップ 3　ファブリック内の各スイッチの DHCHAP GroupList を変更します。

ステップ 4　**Apply Changes** アイコンをクリックして、更新したハッシュ アルゴリズム プライオリティ リストを保存します。

DHCHAP パスワードの概要

DHCHAP 認証を方向ごとに実行するには、接続されたデバイス間の共有シークレット パスワードが必要です。このパスワードを使用するには、DHCHAP に参加するファブリック内のすべてのスイッチで、次の 3 つの設定のいずれかを使用してパスワードを管理します。

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

（注） すべてのパスワードは 64 個の英数字に制限され、変更可能ですが、削除はできません。

ヒント 6 台以上のスイッチを含むファブリックでは、RADIUS または TACACS+ の使用を推奨します。ローカル パスワード データベースを使用する必要がある場合には、設定 3 を使用し、Cisco MDS 9000 ファミリ Fabric Manager を使用して、パスワード データベースを管理します。

ローカル スイッチの DHCHAP パスワードの設定

Fabric Manager を使用してローカル スイッチに DHCHAP パスワードを設定する手順は、次のとおりです。

ステップ 1　**Switches > Security** を展開し、**FC-SP** を選択します。

Information ペインに、FC-SP の設定が表示されます。

ステップ 2　**Local Passwords** タブを選択します。

ステップ 3　**Create Row** アイコンをクリックして、新しいローカル パスワードを作成します。

Create Local Passwords ダイアログボックスが表示されます。

ステップ 4　（任意）同じローカル パスワードを設定するスイッチをチェックします。

ステップ 5　スイッチの WNN を選択し、Password フィールドにパスワードを入力します。

ステップ 6　**Create** をクリックして、更新したパスワードを保存します。

リモート デバイスのパスワード設定の概要

ファブリック内の他のデバイスのパスワードを、ローカル認証データベースに設定できます。他のデバイスは、スイッチ WWN またはデバイス WWN と呼ばれるデバイス名によって識別されます。パスワードは 64 文字に制限され、クリア テキスト（0）または暗号化テキスト（7）で指定できます。

（注） スイッチ WWN は物理スイッチを識別します。スイッチ WWN はスイッチを認証する場合に使用され、VSAN ノードの WWN とは異なります。

リモート デバイスの DHCHAP パスワードの設定

Fabric Manager を使用して、ファブリック内の別のスイッチのリモート DHCHAP パスワードをローカルで設定する手順は、次のとおりです。

ステップ 1　ISL を右クリックし、ドロップダウン リストから **Enable FC-SP** を選択します。

Enable FC-SP ダイアログボックスが表示されます（図 23-5 を参照）。

図 23-5　Enable FC-SP ダイアログボックス

ステップ 2　**Apply** をクリックして、更新したパスワードを保存します。

DHCHAP タイムアウト値の概要

DHCHAP プロトコルの交換中に、Nexus 5000 シリーズ スイッチが待機中の DHCHAP メッセージを指定インターバル内に受信しなかった場合、認証は失敗したとみなされます。このインターバルは 20（認証が実行されない）～ 1000 秒です。デフォルトは 30 秒です。

タイムアウト値を変更する場合には、次の要因について考慮してください。

- 既存の RADIUS および TACACS+ タイムアウト値。
- ファブリック内の全スイッチに同じ値を設定する必要があります。

DHCHAP タイムアウト値の設定

Fabric Manager を使用して DHCHAP タイムアウト値を設定する手順は、次のとおりです。

ステップ 1　**Switches** > **Security** を展開し、**FC-SP** を選択します。

Information ペインに、FC-SP の設定が表示されます。

ステップ 2　**General/Password** タブを選択します。

各スイッチの DHCHAP 一般設定モードが表示されます（図 23-6 を参照）。

図 23-6　General/Password タブ

ステップ 3　ファブリック内の各スイッチの DHCHAP タイムアウト値を変更します。

ステップ 4　**Apply Changes** アイコンをクリックして、更新した情報を保存します。

DHCHAP AAA 認証の設定

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

AAA 認証を設定するには、『*Cisco Nexus 5000 Series CLI Configuration Guide*』を参照してください。

ISL 上での FC-SP のイネーブル化

Fabric Manager には、ISL のどちらかの側のスイッチ上で FC-SP をイネーブルにする、Enable FC-SP と呼ばれる ISL ポップアップ メニューがあります。FC-SP 一般パスワードを入力し、関連ポートの FC-SP インターフェイス モードを ON に設定します。この機能を設定するには、ISL を右クリックして、**Enable FC-SP** をクリックします。

デフォルト設定

表 23-2 に、スイッチのすべてのファブリック セキュリティ機能のデフォルト設定を示します。

表 23-2　ファブリック セキュリティのデフォルト設定

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

CHAPTER 24

ポート セキュリティの設定

Nexus 5000 シリーズ スイッチは、侵入に関する試みを拒否し、管理者にこれらの侵入を報告するポート セキュリティを提供します。

(注) ポート セキュリティは、仮想ファイバ チャネル ポートおよび物理ファイバ チャネル ポートでサポートされています。

この章の内容は、次のとおりです。

- ポート セキュリティの概要（p.24-2）
- ポート セキュリティの設定（p.24-4）
- ポート セキュリティのイネーブル化（p.24-7）
- ポート セキュリティのアクティブ化（p.24-9）
- 自動学習（p.24-13）
- ポート セキュリティの手動設定（p.24-17）
- ポート セキュリティ設定の配信（p.24-20）
- データベース マージの注意事項（p.24-22）
- データベースの相互作用（p.24-23）
- デフォルト設定（p.24-26）

ポート セキュリティの概要

通常、SAN 内のすべてのファイバ チャネル デバイスを任意の SAN スイッチ ポートに接続して、ゾーン メンバシップに基づいて SAN サービスにアクセスできます。ポート セキュリティ機能は、次の方式を使用して Nexus 5000 シリーズ スイッチのスイッチ ポートへの不正アクセスを防止します。

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

ここで説明する内容は、次のとおりです。

- ポート セキュリティの実行（p.24-2）
- 自動学習の概要（p.24-3）
- ポート セキュリティのアクティブ化（p.24-3）

ポート セキュリティの実行

ポート セキュリティを実行するには、デバイスまたはスイッチに、それぞれを接続するポート インターフェイスを設定し、設定をアクティブにします。

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

N ポートおよび xE ポートをそれぞれ設定して、単一ポートまたはポート範囲に限定することができます。

ポート セキュリティ ポリシーは、ポートがアクティブになるごとに、およびポートの起動時に適用されます。

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

- コンフィギュレーション データベース — 設定の変更はすべて、コンフィギュレーション データベースに保存されます。
- アクティブ データベース — ファブリックで現在実行されているデータベースです。ポート セキュリティ機能を実行するには、スイッチに接続しているすべてのデバイスを、ポート セキュリティ アクティブ データベースに登録する必要があります。ソフトウェアはこのアクティブ データベースを使用して、認証を行います。

自動学習の概要

指定した期間にわたって、スイッチがポート セキュリティ設定を自動学習（auto-learn）するように設定できます。この機能を使用すると、任意の Nexus 5000 シリーズ スイッチで、接続先のデバイスおよびスイッチについて自動的に学習できます。ポート セキュリティ機能を最初にアクティブにするときに、この機能を使用すると、各ポートを手動で設定する面倒な作業が軽減されます。自動学習は、VSAN 単位で設定する必要があります。この機能をイネーブルにすると、ポート アクセスを設定していない場合でも、スイッチに接続可能なデバイスおよびスイッチが自動学習されます。

自動学習をイネーブルにすると、スイッチにログインしていないデバイスまたはインターフェイスに関する学習だけが実行されます。自動学習がイネーブルのときにポートをシャットダウンすると、そのポート上で学習されたエントリは消去されます。

学習によって、設定済みのポート セキュリティ ポリシーが上書きされることはありません。たとえば、インターフェイスが特定の pWWN を許可するように設定されている場合、自動学習によって、そのインターフェイスに他の pWWN を許可する新しいエントリが追加されることはありません。自動学習モードであっても、他のすべての pWWN はブロックされます。

シャットダウン状態のポートについては、エントリは学習されません。

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

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

ポート セキュリティのアクティブ化

デフォルトでは、Nexus 5000 シリーズ スイッチでポート セキュリティ機能は非アクティブです。

ポート セキュリティ機能をアクティブにすると、次の処理が行われます。

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

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

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

ヒント ログインが拒否されてシャットダウンしたポートは、以降でログインが許可されるようにデータベースを設定しても、自動的には起動しません。そのポートをオンラインに戻すには、**no shutdown** CLI コマンドを明示的に入力する必要があります。

ポート セキュリティの設定

ポート セキュリティを設定する手順は、使用する機能によって異なります。CFS 配信を使用している場合には、自動学習の動作が異なります。

ここで説明する内容は、次のとおりです。

- 自動学習と CFS 配信を使用するポート セキュリティの設定（p.24-4）
- 自動学習を使用し、CFS 配信を使用しないポート セキュリティの設定（p.24-5）
- 手動データベース設定によるポート セキュリティの設定（p.24-6）

自動学習と CFS 配信を使用するポート セキュリティの設定

自動学習および CFS 配信を使用してポート セキュリティを設定する手順は、次のとおりです。

ステップ 1　ポート セキュリティをイネーブルにします。

「ポート セキュリティのイネーブル化」（p.24-7）を参照してください。

ステップ 2　CFS 配信をイネーブルにします。

「配信のイネーブル化」（p.24-20）を参照してください。

ステップ 3　各 VSAN でポート セキュリティをアクティブにします。

この操作によって、デフォルトで自動学習が有効になります。「ポート セキュリティのアクティブ化」（p.24-9）を参照してください。

ステップ 4　CFS 確定を発行して、この設定をファブリック内のすべてのスイッチにコピーします。

「変更のコミット」（p.24-21）を参照してください。すべてのスイッチでポート セキュリティがアクティブになり、自動学習が有効になります。

ステップ 5　すべてのスイッチおよびホストが自動学習されるまで待機します。

ステップ 6　各 VSAN で自動学習をディセーブルにします。

「自動学習のディセーブル化」（p.24-14）を参照してください。

ステップ 7　CFS 確定を発行して、この設定をファブリック内のすべてのスイッチにコピーします。

「変更のコミット」（p.24-21）を参照してください。すべてのスイッチから自動学習されたエントリが、すべてのスイッチに配信されるスタティックなアクティブ データベースに組み込まれます。

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

「ポート セキュリティ データベースのコピー」（p.24-24）を参照してください。

ステップ 9　CFS 確定を発行して、この設定をファブリック内のすべてのスイッチにコピーします。

「変更のコミット」（p.24-21）を参照してください。これにより、ファブリック内のすべてのスイッチで、コンフィギュレーション データベースが同一になります。

ステップ 10　ファブリック オプションを使用して、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

このステップにより、ポート セキュリティ コンフィギュレーション データベースが、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。

自動学習を使用し、CFS 配信を使用しないポート セキュリティの設定

自動学習を使用し、CFS 配信を使用しないポート セキュリティを設定する手順は、次のとおりです。

ステップ 1　ポート セキュリティをイネーブルにします。

「ポート セキュリティのイネーブル化」（p.24-7）を参照してください。

ステップ 2　各 VSAN のポート セキュリティをアクティブにし、デフォルトで自動学習を有効にします。

「ポート セキュリティのアクティブ化」（p.24-9）を参照してください。

ステップ 3　すべてのスイッチおよびホストが自動学習されるまで待機します。

ステップ 4　各 VSAN で自動学習をディセーブルにします。

「自動学習のディセーブル化」（p.24-14）を参照してください。

ステップ 5　アクティブ データベースを、各 VSAN のコンフィギュレーション データベースにコピーします。

「ポート セキュリティ データベースのコピー」（p.24-24）を参照してください。

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

ステップ 7　ファブリック内のすべてのスイッチについて、ステップ 1 ～ 6 を繰り返します。

手動データベース設定によるポート セキュリティの設定

ポート セキュリティを設定し、ポート セキュリティ データベースを手動設定する手順は、次のとおりです。

ステップ 1　ポート セキュリティをイネーブルにします。

「ポート セキュリティのイネーブル化」（p.24-7）を参照してください。

ステップ 2　各 VSAN のコンフィギュレーション データベースに、すべてのポート セキュリティ エントリを手動で設定します。

「手動データベース設定によるポート セキュリティの設定」（p.24-6）を参照してください。

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

「自動学習のディセーブル化」（p.24-14）を参照してください。

ステップ 4　各 VSAN で自動学習をディセーブルにします。

「自動学習のディセーブル化」（p.24-14）を参照してください。

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

ステップ 6　ファブリック内のすべてのスイッチについて、ステップ 1 ～ 5 を繰り返します。

ポート セキュリティのイネーブル化

デフォルトでは、Nexus 5000 シリーズ スイッチでポート セキュリティ機能はディセーブルです。

Fabric Manager を使用してポート セキュリティ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** を展開し、Logical Domains ペインで **Port Security** を選択します。

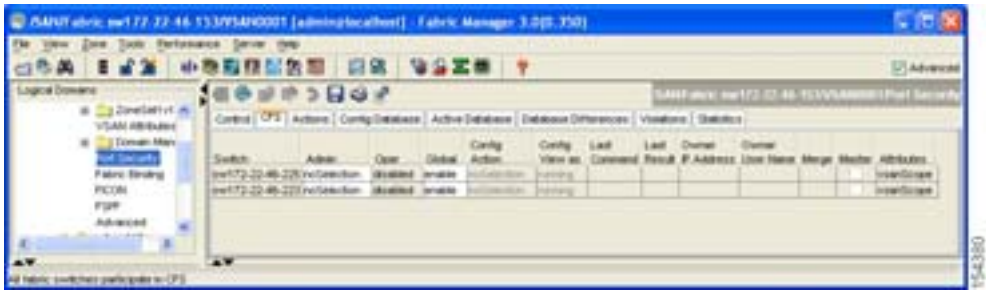
Information ペインに、その VSAN のポート セキュリティ設定が表示されます（図 24-1 を参照）。

図 24-1　ポート セキュリティ設定

ステップ 2　**CFS** タブをクリックします。

図 24-2 のような情報が表示されます。

図 24-2　ポート セキュリティ CFS



ステップ 3　Global カラムの各エントリをクリックし、**enable** を選択して、VSAN 内のすべての参加スイッチ上の CFS をイネーブルにします。

ステップ 4　**Apply Changes** をクリックし、ポート セキュリティ機能の CFS 配布をイネーブルにします。

ステップ 5　**Control** タブをクリックします。

選択した VSAN 内の全スイッチのポート セキュリティ イネーブル ステートが表示されます（図 24-3 を参照）。

図 24-3　ポート セキュリティ設定

ステップ 6　VSAN 内の各スイッチについて、Status カラムで **enable** を選択します。

ステップ 7　**CFS** タブをクリックし、VSAN 内のすべての参加スイッチについて、Command カラムで **commit** を選択します。

ステップ 8　**Apply Changes** をクリックして、VSAN 内の全スイッチに、イネーブルにしたポート セキュリティを配信します。

ポート セキュリティのアクティブ化

ここで説明する内容は、次のとおりです。

- ポート セキュリティのアクティブ化（p.24-9）
- データベースのアクティブ化の拒否（p.24-10）
- ポート セキュリティの強制的なアクティブ化（p.24-10）
- データベースの再アクティブ化（p.24-11）
- コンフィギュレーション データベースへのアクティブ データベースのコピー（p.24-11）
- アクティブなポート セキュリティ設定の表示（p.24-12）
- ポート セキュリティ統計情報の表示（p.24-12）
- ポート セキュリティ違反の表示（p.24-12）

ポート セキュリティのアクティブ化

Fabric Manager を使用してポート セキュリティをアクティブにする手順は、次のとおりです。

ステップ 1　**VSAN** を展開し、Logical Domains ペインで **Port Security** を選択します。

Information ペインに、その VSAN のポート セキュリティ設定が表示されます。

ステップ 2　**Actions** タブをクリックします。

ステップ 3　Activation の下の Action カラムで、ポート セキュリティをアクティブにするスイッチまたは VSAN を選択します。ドロップダウン リストに、次のオプションが表示されます。

- **activate** — 有効なポート セキュリティ設定をアクティブにします。
- **activate（TurnLearningOff）** — 有効なポート セキュリティ設定をアクティブにし、自動学習をオフにします。
- **forceActivate** — 強制的にアクティブにします。
- **forceActivate（TurnLearningOff）** — 強制的にアクティブにし、自動学習をオフにします。
- **deactivate** — 現在アクティブであるすべてのポート セキュリティ設定を非アクティブにします。
- **NoSelection** — 何も実行しません。

ステップ 4　スイッチに適用する Action フィールドを設定します。

ステップ 5　自動学習をディセーブルにするには、VSAN の各スイッチの **AutoLearn** チェックボックスをオフにします。

ステップ 6　**CFS** タブをクリックし、VSAN 内のすべての参加スイッチについて、Command カラムを **commit** に設定します。

ステップ 7　Fabric Manager の **Apply Changes** をクリックして、変更を保存します。

データベースのアクティブ化の拒否

次の場合は、データベースをアクティブ化しようとしても、拒否されます。

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

上記のような矛盾が 1 つまたは複数発生し、データベースのアクティブ化が拒否された場合でも、ポート セキュリティを強制的にアクティブ化すれば、処理を続行できます。

ポート セキュリティの強制的なアクティブ化

ポート セキュリティのアクティブ化要求が拒否された場合、アクティブ化を強制的に実行できます。

（注） アクティブ化を強制すると、アクティブ データベースに違反している既存のデバイスがログアウトします。

Fabric Manager を使用してポート セキュリティ データベースを強制的にアクティブ化する手順は、次のとおりです。

ステップ 1　**VSAN** を展開し、Logical Domains ペインで **Port Security** を選択します。

Information ペインに、その VSAN のポート セキュリティ設定が表示されます。

ステップ 2　**Actions** タブをクリックします。

ステップ 3　Activation の下の **Action** カラムで、ポート セキュリティをアクティブにするスイッチまたは VSAN を選択し、**forceactivate** オプションを選択します。

ステップ 4　スイッチに適用する Action フィールドを選択します。

ステップ 5　**CFS** タブをクリックし、VSAN 内のすべての参加スイッチについて、Command カラムで **commit** を選択します。

ステップ 6　Fabric Manager の **Apply Changes** をクリックして、変更を保存します。

データベースの再アクティブ化

ヒント　自動学習がイネーブルで、データベースをアクティブ化できない場合、処理を継続できません。

Fabric Manager を使用してポート セキュリティ データベースを再アクティブ化する手順は、次のとおりです。

ステップ 1　自動学習をディセーブルにします。

ステップ 2　コンフィギュレーション データベースにアクティブ データベースをコピーします。

ヒント　アクティブ データベースが空の場合には、この手順を実行できません。

ステップ 3　必要に応じて、コンフィギュレーション データベースを変更します。

ステップ 4　データベースをアクティブにします。

コンフィギュレーション データベースへのアクティブ データベースのコピー

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

ステップ 1　**VSAN** を展開し、Logical Domains ペインで **Port Security** を選択します。

Information ペインに、その VSAN のポート セキュリティ設定が表示されます。

ステップ 2　**Actions** タブをクリックします。

その VSAN のスイッチが表示されます。

ステップ 3　データベースをコピーするスイッチの横にある、**CopyActive ToConfig** チェックボックスをオンにします。

セキュリティ設定がアクティブになると、アクティブ データベースがコンフィギュレーション データベースにコピーされます。

ステップ 4　セキュリティ設定をアクティブにしたときにデータベースをコピーしない場合には、**CopyActive ToConfig** チェックボックスをオフにします。

ステップ 5　**CFS** タブをクリックし、VSAN 内のすべての参加スイッチについて、Command カラムで **commit** を選択します。

ステップ 6　これらの変更を保存する場合は **Apply Changes** をクリックします。保存されていない変更を廃棄する場合は **Undo Changes** を クリックします。

アクティブなポート セキュリティ設定の表示

Fabric Manager を使用してアクティブなポート セキュリティ設定を表示する手順は、次のとおりです。

ステップ 1　**VSAN** を展開し、Logical Domains ペインで **Port Security** を選択します。

Information ペインに、その VSAN のポート セキュリティ設定が表示されます。

ステップ 2　**Active Database** タブをクリックします。

その VSAN のアクティブなポート セキュリティ設定が表示されます。

ポート セキュリティ統計情報の表示

Fabric Manager を使用してポート セキュリティ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** を展開し、Logical Domains ペインで **Port Security** を選択します。

Information ペインに、その VSAN のポート セキュリティ設定が表示されます。

ステップ 2　**Statistics** タブをクリックします。

その VSAN のポート セキュリティ統計情報が表示されます。

ポート セキュリティ違反の表示

ポート違反とは、不正なログイン試行のことです（たとえば、不正なファイバ チャネル デバイスからログイン要求があった場合）。Fabric Manager を使用すると、これらの試行に関するリストを VSAN 単位で表示できます。

ポート セキュリティ違反を表示する手順は、次のとおりです。

ステップ 1　**VSAN** を展開し、Logical Domains ペインで **Port Security** を選択します。

Information ペインに、その VSAN のポート セキュリティ設定が表示されます。

ステップ 2　**Violations** タブをクリックします。

その VSAN のポート セキュリティ違反が表示されます。

自動学習

ここで説明する内容は、次のとおりです。

- 自動学習のイネーブル化の概要（p.24-13）
- 自動学習のイネーブル化（p.24-13）
- 自動学習のディセーブル化（p.24-14）
- 自動学習デバイスの許可（p.24-15）
- 許可の例（p.24-15）

自動学習のイネーブル化の概要

自動学習の設定の状態は、ポート セキュリティ機能の状態によって異なります。

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

ヒント　VSAN 上の自動学習がイネーブルである場合、**force** オプションを使用しないと、その VSAN のデータベースをアクティブ化できません。

自動学習のイネーブル化

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

ステップ 1　**VSAN** を展開し、Logical Domains ペインで **Port Security** を選択します。

Information ペインに、その VSAN のポート セキュリティ設定が表示されます（図 24-4 を参照）。

図 24-4　ポート セキュリティ設定

ステップ 2　**Actions** タブをクリックします。

ステップ 3　Activation の下の Action カラムで、ポート セキュリティをアクティブにするスイッチまたは VSAN を選択します。ドロップダウン リストに、次のオプションが表示されます。

- **activate** — 有効なポート セキュリティ設定をアクティブにします。
- **activate（TurnLearningOff）** — 有効なポート セキュリティ設定をアクティブにし、自動学習をオフにします。
- **forceActivate** — 強制的にアクティブにします。
- **forceActivate（TurnLearningOff）** — 強制的にアクティブにし、自動学習をオフにします。
- **deactivate** — 現在アクティブであるすべてのポート セキュリティ設定を非アクティブにします。
- **NoSelection** — 何も実行しません。

