Cisco Nexus 5000 シリーズ NX-OS SAN スイッチング コンフィギュレーション ガイド リリース 5.2(1)N1(1)

初版：2012 年 07 月 02 日

最終更新：2012 年 07 月 02 日

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

Text Part Number: OL-27583-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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

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

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

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

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

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

このマニュアルで使用している IP アドレスは、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。

© 2012 Cisco Systems, Inc. All rights reserved.

目 次

はじめに xix

対象読者 xix

表記法 xix

関連資料 xxi

マニュアルに関するフィードバック xxiii

マニュアルの入手方法およびテクニカル サポート xxiii

このリリースの新規および変更情報 1

概要 3

SAN スイッチングの概要 3

ファイバ チャネル インターフェイスの設定 9

ファイバ チャネル インターフェイスの設定 9

ファイバ チャネル インターフェイスの概要 9

ファイバ チャネルのライセンス要件 9

物理ファイバ チャネル インターフェイス 9

仮想ファイバ チャネル インターフェイス 10

VF ポート 10

VE ポート 11

VNP ポート 12

インターフェイス モード 12

E ポート 13

F ポート 13

NP ポート 13

TE ポート 13

TF ポート 14

TNP ポート 14

SD ポート 14

auto モード 15
インターフェイス ステート 15
管理ステート 15
動作ステート 15
理由コード 16
Buffer-to-Buffer credit（BB_credit） 19
ファイバ チャネル インターフェイスの設定 20
ファイバ チャネル インターフェイスの設定 20
ファイバ チャネル インターフェイスの範囲の設定 21
インターフェイス管理ステートの設定 21
インターフェイス モードの設定 22
インターフェイスの説明の設定 23
ポート速度の設定 23
自動検知 24
SD ポート フレーム カプセル化の設定 25
受信データ フィールド サイズの設定 25
ビット エラーしきい値の概要 25
BB_credit の設定 27
ファイバ チャネル インターフェイスのグローバル属性の設定 28
スイッチ ポート属性のデフォルト値の設定 28
N ポート ID バーチャライゼーションの概要 29
N ポート ID バーチャライゼーションのイネーブル化 29
ポート チャネルの設定例 30
ファイバ チャネル インターフェイスの確認 31
SFP トランスミッタ タイプの確認 31
インターフェイス情報の確認 31
BB_credit 情報の確認 33
ファイバ チャネル インターフェイスのデフォルト設定 33
ドメイン パラメータの設定 35
ドメイン パラメータの設定 35
ファイバ チャネル ドメインについて 35
ドメインの再起動の概要 36

ドメインの再起動 37
ドメイン マネージャの高速再起動について 37
ドメイン マネージャの高速再起動のイネーブル化 38
スイッチ プライオリティの概要 38
スイッチ プライオリティの設定 39
fcdomain の初期化の概要 39
fcdomain のディセーブル化または再イネーブル化 39
ファブリック名の設定 40
着信 RCF の概要 40
着信 RCF の拒否 41
結合ファブリックの自動再構成の概要 41
自動再設定のイネーブル化 42
ドメイン ID 42
ドメイン ID の概要 42
スタティック ドメイン ID または優先ドメイン ID の指定 44
許可ドメイン ID リストの概要 45
許可ドメイン ID リストの設定 46
許可ドメイン ID リストの CFS 配信の概要 46
配信のイネーブル化 47
ファブリックのロック 47
変更のコミット 48
変更の破棄 48
ファブリックのロックのクリア 49
CFS 配信ステータスの表示 49
保留中の変更の表示 49
セッション ステータスの表示 49
連続ドメイン ID 割り当ての概要 50
連続ドメイン ID 割り当てのイネーブル化 50
FC ID 50
固定的 FC ID の概要 51
固定的 FC ID 機能のイネーブル化 51
永続的 FC ID 設定時の注意事項 52

固定的 FC ID の設定 52
HBA の固有エリア FC ID について 53
HBA の固有エリア FC ID の設定 54
固定的 FC ID の選択消去の概要 55
固定的 FC ID の消去 56
fcdomain 情報の確認 56
ファイバ チャネル ドメインのデフォルト設定 57
NPV の設定 59
NPV の設定 59
NPV の概要 59
NPV の概要 59
NPV モード 60
サーバ インターフェイス 60
NP アップリンク 61
FLOGI 動作 61
NPV トラフィック管理 62
自動アップリンク選択 62
トラフィック マップ 63
ディスラプティブ ロード バランシング 63
NPV トラフィック管理の注意事項 64
NPV の注意事項および制限事項 64
NPV の設定 65
NPV のイネーブル化 65
NPV インターフェイスの設定 66
NP インターフェイスの設定 66
サーバ インターフェイスの設定 67
NPV トラフィック管理の設定 68
NPV トラフィック マップの設定 68
ディスラプティブ ロード バランシングのイネーブル化 68
NPV の確認 69
NPV の確認例 70
NPV トラフィック管理の確認 71

FCoE NPV の設定 73

FCoE NPV について 73

FCoE NPV モデル 75

マッピングの要件 76

ポート要件 77

NPV 機能 77

vPC トポロジ 78

サポートされるトポロジおよびサポートされないトポロジ 79

注意事項および制約事項 82

FCoE NPV 設定の制限 83

デフォルト設定 84

FCoE のイネーブル化および NPV のイネーブル化 84

FCoE NPV のイネーブル化 85

FCoE NPV の NPV ポートの設定 86

FCoE NPV の設定の確認 86

FCoE NPV の設定例 88

VSAN トランキングの設定 93

VSAN トランキングの設定 93

VSAN トランキングの概要 93

VSAN トランキングの不一致 94

VSAN トランキング プロトコル 95

VSAN トランキングの設定 95

注意事項および制約事項 95

VSAN トランキング プロトコルのイネーブル化/ディセーブル化 96

トランク モードについて 96

トランク モードの設定 97

トランク許可 VSAN リストについて 98

VSAN の許可アクティブ リストの設定 100

VSAN トランキング情報の表示 101

トランクのデフォルト設定 101

SAN ポート チャネルの設定 103

SAN ポート チャネルの設定 103

SAN ポート チャネルに関する情報 103
ポート チャネルと VSAN トランキングの概要 104
ロード バランシングの概要 105
SAN ポート チャネルの設定 107
SAN ポート チャネルの設定時の注意事項 109
F および TF ポート チャネルの注意事項 109
SAN ポート チャネルの作成 110
ポート チャネル モードについて 110
アクティブ モードの SAN ポート チャネルの設定 111
SAN ポート チャネルの削除について 112
SAN ポート チャネルの削除 113
SAN ポート チャネルのインターフェイス 113
SAN ポート チャネルへのインターフェイスの追加について 113
互換性チェック 114
一時停止状態および分離状態 115
SAN ポート チャネルへのインターフェイスの追加 115
インターフェイスの強制追加 116
SAN ポート チャネルからのインターフェイスの削除について 116
SAN ポート チャネルからのインターフェイスの削除 117
SAN ポート チャネル プロトコル 117
チャネル グループの作成の概要 118
自動作成の注意事項 119
自動作成のイネーブル化および設定 120
手動設定チャネル グループの概要 121
手動設定チャネル グループへの変更 121
ポート チャネルの設定例 122
SAN ポート チャネル設定の確認 122
SAN ポート チャネルのデフォルト設定 124
VSAN の設定と管理 125
VSAN の設定と管理 125
VSAN に関する情報 125
VSAN トポロジ 125

VSAN の利点 128
VSAN とゾーン 128
VSAN の設定 130
VSAN の作成について 131
VSAN の静的な作成 131
ポート VSAN メンバーシップの概要 132
スタティック ポート VSAN メンバーシップの概要 132
VSAN スタティック メンバーシップの表示 133
デフォルト VSAN の概要 134
分離された VSAN の概要 134
分離された VSAN メンバーシップの概要 135
VSAN の動作ステート 135
スタティック VSAN の削除の概要 135
スタティック VSAN の削除 136
ロード バランシングの概要 137
ロード バランシングの設定 137
Interop モードの概要 138
スタティック VSAN 設定の表示 138
デフォルトの VSAN 設定 139
ゾーンの設定と管理 141
ゾーンの設定と管理 141
ゾーン分割に関する情報 141
ゾーン分割の特徴 141
ゾーン分割の例 143
ゾーン実装 144
アクティブおよびフル ゾーン セットの設定時の注意事項 145
ゾーンの設定 147
ゾーンの設定例 147
ゾーン セット 149
ゾーン セットのアクティブ化 149
デフォルト ゾーンの概要 150
デフォルト ゾーンのアクセス権限の設定 151

FC エイリアスの作成の概要 151
FC エイリアスの作成 152
FC エイリアスの作成例 152
ゾーン セットの作成とメンバ ゾーンの追加 153
ゾーンの実行 154
ゾーン セット配信 155
フル ゾーン セット配信のイネーブル化 155
ワンタイム配信のイネーブル化 156
リンクの分離からの回復の概要 156
ゾーン セットのインポートおよびエクスポート 157
ゾーン セット配信 158
ゾーン セットのコピー 158
ゾーン、ゾーン セット、およびエイリアスの名前の変更 159
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 159
ゾーン サーバ データベースのクリア 160
ゾーン情報の確認 161
拡張ゾーン分割 161
拡張ゾーン分割の概要 161
基本ゾーン分割から拡張ゾーン分割への変更 163
拡張ゾーン分割から基本ゾーン分割への変更 163
拡張ゾーン分割のイネーブル化 164
ゾーン データベースの変更 165
ゾーン データベース ロックの解除 166
データベースのマージ 166
ゾーン マージ制御ポリシーの設定 167
デフォルトのゾーン ポリシー 168
システムのデフォルト ゾーン分割設定値の設定 168
拡張ゾーン情報の確認 169
ゾーン データベースの圧縮 169
ゾーンおよびゾーン セットの分析 170
デフォルトの基本ゾーンの設定 170

DDAS 173

DDAS 173

デバイス エイリアスの概要 173

デバイス エイリアスの機能 173

デバイス エイリアスの前提条件 174

ゾーン エイリアスとデバイス エイリアスの比較 174

デバイス エイリアス データベース 175

デバイス エイリアスの作成 175

デバイス エイリアスのモード 176

デバイス エイリアス モードの変更時の注意事項 177

デバイス エイリアス モードの設定 177

デバイス エイリアス配信の概要 178

ファブリックのロック 179

変更のコミット 179

変更の破棄 179

ファブリックのロックの上書き 180

デバイス エイリアスの配布のディセーブル化とイネーブル化 181

レガシー ゾーン エイリアスの設定について 182

ゾーン エイリアスのインポート 182

デバイス エイリアス データベースの結合の注意事項 183

デバイス エイリアス設定の確認 183

デフォルトのデバイス エイリアス設定 184

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 187

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 187

FSPF に関する情報 187

FSPF の例 188

フォールト トレラント ファブリックの例 188

冗長リンクの例 188

FSPF のグローバル設定 189

SPF 計算ホールド タイムの概要 190

Link State Records の概要 190

VSAN での FSPF の設定 190

FSPF のデフォルト設定へのリセット 191

FSPF のイネーブル化またはディセーブル化 191
VSAN の FSPF カウンタのクリア 192
FSPF インターフェイスの設定 192
FSPF リンク コストの概要 193
FSPF リンク コストの設定 193
hello タイム インターバルの概要 193
hello タイム インターバルの設定 193
デッド タイム インターバルの概要 194
デッド タイム インターバルの設定 194
再送信インターバルの概要 195
再送信インターバルの設定 195
インターフェイス単位での FSPF のディセーブル化 196
特定のインターフェイスに対する FSPF のディセーブル化 196
インターフェイスの FSPF カウンタのクリア 197
FSPF ルート 197
ファイバ チャネル ルートの概要 198
ファイバ チャネル ルートの設定 198
順序どおりの配信 199
ネットワーク フレーム順序の再設定の概要 200
SAN ポート チャネル フレームの順序変更について 200
順序どおりの配信のイネーブル化の概要 201
順序どおりの配信のグローバルなイネーブル化 201
特定の VSAN に対する順序どおりの配信のイネーブル化 202
順序どおりの配信のステータスの表示 203
ドロップ遅延時間の設定 203
遅延情報の表示 204
フロー統計情報の設定 204
フロー統計の概要 204
集約フロー統計情報のカウント 204
個々のフロー統計情報のカウント 205
FIB 統計情報のクリア 205
フロー統計情報の表示 206

FSPF のデフォルト設定値 206
FLOGI、ネーム サーバ、FDMI、および RSCN データベースの管理 209
FLOGI、ネーム サーバ、FDMI、および RSCN データベースの管理 209
ファブリック ログインに関する情報 209
ネーム サーバ プロキシ 210
ネーム サーバ プロキシ登録の概要 210
ネーム サーバ プロキシの登録 210
重複 pWWN の拒否について 211
重複 pWWN の拒否 211
ネーム サーバ データベース エントリの概要 211
ネーム サーバのデータベース エントリの表示 212
FDMI 212
FDMI の表示 213
RSCN 213
RSCN 情報の概要 213
RSCN 情報の表示 213
[multi-pid] オプションの概要 214
[multi-pid] オプションの設定 214
ドメイン フォーマット SW-RSCN の抑制 215
RSCN 統計情報のクリア 215
RSCN タイマーの設定 215
RSCN タイマー設定の確認 217
RSCN タイマー設定の配布 217
RSCN タイマー設定の配布のイネーブル化 217
ファブリックのロック 218
RSCN タイマー設定の変更のコミット 218
RSCN タイマー設定の変更の廃棄 219
ロック済みセッションのクリア 219
RSCN 設定の配布情報の表示 219
デフォルトの RSCN 設定値 220
SCSI ターゲットの検出 221
SCSI ターゲットの検出 221
SCSI LUN 検出に関する情報 221

SCSI LUN 検出の開始について 221
SCSI LUN 検出の開始 222
カスタマイズ検出の開始について 223
カスタマイズ検出の開始 223
SCSI LUN 情報の表示 223
拡張ファイバ チャネル機能および概念 225
拡張ファイバ チャネル機能および概念 225
ファイバ チャネルのタイムアウト値 225
すべての VSAN のタイマー設定 225
VSAN ごとのタイマー設定 226
fctimer 配信の概要 227
fctimer の配布のイネーブル化とディセーブル化 227
fctimer 設定変更のコミット 228
fctimer 設定変更の廃棄 228
ファブリックのロックの上書き 229
FABRIC データベースの結合の注意事項 229
設定された fctimer 値の確認 230
World Wide Names（WWN） 230
WWN 情報の確認 231
リンク初期化 WWN の使用方法 231
セカンダリ MAC アドレスの設定 231
HBA の FC ID 割り当て 232
デフォルトの企業 ID リスト 232
企業 ID の設定の確認 234
スイッチの相互運用性 235
Interop モードの概要 235
interop モード 1 の設定 238
相互運用性ステータスの確認 240
拡張機能のデフォルト設定値 244
FC-SP および DHCHAP の設定 247
FC-SP および DHCHAP の設定 247
ファブリック認証に関する情報 247

DHCHAP 248
ファイバ チャネル機能と DHCHAP の互換性 249
DHCHAP イネーブル化の概要 250
DHCHAP のイネーブル化 250
DHCHAP 認証モードの概要 250
DHCHAP モードの設定 251
DHCHAP ハッシュ アルゴリズムの概要 252
DHCHAP ハッシュ アルゴリズムの設定 253
DHCHAP グループ設定の概要 253
DHCHAP グループの設定 253
DHCHAP パスワードの概要 254
ローカル スイッチの DHCHAP パスワードの設定 255
リモート デバイスのパスワード設定の概要 255
リモート デバイスの DHCHAP パスワードの設定 255
DHCHAP タイムアウト値の概要 256
DHCHAP タイムアウト値の設定 256
DHCHAP AAA 認証の設定 257
プロトコル セキュリティ情報の表示 257
設定例 257
デフォルトのファブリック セキュリティ設定値 259
ポート セキュリティの設定 261
ポート セキュリティの設定 261
ポート セキュリティについて 261
ポート セキュリティの実行 262
自動学習の概要 262
ポート セキュリティのアクティブ化 263
ポート セキュリティの設定 263
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 263
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 265
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 266
ポート セキュリティのイネーブル化 266
ポート セキュリティのアクティブ化 267

ポート セキュリティのアクティブ化 267
データベースのアクティブ化の拒否 268
ポート セキュリティの強制的なアクティブ化 268
データベースの再アクティブ化 269
自動学習 270
自動学習のイネーブル化について 270
自動学習のイネーブル化 270
自動学習のディセーブル化 271
自動学習デバイスの許可 271
許可される場合 272
ポート セキュリティの手動設定 274
WWN の識別に関する注意事項 274
許可済みのポート ペアの追加 275
ポート セキュリティ設定の配信 276
ポート セキュリティの配信のイネーブル化 276
ファブリックのロック 277
変更のコミット 278
変更の廃棄 278
アクティベーション設定と自動学習設定の配信 279
ポート セキュリティ データベース結合の注意事項 282
データベースの相互作用 282
データベースのシナリオ 284
ポート セキュリティ データベースのコピー 285
ポート セキュリティ データベースの削除 285
ポート セキュリティ データベースのクリア 285
ポート セキュリティ設定の表示 286
ポート セキュリティのデフォルト設定 286
ファブリック バインディングの設定 289
ファブリック バインディングの設定 289
ファブリック バインディングについて 289
ファブリック バインディングのライセンス要件 289
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 289

ファブリック バインディングの実行 291
ファブリック バインディングの設定 291
ファブリック バインディングの設定 291
ファブリック バインディングのイネーブル化 292
スイッチの WWN リストの概要 293
スイッチ WWN リストの設定 293
ファブリック バインディングのアクティベーションおよび非アクティベーション 293
ファブリック バインディングのアクティベーション 294
ファブリック バインディングの強制的なアクティベーション 294
ファブリック バインディング設定のコピー 295
ファブリック バインディング統計情報のクリア 296
ファブリック バインディング データベースの削除 296
ファブリック バインディング情報の確認 296
ファブリック バインディングのデフォルト設定 297
FCS の設定 299
FCS の設定 299
FCS の概要 299
FCS の特性 300
FCS 名の指定 301
FCS 情報の表示 302
FCS のデフォルト設定 302
ポート トラッキングの設定 303
ポート トラッキングの設定 303
ポート トラッキングに関する情報 303
ポート トラッキングのデフォルト設定値 305
ポート トラッキングの設定 305
ポート トラッキングのイネーブル化 305
リンク対象ポート設定の概要 306
トラッキング対象ポートの動作バインディング 306
複数ポート トラッキングの概要 307
複数ポートのトラッキング 307

VSAN 内のポートの監視の概要 308
VSAN 内のポートのモニタリングの概要 308
強制シャットダウンの概要 309
トラッキング対象ポートの強制シャットダウン 309
ポート トラッキング情報の表示 310

はじめに

ここでは、次の項について説明します。

- 対象読者，xix ページ
- 表記法，xix ページ
- 関連資料，xxi ページ
- マニュアルに関するフィードバック，xxiii ページ
- マニュアルの入手方法およびテクニカル サポート，xxiii ページ

対象読者

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

表記法

コマンドの説明には、次のような表記法が使用されます。

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

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

例では、次の表記法を使用しています。

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

このマニュアルでは、次の表記法を使用しています。

（注） 「注釈」です。 役立つ情報や、このマニュアル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

すべての Cisco NX-OS 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

リリース ノート

リリース ノートは、次の URL から入手できます。
http://www.cisco.com/en/US/products/ps9670/prod_release_notes_list.html

コンフィギュレーション ガイド

これらのガイドは、次の URL から入手できます。
http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html
このカテゴリのマニュアルには次のものが含まれます。

- 『*Adapter-FEX Configuration Guide*』
- 『*Cisco Fabric Manager Configuration Guide*』
- 『*Cisco Nexus 5000 Series NX-OS Software Configuration Guide*』
- 『*Configuration Limits for Cisco NX-OS*』
- 『*FabricPath Configuration Guide*』
- 『*Fibre Channel over Ethernet Configuration Guide*』
- 『*Layer 2 Switching Configuration Guide*』
- 『*Multicast Routing Configuration Guide*』
- 『*Operations Guide*』
- 『*SAN Switching Configuration Guide*』
- 『*Quality of Service Configuration Guide*』
- 『*Security Configuration Guide*』
- 『*System Management Configuration Guide*』

- 『*Unicast Routing Configuration Guide*』

メンテナンスおよび操作ガイド

各機能の『Cisco Nexus 5000 Series NX-OS Operations Guide』は、次の URL から入手できます。
http://www.cisco.com/en/US/products/ps9670/prod_maintenance_guides_list.html

インストレーション ガイドおよびアップグレード ガイド

これらのガイドは、次の URL から入手できます。

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

このカテゴリのマニュアルには次のものが含まれます。

- 『*FabricPath Command Reference*』
- ソフトウェア アップグレード/ダウングレード ガイド
- 規制の順守と安全に関する情報

ライセンス ガイド

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

コマンド リファレンス

これらのガイドは、次の URL から入手できます。

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

このカテゴリのマニュアルには次のものが含まれます。

- 『*Command Reference Master Index*』
- 『*Fabric Extender Command Reference*』
- 『*FabricPath Command Reference*』
- 『*Fibre Channel Command Reference*』
- 『*Fundamentals Command Reference*』
- 『*Layer 2 Interfaces Command Reference*』
- 『*Multicast Routing Command Reference*』
- 『*QoS Command Reference*』
- 『*Security Command Reference*』
- 『*System Management Command Reference*』
- 『*TrustSec Command Reference*』
- 『*Unicast Routing Command Reference*』

- 『*vPC Command Reference*』

テクニカル リファレンス

『*Cisco Nexus 5000 and Cisco Nexus 2000 MIBs Reference*』は、次の URL から入手できます。http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/mib/reference/NX5000_MIBRef.html

エラー メッセージおよびシステム メッセージ

『*Nexus 5000 Series NX-OS System Message Reference*』は、次の URL から入手できます。http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/system_messages/reference/sl_nxos_book.html

トラブルシューティング ガイド

『*Cisco Nexus 5000 Series Troubleshooting Guide*』は、次の URL から入手できます。http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/troubleshooting/guide/N5K_Troubleshooting_Guide.html

マニュアルに関するフィードバック

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

マニュアルの入手方法およびテクニカル サポート

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

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

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

第 1 章

このリリースの新規および変更情報

このリリースには新機能も変更された機能もありません。

第 2 章

概要

この章の内容は、次のとおりです。

- SAN スイッチングの概要，3 ページ

SAN スイッチングの概要

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

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、Cisco Nexus 5000 シリーズ スイッチではオプションです。 拡張モジュールを使用した場合、使用可能なファイバ チャネル ポートは、Cisco Nexus 5010 スイッチで最大 8 個、Cisco Nexus 5020 スイッチで最大 16 個です。

それぞれのファイバチャネルポートは、サーバに接続されたダウンリンクとして、またはデータセンター SAN ファブリックへのアップリンクとして使用できます。

ドメイン パラメータ

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 スイッチはランダムな ID を使用します。

N ポート バーチャライゼーション

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

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

VSAN トランキング

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

SAN ポート チャネル

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

Cisco NX-OS ソフトウェアでは、隣接するスイッチ間でポートチャネル設定情報を交換するときにプロトコルを使用するので、ポートチャネル管理が簡易化されます。たとえば、誤設定の検出や、互換性のある ISL でのポートチャネルの自動作成などの管理機能です。 自動設定モードでは、互換性のあるパラメータを使用する ISL によって、チャネル グループが自動的に構成されます。手動操作は必要ありません。

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

仮想 SAN

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

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

それぞれの VSAN は、独自の一連のファイバ チャネル ファブリック サービスを持つ論理的および機能的に別個の SAN です。 ファブリック サービスのこの分割は、個々の VSAN 内にファブリック再設定およびエラー条件を含めることにより、ネットワークの不安定さを大幅に軽減します。 VSAN が実現する厳密なトラフィック分離は、特定の VSAN の制御およびデータ トラフィックを VSAN 独自のドメイン内に限定することにより、SAN セキュリティを高めることができま

す。 VSAN は、可用性を低下させることなく、分離された SAN アイランドを共通のインフラストラクチャに容易に統合できるようにすることで、コストを削減できます。

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

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

ゾーン分割

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

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

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

デバイス エイリアス サービス

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

ファイバ チャネル ルーティング

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

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

SCSI ターゲット

SCSI ターゲットにはディスク、テープ、およびその他のストレージ デバイスが含まれます。 これらのターゲットは、ネーム サーバに論理ユニット番号（LUN）を登録しません。 SCSI LUN 検出機能は、CLI（コマンドライン インターフェイス）または SNMP（簡易ネットワーク管理プロトコル）を通して、オンデマンドで開始されます。 隣接スイッチが Cisco Nexus 5000 シリーズに含まれる場合、この情報はこれらのスイッチとも同期されます。

拡張ファイバ チャネル機能

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

単一のスイッチに WWN を一意に関連付ける必要があります。 主要スイッチの選択およびドメイン ID の割り当ては、WWN に依存します。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。

ファイバ チャネル標準では、任意のスイッチの F ポートに接続された N ポートに、一意の FC ID を割り当てる必要があります。 使用する FC ID 数を節約するために、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。

FC-SP および DHCHAP

Fibre Channel Security Protocol（FC-SP）は、スイッチ間およびホストとスイッチ間で認証を実行して、企業全体のファブリックに関するセキュリティ問題を解決します。 Diffie-Hellman チャレンジ ハンドシェイク認証プロトコル（DHCHAP）は、Cisco SAN スイッチとその他のデバイス間で認

証を行う FC-SP プロトコルです。 DHCHAP は、CHAP プロトコルと Diffie-Hellman 交換を組み合わせて構成されています。

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

ポート セキュリティ

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

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

ファブリック バインディング

ファブリック バインディングは、ファブリック バインディング設定で指定されたスイッチ間のみでスイッチ間リンク（ISL）がイネーブルにされるようにします。これによって、無許可のスイッチが、ファブリックに参加したり、現在のファブリック処理が中断したりできないようにします。この機能では、Exchange Fabric Membership Data（EEMD）プロトコルを使用することによって、許可されたスイッチのリストがファブリック内の全スイッチで同一になります。

Fabric Configuration Server

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

第 3 章

ファイバチャネルインターフェイスの設定

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設定，9 ページ

ファイバ チャネル インターフェイスの設定

ファイバ チャネル インターフェイスの概要

ファイバ チャネルのライセンス要件

Cisco Nexus 5000 シリーズ スイッチでは、ファイバ チャネル機能は Storage Protocol Services ライセンスに含まれます。

ファイバチャネルインターフェイスとその機能を使用する前に、正しいライセンス（N5010SS または N5020SS）がインストールされていることを確認します。

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

物理ファイバ チャネル インターフェイス

Cisco Nexus 5000 シリーズ スイッチは、2 つのオプション拡張モジュールを使用することにより、最大 16 の物理ファイバ チャネル（FC）アップリンクをサポートします。 最初のモジュールには 8 つの FC インターフェイスが搭載されています。 2 番めのモジュールには 4 つのファイバ チャネル ポートと 4 つのイーサネット ポートが搭載されています。

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、E、F、NP、TE、TF、TNP、SD、auto の各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）カプセル化により、物理イーサネット ケーブルでファイバ チャネルとイーサネット トラフィックを同時に伝送できます。 Cisco Nexus 5000 シリーズ スイッチでは、FCoE 対応の物理イーサネット インターフェイスは、1 つの仮想ファイバ チャネル（vFC）インターフェイスのトラフィックを伝送できます。

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

vFC インターフェイスは、F モードだけをサポートし、トランク モードでだけ動作します。

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

- SAN ポート チャネル
- SPAN 宛先は vFC インターフェイスにすることはできません。
- Buffer-to-Buffer credit（BB_credit）
- Exchange Link Parameter（ELP）または Fabric Shortest Path First（FSPF）プロトコル
- 物理属性の設定（速度、レート、モード、トランスミッタ情報、MTU サイズ）
- ポート トラッキング

VF ポート

Cisco NX-OS Release 5.0(2)N1(1) 以降では、vFC インターフェイスは常にトランク モードで動作します。その他のモードでは動作しません。 vFC インターフェイスでは、**switchport trunk allowed vsan** コマンドを使用して vFC の許可 VSAN を設定できます（FC TF および TE ポートと類似）。ホストに接続されている vFC インターフェイスの場合、ログイン（FLOGI）をサポートする VSAN はポート VSAN だけです。 VF ポートを設定する **switchport trunk allowed vsan** コマンドをインターフェイス モードで使用し、このような vFC インターフェイスの許可 VSAN をポート VSAN に制限することを推奨します。

Cisco NX-OS Release 5.0(2)N1(1) には、160 の vFC インターフェイスのサポートが含まれます。

Cisco Nexus 5000 シリーズ スイッチは、vFC VSAN 割り当てとグローバルな VLAN-to-VSAN マッピング テーブルにより、VF ポートに対して適切な VLAN を選択できます。

10G-FEX インターフェイス上の VF ポート サポート機能は、Cisco Nexus 2000 シリーズ ファブリック エクステンダのストレート型トポロジでだけサポートされます。各ファブリック エクステンダは Cisco Nexus 5000 シリーズ スイッチに直接接続されます。

VE ポート

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

VE ポートに関する注意事項は次のとおりです。

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

  VE ポート上に複数の VSAN を設定できます。 VE ポートの VSAN に対応する FCoE VLAN を、バインドしたイーサネット インターフェイスに設定する必要があります。
- スパニングツリープロトコルは、vFC インターフェイスがバインドされたすべてのインターフェイスの FCoE VLAN 上でディセーブルになります。これには、VE ポートがバインドされたインターフェイスが含まれます。

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

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

vPC トポロジの VE ポート

vPC トポロジの VE ポートに関する注意事項は次のとおりです。

- LAN トラフィック用の vPC 上で接続された FCF 間の FCoE VLAN には、専用リンクが必要です。
- FCoE VLAN はスイッチ間の vPC インターフェイス上に設定しないでください。

FSPF のパラメータ

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

VE ポート設定の制限

インターフェイスタイプ	プラットフォーム		
	Cisco Nexus 50xx シリーズ スイッチ	**Cisco Nexus 5500** シリーズ スイッチ	**10 G** のファブリック エクステンダ
イーサネット インターフェイスにバインドされた VE ポート	16 の VE ポート	16 の VE ポート	未サポート
イーサネット ポートチャネル インターフェイスにバインドされた VE ポート	4 つの VE ポート（特定のピアに対して 1 つの VE ポートに制限）。	4 つの VE ポート	未サポート

VNP ポート

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

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

インターフェイス モード

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

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

仮想ファイバ チャネル インターフェイスは F モードでだけ設定できます。

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

各インターフェイスには、管理設定と動作ステータスが対応付けられます。

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

関連トピック

VSAN の設定と管理, （125 ページ）
NPV の設定, （59 ページ）

E ポート

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

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

関連トピック

SAN ポート チャネルの設定, （103 ページ）

F ポート

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

NP ポート

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

関連トピック

NPV の設定, （59 ページ）

TE ポート

トランキング E ポート（TE ポート）モードでは、インターフェイスがトランキング拡張ポートとして機能します。 別の TE ポートに接続し、2 つのスイッチ間で Extended ISL（EISL）を作成しま

す。 TE ポートは別の Cisco Nexus 5000 シリーズ スイッチまたは Cisco MDS 9000 ファミリ スイッチに接続します。 E ポートの機能を拡張して、次の内容をサポートします。

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

TE ポート モードでは、すべてのフレームが VSAN 情報を含む EISL フレーム フォーマットで送信されます。 相互接続されたスイッチは VSAN ID を使用して、1 つまたは複数の VSAN からのトラフィックを同一の物理リンク上で多重化します。 この機能は、Cisco Nexus 5000 シリーズ スイッチでは VSAN トランキングと呼ばれます。 TE ポートは、クラス 3 およびクラス F サービスをサポートします。

関連トピック

VSAN トランキングの設定, （93 ページ）

TF ポート

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

トランキング F ポート（TF ポート）モードでは、インターフェイスがトランキング拡張ポートとして機能します。 トランキングした別の N ポート（TN ポート）または NP ポート（TNP ポート）に接続して、コア スイッチと NPV スイッチまたは HBA の間のリンクを作成し、タグ付きフレームを伝送できます。 TF ポートは、F ポートの機能を拡張して、VSAN トランキングをサポートします。

TF ポート モードでは、すべてのフレームが、VSAN 情報を含む EISL フレーム フォーマットで送信されます。 相互接続されたスイッチは VSAN ID を使用して、1 つまたは複数の VSAN からのトラフィックを同一の物理リンク上で多重化します。 この機能は、Cisco Nexus 5000 シリーズ スイッチでは VSAN トランキングと呼ばれます。 TF ポートは、クラス 3 およびクラス F サービスをサポートします。

TNP ポート

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

SD ポート

SPAN 宛先ポート（SD ポート）モードでは、インターフェイスがスイッチド ポート アナライザ（SPAN）として機能します。 SPAN 機能は、ファイバ チャネル インターフェイスを通過するネットワーク トラフィックをモニタします。 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。送信元トラフィックのコピーを送信するだけです。 SPAN 機能は他

の機能に割り込むことなく、SPAN 送信元ポートのネットワーク トラフィックのスイッチングに影響しません。

auto モード

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

SD ポートは初期化で判別されず、管理上設定されます。

関連トピック

VSAN トランキングの設定, （93 ページ）

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。

管理ステート

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

表 *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。 次の表に、動作ステートを示します。

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

理由コード

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

表 *3*：インターフェイス ステートの理由コード

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

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

（注） 表に示されている理由コードは一部だけです。

表 *4* : 動作不能ステートの理由コード

理由コード（長いバージョン）	説明	適用可能なモード
Link failure or not connected	物理層リンクが正常に動作していません。	All
SFP not present	Small Form-Factor Pluggable ハードウェアが接続されていません。	All
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。	All
Reconfigure fabric in progress	ファブリックが現在再設定されています。	
Offline	初期化を再試行する前に、スイッチ ソフトウェアが指定された R_A_TOV 時間待機します。	
Inactive	インターフェイス VSAN が削除されているか、suspended ステートにあります。 インターフェイスを正常に動作させるには、設定されたアクティブな VSAN にポートを割り当てます。	
Hardware failure	ハードウェア障害が検出されました。	

理由コード（長いバージョン）	説明	適用可能なモード
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ることがあります。 次に例を示します。 • 設定障害。 • 互換性のない BB_credit 設定。 インターフェイスを正常に動作させるには、まずこのステートの原因となるエラー条件を修正し、次にインターフェイスを管理上シャットダウンにするか、インターフェイスをイネーブルにします。	
Isolation because limit of active port channels is exceeded.	スイッチにアクティブ SAN ポート チャネルの最大数がすでに設定されているので、インターフェイスは隔離されます。	
Isolation due to ELP failure	ポート ネゴシエーションが失敗しました。	E ポートと TE ポートのみ
Isolation due to ESC failure	ポート ネゴシエーションが失敗しました。	
Isolation due to domain overlap	Fibre Channel Domain（fcdomain）のオーバーラップ。	
Isolation due to domain ID assignment failure	割り当てられたドメイン ID が無効です。	
Isolation due to the other side of the link E port isolated	リンクのもう一方の端の E ポートが分離しています。	
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。	

理由コード（長いバージョン）	説明	適用可能なモード
Isolation due to zone merge failure	ゾーン結合に失敗しました。	
Isolation due to VSAN mismatch	ISL の両端の VSAN が異なります。	
port channel administratively down	SAN ポート チャネルに所属するインターフェイスがダウンの状態です。	SAN ポート チャネル インターフェイスのみ
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一のスイッチ ペアに接続されている必要があります。	
Bound physical interface down	仮想ファイバ チャネル インターフェイスにバインドされたイーサネット インターフェイスが動作していません。	仮想ファイバ チャネル インターフェイスのみ
STP not forwarding in FCoE mapped VLAN	仮想ファイバ チャネル インターフェイスにバインドされたイーサネット インターフェイスが、仮想ファイバ チャネル インターフェイスに関連付けられた VLAN に対して STP フォワーディング ステートではありません。	仮想ファイバ チャネル インターフェイスのみ

Buffer-to-Buffer credit（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。

Cisco Nexus デバイスでは、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。 受信 BB_credit では、ピアへの確認応答を必要とせずに、受信側の受信バッファの容量が決まります。 これは、帯域幅遅延が大きいリンク（遅延が大きい長距離リンク）で、遅延時間が長い回線レート トラフィックを維持できるようにするうえで重要です。

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

仮想ファイバ チャネル インターフェイスの場合、BB_credit は使用されません。 仮想ファイバ チャネルインターフェイスは、基本の物理イーサネットインターフェイスの機能に基づいて、フロー制御を実行します。

（注） 受信 BB_credit 値は、ポート モードによって異なります。 物理ファイバ チャネル インターフェイスの場合、F モードおよび E モード インターフェイスのデフォルト値は 16 です。 必要に応じて、この値を変更できます。 最大値は 240 です。

ファイバ チャネル インターフェイスの設定

ファイバ チャネル インターフェイスの設定

ファイバ チャネル インターフェイスを設定する手順は、次のとおりです。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {**fc** *slot*/*port*}|{**vfc** *vfc-id*}	ファイバ チャネル インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。 （注） ファイバ チャネル インターフェイスが設定された場合、自動的に一意の World Wide Name（WWN）が割り当てられます。インターフェイスの動作ステートが up の場合、ファイバ チャネル ID（FC ID）も割り当てられます。

ファイバ チャネル インターフェイスの範囲の設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** { **fc** *slot*/*port* - *port* [, **fc** *slot*/*port* - *port*] | **vfc** *vfc-id* - *vfc-id* [, **vfc** *vfc-id* - *vfc-id*] }	ファイバ チャネル インターフェイスの範囲を選択し、インターフェイス コンフィギュレーション モードを開始します。

インターフェイス管理ステートの設定

インターフェイスを正常にシャットダウンする手順は、次のとおりです。

トラフィック フローをイネーブルにする手順は、次のとおりです。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface** {**fc** *slot*/*port*}|{**vfc** *vfc-id*}	ファイバ チャネル インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **shutdown**	インターフェイスを正常にシャットダウンし、トラフィック フローを管理上ディセーブルにします（デフォルト）。

インターフェイス モードの設定

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	switch(config) # **interface vfc** *vfc-id*}
	
	例：
	`switch(config) # interface vfc 20`
	`switch(config-if) #`
		仮想ファイバ チャネル インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	switch(config-if) # **switchport mode** {**E**|**NP**}
	
	例：
	`switch(config-if) # switchport mode E`
	`switch(config-if) #`
		ポート モードを設定します。
		vFC インターフェイスは、モード E および NP だけをサポートします。
		（注） SD ポートを自動では設定できません。 このポートは管理上設定する必要があります。

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

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

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

```
switch# show running-config
switch(config) # interface vfc20
switch(config-if) # bind interface Ethernet 1/3
switch(config-if) # switchport mode E
switch(config-if) # no shutdown
```

次に、VNP ポート 10 を設定し、イーサネット スロット 2、ポート 1 にバインドする例を示します。

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

インターフェイスの説明の設定

インターフェイスの説明は、トラフィックを識別したり、インターフェイスの使用状況を知る場合に役立ちます。 インターフェイスの説明には、任意の英数字ストリングを指定できます。

インターフェイスの説明を設定する手順は、次のとおりです。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {**fc** *slot*/*port*}|{**vfc** *vfc-id*}	ファイバ チャネル インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **switchport description cisco-HBA2**	インターフェイスの説明を設定します。ストリングの長さは、最大 80 文字まで可能です。
ステップ 4	switch(config-if)# **no switchport description**	インターフェイスの説明をクリアします。

ポート速度の設定

ポート速度は、物理ファイバ チャネル インターフェイスで設定できますが、仮想ファイバ チャネルインターフェイスでは設定できません。デフォルトでは、インターフェイスのポート速度はスイッチによって自動計算されます。

注意 ポート速度の変更は中断を伴う動作です。

インターフェイスのポート速度を設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **interface fc** *slot*/*port*
3. switch(config-if)# **switchport speed 1000**
4. switch(config-if)# **no switchport speed**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface fc** *slot*/*port*	指定されたインターフェイスを選択して、インターフェイス コンフィギュレーション モードを開始します。 （注） 仮想ファイバ チャネル インターフェイスのポート速度は設定できません。
ステップ 3	switch(config-if)# **switchport speed 1000**	インターフェイスのポート速度を 1000 Mbps に設定します。 数値は、Mbps 単位の速度を表します。 1 Gbps インターフェイスには 1000 Mbps の速度、2 Gbps インターフェイスには 2000 Mbps の速度、4 Gbps インターフェイスには 4000、または auto（デフォルト）を設定できます。
ステップ 4	switch(config-if)# **no switchport speed**	インターフェイスの管理速度を工場出荷時のデフォルト（auto）に戻します。

自動検知

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

SD ポート フレーム カプセル化の設定

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

switchport encap eisl コマンドは、デフォルトではディセーブルです。 カプセル化をイネーブルにする場合、すべての発信フレームがカプセル化され、**show interface** *SD_port_interface* コマンド出力に新しい行（Encapsulation is eisl）が表示されます。

受信データ フィールド サイズの設定

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

受信データ フィールド サイズを設定する手順は、次のとおりです。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface fc** *slot*/*port*	ファイバ チャネル インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **switchport fcrxbufsize 2000**	選択されたインターフェイスのデータ フィールド サイズを 2000 バイトに減らします。 デフォルトは 2112 バイトで、範囲は 256 ～ 2112 バイトです。

ビット エラーしきい値の概要

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

ビット エラーは次のような理由のため発生します。

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

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

shutdown/**no shutdown** コマンドを入力して、インターフェイスを再度イネーブルにできます。

しきい値を超えてもインターフェイスがディセーブルにならないようにスイッチを設定できます。

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface fc** *slot*/*port*	ファイバ チャネル インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **switchport ignore bit-errors**	ビットエラーしきい値イベントを検出したとき、インターフェイスがディセーブルにならないようにします。

	コマンドまたはアクション	目的
ステップ 4	switch(config-if)# **no switchport ignore bit-errors**	ビットエラーしきい値イベントを検出したとき、インターフェイスがイネーブルにならないようにします。

BB_credit の設定

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface fc** *slot*/*port*	ファイバ チャネル インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **switchport fcrxbbcredit default**	デフォルトの使用可能な値を選択されたインターフェイスに適用します。 使用可能な値は、ポート モードによって異なります。 デフォルト値は、ポート機能に応じて割り当てられます。
ステップ 4	switch(config-if)# **switchport fcrxbbcredit** *number* **mode** {**E** | **F** | **TE**}	選択したインターフェイスに Buffer-to-Buffer credit 番号を割り当て、必要に応じてポートが E、F、または TE のどのモードで動作するかを指定します。 （注） **mode** に **E**、**F**、または **TE** を指定すると、ポートをそのモードに設定した場合にのみ Buffer-to-Buffer credit 値が適用可能になります。 Buffer-to-Buffer credit には、*number* で 1～240 の範囲の番号を指定します。 デフォルト値は 16 です。
ステップ 5	switch(config-if)# **do show int fc** *slot*/*port*	送受信の Buffer-to-Buffer credit を、このインターフェイスのその他の関連インターフェイス情報とともに表示します。

	コマンドまたはアクション	目的
		（注） 正しい Buffer-to-Buffer credit 値は、レジスタの読み取り時に得られます。 データ トラフィックが遅いときに状況を確認するのに役立ちます。
ステップ 6	switch(config-if)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

ファイバ チャネル インターフェイスのグローバル属性の設定

スイッチ ポート属性のデフォルト値の設定

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

スイッチ ポート属性を設定する手順は、次のとおりです。

手順の概要

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

手順の詳細

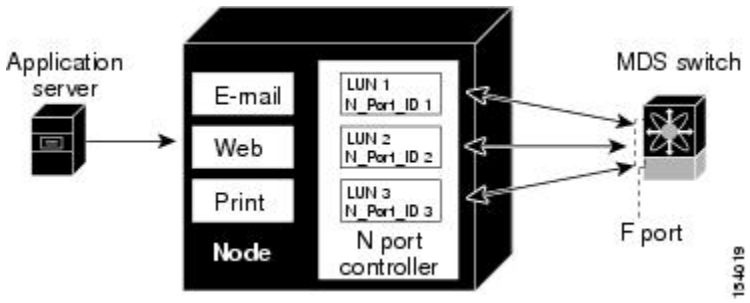
	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no system default switchport shutdown san**	インターフェイス管理ステートのデフォルト設定を up に設定します （出荷時のデフォルト設定は down です）。 ヒント このコマンドは、管理ステートに対してユーザ設定が存在しないインターフェイスにだけ適用されます。
ステップ 3	switch(config)# **system default switchport shutdown san**	インターフェイス管理ステートのデフォルト設定を down に設定します。 これが出荷時のデフォルト設定です。 ヒント このコマンドは、管理ステートに対してユーザ設定が存在しないインターフェイスにだけ適用されます。

	コマンドまたはアクション	目的
ステップ 4	switch(config)# **system default switchport trunk mode auto**	インターフェイスの管理トランク モード ステートのデフォルト設定を auto に設定します。 （注） デフォルト設定のトランク モードは on です。

N ポート ID バーチャライゼーションの概要

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

図 *1* : ***NPIV*** の例



N ポート ID バーチャライゼーションのイネーブル化

スイッチの NPIV 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。

はじめる前に

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

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

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **feature npiv**
3. switch(config)# **no feature npiv**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **feature npiv**	スイッチ上のすべての VSAN の NPIV をイネーブルにします。
ステップ 3	switch(config)# **no feature npiv**	スイッチ上の NPIV をディセーブルにします（デフォルト）。

ポート チャネルの設定例

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

次の例は、ポート チャネルの作成方法を示しています。

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

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

```
switch(config)# interface fc1/4-6
switch(config-if)# shut
switch(config-if)# switchport mode F
switch(config-if)# switchport speed 4000
switch(config-if)# switchport rate-mode dedicated
switch(config-if)# switchport trunk mode on
switch(config-if)# channel-group 2
switch(config-if)# no shut
switch(config-if)# exit
```

次に、NPV スイッチで専用モードでポート チャネルを作成する例を示します。

```
switch(config)# interface san-port-channel 2
switch(config-if)# switchport mode NP
switch(config-if)# no shut
switch(config-if)# exit
```

次に、NPV スイッチ上でポート チャネル メンバ インターフェイスを設定する例を示します。

```
switch(config)# interface fc2/1-2
switch(config-if)# shut
switch(config-if)# switchport mode NP
switch(config-if)# switchport trunk mode on
switch(config-if)# channel-group 2
switch(config-if)# no shut
switch(config-if)# exit
```

ファイバ チャネル インターフェイスの確認

SFP トランスミッタ タイプの確認

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

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

インターフェイス情報の確認

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

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

次に、すべてのインターフェイスを表示する例を示します。

```
switch# show interface

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

次に、指定された複数のインターフェイスを表示する例を示します。

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

次に、特定の 1 つのインターフェイスを表示する例を示します。

```
switch# show interface vfc 1
vfc 1 is up
...
```

次に、インターフェイスの説明を表示する例を示します。

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

次に、すべてのインターフェイスを表示する例を示します（簡略）。

```
switch# show interface brief
```

次に、インターフェイス カウンタを表示する例を示します。

```
switch# show interface counters
```

次に、特定のインターフェイスのトランシーバ情報を表示する例を示します。

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

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

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

次の例では、すべてのインターフェイスの実行コンフィギュレーションを表示する場合のインターフェイスの表示を示します。

```
switch# show running configuration
...
interface fc3/5
  switchport speed 2000
...
interface fc3/5
  switchport mode E
...
interface fc3/5
  channel-group 11 force
  no shutdown
```

次の例では、特定のインターフェイスの実行コンフィギュレーションを表示する場合のインターフェイスの表示を示します。

```
switch# show running configuration fc3/5
interface fc3/5
  switchport speed 2000
```

```
  switchport mode E
  channel-group 11 force
  no shutdown
```

BB_credit 情報の確認

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

```
switch# show interface bbcredit
...
fc2/3 is trunking
    Transmit B2B Credit is 255
    Receive B2B Credit is 12
    Receive B2B Credit performance buffers is 375
      12 receive B2B credit remaining
      255 transmit B2B credit remaining
```

ファイバ チャネル インターフェイスのデフォルト設定

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

表 *5*：デフォルトのネイティブ ファイバ チャネル インターフェイス パラメータ

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

次の表に、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を示します。

表 *6*：デフォルトの仮想ファイバ チャネル インターフェイス パラメータ

パラメータ	デフォルト
インターフェイス モード	F モード
インターフェイス速度	n/a
管理ステート	Shutdown（初期設定時に変更された場合を除く）
トランク モード	On
トランク許可 VSAN	すべての VSAN
インターフェイス VSAN	デフォルト VSAN（1）
EISL カプセル化	n/a
データ フィールド サイズ	n/a

第 4 章

ドメイン パラメータの設定

この章の内容は、次のとおりです。

- ドメイン パラメータの設定，35 ページ

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 スイッチはランダムな ID を使用します。

注意 fcdomain パラメータは、通常変更しないでください。 これらの変更は、管理者が行うか、スイッチ操作を熟知している人が行ってください。

設定を変更した場合は、必ず実行コンフィギュレーションを保存してください。 次回にスイッチを再起動したときに、保存された設定が使用されます。 設定を保存しない場合は、前回保存されたスタートアップ コンフィギュレーションが使用されます。

ファイバ チャネル ドメインについて

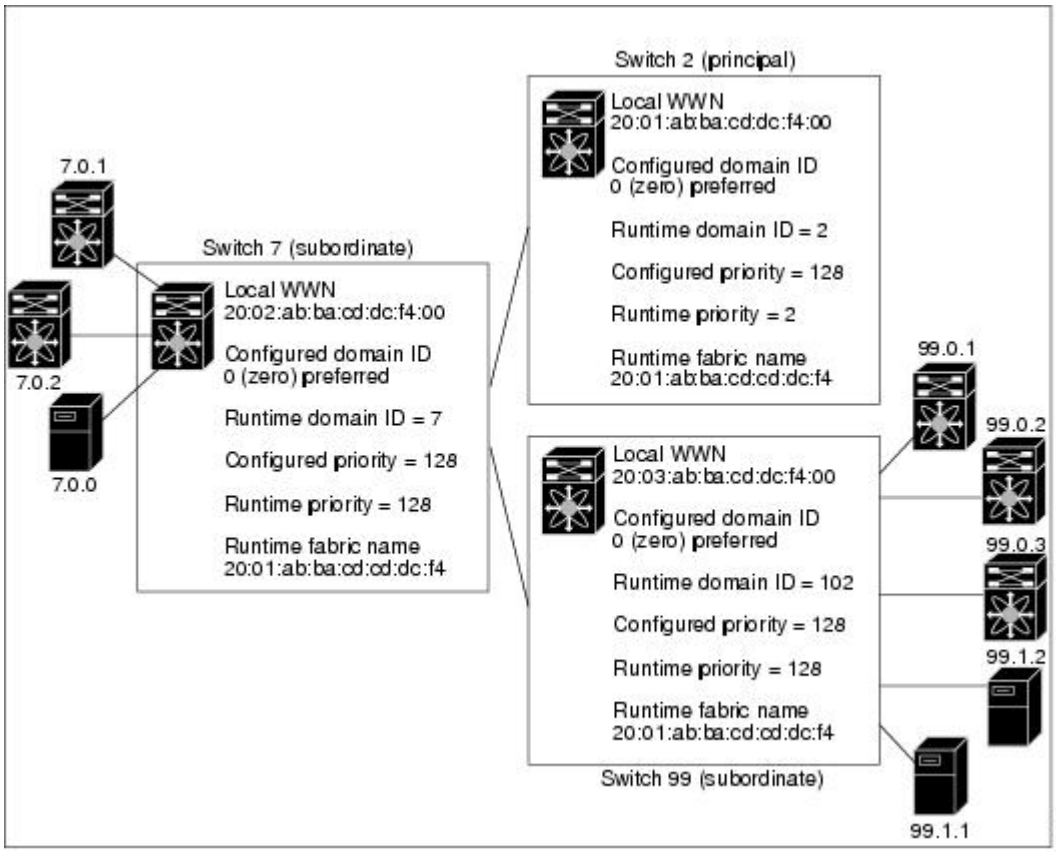
ここでは、fcdomain の各フェーズについて説明します。

- 主要スイッチの選択：このフェーズでは、ファブリック内で一意の主要スイッチを選択できます。
- ドメイン ID の配信：このフェーズでは、ファブリック内のスイッチごとに、一意のドメイン ID を取得できます。
- FC ID の割り当て：このフェーズでは、ファブリック内の対応するスイッチに接続された各デバイスに、一意の FC ID を割り当てることができます。

- ファブリックの再設定：このフェーズでは、ファブリック内のすべてのスイッチを再同期化して、新しい主要スイッチ選択フェーズを同時に再開できるようにします。

次の図は、fcdomain の設定例を示します。

図 *2*： *fcdomain* の設定例



ドメインの再起動の概要

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

ドメイン ID の競合を解消するには、手動でドメイン ID を割り当てる必要があります。 ドメイン ID を手動で割り当てるなど、ほとんどの設定変更では中断再起動が必要になります。 ドメインの非中断再起動は、優先ドメイン ID をスタティック ドメイン ID（実ドメイン ID は変更なし）に変更する場合にかぎり実行できます。

（注） スタティック ドメインはユーザによって固有に設定されるため、実行時のドメインと異なることがあります。ドメインIDが異なる場合は、次回の中断または非中断再起動後にスタティック ドメイン ID を使用するように、実行時のドメイン ID が変更されます。

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

ほとんどの設定は、対応する実行時の値に適用できます。ここでは、実行時の値にfcdomainパラメータを適用する方法について詳細に説明します。

fcdomain restart コマンドを使用すると、変更が実行時の設定に適用されます。disruptiveオプションを使用すると、優先ドメインIDなどほとんどの設定は、対応する実行時の値に適用されます。

ドメインの再起動

ファブリックの中断再起動または非中断再起動を実行する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcdomain restart vsan** *vsan-id*
3. switch(config)# **fcdomain restart disruptive vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcdomain restart vsan** *vsan-id*	トラフィックを中断しないで再設定するようにVSANを設定します。
ステップ 3	switch(config)# **fcdomain restart disruptive vsan** *vsan-id*	データ トラフィックを中断して再設定するようにVSANを設定します。

ドメイン マネージャの高速再起動について

主要リンクで障害が発生した場合、ドメイン マネージャが新しい主要リンクを選択する必要があります。デフォルトでは、ドメイン マネージャはBuild Fabric（BF）フェーズを開始し、その後主要スイッチ選択フェーズが続きます。これらのフェーズは両方ともVSAN内のすべてのスイッチに影響を及ぼし、完了するまで合計15秒以上かかります。ドメイン マネージャが新しい主要リンクの選択に必要な時間を短縮するために、ドメイン マネージャの高速再起動機能をイネーブルにできます。

高速再起動がイネーブルで、バックアップ リンクを利用できる場合、ドメイン マネージャはわずか数ミリ秒で新しい主要リンクを選択し、障害が発生したリンクを交換します。 また、新しい主要リンクの選択に必要な再設定は、VSAN 全体ではなく、障害が発生したリンクに直接接続した 2 つのスイッチにだけ影響します。 バックアップ リンクが利用できない場合、ドメイン マネージャはデフォルトの動作に戻り、BF フェーズを開始します。その後、主要スイッチ選択フェーズが続きます。 高速再起動機能はどのインターオペラビリティ モードでも使用できます。

ドメイン マネージャの高速再起動のイネーブル化

ドメイン マネージャの高速再起動機能をイネーブルにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcdomain optimize fast-restart vsan** *vsan-id*
3. switch(config)# **fcdomain optimize fast-restart vsan** *vsan-id* **-** *vsan-id*
4. switch(config)# **no fcdomain optimize fast-restart vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcdomain optimize fast-restart vsan** *vsan-id*	指定された VSAN でドメイン マネージャの高速再起動をイネーブルにします。
ステップ 3	switch(config)# **fcdomain optimize fast-restart vsan** *vsan-id* **-** *vsan-id*	指定された VSAN の範囲でドメイン マネージャの高速再起動をイネーブルにします。
ステップ 4	switch(config)# **no fcdomain optimize fast-restart vsan** *vsan-id*	指定された VSAN でドメイン マネージャの高速再起動をディセーブル（デフォルト）にします。

スイッチ プライオリティの概要

デフォルトでプライオリティ 128 が設定されています。 プライオリティの有効設定範囲は 1 ～ 254 です。 プライオリティ 1 が最高のプライオリティです。 値 255 は、他のスイッチからは受け入れられますが、ローカルには設定できません。

安定したファブリックに追加された新しいスイッチが、主要スイッチになることはありません。主要スイッチ選択フェーズ中に、最高のプライオリティを持つスイッチが主要スイッチになります。 2 つのスイッチに同じプライオリティが設定されている場合、小さい World Wide Name（WWN）のスイッチが主要スイッチになります。

プライオリティ設定は、fcdomain の再起動時にランタイムに適用されます。 この設定は、中断再起動および非中断再起動のどちらにも適用できます。

スイッチ プライオリティの設定

主要スイッチにプライオリティを設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcdomain priority** *number* **vsan** *vsan-id*
3. switch(config)# **no fcdomain priority** *number* **vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcdomain priority** *number* **vsan** *vsan-id*	指定された VSAN 内のローカル スイッチに指定されたプライオリティを設定します。
ステップ 3	switch(config)# **no fcdomain priority** *number* **vsan** *vsan-id*	指定されたVSANのプライオリティを出荷時の設定（128）に戻します。

fcdomain の初期化の概要

デフォルトでは、fcdomain 機能は各スイッチ上でイネーブルになっています。 スイッチ内で fcdomain 機能をディセーブルにすると、そのスイッチはファブリック内のその他のスイッチと共存できなくなります。 fcdomain 設定は中断再起動の実行時に適用されます。

fcdomain のディセーブル化または再イネーブル化

単一の VSAN または VSAN 範囲で fcdomain をディセーブルまたは再度イネーブルにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **no fcdomain vsan** *vsan-id* **-** *vsan-id*
3. switch(config)# **fcdomain vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **no fcdomain vsan** *vsan-id* **-** *vsan-id*	指定された VSAN 範囲で fcdomain 設定をディセーブルにします。
ステップ 3	switch(config)# **fcdomain vsan** *vsan-id*	指定された VSAN で fcdomain 設定をイネーブルにします。

ファブリック名の設定

ディセーブルにされた fcdomain にファブリック名を設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan** *vsan-id*
3. switch(config)# **no fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan** *vsan-id*	指定された VSAN に設定済みファブリック名の値を割り当てます。
ステップ 3	switch(config)# **no fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan** *vsan-id*	VSAN 3010 のファブリック名の値を出荷時のデフォルト設定（20:01:00:05:30:00:28:df）に変更します。

着信 RCF の概要

rcf-reject オプションはインターフェイス単位、VSAN 単位で設定できます。 デフォルトでは、rcf-reject オプションはディセーブルです（つまり、RCF 要求フレームは自動的に拒否されません）。

rcf-reject オプションは即座に有効になります。

fcdomain の再起動は不要です。

（注） 仮想ファイバ チャネル インターフェイスの RCF 拒否オプションを設定する必要はありません。

着信 RCF の拒否

着信 RCF 要求フレームを拒否する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **interface fc** *slot/port*
3. switch(config-if)# **fcdomain rcf-reject vsan** *vsan-id*
4. switch(config-if)# **no fcdomain rcf-reject vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface fc** *slot/port*	指定されたインターフェイスを設定します。
ステップ 3	switch(config-if)# **fcdomain rcf-reject vsan** *vsan-id*	指定されたVSAN内の指定されたインターフェイス上で RCF フィルタをイネーブルにします。
ステップ 4	switch(config-if)# **no fcdomain rcf-reject vsan** *vsan-id*	指定されたVSAN内の指定されたインターフェイス上でRCFフィルタをディセーブル（デフォルト）にします。

結合ファブリックの自動再構成の概要

デフォルトでは、autoreconfigureオプションはディセーブルです。 重複ドメインを含む、2つの異なる安定したファブリックに属する 2 つのスイッチを結合した場合は、次のようになります。

- 両方のスイッチで autoreconfigure オプションがイネーブルの場合、中断再設定フェーズが開始します。
- いずれかまたは両方のスイッチで autoreconfigure オプションがディセーブルの場合は、2 つのスイッチ間のリンクが隔離されます。

autoreconfigure オプションは実行時に即座に有効になります。 fcdomain を再起動する必要はありません。 ドメインが重複によって現在隔離されており、後で両方のスイッチの autoreconfigure オ

プションをイネーブルにする場合は、ファブリックは隔離状態のままです。 ファブリックを接続する前に両方のスイッチでautoreconfigureオプションをイネーブルにした場合、中断再設定（RCF）が発生します。 中断再設定が発生すると、データ トラフィックが影響を受けることがあります。 fcdomain に非中断再設定を行うには、重複リンク上の設定済みドメインを変更し、ドメインの重複を排除します。

自動再設定のイネーブル化

特定の VSAN（または VSAN 範囲）で自動再設定をイネーブルにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcdomain auto-reconfigure vsan** *vsan-id*
3. switch(config)# **no fcdomain auto-reconfigure vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcdomain auto-reconfigure vsan** *vsan-id*	指定された VSAN で自動再設定オプションをイネーブルにします。
ステップ 3	switch(config)# **no fcdomain auto-reconfigure vsan** *vsan-id*	指定された VSAN で自動再設定オプションをディセーブルにし、出荷時のデフォルト設定に戻します。

ドメイン ID

ドメイン ID は VSAN 内のスイッチを一意に識別します。 スイッチは異なる VSAN に異なるドメイン ID を持つことがあります。 ドメイン ID は FC ID 全体の一部です。

ドメイン ID の概要

設定済みドメイン ID のタイプは優先またはスタティックになります。 デフォルトで、設定済みドメイン ID は 0（ゼロ）、設定タイプは優先です。

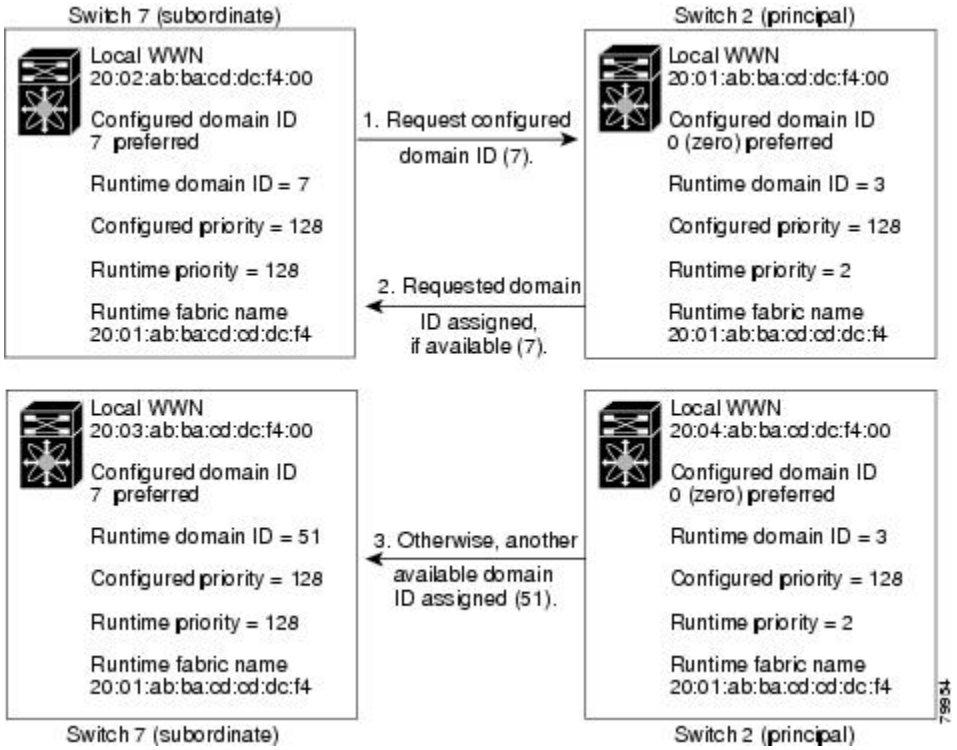
（注） 値 0（ゼロ）を設定できるのは、優先オプションを使用した場合だけです。

ドメイン ID を設定しない場合、ローカル スイッチは要求内でランダムな ID を送信します。 スタティック ドメイン ID を使用することを推奨します。

下位スイッチがドメインを要求する場合は、次のプロセスが実行されます（次の図を参照）。

- ローカル スイッチは主要スイッチに設定済みドメイン ID 要求を送信します。
- 要求されたドメイン ID が使用可能な場合、主要スイッチはこの ID を割り当てます。 使用不可能な場合は、使用可能な別のドメイン ID を割り当てます。

図 *3*： *preferred* オプションを使用した設定プロセス



下位スイッチの動作は、次の 3 つの要素により異なります。

- 許可ドメイン ID リスト。
- 設定済みドメイン ID。
- 主要スイッチが要求元スイッチに割り当てたドメイン ID。

状況に応じて、次のように変更されます。

- 受信されたドメイン ID が許可リストに含まれない場合は、要求されたドメイン ID が実行時ドメイン ID になり、該当する VSAN のすべてのインターフェイスが隔離されます。
- 割り当てられたドメイン ID と要求されたドメイン ID が同じである場合は、優先およびスタティック オプションは関係せず、割り当てられたドメイン ID が実行時ドメイン ID になります。

- 割り当てられたドメイン ID と要求されたドメイン ID が異なる場合は、次のようになります。
  - 設定タイプがスタティックの場合は、割り当てられたドメイン ID が廃棄され、すべてのローカル インターフェイスは隔離され、ローカル スイッチには設定済みのドメイン ID が自動的に割り当てられます（この ID が実行時ドメイン ID になります）。
  - 設定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。

設定済みドメイン ID を変更したときに、変更が受け入れられるのは、新しいドメイン ID が、VSAN 内に現在設定されているすべての許可ドメイン ID リストに含まれている場合だけです。または、ドメイン ID を 0 の優先に設定することもできます。

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

（注） 許可ドメイン ID リストを設定した場合、追加するドメイン ID は VSAN のその範囲内にある必要があります。

関連トピック

許可ドメイン ID リストの概要, （45 ページ）

スタティック ドメイン ID または優先ドメイン ID の指定

スタティック ドメイン ID タイプを割り当てる場合、特定のドメイン ID を要求します。 スイッチが要求したアドレスを取得しない場合、スイッチ自身をファブリックから隔離します。 優先ドメイン ID を指定した場合も特定のドメイン ID を要求しますが、要求したドメイン ID を取得できない場合スイッチは、別のドメイン ID を受け入れます。

static オプションは、中断再起動または非中断再起動後の実行時に適用できますが、preferred オプションは中断再起動後の実行時のみ適用できます。

（注） 1 つの VSAN 内のスイッチは、すべて同じドメイン ID タイプ（スタティックまたは優先）を持っている必要があります。 スイッチによって static と preferred のドメイン ID タイプが混在する設定の場合、リンクの分離が発生することがあります。

static または preferred ドメイン ID を指定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcdomain domain** *domain-id* **static vsan** *vsan-id*
3. switch(config)# **no fcdomain domain** *domain-id* **static vsan** *vsan-id*
4. switch(config)# **fcdomain domain** *domain-id* **preferred vsan** *vsan-id*
5. switch(config)# **no fcdomain domain** *domain-id* **preferred vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcdomain domain** *domain-id* **static vsan** *vsan-id*	特定の値だけを受け入れるように指定の VSAN 内のスイッチを設定し、要求されたドメイン ID が許可されない場合は、指定の VSAN 内のローカル インターフェイスを隔離ステートに移行します。
ステップ 3	switch(config)# **no fcdomain domain** *domain-id* **static vsan** *vsan-id*	設定済みドメイン ID を、指定 VSAN 内の出荷時のデフォルト設定にリセットします。 設定済みドメイン ID は 0 preferred になります。
ステップ 4	switch(config)# **fcdomain domain** *domain-id* **preferred vsan** *vsan-id*	preferred ドメイン ID 3 を要求するために指定の VSAN 内のスイッチを設定し、主要スイッチによって割り当てられた値をすべて受け入れます。 ドメインの範囲は 1 ～ 239 です。
ステップ 5	switch(config)# **no fcdomain domain** *domain-id* **preferred vsan** *vsan-id*	指定の VSAN 内の設定済みドメイン ID を 0（デフォルト）にリセットします。 設定済みドメイン ID は 0 preferred になります。

許可ドメイン ID リストの概要

デフォルトでは、割り当て済みのドメイン ID リストの有効範囲は 1 ～ 239 です。 許可ドメイン ID リストに複数の範囲を指定し、各範囲をカンマで区切れます。 主要スイッチは、ローカルに設定された許可ドメイン リストで使用可能なドメイン ID を割り当てます。

ドメイン ID が重複しないように、許可ドメイン ID リストを使用して VSAN を設計してください。 このリストは将来 NAT 機能を使用しない IVR を実装する必要がある場合に役立ちます。

ファブリック内の 1 つのスイッチに許可リストを設定する場合は、整合性を保つために、ファブリック内のその他のすべてのスイッチに同じリストを設定するか、CFS を使用して設定を配信することを推奨します。

許可ドメイン ID リストは、次の条件を満たす必要があります。

- 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 が許可リストに含まれている必要があります。
- このスイッチが下位スイッチである場合は、ローカル実行時ドメイン ID が許可リストに含まれている必要があります。
- ローカルに設定されたスイッチのドメイン ID が許可リスト内に含まれている必要があります。
- 割り当てられたドメイン ID の一部が、その他の設定済みドメイン ID のリストのいずれかに含まれている必要があります。

許可ドメイン ID リストの設定

許可ドメイン ID リストを設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcdomain allowed** *domain-id range* **vsan** *vsan-id*
3. switch(config)# **no fcdomain allowed** *domain-id range* **vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcdomain allowed** *domain-id range* **vsan** *vsan-id*	指定の VSAN でドメイン ID 範囲を持つスイッチを許可するようにリストを設定します。
ステップ 3	switch(config)# **no fcdomain allowed** *domain-id range* **vsan** *vsan-id*	指定の VSAN でドメイン ID 1 ～ 239 のスイッチを許可する出荷時のデフォルト設定に戻します。

許可ドメイン ID リストの CFS 配信の概要

Cisco Fabric Services（CFS）インフラストラクチャを使用して、ファブリック内のすべての Cisco SAN スイッチへの許可ドメイン ID リスト設定情報の配信をイネーブルにできます。 この機能を使用すると、1 つのスイッチのコンソールからファブリック全体の設定を同期化できます。 VSAN 全体に同じ設定が配信されるので、誤設定や、同じ VSAN 内の 2 つのスイッチが互換性のない許可ドメインを設定してしまう可能性を防止します。

CFS を使用して許可ドメイン ID リストを配信し、VSAN 内のすべてのスイッチで許可ドメイン ID リストの整合性をとるようにします。

（注） 許可ドメイン ID リストを設定してそれを主要スイッチにコミットするようお勧めします。

追加情報については、『*Cisco Nexus 5000 Series System Management Configuration Guide*』の「Using Cisco Fabric Services」を参照してください。

配信のイネーブル化

許可ドメイン ID リストの CFS 配信はデフォルトではディセーブルになっています。 許可ドメイン ID リストを配信するすべてのスイッチで配信をイネーブルにする必要があります。

許可ドメイン ID リスト設定の配信をイネーブル（またはディセーブル）にする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcdomain distribute**
3. switch(config)# **no fcdomain distribute**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcdomain distribute**	ドメイン設定の配信をイネーブルにします。
ステップ 3	switch(config)# **no fcdomain distribute**	ドメイン設定の配信をディセーブル（デフォルト）にします。

ファブリックのロック

既存の設定を変更するときの最初のアクションによって、保留中の設定が作成され、ファブリック内の機能がロックされます。 ファブリックがロックされると、次のような状況になります。

- 他のユーザがこの機能の設定に変更を加えることができなくなります。
- アクティブな設定をコピーすると保留中の設定が作成されます。以降の変更は保留中の設定に行われ、アクティブな設定（およびファブリック内の他のスイッチ）への変更をコミットまたは廃棄するまでそのままです。

変更のコミット

VSAN 内の他の SAN スイッチに保留中のドメイン設定の変更を適用するには、変更をコミットする必要があります。 保留中の設定変更が配信され、コミットが正常に行われると、設定の変更が VSAN 全体の SAN スイッチのアクティブな設定に適用され、ファブリック ロックが解除されます。

保留中のドメイン設定変更をコミットして、ロックを解除する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcdomain commit vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcdomain commit vsan** *vsan-id*	保留中のドメイン設定変更をコミットします。

変更の破棄

いつでもドメイン設定への保留変更を廃棄して、ファブリックのロックを解除できます。 保留中の変更を廃棄（中断）する場合、設定には影響せずに、ロックが解除されます。

保留中のドメイン設定変更を廃棄して、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。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcdomain abort vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcdomain abort vsan** *vsan-id*	保留中のドメイン設定変更を廃棄します。

ファブリックのロックのクリア

ドメイン設定作業を実行し、変更をコミットまたは廃棄してロックを解除していない場合、管理者はファブリック内の任意のスイッチからロックを解除できます。 管理者がこのタスクを実行すると、保留中の変更は廃棄され、ファブリック ロックが解除されます。

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

ファブリック ロックを解除するには、管理者の権限を持つログイン ID を使用して EXEC モードで **clear fcdomain session vsan** コマンドを入力します。