ステップ 4　そのスイッチに適用する、いずれかのポート セキュリティ オプションを選択します。

ステップ 5　自動学習をイネーブルにするには、VSAN の各スイッチの **AutoLearn** チェックボックスをオンにします。

ステップ 6　**Apply Changes** アイコンをクリックして、これらの変更を保存します。

自動学習のディセーブル化

Fabric Manager を使用して自動学習をディセーブルにする手順は、次のとおりです。

ステップ 1　**VSAN** を展開し、Logical Domains ペインで **Port Security** を選択します。

Information ペインに、その VSAN のポート セキュリティ設定が表示されます（図 24-4 を参照）。

ステップ 2　**Actions** タブをクリックします。

その VSAN のスイッチが表示されます。

ステップ 3　自動学習をディセーブルにするには、スイッチの横にある **AutoLearn** チェックボックスをオフにします。

ステップ 4　**Apply Changes** アイコンをクリックして、これらの変更を保存します。

自動学習デバイスの許可

表 24-1 に、デバイス要求に対して接続が許可される条件を示します。

表 24-1　許可される自動学習デバイス要求

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

許可の例

ポート セキュリティ機能がアクティブで、アクティブ データベースに次の条件が指定されているものとします。

- pWWN（P1）には、インターフェイス fc2/1（F1）からアクセスできる
- pWWN（P2）には、インターフェイス fc2/2（F1）からアクセスできる
- nWWN（N1）には、インターフェイス fc2/2（F2）からアクセスできる
- インターフェイス vfc3/1（F3）からは、任意の WWN にアクセスできる
- nWWN（N3）には、任意のインターフェイスからアクセスできる
- pWWN（P3）には、インターフェイス fc2/4（F4）からアクセスできる
- sWWN（S1）には、インターフェイス fc3/1 ～ 3（F10 ～ F13）からアクセスできる
- pWWN（P10）には、インターフェイス vfc4/1（F11）からアクセスできる

表 24-2 に、このアクティブ データベースに対するポート セキュリティ許可の結果を示します。ここに示す条件は、表 24-1 の条件に基づいています。

表 24-2　各シナリオの許可結果

デバイス接続要求	許可	条件	理由
P1、N2、F1	許可	1	競合しません。
P2、N2、F1	許可	1	競合しません。
P3、N2、F1	拒否	2	F1 が P1/P2 にバインドされています。
P1、N3、F1	許可	6	N3 に関するワイルドカード一致です。
P1、N1、F3	許可	5	F3 に関するワイルドカード一致です。
P1、N4、F5	拒否	2	P1 が F1 にバインドされています。

表 24-2　各シナリオの許可結果（続き）

デバイス接続要求	許可	条件	理由
P5、N1、F5	拒否	2	N1 は F2 でのみ許可されます。
P3、N3、F4	許可	1	競合しません。
S1、F10	許可	1	競合しません。
S2、F11	拒否	7	P10 が F11 にバインドされています。
P4、N4、F5（自動学習が有効）	許可	3	競合しません。
P4、N4、F5（自動学習が無効）	拒否	4	一致しません。
S3、F5（自動学習が有効）	許可	3	競合しません。
S3、F5（自動学習が無効）	拒否	4	一致しません。
P1、N1、F6（自動学習が有効）	拒否	2	P1 が F1 にバインドされています。
P5、N5、F1（自動学習が有効）	拒否	7	P1 および P2 だけが F1 にバインドされています。
S3、F4（自動学習が有効）	拒否	7	P3 と F4 がペアになります。
S1、F3（自動学習が有効）	許可	5	競合しません。
P5、N3、F3	許可	6	F3 および N3 に関するワイルドカード（*）一致です。
P7、N3、F9	許可	6	N3 に関するワイルドカード（*）一致です。

ポート セキュリティの手動設定

Nexus 5000 シリーズ スイッチにポート セキュリティを設定する手順は、次のとおりです。

ステップ 1　保護する必要があるポートの WWN を識別します。

「許可済みのポート ペアの追加」（p.24-18）を参照してください。

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

ステップ 3　ポート セキュリティ データベースをアクティブにします。

ステップ 4　設定を確認します。

ここで説明する内容は、次のとおりです。

- WWN の識別の注意事項（p.24-17）
- 許可済みのポート ペアの追加（p.24-18）
- ポート セキュリティ設定の削除（p.24-19）

WWN の識別の注意事項

ポート セキュリティを手動で設定する場合は、次の点に注意してください。

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

許可済みのポート ペアの追加

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

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

Fabric Manager を使用して、許可済みのポート ペアをポート セキュリティに追加する手順は、次のとおりです。

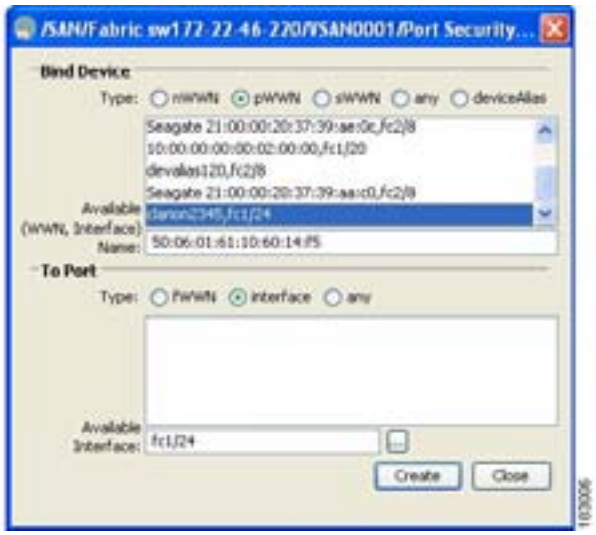
ステップ 1　**VSAN** を展開し、Logical Domains ペインで **Port Security** を選択します。

ステップ 2　**Config Database** タブをクリックします。

ステップ 3　**Create Row** をクリックして、許可済みのポート ペアを追加します。

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

図 24-5　Create Port Security ダイアログボックス



ステップ 4　リストから、ポート セキュリティ設定を作成するデバイスをダブルクリックします。

ステップ 5　リストから、デバイスをバインドするポートをダブルクリックします。

ステップ 6　**Create** をクリックして、ポート セキュリティ設定を作成します。

ステップ 7　**Apply Changes** アイコンをクリックして、これらの変更を保存します。

ポート セキュリティ設定の削除

スイッチ上の既存のデータベースからポート セキュリティ設定を削除する手順は、次のとおりです。

ステップ 1　**VSAN** を展開し、Logical Domains ペインで **Port Security** を選択します。

ステップ 2　**Config Database** タブをクリックします。

VSAN の既存のポート セキュリティ設定が表示されます。

ステップ 3　削除する行をクリックします。

ステップ 4　**Delete Row** を選択します。

確認ダイアログボックスが表示されます。

ステップ 5　行を削除するには、**Yes** をクリックします。行を削除しないで確認ダイアログボックスを閉じるには、**No** をクリックします。

ステップ 6　**Apply Changes** アイコンをクリックして、これらの変更を保存します。

ポート セキュリティ設定の配信

ポート セキュリティ機能は、Cisco Fabric Services（CFS）インフラストラクチャを使用して効率的なデータベース管理を実行し、VSAN 内のファブリック全体に単一の設定を提供して、ファブリック全体でポート セキュリティ ポリシーを施行します（第 7 章「CFS の使用」を参照）。

ここでは、次の内容について説明します。

- 配信のイネーブル化（p.24-20）
- ファブリックのロック（p.24-21）
- 変更のコミット（p.24-21）
- アクティブ化および自動学習の設定の配信（p.24-21）

配信のイネーブル化

配信モードで実行されたすべての設定は、（一時的な）保留データベースに保管されます。設定を変更するには、保留データベースの変更を設定にコミットするか、廃棄する必要があります。この処理の実行中は、ファブリックはロックされた状態になります。保留データベースの変更は、変更をコミットするまでは、設定に反映されません。

（注） CFS 配信がイネーブルの場合、CFS コミットが実行されるまでは、ポートのアクティブ化または非アクティブ化および自動学習のイネーブル化またはディセーブル化は有効になりません。適正な設定を保持するには、必ず、CFS コミットに関するいずれかの処理を行ってください。「アクティブ化および自動学習の設定の配信」（p.24-21）を参照してください。

ヒント ポート セキュリティのアクティブ化後、および自動学習のイネーブル化後に、コミットを実行することを推奨します。

Fabric Manager を使用して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** を展開し、Logical Domains ペインで **Port Security** を選択します。

Information ペインに、その VSAN のポート セキュリティ設定が表示されます（図 24-4 を参照）。

ステップ 2　**Control** タブをクリックします。

その VSAN のスイッチが表示されます。

ステップ 3　**Command** カラムで、ドロップダウン リストから **enable** または **disable** を選択します。

ステップ 4　**Apply Changes** アイコンをクリックして、変更を保存します。

ファブリックのロック

既存設定の変更を開始すると、保留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。

- 他のユーザは、この機能の設定を変更できなくなります。
- コンフィギュレーション データベースのコピーが、保留中のデータベースになります。

変更のコミット

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

アクティブ化および自動学習の設定の配信

配信モードでのアクティブ化および自動学習の設定は、保留データベースの変更をコミットするときに実行される動作として認識されます。

学習されたエントリは一時的なもので、ログインが許可されるかどうかには影響しません。したがって、学習されたエントリは配信には含まれません。学習をディセーブルにして保留データベースの変更をコミットすると、学習されたエントリがアクティブ データベース内のスタティックなエントリになり、ファブリック内のすべてのスイッチに配信されます。コミット実行後は、すべてのスイッチのアクティブ データベースが同一になるので、学習をディセーブルにできます。

変更をコミットする場合、保留データベースに複数のアクティブ化および自動学習の設定が含まれていると、アクティブ化と自動学習の変更が統合され、処理結果が変更されることがあります（表 24-3 を参照）。

表 24-3　配信モードでのアクティブ化および自動学習の設定シナリオ

シナリオ	操作	配信がオフの場合	配信がオンの場合
コンフィギュレーション データベースに A と B が存在し、アクティブ化は実行されていない状態で、デバイス C と D がログインしている。	**1.** ポート セキュリティ データベースをアクティブ化し、自動学習をイネーブルに設定	コンフィギュレーション データベース = {A、B} アクティブ データベース = {A、B、C[1]、D*}	コンフィギュレーション データベース = {A、B} アクティブ データベース = { ヌル } 保留データベース = {A、B + アクティブ化がイネーブル }
	2. 新規エントリ E をコンフィギュレーション データベースに追加	コンフィギュレーション データベース = {A、B、E} アクティブ データベース = {A、B、C*、D*}	コンフィギュレーション データベース = {A、B} アクティブ データベース = { ヌル } 保留データベース = {A、B、E + アクティブ化がイネーブル }
	3. コミットを発行	適用外	コンフィギュレーション データベース = {A、B、E} アクティブ データベース = {A、B、E、C*、D*} 保留データベース = 空

表 24-3　配信モードでのアクティブ化および自動学習の設定シナリオ（続き）

シナリオ	操作	配信がオフの場合	配信がオンの場合
コンフィギュレーション データベースに A と B が存在し、アクティブ化は実行されていない状態で、デバイス C と D がログインしている。	**1.** ポート セキュリティ データベースをアクティブ化し、自動学習をイネーブルに設定	コンフィギュレーション データベース = {A、B} アクティブ データベース = {A、B、C*、D*}	コンフィギュレーション データベース = {A、B} アクティブ データベース = { ヌル } 保留データベース = {A、B + アクティブ化がイネーブル }
	2. 学習をディセーブルにする	コンフィギュレーション データベース = {A、B} アクティブ データベース = {A、B、C、D}	コンフィギュレーション データベース = {A、B} アクティブ データベース = { ヌル } 保留データベース = {A、B + アクティブ化がイネーブル + 学習がディセーブル }
	3. コミットを発行	適用外	コンフィギュレーション データベース = {A、B} アクティブ データベース = {A、B}、デバイス C と D がログアウト。自動学習をディセーブルにしたアクティブ化と同等。 保留データベース = 空

1. *（アスタリスク）は学習されたエントリを意味します。

ヒント　各処理の最後にコミットを実行することを推奨します。つまり、ポート セキュリティのアクティブ化のあと、および自動学習のイネーブル化のあとです。

データベース マージの注意事項

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 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。詳細については、「CFS マージのサポート」（p.7-7）を参照してください。

2 つのファブリック間で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。
- 両方のデータベースの各 VSAN のコンフィギュレーションの合計数が、2000 を超えていないことを確認してください。

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

データベースの相互作用

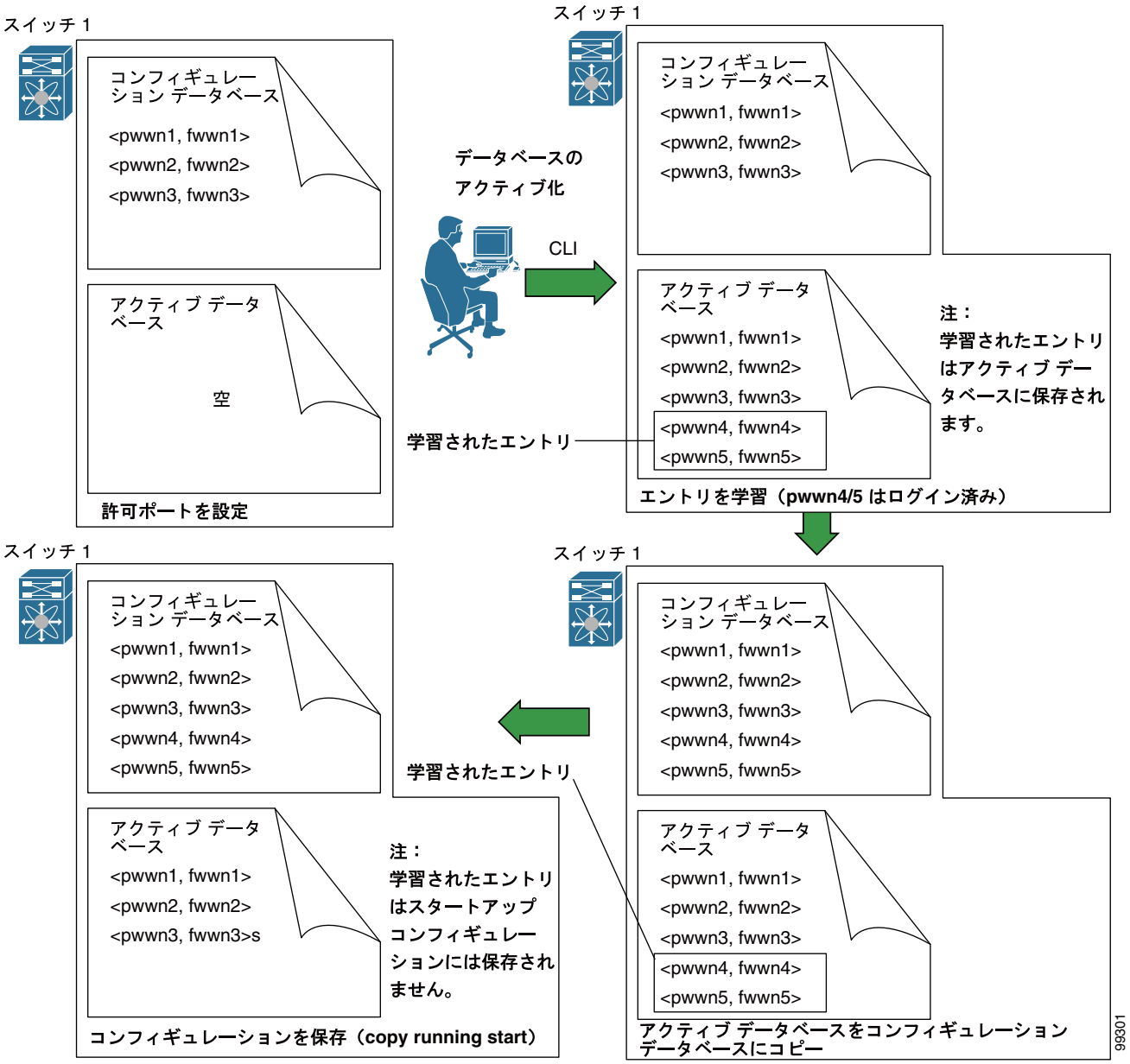
ここで説明する内容は、次のとおりです。

- データベースのシナリオ（p.24-23）
- ポート セキュリティ データベースのコピー（p.24-24）
- ポート セキュリティ データベースの削除（p.24-25）
- ポート セキュリティ データベースのクリア（p.24-25）

データベースのシナリオ

図 24-6 の各シナリオは、ポート セキュリティ設定に基づくアクティブ データベースとコンフィギュレーション データベースのステータスを示しています。

図 24-6　ポート セキュリティ データベースのシナリオ



ポート セキュリティ データベースのコピー

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

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

ステップ 1　***Fabric*** を展開し、**VSAN** を展開して、Logical Domains ペインで **Port Security** を選択します。

ステップ 2　**Actions** タブをクリックします。

すべてのコンフィギュレーション データベースが表示されます。

ステップ 3　適切なコンフィギュレーション データベースを選択し、**Copy Active to Config** チェックボックスをオンにします。

ステップ 4　**Apply Changes** アイコンをクリックして変更を保存します。

Fabric Manager を使用して、アクティブ データベースとコンフィギュレーション データベース間の差分を表示する手順は、次のとおりです。

ステップ 1　***Fabric*** を展開し、**VSAN** を展開して、Logical Domains ペインで **Port Security** を選択します。

Information ペインに、ポート セキュリティ情報が表示されます。

ステップ 2　**Database Differences** タブをクリックします。

すべてのコンフィギュレーション データベースが表示されます。

ステップ 3　適切なコンフィギュレーション データベースを選択します。**Active** または **Config** オプションを選択して、選択したデータベースとアクティブ / コンフィギュレーション データベース間の差分を比較します。

ステップ 4　**Apply Changes** アイコンをクリックして変更を保存します。

ポート セキュリティ データベースの削除

ヒント　配信がイネーブルの場合、削除を実行すると、データベースのコピーが作成されます。データベースを実際に削除するには、明示的な削除が必要です。

Fabric Manager を使用してポート セキュリティ データベースを削除する手順は、次のとおりです。

ステップ 1　***Fabric*** を展開し、**VSAN** を展開して、Logical Domains ペインで **Port Security** を選択します。

Information ペインに、ポート セキュリティ情報が表示されます。

ステップ 2　**Config Database** タブをクリックします。

すべてのコンフィギュレーション データベースが表示されます。

ステップ 3　適切なコンフィギュレーション データベースを選択し、**Delete Row** ボタンをクリックします。

ステップ 4　コンフィギュレーション データベースを削除する場合は、**Yes** をクリックします。

ポート セキュリティ データベースのクリア

Fabric Manager を使用して、指定した VSAN に関するすべての既存の統計情報をポート セキュリティ データベースからクリアする手順は、次のとおりです。

ステップ 1　***Fabric*** を展開し、**VSAN** を展開して、Logical Domains ペインで **Port Security** を選択します。

Information ペインに、ポート セキュリティ情報が表示されます（図 24-4 を参照）。

ステップ 2　**Statistics** タブをクリックします。

すべてのコンフィギュレーション データベースが表示されます。

ステップ 3　適切なコンフィギュレーション データベースを選択し、**Clear** オプションを選択します。

ステップ 4　**Apply Changes** アイコンをクリックして変更を保存します。

Fabric Manager を使用して、VSAN 内の指定したインターフェイスについて、すべての学習済みエントリをアクティブ データベースからクリアする手順は、次のとおりです。

ステップ 1　***Fabric*** を展開し、**VSAN** を展開して、Logical Domains ペインで **Port Security** を選択します。

Information ペインに、ポート セキュリティ情報が表示されます。

ステップ 2　**Actions** タブをクリックします。

すべてのコンフィギュレーション データベースが表示されます。

ステップ 3　適切なコンフィギュレーション データベースを選択し、**AutoLearn** オプションを選択します。

ステップ 4　**Apply Changes** アイコンをクリックして変更を保存します。

（注） Statistics タブおよび AutoLearn オプションで情報をクリアできるのは、ロックが適用されないローカル スイッチだけです。また、学習済みエントリはスイッチのローカル情報になるだけで、配信には含まれません。

デフォルト設定

表 24-4 に、スイッチのすべてのポート セキュリティ機能のデフォルト設定を示します。

表 24-4　セキュリティのデフォルト設定

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

CHAPTER 25

ファブリック バインディングの設定

この章では、Nexus 5000 シリーズ スイッチで提供されるファブリック バインディング機能について説明します。この章の内容は、次のとおりです。

- ファブリック バインディングの概要（p.25-2）
- ファブリック バインディングの設定（p.25-4）
- デフォルト設定（p.25-13）

ファブリック バインディングの概要

ファブリック バインディング機能では、ファブリック内の指定したスイッチ間だけで確実に ISL をイネーブルにすることができます。ファブリック バインディングは VSAN 単位で設定します。

この機能を使用すると、不正なスイッチがファブリックに参加したり、現在のファブリック処理が中断されたりすることがなくなります。Exchange Fabric Membership Data（EFMD）プロトコルにより、ファブリック内の全スイッチで、許可されたスイッチのリストが同一になります。

ここで説明する内容は、次のとおりです。

- ライセンスの要件（p.25-2）
- ポート セキュリティとファブリック バインディングの比較（p.25-2）
- ファブリック バインディングの実行（p.25-3）

ライセンスの要件

ファブリック バインディングには、ストレージ プロトコル サービス ライセンスが必要です。詳細については、『*Nexus 5000 Series Switch CLI Software Configuration Guide*』を参照してください。

ポート セキュリティとファブリック バインディングの比較

ポート セキュリティとファブリック バインディングは、相互に補完するように設定できる 2 つの独立した機能です。表 25-1 に、2 つの機能の比較を示します。

表 25-1　ファブリック バインディングとポート セキュリティの比較

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

xE ポートのポート レベル チェックは、次のように実行されます。

- スイッチのログインは、特定の VSAN に対して、ポート セキュリティ バインディングとファブリック バインディングの両方を使用します。
- バインディング チェックは、ポート VSAN 上で次のように実行されます。
  - ポート VSAN 上での E ポート セキュリティ バインディング チェック
  - 許可された各 VSAN での TE ポート セキュリティ バインディング チェック

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

ファブリック バインディングの実行

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

ファブリック バインディングの設定

ファブリック バインディング機能では、ファブリック バインディング設定で指定したスイッチ間だけで ISL をイネーブルにすることができます。ファブリック バインディングは VSAN 単位で設定します。

ここで説明する内容は、次のとおりです。

- ファブリック バインディングの設定（p.25-4）
- ファブリック バインディングのイネーブル化（p.25-5）
- スイッチ WWN リストの概要（p.25-5）
- スイッチ WWN リストの設定（p.25-6）
- ファブリック バインディングのアクティブ化と非アクティブ化の概要（p.25-7）
- ファブリック バインディングのアクティブ化（p.25-7）
- ファブリック バインディングの強制的なアクティブ化（p.25-8）
- ファブリック バインディング設定のコピー（p.25-8）
- ファブリック バインディング設定の作成（p.25-9）
- ファブリック バインディング設定の削除（p.25-9）
- コンフィギュレーション ファイルへのファブリック バインディングのコピー（p.25-10）
- EFMD 統計情報の表示（p.25-10）
- ファブリック バインディング違反の表示（p.25-11）
- ファブリック バインディングのアクティブ データベースの表示（p.25-11）
- ファブリック バインディング設定の保存（p.25-12）
- ファブリック バインディング統計情報のクリア（p.25-12）
- ファブリック バインディング データベースの削除（p.25-13）