```
switch# clear fcdomain session vsan 10
```

CFS 配信ステータスの表示

許可ドメイン ID リストの CFS 配信のステータスは **show fcdomain status** コマンドを使用して表示できます。

```
switch# show fcdomain status
CFS distribution is enabled
```

保留中の変更の表示

保留中の設定変更は **show fcdomain pending** コマンドを使用して表示できます。

```
switch# show fcdomain pending vsan 10
Pending Configured Allowed Domains
---------------------------------
VSAN 10
Assigned or unallowed domain IDs: 1-9,24,100,231-239.
[User] configured allowed domain IDs: 10-230.
```

保留中の設定と現在の設定の違いは、**show fcdomain pending-diff** コマンドを使用して表示できます。

```
switch# show fcdomain pending-diff vsan 10
Current Configured Allowed Domains
---------------------------------
VSAN 10
Assigned or unallowed domain IDs: 24,100.
[User] configured allowed domain IDs: 1-239.
Pending Configured Allowed Domains
---------------------------------
VSAN 10
Assigned or unallowed domain IDs: 1-9,24,100,231-239.
[User] configured allowed domain IDs: 10-230.
```

セッション ステータスの表示

配信セッションのステータスは **show fcdomain session-status vsan** コマンドを使用して表示できます。

```
switch# show fcdomain session-status vsan 1
Last Action: Distribution Enable
Result: Success
```

連続ドメイン ID 割り当ての概要

デフォルトでは、連続ドメイン割り当てはディセーブルです。 下位スイッチが主要スイッチに複数の不連続ドメインを要求した場合は、次のようになります。

- 主要スイッチで連続ドメイン割り当てがイネーブルの場合、主要スイッチは連続ドメインを特定し、それらを下位スイッチに割り当てます。 連続ドメインが使用できない場合、スイッチ ソフトウェアはこの要求を拒否します。
- 主要スイッチで連続ドメイン割り当てがディセーブルの場合、主要スイッチは使用可能なドメインを下位スイッチに割り当てます。

連続ドメイン ID 割り当てのイネーブル化

特定のVSAN（またはVSAN範囲）で連続ドメインをイネーブルにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcdomain contiguous-allocation vsan** *vsan-id* **-** *vsan-id*
3. switch(config)# **no fcdomain contiguous-allocation vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcdomain contiguous-allocation vsan** *vsan-id* **-** *vsan-id*	指定されたVSAN範囲で連続割り当てオプションをイネーブルにします。 （注） **contiguous-allocation** オプションは実行時に即座に有効になります。 fcdomain を再起動する必要はありません。
ステップ 3	switch(config)# **no fcdomain contiguous-allocation vsan** *vsan-id*	指定された VSAN で連続割り当てオプションをディセーブルにし、出荷時の設定に戻します。

FC ID

SAN スイッチにログインした N ポートには、FC ID が割り当てられます。 デフォルトでは、固定的 FC ID 機能はイネーブルです。 この機能がディセーブルの場合は、次のようになります。

- N ポートは SAN スイッチにログインします。 要求元 N ポートの WWN および割り当てられた FC ID が維持され、揮発性キャッシュに格納されます。 この揮発性キャッシュの内容は、再起動時に保存されません。
- スイッチは、FC ID と WWN のバインディングをベストエフォート方式で保持するように設計されています。 たとえば、スイッチから 1 つの N ポートを切断したあとに、別のデバイスから FC ID が要求されると、この要求が許可されて、WWN と初期 FC ID の関連付けが解除されます。
- 揮発性キャッシュには、WWN と FC ID のバインディングのエントリを 4000 まで格納できます。 このキャッシュが満杯になると、新しい（より最近の）エントリによって、キャッシュ内の最も古いエントリが上書きされます。 この場合、最も古いエントリの対応する WWN と FC ID の関連付けが失われます。
- N ポートを取り外し、同じスイッチの任意のポートに接続すると、（このポートが同じ VSAN に属するかぎり）この N ポートには同じ FC ID が割り当てられます。

固定的 FC ID の概要

永続的 FC ID がイネーブルの場合は、次のようになります。

- fcdomain 内の現在使用中の FC ID は、再起動後も保存されます。
- fcdomain は、デバイス（ホストまたはディスク）をポートインターフェイスに接続したあとに学習されたダイナミック エントリを、自動的にデータベースに入力します。

（注） AIX または HP-UX ホストからスイッチに接続する場合は、それらのホストに接続する VSAN で固定的 FC ID 機能をイネーブルにする必要があります。

（注） 永続的 FC ID がイネーブルである場合、再起動後に FC ID を変更できません。 FC ID はデフォルトではイネーブルですが、各 VSAN に対してディセーブルにできます。

F ポートに割り当てられた固定的 FC ID は、インターフェイス間を移動させることができ、同じ固定的 FC ID をそのまま維持することができます。

固定的 FC ID 機能のイネーブル化

永続的 FC ID 機能をイネーブルにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcdomain fcid persistent vsan** *vsan-id*
3. switch(config)# **no fcdomain fcid persistent vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcdomain fcid persistent vsan** *vsan-id*	指定された VSAN の FC ID 永続性をアクティブ（デフォルト）にします。
ステップ 3	switch(config)# **no fcdomain fcid persistent vsan** *vsan-id*	指定された VSAN の FC ID 永続性機能をディセーブルにします。

永続的 FC ID 設定時の注意事項

固定的 FC ID 機能をイネーブルにすると、固定的 FC ID サブモードを開始して、FC ID データベースにスタティックまたはダイナミックエントリを追加できるようになります。デフォルトでは、追加されたすべてのエントリはスタティックです。 固定的 FC ID は VSAN 単位で設定します。

永続的 FC ID を手動で設定するための要件は、次のとおりです。

- 必要な VSAN 内で固定的 FC ID 機能がイネーブルになっていることを確認します。
- 目的の VSAN がアクティブ VSAN であることを確認します。 永続的 FC ID は、アクティブ VSAN だけで設定できます。
- FC ID のドメイン部分が必要な VSAN 内の実行時ドメイン ID と同じであることを確認します。 ソフトウェアがドメインの不一致を検出した場合、コマンドは拒否されます。
- エリアを設定するときに、FC ID のポート フィールドが 0（ゼロ）であることを確認します。

固定的 FC ID の設定

永続的 FC ID を設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcdomain fcid database**
3. switch(config-fcid-db)# **vsan** *vsan-id* **wwn 33:e8:00:05:30:00:16:df fcid** *fcid*
4. switch(config-fcid-db)# **vsan** *vsan-id* **wwn 11:22:11:22:33:44:33:44 fcid** *fcid* **dynamic**
5. switch(config-fcid-db)# **vsan** *vsan-id* **wwn 11:22:11:22:33:44:33:44 fcid** *fcid* **area**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcdomain fcid database**	FC ID データベース コンフィギュレーション サブモードを開始します。
ステップ 3	switch(config-fcid-db)# **vsan** *vsan-id* **wwn 33:e8:00:05:30:00:16:df fcid** *fcid*	指定の VSAN のデバイス WWN（33:e8:00:05:30:00:16:df）に FC ID 0x070128 を設定します。 （注） 重複 FC ID の割り当てを回避するには、**show fcdomain address-allocation vsan** コマンドを使用して、使用中の FC ID を表示します。
ステップ 4	switch(config-fcid-db)# **vsan** *vsan-id* **wwn 11:22:11:22:33:44:33:44 fcid** *fcid* **dynamic**	ダイナミック モードで、指定の VSAN のデバイス WWN（11:22:11:22:33:44:33:44）に FC ID 0x070123 を設定します。
ステップ 5	switch(config-fcid-db)# **vsan** *vsan-id* **wwn 11:22:11:22:33:44:33:44 fcid** *fcid* **area**	指定の VSAN のデバイス WWN（11:22:11:22:33:44:33:44）に FC ID 0x070100 ～ 0x701FF を設定します。 （注） この fcdomain のエリア全体を保護するには、FC ID の末尾 2 文字に 00 を割り当てます。

HBA の固有エリア FC ID について

（注） ここに記載された説明が適用されるのは、Host Bus Adapter（HBA; ホストバスアダプタ）ポートとストレージ ポートが同じスイッチに接続されている場合だけです。

HBA とストレージ ポートが同じスイッチに接続されている場合は、それぞれのポートに異なるエリア ID を設定しなければならないことがあります。 たとえば、ストレージ ポート FC ID が 0x6f7704 の場合、このポートのエリアは 77 です。 この場合、HBA ポートのエリアには 77 以外の値を設定できます。 HBA ポートの FC ID は、ストレージ ポートの FC ID と異なる値に手動で設定する必要があります。

Cisco SAN スイッチでは、FC ID の永続性機能により、この要件が満たされます。 この機能を使用すると、ストレージ ポートまたは HBA ポートに異なるエリアを持つ FC ID を事前に割り当てることができます。

HBA の固有エリア FC ID の設定

次のタスクでは、111（16 進値では 6f）のスイッチ ドメインの設定例を使用します。 サーバは FCoE を介してスイッチに接続されます。 HBA ポートはインターフェイス vfc20 に接続され、ストレージ ポートは同じスイッチのインターフェイス fc2/3 に接続されます。

HBA ポートに異なるエリア ID を設定する手順は、次のとおりです。

手順の概要

1. **show flogi database** コマンドを使用して、HBA のポート WWN（Port Name フィールド）ID を取得します。
2. SAN スイッチの HBA インターフェイスをシャットダウンします。
3. **show fcdomain vsan** コマンドを使用して、FC ID 機能がイネーブルであることを確認します。
4. SAN スイッチで永続的 FC ID 機能をイネーブルにします。
5. 異なるエリアの新しい FC ID を割り当てます。 この例では、*77* を *ee* に置き換えます。
6. SAN スイッチの HBA インターフェイスをイネーブルにします。
7. **show flogi database** コマンドを使用して、HBA の pWWN ID を確認します。

手順の詳細

ステップ 1 **show flogi database** コマンドを使用して、HBA のポート WWN（Port Name フィールド）ID を取得します。

```
switch# show flogi database

--------------------------------------------------------------------
INTERFACE VSAN  FCID           PORT NAME                NODE NAME
--------------------------------------------------------------------
 vfc20     3   0x6f7703  50:05:08:b2:00:71:c8:c2   50:05:08:b2:00:71:c8:c0
 fc2/3     3   0x6f7704  50:06:0e:80:03:29:61:0f   50:06:0e:80:03:29:61:0f
```

（注） この設定では、両方の FC ID に同じエリア 77 が割り当てられています。

ステップ 2 SAN スイッチの HBA インターフェイスをシャットダウンします。

```
switch# configuration terminal
switch(config)# interface vfc 20

switch(config-if)# shutdown

switch(config-if)# end
```

ステップ 3 **show fcdomain vsan** コマンドを使用して、FC ID 機能がイネーブルであることを確認します。

```
switch# show fcdomain vsan 1
...
Local switch configuration information:
        State: Enabled
        FCID persistence: Disabled
```

この機能がディセーブルの場合は、次の手順に進み、永続的 FC ID をイネーブルにします。

この機能がすでにイネーブルの場合は、その後の手順にスキップします。

ステップ 4 SAN スイッチで永続的 FC ID 機能をイネーブルにします。

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

ステップ 5 異なるエリアの新しい FC ID を割り当てます。 この例では、*77* を *ee* に置き換えます。

```
switch# configuration terminal
switch(config)# fcdomain fcid database
switch(config-fcid-db)# vsan 3 wwn 50:05:08:b2:00:71:c8:c2
fcid 0x6fee00 area
```

ステップ 6 SAN スイッチの HBA インターフェイスをイネーブルにします。

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

switch(config-if)# end
```

ステップ 7 **show flogi database** コマンドを使用して、HBA の pWWN ID を確認します。

```
switch# show flogi database

--------------------------------------------------------------------
INTERFACE VSAN  FCID      PORT NAME                NODE NAME
--------------------------------------------------------------------
 vfc20    3   0x6fee00    50:05:08:b2:00:71:c8:c2   50:05:08:b2:00:71:c8:c0
 fc2/3    3   0x6f7704    50:06:0e:80:03:29:61:0f   50:06:0e:80:03:29:61:0f
```

（注） これで、両方の FC ID にそれぞれ異なるエリアが割り当てられました。

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 エントリおよび FC ID は、削除できません。 次の表に、永続的 FC ID が消去されると削除または保持される FC ID エントリを示します。

表 *7*：消去される *FC ID*

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

固定的 FC ID の消去

永続的 FC ID を消去する手順は、次のとおりです。

手順の概要

1. switch# **purge fcdomain fcid vsan** *vsan-id*
2. switch# **purge fcdomain fcid vsan** *vsan-id* **-** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **purge fcdomain fcid vsan** *vsan-id*	指定の VSAN の未使用のダイナミック FC ID をすべて消去します。
ステップ 2	switch# **purge fcdomain fcid vsan** *vsan-id* **-** *vsan-id*	指定の VSAN 範囲の未使用のダイナミック FC ID をすべて消去します。

fcdomain 情報の確認

（注） fcdomain機能がディセーブルである場合、表示された実行時ファブリック名は設定済みファブリック名と同じです。

次に、fcdomain 設定に関する情報を表示する例を示します。

```
switch# show fcdomain vsan 2
```

指定されたVSANに属するすべてのスイッチのドメインIDリストを表示するには、**show fcdomain domain-list** コマンドを使用します。 このリストには、各ドメインIDを所有するスイッチのWWNが記載されています。 この例では次の値が使用されています。

- 20:01:00:05:30:00:47:df の WWN を持つスイッチが主要スイッチで、ドメインは 200 です。
- 20:01:00:0d:ec:08:60:c1 の WWN を持つスイッチはローカル スイッチ（CLI コマンドを入力してドメイン リストを表示したスイッチ）で、ドメインは 99 です。
- IVR マネージャは 20:01:00:05:30:00:47:df を仮想スイッチの WWN として使用して仮想ドメイン 97 を取得しました。

```
switch# show fcdomain domain-list vsan 76
Number of domains: 3
Domain ID              WWN
---------    -----------------------
0xc8(200)    20:01:00:05:30:00:47:df [Principal]
 0x63(99)    20:01:00:0d:ec:08:60:c1 [Local]
 0x61(97)    50:00:53:0f:ff:f0:10:06 [Virtual (IVR)]
```

このスイッチに設定された許可ドメイン ID のリストを表示するには、**show fcdomain allowed vsan** コマンドを使用します。

```
switch# show fcdomain allowed vsan 1
Assigned or unallowed domain IDs: 1-96,100,111-239.
[Interoperability Mode 1] allowed domain IDs: 97-127.
[User] configured allowed domain IDs: 50-110.
```

このスイッチに interop 1 モードが必要な場合は、要求されたドメイン ID がスイッチ ソフトウェア チェックに合格することを確認してください。

次に、指定の VSAN の既存の永続的 FC ID をすべて表示する例を示します。 unused オプションを指定すると、未使用の永続的 FC ID だけを表示できます。

```
switch# show fcdomain fcid persistent vsan 1000
```

次に、指定の VSAN または SAN ポート チャネルのフレームおよびその他の fcdomain 統計情報を表示する例を示します。

```
switch# show fcdomain statistics vsan 1
VSAN Statistics
        Number of Principal Switch Selections: 5
        Number of times Local Switch was Principal: 0
        Number of 'Build Fabric's: 3
        Number of 'Fabric Reconfigurations': 0
```

次に、割り当てられた FC ID および空いている FC ID のリストを含めて、FC ID 割り当てに関する統計情報を表示する例を示します。

```
switch# show fcdomain address-allocation vsan 1
```

次に、有効なアドレス割り当てキャッシュを表示する例を示します。 ファブリックから取り除かれたデバイス（ディスクやホスト）を元のファブリックに戻す場合、主要スイッチはキャッシュを使用して FC ID を再度割り当てます。 キャッシュ内では、VSAN はこのデバイスを含む VSAN を、WWN は FC ID を所有していたデバイスを、マスクは FC ID に対応する 1 つのエリアまたはエリア全体を表します。

```
switch# show fcdomain address-allocation cache
```

ファイバ チャネル ドメインのデフォルト設定

次の表は、すべての fcdomain パラメータのデフォルト設定を示します。

表 *8*：デフォルト *fcdomain* パラメータ

パラメータ	デフォルト
fcdomain 機能	イネーブル
設定済みドメイン ID	0（ゼロ）
設定済みドメイン	Preferred
auto-reconfigure オプション	ディセーブル
連続割り当てオプション	ディセーブル
プライオリティ	128

パラメータ	デフォルト
許可リスト	1 ～ 239
ファブリック名	20:01:00:05:30:00:28:df
rcf-reject	ディセーブル
固定的 FC ID	イネーブル
許可ドメイン ID リスト設定の配信	ディセーブル

第 5 章

NPV の設定

この章の内容は、次のとおりです。

- NPV の設定，59 ページ

NPV の設定

NPV の概要

NPV の概要

デフォルトでは、Cisco Nexus 5000 シリーズ スイッチは、ファブリック モードで動作します。 このモードでは、スイッチは標準のファイバ チャネル スイッチング機能を提供します。

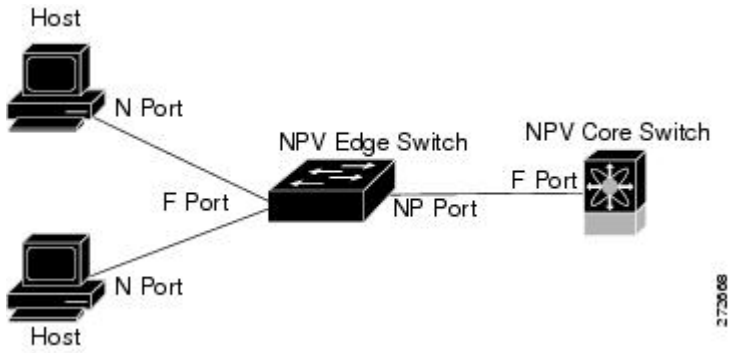
ファブリック モードでは、SAN に参加する各スイッチにドメイン ID が割り当てられます。 各 SAN（または VSAN）は、最大 239 個のドメイン ID 数をサポートするため、SAN におけるスイッチ数は 239 台に制限されます。 多数のエッジ スイッチが配置されている SAN トポロジでは、SAN はこの制限を超えて拡張する必要がある場合があります。 NPV は、コア スイッチのドメイン ID を複数のエッジ スイッチ間で共有することによって、このドメイン ID の制限を解消します。

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

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

次の図に、インターフェイスレベルでの NPV 構成を示します。

図 *4*： *NPV* のインターフェイスでの設定



NPV モード

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

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

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

サーバ インターフェイス

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

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

サーバ インターフェイスが、コアスイッチまでの NP アップリンク間で自動的に配布されます。サーバ インターフェイスに接続されたすべてのエンド デバイスは、同じ NP アップリンクにマッピングされます。

Cisco Nexus 5000 シリーズ スイッチでは、サーバ インターフェイスは物理インターフェイスでも仮想ファイバ チャネル インターフェイスでも構いません。

関連トピック

NPV の設定, （59 ページ）

NP アップリンク

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

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

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

Cisco Nexus 5000 シリーズ スイッチでは、NP アップリンク インターフェイスはネイティブ ファイバ チャネル インターフェイスである必要があります。

関連トピック

ファブリック ログインに関する情報, （209 ページ）

FLOGI 動作

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

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

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

表 *9*： エッジ スイッチ *FLOGI* パラメータ

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

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

（注） NP ポートの内部 FLOGI の Buffer-to-Buffer State Change Number（BB_SCN）は、常にゼロに設定されます。 BB_SCN はエッジ スイッチの F ポートでサポートされます。

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

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

関連トピック

ゾーンの設定と管理, （141 ページ）

NPV トラフィック管理

自動アップリンク選択

NPV は、NP アップリンクの自動選択をサポートしています。 サーバ インターフェイスがアップになると、サーバ インターフェイスと同じ VSAN 内で利用可能な NP アップリンクから負荷が最も少ない NP アップリンク インターフェイスが選択されます。

新しい NP アップリンク インターフェイスが動作可能になっても、新たに利用可能になったアップリンクを含めるために既存の負荷は自動的に再分散されません。 NP アップリンクが新しい NP アップリンクを選択できるようになってから、サーバ インターフェイスが作動します。

トラフィック マップ

Release 4.0(1a)N2(1) 以降のソフトウェア リリースでは、NPV はトラフィック マップをサポートします。 トラフィック マップにより、サーバ インターフェイスがコア スイッチに接続するために使用可能な NP アップリンクを指定できます。

（注） NPV トラフィック マップがサーバ インターフェイスに設定されると、サーバ インターフェイスはそのトラフィック マップ内の NP アップリンクからだけ選択する必要があります。 指定された NP アップリンクがいずれも動作していない場合、サーバは非動作状態のままになります。

NPV トラフィック マップ機能を使用すると、次のようなメリットが得られます。

- 特定のサーバ インターフェイス（またはサーバ インターフェイスの範囲）に NP アップリンクの事前設定された設定を割り当てることによって、トラフィック エンジニアリングが容易になります。
- インターフェイスの再初期化またはスイッチの再起動後に、サーバ インターフェイスは常に同じ NP アップリンク（または指定された NP アップリンクのセットのいずれか）に接続するので、永続的な FC ID 機能の適切な動作が確保されます。

ディスラプティブ ロード バランシング

Release 4.0(0)N1(2a) 以降のソフトウェア リリースでは、NPV はディスラプティブ ロード バランシングをサポートします。 ディスラプティブ ロード バランシングがイネーブルの場合、新しい NP アップリンクが動作すると、NPV はすべての利用可能な NP アップリンク全体にサーバ インターフェイスを再配布します。 サーバ インターフェイスを 1 つの NP アップリンクからの別の NP アップリンクに移動するために、NPV はサーバ インターフェイスを強制的に再初期化して、サーバがコア スイッチへのログインを新たに実行するようにします。

別のアップリンクに移されたサーバ インターフェイスだけが再初期化されます。 移されたサーバ インターフェイスごとにシステム メッセージが生成されます。

（注） サーバ インターフェイスを再配布すると、接続されたエンド デバイスへのトラフィックが中断されます。

サーバ トラフィックの中断を避けるために、新しい NP アップリンクを追加してから、この機能をイネーブルし、サーバ インターフェイスが再配布されてからこの機能を再度ディセーブルにしてください。

ディスラプティブ ロード バランシングがイネーブルでない場合、サーバ インターフェイスの一部またはすべてを手動で再初期化して、新しい NP アップリンク インターフェイスにサーバ トラフィックを分散することができます。

NPV トラフィック管理の注意事項

NPV トラフィック管理を導入する際には、次の注意事項に従ってください。

- NPV トラフィック管理は、自動トラフィック エンジニアリングがネットワーク要件を満たさない場合にだけ使用してください。
- すべてのサーバインターフェイスにトラフィック マップを設定する必要はありません。 NPV はデフォルトで自動トラフィック管理を使用します。
- NP アップリンク インターフェイスのセットを使用するように設定されたサーバ インターフェイスは、利用可能な NP アップリンク インターフェイスがなくても、他の利用可能な NP アップリンク インターフェイスを使用できません。
- ディスラプティブ ロード バランシングがイネーブルになると、サーバ インターフェイスは 1 つの NP アップリンクから別の NP アップリンクに移動される場合があります。 NP アップリンク インターフェイスの間を移動すると、NPV では、トラフィックを中断して、コア スイッチに再度ログインする必要があります。
- サーバのセットを特定のコア スイッチにリンクするには、サーバ インターフェイスを NP アップリンク インターフェイスのセット（すべてこのコア スイッチに接続されている）に関連付けてください。
- コア スイッチに永続的な FC ID を設定し、トラフィック マップ機能を使用してサーバ インターフェイスのトラフィックを NP アップリンク（すべて関連付けられたコア スイッチに接続している）上に誘導します。

NPV の注意事項および制限事項

NPV を設定する場合、次の注意事項および制限事項に注意してください。

- NPV モードでは、2 つのエンド デバイス間のやり取りに、エッジ スイッチからコアへの同じアップリンクが使用されるため、順序どおりのデータ配信を行う必要はありません。 エッジ スイッチのアップストリームのコア スイッチが設定されている場合は、順序どおりの配信を実行します。
- コア スイッチ上で使用できるすべてのメンバ タイプを使用して、エッジ スイッチに接続されているエンドデバイスのゾーン分割を設定できます。 fWWN、sWWN、ドメイン、またはポートベースのゾーン分割では、コンフィギュレーション コマンドでコア スイッチの fWWN、sWWN、ドメイン、またはポートを使用してください。
- NPV モードでは、ポート トラッキングはサポートされません。
- NPV スイッチを介してログインするデバイスには、コア スイッチでポート セキュリティがサポートされます。 ポート セキュリティは、コア スイッチでインターフェイスごとにイネーブルにされます。 NPV スイッチを介してログインするデバイスのコア スイッチでセキュリティ ポートをイネーブルにするには、次の要件に従う必要があります。

- 内部 FLOGI がポート セキュリティ データベースに存在している必要があります。これによりコア スイッチのポートで通信やリンクが許可されます。
- すべてのエンド デバイスの pWWN もポート セキュリティ データベースに存在する必要があります。

- エッジ スイッチは複数のコア スイッチに接続できます。 つまり、異なる NP ポートを異なるコア スイッチに接続できます。
- NPV は初回ログイン時にロード バランシング アルゴリズムを使用して、自動的に VSAN 内のエンド デバイスを NP アップリンクの 1 つ（同じ VSAN 内）に割り当てます。 同じ VSAN に複数の NP アップリンクがある場合は、エンド デバイスを特定の NP アップリンクに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使用可能状態に戻った場合、インターフェイスは同じ NP アップリンクに割り当てられるとはかぎりません。
- 割り当てられた NP アップリンクが動作可能になると、サーバ インターフェイスだけが使用できます。
- NPV モードでは、サーバをスイッチに接続できます。
- NPV モードでは、ターゲットをスイッチに接続できません。
- ファイバ チャネル スイッチングは、エッジ スイッチで実行されません。すべてのトラフィックはコア スイッチでスイッチングされます。
- NPV は NPIV 対応のモジュール サーバをサポートします。 この機能は階層型 NPIV と呼ばれます。
- NPV モードでは F、NP、および SD ポートだけがサポートされます。

NPV の設定

NPV のイネーブル化

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

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

NPV をイネーブルにする手順は、次のとおりです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **npv enable**
3. switch(config-npv)# **no npv enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **npv enable**	NPV モードをイネーブルにします。 スイッチが再起動し、NPV モードで起動します。 （注） 再起動時に write-erase 操作が実行されます。
ステップ 3	switch(config-npv)# **no npv enable**	NPV モードをディセーブルにします。これによりスイッチがリロードされます。

NPV インターフェイスの設定

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

NP インターフェイスの設定

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

サーバ インターフェイスを設定する手順は、次のとおりです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface fc** *slot*/*port*
3. switch(config-if)# **switchport mode NP**
4. switch(config-if)# **no shutdown**

手順の詳細

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

サーバ インターフェイスの設定

サーバ インターフェイスを設定する手順は、次のとおりです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** {**fc** *slot*/*port* | **vfc** *vfc-id*}
3. switch(config-if)# **switchport mode F**
4. switch(config-if)# **no shutdown**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {**fc** *slot*/*port* | **vfc** *vfc-id*}	サーバ インターフェイスを選択します。
ステップ 3	switch(config-if)# **switchport mode F**	このインターフェイスを F ポートとして設定します。
ステップ 4	switch(config-if)# **no shutdown**	インターフェイスをアップにします。

NPV トラフィック管理の設定

NPV トラフィック マップの設定

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

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

トラフィック マップを設定する手順は、次のとおりです。

手順の概要

1. switch# **config t**
2. switch(config)# **npv traffic-map server-interface** {**fc** *slot/port* | **vfc** *vfc-id*} **external-interface fc** *slot/port*
3. switch(config)# **no npv traffic-map server-interface** {**fc** *slot/port* | **vfc** *vfc-id*} **external-interface fc** *slot/port*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **config t**	NPV のコンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **npv traffic-map server-interface** {**fc** *slot/port* | **vfc** *vfc-id*} **external-interface fc** *slot/port*	サーバ インターフェイス（またはサーバ インターフェイスの範囲）とNPアップリンク インターフェイス（またはNP アップリンクインターフェイスの範囲）の間にマッピングを設定します。
ステップ 3	switch(config)# **no npv traffic-map server-interface** {**fc** *slot/port* | **vfc** *vfc-id*} **external-interface fc** *slot/port*	指定されたサーバインターフェイスとNPアップリンク インターフェイスの間のマッピングを削除します。

ディスラプティブ ロード バランシングのイネーブル化

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

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **npv auto-load-balance disruptive**
3. switch (config)# **no npv auto-load-balance disruptive**

手順の詳細

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

NPV の確認

NPV に関する情報を表示する手順は、次のとおりです。

手順の概要

1. switch# **show npv flogi-table** [**all**]

手順の詳細

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

NPV の確認例

サーバ インターフェイスのデバイスおよび割り当てられた NP アップリンクのリストを表示するには、Cisco Nexus 5000 シリーズ スイッチで **show npv flogi-table** コマンドを次のように入力します。

```
switch# show npv flogi-table
--------------------------------------------------------------------------------
SERVER                                                                          EXTERNAL
INTERFACE VSAN FCID            PORT NAME               NODE NAME               INTERFACE
--------------------------------------------------------------------------------
vfc3/1    1    0xee0008 10:00:00:00:c9:60:e4:9a 20:00:00:00:c9:60:e4:9a fc2/1

vfc3/1    1    0xee0009 20:00:00:00:0a:00:00:01 20:00:00:00:c9:60:e4:9a fc2/2
vfc3/1    1    0xee000a 20:00:00:00:0a:00:00:02 20:00:00:00:c9:60:e4:9a fc2/3

vfc3/1    1    0xee000b 33:33:33:33:33:33:33:33 20:00:00:00:c9:60:e4:9a fc2/4
Total number of flogi = 4
```

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

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

```
switch# show npv status
npiv is enabled

External Interfaces:
====================
  Interface: fc2/1, VSAN: 1, FCID: 0x1c0000, State: Up
  Interface: fc2/2, VSAN: 1, FCID: 0x040000, State: Up
  Interface: fc2/3, VSAN: 1, FCID: 0x260000, State: Up
  Interface: fc2/4, VSAN: 1, FCID: 0x1a0000, State: Up
  Number of External Interfaces: 4

Server Interfaces:
==================
  Interface: vfc3/1, VSAN: 1, NPIV: No, State: Up
  Number of Server Interfaces: 1
```

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

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

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

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

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

NPV トラフィック管理の確認

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

```
switch# show npv traffic-map
NPV Traffic Map Information:
----------------------------------------
Server-If       External-If(s)
----------------------------------------
fc1/3           fc1/10,fc1/11
fc1/5           fc1/1,fc1/2
----------------------------------------
```

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

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

```
switch# show npv status
npiv is enabled
disruptive load balancing is enabled
External Interfaces:
====================
  Interface: fc2/1, VSAN: 2, FCID: 0x1c0000, State: Up
...
```

第 6 章

FCoE NPV の設定

この章の内容は、次のとおりです。

- FCoE NPV について，73 ページ
- FCoE NPV モデル，75 ページ
- マッピングの要件，76 ページ
- ポート要件，77 ページ
- NPV 機能，77 ページ
- vPC トポロジ，78 ページ
- サポートされるトポロジおよびサポートされないトポロジ，79 ページ
- 注意事項および制約事項，82 ページ
- デフォルト設定，84 ページ
- FCoE のイネーブル化および NPV のイネーブル化，84 ページ
- FCoE NPV のイネーブル化，85 ページ
- FCoE NPV の NPV ポートの設定，86 ページ
- FCoE NPV の設定の確認，86 ページ
- FCoE NPV の設定例，88 ページ

FCoE NPV について

Cisco NX-OS Release 5.0(3)N2(1) 以降、Cisco Nexus 5000 シリーズ スイッチでは FCoE NPV がサポートされます。 FCoE NPV 機能は、FIP スヌーピングの拡張版であり、FCoE 対応ホストから FCoE 対応 FCoE フォワーダ（FCF）スイッチに安全に接続する方法を提供します。 FCoE NPV 機能には次の利点があります。

- FCoE NPV には、FCF でのホストのリモート管理に付随する管理上およびトラブルシューティング上の問題がありません。
- FCoE NPV は、トラフィックエンジニアリング、VSAN 管理、およびトラブルシューティングといった NPV の機能を維持しながら、NVP 機能の拡張として FIP スヌーピングを実装します。
- FCoE NPV および NPV の併用により、FC ポートと FCoE ポートを同時に使用した通信が可能になります。 これにより、FC から FCoE トポロジへの移行がスムースになります。

FCoE NPV をイネーブルにするには、次のいずれかの方法を選択します。

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

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

FCoE 対応スイッチとの相互運用性

Cisco NX-OS Release 5.0(3)N2(1) 以降、Cisco Nexus 5000 シリーズ スイッチは次の FCoE 対応スイッチと相互運用します。

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

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

ライセンシング

次の表に、FCoE NPV のライセンス要件を示します。

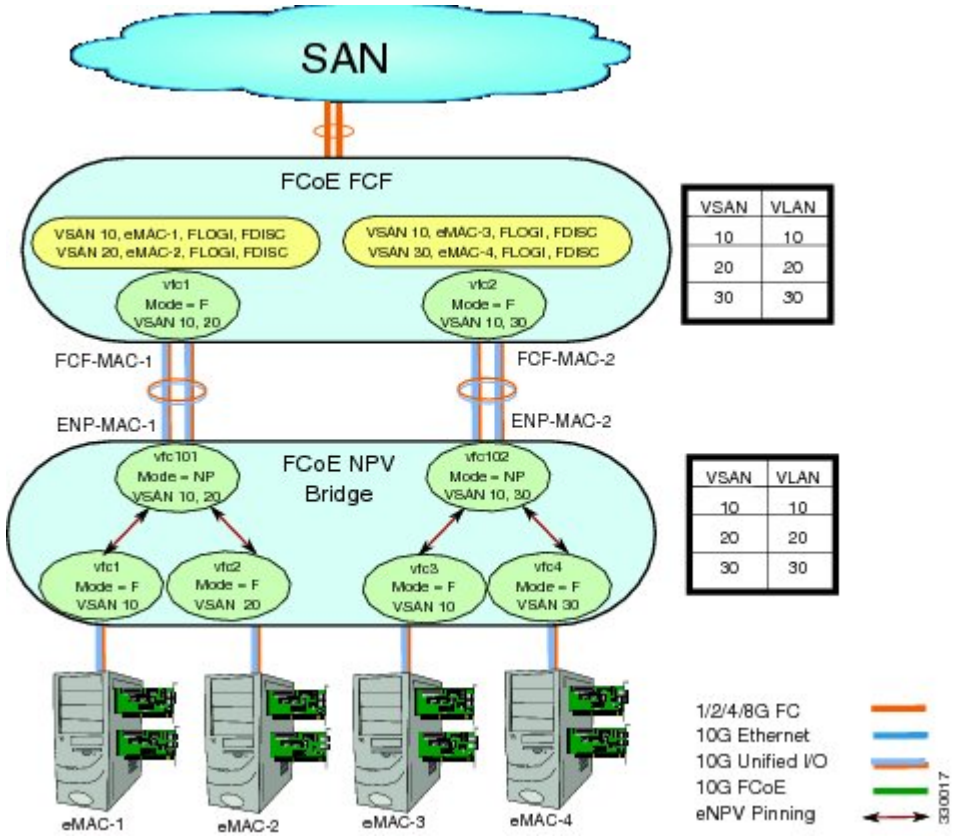
製品	ライセンス要件
NX-OS	FCoE NPV には、ライセンス（FCOE_NPV_PKG）が別途必要です。ストレージ プロトコル サービス ライセンスには FCoE NPV のライセンスも含まれています。 FCoE および NPV にはストレージ プロトコル サービス パッケージ（FC_FEATURES_PKG）が必要です。 ライセンシングおよび Cisco NX-OS ライセンスのインストールが必要な機能の詳細については『Cisco NX-OS Licensing Guide』を参照してください。 ライセンシングに関する問題のトラブルシューティングの詳細については『Cisco Nexus 5000 Series NX-OS Troubleshooting Guide』を参照してください。

FCoE NPV モデル

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

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

図 *5*：*FCoE NPV* モデル



マッピングの要件

VSAN および VLAN-VSAN マッピング

ホストから接続する VSAN を作成し、さらにそれらの VSAN それぞれに専用の VLAN を作成して、マッピングする必要があります。 マッピングした VLAN を使用して、対応する VSAN の FIP および FCoE のトラフィックを伝送します。 VLAN-VSAN マッピングは、ファブリック全体で一貫した設定とする必要があります。 Cisco Nexus 5000 シリーズ スイッチは 32 個の VSAN をサポートします。

FC マッピング

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

ポート要件

VF ポート

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

この VF ポートは、次のパラメータで設定する必要があります。

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

VNP ポート

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

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

NPV 機能

次の NPV 機能は FCoE NPV 機能に適用されます。

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

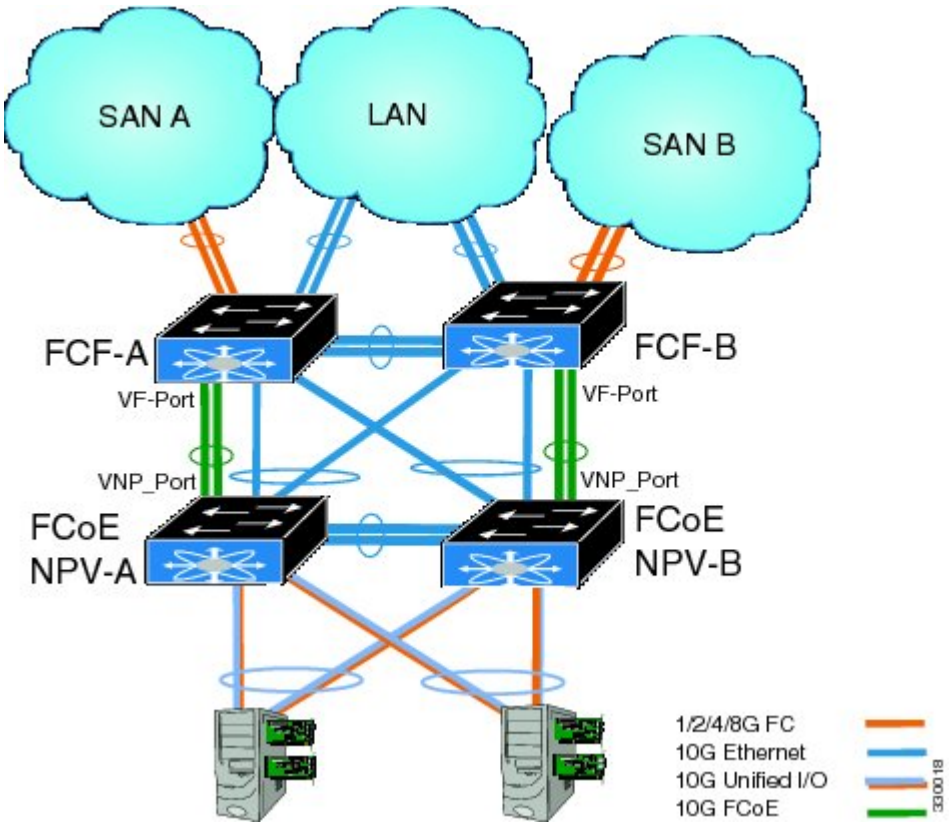
- FCoE NPV ブリッジでの FCoE フォワーディング
- VNP ポートを介して受信された FCoE フレームは、L2_DA が、VF ポートでホストに割り当てられている FCoE MAC アドレスのいずれかに一致する場合にのみ転送されます。それ以外の場合、FCoE フレームは破棄されます。

vPC トポロジ

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

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

図 *6*：スイッチ間 *vPC* トポロジでの *VNP* ポート



サポートされるトポロジおよびサポートされないトポロジ

FCoE NPV は次のトポロジをサポートしています。

図 *7*：非 ***vPC*** ポート チャネル上で ***Cisco Nexus 5000*** シリーズ スイッチに接続した ***FCoE NPV*** デバイスとして機能する ***Cisco Nexus 5000*** シリーズ スイッチ

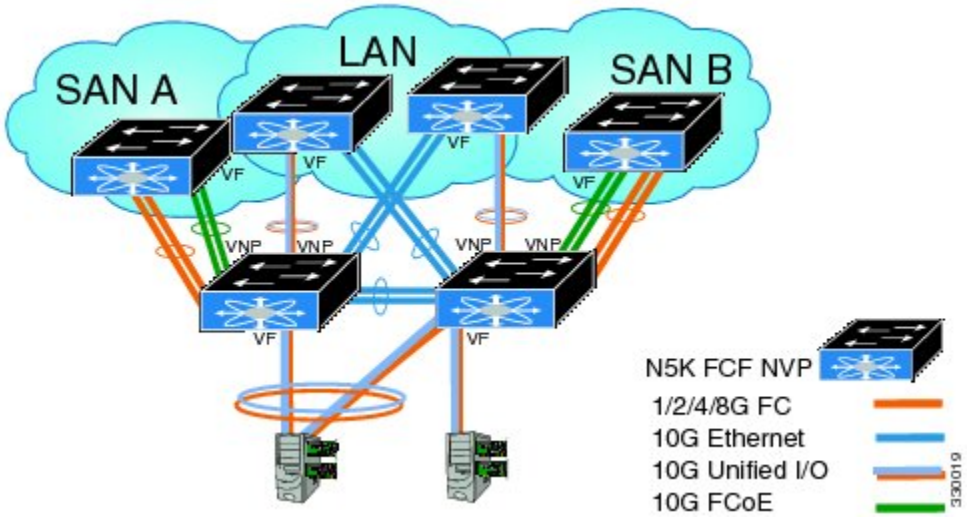


図 *8*：***vPC*** 上で別の ***Cisco Nexus 5000*** シリーズ スイッチに接続した ***FCoE NPV*** デバイスとして機能する ***Cisco Nexus 5000*** シリーズ スイッチ

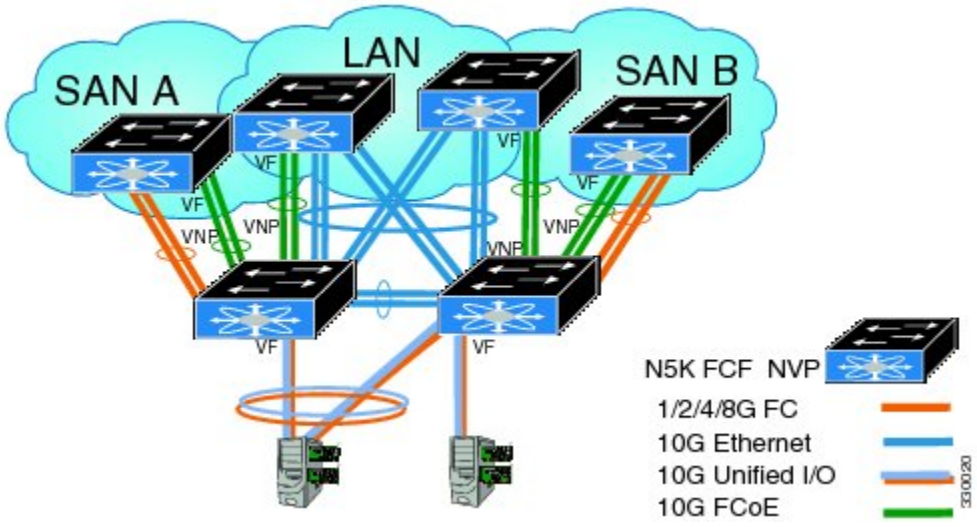


図 *9*：非 ***vPC*** ポート チャネル上で ***Cisco Nexus 5000*** シリーズ スイッチに接続した ***FCoE NPV*** デバイスとして機

能する ***Cisco Nexus 5000*** シリーズ スイッチ（***10GB*** ファブリック エクステンダ装備）

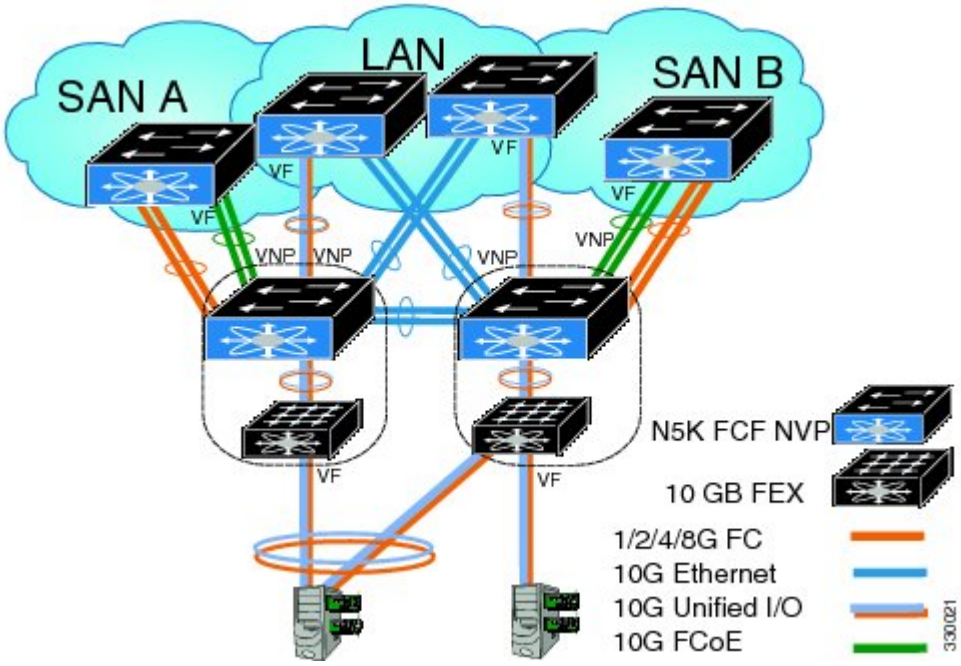
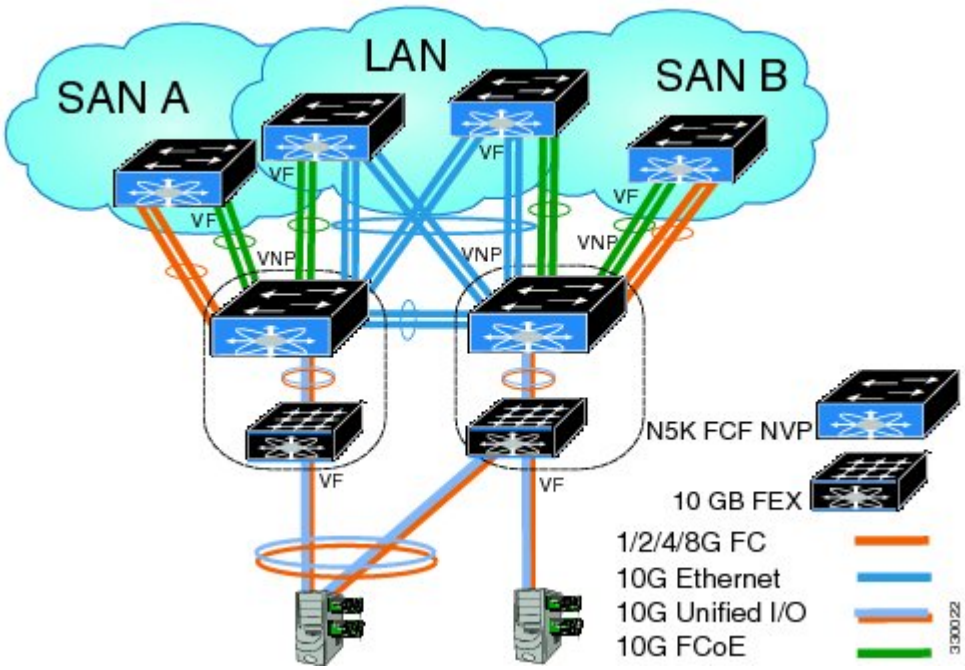


図 ***10*** : ***vPC*** 上で別の ***Cisco Nexus 5000*** シリーズ スイッチに接続した ***FCoE NPV*** デバイスとして機能する ***Cisco Nexus 5000*** シリーズ スイッチ（***10GB*** ファブリック エクステンダ装備）



サポートされていないトポロジ

FCoE NPV は次のトポロジをサポートしていません。

図 *11*：複数の *VF* ポート上で同一の *FCoE NPV* ブリッジに接続する *FCF* として機能する *Cisco Nexus 5010* スイッチまたは *Nexus 5020* スイッチ

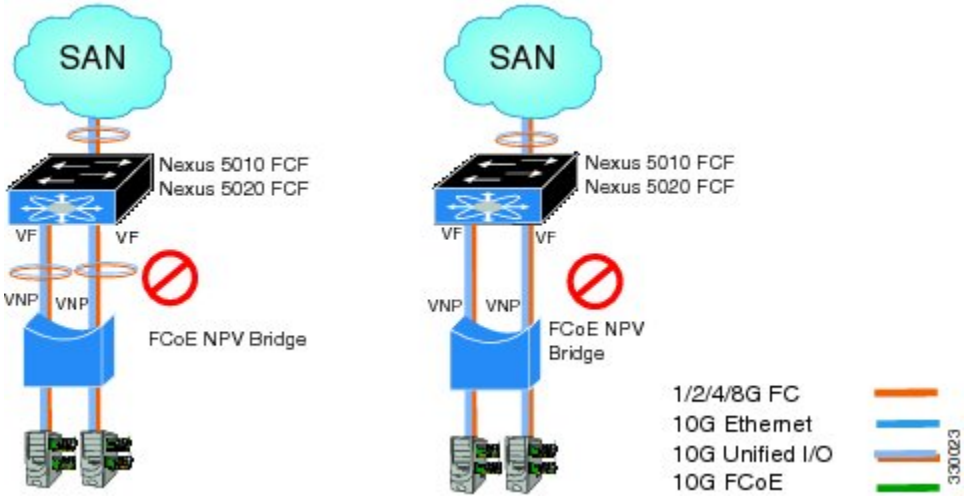


図 *12*：複数の *VF* ポート上で同一の *FCoE NPV* ブリッジに接続する *10GB* ファブリック エクステンダ

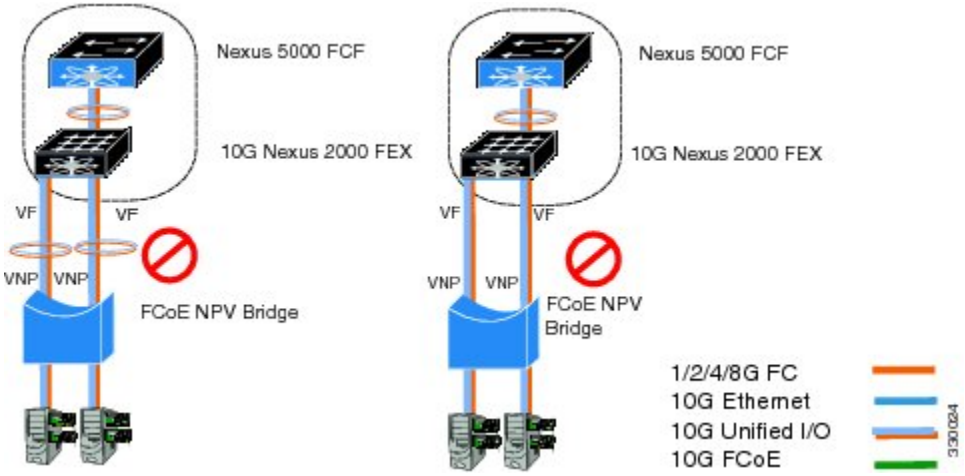


図 *13*：*FIP* スヌーピング ブリッジまたは別の *FCoE NPV* スイッチに接続する *FCoE NPV* ブリッジとして機能する *Cisco Nexus 5000* シリーズ スイッチ

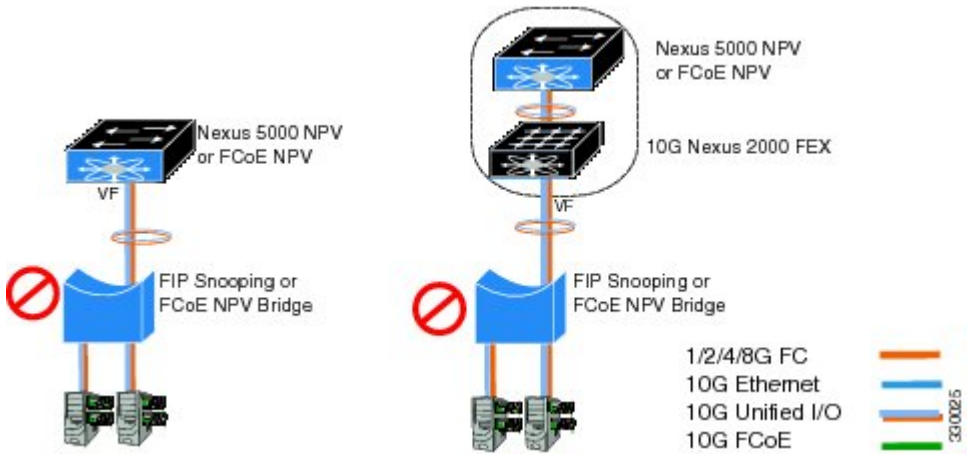
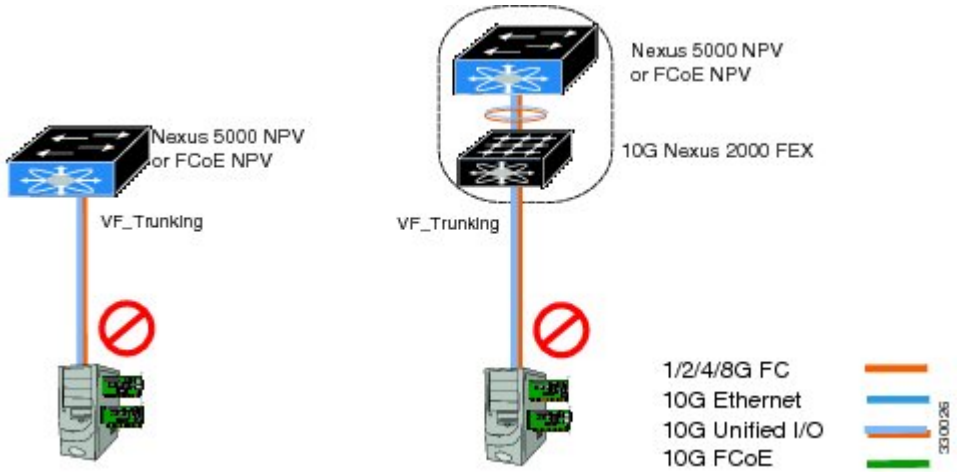