ファブリック バインディングの設定

ファブリック内の各スイッチにファブリック バインディングを設定する手順は、次のとおりです。

ステップ 1　ファブリック設定機能をイネーブルにします。

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

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

ステップ 4　ファブリック バインディング アクティブ データベースを、ファブリック バインディング コンフィギュレーション データベースにコピーします。

ステップ 5　ファブリック バインディング設定を保存します。

ステップ 6　ファブリック バインディング設定を確認します。

ファブリック バインディングのイネーブル化

ファブリック バインディングに参加させるファブリック内の各スイッチで、ファブリック バインディング機能をイネーブルにする必要があります。デフォルトでは、この機能は Nexus 5000 シリーズ スイッチでディセーブルです。ファブリック バインディング機能の設定および確認コマンドを使用できるのは、スイッチ上でファブリック バインディングがイネーブルに設定されている場合だけです。この設定をディセーブルにすると、関連するすべてのコンフィギュレーションが自動的に廃棄されます。

Fabric Manager を使用して、参加させるスイッチのファブリック バインディングをイネーブルにする手順は、次のとおりです。

ステップ 1　Logical Domains ペインで、ファブリック バインディングをイネーブルにするスイッチが存在する VSAN を展開します。**Fabric Binding** を展開します（図 25-1 を参照）。

図 25-1　ファブリック バインディングの設定

Information ペインのデフォルト タブは、**Control** タブです。

ステップ 2　Command ドロップダウン リストで **enable または disable** を選択し、スイッチ上のファブリック バインディングをイネーブルまたはディセーブルに設定します。

ステップ 3　**Apply Changes** アイコンをクリックして変更を保存します。

スイッチ WWN リストの概要

ユーザ指定のファブリック バインディング リストには、ファブリック内の sWWN のリストが含まれています。sWWN がファブリックへの参加を試みたとき、その sWWN がリストに含まれていない場合、またはその sWWN が許可リストで指定されたドメイン ID と異なるドメイン ID を使用していた場合には、その VSAN 内でスイッチとファブリック間の ISL が自動的に隔離され、スイッチのファブリックへの参加は拒否されます。

スイッチ WWN リストの設定

Fabric Manager を使用して、FICON VSAN 用の sWWN およびドメイン ID のリストを設定する手順は、次のとおりです。

ステップ 1　Logical Domains ペインで、ファブリック バインディングが設定されている VSAN を展開します。**Fabric Binding** を展開します（図 25-1 を参照）。

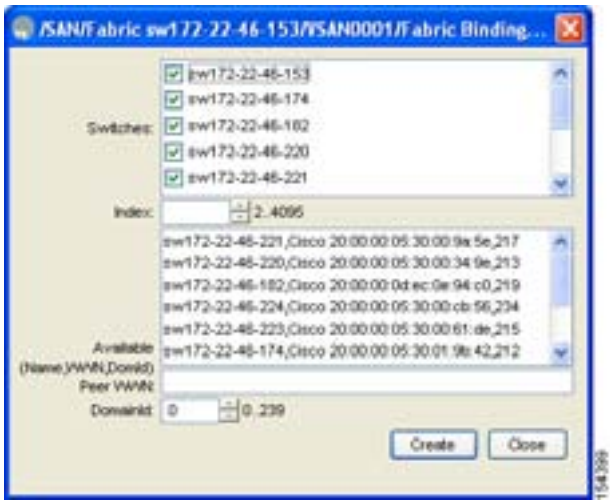
ステップ 2　選択した VSAN で、ファブリック バインディングがイネーブルであることを確認します。

ステップ 3　Information ペインで **Config Database** タブをクリックします。

ステップ 4　**Create Row** をクリックします。

Create Config Database ダイアログボックスが表示されます（図 25-2 を参照）。

図 25-2　Create Config Database ダイアログボックス



ステップ 5　追加するスイッチを選択します。

ステップ 6　スイッチの sWWN およびドメイン ID を、設定したデータベース リストに追加します。

設定したデータベース リストには、複数のスイッチの sWWN およびドメイン ID を追加できます。

ステップ 7　**Create** をクリックします。

ファブリック バインディングのアクティブ化と非アクティブ化の概要

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

デフォルトでは、ファブリック バインディング機能は非アクティブです。コンフィギュレーション データベース内の既存のエントリがファブリックの現在の状態と矛盾していると、スイッチ上のファブリック バインディング データベースをアクティブにできません。たとえば、ログイン済みのスイッチの 1 つが、コンフィギュレーション データベースによってログインを拒否されている場合などです。これらの状態は、強制的に上書きすることができます。

（注） データベースをアクティブにすると、現在のアクティブ データベースに違反するログイン済みのスイッチはログアウトされ、ファブリック バインディング制限によって以前にログインを拒否されたすべてのスイッチが、再初期化されます。

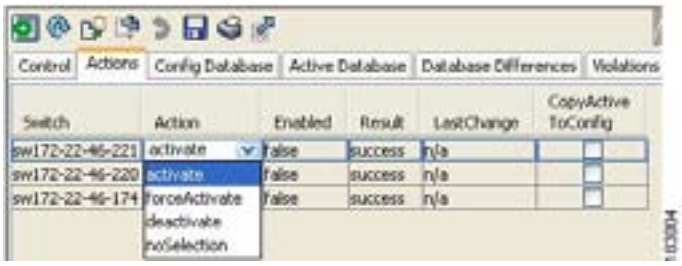
ファブリック バインディングのアクティブ化

Fabric Manager を使用してファブリック バインディングをアクティブ化、非アクティブ化、または強制実行する手順は、次のとおりです。

ステップ 1　Logical Domains ペインで、ファブリック バインディングが設定されている VSAN を展開します。**Fabric Binding** を展開します。

ステップ 2　Information ペインで **Actions** タブをクリックします（図 25-3 を参照）。

図 25-3　ファブリック バインディングの Actions タブ



ステップ 3　**Action** ドロップダウン リストで、スイッチ上のファブリック バインディングの **activate**、**deactivate**、または **force activate** を選択します。

ステップ 4　**Apply Changes** アイコンをクリックして変更を保存します。

スイッチの Enabled カラムに True が表示されます。

ファブリック バインディングの強制的なアクティブ化

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

Fabric Manager を使用してファブリック バインディング データベースを強制的にアクティブ化する手順は、次のとおりです。

ステップ 1　Logical Domains ペインで、ファブリック バインディングが設定されている VSAN を展開します。**Fabric Binding** を展開します。

ステップ 2　Information ペインで **Actions** タブをクリックします（図 25-3 を参照）。

ステップ 3　Action ドロップダウン リストで、ファブリック バインディングをアクティブにする VSAN に対して **forceActivate** を選択します。

ステップ 4　**Apply Changes** をクリックして、ファブリック バインディングをアクティブにします。

スイッチの Enabled カラムに True が表示されます。

ファブリック バインディング設定のコピー

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

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

ステップ 1　Logical Domains ペインで、ファブリック バインディングが設定されている VSAN を展開します。**Fabric Binding** を展開します。

ステップ 2　Information ペインで **Actions** タブをクリックします。

ステップ 3　**Copy Active to Config** チェックボックスをオンにします。

ステップ 4　**Apply Changes** アイコンをクリックして変更を保存します。

ファブリック バインディング設定の作成

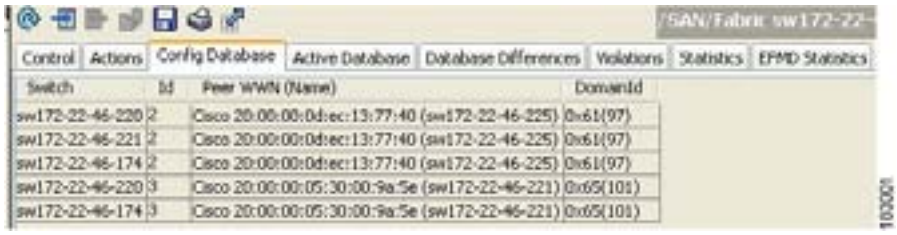
Fabric Manager を使用してファブリック バインディング設定を作成する手順は、次のとおりです。

ステップ 1　Logical Domains ペインで、ファブリック バインディングが設定されている VSAN を展開します。**Fabric Binding** を展開します。

ステップ 2　Information ペインで **Config Database** タブをクリックします。

図 25-4 のような情報が表示されます。

図 25-4　ファブリック バインディング データベースの設定



ステップ 3　**Insert Row** をクリックします。

Create Config Database ダイアログボックスが表示されます（図 25-2 を参照）。

ステップ 4　スイッチおよびインデックスを選択し、ピアの WWN およびドメイン ID を指定します。

ステップ 5　**Create** をクリックして、ファブリック バインディング データベース設定を作成します。

ファブリック バインディング設定を保存すると、コンフィギュレーション データベースおよびアクティブ データベースは両方ともスタートアップ コンフィギュレーションに保存され、再起動後も使用できるようになります。

ファブリック バインディング設定の削除

Fabric Manager を使用してファブリック バインディング設定を削除する手順は、次のとおりです。

ステップ 1　Logical Domains ペインで、ファブリック バインディングが設定されている VSAN を展開します。**Fabric Binding** を展開します。

ステップ 2　Information ペインで **Config Database** タブをクリックします。

図 25-4 のような情報が表示されます。

ステップ 3　ファブリック バインディング設定を削除する VSAN 行をクリックします。

ステップ 4　**Delete Row** をクリックして、ファブリック バインディング設定を削除します。

コンフィギュレーション ファイルへのファブリック バインディングのコピー

Fabric Manager を使用してアクティブ ファブリック バインディングをコンフィギュレーション ファイルにコピーする手順は、次のとおりです。

ステップ 1　Logical Domains ペインで、ファブリック バインディングが設定されている VSAN を展開します。**Fabric Binding** を展開します。

ステップ 2　Information ペインで **Actions** タブをクリックします（図 25-3 を参照）。

ステップ 3　ファブリック バインディングをコピーする VSAN の **CopyActive ToConfig** チェックボックスをオンにします。

ステップ 4　**Apply Changes** アイコンをクリックし、ファブリック バインディングをコピーします。

注意　FICON がイネーブルである VSAN 内でファブリック バインディングを非アクティブまたはディセーブルにすることはできません。

EFMD 統計情報の表示

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

ステップ 1　Logical Domains ペインで、ファブリック バインディングが設定されている VSAN を展開します。**Fabric Binding** を展開します。

ステップ 2　**EFMD Statistics** タブをクリックします。

統計情報が表示されます。

ファブリック バインディング違反の表示

Fabric Manager を使用してファブリック バインディング違反を表示する手順は、次のとおりです。

ステップ 1　Logical Domains ペインで、ファブリック バインディングが設定されている VSAN を展開します。**Fabric Binding** を展開します。

ステップ 2　**Violations** タブをクリックします。

違反情報が表示されます。

ファブリック バインディングのアクティブ データベースの表示

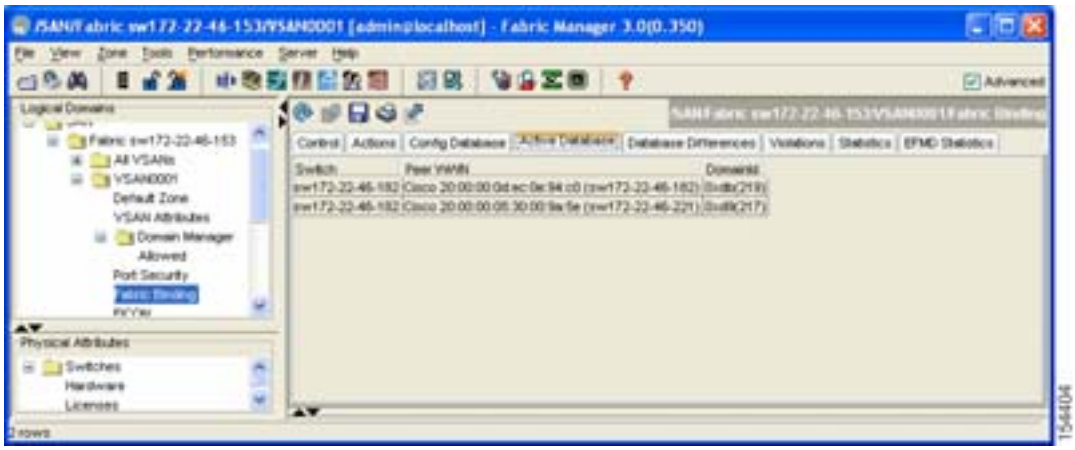
Fabric Manager を使用してファブリック バインディング アクティブ データベースを表示する手順は、次のとおりです。

ステップ 1　Logical Domains ペインで、ファブリック バインディングが設定されている VSAN を展開します。**Fabric Binding** を展開します。

ステップ 2　**Active Database** タブをクリックします。

アクティブ データベースの情報が表示されます（図 25-5 を参照）。

図 25-5　ファブリック バインディングのアクティブ データベース



ファブリック バインディング設定の保存

ファブリック バインディング設定を保存すると、コンフィギュレーション データベースおよびアクティブ データベースは両方ともスタートアップ コンフィギュレーションに保存され、再起動後も使用できるようになります。

Fabric Manager を使用してファブリック バインディング設定を保存する手順は、次のとおりです。

ステップ 1　Logical Domains ペインで、ファブリック バインディングが設定されている VSAN を展開します。**Fabric Binding** を展開します。

ステップ 2　**Actions** タブをクリックします（図 25-3 を参照）。

ステップ 3　**Copy Active to Config** チェックボックスをオンにして、アクティブ データベースをコンフィギュレーション データベースにコピーします。

設定したデータベースが空の場合、この動作は実行されません。

ステップ 4　**Database Differences** タブをクリックして、データベースを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 データベースと比較して、アクティブ データベースとコンフィギュレーション データベースの差分を表示します。

ファブリック バインディング統計情報のクリア

Fabric Manager を使用して、指定した VSAN に関するすべての既存の統計情報をファブリック バインディング データベースからクリアする手順は、次のとおりです。

ステップ 1　Logical Domains ペインで、ファブリック バインディングが設定されている VSAN を展開します。**Fabric Binding** を展開します。

ステップ 2　Information ペインで **Statistics** タブをクリックします。

Information ペインに統計情報が表示されます。

ステップ 3　**Clear** チェックボックスをオンにします。

ステップ 4　**Apply Changes** アイコンをクリックして変更を保存します。

ファブリック バインディング データベースの削除

Fabric Manager を使用して、指定した VSAN の設定済みデータベースを削除する手順は、次のとおりです。

ステップ 1　Logical Domains ペインで、ファブリック バインディングが設定されている VSAN を展開します。**Fabric Binding** を展開します。

ステップ 2　Information ペインで **Config Database** タブをクリックします。

ステップ 3　削除するデータベースを選択します。

ステップ 4　**Delete Row** をクリックします。

デフォルト設定

表 25-2 に、ファブリック バインディング機能のデフォルト設定を示します。

表 25-2　ファブリック バインディングのデフォルト設定

パラメータ	デフォルト
ファブリック バインディング	ディセーブル

CHAPTER 26

FCS の設定

この章では、Nexus 5000 シリーズ スイッチに組み込まれた Fabric Configuration Server（FCS）機能について説明します。この章の内容は、次のとおりです。

- FCS の概要（p.26-2）
- FCS 検出情報の表示（p.26-4）
- FCS 要素の表示（p.26-5）
- FCS プラットフォームの作成（p.26-6）
- FCS Fabric Port の表示（p.26-7）
- デフォルト設定（p.26-8）

FCS の概要

FCS を使用すると、トポロジ アトリビュートを検出したり、ファブリック要素のコンフィギュレーション情報リポジトリを維持することができます。通常、管理アプリケーションは N ポートを通してスイッチの FCS に接続されます。FCS は次のオブジェクトに基づいて、ファブリック全体を表示します。

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

各オブジェクトには、それぞれ独自の一連のアトリビュートと値があります。一部のアトリビュートにはヌル値も定義できます。

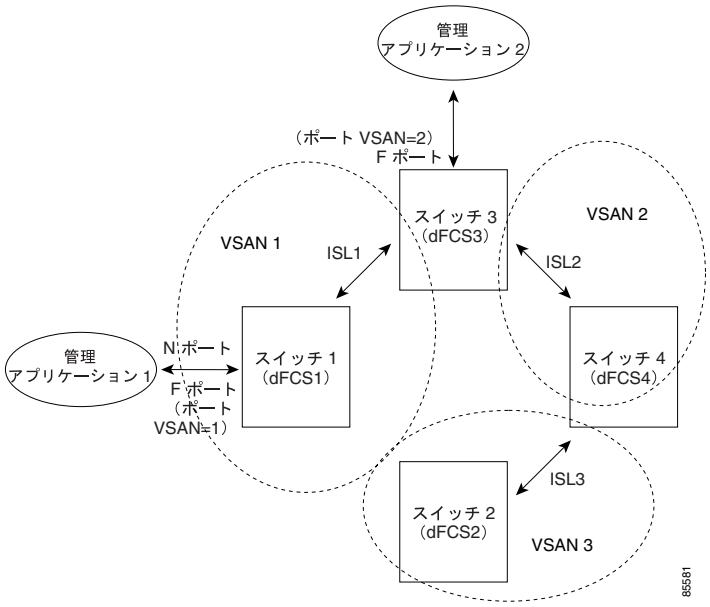
Nexus 5000 シリーズ スイッチ環境では、ファブリックを複数の VSAN で構成できます。VSAN ごとに FCS のインスタンスが 1 つ存在します。

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

スイッチに管理アプリケーションが接続されている場合、スイッチの FCS に転送されるすべてのフレームは、スイッチ ポート（F ポート）のポート VSAN に属します。管理アプリケーションの表示対象はこの VSAN に限定されます。ただし、このスイッチが属する他の VSAN に関する情報は、SNMP（簡易ネットワーク管理プロトコル）または CLI（コマンドライン インターフェイス）を使用して取得できます。

図 26-1 では、Management Application 1（M1）はポート VSAN ID が 1 の F ポートを介して接続され、Management Application 2（M2）はポート VSAN ID が 2 の F ポートを介して接続されています。M1 はスイッチ S1 および S3 の FCS 情報を、M2 はスイッチ S3 および S4 の FCS 情報を問い合わせることができます。スイッチ S2 情報はどちらにも提供されません。FCS は、VSAN で表示可能なこれらのスイッチ上でのみ動作します。S3 は VSAN 1 にも属していますが、M2 は VSAN 2 にのみ FCS 要求を送信できます。

図 26-1　VSAN 環境における FCS



FCS の特性

FCS には次の特性があります。

- 次のようなネットワーク管理をサポートします。
  - N ポート管理アプリケーションは、ファブリック要素に関する情報を問い合わせて取得することができます。
  - SNMP Manager は FCS MIB（管理情報ベース）を使用して、ファブリック トポロジ情報の検出を開始して、取得することができます。
- 標準の F ポートおよび E ポートだけでなく、TE ポートもサポートします。
- プラットフォームに登録された論理名および管理アドレスを使用して、一連のノードを維持することができます。FCS はすべての登録情報のバックアップをセカンダリ ストレージに維持し、変更があるたびに更新します。再起動またはスイッチオーバーが発生すると、FCS はセカンダリ ストレージ情報を取得し、データベースを再構築します。
- SNMP マネージャは FCS に、ファブリック内のすべての IE、ポート、およびプラットフォームについて問い合わせることができます。

FCS 検出情報の表示

Device Manager を使用して FCS 検出情報を表示する手順は、次のとおりです。

ステップ 1　**FC** > **Advanced** > **Fabric Config Server** を選択します。

Fabric Config Server ダイアログボックスが表示されます（図 26-2 を参照）。

図 26-2　Fabric Config Server ダイアログボックス

ステップ 2　**Discovery** タブをクリックします。

ステップ 3　**Discover** をクリックしてファブリックを再検出し、**Refresh** をクリックして表示内容を更新します。

FCS 要素の表示

Device Manager を使用して FCS IE 情報を表示する手順は、次のとおりです。

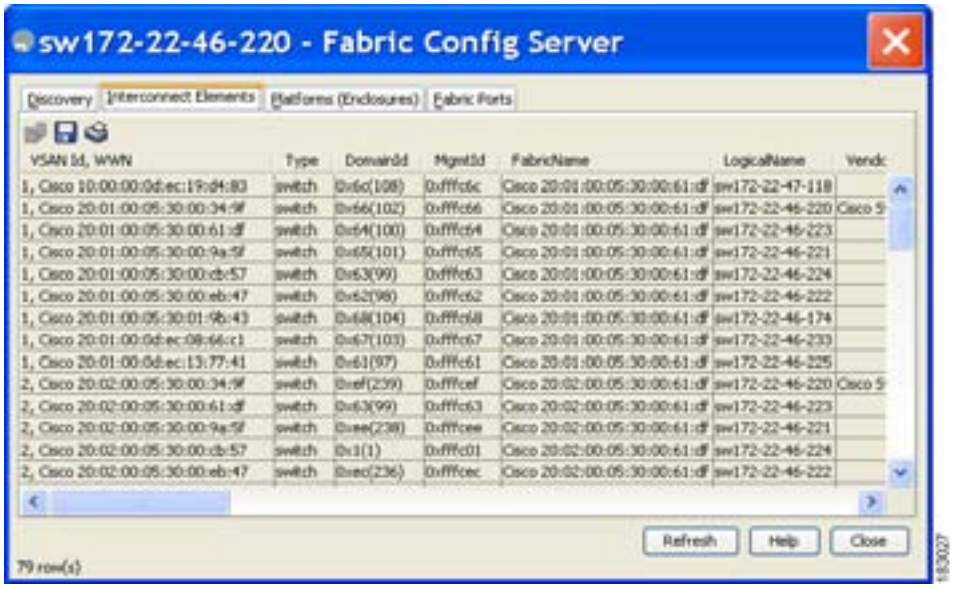
ステップ 1　**FC** > **Advanced** > **Fabric Config Server** を選択します。

Fabric Config Server ダイアログボックスが表示されます。

ステップ 2　**Interconnect Elements** タブをクリックします。

図 26-3 のようなダイアログボックスが表示されます。

図 26-3　FCS Interconnect Elements タブ



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

FCS プラットフォームの作成

Device Manager を使用して FCS プラットフォームを作成する手順は、次のとおりです。

ステップ 1　**FC** > **Advanced** > **Fabric Config Server** を選択します。

Fabric Config Server ダイアログボックスが表示されます。

ステップ 2　**Platforms**（**Enclosures**）タブをクリックします。

ステップ 3　**Create** をクリックします。

Create Fabric Config Server ダイアログボックスが表示されます（図 26-4 を参照）。

図 26-4　Create Fabric Config Server ダイアログボックス

ステップ 4　VSAN ID を入力します。または利用可能な VSAN ID のドロップダウン リストから ID を選択します。

ステップ 5　Name フィールドに、Fabric Configuration Server の名前を入力します。

ステップ 6　サーバの種類を選択します（**Gateway**、**Host**、**Storage**）。

ステップ 7　サーバの WWN を入力します。

ステップ 8　サーバの管理アドレスを入力します。

ステップ 9　**Create** をクリックしてサーバを作成します。

FCS Fabric Port の表示

Device Manager を使用して FCS 検出情報を表示する手順は、次のとおりです。

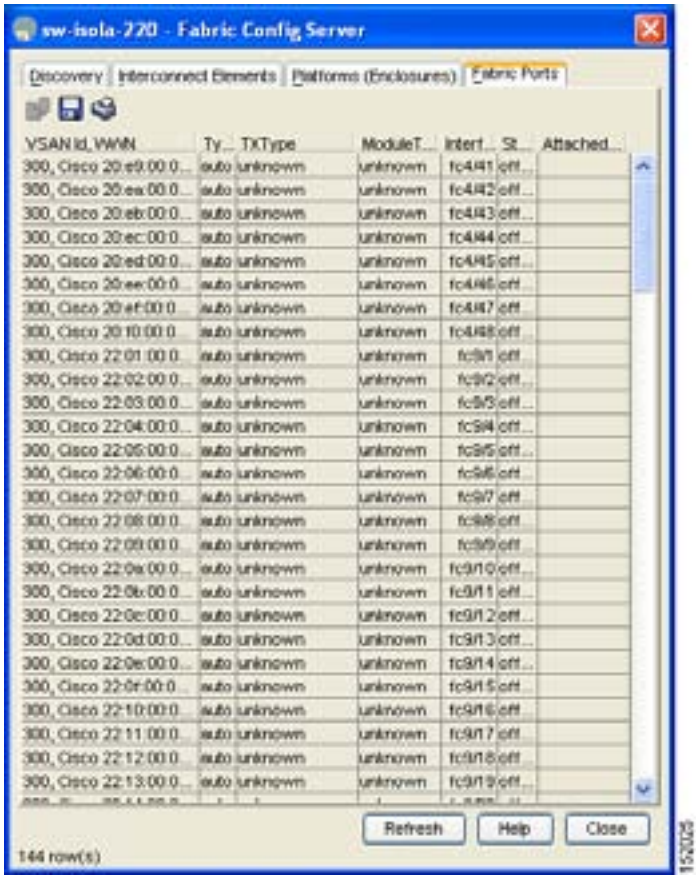
ステップ 1　**FC** > **Advanced** > **Fabric Config Server** を選択します。

Fabric Config Server ダイアログボックスが表示されます。

ステップ 2　**Fabric Ports** タブをクリックします。

ファブリック ポートのリストが表示されます（図 26-5 を参照）。

図 26-5　FCS Fabric Ports タブ



ステップ 3　**Refresh** をクリックして表示内容を更新します。

デフォルト設定

表 26-1 に、FCS のデフォルト設定値を示します。

表 26-1　FCS のデフォルト設定値

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

CHAPTER 27

ポート トラッキングの設定

Nexus 5000 シリーズ スイッチは、物理ファイバ チャネル インターフェイスのポート トラッキング機能を提供します（仮想ファイバ チャネル インターフェイスのポート トラッキング機能は提供しません）。この機能はリンクの動作ステートに関する情報を使用して、エッジ デバイスを接続するリンクの障害を引き起こします。この処理では、間接障害が直接障害に変換されるため、冗長リンクへの復旧処理が迅速に行われます。ポート トラッキング機能がイネーブルになっている場合、この機能はリンク障害時に設定されたリンクをダウンにし、トラフィックを別の冗長リンクに強制的にリダイレクトします。

この章の内容は、次のとおりです。

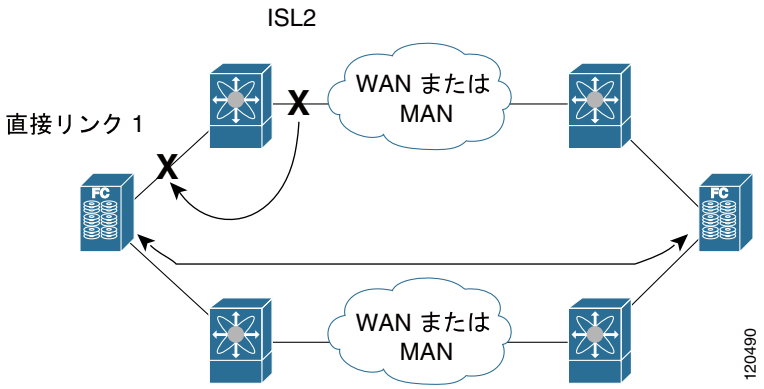
- ポート トラッキングの概要（p.27-2）
- ポート トラッキングの設定（p.27-3）
- ポート トラッキングのデフォルト設定値（p.27-8）

ポート トラッキングの概要

一般的に、ホストはスイッチに直接接続されているリンク（直接リンク）上でのリンク障害からはすぐに復旧できます。しかし、キープアライブ メカニズムを備えた WAN や MAN ファブリック内のスイッチ間で発生する間接的なリンク障害からの復旧は、Time Out Value（TOV）や Registered State Change Notification（RSCN）情報などの複数の要因に左右されます（「ファイバ チャネルの TOV」[p.22-2] および 「RSCN 情報の概要」[p.19-7] を参照）。

図 27-1 で、ホストに対する直接リンク 1 に障害が発生した場合、ただちに復旧可能です。ただし、2 つのスイッチ間の ISL 2 に障害が発生した場合、復旧は TOV や RSCN などに左右されます。

図 27-1　ポート トラッキングによるトラフィックの復旧



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

この章では次の用語を使用します。

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

ポート トラッキングには次の機能があります。

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

ポート トラッキングの設定

ポート トラッキングを設定する際、次の点に注意してください。

- トラッキング対象ポートとリンク対象ポートが同じシスコ スイッチ上に存在することを確認します。
- トラッキング対象ポートがダウンしたときに、リンク対象ポートが自動的にダウンすることを確認します。
- 再帰依存を回避するためにリンク対象ポートに再度トラッキング（たとえば、ポート fc2/2 からポート fc2/4 にトラッキングし、さらにポート fc2/2 に戻す）しないでください。

ここで説明する内容は、次のとおりです。

- ポート トラッキングのイネーブル化（p.27-4）
- リンク対象ポート設定の概要（p.27-4）
- トラッキング対象ポートの動作バインディング（p.27-5）
- 複数ポート トラッキングの概要（p.27-7）
- 複数ポートのトラッキング（p.27-7）
- VSAN 内のポートの監視の概要（p.27-7）
- VSAN 内のポートの監視（p.27-8）
- 強制シャットダウンの概要（p.27-8）
- トラッキング対象ポートの強制シャットダウン（p.27-8）

ポート トラッキングのイネーブル化

デフォルトでは、ポート トラッキング機能は Nexus 5000 シリーズ スイッチでディセーブルです。この機能をイネーブルにすると、ポート トラッキングはスイッチ全体でグローバルにイネーブルになります。

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

Fabric Manager を使用してポート トラッキングをイネーブルにする手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches** > **Interfaces** を展開して、**Port Tracking** を選択します。

Information ペインにポート トラッキング情報が表示されます（図 27-2 を参照）。デフォルト タブは Controls タブです。

図 27-2　ポート トラッキング

ステップ 2　Command カラムで、ポート トラッキングの **enable** または **disable** を選択します。

選択に応じて Status カラムで対応するエントリが変更されます。

ステップ 3　**Apply Changes** アイコンをクリックして変更を保存します。

Result カラムのエントリが success に変わります。

リンク対象ポート設定の概要

ポートをリンクするには、次の 2 通りの方法があります。

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

トラッキング対象ポートの動作バインディング

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

トラッキング対象ポートの動作バインディングを設定する手順は、次のとおりです。

ステップ 1　Physical Attributes ペインで、**Switches** > **Interfaces** を展開して、**Port Tracking** を選択します。

Information ペインにポート トラッキング情報が表示されます。デフォルト タブは Controls タブです。

図 27-3　Port Tracking Controls タブ

ステップ 2　**Dependencies** タブをクリックします。

ステップ 3　**Create Row** をクリックします。

Create Port Tracking Dependencies ダイアログボックスが表示されます（図 27-4 を参照）。

図 27-4　Create Port Tracking Dependencies ダイアログボックス

ステップ 4　トラッキングするポートのスイッチをドロップダウン リストから選択します。

ステップ 5　トラッキング対象ポートにバインディングするリンク対象ポートを、リストのブラウザ ボタンをクリックして選択します。

ステップ 6　選択したポートを 1 つの VSAN だけでトラッキングする場合は **Single VSAN** オプション ボタンをクリックします。選択したポートを利用可能なすべての VSAN でトラッキングする場合は **All VSANs** オプション ボタンをクリックします。

詳細については「VSAN 内のポートの監視の概要」（p.27-7）を参照してください。

ステップ 7　上記のステップで Single VSAN を選択した場合は、ポートを監視する VSAN の ID を入力します。

ステップ 8　トラッキング対象ポートを強制的にシャットダウンする場合は、**Forceshut** チェックボックスをオンにします。

詳細については「強制シャットダウンの概要」（p.27-8）を参照してください。

ステップ 9　**Create** をクリックしてこの依存関係を作成します。

トラッキングが確立されると、ダイアログボックスの左下に **Success** と表示されます（図 27-5 を参照）。

図 27-5　ポート トラッキングが正しく確立された場合

ステップ 10　**Close** をクリックして、ダイアログボックスを閉じます。

次に、特定のインターフェイスのポート トラッキングをイネーブルにする例を示します。

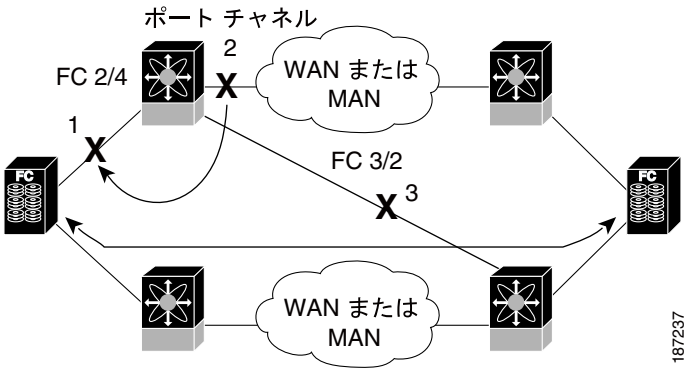
```
switch# configure
switch(config)# interface fc 2/4
switch(config-if)# port-track interface san-port-channel 2
```

複数ポート トラッキングの概要

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

図 27-6 で、直接リンク 1 がダウンするのは、ISL 2 と 3 の両方に障害が発生した場合だけです。ISL 2 または 3 が動作しているかぎり、直接リンク 1 はダウンしません。

図 27-6　ポート トラッキングによるトラフィックの復旧



複数ポートのトラッキング

複数ポートのトラッキングについては、「トラッキング対象ポートの動作バインディング」（p.27-5）を参照してください。

次に、複数のインターフェイスのポート トラッキングをイネーブルにする例を示します。

```
switch# configure
switch(config)# interface fc 2/3
switch(config-if)# port-track interface fc 2/3
switch(config-if)# port-track interface san-port-channel 2
```

VSAN 内のポートの監視の概要

トラッキング対象ポート上のすべての動作 VSAN から任意の VSAN をリンク対象ポートに設定するには、必要な VSAN を指定します。この柔軟性により、トラッキング対象ポートの細かさの度合いが大きくなります。トラッキング対象ポートが TE ポートの場合、ポートの動作ステートがダウンにならずに、ポート上の動作 VSAN がダイナミックに変わる場合があります。この場合、リンク対象ポートのポート VSAN は、トラッキング対象ポート上の動作 VSAN 上で監視できます。

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

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

VSAN 内のポートの監視

特定の VSAN でトラッキング対象ポートを監視する手順については、「トラッキング対象ポートの動作バインディング」（p.27-5）を参照してください。

強制シャットダウンの概要

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

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

トラッキング対象ポートの強制シャットダウン

トラッキング対象ポートを強制的にシャットダウンする手順については、「トラッキング対象ポートの動作バインディング」（p.27-5）を参照してください。

ポート トラッキングのデフォルト設定値

表 27-1 に、ポート トラッキング パラメータのデフォルト設定値を示します。

表 27-1　ポート トラッキング パラメータのデフォルト値

パラメータ	デフォルト
ポート トラッキング	ディセーブル
動作バインディング	ポート トラッキングとともにイネーブル

CHAPTER 28

ネットワーク モニタリング

Fabric Manager の主な目的は、ネットワークを管理することです。特に重要なネットワーク管理機能は、Storage Area Network（SAN; ストレージ エリア ネットワーク）の検出およびネットワーク モニタリングの 2 つです。

この章の内容は、次のとおりです。

- SAN 検出およびトポロジ マッピングの概要（p.28-2）
- ヘルスおよびイベント モニタリング（p.28-5）

SAN 検出およびトポロジ マッピングの概要

Fabric Manager には、広範囲の SAN 検出、トポロジ マッピング、および情報表示機能があります。Fabric Manager は、接続先スイッチへの SNMP（簡易ネットワーク管理プロトコル）クエリーによって、ファブリック トポロジ上の情報を収集します。そしてファブリック トポロジを再作成し、カスタマイズ可能なマップで提示し、複数の表示オプションにより、コンポーネントおよび設定情報を提供します。

ここで説明する内容は、次のとおりです。

- デバイスの検出（p.28-2）
- トポロジ マッピング（p.28-2）
- コンポーネント管理（p.28-4）
- Device Manager からのログの表示（p.28-5）

デバイスの検出

Fabric Manager を起動すると、SAN 検出プロセスが開始されます。ネーム サーバ レジストレーション、Fibre Channel Generic Services（FC-GS）、Fabric Shortest Path First（FSPF）、および SCSI-3 など、シード スイッチからポーリングした情報を使用して、Fabric Manager は 1 つまたは複数のファブリック上の全デバイスおよび相互接続を自動的に検出します。すべての使用可能なスイッチ、Host Bus Adapter（HBA）、およびストレージ デバイスが検出されます。Cisco SAN スイッチは、Fabric Device Management Interface（FDMI）を使用して、ホストのエージェントを使用せずに、HBA のモデル、シリアル番号、ファームウェア バージョン、およびホスト オペレーティング システムのタイプおよびバージョンを検出します。この情報は、各スイッチへの SNMP クエリーによって収集されます。検出されるデバイス情報は、デバイス名、ソフトウェア リビジョン レベル、ベンダー、ISL（スイッチ間リンク）、SAN ポート チャネル、VSAN などです。

トポロジ マッピング

Fabric Manager は、ファブリックのトポロジ表示を基盤にしています。デバイス検出情報に基づくトポロジ マップを表示することにより、Fabric Manager では、単一ウィンドウに複数のファブリックが正確に表示されます。トポロジ マップのアイコン レイアウトは、ドラッグアンドドロップ方式のインターフェイスにより簡単に変更できます。トポロジ マップにはデバイスの相互接続が図示されるほか、使用しきい値を超えているゾーン、VSAN、ISL などの設定情報がハイライト表示されます。また、CLI（コマンドライン インターフェイス）セッションの起動、SAN ポート チャネルの設定、Device Manager のオープンのビジュアル コンテキストも用意されています。

トポロジ マップの使用方法

Fabric Manager のトポロジ マップのファブリック表示は、すべてのスイッチ、エンド デバイス、およびリンクの表示から、スイッチ間の複数リンクを単一の太線で示したコア スイッチだけの表示まで、任意にカスタマイズできます。表示を変更するには、トポロジ マップの左側にあるアイコンを使用するか、トポロジ マップ内の任意の場所を右クリックして表示されるマップ コントロールを使用します。

トポロジ マップを拡大または縮小して、SAN の全体図を表示したり、重要な領域だけを拡大して表示できます。また、ファブリック全体を示すオーバービュー ウィンドウを開くこともできます。このウィンドウ内を右クリックし、表示したい領域をボックスで囲んで指定すれば、その領域をメインのトポロジ マップ ビューに表示できます。

Logical Domains ペインからファブリックまたは VSAN を選択し、トポロジ表示の範囲を限定することもできます。選択したファブリックまたは VSAN だけがトポロジ マップに表示されます。

リンクまたはスイッチ上にマウス ポインタを移動すると、その SAN コンポーネントの簡単な説明がステータス情報とともに表示されます。コンポーネント上を右クリックすると、ポップアップ メニューが表示されます。コンポーネントの詳細情報を表示したり、コンポーネントの設定を聞いたり、そのコンポーネントの機能をテストすることができます。

リンクをダブルクリックすると、Information ペインにリンクのステータスおよび設定情報が表示されます。スイッチをダブルクリックすると、そのスイッチの Device Manager が起動します。

カスタマイズしたトポロジ マップ レイアウトの保存

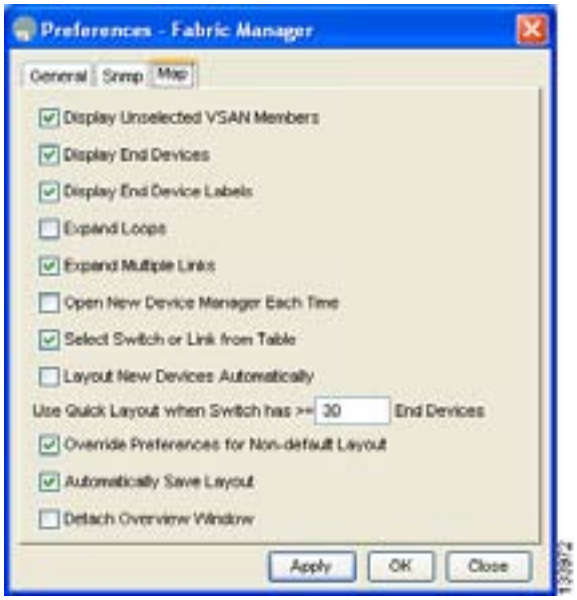
トポロジ マップの変更を保存しておくと、特定のファブリックの Fabric Manager クライアントの起動時に、いつでもカスタマイズしたビューを表示できます。

Fabric Manager を使用して、カスタマイズしたレイアウトを保存する手順は、次のとおりです。

ステップ 1　**File** > **Preferences** を選択し、Fabric Manager preferences ダイアログボックスを開きます。

ステップ 2　**Map** タブをクリックし、**Automatically Save Layout** チェックボックスをオンにして、トポロジ マップの変更を保存します（図 28-1 を参照）。

図 28-1　Fabric Manager のプリファレンス



ステップ 3　**Apply** をクリックし、次に **OK** をクリックして変更を保存します。

Fabric Manager トポロジ マップでのラックの使用

すべてのデバイスが FC-GS-3 リクエストに応答できるわけではないので、単一のサーバまたはストレージ サブシステム上の異なるポートが、トポロジ マップ上に個々のエンド デバイスとして表示されることがあります。これらのポートを Fabric Manager 用の単一ラックにグループ化する方法については、「デバイス グループの変更」（p.5-23）を参照してください。

Alias -> Enclosure を選択すると、ホストおよびストレージ エレメントが Information ペインに表示されます。これはラックの名前を指定するためのショートカットです。このショートカットを使用するには、ホストまたはストレージのテーブルで単一ラックとしてグループ化する各行をハイライト表示し、**Alias -> Enclosure** を選択します。選択した各行のラック名として、エイリアスの最初のトークンが自動的に設定されます。

複数ファブリックのマッピング

複数のファブリックにログインするには、同じユーザ名およびパスワードを使用する必要があります。シード スイッチを選択しなくても、両方のファブリックの情報が表示されます。ファブリックの詳細を表示するには、Fabric ペインの下部で、そのファブリックのタブを選択するか、またはファブリックのクラウド アイコンをダブルクリックします。

引き続き Fabric Manager を使用してファブリックを管理するには、「Fabric Manager Server ファブリックの管理」（p.3-5）の手順に従います。

コンポーネント管理

Fabric Manager の Information ペインには、ファブリック内のすべてのスイッチ、リンク、およびホストのコンポーネント、設定、およびステータス情報が表示されます。コンポーネント管理には、ベンダーの名前とモデル、およびソフトウェアまたはファームウェアのバージョンが含まれます。ファブリック内の VSAN、スイッチ、ホスト、およびストレージ エレメントの数を表示するには、Logical Domains ペインでファブリックまたは VSAN を選択し、Information ペインで **Summary** タブを選択します。Fabric Manager のユーザ インターフェイスの詳細は、「Fabric Manager Client の概観」（p.5-8）を参照してください。

Fabric Manager Web Server からの Inventory タブの使用方法

Fabric Manager Web Server が設定されていれば、このアプリケーションを起動して Inventory タブを選択し、Fabric Manager Server が管理しているファブリックのサマリーを表示できます。Inventory タブには、選択した SAN、ファブリック、またはスイッチのコンポーネントが表示されます。

Fabric Manager Web Server の設定および使用方法の詳細については、『*Cisco MDS 9000 Family Fabric Manager Configuration Guide* 』を参照してください。

Fabric Manager Web Server を使用してシステム メッセージをリモートで表示する手順は、次のとおりです。

ステップ 1　Fabric Manager Web Server で使用するブラウザを指定します。

ステップ 2　**Events** タブをクリックし、次に **Details** を選択するとシステム メッセージが表示されます。

イベント テーブル内のカラムはソートできます。また、Filter ボタンを使用して、テーブル内のメッセージの範囲を制限できます。

Device Manager からのログの表示

Fabric Manager Server と同じワークステーションから Device Manager を実行している場合には、Device Manager からシステム メッセージを表示できます。Device Manager で **Logs** > **Events** > **current** を選択すると、システム メッセージが表示されます。イベント テーブル内のカラムはソートできます。また、Find ボタンを使用して、テーブル内のテキストを検索できます。

スイッチに保存されているログは、ローカル Syslog サーバが設定されていなくても、またはスイッチの Syslog サーバ リストにローカル PC が含まれていなくても表示できます。ただし、メモリに制限があるので、特定のサイズに達すると古いログは消去されます。スイッチの Syslog には、2 つのログがあります。Critical 以上の重大度のメッセージが限定数だけ保存される NVRAM（不揮発性 RAM）ログ、および Notice 以上の重大度のメッセージが保存される非永続的なログです。ハードウェア メッセージは、これらのログに含まれます。

ヘルスおよびイベント モニタリング

Fabric Manager では、Cisco SAN スイッチと連動して、ファブリックおよびスイッチのヘルスおよびステータスを表示できます。ファブリックおよびコンポーネントの情報は、Online System Health Management、Call Home、システム メッセージ、および SNMP 通知など、複数の情報源から収集されます。これらの情報は、Fabric Manager または Device Manager の複数のメニューから表示できます。

Fabric Manager Events タブ

topology ウィンドウから使用できる Fabric Manager Events タブには、Fabric Manager がファブリック内の情報源から受信したイベントが表示されます。情報源には、SNMP イベント、RMON イベント、システム メッセージ、システム ヘルス メッセージが含まれます。Events タブには、イベント名、イベントの発信元および時刻、重大度、イベントの説明を含むイベント テーブルが表示されます。テーブルは、任意のカラムのヘッダーによりソートできます。

Fabric Manager Web Server Report のイベント情報

Fabric Manager Web Server のクライアントに、Performance Manager により収集された情報を表示できます。この情報には、ファブリックから Fabric Manager Server に送信されたイベントが含まれています。レポートを表示するには、**Performance Manager** > **Reports** を選択します。ブラウザ上に Web クライアントが開き、Fabric Manager Server がモニタしているすべてのファブリックのサマリーが表示されます。特定のファブリックを選択して **Events** タブを選択すると、選択したファブリックで発生したイベントのサマリーまたは詳細レポートを表示できます。サマリーには、ファブリック上でダウンしているスイッチ数、ISL 数、ホスト数、またはストレージ エレメント数、およびその SAN エンティティに対してロギングされた警告メッセージ数が表示されます。詳細ビューには、ファブリックからロギングされたすべてのイベントのリストが表示されます。表示するイベントは重大度、時刻範囲、タイプによって制限できます。

Device Manager のイベント

Device Manager で **Logs** > **Events** を選択すると、イベントが表示されます。Device Manager では、現在のイベントのリスト、または Fabric Manager のホストに保管されている古いイベント リストを表示できます。イベント テーブルには、時刻、情報源、重大度、簡単な説明を含む各イベントの詳細が表示されます。

CHAPTER 29

Performance Manager

Fabric Manager の主な目的は、ネットワークを管理することです。管理機能の中で重要なのは、ネットワーク パフォーマンス モニタリング機能です。この章の内容は、次のとおりです。