図 *14* : ***FCoE NPV*** モードでホストに接続する ***VF*** ポート トランク



注意事項および制約事項

FCoE NPV 機能の設定時の注意事項および制約事項は、次のとおりです。

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

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

- FCoE NPV をイネーブルにして、VNP ポートを設定すると、Cisco NX-OS Release 5.0(3) N 1(1) またはそれ以前のリリースへのインサービス ソフトウェア ダウングレード（ISSD）はできません。

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

FCoE NPV 設定の制限

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

表 *10*：*VNP* ポート設定の制限

インターフェイスタイプ	Cisco Nexus 5000 シリーズ	Cisco Nexus 5500 プラットフォーム	Cisco Nexus 2000 シリーズ（10G インターフェイス）
イーサネットインターフェイスにバインドした VNP ポート	4 個の VNP ポート	16 個の VNP ポート	未サポート
イーサネット ポートチャネルインターフェイスにバインドした VNP ポート	2 個の VNP ポート	16 個の VNP ポート	未サポート
仮想イーサネット（vEth）インターフェイスにバインドした VNP ポート	未サポート	未サポート	未サポート

設定に対する制限のガイドラインは次のとおりです。

- 特定の FCF と FCoE NPV ブリッジの間でサポートできる VF ポート インターフェイスと VN ポート インターフェイスの数は、FCF から MAC に対する FCF のアドバタイジング能力によっても左右されます。
  - FCF がそのすべてのインターフェイス上で同じ FCF-MAC のアドレスをアドバタイズできる場合、FCoE NPV ブリッジは、1 つの VNP ポート上でその FCF に接続できます。このシナリオでは、1 つのポートチャネルインターフェイスを使用して冗長性を実現することを推奨します。
  - FCF が複数の FCF-MAC アドレスをアドバタイズする場合は、表 1-2 の制限が適用されます。 追加情報については、FCF スイッチのベスト プラクティスの推奨事項を参照してください。

- サポートされる VSAN の総数は 31 です（EVFP VSAN を除く）。
- サポートされる FCID の総数は 2048 です。

デフォルト設定

次の表に、各 FCoE NPV パラメータのデフォルト設定を示します。

表 *11*：デフォルトの *FCoE NPV* パラメータ

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

FCoE のイネーブル化および NPV のイネーブル化

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

1. FCoE をイネーブルにします。

```
switch# config t
switch(config)# feature fcoe
FC license checked out successfully
fc_plugin extracted successfully
FC plugin loaded successfully
FCoE manager enabled successfully
FC enabled on all modules successfully
Warning: Ensure class-fcoe is included in qos policy-maps of all types
```

2. NPV をイネーブルにします。

```
switch# config t
switch(config)# feature npv
```

FCoE NPV のイネーブル化

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

はじめる前に

FCoE NPV には次の前提条件があります。

- 正しいライセンスがインストールされていることを確認します。
- Cisco Nexus 5500 プラットフォーム スイッチでは、1 つの物理 VF ポート上で FCF が複数の FC ポートおよび複数ログイン（FLOGI）をサポートしていることを確認します。
- VNP ポートを設定します。

手順の概要

1. **config t**
2. **feature fcoe-npv**
3. **exit**
4. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**feature fcoe-npv** 例： switch(config)# feature fcoe-npv	FCoE NPV をイネーブルにします。
ステップ 3	**exit** 例： switch(config)# exit	設定モードを終了します。

	コマンドまたはアクション	目的
ステップ 4	**copy running-config startup-config** 例： switch# copy running-config startup-config	実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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

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

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

```
switch# config t
switch(config)# feature fcoe
switch(config)# feature npv
```

FCoE NPV の NPV ポートの設定

FCoE NPV の NPV ポートを設定できます。

1. vFC ポートを作成します。

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

2. その vFC をイーサネット ポートにバインドします。

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

3. ポート モードを NP に設定します。

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

4. ポートをアップ状態にします。

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

FCoE NPV の設定の確認

FCoE NPV の設定情報を表示するには、次のいずれかの作業を実行します。

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

これらのコマンドの出力にある各フィールドの詳細については、『Cisco Nexus 5000 Series Command Reference』を参照してください。

FCoE NPV の設定例

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

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

switch(config)# feature lacp

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

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

This example shows a summary of the interface configuration information for trunked NP
ports:
switch# show interface brief | grep TNP
fc2/5      400    NP     on      trunking         swl    TNP     2    --
fc2/6      400    NP     on      trunking         swl    TNP     2    --
vfc130     1      NP     on      trunking         --     TNP     auto --
switch#
```

次に、FCoE に関する実行コンフィギュレーション情報の例を示します。

```
switch# show running-config fcoe_mgr

!Command: show running-config fcoe_mgr
!Time: Wed Jun  1 21:59:39 2011

version 5.0(3)N2(1)

interface vfc1
  bind interface Ethernet1/19

interface vfc2
  bind interface Ethernet1/2

interface vfc90
  bind interface Ethernet1/9

interface vfc100
  bind interface Ethernet1/10

interface vfc110
  bind interface port-channel110

interface vfc111
  bind interface Ethernet1/11

interface vfc120
  bind interface port-channel120

interface vfc130
```

```
  bind interface port-channel130

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

次に、FCoE VLAN から VSAN へのマッピングの例を示します。

```
switch# show vlan fcoe

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

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

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

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

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

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

```
switch# show interface vfc 1
vfc1 is trunking (Not all VSANs UP on the trunk)
    Bound interface is Ethernet1/19
    Hardware is Virtual Fibre Channel
    Port WWN is 20:00:00:05:9b:74:bd:bf
    Admin port mode is F, trunk mode is on
    snmp link state traps are enabled
    Port mode is TF
    Port vsan is 20
    Trunk vsans (admin allowed and active) (1,20,100,200,300,400,500)
    Trunk vsans (up)                       (20)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             (1,100,200,300,400,500)
    1 minute input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    1 minute output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      355278397 frames input, 573433988904 bytes
        0 discards, 0 errors
      391579316 frames output, 572319570200 bytes
        0 discards, 0 errors
    last clearing of "show interface" counters Tue May 31 20:56:41 2011
```

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

次に、NPV FLOGI セッションに関する情報の例を示します。

```
switch# show npv flogi-table
--------------------------------------------------------------------------------
SERVER                                                                          EXTERNAL
INTERFACE VSAN FCID            PORT NAME               NODE NAME               INTERFACE
--------------------------------------------------------------------------------
vfc1      20   0x670000 21:01:00:1b:32:2a:e5:b8 20:01:00:1b:32:2a:e5:b8 fc2/6

Total number of flogi = 1.
```

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

```
switch# show npv status

npiv is enabled

disruptive load balancing is disabled

External Interfaces:
====================
  Interface:  fc2/5, State: Trunking
        VSAN:    1, State: Up
        VSAN:  200, State: Up
        VSAN:  400, State: Up
        VSAN:   20, State: Up
        VSAN:  100, State: Up
        VSAN:  300, State: Up
        VSAN:  500, State: Up, FCID: 0xa10000
  Interface:  fc2/6, State: Trunking
        VSAN:    1, State: Up
        VSAN:  200, State: Up
        VSAN:  400, State: Up
        VSAN:   20, State: Up
        VSAN:  100, State: Up
        VSAN:  300, State: Up
        VSAN:  500, State: Up, FCID: 0xa10001
  Interface:  vfc90, State: Down
  Interface: vfc100, State: Down
  Interface: vfc110, State: Down
  Interface: vfc111, State: Down
  Interface: vfc120, State: Down
  Interface: vfc130, State: Trunking
        VSAN:    1, State: Waiting For VSAN Up
        VSAN:  200, State: Up
        VSAN:  400, State: Up
        VSAN:  100, State: Up
        VSAN:  300, State: Up
        VSAN:  500, State: Up, FCID: 0xa10002

  Number of External Interfaces: 8

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

  Number of Server Interfaces: 8
```

次に、ポート チャネル 130 の実行コンフィギュレーションの例を示します。

```
switch# show running-config interface port-channel 130
```

```
!Command: show running-config interface port-channel130
!Time: Wed Jun  1 22:01:05 2011

version 5.0(3)N2(1)

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

次に、ISSU に対する FCoE NPV の影響の例を示します。

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

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


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

vfc90
vfc100
vfc110
vfc111
vfc120
vfc130

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

第 7 章

VSAN トランキングの設定

この章の内容は、次のとおりです。

- VSAN トランキングの設定，93 ページ

VSAN トランキングの設定

VSAN トランキングの概要

VSAN トランキングにより、相互接続ポートは複数の VSAN でフレームを送受信できます。 トランキングは E ポートおよび F ポートでサポートされます。

Cisco NX-OS Release 5.0(2)N1(1) から、VSAN トランキングは、ネイティブ ファイバ チャネル インターフェイスと仮想ファイバ チャネル インターフェイスでサポートされます。

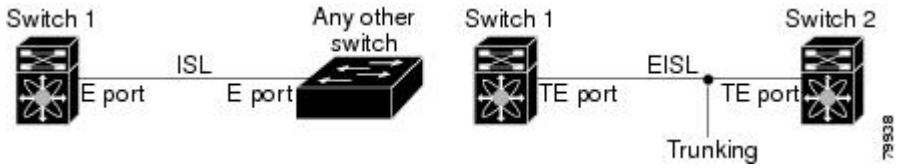
VSAN トランキング機能には、次の制限事項があります。

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

E ポートのトランキング

E ポートをトランキングすると、相互接続ポートが拡張 ISL（EISL）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 *15*：*E* ポートのトランキング



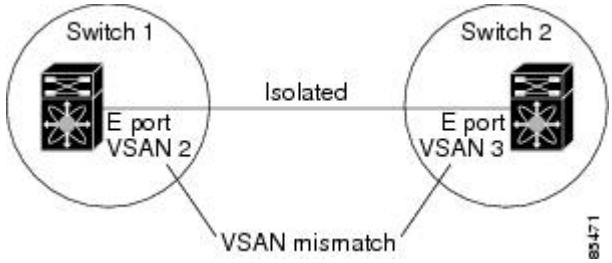
F ポートのトランキング

F ポートをトランキングすると、相互接続ポートが同一物理リンクによって、複数の VSAN でタグ付きフレームを送受信できます。

VSAN トランキングの不一致

E ポート間で VSAN が正しく設定されなかった場合、2 つの VSAN でトラフィックが結合される（その結果、2 つの VSAN が一致しなくなる）などの問題が発生します。 VSAN トランキング プロトコルは、VSAN インターフェイスを ISL の両端で検証し、VSAN の結合を防ぎます（次の図を参照）。

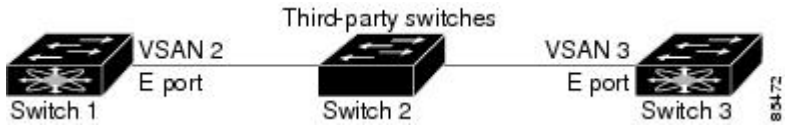
図 *16*：*VSAN* の不一致



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

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

図 *17*：サードパーティ製スイッチによる *VSAN* の不一致



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

VSAN トランキング プロトコル

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

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

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

VSAN トランキングの設定

注意事項および制約事項

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

TE ポートと TF-TNP ポートの相違点

TE ポートの場合、そのインターフェイスで VSAN が起動してピアがネゴシエーション フェーズにあるとき、VSAN は初期状態にあります。 ハンドシェイクが完了すると、成功した場合はアップの状態に、失敗した場合は分離状態に移行します。 Device Manager では、初期化状態ではポート ステータスが黄色で表示され、VSAN がアップすると緑色で表示されます。

TF ポートの場合、ハンドシェイク後に許可 VSAN のいずれかがアップ状態に移行します。 ピアとのハンドシェイクが完了し、それが成功した場合でも、他の VSAN はすべて初期状態となりま

す。 対応する VSAN にある、トランキングされた F または NP ポートを使用してサーバまたはターゲットがログインしたとき、各 VSAN は、初期化状態からアップ状態に移行します。

VSAN トランキング プロトコルのイネーブル化/ディセーブル化

スイッチの VSAN トランキング プロトコルをイネーブルまたはディセーブルにするには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **no trunk protocol enable**
3. switch(config)# **trunk protocol enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **no trunk protocol enable**	トランキング プロトコルをディセーブルにします。
ステップ 3	switch(config)# **trunk protocol enable**	トランキング プロトコルをイネーブルにします（デフォルト）。

トランク モードについて

デフォルトでは、すべてのファイバ チャネルでトランク モードはイネーブルです。 ただし、トランク モード設定は E ポート モードでしか有効になりません。 トランク モードを on（イネーブル）、off（ディセーブル）、または auto（自動）に設定できます。 デフォルトのトランク モードは on です。 リンクの両端のトランク モード設定によって、両端のリンクおよびポート モードのトランキング ステートが決まります（次の表を参照）。

表 *12*：スイッチ間のトランク モード ステータス

トランク モードの設定	最終的なステートとポート モード		
Switch 1	**Switch 2**	**トランキング ステート**	**Port Mode**
On	auto または on	トランキング（EISL）	TE ポート

トランクモードの設定	最終的なステートとポート モード		
Switch 1	**Switch 2**	**トランキング ステート**	**Port Mode**
Off	auto、on、または off	トランキングなし（ISL）	E ポート
Auto	Auto	トランキングなし（ISL）	E ポート

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

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

トランク モードの設定

トランク モードを設定するには、次の作業を行います。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface** {**fc** *slot/port* | **vfc** *vfc-id*}	指定のファイバ チャネルまたは仮想ファイバ チャネル インターフェイスを設定します。
ステップ 3	switch(config-if)# **switchport trunk mode on**	指定されたインターフェイスのトランク モードをイネーブルにします（デフォルト）。

	コマンドまたはアクション	目的
ステップ 4	switch(config-if)# **switchport trunk mode off**	指定されたインターフェイスのトランク モードをディセーブルにします。 （注） トランク モードは、仮想ファイバ チャネル インターフェイスではオフにできません。
ステップ 5	switch(config-if)# **switchport trunk mode auto**	インターフェイスの自動検知を提供するトランク モードを **auto** モードに設定します。

次に、トランク モードで vFC インターフェイスを設定する例を示します。

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

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

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

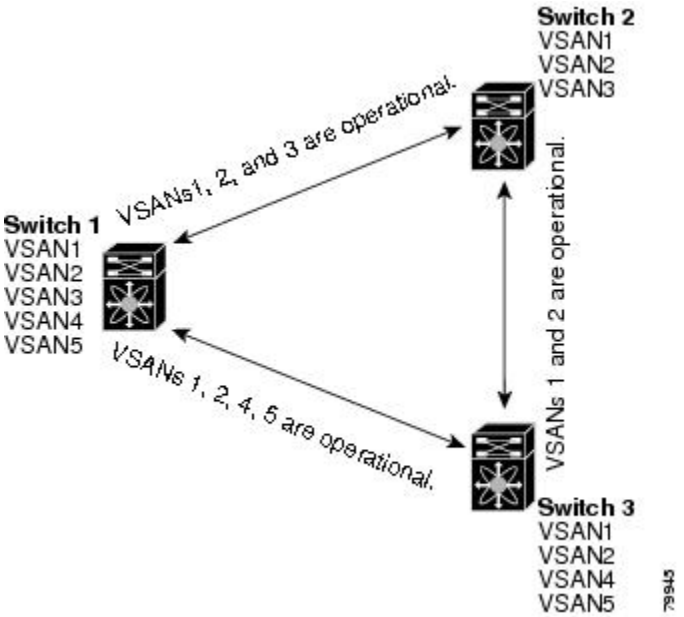
トランク許可 VSAN リストについて

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

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

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

図 *18*： *allowed-active VSAN* のデフォルト設定



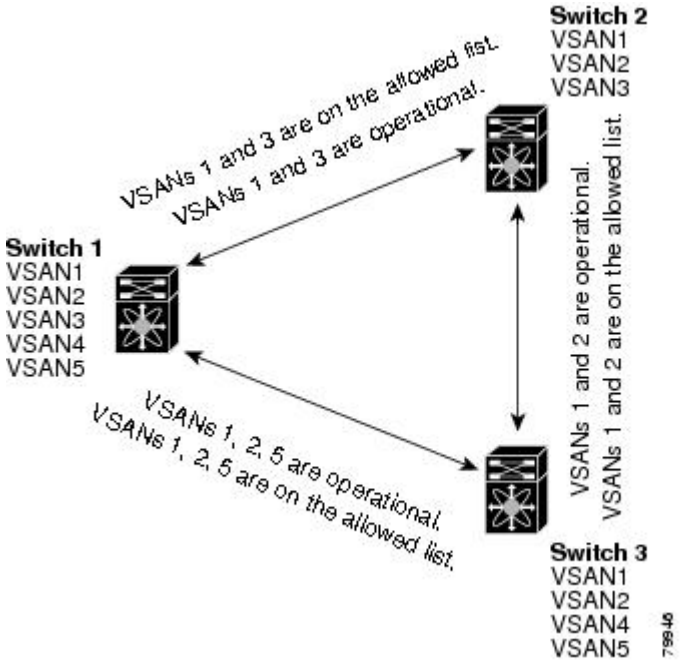
allowed-active リストから選択した VSAN セットを設定して、トランキング ISL に指定された VSAN へのアクセスを制御できます。

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

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

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

図 *19*：通信可能な許可 *VSAN* の設定



VSAN の許可アクティブ リストの設定

インターフェイスに allowed-active VSAN リストを設定するには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **interface fc** *slot/port*
3. switch(config-if)# **switchport trunk allowed vsan** *vsan-id* **-** *vsan-id*
4. switch(config-if)# **switchport trunk allowed vsan add** *vsan-id*
5. switch(config-if)# **no switchport trunk allowed vsan** *vsan-id* **-** *vsan-id*
6. switch(config-if)# **no switchport trunk allowed vsan add** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **interface fc** *slot/port*	指定されたインターフェイスを設定します。
ステップ 3	switch(config-if)# **switchport trunk allowed vsan** *vsan-id* **-** *vsan-id*	指定された VSAN 範囲の許可リストを変更します。
ステップ 4	switch(config-if)# **switchport trunk allowed vsan add** *vsan-id*	指定された VSAN を新しい許可リストに追加します。
ステップ 5	switch(config-if)# **no switchport trunk allowed vsan** *vsan-id* **-** *vsan-id*	指定された VSAN 範囲を削除します。
ステップ 6	switch(config-if)# **no switchport trunk allowed vsan add** *vsan-id*	追加された許可リストを削除します。

VSAN トランキング情報の表示

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

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

```
switch# show interface fc3/3
fc3/3 is up
    Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:83:00:0d:ec:6d:78:40
    Peer port WWN is 20:0c:00:0d:ec:0d:d0:00
    Admin port mode is auto, trunk mode is on
...
```

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

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

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

```
switch# show interface trunk vsan 1-1000
fc3/1 is not trunking
...
fc3/11 is trunking
    Belongs to san-port-channel 6
    Vsan 1 is up, FCID is 0xef0000
    Vsan 2 is up, FCID is 0xef0000
...
san-port-channel 6 is trunking
    Vsan 1 is up, FCID is 0xef0000
    Vsan 2 is up, FCID is 0xef0000
```

トランクのデフォルト設定

次の表に、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*：デフォルト トランク設定パラメータ

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

第 8 章

SAN ポート チャネルの設定

この章の内容は、次のとおりです。

- SAN ポート チャネルの設定，103 ページ

SAN ポート チャネルの設定

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

Cisco Nexus 5000 シリーズ スイッチでは、SAN ポート チャネルは物理ファイバ チャネル インターフェイスを含むことがありますが、仮想ファイバ チャネル インターフェイスを含みません。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むことができます。

SAN ポート チャネルに関する情報

E ポート チャネルについて

E ポート チャネルは、複数の E ポートを 1 つの論理インターフェイスに集約し、より精度の高い集約帯域幅、ロード バランシング、およびリンク冗長性を提供する機能です。 ポート チャネルはスイッチング モジュール間のインターフェイスに接続できるため、スイッチング モジュールで障害が発生してもポート チャネルのリンクがダウンすることはありません。

SAN ポート チャネルには、次の機能があります。

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

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

NPV ポート チャネルおよび NP ポート チャネルについて

Cisco Nexus 5000 シリーズ スイッチは、NPV モードで最大 4 つの SAN ポート チャネルをサポートします（ポートチャネルあたり 8 つのインターフェイス）。 これは、NPV モードの Cisco Nexus 5000 シリーズ スイッチでは最大 4 つの NP ポートチャネルをサポートすることを意味します。 F ポート/E ポートのチャネリングに制限はありません。 ポート チャネル番号は、各チャネル グループに関連付けられた（スイッチごとに）一意の識別番号です。 この番号の範囲は 1 ～ 256 です。

F および TF ポート チャネルについて

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

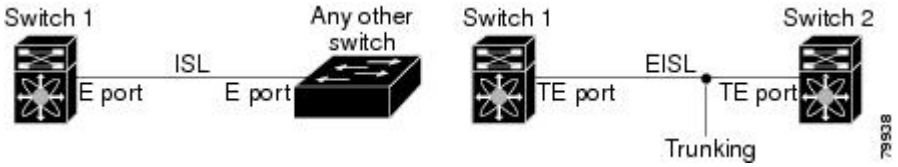
ポート チャネルと VSAN トランキングの概要

Cisco Nexus 5000 シリーズ のスイッチでは、次のように VSAN（仮想 SAN）トランキングおよびポート チャネルを実装しています。

- SAN ポート チャネルでは、複数の物理リンクを 1 つの集約論理リンクに結合できます。
- 次の図の左側に示すように、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、スイッチ間リンク（ISL）と呼ばれます。
- VSAN トランキングを使用すると、複数の VSAN のトラフィックを伝送する EISL 形式でのフレーム伝送が可能になります。 トランキングが E ポートで動作可能な場合、その E ポート

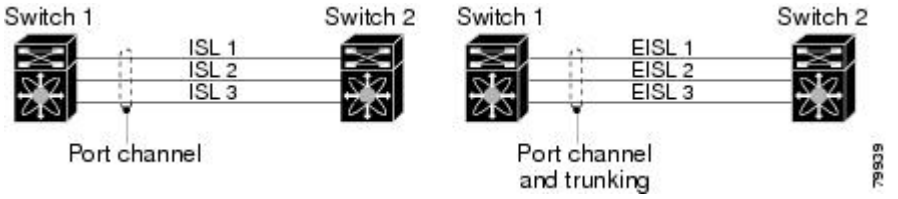
は TE ポートになります。 次の図の右側に示すように、EISL はシスコ スイッチ間のみで接続されます。

図 *20*： *VSAN* トランキングのみ



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

図 *21*： ポート チャネルと *VSAN* トランキング



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

ロード バランシングの概要

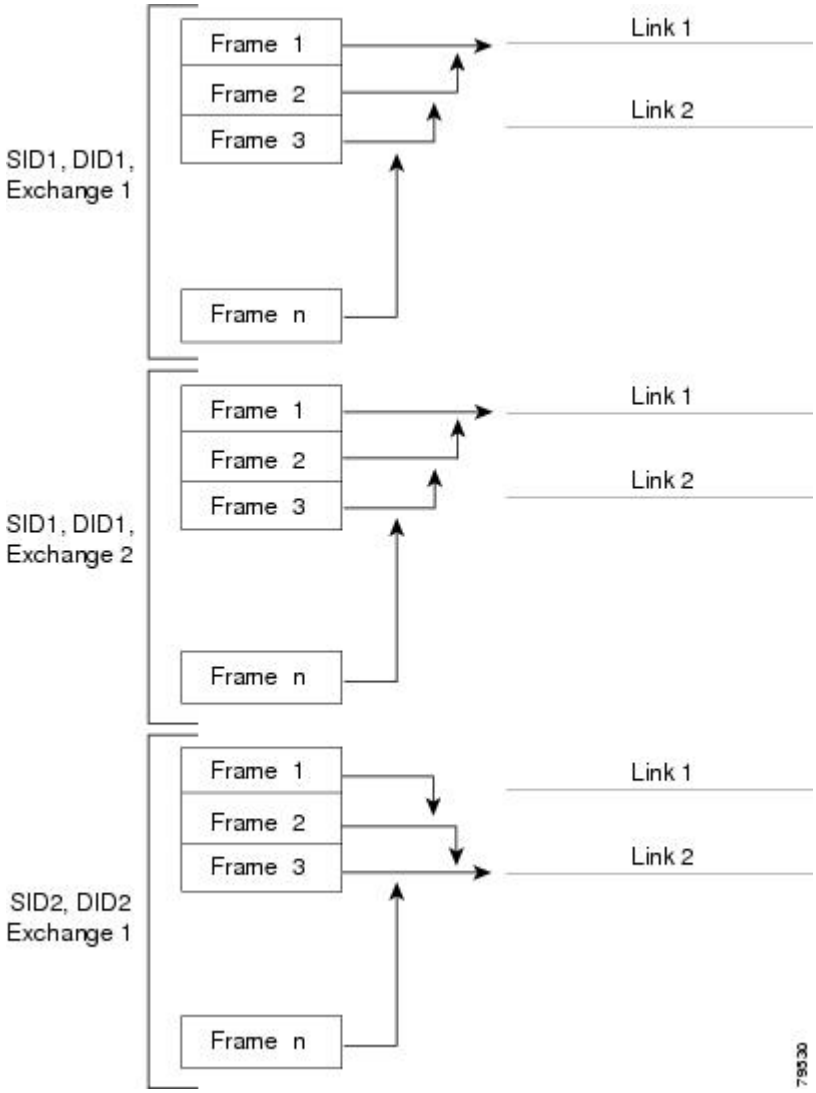
ロード バランシング機能は、次の方式を使用して提供できます。

- フローベース：送信元と宛先間のすべてのフレームが所定のフローで同一のリンクをたどります。 つまり、フローの最初のエクスチェンジで選択されたリンクが、後続のすべてのエクスチェンジで使用されます。

- エクスチェンジベース：エクスチェンジの最初のフレームがリンクに割り当てられ、エクスチェンジの後続のフレームが同一のリンクをたどります。 ただし、後続のエクスチェンジは、別のリンクを使用できます。 この方式によって、より精度の高いロード バランシングが可能になり、さらに各エクスチェンジでのフレームの順序が維持されます。

次の図は、フロー ベースのロード バランシングがどのように機能するかを示します。 フローの最初のフレームが転送のためにインターフェイスで受信されると、リンク 1 が選択されます。 そのフローの各後続のフレームが、同一のリンク上に送信されます。 SID1 および DID1 のフレームは、リンク 2 を使用しません。

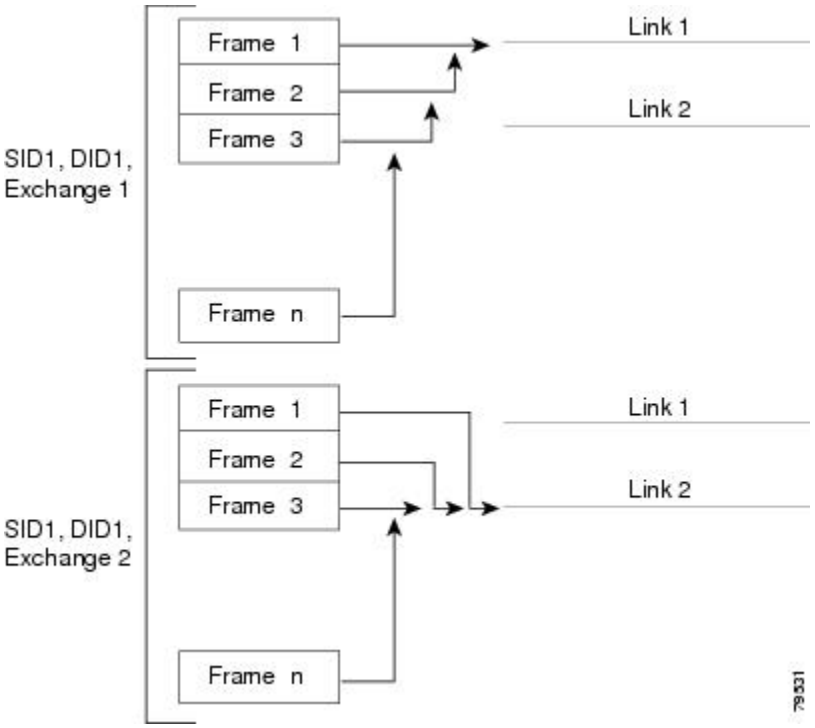
図 *22*： *SID1*、*DID1*、およびフロー ベースのロード バランシング



次の図は、エクスチェンジ ベースのロード バランシングがどのように機能するかを示します。 エクスチェンジで最初のフレームが転送用にインターフェイスで受信されると、リンク 1 がハッ

シュアルゴリズムによって選択されます。そのやり取りの残りすべてのフレームは、同じリンクで送信されます。 エクスチェンジ 1 では、リンク 2 を使用するフレームはありません。 次のエクスチェンジでは、ハッシュ アルゴリズムによってリンク 2 が選択されます。 やり取り 2 のすべてのフレームではリンク 2 が使用されます。

図 *23* : ***SID1***、***DID1***、およびエクスチェンジ ベースのロード バランシング



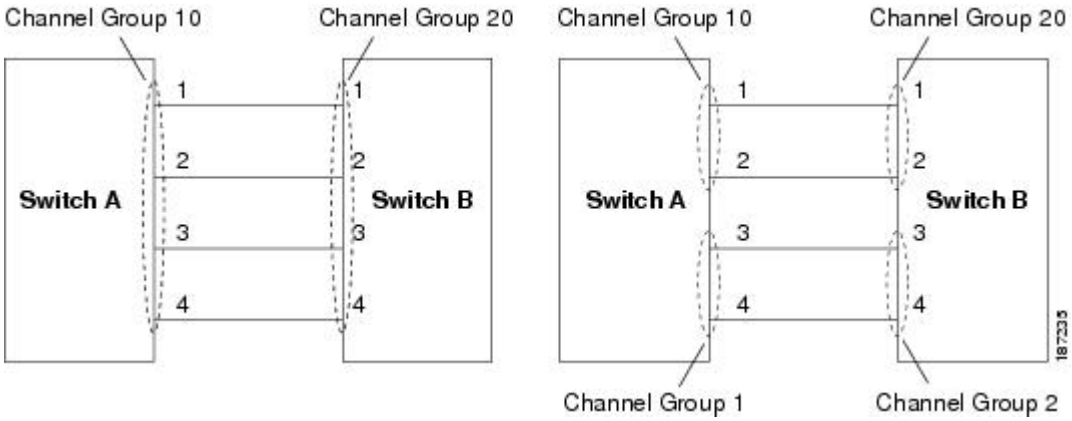
SAN ポート チャネルの設定

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

SAN ポート チャネルの設定

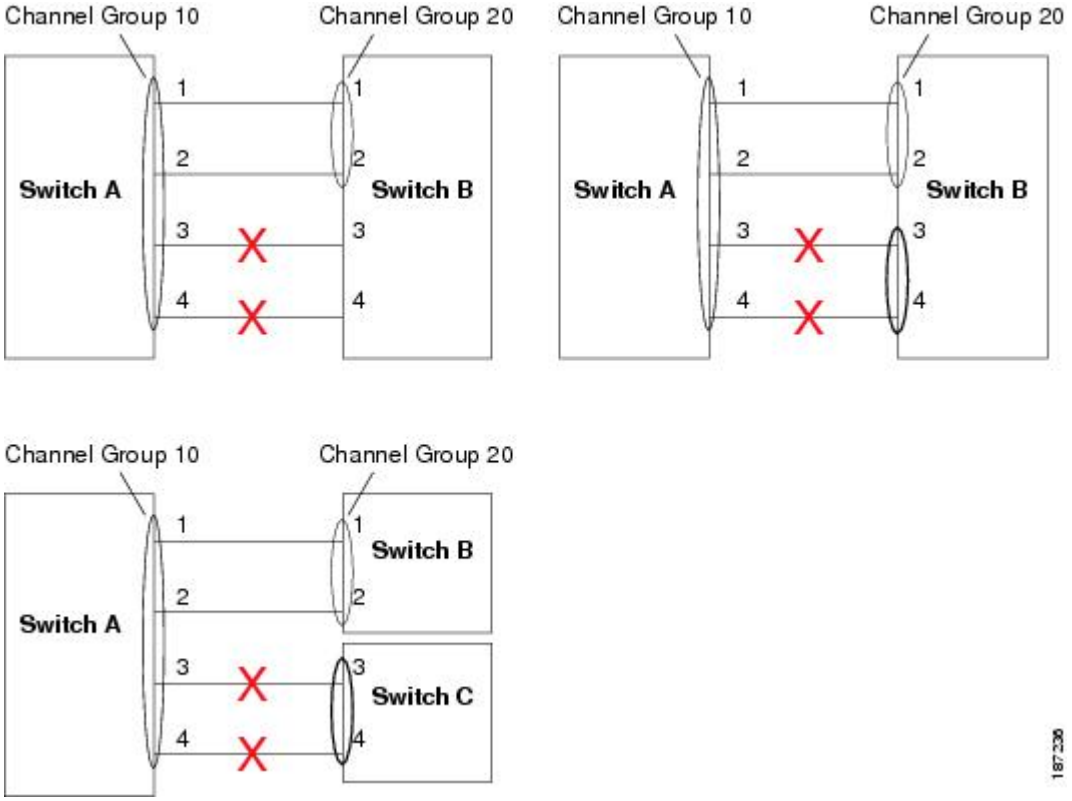
次の図は、有効な SAN ポート チャネルの設定例を示します。

図 *24*：有効な *SAN* ポート チャネルの設定



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

図 *25*：誤った設定



SAN ポート チャネルの設定時の注意事項

SAN ポート チャネルを設定する前に、次の注意事項を守ってください。

- 両方の拡張モジュールからファイバ チャネル ポートを使用して SAN ポート チャネルを設定し、アベイラビリティを向上させます（いずれかの拡張モジュールが故障した場合）。
- 1 つの SAN ポート チャネルが異なるスイッチ群に接続されないようにします。 SAN ポート チャネルでは、同一のスイッチ群内でのポイントツーポイント接続が必要です。
- SAN ポート チャネルを誤って設定すると、誤設定メッセージを受け取る場合があります。このメッセージを受け取った場合、エラーが検出されてポート チャネルの物理リンクはディセーブルになります。
- 次の要件を満たしていない場合に、SAN ポート チャネルのエラーが検出されます。
  - SAN ポート チャネルの両側のスイッチが、同じ数のインターフェイスに接続されている必要があります。
  - 各インターフェイスは、反対側の対応するインターフェイスに接続されている必要があります。
  - ポート チャネルを設定したあとで、SAN ポート チャネルのリンクを変更できません。ポート チャネルを設定したあとにリンクを変更する場合は、必ずそのポート チャネル内でリンクをインターフェイスに再接続し、再度イネーブルにしてください。

    3つすべての条件が満たされていない場合、そのリンクはディセーブルになっています。

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

F および TF ポート チャネルの注意事項

F および TF ポート チャネルの注意事項は次のとおりです。

- ポートを F モードとしておく必要があります。
- 自動作成はサポートされません。
- ON モードはサポートされません。 サポートされるのは Active-Active モードだけです。 デフォルトでは、NPV スイッチのモードは Active です。
- MDS スイッチの F ポート チャネル経由でログインしたデバイスは、IVR の非 NAT 設定でサポートされません。 このデバイスをサポートするのは IVR NAT 設定だけです。
- ポート セキュリティ ルールは、物理 pWWN だけで単一リンク レベルで実行されます。
- F ポート チャネル経由でログインする N ポートのネーム サーバ登録では、ポート チャネル インターフェイスの fWWN を使用します。
- DPVM 設定はサポートされません。

- ポート チャネルのポート VSAN はダイナミック ポート VSAN メンバーシップ（DPVM）を使用して設定できません。

SAN ポート チャネルの作成

SAN ポート チャネルを作成する手順は、次のとおりです。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface san-port-channel** *channel-number*	デフォルトのモード（オン）を使用して、指定された SAN ポート チャネルを作成します。 SAN ポート チャネル番号の範囲は、1 ～ 256 です。

ポート チャネル モードについて

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

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

（注） F ポート チャネルはアクティブ モードのみでサポートされます。

次の表では、オン モードとアクティブ モードを比較します。

表 *14*：チャネル グループ設定の相違点

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

アクティブ モードの SAN ポート チャネルの設定

アクティブ モードを設定する手順は、次のとおりです。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface san-port-channel** *channel-number*	デフォルトのオン モードを使用して、指定されたポート チャネルを設定します。 SAN ポート チャネル番号の範囲は、1 ～ 256 です。
ステップ 3	switch(config-if)# **channel mode active**	アクティブ モードを設定します。
ステップ 4	switch(config-if)# **no channel mode active**	デフォルトのオン モードに戻します。

アクティブ モードの設定例

アクティブ モードを設定する手順は、次のとおりです。

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

SAN ポート チャネルの削除について

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

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

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

関連トピック

インターフェイス管理ステートの設定, （21 ページ）

SAN ポート チャネルの削除

SAN ポート チャネルを削除する手順は、次のとおりです。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **no interface san-port-channel** *channel-number*	指定されたポート チャネル、関連するインターフェイス マッピング、およびこの SAN ポート チャネルのハードウェア アソシエーションを削除します。

SAN ポート チャネルのインターフェイス

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

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

SAN ポート チャネルへのインターフェイスの追加について

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

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

互換性チェック

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

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

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

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

Cisco NX-OS Release 5.0(2)N2(1) 以降、**channel-group force** コマンドを入力して、チャネル グループにポートを強制的に追加した後で、次の 2 つの状態が発生します。

- インターフェイスがポートチャネルに参加すると、次のパラメータは削除され、動作上ポート チャネルの値と置き換えられます。ただし、この変更は、インターフェイスの実行コンフィギュレーションには反映されません。
  - QoS
  - 帯域幅
  - 遅延
  - STP
  - サービス ポリシー
  - ACL

  インターフェイスがポートチャネルに参加または脱退した場合、次のパラメータは影響を受けません。
  - ビーコン
  - 説明
  - CDP
  - LACP ポート プライオリティ

- デバウンス
- UDLD
- シャットダウン
- SNMP トラップ

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、互換性チェックは失敗し、インターフェイスは設定されたモードに基づいて中断ステートまたは隔離ステートになります。

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

SAN ポート チャネルへのインターフェイスの追加

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface** *type slot*/*port*	指定されたインターフェイスのコンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **channel-group** *channel-number*	ファイバ チャネル インターフェイスを指定されたチャネル グループに追加します。 チャネル グループが存在しない場合は、作成されます。 ポートがシャットダウンします。

インターフェイスの強制追加

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

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

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

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

SAN ポート チャネルへポートを強制的に追加する手順は、次のとおりです。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface** *type slot*/*port*	指定されたインターフェイスのコンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **channel-group** *channel-number* **force**	指定されたチャネル グループにインターフェイスを強制的に追加します。 E ポートがシャットダウンします。

SAN ポート チャネルからのインターフェイスの削除について

物理インターフェイスが SAN ポート チャネルから削除された場合は、チャネル メンバーシップが自動更新されます。 削除されたインターフェイスが最後の動作可能なインターフェイスである場合は、ポート チャネルのステータスは、down ステートに変更されます。 SAN ポート チャネル

からインターフェイスを削除すると、SAN ポート チャネルのチャネル サイズと帯域幅が減少します。

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

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

SAN ポート チャネルからのインターフェイスの削除

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch(config)# **interface** *type slot/port*	指定されたインターフェイスのコンフィギュレーション モードを開始します。
ステップ 2	switch(config-if)# **no channel-group** *channel-number*	物理ファイバチャネルインターフェイスを指定されたチャネル グループから削除します。

SAN ポート チャネル プロトコル

スイッチ ソフトウェアでは、安定性のあるエラー検出および同期化機能を提供します。 チャネル グループは手動で設定するか、または自動的に作成できます。 どちらの場合でも、チャネル グループの機能および設定可能なパラメータは同じです。 対応付けられた SAN ポート チャネル インターフェイスに適用される設定の変更は、チャネル グループ内のすべてのメンバに伝播されます。

SAN ポート チャネルの設定を交換するプロトコルが Cisco SAN スイッチでサポートされます。これにより、互換性のない ISL でのポート チャネル管理が簡素化されます。 追加された自動作成

モードでは、互換性のあるパラメータを持つ ISL でチャネル グループを自動的に作成でき、手動での作業は必要ありません。

デフォルトではポート チャネル プロトコルがイネーブルになっています。

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

ポート チャネル プロトコルは、次の 2 つのサブプロトコルを使用します。

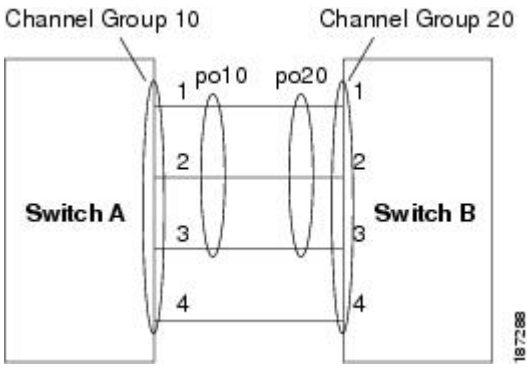
- 起動プロトコル：自動的に誤設定を検出するため、これらを修正できます。このプロトコルは両側で SAN ポート チャネルを同期化するため、特定のフロー（送信元 FC ID、宛先 FC ID、および OX_ID によって識別される）のフレームは両方向ともすべて同じ物理リンクを経由して伝送されます。これにより、FCIP リンク上の SAN ポート チャネルで書き込みアクセラレーションなどのアプリケーションを動作させることができます。
- 自動作成プロトコル：互換性のあるポートを SAN ポート チャネルに自動的に集約します。

チャネル グループの作成の概要

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

最初の ISL は個別リンクとしてアップします。次の図に示した例では、これはリンク A1 ～ B1 です。次のリンク（たとえば A2-B2）がアップすると、ポート チャネル プロトコルは、このリンクがリンク A1-B1 と互換性があるかどうかを識別し、それぞれのスイッチでチャネル グループ 10 および 20 を自動的に作成します。それぞれのポートの設定に互換性がある場合、リンク A3-B3 はチャネル グループ（およびポート チャネル）に参加できます。リンク A4-B4 はチャネル グループ内の既存のメンバ ポートと互換性がないため、個別のリンクとして動作します。

図 *26*：チャネル グループの自動作成



チャネル グループ番号は動的に割り当てられます（チャネル グループが形成される場合）。

チャネル グループ番号は、ポートの初期化の順序により同一のポート チャネル群が再起動すると変化する場合があります。

次の表に、ユーザ設定のチャネル グループと自動設定のチャネル グループの相違点を示します。

表 *15*：チャネル グループ設定の相違点

ユーザ設定のチャネル グループ	自動設定のチャネル グループ
ユーザが手動で設定します。	2 つの互換性のあるスイッチ間で互換性のあるリンクがアップしたときに自動的に作成されます（両端のすべてのポートでチャネル グループの自動作成がイネーブルになっている場合）。
メンバ ポートはチャネル グループの自動作成には参加できません。 自動作成機能は設定できません。	これらのポートは、ユーザ設定のチャネル グループのメンバにはなりません。
チャネル グループのポートの一部を使用して SAN ポート チャネルを作成できます。 オン モードまたはアクティブ モードの設定に応じて、互換性のないポートは中断ステートまたは隔離ステートのままになります。	チャネル グループに含まれるすべてのポートが SAN ポート チャネルに参加します。 いずれのメンバ ポートも隔離ステートまたは中断ステートになりません。その代わりに、リンクに互換性がない場合、メンバ ポートはチャネル グループから削除されます。
SAN ポート チャネルに対する管理設定は、チャネル グループのすべてのポートに適用され、ポート チャネル インターフェイスの設定は保存できます。	SAN ポート チャネルに対する管理設定は、チャネル グループのすべてのポートに適用され、メンバ ポートの設定は保存されますが、ポート チャネル インターフェイスの設定は保存されません。 このチャネル グループは、必要に応じて明示的に変更できます。
任意のチャネル グループの削除およびチャネル グループへのメンバの追加が可能です。	チャネル グループは削除できません。 チャネル グループのメンバの追加および削除はできません。 メンバ ポートが存在しない場合、チャネル グループは削除されます。

自動作成の注意事項

自動作成プロトコルを使用する場合、次の注意事項に従ってください。

- 自動作成機能がイネーブルの場合、ポートを SAN ポート チャネルの一部として設定できません。 これらの 2 つの設定を同時に使用できません。

- 自動作成は、SAN ポート チャネルのネゴシエーションを行うローカル ポートとピア ポートの両方でイネーブルにする必要があります。
- 集約は、次の 2 通りの方法で実行されます。
  - ポートを互換性のある自動作成 SAN ポート チャネルへ集約する。
  - ポートを互換性のある別のポートと集約して新しい SAN ポート チャネルを構成する。
- 新しく作成される SAN ポート チャネルには、最大利用可能ポート チャネルからアベイラビリティに基づいて番号が降順に割り当てられます。 すべてのポート チャネル番号を使い切ると、集約は許可されなくなります。
- メンバーシップの変更または自動作成された SAN ポート チャネルの削除はできません。
- 自動作成をディセーブルにすると、メンバ ポートはすべて自動作成された SAN ポート チャネルから削除されます。
- 自動作成された SAN ポート チャネルからすべてのメンバが削除されると、チャネルは自動的に削除され、チャネル番号は再利用できるように解放されます。
- 自動作成された SAN ポート チャネルは、再起動後は存在しません。 自動作成された SAN ポート チャネルを手動で設定すると、再起動後も維持できます。 SAN ポート チャネルを手動で設定すると、自動作成機能はすべてのメンバ ポートでディセーブルになります。
- 自動作成機能は、ポート単位またはスイッチ内のすべてのポートに対して、イネーブルまたはディセーブルに設定できます。 この設定がイネーブルの場合、チャネル グループ モードはアクティブと見なされます。 このタスクのデフォルトはディセーブルです。
- インターフェイスに対してチャネル グループの自動作成がイネーブルになっている場合、最初に自動作成をディセーブルにしてから、以前のソフトウェア バージョンにダウングレードするか、または手動設定されたチャネル グループでインターフェイスを設定する必要があります。

ヒント Cisco Nexus 5000 シリーズ スイッチで自動作成をイネーブルにする場合、自動作成設定を使用せずに、スイッチ間で少なくとも 1 つのポートを相互接続しておくことを推奨します。 2 つのスイッチ間のすべてのポートを自動作成機能で同時に設定する場合、ポートは自動作成された SAN ポート チャネルに追加される際に自動的にディセーブル化され、再度イネーブルになるため、2 つのスイッチ間でトラフィックが中断される可能性があります。

自動作成のイネーブル化および設定

自動チャネル グループを設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **interface** *type slot*/*port*
3. switch(config- if)# **channel-group auto**
4. switch(config- if)# **no channel-group auto**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface** *type slot*/*port*	指定されたインターフェイスのコンフィギュレーション モードを開始します。
ステップ 3	switch(config- if)# **channel-group auto**	選択したインターフェイスでチャネル グループを自動作成します。
ステップ 4	switch(config- if)# **no channel-group auto**	現在のインターフェイスのチャネル グループの自動作成をディセーブルにします（システムのデフォルト設定で自動作成がイネーブルになっている場合も同様）。

自動作成の設定例

次に、自動チャネル グループを設定する例を示します。

```
switch(config)# interface fc2/3
switch(config-if)# channel-group auto
```

手動設定チャネル グループの概要

ユーザによって設定されたチャネル グループを自動作成チャネル グループに変更できません。ただし、自動作成されたチャネル グループから手動チャネル グループへの変更は可能です。 このタスクは元に戻せません。 チャネル グループ番号は変わりませんが、メンバ ポートは手動設定されたチャネル グループのプロパティに従って動作します。また、チャネル グループの自動作成はすべてのポートに対して暗黙的にディセーブルになります。

手動設定にする場合は、必ず SAN ポート チャネルの両側で実行してください。

手動設定チャネル グループへの変更

自動作成されたチャネル グループをユーザ設定チャネル グループに変換するには、**san-port-channel** *channel-group-number* persistent EXEC コマンドを使用します。 SAN ポート チャネルが存在しない場合、このコマンドは実行されません。

ポート チャネルの設定例

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

次の例は、ポート チャネルの作成方法を示しています。

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

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

```
switch(config)# interface fc1/4-6
switch(config-if)# shut
switch(config-if)# switchport mode F
switch(config-if)# switchport speed 4000
switch(config-if)# switchport rate-mode dedicated
switch(config-if)# switchport trunk mode on
switch(config-if)# channel-group 2
switch(config-if)# no shut
switch(config-if)# exit
```

次に、NPV スイッチで専用モードでポート チャネルを作成する例を示します。

```
switch(config)# interface san-port-channel 2
switch(config-if)# switchport mode NP
switch(config-if)# no shut
switch(config-if)# exit
```

次に、NPV スイッチ上でポート チャネル メンバ インターフェイスを設定する例を示します。

```
switch(config)# interface fc2/1-2
switch(config-if)# shut
switch(config-if)# switchport mode NP
switch(config-if)# switchport trunk mode on
switch(config-if)# channel-group 2
switch(config-if)# no shut
switch(config-if)# exit
```

SAN ポート チャネル設定の確認

EXEC モードからいつでも既存の SAN ポート チャネルの特定の情報を表示できます。 次の **show** コマンドを実行すると、既存の SAN ポート チャネルの詳細が表示されます。

show san-port-channel summary コマンドを実行すると、スイッチ内の SAN ポート チャネルの概要が表示されます。 各 SAN ポート チャネルの 1 行ずつの概要には、管理ステート、動作可能ステート、接続されてアクティブな状態（アップ）のインターフェイスの数、コントロールプレーン トラフィック（ロード バランシングなし）を伝送するために SAN ポート チャネルで選択された主要な動作可能インターフェイスである First Operational Port（FOP）を表示します。 FOP は

SANポートチャネルで最初にアップするポートで、このポートがダウンした場合は変わることがあります。 FOP はアスタリスク（*）でも識別できます。

VSAN の設定情報を表示するには、次のいずれかのタスクを実行します。

手順の概要

1. switch# **show san-port-channel summary** | **database** | **consistency** [**details**] | **usage** | **compatibility-parameters**
2. switch# **show san-port-channel database interface san-port-channel** *channel-number*
3. switch# switch# **show interface fc** *slot*/*port*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **show san-port-channel summary**	**database**	**consistency** [**details**]	**usage**	**compatibility-parameters**	SAN ポート チャネルの情報を表示します。
ステップ 2	switch# **show san-port-channel database interface san-port-channel** *channel-number*	指定された SAN ポート チャネルの情報を表示します。
ステップ 3	switch# switch# **show interface fc** *slot*/*port*	指定されたファイバチャネルインターフェイスの VSAN 設定情報を表示します。

確認コマンドの例

次に、SAN ポート チャネル情報の概要を表示する例を示します。

```
switch# show san-port-channel summary
--------------------------------------------------------------------------------
Interface                  Total Ports        Oper Ports        First Oper Port
--------------------------------------------------------------------------------
san-port-channel 7             2                 0                 --
san-port-channel 8             2                 0                 --
san-port-channel 9             2                 2
```

次に、SAN ポート チャネルの一貫性を表示する例を示します。

```
switch# show san-port-channel consistency
Database is consistent
```

次に、使用および未使用ポート チャネル番号の詳細を表示する例を示します。

```
switch# show san-port-channel usage
Totally 3 port-channel numbers used
===================================
Used  :   77 - 79
Unused:   1 - 76 , 80 - 256
```

自動作成された SAN ポート チャネルは、手動で作成された SAN ポート チャネルと区別できるように、明示的に示されます。 次に、自動作成されたポート チャネルを表示する例を示します。

```
switch# show interface fc2/1
fc2/1 is trunking
    Hardware is Fibre Channel, FCOT is short wave laser
    Port WWN is 20:0a:00:0b:5f:3b:fe:80
    ...
    Receive data field Size is 2112
    Beacon is turned off
    Port-channel auto creation is enabled
Belongs to port-channel 123
...
```

SAN ポート チャネルのデフォルト設定

次の表に、SAN ポート チャネルのデフォルト設定を示します。

表 *16*：デフォルト *SAN* ポート チャネル パラメータ

パラメータ	デフォルト
ポート チャネル	FSPF はデフォルトでイネーブルになっています。
ポート チャネル作成	管理上のアップ状態
デフォルト ポート チャネル モード	オン
自動作成	ディセーブル

第 9 章

VSAN の設定と管理

この章の内容は、次のとおりです。

- VSAN の設定と管理，125 ページ

VSAN の設定と管理

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

VSAN に関する情報

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

VSAN トポロジ

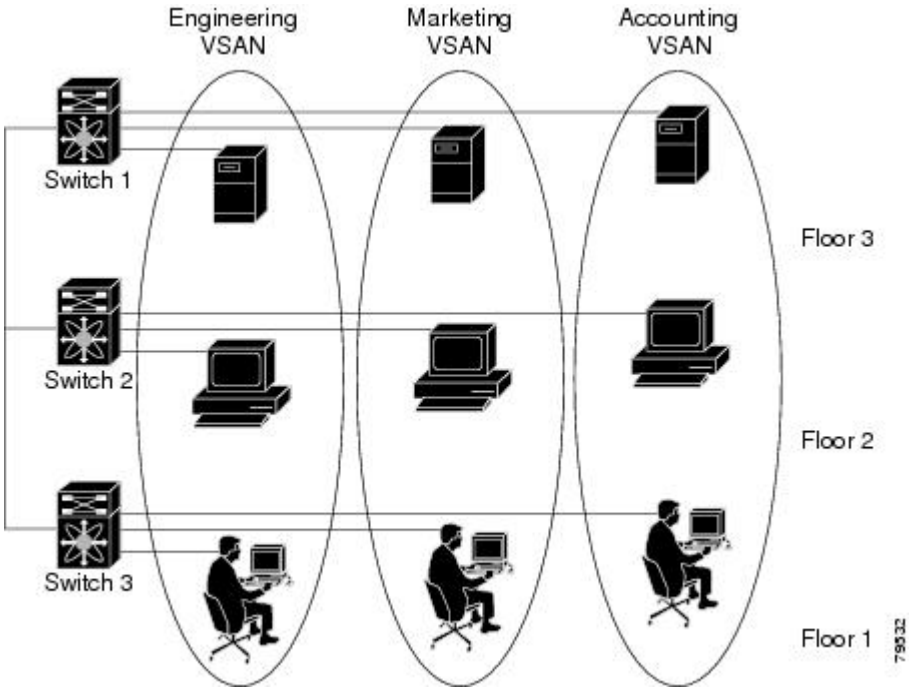
VSAN を導入することによって、ネットワーク管理者はスイッチ、リンク、および 1 つまたは複数の VSAN を含むトポロジを 1 つ作成できます。 このトポロジの各 VSAN では、SAN の動作およびプロパティが同じです。 VSAN には次の特性もあります。

- 複数の VSAN で同じ物理トポロジを共有できます。
- 同じファイバ チャネル ID（FC ID）を別の VSAN 内のホストに割り当て、VSAN のスケーラビリティを高めることができます。

- VSANの各インスタンスは、FSPF、ドメインマネージャ、およびゾーン分割などの必要なすべてのプロトコルを実行します。
- VSAN内のファブリック関連の設定は、別のVSAN内の関連トラフィックに影響しません。
- あるVSAN内のトラフィック中断を引き起こしたイベントはそのVSAN内にとどまり、他のVSANに伝播されません。

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

図 *27*： 論理 *VSAN* の区分け

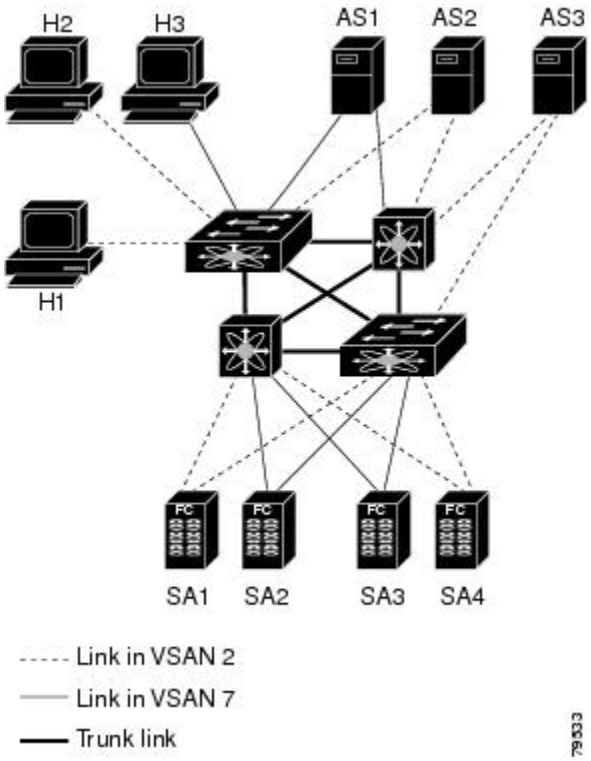


アプリケーションサーバまたはストレージアレイは、ファイバチャネルまたは仮想ファイバチャネル インターフェイスを使用してスイッチに接続できます。 VSANには、ファイバ チャネル インターフェイスと仮想ファイバ チャネル インターフェイスを組み合わせて含めることができます。

次の図に、VSAN 2（破線）とVSAN 7（実線）の2つの定義済みVSANからなるファイバ チャネル スイッチングの物理インフラストラクチャを示します。 VSAN 2には、ホストH1とH2、アプ

リケーション サーバ AS2 と AS3、ストレージ アレイ SA1 と SA4 が含まれます。 VSAN 7 は、H3、AS1、SA2、および SA3 と接続します。

図 *28*： *2* つの *VSAN* の例



このネットワークにある 4 つのスイッチは、VSAN 2 トラフィックおよび VSAN 7 トラフィックを伝送する VSAN トランク リンクに

よって相互接続されています。 各 VSAN に異なるスイッチ間トポロジを設定できます。 上の図では、VSAN 2 と VSAN 7 のスイッチ間トポロジは同じです。

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

このようなグループを作成する基準は、VSAN トポロジによって異なります。

- VSAN は、次の条件に基づいてトラフィックを分離できます。
  - ストレージ プロバイダー データセンター内の異なるお客様
  - 企業ネットワークの業務またはテスト
  - ロー セキュリティおよびハイ セキュリティの要件
  - 別個の VSAN によるバックアップ トラフィック

- ユーザ トラフィックからのデータの複製

- VSAN は、特定の部門またはアプリケーションのニーズを満たせます。

VSAN の利点

VSAN には、次のような利点があります。

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

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

VSAN とゾーン

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

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

表 *17*： *VSAN* とゾーンの比較

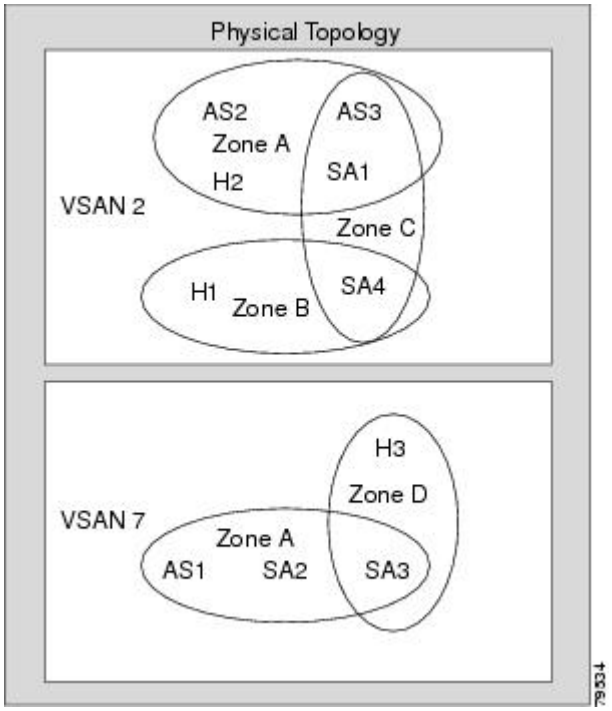
VSAN 特性	ゾーン特性
VSAN は、SAN とルーティング、ネーミング、およびゾーン分割プロトコルが同じです。	ルーティング、ネーミング、およびゾーニング プロトコルは、ゾーン単位で利用できません。
VSAN は、ユニキャスト、マルチキャスト、およびブロードキャスト トラフィックを制限します。	ゾーンは、ユニキャスト トラフィックを制限します。

VSAN 特性	ゾーン特性
メンバーシップは、一般的に VSAN ID を使用して F ポートに定義されます。	メンバーシップは、通常 pWWN によって定義されます。
HBA またはストレージ デバイスは、1 つの VSAN（F ポートに対応付けられた VSAN）だけに所属できます。	HBA またはストレージデバイスは、複数のゾーンに所属できます。
VSAN は、各 E ポート、送信元ポート、および宛先ポートでメンバーシップを実行します。	ゾーンは、送信元ポートおよび宛先ポートだけでメンバーシップを実行します。
VSAN は、規模が大きい環境（ストレージ サービス プロバイダー）で定義されます。	ゾーンは、ゾーンの外部に表示されないイニシエータおよびターゲットのセットで定義されます。
VSAN は、ファブリック全体を網羅します。	ゾーンは、ファブリック エッジで設定されます。

次の図は、VSAN とゾーン間の考えられる関係性を示します。 VSAN 2 には、ゾーン A、ゾーン B、ゾーン C の 3 つのゾーンが定義されています。 ゾーン C は、ファイバ チャネル標準に準拠してゾーン A とゾーン B にオーバーラップしています。 VSAN 7 には、ゾーン A とゾーン D の 2

つのゾーンが定義されています。 VSAN 境界を越えるゾーンはありません。 VSAN 2 に定義されたゾーン A は、VSAN 7 に定義されたゾーン A とは別個のものです。

図 *29* : ***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）、および独立 VSAN（VSAN 4094）で VSAN を識別します。
- ステート：VSAN の管理ステートを active（デフォルト）または suspended ステートに設定できます。 VSAN が作成されると、VSAN はさまざまな状態またはステートに置かれます。
  - VSAN の active ステートは、VSAN が設定されイネーブルであることを示します。 VSAN をイネーブルにすることによって、VSAN のサービスをアクティブにします。
  - VSAN の suspended ステートは、VSAN が設定されているがイネーブルではないことを示します。 この VSAN にポートが設定されている場合、ポートはディセーブルの状態です。 このステートを使用して、VSAN の設定を失うことなく VSAN を非アクティブにします。 suspended ステートの VSAN のすべてのポートは、ディセーブルの状態です。 VSAN を suspended ステートにすることによって、ファブリック全体のすべての VSAN パラメータを事前設定し、VSAN をただちにアクティブにできます。

- VSAN 名：このテキスト ストリングは、管理目的で VSAN を識別します。 名前は、1 ～ 32 文字で指定できます。また、すべての VSAN で一意である必要があります。 デフォルトでは、VSAN 名は VSAN と VSAN ID を表す 4 桁のストリングを連結したものです。 たとえば、VSAN 3 のデフォルト名は VSAN0003 です。