- Performance Manager の概要（p.29-2）
- フロー統計情報の設定（p.29-5）

Performance Manager の概要

Performance Manager はネットワーク デバイスの統計情報の履歴を収集し、Web ブラウザを使用してこの情報をグラフィック表示します。最近の統計情報は詳細が、古い統計情報はサマリーが表示されます。Performance Manager は Cisco Traffic Analyzer などの外部ツールとも統合されています。

Performance Manager には、3 つの処理ステージがあります。

- 定義 — Flow Wizard でスイッチにフローをセットアップします。
- 収集 — Web Server Performance Collection 画面で目的のファブリックに関する情報を収集します。
- 提示 — Fabric Manager Web Server を通じて、収集したデータを表示する Web ページを生成します。

Performance Manager は ISL（スイッチ間リンク）、ホスト、ストレージ エレメント、および設定済みフローの統計情報を収集できます。フローの定義基準は、ホストからストレージ（またはストレージからホスト）のリンクです。Performance Manager は収集コンフィギュレーション ファイルに基づいて、ファブリックから統計情報を収集します。これらのファイルにより、Performance Manager が統計情報を収集する Storage Area Network（SAN; ストレージ エリア ネットワーク）エレメントおよび SAN リンクが決まります。この設定に基づいて、Performance Manager は適切なデバイス（スイッチ、ホスト、またはストレージ エレメント）と通信し、5 分間の規定時間内に適切な情報を収集します。

Performance Manager はラウンドロビン データベースを使用して、ファブリックから収集された統計データを保持します。このデータは収集コンフィギュレーション ファイル内で設定されたパラメータに基づいて、格納されます。ポーリング インターバルごとに、Performance Manager は関連する統計情報を収集し、ラウンドロビン データベース内に格納します。このデータベースのサイズは固定されていて、設定された上限を超えることはありません。

Performance Manager は一連のアーカイブ データを作成し、リアルタイム ラウンドロビン データベース内のサマリー情報を保持します。このアーカイブ データを使用して、日次、週次、月次、および年次の統合レポートが生成されます。Performance Manager はこの方法を使用して、重要な履歴データを維持します。増え続けるデータベース サイズを拡張するためのコストは不要です。

（注） Fabric Manager Server でユーザ証明書を変更する場合は、Performance Manager を再起動する必要があります。

ここで説明する内容は、次のとおりです。

- データ補間（p.29-3）
- データ収集（p.29-3）
- パフォーマンスしきい値の使用方法（p.29-3）
- フロー セットアップ ウィザード（p.29-4）

データ補間

Performance Manager 固有の機能の 1 つとして、統計的なポーリング結果が失われたり、遅延した場合にデータを補間する機能があります。その他のパフォーマンス ツールでは失われたデータ ポイントがゼロとして格納されることがありますが、この方法では過去の傾向が正しく反映されないことがあります。Performance Manager は失われたデータの前のデータ ポイントと、失われたデータのあとのポーリング インターバル中に格納されたデータ ポイントを比較して、失われたデータ ポイントを補間します。これによって、パフォーマンス情報の継続性が保たれます。

データ収集

2 つの変数（受信バイト数と送信バイト数）に関するデータを 1 年分収集するには、76 KB のサイズの Round-Robin Database（RRD）ファイルが必要です。エラーおよび廃棄数も収集する場合、RRD ファイル サイズは 110 KB になります。デフォルト内部値は次のとおりです。

- 5 分間のサンプル× 600 回（2 日と 2 時間）
- 30 分間のサンプル× 700 回（12.5 日）
- 2 時間のサンプル× 775 回（50 日）
- 1 日のサンプル× 300 回

1000 ポート SAN の履歴データを、エラー数および廃棄数を含めて 1 年分収集するには、110 MB が必要です。この SAN にファブリック ポートが同じように配置された 20 台のスイッチが存在する場合、データを監視するために、スイッチごとに約 2 ～ 3 個の SNMP（簡易ネットワーク管理プロトコル）パケット、合計で約 100 個の要求 / 応答 SNMP パケットが 5 分おきに送信されます。

変数カウンタ要求が関係するため、フローのストレージ スペース要件の予測は困難です。フローが追加されるたびに 76 KB 増加します。

（注） Performance Manager は、管理不能なスイッチおよび他社製スイッチに関する統計情報は収集しません。ループ デバイス（FL/NL）は収集されません。

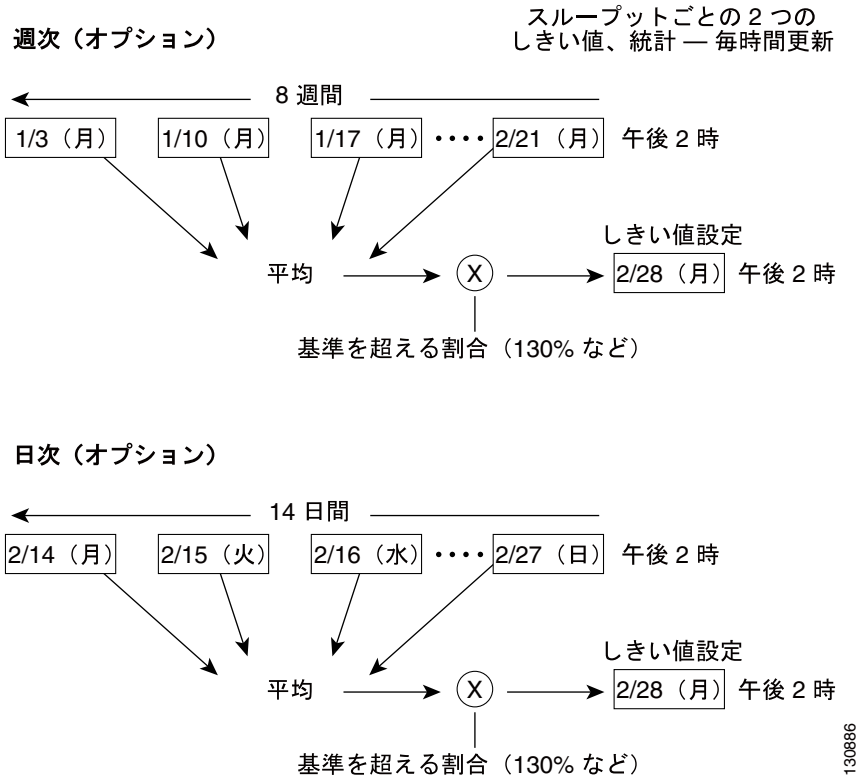
パフォーマンスしきい値の使用方法

Performance Manager Configuration Wizard では、監視対象のトラフィックが、設定した利用率を超えた場合にイベントをトリガーする 2 つのしきい値を設定できます。イベント トリガーは、Fabric Manager Web クライアントの Events ブラウザ ページに通知される Critical または Warning のどちらかのイベントとして設定します。

絶対値しきい値は、収集された統計情報に直接適用されます。統計情報が、合計リンク容量のパーセンテージとして、しきい値に設定された利用率と比較されます。統計が、設定されたしきい値を超えていると、Fabric Manager Web クライアントの Events タブにイベントが表示されます。

同じタイム ウィンドウ（毎日、毎週、または 2 週間おき）のリンクごとに、典型的なトラフィック パターンに適合するしきい値が、基準しきい値に基づいて作成されます。基準しきい値は平均の割合（110% ～ 500%）として設定されます。100% は計算された重み付き平均です。図 29-1 に、毎週または毎日のオプションに対応する基準しきい値の設定例を示します。

図 29-1　基準しきい値の例



しきい値を、月曜日午後 2 時に関して設定し、基準しきい値はこの統計情報の平均の 130% に設定します。平均は、これまでの月曜午後 2 時に発生した統計値（毎週を選択した場合）、またはこれまでの毎日午後 2 時に発生した統計値（毎日を選択した場合）から計算されます。

フロー セットアップ ウィザード

Performance Manager Flow および Performance Manager Setup Wizard を使用すると、設定が大幅に簡単になります。必要な処理は、取り込む統計情報のカテゴリを選択することのみです。この選択を行うと、監視するフローおよびリンクのリストが表示されます。必要に応じてエントリを削除したり、表示されたリストを単に受け入れてデータ収集を開始できます。ホストおよびストレージ リンクの統計情報はスイッチ上の特定のポートと関連していないため、接続を別のポートに移動した場合、長期間の統計情報が失われることはありません。

フロー統計情報の設定

フロー統計では、集約統計テーブルの入力トラフィックがカウントされます。収集できる統計情報は次の 2 種類です。

- 集約フロー統計（VSAN のトラフィックをカウント）
- フロー統計（VSAN の送信元と宛先の ID ペアをカウント）

ここで説明する内容は、次のとおりです。

- フロー統計の概要（p.29-5）
- フロー統計のカウント（p.29-5）

フロー統計の概要

フロー カウンタをイネーブルにすると、集約フロー統計とフロー統計に最大 1024 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 インデックスの数値スペースは集約フロー統計とフロー統計で共用されます。

表 29-1 に、監視対象のトラフィックのタイプを定義する Flow Type オプション ボタンの説明を示します。

表 29-1　Performance Manager のフロー タイプ

フロー タイプ	説明
Host->Storage	ホストからストレージ エレメントまでのデータを監視する一方向フロー
Storage->Host	ストレージ エレメントからホストまでのデータを監視する一方向フロー
Both	ホストとストレージ エレメント間のデータを監視する双方向フロー

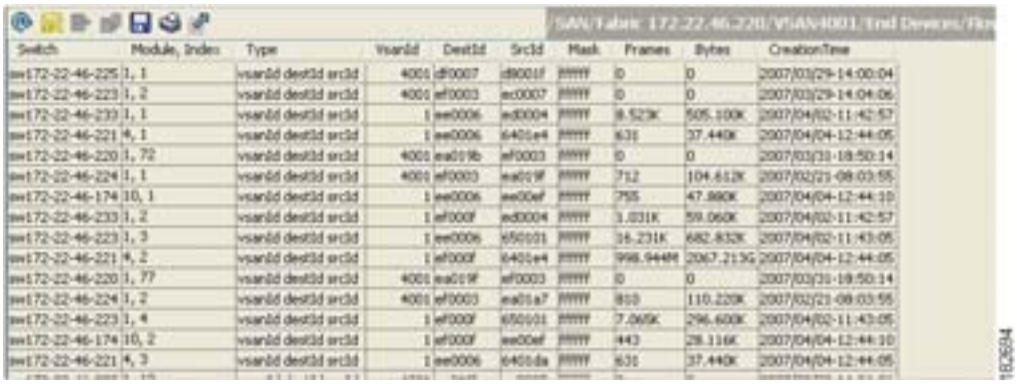
フロー統計のカウント

Fabric Manager を使用してアクティブ ゾーン セットをカウントする手順は、次のとおりです。

ステップ 1　**End Devices** を展開してから、Physical Attributes ペインの **Flow Statistics** を選択します。

フロー統計が表示されます（図 29-2 を参照）。

図 29-2　Fabric Manager のフロー統計



ステップ 2　**Create** アイコンをクリックして、フローを作成します。

(注)　Performance Manager を使用してファブリックを管理する場合は、ファブリック上でフローおよび収集の初期セットを設定する必要があります。

(注)　フローの作成時には、デバイス タイプが正しく設定されていることを確認してください。

Define Traffic Flows ダイアログボックスが表示されます（図 29-3 を参照）。

図 29-3　Define Traffic Flows ダイアログボックス

ステップ 3　フローを作成する VSAN を選択します。フローはアクティブ ゾーン セット単位で定義されます。

ステップ 4　定義したいフロー タイプの **Type** オプション ボタンをクリックします。

ステップ 5　（任意）既存のフロー データを削除する場合には、**Clear old flows on modified switches** チェックボックスをオンにします。

ステップ 6　（任意）柔軟性を高めるためにすべてのカード上のフローを作成する場合は、**Create flows on all cards** チェックボックスをオンにします。

ステップ 7　**Next** をクリックし、選択した VSAN で使用できるフローを確認します。

Review Traffic Flows ダイアログボックスが表示されます（図 29-4 を参照）。

図 29-4　Review Traffic Flows ダイアログボックス

ステップ 8　不要なフローを削除します。

ステップ 9　**Finish** をクリックして、フローを作成します。

CHAPTER 30

Nexus 5000 管理ソフトウェアの FAQ

この章では、Cisco Fabric Manager および Device Manager に関する主な FAQ について回答します。この章の内容は、次のとおりです。

- Nexus 5000 シリーズの問題
- Fabric Manager の一般的な問題

Nexus 5000 シリーズの問題

ここでは、Nexus 5000 シリーズ スイッチに特有の問題について説明します。次の内容が含まれます。

- Display FCoE モードについて（p.30-2）
- Display FCoE モードへのスイッチング（p.30-2）

Display FCoE モードについて

Fabric Manager が Display FCoE モードを実行している場合、Fabric Manager は新たにツリー ノード、メニュー項目、ツールバー ボタン、および Fibre Channel over Ethernet（FCoE）に関連したトポロジ ノード / リンクを表示します。

これらの機能には、次の内容が含まれます。

- Virtual Interface Group（VIG）ウィザードおよび Virtual Interface ウィザード ツールバー ボタンおよびメニュー項目の表示
- Physical Attributes ツリーの VIG および仮想インターフェイス ツリー ノードの表示
- トポロジの FCoE リンクを二点鎖線として表示
- トポロジの異なるアイコンを使用した Nexus 5000 シリーズ スイッチの表示

Display FCoE モードへのスイッチング

Fabric Manager を Display FCoE モードにスイッチングする手順は、次のとおりです。

- server.properties ファイルを編集します。このファイルは、Fabric Manager サーバの <installation directory>/conf フォルダにあります。
- 「displayFCoE」のテキストによるファイルを検索します。「displayFCoE」は FCoE プロパティを表示します。
- displayFCoE プロパティを **true** に変更します。
- ファイルを保存し、エディタを終了します。
- Fabric Manager サーバを再起動します。

これらの手順を完了すると、ファイルには次の行が含まれます。

```
# FM Client and Server Attributes
# Display FCoE feature related tree nodes, menu items, toolbar buttons,
topology nodes/links if Nexus 5k switches are present in the fabric
displayFCoE = true
```

Fabric Manager の一般的な問題

Fabric Manager の FAQ の詳細については、次の URL にある『*Management Software FAQ*』を参照してください。

http://cisco.com/en/US/docs/storage/san_switches/mds9000/sw/rel_3_x/configuration/guides/fm_3_2/tsfm.html

CHAPTER 31

ファブリックのトラブルシューティング

この章では、スイッチの問題を解決するために使用する基本的なトラブルシューティング方法について説明します。この章の内容は、次のとおりです。

- トラブルシューティングのツールおよび技術（p.31-2）
- スイッチ デバイス状態の分析（p.31-4）
- スイッチ ファブリック設定の分析（p.31-5）
- エンドツーエンド接続の分析（p.31-7）
- ping ツールの使い方（fcping）（p.31-9）
- Trace Route（fctrace）などのトラブルシューティング ツールの使い方（p.31-10）
- ゾーン マージ結果の分析（p.31-11）
- show tech support コマンドの使用（p.31-12）
- CLI コマンドの実行（p.31-14）
- その他のスイッチの検索（p.31-16）
- ファイバ チャネルの TOV（p.31-18）
- ファブリック アナライザの設定（p.31-21）
- WWN の設定（p.31-27）
- セカンダリ MAC アドレスの設定（p.31-28）
- HBA の FC ID 割り当て（p.31-29）
- デフォルト設定（p.31-29）

トラブルシューティングのツールおよび技術

シスコ スイッチの監視およびトラブルシューティングには、複数の技術およびツールを使用できます。これらのツールは完全な統合型マルチレベル分析ソリューションを提供します。

Fabric Manager Server — Cisco Fabric Manager Server は、ストレージ ネットワーク パフォーマンスに関する長期の詳細情報を提供します。ファブリック全体のパフォーマンス傾向を分析するには、Performance Manager を使用します。これは、ネットワークのホットスポットを解決するための、より詳細な分析の開始ポイントになります。

Device Manager — Fabric Manager Server によってパフォーマンスの問題が検出された場合には、Cisco Device Manager を使用して、ポート単位の統計情報をリアルタイムで表示できます。プロトコルの詳細、エラー数、廃棄数、バイト数、およびフレーム数が表示されます。サンプリングは 2 秒おきに実行でき、値はテキスト形式、または円グラフ、棒グラフ、面グラフ、折れ線グラフで表示できます。

Traffic Analyzer — Fabric Manager Server からファイバ チャネル用 Cisco Traffic Analyzer を起動して、トラフィックを詳細に分析することもできます。Cisco Traffic Analyzer を使用すると、VSAN（仮想 SAN）およびプロトコル別にトラフィックを分類して、Logical Unit Number（LUN）レベルで SCSI トラフィックを調べることができます。

Protocol Analyzer — より詳細な調査が必要な場合は、Cisco Traffic Analyzer のコンテキスト内でファイバ チャネル用 Cisco Protocol Analyzer を起動することができます。Cisco Protocol Analyzer を使用すると、ファイバ チャネルおよび Wireshark 用にシスコ社が開発した SCSI デコーダを使用して、ファイバ チャネル フレームの実際のシーケンスを容易に調査できます。

Port Analyzer Adapter（PAA） — Fabric Manager Server および Device Manager は SNMP（簡易ネットワーク管理プロトコル）を使用して統計情報を収集します。内蔵のスイッチ統計情報カウンタがすべて活用されます。

Cisco Traffic Analyzer と Cisco Protocol Analyzer を統合すると、ファイバ チャネル トラフィックそのものを分析でき、スイッチ分析機能が拡張されます。シスコの Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）は、他の機能に影響しない柔軟な技術によってこれらのソリューションを実現し、1 つまたは複数のポートからファブリック内の別のスイッチ ポートに、選択的にトラフィックをミラーリングできます。

Cisco PAA は、SPAN トラフィックをイーサネット ヘッダーにカプセル化し、分析できるように PC またはワークステーションに転送します。SPAN を使用した場合は、ファイバ チャネルの制御トラフィックおよびデータ プレーン トラフィックを使用できます。イーサネット パケットは PAA によってブロードキャストされるので、IP ネットワーク間ではルーティングできません。ハブおよびスイッチは、同じイーサネット サブネット内にある場合に使用できます。PAA と PC 間の直接接続もサポートされています。PAA ではファイバ チャネル データが切り捨てられるため、イーサネット トラフィックを削減できます。

Cisco Traffic Analyzer および Cisco Protocol Analyzer では、SPAN トラフィックを PC またはワークステーションにトランスポートするために PAA が必要です。

（注） Cisco Traffic Analyzer は Cisco PAA 2 と組み合わせた場合に最適に機能します。これは、切り捨てられたデータ長が Cisco PAA 2 によって提供され、正確なバイト数の報告が可能になるためです。

Cisco Traffic Analyzer

ファイバ チャネル用 Cisco Traffic Analyzer は SPAN トラフィック、または Cisco Protocol Analyzer を使用してキャプチャされたトラフィックのリアルタイム分析を実行します。複数の Cisco PAA からのファイバ チャネル トラフィックを集約して、Cisco Traffic Analyzer で分析できます。

1 つの SPAN 宛先ポートに送信できる SPAN 発信元数には制限があります。集約により、Cisco Traffic Analyzer が統合レポート セットで分析可能な情報量が拡張されます。

（注） 集約機能は、単一 PC とのイーサネット接続によって収集される情報に限定されます。複数の PC 間で集約することはできません。

Cisco Traffic Analyzer は Web サーバを介してレポートを表示するため、レポートはローカルまたはリモートで表示できます。トラフィック分析機能は「ntop」オープンソース ソフトウェアによって提供されます。このソフトウェアは、ファイバ チャネルと SCSI の分析、および拡張された SPAN 用 ISL（スイッチ間リンク）ヘッダー サポートを追加するためにシスコが拡張した機能です。ntop は Cisco.com ソフトウェア ダウンロード センターの Cisco Port Analyzer Adapter から入手できます。また、インターネット（http://www.ntop.org/ntop.html）から入手することもできます。シスコの拡張 ntop は、Microsoft Windows および Linux の各オペレーティング システムで稼働します。

ファイバ チャネル用 Cisco Traffic Analyzer は、ネットワーク全体の統計情報に関するレポートを表示します。Summary Traffic レポートには、フレーム サイズ範囲ごとのトラフィックの割合が表示されます。トラフィックの割合は、SCSI、ELS などのプロトコルごとに分類されます。分析中の SPAN トラフィックの平均スループットおよびピーク スループットも表示されます。

Cisco Traffic Analyzer を使用すると、VSAN 単位でファイバ チャネル トラフィックを分析できます。Domain Traffic Distribution グラフは、特定の VSAN のスイッチで送受信されたトラフィック量（バイト）を示します。FC Traffic Matrix グラフは、ファイバ チャネルの発信元と宛先の間で送受信されたトラフィック量を示します。VSAN ごとの合計バイト数およびフレーム数も表示されます。

ホストおよびストレージ ポートごとに統計情報を分析できます。SCSI 読み取りトラフィックと書き込みトラフィックの割合、SCSI トラフィックとその他のトラフィックの割合、および送信バイト / フレームと受信バイト / フレームの割合を表示できます。各ポートで送受信されたデータのピークおよび平均スループット値を表示できます。

Cisco Protocol Analyzer

ファイバ チャネル用 Cisco Protocol Analyzer を使用すると、ファイバ チャネル トラフィック フレームをリアルタイムで表示したり、またはキャプチャ ファイルから取り込んで表示することができます。ファイバ チャネルおよび SCSI デコーダにより、トラフィックをフレーム レベルで表示および分析できます。完全にデコードするために応答と要求が比較され、ナビゲーションが大幅に簡単になります。応答とステータス間の応答時間が表示されます。

Cisco Protocol Analyzer は VSAN を認識するため、VSAN をキャプチャおよびディスプレイ フィルタの基準として使用することができます。カラムに VSAN 番号も表示できます。プロトコル配信割合や、特定のファイバ チャネル発信元と宛先ペア間で転送される合計バイトまたはフレーム数に関するサマリー統計情報を表示できます。ファイル キャプチャおよびフィルタリング制御も実行できます。キャプチャされたファイルは、Cisco Protocol Analyzer または Cisco Traffic Analyzer で分析できます。

操作が簡単な多数の機能が追加されています。特定の基準を満たすフレームを検索して、マークを付けることができます。フレーム（パケット）リストのエントリを色分けして、目的の項目を強調したり、必要に応じてカラムを追加または削除することができます。

プロトコル分析機能は Wireshark オープンソース ソフトウェアによって提供されます。このソフトウェアは、ファイバ チャネルおよび SCSI プロトコルをデコードしたり、SPAN 用の拡張 ISL ヘッダーをサポートしたりするために、シスコによって拡張されたものです。Wireshark は Cisco.com ソフトウェア ダウンロード センターの Cisco Port Analyzer Adapter から入手できます。Wireshark はインターネット（http://www.wireshark.org）から入手することもできます。Wireshark は Microsoft Windows、Solaris、および Linux の各オペレーティング システムで稼働します。