（注） VSAN 名は一意である必要があります。

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

VSAN の作成について

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

VSAN の静的な作成

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

VASN を作成するには、次の作業を行います。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **vsan database**	VSAN に対するデータベースを設定します。 アプリケーション特有の VSAN パラメータは、このプロンプトから設定できません。
ステップ 3	switch(config-vsan-db)# **vsan** *vsan-id*	VSAN が存在しない場合は、指定された ID で VSAN を作成します。
ステップ 4	switch(config-vsan-db)# **vsan** *vsan-id* **name** *name*	割り当てられた名前で VSAN をアップデートします。
ステップ 5	switch(config-vsan-db)# **vsan** *vsan-id* **suspend**	選択された VSAN を中断します。
ステップ 6	switch(config-vsan-db)# **no vsan** *vsan-id* **suspend**	前のステップで入力した **suspend** コマンドを無効にします。
ステップ 7	switch(config-vsan-db)# **end**	EXEC モードに戻ります。

ポート VSAN メンバーシップの概要

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

- スタティック：ポートに VSAN を割り当てます。
- ダイナミック：デバイス WWN に基づいて VSAN を割り当てます。 この方法は Dynamic Port VSAN Membership（DPVM）機能といいます。 Cisco Nexus 5000 スイッチは DPVM をサポートしません。

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

関連トピック

スタティック ポート VSAN メンバーシップの概要, （132 ページ）
VSAN トランキングの設定, （93 ページ）

スタティック ポート VSAN メンバーシップの概要

インターフェイス ポートの VSAN メンバーシップをスタティックに割り当てるには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **vsan database**
3. switch(config-vsan-db)# **vsan** *vsan-id*
4. switch(config-vsan-db)# **vsan** *vsan-id* **interface** {*fc slot*/*port* | **vfc** *vfc-id*}
5. switch(config-vsan-db)# **vsan** *vsan-id* {*fc slot*/*port* | **vfc** *vfc-id*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **vsan database**	VSAN に対するデータベースを設定します。
ステップ 3	switch(config-vsan-db)# **vsan** *vsan-id*	VSAN が存在しない場合は、指定された ID で VSAN を作成します。
ステップ 4	switch(config-vsan-db)# **vsan** *vsan-id* **interface** {*fc slot*/*port* | **vfc** *vfc-id*}	指定されたインターフェイスのメンバーシップを VSAN に割り当てます。
ステップ 5	switch(config-vsan-db)# **vsan** *vsan-id* {*fc slot*/*port* | **vfc** *vfc-id*}	変更された VSAN を反映させるために、インターフェイスのメンバーシップ情報を更新します。 （注） FC または vFC インターフェイスの VSAN メンバーシップを削除するには、別の VSAN にそのインターフェイスの VSAN メンバーシップを割り当てます。 VSAN 1 に割り当てることを推奨します。

VSAN スタティック メンバーシップの表示

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

次に、指定された VSAN のメンバーシップ情報を表示する例を示します。

```
switch # show vsan 1 membership
vsan 1 interfaces:
        fc2/1   fc2/2   fc2/3   fc2/4

        san-port-channel 3  vfc1/1
```

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

次に、すべての VSAN のメンバーシップ情報を表示する例を示します。

```
switch # show vsan membership
vsan 1 interfaces:
        fc2/1   fc2/2   fc2/3   fc2/4

        san-port-channel 3  vfc3/1
vsan 2 interfaces:
        fc2/3 vfc4/1
vsan 7 interfaces:
vsan 100 interfaces:
vsan 4094(isolated vsan) interfaces:
```

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

```
switch # show vsan membership interface fc2/1
fc2/1
        vsan:1
        allowed list:1-4093
```

デフォルト VSAN の概要

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

（注） VSAN 1 は削除できませんが、中断できます。

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

分離された VSAN の概要

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

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

注意 独立 VSAN を使用してポートを設定しないでください。

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

分離された VSAN メンバーシップの概要

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

VSAN の動作ステート

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

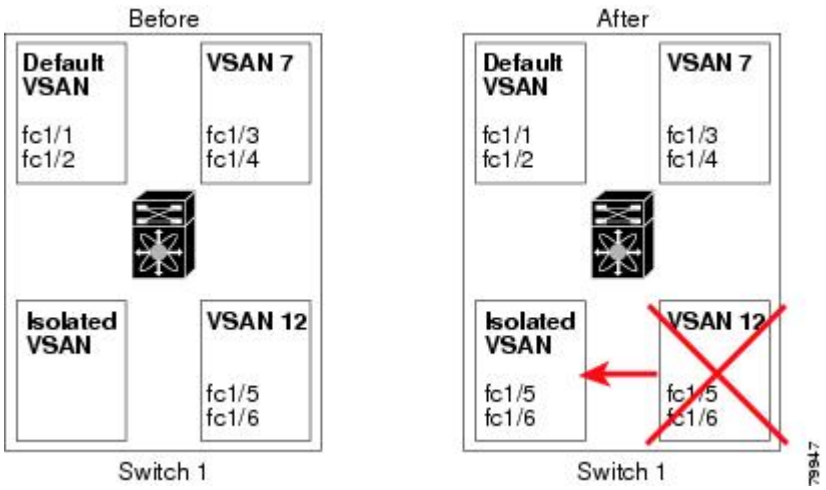
スタティック VSAN の削除の概要

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 メンバーシップの詳細は、VSAN マネージャによって保持されます。 コンフィギュレーションから VSAN を削除すると、この機能が影響を受けます。 VSAN が削除されると、VSAN 内のすべてのポートが非アクティブになり、ポートが独立 VSAN に移動されます。 同一の VSAN が再作成されると、ポートはその VSAN に自動的に割り当て

られることはありません。ポートVSANメンバーシップを明示的に再設定する必要があります（次の図を参照してください）。

図 *30*： ***VSAN*** ポート メンバーシップの詳細



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

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

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

関連トピック

VSAN トランキングの設定，（93 ページ）

スタティック VSAN の削除

VSAN および各種の属性を削除するには、次の作業を行います。

手順の概要

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

手順の詳細

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

ロード バランシングの概要

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

ロード バランシングの設定

既存の VSAN でロード バランシングを設定するには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **vsan database**
3. switch(config-vsan-db)# **vsan** *vsan-id*
4. switch(config-vsan-db)# **vsan** *vsan-id* **loadbalancing src-dst-id**
5. switch(config-vsan-db)# **no vsan** *vsan-id* **loadbalancing src-dst-id**
6. switch(config-vsan-db)# **vsan** *vsan-id* **loadbalancing src-dst-ox-id**
7. switch(config-vsan-db)# **vsan** *vsan-id* **suspend**
8. switch(config-vsan-db)# **no vsan** *vsan-id* **suspend**
9. switch(config-vsan-db)# **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **vsan database**	VSAN データベース コンフィギュレーション サブモードを開始します。
ステップ 3	switch(config-vsan-db)# **vsan** *vsan-id*	既存の VSAN を指定します。
ステップ 4	switch(config-vsan-db)# **vsan** *vsan-id* **loadbalancing src-dst-id**	選択された VSAN に対してロード バランシングの保証をイネーブルにし、スイッチがパス選択プロセスで送信元/宛先 ID を使用するようにします。
ステップ 5	switch(config-vsan-db)# **no vsan** *vsan-id* **loadbalancing src-dst-id**	前のステップで入力したコマンドを無効にし、ロード バランシング パラメータのデフォルト値に戻します。
ステップ 6	switch(config-vsan-db)# **vsan** *vsan-id* **loadbalancing src-dst-ox-id**	送信元 ID、宛先 ID、OX ID（デフォルト）を使用するようにパス選択設定を変更します。
ステップ 7	switch(config-vsan-db)# **vsan** *vsan-id* **suspend**	選択された VSAN を中断します。
ステップ 8	switch(config-vsan-db)# **no vsan** *vsan-id* **suspend**	前のステップで入力した **suspend** コマンドを無効にします。
ステップ 9	switch(config-vsan-db)# **end**	EXEC モードに戻ります。

Interop モードの概要

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

関連トピック

スイッチの相互運用性, （235 ページ）

スタティック VSAN 設定の表示

次に、特定の VSAN に関する情報を表示する例を示します。

```
switch# show vsan 100
```

次に、VSAN 使用状況を表示する例を示します。

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

次に、すべての VSAN を表示する例を示します。

```
switch# show vsan
```

デフォルトの VSAN 設定

次の表に、設定されたすべての VSAN のデフォルト設定を示します。

表 *18*：デフォルト *VSAN* パラメータ

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

第 10 章

ゾーンの設定と管理

この章の内容は、次のとおりです。

- ゾーンの設定と管理，141 ページ

ゾーンの設定と管理

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

FC-GS-4 および FC-SW-3 規格で指定されている高度なゾーン分割機能がサポートされます。 既存の基本ゾーン分割機能または規格に準拠した高度なゾーン分割機能のどちらも使用できます。

ゾーン分割に関する情報

ゾーン分割の特徴

ゾーン分割には、次の特徴があります。

- 1 つのゾーンは、複数のゾーン メンバーから構成されます。
  - ゾーンのメンバ同士はアクセスできますが、異なるゾーンのメンバ同士はアクセスできません。
  - ゾーン分割がアクティブでない場合、すべてのデバイスがデフォルト ゾーンのメンバとなります。
  - ゾーン分割がアクティブの場合、アクティブ ゾーン（アクティブ ゾーン セットに含まれるゾーン）にないデバイスがデフォルト ゾーンのメンバとなります。
  - ゾーンのサイズを変更できます。

- デバイスは複数のゾーンに所属できます。
- 物理ファブリックでは、最大 16,000 メンバを収容できます。 これには、ファブリック内のすべての VSAN が含まれます。

- ゾーン セットは、1 つまたは複数のゾーンで構成されます。
  - ゾーンセットは、単一エンティティとしてファブリックのすべてのスイッチでアクティブまたは非アクティブにできます。
  - アクティブにできるのは、常に 1 つのゾーン セットだけです。
  - 1 つのゾーンを複数のゾーン セットのメンバにできます。
  - ゾーン スイッチあたりの最大ゾーン セット数は 500 です。

- ゾーン分割は、ファブリックの任意のスイッチから管理できます。
  - 任意のスイッチからゾーンをアクティブにした場合、ファブリックのすべてのスイッチがアクティブ ゾーン セットを受信します。 また、ファブリック内のすべてのスイッチにフル ゾーン セットが配布されます（この機能が送信元スイッチでイネーブルである場合）。
  - 既存のファブリックに新しいスイッチが追加されると、新しいスイッチによってゾーンセットが取得されます。

- ゾーンの変更を中断せずに設定できます。
  - 影響を受けないポートまたはデバイスのトラフィックを中断させることなく、新しいゾーンおよびゾーン セットをアクティブにできます。

- ゾーン メンバーシップは、次の識別情報を使用して指定できます。
  - Port World Wide Name（pWWN）：スイッチに接続された N ポートの pWWN をゾーンのメンバーとして指定します。
  - ファブリック pWWN：ファブリック ポートの WWN（スイッチ ポートの WWN）を指定します。 このメンバーシップは、ポートベース ゾーン分割とも呼ばれます。
  - FC ID：スイッチに接続された N ポートの FC ID をゾーンのメンバーとして指定します。
  - インターフェイスおよびSwitch WWN（sWWN）：sWWNによって識別されたスイッチのインターフェイスを指定します。 このメンバーシップは、インターフェイス ゾーン分割とも呼ばれます。
  - インターフェイスおよびドメイン ID：ドメイン ID によって識別されたスイッチのインターフェイスを指定します。
  - ドメイン ID およびポート番号：シスコ スイッチ ドメインのドメイン ID を指定し、さらに他社製スイッチに所属するポートを指定します。

（注） 仮想ファイバ チャネル インターフェイスのスイッチに接続された N ポートでは、N ポートの pWWN、N ポートの FC ID、または仮想ファイバ チャネル インターフェイスのファブリック pWWN を使用して、ゾーン メンバーシップを指定できます。

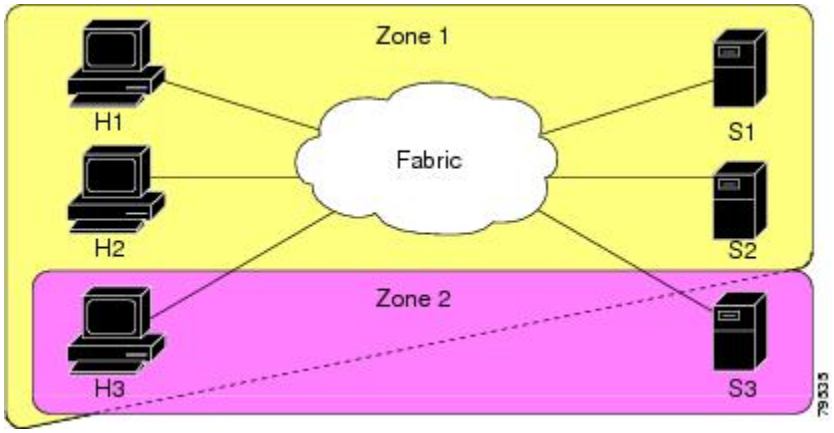
- デフォルト ゾーン メンバーシップには、特定のメンバーシップとの関係を持たないすべてのポートまたは WWN が含まれます。 デフォルト ゾーン メンバー間のアクセスは、デフォルト ゾーン ポリシーによって制御されます。
- VSAN あたり最大 8000 ゾーン、スイッチ上の全 VSAN で最大 8000 ゾーンを設定できます。

（注） インターフェイスベース ゾーン分割は、Cisco SAN スイッチだけで機能します。 インターフェイスベース ゾーン分割は、interop モードで設定された VSAN では機能しません。

ゾーン分割の例

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

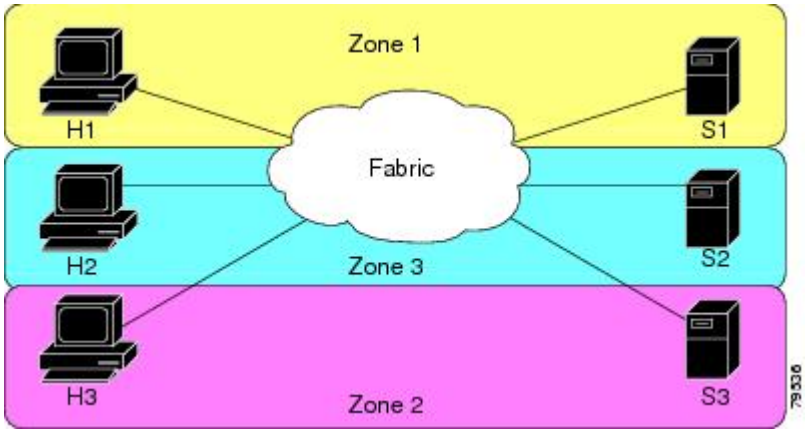
図 *31*： *2* つのゾーンによるファブリック



ほかの方法を使用して、このファブリックを複数のゾーンに分割することもできます。 次の図は、別の方法を示します。 新しいソフトウェアをテストするために、ストレージ システム S2 を分離する必要があると想定します。 これを実行するために、ホスト H2 とストレージ S2 だけを含

むゾーン 3 が設定されます。 ゾーン 3 ではアクセスを H2 と S2 だけに限定し、ゾーン 1 ではアクセスを H1 と S1 だけに限定できます。

図 *32*：*3* つのゾーンによるファブリック



ゾーン実装

Cisco SAN スイッチは、自動的に次の基本的なゾーン機能をサポートします（設定を追加する必要はありません）。

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

必要に応じて、さらに次のゾーン機能を設定できます。

- VSAN 単位ですべてのスイッチにフル ゾーン セットを伝播します。
- ゾーン分割されていないメンバのデフォルト ポリシーを変更します。

- VSAN を interop モードに設定することによって、他のベンダーと相互運用できます。 相互に干渉することなく、同じスイッチ内で 1 つの VSAN を interop モードに、別の VSAN を基本モードに設定することもできます。
- E ポートを分離状態から復旧します。

アクティブおよびフル ゾーン セットの設定時の注意事項

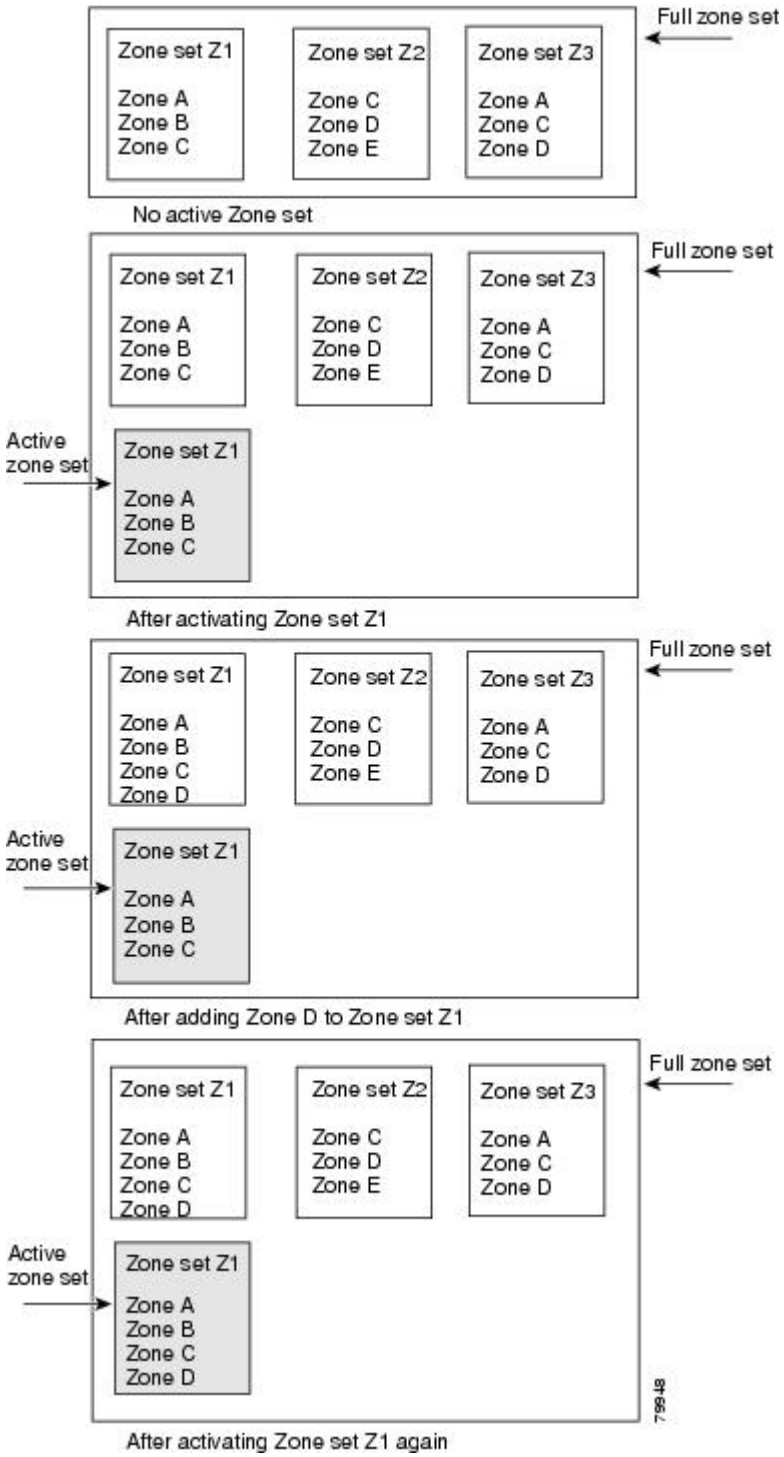
ゾーン セットを設定する前に、次の注意事項について検討してください。

- 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っても、フル ゾーン セットを変更できます。 ただし、加えられた変更が有効になるのは、再アクティブ化したときです。
- アクティブ化が実行されると、永続的なコンフィギュレーションにアクティブ ゾーン セットが自動保存されます。 これにより、スイッチのリセットにおいてもスイッチはアクティブ ゾーン セット情報を維持できます。
- ファブリックのその他すべてのスイッチは、アクティブ ゾーン セットを受信するので、それぞれのスイッチでゾーン分割を実行できます。
- ハードおよびソフト ゾーン分割は、アクティブ ゾーン セットを使用して実装されます。 変更は、ゾーン セットのアクティブ化によって有効になります。
- アクティブ ゾーン セットに含まれない FC ID または Nx ポートは、デフォルト ゾーンに所属します。デフォルト ゾーン情報は、他のスイッチに配信されません。

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

次の図は、アクティブなゾーン セットに追加されるゾーンを示します。

図 *33*：アクティブおよびフル ゾーン セット



ゾーンの設定

ゾーンを設定し、ゾーン名を割り当てるには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **zone name** *zone-name* **vsan** *vsan-id*
3. switch(config-zone)# **member** *type value*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **zone name** *zone-name* **vsan** *vsan-id*	指定された VSAN にゾーンを設定します。 （注） すべての英数字か、または記号（$、-、^、_）のうち 1 つがサポートされます。
ステップ 3	switch(config-zone)# **member** *type value*	指定されたタイプ（pWWN、ファブリック pWWN、FC ID、FC エイリアス、ドメイン ID、またはインターフェイス）および値に基づいて、指定されたゾーンにメンバを設定します。 **注意** 同じファブリック内に FabricWare を実行する Cisco MDS 9020 スイッチがある場合には、Cisco NX-OS を実行するすべての SAN スイッチには、pWWN タイプのゾーン分割だけを設定する必要があります。 **ヒント** 該当する表示コマンド（たとえば、**show interface** または **show flogi database**）を使用して、必要な値を 16 進表記で取得します。

ゾーンの設定例

表 *19*：*member* コマンドのタイプおよび値の構文

ドメイン ID	**member domain-id** *domain-id* **portnumber** *number*
FC エイリアス	**member fcalias** *fc-alias-name*
FC ID	**member fcid** *fcid*
ファブリック pWWN	**member fwwn** *fwwn-id*

ローカル sWWN インターフェイス	**member interface** *type slot*/*port*
ドメイン ID インターフェイス	**member interface** *type slot*/*port* **domain-id** *domain-id*
リモート sWWN インターフェイス	**member interface** *type slot*/*port* **swwn** *swwn-id*
pWWN	**member pwwn** *pwwn-id*

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

次の例では、ゾーン メンバを設定します。

```
switch(config)# zone name MyZone vsan 2
```

pWWN の例：

```
switch(config-zone)# member pwwn 10:00:00:23:45:67:89:ab
```

ファブリック pWWN の例：

```
switch(config-zone)# member fwwn 10:01:10:01:10:ab:cd:ef
```

FC ID の例：

```
switch(config-zone)# member fcid 0xce00d1
```

FC エイリアスの例：

```
switch(config-zone)# member fcalias Payroll
```

ドメイン ID の例：

```
switch(config-zone)# member domain-id 2 portnumber 23
```

ローカル sWWN インターフェイスの例：

```
switch(config-zone)# member interface fc 2/1
```

リモート sWWN インターフェイスの例：

```
switch(config-zone)# member interface fc 2/1 swwn 20:00:00:05:30:00:4a:de
```

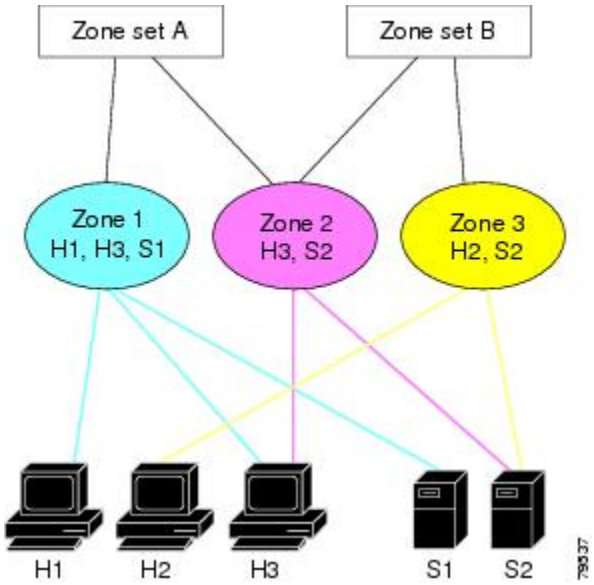
ドメイン ID インターフェイスの例：

```
switch(config-zone)# member interface fc 2/1 domain-id 25
```

ゾーン セット

次の図では、それぞれ独自のメンバーシップ階層とゾーン メンバを持つセットが 2 つ作成されます。

図 *34*：ゾーン セット、ゾーン、ゾーン メンバの階層



ゾーンは、アクセス コントロールを指定するための方式を提供します。ゾーンセットは、ファブリックでアクセス コントロールを実行するためのゾーンの分類です。ゾーン セット A またはゾーン セット B のいずれか（両方でなく）をアクティブにできます。

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

ゾーン セットのアクティブ化

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

既存のゾーン セットをアクティブまたは非アクティブにするには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **zoneset activate name** *zoneset-name* **vsan** *vsan-id*
3. switch(config)# **no zoneset activate name** *zoneset-name* **vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **zoneset activate name** *zoneset-name* **vsan** *vsan-id*	指定されたゾーン セットをアクティブにします。
ステップ 3	switch(config)# **no zoneset activate name** *zoneset-name* **vsan** *vsan-id*	指定されたゾーン セットを非アクティブにします。

デフォルト ゾーンの概要

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

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

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

（注） スイッチが初めて初期化されたとき、ゾーンは設定されておらず、すべてのメンバがデフォルトゾーンに所属するものと見なされます。 メンバは、相互に通信する許可を受けていません。

ファブリックの各スイッチにデフォルト ゾーン ポリシーを設定します。 ファブリックの 1 つのスイッチでデフォルトゾーン ポリシーを変更する場合、必ずファブリックの他のすべてのスイッチでも変更してください。

（注） デフォルト ゾーン設定のデフォルト設定値は変更できます。

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

デフォルト ゾーンのアクセス権限の設定

デフォルト ゾーン内のメンバに対してトラフィックを許可または拒否するには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **zone default-zone permit vsan** *vsan-id*
3. switch(config)# **no zone default-zone permit vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **zone default-zone permit vsan** *vsan-id*	デフォルト ゾーン メンバへのトラフィック フローを許可します。
ステップ 3	switch(config)# **no zone default-zone permit vsan** *vsan-id*	デフォルト ゾーン メンバへのトラフィック フローを拒否（デフォルト）します。

FC エイリアスの作成の概要

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

- pWWN：N ポートの 16 進表記の WWN（10:00:00:23:45:67:89:ab など）
- fWWN：ファブリック ポート名の WWN は 16 進形式です（10:00:00:23:45:67:89:ab など）。
- FC ID：0xhhhhhh 形式の N ポート ID（0xce00d1 など）
- ドメイン ID：ドメイン ID は 1 ～ 239 の整数です。 このメンバーシップ設定を完了するには、他社製スイッチの必須ポート番号が必要です。
- インターフェイス：インターフェイスベース ゾーン分割は、スイッチ インターフェイスがゾーンを設定するのに使用される点でポートベース ゾーン分割と似ています。 スイッチ インターフェイスをローカル スイッチとリモート スイッチの両方でゾーン メンバとして指定できます。 リモート スイッチを指定するには、特定の VSAN 内のリモート Switch WWN（sWWN）またはドメイン ID を入力します。

ヒント　スイッチは、VSAN あたり最大 2048 のエイリアスをサポートします。

FC エイリアスの作成

エイリアスを作成するには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcalias name** *alias-name***vsan** *vsan-id*
3. switch(config-fcalias)# **member** *type value*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcalias name** *alias-name***vsan** *vsan-id*	エイリアス名を設定します。 エイリアス名には最大 64 文字の英数字文字列を指定します。大文字と小文字は区別されます。
ステップ 3	switch(config-fcalias)# **member** *type value*	指定されたタイプ（pWWN、ファブリック pWWN、FC ID、ドメイン ID、またはインターフェイス）および値に基づいて、指定された FC エイリアスにメンバを設定します。 （注） 複数のメンバを複数の行で指定できます。

FC エイリアスの作成例

表 *20* : ***member*** コマンドのタイプおよび値の構文

デバイス エイリアス	**member device-alias** *device-alias*
ドメイン ID	**member domain-id** *domain-id* **portnumber** *number*
FC ID	**member fcid** *fcid*
ファブリック pWWN	**member fwwn** *fwwn-id*
ローカル sWWN インターフェイス	**member interface** *type slot*/*port*
ドメイン ID インターフェイス	**member interface** *type slot*/*port* **domain-id** domain-id
リモート sWWN インターフェイス	**member interface** *type slot*/*port* **swwn** *swwn-id*

pWWN	**member pwwn** *pwwn-id*

次に、異なるタイプのメンバ エイリアスを設定する例を示します。

```
switch(config)# fcalias name AliasSample vsan 3
```
pWWN の例：
```
switch(config-fcalias)# member pwwn 10:00:00:23:45:67:89:ab
```
fWWN の例：
```
switch(config-fcalias)# member fwwn 10:01:10:01:10:ab:cd:ef
```
FC ID の例：
```
switch(config-fcalias)# member fcid 0x222222
```
ドメイン ID の例：
```
switch(config-fcalias)# member domain-id 2 portnumber 23
```
ローカル sWWN インターフェイスの例：
```
switch(config-fcalias)# member interface fc 2/1
```
リモート sWWN インターフェイスの例：
```
switch(config-fcalias)# member interface fc 2/1 swwn 20:00:00:05:30:00:4a:de
```
ドメイン ID インターフェイスの例：
```
switch(config-fcalias)# member interface fc2/1 domain-id 25
```
デバイス エイリアスの例：
```
switch(config-fcalias)# member device-alias devName
```

ゾーン セットの作成とメンバ ゾーンの追加

複数のゾーンを含むゾーン セットを作成するには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **zone set name** *zoneset-name* **vsan** *vsan-id*
3. switch(config-zoneset)# **member** *name*
4. switch(config-zoneset)# **zone name** *zone-name*
5. switch(config-zoneset-zone)# **member fcid** *fcid*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **zone set name** *zoneset-name* **vsan** *vsan-id*	設定したゾーン セット名でゾーン セットを設定します。 ヒント　ゾーンセットをアクティブにするには、まずゾーンとゾーン セットを 1 つ作成する必要があります。

	コマンドまたはアクション	目的
ステップ 3	switch(config-zoneset)# **member** *name*	以前指定したゾーンセットのメンバとしてゾーンを追加します。 ヒント　指定されたゾーン名が事前に設定されていない場合、このコマンドを実行すると「zone not present」エラーメッセージが返されます。
ステップ 4	switch(config-zoneset)# **zone name** *zone-name*	指定されたゾーン セットにゾーンを追加します。 ヒント　ゾーン セット プロンプトからゾーンを作成する必要がある場合は、このステップを実行します。
ステップ 5	switch(config-zoneset-zone)# **member fcid** *fcid*	新しいゾーンに新しいメンバを追加します。 ヒント　ゾーン セット プロンプトからゾーンにメンバを追加する必要がある場合は、このステップを実行します。

ヒント　アクティブ ゾーン セットを保存するために、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーする必要はありません。 ただし、明示的にフル ゾーン セットを保存するには、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーする必要があります。

ゾーンの実行

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

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

ハード ゾーン分割は、N ポートから送信される各フレームでハードウェアによって実行されます。 スイッチにフレームが着信した時点で、送信元/宛先 ID と許可済みの組み合わせが照合されるため、ワイヤスピードでフレームを送信できます。ハードゾーン分割は、ゾーン分割のすべての形式に適用されます。

（注）　ハード ゾーン分割は、すべてのフレームでゾーン分割制限を実行し、不正なアクセスを防ぎます。

Cisco SAN のスイッチは、ハードとソフトの両方のゾーン分割をサポートします。

ゾーン セット配信

フル ゾーン セットは、EXEC モード レベルで **zoneset distribute vsan** コマンドを使用する一時配信、またはコンフィギュレーション モード レベルで **zoneset distribute full vsan** コマンドを使用するフル ゾーン セット配信のどちらかの方式を使用して配信できます。 次の表に、これらの方式の相違点を示します。