スイッチ デバイス状態の分析

Switch Health オプションを使用すると、特定のスイッチのコンポーネント ステータスを判別できます。

Fabric Manager でスイッチ ヘルス オプションを使用して特定のスイッチのコンポーネント ステータスを判断する手順は、次のとおりです。

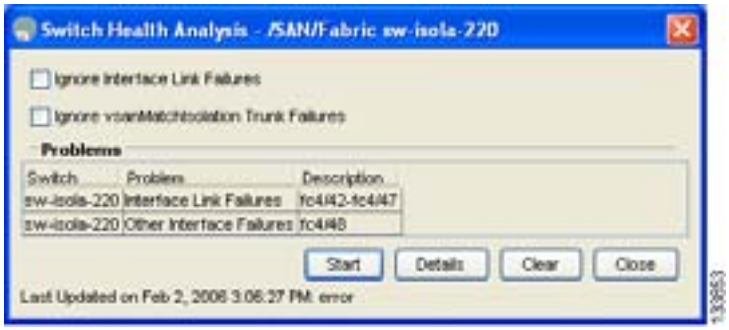
ステップ 1　**Tools** > **Switch Health** を選択します。

Switch Health Analysis ウィンドウが表示されます。

ステップ 2　**Start** をクリックして、選択したスイッチに現在影響を与えている問題を調べます。

Switch Health Analysis ウィンドウに問題が表示されます（図 31-1 を参照）。

図 31-1　Switch Health Analysis の結果



ステップ 3　**Clear** をクリックして、Switch Health Analysis ウィンドウの内容を削除します。

ステップ 4　**Close** をクリックして、ウィンドウを閉じます。

スイッチ ファブリック設定の分析

Fabric Configuration オプションを使用すると、現在の設定を特定のスイッチまたはポリシー ファイルと比較して、スイッチの設定を分析することができます。スイッチの設定をファイルに保存し、ファイル内の設定とすべてのスイッチを比較することができます。

Fabric Manger で Fabric Configuration オプションを使用してスイッチの設定を分析する手順は、次のとおりです。

ステップ 1　**Tools** > **Fabric Configuration** を選択します。

Fabric Configuration Analysis ダイアログボックスが表示されます。

ステップ 2　選択したスイッチを別のスイッチと比較するか、またはポリシー ファイルと比較するかを決定します。

- スイッチと比較する場合は、**Policy Switch** をオンにし、ドロップダウン矢印を選択して、スイッチのリストを表示します。
- ポリシーと比較する場合は、**Policy File** を選択します。このオプションの右にある **...** ボタンをクリックして、ファイル システムをブラウズし、ポリシー ファイル（*.XML）を選択します。

ステップ 3　**Rules** をクリックして、Fabric Configuration Analysis ツールを実行する場合に適用する規則を設定します。

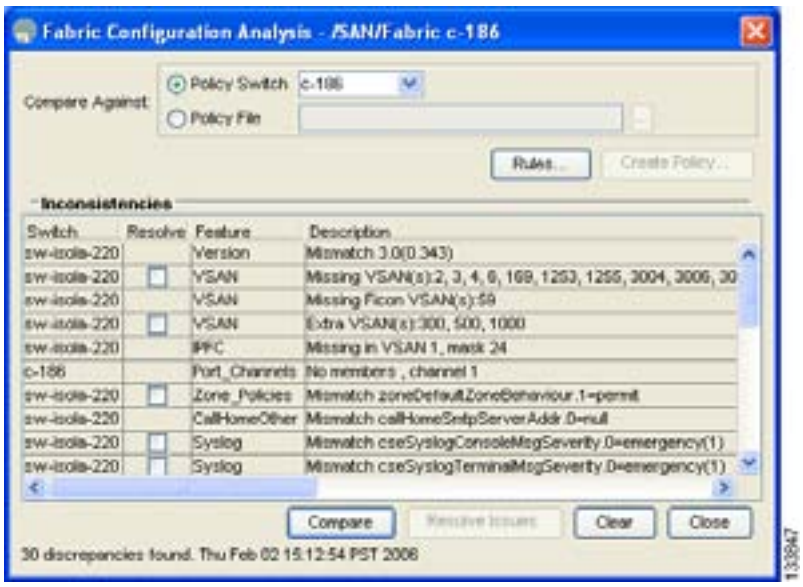
Rules ウィンドウが表示されます。

ステップ 4　必要に応じて規則を変更し、**OK** をクリックします。

ステップ 5　**Compare** をクリックします。

設定が分析され、比較によって検出された問題点が表示されます（図 31-2 を参照）。

図 31-2　Fabric Configuration Analysis の結果



ステップ 6　解決する問題点に対応する Resolve カラムのチェックボックスをオンにします。

ステップ 7　この問題を解決するには、**Resolve Issues** をクリックします。

ステップ 8　**Clear** をクリックして、ウィンドウの内容を削除します。

ステップ 9　**Close** をクリックして、ウィンドウを閉じます。

エンドツーエンド接続の分析

End to End Connectivity オプションを使用すると、スイッチ ファブリック内のデバイス間の接続およびルートを判別できます。接続ツールは ping テストを使用し、エンド デバイスの各ペアが同じ VSAN 内または同じアクティブ ゾーン内にあるかを調べて、各ペアが相互に通信可能かどうかをチェックします。このオプションは、ファイバ チャネル ネットワーク用に変更された ping および traceroute コマンドのバージョンを使用します。

Fabric Manager で End to End Connectivity オプションを使用して接続およびルートを判別する手順は、次のとおりです。

ステップ 1　**Tools** > **End to End Connectivity** を選択します。

End to End Connectivity Analysis ダイアログボックスが表示されます。

ステップ 2　接続を確認する VSAN を VSAN ドロップダウン リストから選択します。

ステップ 3　分析対象をすべてのアクティブ ゾーンにするか、またはデフォルト ゾーンにするかを選択します。

ステップ 4　**Ensure that members can communicate** をクリックして、選択されたエンド ポイント間のファイバ チャネルに ping を実行します。

ステップ 5　パケット数、各パケットのサイズ、およびタイムアウト（ミリ秒）を識別します。

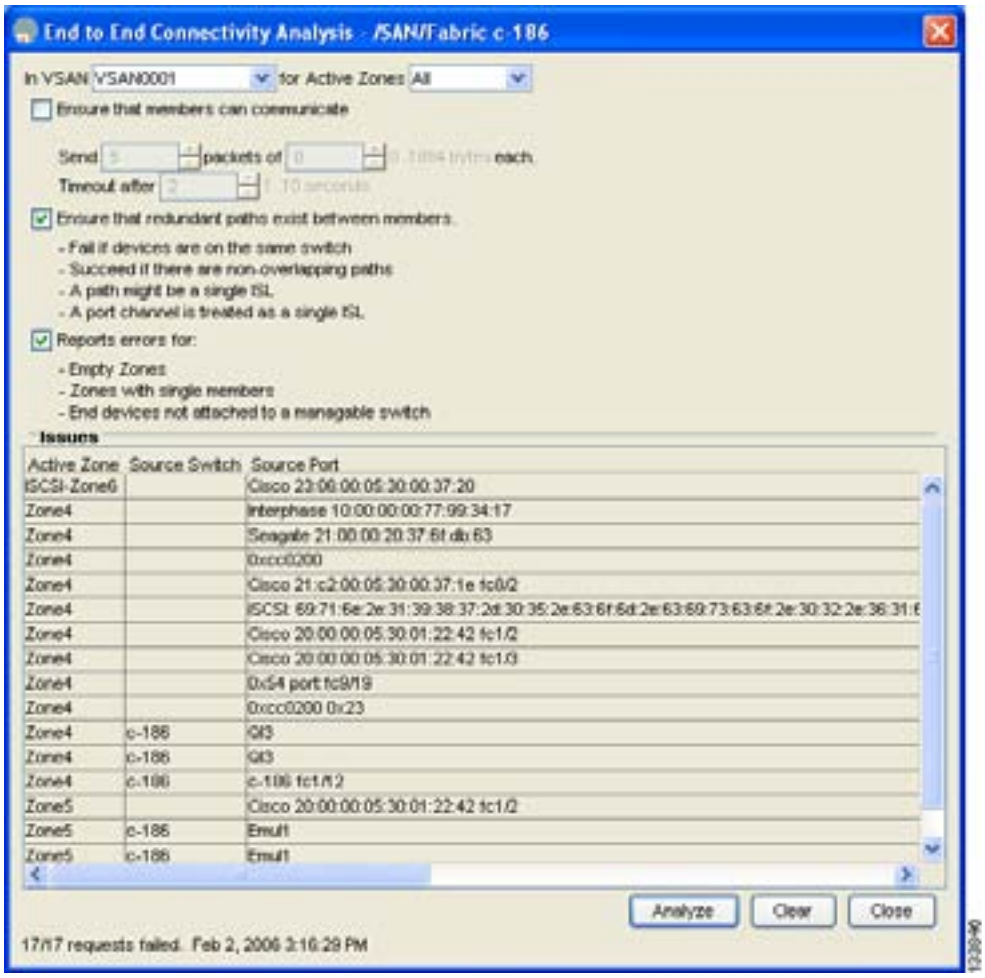
ステップ 6　**Ensure that redundant paths exist between members** チェックボックスをオンにして、エンドポイント間の冗長パスを分析します。

ステップ 7　**Report errors for** チェックボックスをオンにして、ゾーンおよびデバイス エラーのレポートを表示します。

ステップ 8　**Analyze** をクリックします。

End to End Connectivity Analysis ウィンドウに、選択されたエンド ポイントが接続先スイッチおよび接続に使用されている発信元および宛先ポートとともに表示されます。図 31-3 を参照してください。

図 31-3　End to End Connectivity Analysis の結果



出力には、失敗したすべての要求が表示されます。

- Ignoring empty zone — 空のゾーンには要求が発行されません。
- Ignoring zone with single member — メンバーが 1 つしかないゾーンには要求が発行されません。
- Source/Target are unknown — ポートに対応するネーム サーバが存在しないか、または検出中にポートが検出されませんでした。
- Both devices are on the same switch — 同一スイッチ上に両方のデバイスがあります。
- No paths exist between the two devices — 2 つのデバイス間にはパスが存在しません。
- VSAN does not have an active zone set and the default zone is denied — VSAN 上にアクティブ ゾーン セットがなく、デフォルトのゾーンが拒否されます。
- Average time micro secs — 遅延値が、指定されたしきい値を超過しました。

ステップ 9　**Clear** をクリックして、ウィンドウの内容を削除します。

ステップ 10　**Close** をクリックして、ウィンドウを閉じます。

ping ツールの使い方（fcping）

ping ツールを使用すると、別のスイッチから使用しているスイッチ上のポートの接続を確認できます。

Fabric Manager で ping ツールを使用して接続を確認する手順は、次のとおりです。

ステップ 1　**Tools** > **Ping** を選択します。

Fabric ペインでホストおよびストレージ デバイスを右クリックし、コンテキスト メニューから選択することもできます。

Ping ダイアログボックスが表示されます。

ステップ 2　Source Switch ドロップダウン リストで発信元スイッチを選択します。

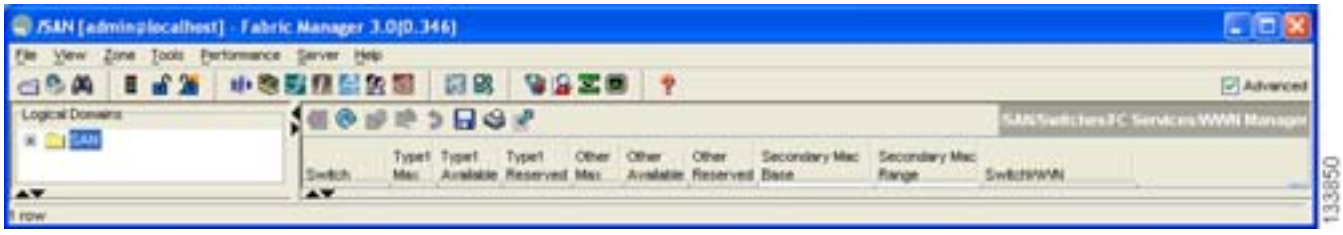
ステップ 3　VSAN ドロップダウン リストで、接続を確認する VSAN を選択します。

ステップ 4　Target Endport ドロップダウン リストで、接続を確認するターゲット エンド ポートを選択します。

ステップ 5　**Start** をクリックして、スイッチと選択したポート間に ping を実行します。

Ping Results ダイアログボックスが表示されます（図 31-4 を参照）。

図 31-4　ping の結果



ステップ 6　**Clear** をクリックしてウィンドウの内容をクリアし、新しい ping を実行します。または **Close** をクリックしてウィンドウを閉じます。

Trace Route（fctrace）などのトラブルシューティング ツールの使い方

Fabric Manager Tools メニューで次のオプションを使用すると、選択されたオブジェクトとの接続を確認したり、その他の管理ツールを開くことができます。

- Trace Route — Fabric ペインで現在選択されている 2 つのエンド デバイス間の接続を確認します。
- Device Manager — Fabric ペインで選択されたスイッチごとに Device Manager を起動します。
- Command Line Interface — Fabric ペインで選択されたスイッチとの Telnet または Secure Shell（SSH; セキュア シェル）セッションを開きます。

Fabric Manager で Trace Route オプションを使用して接続を確認する手順は、次のとおりです。

ステップ 1　**Tools** > **Trace Route** を選択します。

Trace Route ダイアログボックスが表示されます。

ステップ 2　Source Switch ドロップダウン リストで発信元スイッチを選択します。

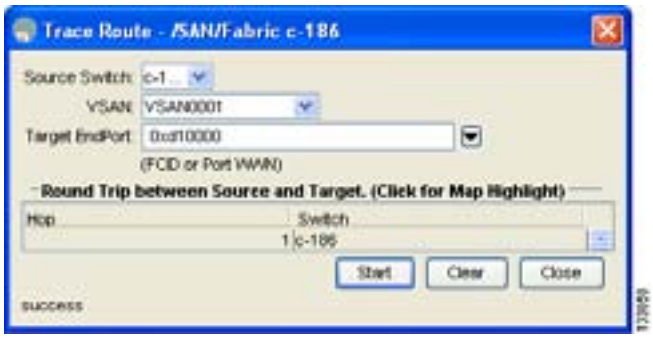
ステップ 3　VSAN ドロップダウン リストで、接続を確認する VSAN を選択します。

ステップ 4　Target Endport ドロップダウン リストで、接続を確認するターゲット エンド ポートを選択します。

ステップ 5　**Start** をクリックして、スイッチと選択したポート間の traceroute を実行します。

ダイアログボックスの下部に結果が表示されます（図 31-5 を参照）。

図 31-5　正しいトレース ルートの結果



ステップ 6　**Clear** をクリックしてウィンドウの内容をクリアし、新しい traceroute を実行します。または **Close** をクリックしてウィンドウを閉じます。

ゾーン マージ結果の分析

Zone メニューの Zone Merge オプションを使用すると、接続された 2 つのスイッチのゾーン設定に互換性があるかどうかを判別できます。

Fabric Manager で Zone Merge オプションを使用してゾーン設定に互換性があるかどうかを判別する手順は、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。

ステップ 2　各ドロップダウン リストでスイッチを選択します。

ステップ 3　ゾーン マージ分析を実行する VSAN を選択します。

ステップ 4　必要に応じてステップ 3 を繰り返します。

ステップ 5　**Analyze** をクリックします。

Zone Merge Analysis ウィンドウに、選択された 2 つのスイッチのゾーン設定に関する不整合が表示されます。図 31-6 を参照してください。

図 31-6　Zone Merge Analysis の結果

ステップ 6　**Clear** をクリックして、ウィンドウの内容を削除します。

ステップ 7　**Close** をクリックして、ウィンドウを閉じます。

show tech support コマンドの使用

show tech support コマンドは、ご使用のスイッチに関する大量の情報を収集してトラブルシューティングを行う場合に便利です。この出力は、テクニカル サポート担当者に問題を報告する場合に提供できます。

Fabric Manager では、ファブリック内の 1 つまたは複数のスイッチに対して **show tech support** コマンドを入力できます。各コマンドの結果は、指定したディレクトリ内のテキスト ファイル（各スイッチに 1 つずつ）に書き込まれます。これらのファイルを表示するには、Fabric Manager を使用します。

Fabric Manager マップを JPG ファイルとして保存することもできます。ファイルはシード スイッチの名前で保存されます（172.22.94.250.jpg など）。

すべてのファイル（**show tech support** コマンドの出力およびマップ ファイル イメージ）を zip ファイルに圧縮し、zip ファイルをテクニカル サポートに送信できます。

Fabric Manager で **show tech support** コマンドを入力する手順は、次のとおりです。

ステップ 1　**Tools > Show Tech Support** を選択します。

Show Tech Support ダイアログボックスが表示されます。

ステップ 2　各スイッチのチェックボックスをオンにして、テクニカル サポート情報を表示するスイッチを選択します。

ステップ 3　タイムアウト値を設定します。

デフォルトは 30 秒です。

ステップ 4　テキスト ファイル（**show tech support** コマンド情報を含む）を書き込むフォルダを選択します。

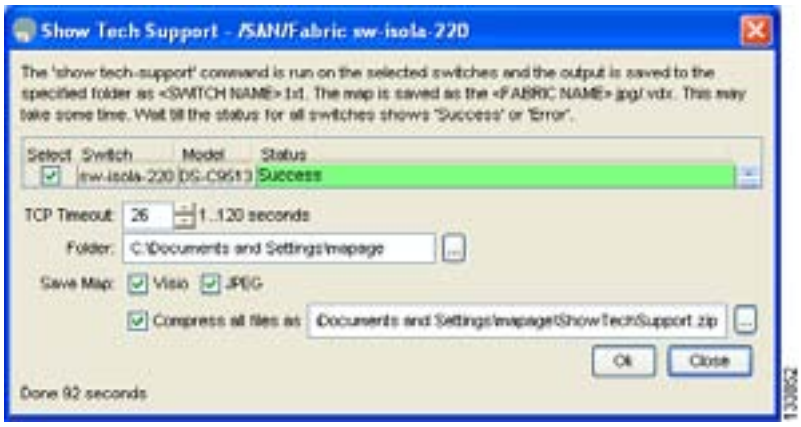
ステップ 5　マップのスクリーンショットを JPG ファイルとして保存する場合は、**Save Map** チェックボックスをオンにします。

ステップ 6　ファイルを zip ファイルに圧縮するには、**Compress all files as** チェックボックスをオンにします。

ステップ 7　指定したスイッチで **show tech support** コマンドを開始するには、**OK** をクリックします。**show tech support** コマンドを使用しないで Show Tech Support ダイアログボックスを閉じるには、**Close** ボタンをクリックします（図 31-7 を参照）。

各スイッチの横にある Status カラム内に、ステータスがハイライト表示されます。イエローのハイライト表示は、このスイッチ上で **show tech support** コマンドが現在実行中であることを示します。レッドのハイライト表示は、エラーを示します。図 31-7 に示すようなグリーンのハイライト表示は、**show tech support** コマンドが正常に終了したことを示します。

図 31-7　show tech support コマンドの正しい結果



ステップ 8　プロンプトが表示されたら、該当するスイッチのフィールドにユーザ名とパスワードを入力します。

（注）　Fabric Manager からスイッチに **show tech support** コマンドを正常に入力するには、スイッチにこのユーザ名およびパスワードを設定する必要があります。Fabric Manager はこのユーザ名およびパスワードが設定されていないスイッチにはログインできず、エラーが戻されます。

（注）　Fabric Manager を使用しないで **show tech support** ファイルを表示する場合は、任意のテキスト エディタでファイルを開くことができます。各ファイルには、スイッチの IP アドレスと .TXT 拡張子の名前が付いています（111.22.33.444.txt など）。

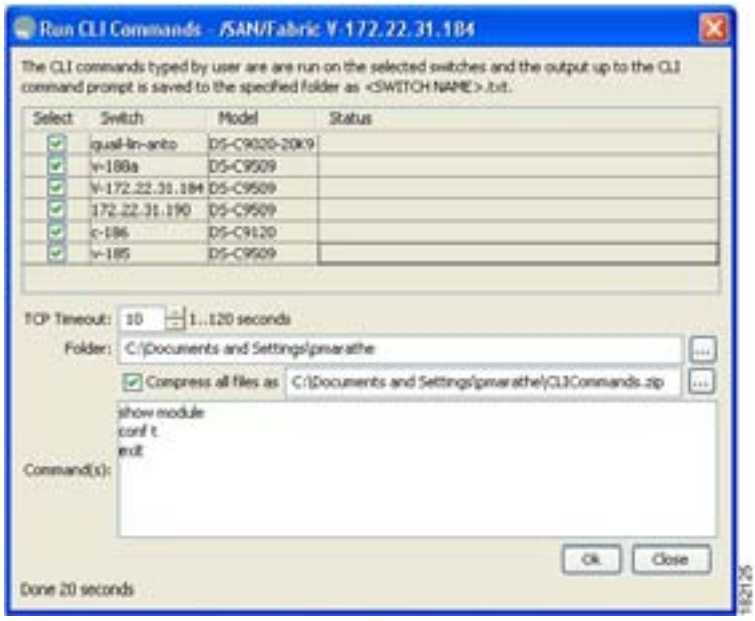
CLI コマンドの実行

Run CLI コマンド機能を使用して、複数のスイッチで CLI（コマンドラインインターフェイス）コマンドを実行できます。Fabric Manager を使用して CLI コマンドを実行する手順は、次のとおりです。

ステップ 1　**Tools** > **Run CLI Commands** を選択します。

すべてのスイッチが選択された Run CLI Commands ダイアログボックスが表示されます（図 31-8 を参照）。

図 31-8　Run CLI Commands ダイアログボックス



ステップ 2　CLI コマンドを実行しない場合は、スイッチのチェックボックスをオフにします。

ステップ 3　ファイルの保存場所を指定します。

（注）　スイッチごとにレポートが発行されます。レポートを見て、CLI コマンド エラー実行されていないことを確認します。

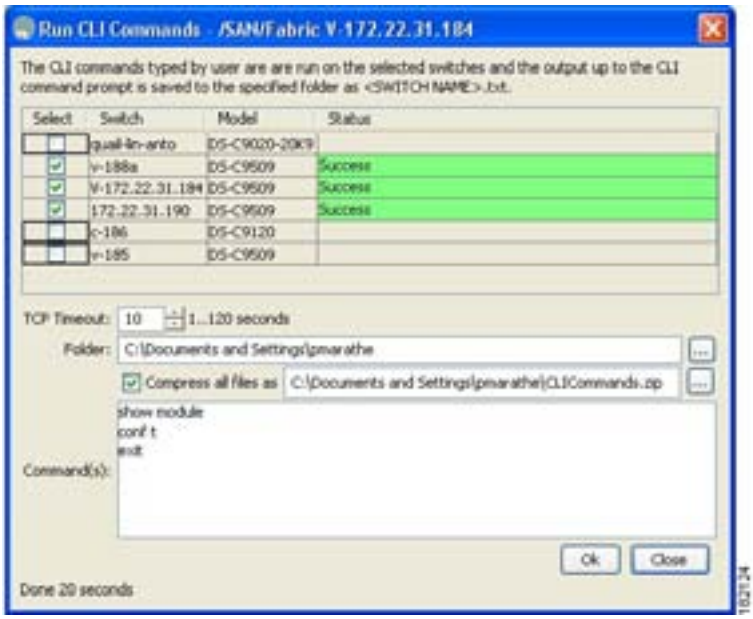
ステップ 4　Commands(s) テキスト ボックスにコマンドを入力します。入力するコマンドがコンフィギュレーションモード コマンドであれば、**exit** コマンドも入力します。

（注）　実行コマンドは、コンフィギュレーションモードでは指定できません。

ステップ 5　**OK** をクリックして CLI コマンドを実行します。

各スイッチのステータスを示す Run CLI コマンド ダイアログボックスが表示されます（図 31-9 を参照）。

図 31-9　Run CLI Commands ステータス



ステップ 6　**Close** をクリックして、ダイアログボックスを閉じます。

夏時間の調整

（注）　2007 年の米国夏時間は 3 月の第 2 日曜から始まり、11 月の第 1 日曜に終わります。

Fabric Manager の Run CLI コマンド機能を使用して、スイッチの時刻変更設定を行います。Command(s) テキスト ボックスに次のコマンドを入力します。

```
configure
no clock summer-time
clock summer-time daylight_timezone_name 2 Sunday March 02:00 1 Sunday November 02:00
60
```

その他のスイッチの検索

Locate Switches オプションは SNMPv2 を使用し、読み取り専用コミュニティ ストリング public を指定して、SNMP 要求に応答するデバイスを検出します。この機能を使用できるのは、次の場合です。

- 管理 IP アドレスを提供する FC-GS3 FCS 標準が実装されていないサードパーティ製スイッチが含まれている場合
- サブネット内のその他のシスコ スイッチを検出する必要があるにもかかわらず、ファブリックに物理的に接続されていない場合

Fabric Manager を使用して現在検出されているファブリックに含まれないスイッチを検出する手順は、次のとおりです。

ステップ 1　**File > Locate Switches and Devices** を選択します。

Locate Switches ダイアログボックスが表示されます。

ステップ 2　Comma Separated Subnets フィールドに特定のサブネットに属す特定のアドレス範囲を入力して、スイッチの検索範囲を制限します。

サブネット 192.168.199.0 に属すシスコ スイッチを検索するには、次のストリングを使用します。

192.168.100.[1-254]

カンマで区切って、複数の範囲を指定できます。たとえば、2 つのサブネット 192.168.199.0 および 192.169.100.0 内のすべてのデバイスを検索するには、次のストリングを使用します。

192.168.100.[1-254], 192.169.100.[1-254]

ステップ 3　Read Community フィールドに適切な読み取りコミュニティ ストリングを入力します。

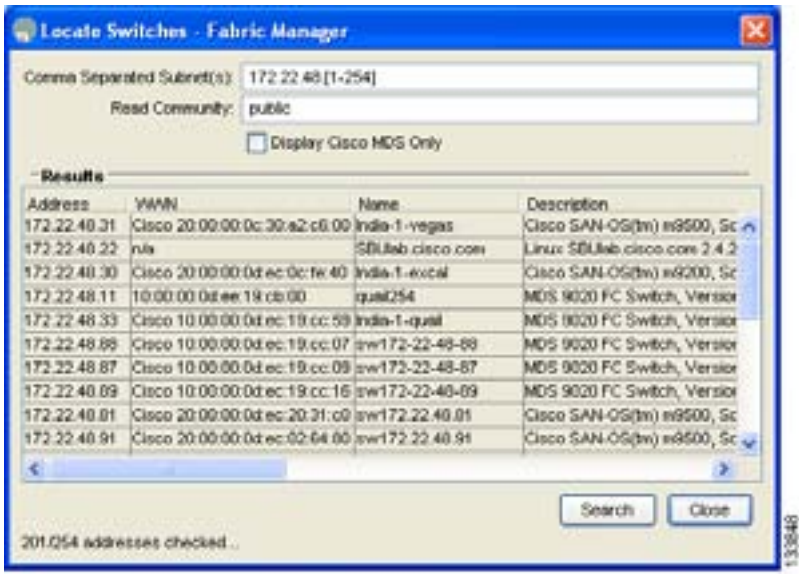
このストリングのデフォルト値は **public** です。

ステップ 4　**Display Cisco Nexus 5000 family Only** をクリックして、ネットワーク ファブリック内の Nexus 5000 シリーズ スイッチだけを表示します。

ステップ 5　**Search** をクリックして、ネットワーク ファブリック内のスイッチおよびデバイスを検出します。

Locate Switches ウィンドウに検出結果が表示されます（図 31-10 を参照）。

図 31-10　スイッチおよびデバイスの検索結果



（注） デバイス ロケータがネットワーク ファブリック内のデバイス検出を試みるごとに、画面左下にある数字が増加します。検出プロセスが完了した場合、この数字は表示行数を示します。

ステップ 6　**Close** をクリックして、ダイアログボックスを閉じます。

ファイバ チャネルの TOV

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）を設定します。

- Distributed Services TOV（D_S_TOV）— 有効範囲は 5,000 ～ 10,000 ミリ秒です。デフォルトは 5,000 ミリ秒です。
- Error Detect TOV（E_D_TOV）— 有効範囲は 1,000 ～ 10,000 ミリ秒です。デフォルトは 2,000 ミリ秒です。この値は、ポート初期化中に他端と比較されます。
- Resource Allocation TOV（R_A_TOV）— 有効範囲は 5,000 ～ 10,000 ミリ秒です。デフォルトは 10,000 ミリ秒です。この値は、ポート初期化中に他端と比較されます。

（注） Fabric Stability TOV（F_S_TOV）定数は設定できません。

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 を一時停止するしないかぎり、グローバルに変更できません。

Fabric Manager を使用してタイムアウトを設定する手順は、次のとおりです。

ステップ 1　Logical Domains ペインで **SAN** を選択して、すべての VSAN を含めます。

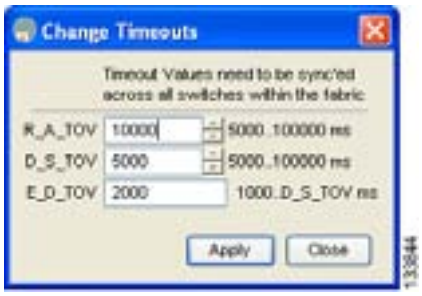
ステップ 2　Physical Attributes ペインで **Switches** を展開して **FC Services** を展開し、**Timers & Policies** を選択します。

Information ペインにスイッチのタイマーが表示されます。

ステップ 3　**Change Timeouts** をクリックして、タイムアウト値を設定します。

Change Timeouts ダイアログボックスが表示されます（図 31-11 を参照）。

図 31-11　Change Timeouts ダイアログボックス



ステップ 4　R_A_TOV（Resource Allocation Timeout Value）、D_S_TOV（Distributed Services Timeout Value）、E_D_TOV（Error Detect Timeout Value）の値を表示します。

ステップ 5　**Apply** をクリックします。

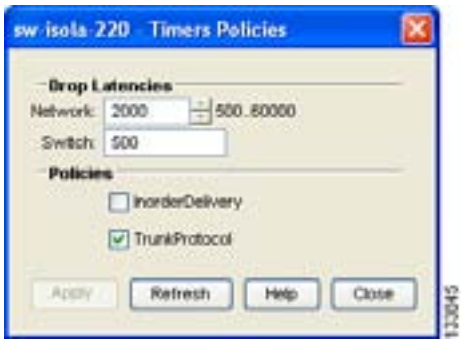
ステップ 6　**Close** をクリックして、ダイアログボックスを閉じます。

Device Manager でタイマー ポリシーを設定する手順は、次のとおりです。

ステップ 1　**FC** > **Advanced** > **Timers/Policies** を選択します。

ダイアログボックスに単一スイッチのタイマー ポリシーが表示されます（図 31-12 を参照）。

図 31-12　Device Manager のタイマー ポリシー設定



ステップ 2　ドロップダウン リストからネットワークを選択し、スイッチを指定します。

ステップ 3　**InOrderDeliver** および **Trunk Protocol** またはどちらかのチェックボックスをオンにします。

ステップ 4　**Apply** をクリックします。

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。

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 を設定して FC や IP トンネルなどに特別にリンクさせることができます。個別の VSAN に、異なる E_D_TOV、R_A_TOV、D_S_TOV 値を設定できます。タイマー値が変更されると、アクティブな VSAN は一時停止してアクティブになります。

注意　以前のバージョンでは VSAN ごとの FC タイマーをサポートしておらず、中断のないダウングレードは実行できません。

（注）　この設定はファブリックのすべてのスイッチに伝播する必要があります。ファブリックのすべてのスイッチが同じ値に設定されていることを確認してください。

Fabric Manager を使用して VSAN ごとの FC タイマーを設定する手順は、次のとおりです。

ステップ 1　Logical Domains ペインで、タイマーを設定する VSAN を選択します。

ポリシー選択時に VSAN を指定しない場合、変更された値はスイッチのすべての VSAN に適用されます。

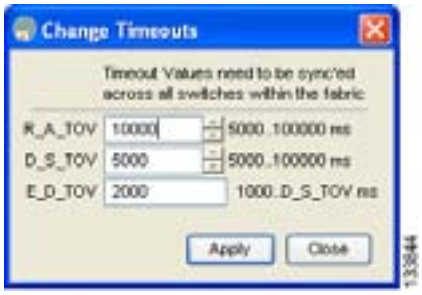
ステップ 2　Physical Attributes ツリーで **Switches** を展開して **FC Services** を展開し、**Timers & Policies** を選択します。

Information ペインに、選択した VSAN のスイッチのタイムアウトだけが表示されます。

ステップ 3　**Change Timeouts** をクリックして、タイムアウト値を設定します。

Change Timeouts ダイアログボックスが表示されます（図 31-13 を参照）。

図 31-13　Fabric Manager で VSAN ごとに変更するタイムアウト



ステップ 4　図 31-13 に示すように、タイムアウト値を変更します。

ステップ 5　R_A_TOV（Resource Allocation Timeout Value）、D_S_TOV（Distributed Services Timeout Value）、E_D_TOV（Error Detect Timeout Value）の値を表示します。

ステップ 6　**Apply** をクリックします。

ステップ 7　**Close** をクリックして、ダイアログボックスを閉じます。

ファブリック アナライザの設定

ファイバ チャネル プロトコル アナライザは、リンク上でフレームおよび順序付きセットをキャプチャし、デコードして、分析します。既存のファイバ チャネル アナライザは、ワイヤ スピードでトラフィックをキャプチャできます。これらは高価であり、フレームのデコードに対するサポートは制限されています。また、既存のアナライザはトラフィックのスヌーピング時に、リンク上のトラフィックを中断させます。

Cisco Fabric Analyzer を使用すると、ユーザは接続を中断したり、分析箇所にローカルに接続することなく、スイッチからファイバ チャネル制御トラフィックをキャプチャして、デコードすることができます。

シスコのファイバ チャネル プロトコル アナライザは、次の 2 つの一般的なパブリックドメイン ソフトウェア アプリケーションに基づいています。

- libpcap — http://www.tcpdump.org を参照
- Wireshark — http://www.wireshark.com を参照

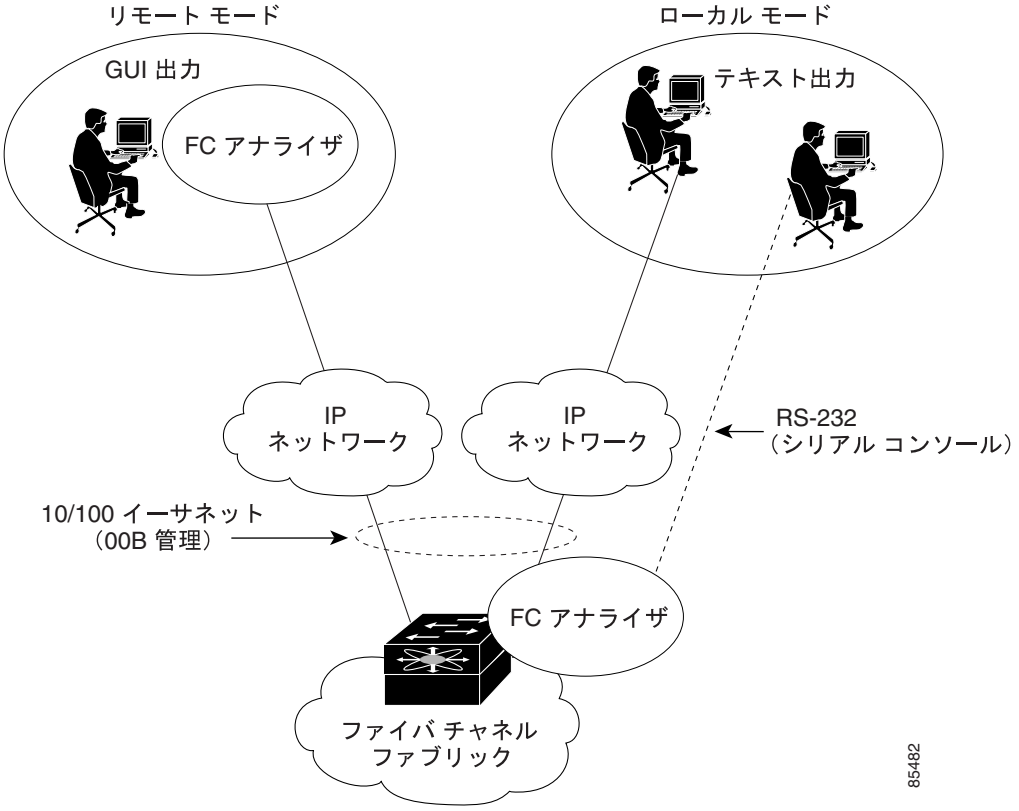
（注） Cisco Fabric Analyzer は、データ トラフィックでなく、制御トラフィックのキャプチャおよびデコードに役立ちます。制御パスのキャプチャに最適であり、高速データ パスのキャプチャを想定してはいません。

Cisco Fabric Analyzer の概要

Cisco Fabric Analyzer は 2 つの異なるコンポーネントで構成されます（図 31-14 を参照）。

- ソフトウェア — Cisco Nexus 5000 シリーズ スイッチで稼働し、2 つのキャプチャ モードをサポートします。
  - テキストベース アナライザ — ローカル キャプチャをサポートし、キャプチャされたフレームをデコードします。
  - デーモン — リモート キャプチャをサポートします。
- GUI ベース クライアント — Windows や Linux など、libpcap をサポートするホスト上で稼働し、Cisco Nexus 5000 シリーズ スイッチのリモート キャプチャ デーモンと通信します。

図 31-14　Cisco Fabric Analyzer の使用法



ローカル テキストベース キャプチャ

このコンポーネントは、Cisco Nexus 5000 シリーズ スイッチのスーパーバイザ モジュールに送受信されるトラフィックをキャプチャする、コマンドライン駆動のテキストベース インターフェイスです。このデコーダには完全な機能性があり、迅速にデバッグする場合や、リモート キャプチャ デーモンがイネーブルでないときに使用する場合に役に立ちます。また、このツールは Cisco Nexus 5000 シリーズ スイッチからアクセスされるため、スイッチごとにアクセスを制限する役割ベース ポリシーによって保護されています。

リモート キャプチャ デーモン

このデーモンはリモート キャプチャ コンポーネントのサーバ側にあります。ホストで稼働する Wireshark アナライザはクライアント側にあります。これらは Remote Capture Protocol（RPCAP）を使用して相互に通信します。RPCAP は、TCP ベースの制御接続、および TCP（デフォルト）または UDP に基づく TCP ベースまたは UDP ベースのデータ接続の 2 つのエンドポイントを使用します。制御接続はキャプチャをリモート制御する場合に使用します（キャプチャの開始や停止、またはキャプチャ フィルタの指定）。リモート キャプチャを実行できるのは、明示的に設定されたホストに対してのみです。この技術の利用により、ネットワーク内の不正なマシンがネットワーク内の制御トラフィックをスヌーピングするのを防ぎます。

RPCAP はファイアウォールの制限に基づいて、2 つの設定接続モードをサポートします。

- パッシブ モード（デフォルト）— 設定されたホストがスイッチとの接続を開始します。複数のホストをパッシブ モードに設定したり、複数のホストを接続して、同時にリモート キャプチャを受信できます。
- アクティブ モード — スイッチが、設定されたホストとの通信を（一度に 1 つずつ）開始します。

キャプチャ フィルタを使用すると、クライアントに実際に送信されるトラフィック量を制限できます。キャプチャ フィルタはスイッチでなく、Wireshark のクライアント側で指定されます。

GUI ベース クライアント

Wireshark ソフトウェアは、PC やワークステーションなどのホスト上で稼働し、リモート キャプチャ デーモンと通信します。このソフトウェアは、http://www.wireshark.org のパブリック ドメインから入手できます。Wireshark GUI フロントエンドはカラー表示、フィルタ定義中のグラフィックによる支援、および特定のフレームの検索など、豊富なインターフェイスをサポートします。これらの機能については、Wireshark の Web サイトを参照してください。

Wireshark によるリモート キャプチャが、Cisco Nexus 5000 シリーズ スイッチからのファイバ チャネル フレームのキャプチャおよびデコードをサポートしている場合、Wireshark が稼働するホストをスイッチにファイバ チャネル接続する必要はありません。スイッチで稼働するリモート キャプチャ デーモンは、帯域外イーサネット管理ポートを介して、キャプチャされたフレームを送信します。この機能を使用すると、デスクトップまたはラップトップからファイバ チャネル フレームをキャプチャし、デコードできます。

Cisco Fabric Analyzer の設定

Cisco Fabric Analyzer は、2 つのキャプチャのいずれかを実行するように設定できます。

- ローカル キャプチャ — ローカル キャプチャは、永続ストレージに保存したりスタンバイに同期することはできません。ローカル キャプチャはファブリック アナライザのテキスト バージョンを、コンソール画面から直接起動します。キャプチャはローカル ファイル システムにも保存できます。
- リモート キャプチャ — リモート キャプチャは永続ストレージに保存できます。また、必要に応じてスタンバイ スーパーバイザ モジュールと同期化したり、ステートレス再起動を発行できます。

Cisco Fabric Analyzer 機能を使用するには、トラフィックがスーパーバイザ モジュールを通過している必要があります。

リモート IP アドレスへのキャプチャの送信

注意　スーパーバイザ モジュール上で制御トラフィックをキャプチャするには、eth2 インターフェイスを使用する必要があります。

リモート トラフィックをキャプチャするには、次のいずれかのオプションを使用します。

- キャプチャ インターフェイスは、Wireshark でリモート デバイスとして指定できます。

  ```
  rpcap://<ipaddress or switch hostname>/eth2
  ```

  たとえば、

  ```
  rpcap://cp-16/eth2
  rpcap://17.2.1.1/eth2
  ```

- キャプチャ インターフェイスは、キャプチャ ダイアログボックス内で指定するか、または Wireshark の起動時にコマンドラインに -i オプションを使用して指定します。

  ```
  wireshark -i rpcap://<ipaddress|hostname>[:<port>]/<interface>
  ```

  たとえば、

  ```
  wireshark -i rpcap://172.22.1.1/eth2
  ```

  または

  ```
  wireshark -i rpcap://customer-switch.customer.com/eth2
  ```

（注）　たとえば、Windows 2000 で設定する場合は、デスクトップの［**スタート**］をクリックし、［**ファイル名を指定して実行 ...**］を選択します。続いて、ファイル名を指定して実行ウィンドウの名前フィールドに必要なコマンドライン オプションを入力します。

キャプチャされたフレームの表示

ディスプレイ フィルタ機能を使用することにより、キャプチャされたフレームを選択的に表示できます。たとえば、キャプチャされたすべてのフレームでなく、Exchange Link Protocol（ELP）要求フレームだけを表示できます。この機能はキャプチャされたフレームの表示だけを制限します。キャプチャされたフレーム、または保存されたフレームには影響しません。ディスプレイ フィルタを指定、使用、および保存する手順については、Wireshark Web サイト（http://www.wireshark.org）を参照してください。

次に、この機能の使用方法を示します。

- 指定された VSAN 内のすべてのパケットを表示するには、次の式を使用します。

  ```
  mdshdr.vsan == 2
  ```

- すべての SW_ILS フレームを表示するには、次の式を使用します。

  ```
  fcswils
  ```

- クラス F フレームを表示するには、次の式を使用します。

  ```
  mdshdr.sof == SOFf
  ```

- すべての FSPF フレームを表示するには、次の式を使用します。
  `swils.opcode == HLO || swils.opcode == LSU || swils.opcode == LSA`
- すべての FLOGI フレームを表示するには、次の式を使用します。
  `fcels.opcode == FLOGI`
- VSAN 1 内のすべての FLOGI フレームを表示するには、次の式を使用します。
  `fcels.opcode == FLOGI && mdshdr.vsan == 2`
- すべてのネーム サーバ フレームを表示するには、次の式を使用します。
  `dNS`

ディスプレイ フィルタの定義

ディスプレイ フィルタで制限されるのは表示可能なフレームであり、キャプチャ対象のフレームではありません（任意の view コマンドと同様）。表示するフィルタは、GUI アプリケーションを使用して、複数の方法で定義できます。

- 自動定義
- 手動定義
- 支援付きの手動定義
- ローカル キャプチャにおける手動のみの定義
- 支援なし

定義に関係なく、各フィルタを保存し、名前で識別する必要があります。

（注） GUI 支援機能は Wireshark の一部です。詳細については、http://www.wireshark.org を参照してください。

キャプチャ フィルタ

リモート キャプチャ中にキャプチャ フィルタ機能を使用すると、キャプチャするフレームを制限できます。この機能は、キャプチャされて、リモート スイッチからホストに送信されるフレームを制限します。たとえば、クラス F フレームだけをキャプチャできます。キャプチャ フィルタは、リモート キャプチャで消費される帯域幅を制限する場合に便利です。

ディスプレイ フィルタと異なり、キャプチャ フィルタではキャプチャ対象が、指定されたフレームに限定されます。完全に新しいキャプチャを指定しないかぎり、他のフレームは表示されません。

キャプチャ フィルタの構文は、ディスプレイ フィルタの構文と異なります。キャプチャ フィルタは、libpcap フリーウェアと併用される Berkeley Packet Filter（BPF）ライブラリを使用します。有効なすべてのファイバ チャネル キャプチャ フィルタ フィールドのリストについては以降で説明します。

キャプチャ フィルタの設定手順については、Wireshark Web サイト（http://www.wireshark.org）を参照してください。

次に、この機能の使用方法を示します。

- 指定された VSAN のフレームだけをキャプチャするには、次の式を使用します。
  `vsan = 1`

- クラス F フレームだけをキャプチャするには、次の式を使用します。
  `class_f`
- クラス ファイバ チャネル ELS フレームだけをキャプチャするには、次の式を使用します。
  `els`
- ネームサーバ フレームだけをキャプチャするには、次の式を使用します。
  `dns`
- SCSI コマンド フレームだけをキャプチャするには、次の式を使用します。
  `fcp_cmd`

(注) この機能は libpcap の一部です。詳細については、http://www.tcpdump.org を参照してください。

使用可能なキャプチャ フィルタ

ここでは、使用可能なキャプチャ フィルタを示します。

```
o vsan
o src_port_idx
o dst_port_idx
o sof
o r_ctl
o d_id
o s_id
o type
o seq_id
o seq_cnt
o ox_id
o rx_id
o els
o swils
o fcp_cmd   (FCP Command frames only)
o fcp_data (FCP data frames only)
o fcp_rsp   (FCP response frames only)
o class_f
o bad_fc
o els_cmd
o swils_cmd
o fcp_lun
o fcp_task_mgmt
o fcp_scsi_cmd
o fcp_status
o gs_type      (Generic Services type)
o gs_subtype   (Generic Services subtype)
o gs_cmd
o gs_reason
o gs_reason_expl
o dns   (name server)
o udns (unzoned name server)
o fcs   (fabric configuration server)
o zs    (zone server)
o fc    (use as fc[x:y] where x is offset and y is length to compare)
o els   (use as els[x:y] similar to fc)
o swils (use as swils[x:y] similar to fc)
o fcp   (use as fcp[x:y] similar to fc)
o fcct (use as fcct[x:y] similar to fc)
```

WWN の設定

スイッチの WWN は、イーサネット MAC（メディア アクセス制御）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 Nexus 5000 シリーズ スイッチは、3 つの Network Address Authority（NAA）アドレス フォーマットをサポートします（表 31-1 を参照）。

表 31-1　NAA WWN の標準フォーマット

NAA アドレス	NAA タイプ	WWN フォーマット	
IEEE 48 ビット アドレス	タイプ 1 = 0001b	000 0000 0000b	48 ビット MAC アドレス
IEEE 拡張	タイプ 2 = 0010b	ローカルに割り当て	48 ビット MAC アドレス
IEEE 登録	タイプ 5 = 0101b	IEEE 企業 ID：24 ビット	VSID：36 ビット

注意　WWN の変更は、管理者や、スイッチの動作に精通した担当者が実行してください。

リンク初期化 WWN の使用法

ELP および Exchange Fabric Protocol（EFP）は、リンク初期化中に WWN を使用します。使用方法の詳細は、Cisco SAN-OS ソフトウェア リリースごとに異なります。

ELP と EFP のどちらも、リンク初期化中にデフォルトで VSAN WWN を使用します。ただし、ELP の使用方法はピア スイッチの使用方法に応じて変わります。

- ピア スイッチの ELP が sWWN を使用する場合、ローカル スイッチも sWWN を使用します。
- ピア スイッチの ELP が VSAN WWN を使用する場合、ローカル スイッチも VSAN WWN を使用します。

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手順は、次のとおりです。

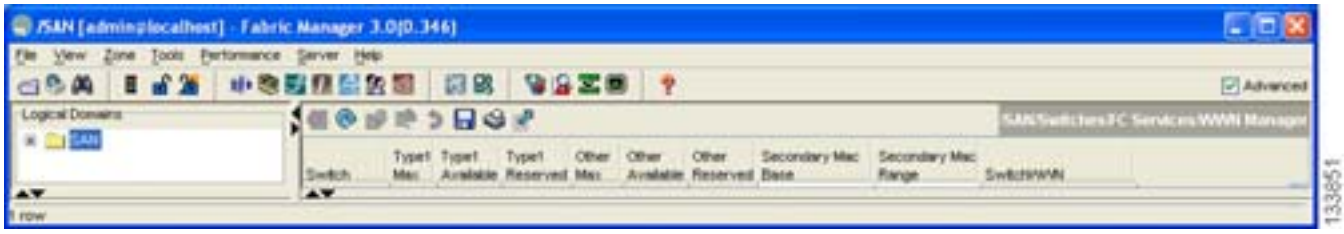
ステップ 1　Logical Domains ペインで SAN（または VSAN）を選択します。

Information ペインにスイッチのリストが表示されます。

ステップ 2　Physical Attributes ペインで **Switches** を展開して **FC Services** を展開し、**WWN Manager** を選択します。

ステップ 3　Information ペインをスクロールし、セカンダリ MAC アドレスを設定するスイッチを表示します（図 31-15 を参照）。

図 31-15　セカンダリ MAC アドレスの設定



ステップ 4　**Secondary Mac Base** フィールドにセカンダリ MAC アドレスを入力します。

ステップ 5　**Secondary Mac Range** フィールドにセカンダリ MAC アドレスを入力します。

ステップ 6　**Apply Changes** アイコンをクリックします。

WWN 情報の表示

WWN 設定のステータスを表示する手順は、次のとおりです。

ステップ 1　Logical Domains ペインで SAN（または VSAN）を選択します。

Information ペインにスイッチのリストが表示されます。

ステップ 2　Physical Attributes ペインで、**Switches** > **FC Services** > **WWN Manager** を選択します。

SAN または VSAN に各スイッチの WWN 情報が表示されます。

HBA の FC ID 割り当て

ファイバ チャネル標準では、任意のスイッチの Fx ポートに接続された N ポートに、一意の FC ID を割り当てる必要があります。使用する FC ID 数を保護するために、Cisco Nexus 5000 シリーズ スイッチは特殊な割り当て方式を使用します。「HBA の FC ID 割り当て」（p.31-29）を参照してください。

デフォルト設定

表 31-2 に、この章で説明した機能のデフォルト設定値を示します。

表 31-2　拡張機能のデフォルト設定値

パラメータ	デフォルト
CIM サーバ	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
fc trace 呼び出しのタイムアウト時間	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

INDEX

Symbols

*（アスタリスク）
　自動学習エントリ　24-22
　ポート セキュリティ ワイルドカード　24-16

A

AAA
　DHCHAP 認証　23-10
auto ポート モード
　説明　10-5

B

BB_credit
　原因コード　10-7
　設定　10-13
　説明　10-7
Brocade
　ネイティブ interop モード　22-10
Buffer-to-Buffer credit、BB_credit を参照

D

DHCHAP
　AAA 認証　23-10
　AAA 認証の設定　23-10
　FC-SP も参照
　イネーブル化（手順）　23-4
　グループ設定　23-7
　セキュリティ情報の表示　23-10
　設定　23-3 – 23-11
　タイムアウト値　23-9
　デフォルトの設定値　23-11
　認証モード　23-4
　ハッシュ アルゴリズム　23-6
　リモート デバイスのパスワード　23-8
　ローカル スイッチのパスワード　23-7
Diffie-Hellman Challenge Handshake Authentication Protocol、DHCHAP を参照

E

E ポート
　FCS サポート　26-2
　FSPF トポロジ　18-2
　トランキング設定　13-4
　ファブリック バインディング チェック　25-2
　分離　10-7
　リンク分離からの回復　16-26
E ポート モード
　サービス クラス　10-4
　説明　10-4
EFMD
　ファブリック バインディング　25-2
　ファブリック バインディングの開始　25-4
EISL
　ポート チャネル リンク　14-2
Exchange Fabric Membership Data、EFMD を参照
Exchange Link Parameter、ELP を参照

F

F ポート
　Fx ポートも参照
　説明　10-4
F ポート モード
　サービス クラス　10-4
　説明　10-4
Fabric Configuration Server、FCS を参照
Fabric Device Management Interface（FDMI）、FDMI を参照
Fabric Shortest Path First、FSPF を参照
FC ID
　FC エイリアス メンバーの設定　16-18
　HBA の割り当て　22-7
　固定的　11-18, 11-24

説明 11-17
デフォルトの企業 ID リストの割り当て 22-8
割り当て 11-2, 22-7
fcaliases
コピー 16-31
作成 16-18
使用方法 17-9
ゾーンの設定 16-17
名前の変更 16-30
メンバーの追加 16-19
fcdomain
CFS 配布の設定 11-13
オーバーラップ分離 10-7
結合ファブリックの自動再構成 11-7
再起動 11-3
自動再構成のイネーブル化 11-8
情報の表示 11-24
初期化 11-5
説明 11-1
着信 RCF 11-6
デフォルトの設定値 11-24
ドメイン ID 11-9
ドメイン マネージャの高速再起動 11-4
FCS
Device Manager を使用したファブリック ポートの表示 26-6
情報の表示 26-4
説明 26-2
デフォルトの設定値 26-8
特性 26-3
名前の設定 26-3
FC-SP
DHCHAP も参照
ISL 上でのイネーブル化 23-10
イネーブル化（手順） 23-4
認証 23-1
fctimers
設定値の表示 22-5
配信 22-4
FDMI
データベース情報の表示 19-6
Fibre Channel Security Protocol、FC-SP を参照
FLOGI
説明 19-1
FSPF
Link State Record のデフォルト 18-4
VSAN カウンタのクリア 18-6
VSAN の設定 18-5
イネーブル化 18-5
インターフェイスでのディセーブル化 18-10
インターフェイスの設定 18-7 - 18-12
グローバル設定 18-3
再コンバージェンス時間 18-2
再送信インターバル 18-9
順序どおりの配信 18-14
冗長リンク 18-2
設定のリセット 18-5
説明 18-2
相互運用性 22-11
ディセーブル化 18-5
デッド タイム インターバル 18-8
デフォルト設定へのリセット 18-5
デフォルトの設定値 18-19
トポロジ例 18-2
ハロー タイム インターバルの設定 18-8
フォールトトレラント ファブリック 18-2
リンク コストの計算 18-7
ルーティング サービス 18-1, 18-2
ルーティング プロトコルのディセーブル化 18-6
FSPF ルート
設定 18-13
説明 18-13
fWWN
FC エイリアス メンバーの設定 16-18
Fx ポート
VSAN メンバシップ 15-4

H

HBA
FC ID の割り当て 22-7
HBA ポート
エリア FC ID の設定 11-21

I

ID の交換
順序どおりの配信 18-15
パス選択 15-11
interop モード
説明 22-10

デフォルトの設定値　22-14
モード 1 の設定　22-10
IOD、順序どおりの配信を参照
ISL
ポート チャネル リンク　14-2

L

Logical Unit Number、LUN を参照

M

MAC アドレス
セカンダリの設定　22-6
McData
ネイティブ interop モード　22-10

N

N ポート
Nx ポートも参照
ゾーン メンバシップ　16-2
ゾーンの実行　16-23
ハード ゾーン分割　16-23
NL ポート　26-2
ハード ゾーン分割　16-23
NP リンク　12-2
NPV の設定　12-5
NPV モード　12-2
NPV、設定　12-5
Nx ポート
FCS サポート　26-2
N ポートも参照

P

PLOGI
ネーム サーバ　19-5
Port World Wide Name、pWWN を参照
pWWN
FC エイリアス メンバーの設定　16-18
拒否、重複　19-4
ゾーン メンバシップ　16-2

R

RCF
説明　11-3
着信　11-6
着信拒否　11-7
Registered State Change Notification（RSCN）、RSCN を参照
RSCN
情報の表示　19-7
デフォルトの設定値　19-11
ドメイン フォーマット SW-RSCN の抑制　19-9
RSCN タイマー
設定　19-11

S

SCSI LUN
カスタマイズ検出　21-3
検出の開始　21-2
情報の表示　21-4
ターゲットの検出　21-1
SD ポート モード
インターフェイス モード　10-5
説明　10-4
Small Computer System Interface、SCSI を参照
SPAN 宛先ポート モード、SD ポート モードを参照
sWWN
ファブリック バインディングの設定　25-5

T

TE ポート
FCS サポート　26-2, 26-3
FSPF トポロジ　18-2
相互運用性　22-11
トランキングの制約事項　13-2
ファブリック バインディング チェック　25-2
リンク分離からの回復　16-26
TE ポート モード
サービス クラス　10-4
説明　10-4
Time Out Value、TOV を参照
TOV
VSAN の設定　22-3
相互運用性　22-10

デフォルトの設定値　22-14
範囲　22-2

V

VSAN
DHCHAP との互換性　23-4
FC ID　15-2
FCS サポート　26-2
FSPF　18-5
FSPF 接続　18-2
FSPF の設定　18-4
TE ポート モード　10-4
機能　15-2
許可アクティブ　13-2
許可アクティブ リストの設定　13-7
削除　15-10
ステート　15-6
設定　15-6
設定の表示　15-12
説明　15-1 – 15-4
相互運用性モード　22-11
ゾーンとの比較（表）　15-4
タイマーの設定　22-3
デフォルトの設定値　15-12
ドメイン ID 自動再構成　11-8
トラフィックの分離　15-3
トランキング ポート　15-8
トランク許可　13-2
トランク許可リストの設定　13-5 – 13-7
名前　15-6
ネーム サーバ　19-3
不一致　10-7
複数のゾーン　16-5
分離　15-9
ポート トラッキング　27-7
利点　15-3
ロード バランシング属性　15-6
VSAN ID
VSAN メンバシップ　15-4
許可リスト　13-8
説明　15-6
トラフィックの多重化　10-4
範囲　15-4

W

World Wide Name、WWN を参照
WWN
情報の表示　22-6
セカンダリ MAC アドレス　22-6
中断された接続　10-8
ポート セキュリティ　24-17

あ

アクティブなゾーン セット
考慮事項　16-4
配信のイネーブル化　16-24
宛先 ID
エクスチェンジ ベース　14-4
順序どおりの配信　18-15
パス選択　15-11
フロー ベース　14-4

い

インターフェイス
FC エイリアス メンバーの設定　16-18
VSAN への割り当て　15-8
一時停止状態　14-14
情報の表示　10-15
説明の設定　10-10, 10-11
データ フィールド サイズの設定　10-12
デフォルトの設定値　10-16
分離状態　14-14
ポート チャネルからの削除　14-15
ポート チャネルへの強制追加　14-14
ポート チャネルへの追加　14-13, 14-14
インターフェイスの統計情報
説明　10-14

か

拡張ゾーン
イネーブル化（手順）　16-36
基本ゾーンからの変更　16-34
説明　16-33
データベースの変更　16-36
拡張ポート モード、E ポート モードを参照
間接リンク障害

回復 27-2
管理ステート
設定 10-9
説明 10-5
関連資料 xxiii

き

企業 ID
FC ID の割り当て 22-8

け

結合ファブリック
自動再構成 11-7
原因コード
説明 10-6

こ

固定的 FC ID
イネーブル化（手順） 11-18
設定 11-19
説明 11-18
固有エリア FC ID
設定 11-21
説明 11-20

さ

再送信インターバル
FSPF の設定 18-9
説明 18-9

し

実行時チェック
スタティック ルート 18-13
主要スイッチ
ドメイン ID の割り当て 11-10
順序どおりの配信
グローバルなイネーブル化 18-16
ステータスの表示 18-17
注意事項 18-16
ポート チャネル フレーム順序の再設定 18-16
冗長性
VSAN 15-4
冗長物理リンク
例（図） 18-3

す

スイッチ プライオリティ
設定 11-5
デフォルト 11-5
スケーラビリティ
VSAN 15-4
スタティック ルート
実行時チェック 18-13
ストレージ デバイス
アクセス制御 16-1

せ

セカンダリ MAC アドレス
設定 22-6

そ

相互運用性
interop モード 1 の設定 22-10
VSAN 15-12
送信元 ID
エクスチェンジ ベース 14-4
順序どおりの配信 18-15
パス選択 15-11
フロー ベース 14-4
ゾーン
FC エイリアスの設定 16-17
pWWN を使用したメンバシップ 15-4
VSAN との比較（表） 15-4
アクセス制御 16-13
エイリアスの設定 16-17
拡張ゾーンからの変更 16-35
拡張ゾーンも参照
機能 16-1, 16-4
結合ファブリック 10-7
コピー 16-31
実行 16-22
情報の表示 16-33

設定 16-22
ゾーン セットへの追加 16-22
ゾーン メンバーの追加 16-10
ゾーン分割、ゾーン セットも参照
データベースのインポート 16-26
データベースのエクスポート 16-26
デバイス エイリアスとの比較（表） 17-2
デフォルト ゾーンも参照
デフォルト ポリシー 16-3
名前の変更 16-30
ハード ゾーン分割、ソフト ゾーン分割も参照
バックアップ（手順） 16-29
復元（手順） 16-29
フル ゾーン データベースの編集 16-7
ゾーン エイリアス
インポート 17-9
デバイス エイリアスへの変換 17-9
ゾーン サーバ データベース
削除 16-32
ゾーン セット
アクティブ ゾーン セットも参照
アクティブ ゾーン セット、フル ゾーン セットも参照
アクティブ化 16-13
インポート 16-26
エクスポート 16-26
機能 16-1
考慮事項 16-4
コピー 16-27, 16-31
作成 16-13, 16-22
情報の表示 16-33
設定 16-12 - 16-17
設定の配信 16-23
ゾーン、ゾーン分割も参照
データベースのインポート 16-26
データベースのエクスポート 16-26
名前の変更 16-30
配信のイネーブル化 16-24
メンバー ゾーンの追加 16-22
ワンタイム配信 16-25
ゾーン データベース
MDS 以外のデータベースの移行 16-32
ゾーン メンバー
pWWN メンバーへの変換 16-21
情報の表示 16-16
ゾーンへの追加 16-10
ゾーン属性グループ
コピー 16-31
ゾーン分割
実装 16-4
説明 16-1
ゾーン、ゾーン セットも参照
例 16-3
ソフト ゾーン分割
説明 16-23
ゾーン分割も参照

て

デッド タイム インターバル
説明 18-8
デバイス エイリアス
拡張モード 17-4
機能 17-2
作成（手順） 17-7
情報の表示 17-10
使用方法 17-9
説明 17-1
ゾーン エイリアスの変換 17-9
ゾーンとの比較（表） 17-2
データベースの変更 17-3
デフォルトの設定値 17-10
要件 17-2
レガシー ゾーン エイリアスのインポート 17-9
デバイス エイリアス データベース
ファブリックのロック 17-7
変更のコミット 17-7
変更の廃棄 17-8
マージ 17-9
デフォルト ゾーン
アクセス権限の設定 16-17
設定 16-17
説明 16-16
相互運用性 22-11
ポリシー 16-17
ポリシーの設定 16-12

と

動作ステート
説明 10-6
ドメイン ID

CFS 配布の設定　11-13
FC エイリアス メンバーの設定　16-18
許可リスト　11-11
許可リストの設定　11-12
スタティック　11-11
説明　11-9
相互運用性　22-10
配信　11-2
優先　11-11
連続割り当てのイネーブル化　11-16
割り当て障害　10-7
ドメイン マネージャ
高速再起動機能　11-4
分離　10-7
トラッキング対象ポート
動作のバインディング　27-4
トラフィックの分離
VSAN　15-4
トランキング
情報の表示　13-7
制約事項　13-2
設定ガイドライン　13-2
説明　13-1
相互運用性　22-11
トラフィックのマージ　13-2
ポート チャネルとの比較　14-2
リンク状態　13-4
トランキング E ポート モード、TE ポート モードを参照
トランキング プロトコル
説明　13-3
デフォルト状態　13-3
デフォルトの設定　13-8
ポート分離の検出　13-2
トランキング ポート
VSAN との対応　15-8
トランク モード
設定　13-4
トランク許可 VSAN リスト
説明　13-5 – 13-6
ドロップ遅延時間
設定　18-18

に

認証
ファブリック セキュリティ　23-1

ね

ネーム サーバ
LUN 情報　21-2
相互運用性　22-11
重複 pWWN の拒否　19-4

は

ハード ゾーン分割
説明　16-23
パスワード
DHCHAP　23-7, 23-8
ハロー タイム インターバル
FSPF の設定　18-8
説明　18-8

ひ

ビット エラー
理由　10-13

ふ

ファイバ チャネル
タイムアウト値　22-1 – 22-4
ファブリック バインディングの sWWN　25-6
ファイバ チャネル インターフェイス
BB_credit　10-7
イネーブル化　10-9
インターフェイスも参照
管理ステート　10-5
原因コード　10-6
情報の表示　10-15
ステート　10-5
設定　10-8
説明の設定　10-10, 10-11
ディセーブル化　10-9
動作ステート　10-6
フレームのカプセル化の設定　10-12
ポート チャネルからの削除　14-15
ファイバ チャネル ドメイン、fcdomain を参照
ファブリック

ファブリック フレームの構築も参照
ファブリック pWWN
ゾーン メンバシップ 16-2
ファブリック、RCF; ファブリック フレームの構築を参照
ファブリック WWN、fWWN を参照
ファブリック セキュリティ
デフォルトの設定値 23-11
認証 23-1
ファブリック バインディング
config データベースの削除（手順） 25-9
config データベースの作成（手順） 25-9
DHCHAP との互換性 23-4
E ポートのチェック 25-2
EFMD 25-2
EFMD 統計情報の表示（手順） 25-10
sWWN リスト 25-5
TE ポートのチェック 25-2
アクティブ データベースの表示（手順） 25-11
アクティブ化 25-6
イネーブル化（手順） 25-4
違反の表示（手順） 25-11
開始プロセス 25-4
強制的なアクティブ化 25-8
コンフィギュレーション データベースへのコピー 25-8
コンフィギュレーション データベースへの保存 25-8
コンフィギュレーション ファイルへのコピー（手順） 25-10
実行 25-3
説明 25-1
データベースの削除 25-12
デフォルトの設定値 25-13
統計情報のクリア 25-12
ポート セキュリティとの比較 25-2
ライセンスの要件 25-2
ファブリック フレームの構築
説明 11-3
ファブリック フレームの再設定、RCF を参照
ファブリック ポート モード、F ポート モードを参照
ファブリック ログイン、FLOGI を参照
ファブリック再設定
fcdomain のフェーズ 11-2
フォールトトレラント ファブリック
例（図） 18-2
フル ゾーン セット
考慮事項 16-4
配信のイネーブル化 16-24
フレームのカプセル化
設定 10-12
分離された VSAN
説明 15-9
メンバシップの表示 15-9

ほ

ポート セキュリティ
CFS 配布の設定 24-19 - 24-22
DHCHAP との互換性 23-4
WWN の識別 24-17
アクティブ化 24-3, 24-9
アクティブ化の拒否 24-9
イネーブル化（手順） 24-6
違反の表示（手順） 24-12
強制的なアクティブ化 24-10
許可済みペアの追加 24-18
実行メカニズム 24-2
自動学習 24-2
自動学習を使用しない手動設定 24-15
設定ガイドライン 24-3
設定の表示（手順） 24-12
ディセーブル化 24-6
データベースからのエントリの削除（手順） 24-19
デフォルトの設定値 24-26
統計情報の表示（手順） 24-12
非アクティブ化 24-9
ファブリック バインディングとの比較 25-2
不正アクセスの防止 24-2
ライセンスの要件 24-2
ポート セキュリティ データベース
コンフィギュレーション データベースへのアクティブ データベースのコピー（手順） 24-11
再アクティブ化 24-10
シナリオ 24-23
手動設定時の注意事項 24-5
相互作用 24-22
マージに関する注意事項 24-22
ポート セキュリティ自動学習
CFS 使用時の設定の注意事項 24-4
CFS を使用しない設定の注意事項 24-5

イネーブル化（手順） 24-13
許可の例 24-15
説明 24-2
ディセーブル化 24-14
デバイスの許可 24-14
ポート チャネル
DHCHAP との互換性 23-4
インターフェイスの強制追加 14-14
インターフェイスの削除 14-15
インターフェイスの状態 14-14
インターフェイスの追加 14-13, 14-14
管理上のダウン 10-8
互換性チェック 14-13
誤設定エラー検出 14-7
削除 14-11
作成 14-10
順序保証 18-16
設定 14-12
設定ガイドライン 14-7
設定の確認 14-21
説明 14-1
相互運用性 22-11
デフォルトの設定 14-21
トランキングとの比較 14-2
リンク障害 18-3
リンク変更 18-16
ロード バランシング 14-3
ポート チャネル プロトコル
自動作成 14-18
自動作成のイネーブル化 14-19
自動作成の設定 14-19
手動設定への自動作成グループの変換 14-19
説明 14-16
チャネル グループの作成 14-17
ポート トラッキング
VSAN 内のポートの監視 27-7
イネーブル化（手順） 27-3
説明 27-1
注意事項 27-3
デフォルトの設定値 27-8
複数ポート 27-6
ポート モード
auto 10-5

ま

マニュアル
関連資料 xxii
その他の資料 xxii, xxiii

り

リンク コスト
FSPF の設定 18-7
リンク障害
回復 27-2

る

ルート コスト
計算 18-7

ろ

ロード バランシング
VSAN の属性 15-6
設定 15-11
説明 14-3, 15-11
属性 15-11
ポート チャネル 14-2