表 *21*：ゾーン セット配信の相違

一時配信 **zoneset distribute vsan** コマンド（**EXEC** モード）	フル ゾーン セット配信 **zoneset distribute full vsan** コマンド（コンフィギュレーション モード）
フル ゾーン セットはすぐに配信されます。	フルゾーンセットはすぐには配信されません。
アクティブ化、非アクティブ化、または結合時には、アクティブ ゾーン セットと同時にフル ゾーン セット情報を伝播しません。	アクティブ化、非アクティブ化、または結合時には、アクティブ ゾーン セットと同時にフル ゾーン セット情報を伝播します。

フル ゾーン セット配信のイネーブル化

Cisco SAN のすべてのスイッチは、新しい E ポート リンクが立ち上がったとき、または新しいゾーン セットが VSAN でアクティブにされたときに、アクティブ ゾーン セットを配信します。 ゾーンセットの配信は、隣接スイッチへのマージ要求の送信時、またはゾーンセットのアクティブ化の際に行われます。

VSAN 単位で、VSAN 上のすべてのスイッチへのフル ゾーンセットおよびアクティブ ゾーンセットの配信をイネーブルにするには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **zoneset distribute full vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ **1**	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ **2**	switch(config)# **zoneset distribute full vsan** *vsan-id*	アクティブ ゾーン セットとともにフル ゾーン セットの送信をイネーブルにします。

ワンタイム配信のイネーブル化

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

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

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

このコマンドではフル ゾーンセット情報の配信だけを実行し、スタートアップ コンフィギュレーションへの情報の保存は行いません。 フル ゾーンセット情報をスタートアップ コンフィギュレーションに保存する場合は、**copy running-config start-config** コマンドを明示的に入力する必要があります。

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

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

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

    session:none
    hard-zoning:enabled
Default zone:
    qos:none broadcast:disabled ronly:disabled
Full Zoning Database :
    Zonesets:0  Zones:0 Aliases: 0
Active Zoning Database :
    Name: nozoneset  Zonesets:1  Zones:2
Status: Zoneset distribution completed at 04:01:06 Aug 28 2010
```

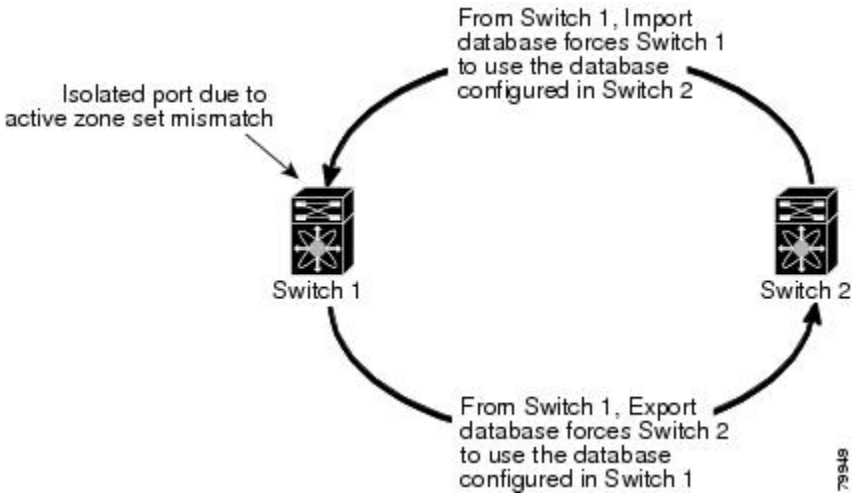
リンクの分離からの回復の概要

ファブリックの 2 つのスイッチが TE ポートまたは E ポートを使用して結合される場合、アクティブ ゾーン セットのデータベースが 2 つのスイッチまたはファブリック間で異なると、この TE ポートおよび E ポートが分離することがあります。 TE ポートまたは E ポートが分離した場合、次の 3 つのオプションのいずれかを使用して分離状態からポートを回復できます。

- 近隣スイッチのアクティブ ゾーン セット データベースをインポートし、現在のアクティブ ゾーン セットと交換します（次の図を参照してください）。
- 現在のデータベースを隣接のスイッチにエクスポートします。

- フル ゾーン セットを編集し、修正されたゾーン セットをアクティブにしてから、リンクを立ち上げることにより、手動で矛盾を解決します。

図 *35*：データベースのインポートとエクスポート



ゾーン セットのインポートおよびエクスポート

ゾーン セット情報を隣接スイッチにエクスポート、または隣接スイッチからインポートするには、次の作業を行います。

手順の概要

1. switch# **zoneset import interface fc** *slot*/*port* **vsan** *vsan-id*
2. switch# **zoneset export vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **zoneset import interface fc** *slot*/*port* **vsan** *vsan-id*	VSAN または VSAN の範囲に指定されたインターフェイスを介して接続された隣接スイッチからゾーン セットをインポートします。
ステップ 2	switch# **zoneset export vsan** *vsan-id*	指定された VSAN または VSAN の範囲を介して接続された隣接スイッチにゾーン セットをエクスポートします。

ゾーン セット配信

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

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

アクティブ ゾーン セットは、フル ゾーン セットに含まれません。 フル ゾーン セットが失われた場合または伝播されなかった場合に、既存のゾーン セットに変更を加えても、アクティブにできません。

注意 同一名のゾーンがフル ゾーン データベースにすでに存在する場合、アクティブ ゾーン セットをフル ゾーン セットにコピーすると、その同一名のゾーンが上書きされることがあります。

ゾーン セットのコピー

Cisco SAN スイッチでは、アクティブ ゾーン セットは編集できません。 ただし、アクティブ ゾーン セットをコピーして、編集可能な新しいゾーン セットを作成できます。

ゾーン セットのコピーを作成するには、次の作業を行います。

手順の概要

1. switch# **zone copy active-zoneset full-zoneset vsan** *vsan-id*
2. switch# **zone copy vsan** *vsan-id* **active-zoneset scp://guest@myserver/tmp/active_zoneset.txt**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **zone copy active-zoneset full-zoneset vsan** *vsan-id*	指定された VSAN のアクティブ ゾーン セットのコピーをフル ゾーン セットに作成します。
ステップ 2	switch# **zone copy vsan** *vsan-id* **active-zoneset scp://guest@myserver/tmp/active_zoneset.txt**	SCP を使用して、指定された VSAN のアクティブ ゾーンをリモート ロケーションにコピーします。

ゾーン、ゾーン セット、およびエイリアスの名前の変更

ゾーン、ゾーン セット、FC エイリアス、またはゾーン属性グループの名前を変更するには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **zoneset rename** oldname newname **vsan** *vsan-id*
3. switch(config)# **zone rename** oldname newname **vsan** *vsan-id*
4. switch(config)# **fcalias rename** oldname newname **vsan** *vsan-id*
5. switch(config)# **zone-attribute-group rename** oldname newname **vsan** *vsan-id*
6. switch(config)# **zoneset activate name** newname **vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **zoneset rename** oldname newname **vsan** *vsan-id*	指定された VSAN のゾーン セット名を変更します。
ステップ 3	switch(config)# **zone rename** oldname newname **vsan** *vsan-id*	指定された VSAN のゾーン名を変更します。
ステップ 4	switch(config)# **fcalias rename** oldname newname **vsan** *vsan-id*	指定された VSAN の fcalias 名を変更します。
ステップ 5	switch(config)# **zone-attribute-group rename** oldname newname **vsan** *vsan-id*	指定された VSAN のゾーン属性グループ名を変更します。
ステップ 6	switch(config)# **zoneset activate name** newname **vsan** *vsan-id*	ゾーン セットをアクティブにし、アクティブ ゾーン セット内の新しいゾーン名に更新します。

ゾーン、ゾーン セット、FC エイリアス、およびゾーン属性グループのコピー

ゾーン、ゾーン セット、FC エイリアス、またはゾーン属性グループをコピーするには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **zoneset clone** *oldname newname* **vsan** *vsan-id*
3. switch(config)# **zone clone** *oldname newname* **vsan** *number*
4. switch(config)# **fcalias clone** *oldname newname* **vsan** *vsan-id*
5. switch(config)# **zone-attribute-group clone** *oldname newname* **vsan** *vsan-id*
6. switch(config)# **zoneset activate name** *newname* **vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **zoneset clone** *oldname newname* **vsan** *vsan-id*	指定された VSAN のゾーン セットをコピーします。
ステップ 3	switch(config)# **zone clone** *oldname newname* **vsan** *number*	指定された VSAN 内のゾーンをコピーします。
ステップ 4	switch(config)# **fcalias clone** *oldname newname* **vsan** *vsan-id*	指定された VSAN の FC エイリアス名をコピーします。
ステップ 5	switch(config)# **zone-attribute-group clone** *oldname newname* **vsan** *vsan-id*	指定された VSAN のゾーン属性グループをコピーします。
ステップ 6	switch(config)# **zoneset activate name** *newname* **vsan** *vsan-id*	ゾーンセットをアクティブにし、アクティブ ゾーン セット内の新しいゾーン名に更新します。

ゾーン サーバ データベースのクリア

指定された VSAN のゾーン サーバ データベース内のすべての設定情報をクリアできます。

ゾーン サーバ データベースをクリアするには、次のコマンドを使用します。

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

（注） **clear zone database** コマンドを入力したあとに、明示的に **copy running-config startup-config** を入力して、次にスイッチを起動するときに確実に実行コンフィギュレーションが使用されるようにする必要があります。

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

ゾーン情報の確認

ゾーン情報を表示するには、**show** コマンドを使用します。 特定のオブジェクトの情報（たとえば、特定のゾーン、ゾーン セット、VSAN、エイリアス、または brief や active などのキーワード）を要求する場合、指定されたオブジェクトの情報だけが表示されます。

次に、すべての VSAN のゾーン情報を表示する例を示します。

```
switch# show zone
```

次に、特定の VSAN のゾーン情報を表示する例を示します。

```
switch# show zone vsan 1
```

次に、VSAN 範囲に設定されたゾーン セットを表示する例を示します。

```
switch# show zoneset vsan 2-3
```

次に、特定のゾーンのメンバを表示する例を示します。

```
switch# show zone name Zone1
```

次に、FC エイリアス設定を表示する例を示します。

```
switch# show fcalias vsan 1
```

次に、メンバが属しているすべてのゾーンを表示する例を示します。

```
switch# show zone member pwwn 21:00:00:20:37:9c:48:e5
```

次に、他のスイッチと交換される制御フレームの数を表示する例を示します。

```
switch# show zone statistics
```

次に、アクティブ ゾーン セットを表示する例を示します。

```
switch# show zoneset active
```

次に、アクティブ ゾーンを表示する例を示します。

```
switch# show zone active
```

次に、ゾーン ステータスを表示する例を示します。

```
switch# show zone status
```

拡張ゾーン分割

ゾーン分割機能は、FC-GS-4 および FC-SW-3 規格に準拠しています。 どちらの規格も、前の項で説明した基本ゾーン分割機能と、この項で説明する拡張ゾーン分割機能をサポートしています。

拡張ゾーン分割の概要

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

表 *22*：拡張ゾーン分割の利点

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

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 タイプ（シンボリック ノード名およびその他のタイプ）は他社製スイッチによって使用されることがあります。 結合時に、シスコ固有のタイプは他社製スイッチによって誤って解釈されることがあります。	メンバ タイプを一意に識別するために、ベンダー固有のタイプ値とベンダー ID が提供されます。	ベンダー タイプが一意です。
fWWN ベースのゾーン メンバーシップは、シスコの interop モードでだけサポートされます。	標準の interop モード（interop モード 1）で fWWN ベースのメンバーシップがサポートされます。	fWWN ベースのメンバ タイプは標準化されています。

基本ゾーン分割から拡張ゾーン分割への変更

基本ゾーン分割モードから拡張ゾーン分割モードに変更するには、次の作業を行います。

手順の概要

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。
2. 1 つ以上のスイッチが拡張モードで動作できない場合、拡張モードへ変更できません。
3. 動作モードを拡張ゾーン分割モードに設定します。

手順の詳細

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。

ステップ 2 1 つ以上のスイッチが拡張モードで動作できない場合、拡張モードへ変更できません。

ステップ 3 動作モードを拡張ゾーン分割モードに設定します。

拡張ゾーン分割から基本ゾーン分割への変更

Cisco SAN スイッチでは、ほかの Cisco NX-OS リリースへのダウングレードおよびアップグレードを可能にするために、拡張ゾーン分割から基本ゾーン分割に変更できます。

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には、次の作業を行います。

手順の概要

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。
2. このような設定が存在する場合は、次に進む前にこれらの設定を削除します。既存の設定を削除しないと、スイッチ ソフトウェアは自動的にこれらの設定を削除します。
3. 動作モードを基本ゾーン分割モードに設定します。

手順の詳細

ステップ 1 アクティブおよびフル ゾーン セットに拡張ゾーン分割モード固有の設定が含まれていないことを確認します。

ステップ 2 このような設定が存在する場合は、次に進む前にこれらの設定を削除します。 既存の設定を削除しないと、スイッチ ソフトウェアは自動的にこれらの設定を削除します。

ステップ 3 動作モードを基本ゾーン分割モードに設定します。

拡張ゾーン分割のイネーブル化

デフォルトでは、拡張ゾーン分割機能はすべての Cisco SAN スイッチでディセーブルです。

VSAN 内で拡張ゾーン分割をイネーブルにするには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **zone mode enhanced vsan** *vsan-id*
3. switch(config)# **no zone mode enhanced vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **zone mode enhanced vsan** *vsan-id*	指定された VSAN で拡張ゾーン分割をイネーブルにします。
ステップ 3	switch(config)# **no zone mode enhanced vsan** *vsan-id*	指定された VSAN で拡張ゾーン分割をディセーブルにします。

ゾーン データベースの変更

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

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

VSAN 内のゾーン分割データベースに対する変更をコミットまたは廃棄するには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **zone commit vsan** *vsan-id*
3. switch(config)# **zone commit vsan** *vsan-id* **force**
4. switch(config)# **no zone commit vsan** *vsan-id*
5. switch(config)# **no zone commit vsan** *vsan-id* **force**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **zone commit vsan** *vsan-id*	拡張ゾーン データベースに変更を適用し、セッションをクローズします。
ステップ 3	switch(config)# **zone commit vsan** *vsan-id* **force**	拡張ゾーン データベースに変更を強制的に適用し、別のユーザが作成したセッションをクローズします。
ステップ 4	switch(config)# **no zone commit vsan** *vsan-id*	拡張ゾーン データベースへの変更を廃棄し、セッションをクローズします。
ステップ 5	switch(config)# **no zone commit vsan** *vsan-id* **force**	拡張ゾーン データベースへの変更を強制的に廃棄し、別のユーザが作成したセッションをクローズします。

ゾーン データベース ロックの解除

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

```
switch# configuration terminal
switch(config)# no zone commit vsan 2
```

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

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

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

データベースのマージ

結合方式は、ファブリック全体の結合制御設定によって異なります。

- 制限：2 つのデータベースが同一でない場合、スイッチ間の ISL は分離されます。
- 許可：2 つのデータベースは、次の表で指定された結合規則を使用して結合されます。

表 *23*：データベースのゾーン結合ステータス

ローカル データベース	隣接データベース	結合ステータス	結合結果
データベースに、同じ名前のゾーン セットが含まれる。拡張ゾーン分割モードでは、interop モード 1 のアクティブ ゾーン セットには名前がありません。 ゾーン セット名が存在するのは、フル ゾーン セットの場合だけです。 ただし、ゾーン、エイリアス、および属性グループは異なります。		成功	ISL は分離されます。
データベースに、名前は 1 で同じだが、異なる番号を持つゾーン、ゾーン エイリアス、またはゾーン属性グループ オブジェクトが含まれる。		失敗	ローカル データベースには隣接データベースの情報が存在します。
データなし	データあり	成功	ローカル データベースおよび隣接データベースが結合されます。

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

結合プロセスは次のように動作します。

- ソフトウェアがプロトコルバージョンを比較します。プロトコルバージョンが異なる場合、ISL は分離されます。
- プロトコル バージョンが同じである場合、ゾーン ポリシーが比較されます。 ゾーン ポリシーが異なる場合、ISL は分離されます。
- ゾーン結合オプションが同じである場合、結合制御設定に基づいて比較が行われます。
  - 設定が「制限」の場合、アクティブ ゾーン セットとフル ゾーン セットが同じになる必要があります。 これらが同じでない場合、リンクは分離されます。
  - 設定が「許可」の場合、結合規則を使用して結合が行われます。

ゾーン マージ制御ポリシーの設定

結合制御ポリシーを設定するには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **zone merge-control restrict vsan** *vsan-id*
3. switch(config)# **no zone merge-control restrict vsan** *vsan-id*
4. switch(config)# **zone commit vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **zone merge-control restrict vsan** *vsan-id*	現在の VSAN の結合制御設定を「制限」に設定します。
ステップ 3	switch(config)# **no zone merge-control restrict vsan** *vsan-id*	現在の VSAN の結合制御設定をデフォルトの「許可」に設定します。

	コマンドまたはアクション	目的
ステップ 4	switch(config)# **zone commit vsan** *vsan-id*	指定された VSAN に対する変更をコミットします。

デフォルトのゾーン ポリシー

デフォルト ゾーン内のトラフィックを許可または拒否するには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **zone default-zone permit vsan** *vsan-id*
3. switch(config)# **no zone default-zone permit vsan** *vsan-id*
4. switch(config)# **zone commit vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **zone default-zone permit vsan** *vsan-id*	デフォルト ゾーン メンバへのトラフィック フローを許可します。
ステップ 3	switch(config)# **no zone default-zone permit vsan** *vsan-id*	デフォルト ゾーン メンバへのトラフィック フローを拒否し、出荷時の設定に戻します。
ステップ 4	switch(config)# **zone commit vsan** *vsan-id*	指定されたVSANに対する変更をコミットします。

システムのデフォルト ゾーン分割設定値の設定

スイッチ上の新しい VSAN のデフォルトのゾーン ポリシーおよびフル ゾーン配信のデフォルト設定値を設定できます。 スイッチ全体のデフォルト設定値を設定するには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **system default zone default-zone permit**
3. switch(config)# **no system default zone default-zone permit**
4. switch(config)# **system default zone distribute full**
5. switch(config)# **no system default zone distribute full**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **system default zone default-zone permit**	スイッチ上の新しい VSAN のデフォルト ゾーン分割ポリシーとして permit（許可）を設定します。
ステップ 3	switch(config)# **no system default zone default-zone permit**	スイッチ上の新しい VSAN のデフォルト ゾーン分割ポリシーとして deny（拒否）（デフォルト）を設定します。
ステップ 4	switch(config)# **system default zone distribute full**	スイッチ上の新しいVSANのデフォルトとして、フルゾーン データベース配信をイネーブルにします。
ステップ 5	switch(config)# **no system default zone distribute full**	スイッチ上の新しいVSANのデフォルトとして、フルゾーンデータベース配信をディセーブル（デフォルト）にします。アクティブ ゾーンデータベースだけが配信されます。

拡張ゾーン情報の確認

次に、指定された VSAN のゾーン ステータスを表示する例を示します。

```
switch# show zone status vsan 2
```

ゾーン データベースの圧縮

過剰なゾーンを削除し、VSAN のゾーン データベースを圧縮できます。

（注） スイッチが VSAN あたり 2000 を超えるゾーンをサポートしていても、ネイバーがサポートしていない場合、結合は失敗します。 また、そのスイッチが VSAN あたり 2000 を超えるゾーンをサポートしていても、ファブリック内のすべてのスイッチが VSAN あたり 2000 を超えるゾーンをサポートしていない場合には、ゾーン セットのアクティブ化に失敗することがあります。

VSAN のゾーンを削除して、ゾーン データベースを圧縮するには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **no zone name** *zone-name* **vsan** *vsan-id*
3. switch(config)# **zone compact vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **no zone name** *zone-name* **vsan** *vsan-id*	ゾーンを削除し、ゾーン数を 2000 以下にします。
ステップ 3	switch(config)# **zone compact vsan** *vsan-id*	指定された VSAN のゾーン データベースを圧縮し、ゾーンが削除されたときに開放されたゾーン ID を回復します。

ゾーンおよびゾーン セットの分析

スイッチ上のゾーンおよびゾーン セットをより的確に管理するために、**show zone analysis** コマンドを使用して、ゾーン情報とゾーン セット情報を表示できます。

次に、フル ゾーン分割の分析を表示する例を示します。

```
switch# show zone analysis vsan 1
```

次に、アクティブ ゾーニングの分析を表示する例を示します。

```
switch# show zone analysis active vsan 1
```

コマンド出力に表示される情報の詳細については、『Cisco Nexus 5000 シリーズ *Switch Command Reference*』を参照してください。

デフォルトの基本ゾーンの設定

次の表に、基本ゾーン パラメータのデフォルト設定を示します。

表 *24*：デフォルトの基本ゾーン パラメータ

パラメータ	デフォルト
デフォルト ゾーン ポリシー	すべてのメンバで拒否
フル ゾーン セット配信	フル ゾーン セットは配信されない

パラメータ	デフォルト
拡張ゾーン分割	ディセーブル

第 11 章

DDAS

この章の内容は、次のとおりです。

- DDAS, 173 ページ

DDAS

Cisco SAN のスイッチは、ファブリック規模単位で配信デバイス エイリアス サービス（デバイス エイリアス）をサポートします。

デバイス エイリアスの概要

Cisco SAN スイッチで（ゾーン分割、DPVM、ポート セキュリティなど）異なる機能を設定するためにデバイスのポート WWN（pWWN）が指定されている必要がある場合、これらの機能の設定を行うたびに適切なデバイス名を割り当てなければなりません。 デバイス名が間違っていると、予期しない結果を引き起こす可能性があります。 pWWN にわかりやすい名前を定義し、必要とされるすべてのコンフィギュレーション コマンドでこの名前を使用すれば、こうした問題を回避できます。 このようなわかりやすい名前をデバイス エイリアスと呼びます。

デバイス エイリアスの機能

デバイス エイリアスには、次のような特徴があります。

- デバイス エイリアス情報は、VSAN 設定とは無関係です。
- デバイス エイリアス設定および配布は、ゾーン サーバおよびゾーン サーバ データベースとは無関係です。
- データを失うことなく、従来のゾーン エイリアス設定をインポートできます。
- デバイス エイリアス アプリケーションは Cisco Fabric Services（CFS）インフラストラクチャを使用して、効率的なデータベースの管理および配布を実現します。 デバイス エイリアスは、協調型配信モードおよびファブリック規模の配信範囲を使用します。

- 基本モードと拡張モード。
- ゾーン、IVR ゾーン、またはポート セキュリティ機能を設定するために使用されたデバイス エイリアスは、それぞれの pWWN と一緒に、**show** コマンド出力に自動的に表示されます。

追加情報については、『*Cisco Nexus 5000 Series System Management Configuration Guide*』の「Using Cisco Fabric Services」を参照してください。

関連トピック

デバイス エイリアスのモード, （176 ページ）

デバイス エイリアスの前提条件

デバイス エイリアスには、次の要件があります。

- デバイス エイリアスを割り当てることができるのは pWWN だけです。
- pWWN とマッピングされるデバイス エイリアスは、1 対 1 の関係である必要があります。
- デバイス エイリアス名には、最大 64 文字の英数字を使用でき、次の文字を 1 つまたは複数加えることができます。
  - a ～ z および A ～ Z
  - デバイス エイリアス名は、先頭の文字が英数字である必要があります（a ～ z または A ～ Z）。
  - 1 ～ 9
  - -（ハイフン）および _（下線）
  - $（ドル記号）および ^（キャレット）記号

ゾーン エイリアスとデバイス エイリアスの比較

次の表で、ゾーン ベースのエイリアス設定とデバイス エイリアス設定の違いを比較します。

表 *25*：ゾーン エイリアスとデバイス エイリアスの比較

ゾーン ベースのエイリアス	デバイス エイリアス
エイリアスは指定した VSAN に限定されます。	VSAN 番号を指定せずにデバイス エイリアスを定義できます。また、同一の定義を何の制約もなく 1 つまたは複数の VSAN で使用できます。
ゾーン エイリアスは、ゾーン分割設定の一部です。他の機能の設定にはエイリアス マッピングを使用できません。	pWWN を使用するすべての機能にデバイス エイリアスを使用できます。

ゾーン ベースのエイリアス	デバイス エイリアス
エンドデバイスを指定するのにすべてのゾーン メンバ タイプを使用できます。	pWWN だけがサポートされます。
設定はゾーン サーバデータベース内に含まれ、他の機能では使用できません。	デバイスエイリアスは、ゾーン分割に限定されていません。 デバイス エイリアス設定を FCNS、ゾーン、fcping、および traceroute アプリケーションで使用することができます。

デバイス エイリアス データベース

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

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

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

デバイス エイリアス データベースの変更は、アプリケーションによって検証されます。 いずれかのアプリケーションがデバイスエイリアスデータベースの変更を受け入れることができない場合、これらの変更は拒否されます。これは、コミットまたは結合の操作によって行われたデバイス エイリアス データベースの変更に適用されます。

デバイス エイリアスの作成

保留データベースにデバイス エイリアスを作成する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **device-alias database**
3. switch(config-device-alias-db)# **device-alias name** *device-name* **pwwn** *pwwn-id*
4. switch(config-device-alias-db)# **no device-alias name** *device-name*
5. switch(config-device-alias-db)# **device-alias rename** *old-device-name new-device-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **device-alias database**	保留データベース コンフィギュレーション サブモードを開始します。
ステップ 3	switch(config-device-alias-db)# **device-alias name** *device-name* **pwwn** *pwwn-id*	pWWN によって識別されるデバイスのデバイス名を指定します。 これが最初に入力されたデバイス エイリアス コンフィギュレーション コマンドであるため、保留データベースへの書き込みを開始し、同時にファブリックをロックします。
ステップ 4	switch(config-device-alias-db)# **no device-alias name** *device-name*	pWWN によって識別されるデバイスのデバイス名を削除します。
ステップ 5	switch(config-device-alias-db)# **device-alias rename** *old-device-name new-device-name*	既存のデバイス エイリアスを新しい名前に変更します。

デバイス エイリアスの作成例

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

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

デバイス エイリアスのモード

エイリアスが基本モードまたは拡張モードで動作するように指定できます。

基本モード（デフォルト モード）で動作する場合、デバイス エイリアスはすぐに pWWN に展開されます。 基本モードで、デバイス エイリアスがたとえば新しい Host Bus Adapter（HBA）を指定するように変更された場合、その変更はゾーン サーバには反映されません。 ユーザは以前の HBA の pWWN を削除して新しい HBA の pWWN を追加し、ゾーンセットを再度アクティブ化する必要があります。

拡張モードで動作する場合、アプリケーションは「ネイティブ」形式でのデバイス エイリアス名を受け入れます。 デバイス エイリアスを pWWN に展開する代わりに、デバイス エイリアス名が設定に保存され、ネイティブ デバイス エイリアス形式で配布されます。 このため、ゾーン サーバ、PSM、または DPVM などのアプリケーションは、自動的にデバイス エイリアス メンバーシップの変更を追跡し、それに応じて変更を実行します。 拡張モードでの動作の主な利点は、変更の実施を 1 カ所で行えるということです。

デバイス エイリアス モードを変更すると、デバイス エイリアスの配布がイネーブルまたはオンの場合にだけ、変更がネットワーク内のほかのスイッチに配布されます。 イネーブルまたはオン以外の場合、モード変更はローカル スイッチでだけ行われます。

（注） 拡張モードまたはネイティブ デバイス エイリアス ベースの設定は、interop モードの VSAN では受け入れられません。 対応するゾーンにネイティブ デバイス エイリアス ベースのメンバがある場合、IVR ゾーンセットのアクティベーションは interop モードの VSAN で失敗します。

デバイス エイリアス モードの変更時の注意事項

デバイス エイリアス モードを変更する場合は、次の注意事項に従ってください。

- 異なるデバイス エイリアス モードで稼働している 2 つのファブリックが結合されると、デバイス エイリアスの結合は失敗します。 結合プロセス中、一方のモードまたは他方のモードに自動的に変換できません。 このような状況では、どちらか一方のモードを選択する必要があります。
- 拡張モードから基本モードに変更する前に、最初にローカル スイッチとリモート スイッチの両方からすべてのネイティブ デバイス エイリアス ベースの設定を明示的に削除するか、またはすべてのデバイス エイリアス ベース設定のメンバを対応する pWWN に置き換える必要があります。
- デバイス エイリアス データベースからデバイス エイリアスを削除すると、すべてのアプリケーションは対応するデバイス エイリアスの実行を自動的に中止します。 対応するデバイス エイリアスがアクティブなゾーンセットの一部である場合、その pWWN を出入りするすべてのトラフックが中断されます。
- デバイス エイリアス名を変更すると、デバイス エイリアス データベース内のデバイス エイリアス名が変更されるだけでなく、すべてのアプリケーションの対応するデバイス エイリアス設定も置き換えられます。
- デバイス エイリアス データベースに新しいデバイス エイリアスが追加され、そのデバイス エイリアスにアプリケーション設定が存在する場合、設定は自動的に有効になります。 たとえば、対応するデバイス エイリアスがアクティブなゾーンセットの一部で、デバイスがオンラインの場合、ゾーン分割が自動的に実行されます。 ゾーンセットを再度アクティブ化する必要はありません。
- デバイス エイリアス名が新しい HBA の pWWN にマッピングされると、それに応じてアプリケーションの適用方法が変更されます。 この場合、ゾーン サーバは、新しい HBA の pWWN に基づいて自動的にゾーン分割を適用します。

デバイス エイリアス モードの設定

デバイス エイリアスが拡張モードで動作するように設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **device-alias mode enhanced**
3. switch(config)# **no device-alias mode enhance**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **device-alias mode enhanced**	拡張モードで動作するデバイス エイリアスを割り当てます。
ステップ 3	switch(config)# **no device-alias mode enhance**	基本モードで動作するデバイス エイリアスを割り当てます。

デバイス エイリアス モードの設定の表示

現在のデバイス エイリアス モード設定を表示するには、**show device-alias status** コマンドを入力します。

```
switch# show device-alias status
Fabric Distribution: Enabled
Database:- Device Aliases 0 Mode: Basic
Locked By:- User "admin" SWWN 20:00:00:0d:ec:30:90:40
Pending Database:- Device Aliases 0 Mode: Basic
```

デバイス エイリアス配信の概要

デフォルトでは、デバイス エイリアスの配布はイネーブルになっています。 デバイス エイリアス機能は CFS を使用して、ファブリック内のすべてのスイッチに変更内容を配布します。

デバイス エイリアスの配布がディセーブルの場合、データベースの変更内容はファブリック内のスイッチに配布されません。 ファブリック内のすべてのスイッチで同じ変更を手動で行い、デバイス エイリアス データベースを最新の状態に維持する必要があります。 すぐにデータベースの変更が行われるので、保留中のデータベースおよびコミットまたは中断の操作はありません。 変更をコミットしていない状態で配布をディセーブルにすると、コミット作業は失敗します。

次に、失敗したデバイス エイリアスのステータスを表示する例を示します。

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

ファブリックのロック

デバイス エイリアス設定作業を行うと（どのデバイス エイリアス作業かに関係なく）、ファブリックはデバイスエイリアス機能に対して自動的にロックされます。ファブリックがロックされると、次のような状況になります。

- 他のユーザがこの機能の設定に変更を加えることができなくなります。
- 有効なデータベースのコピーが取得され、保留データベースとして使用されます。保留中のデータベースに対して、以降の変更が行われます。保留中のデータベースへの変更内容をコミットまたは廃棄（**中断**）するまで、保留中のデータベースは使用されます。

変更のコミット

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

- 有効なデータベースの内容が、保留中のデータベースの内容に上書きされます。
- 保留中のデータベースがファブリック内のスイッチに配布され、これらのスイッチの有効なデータベースが新しい変更内容に上書きされます。
- 保留中のデータベースの内容が空になります。
- ファブリック ロックがこの機能に対して解除されます。

変更内容をコミットする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **device-alias commit**

手順の詳細

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

変更の破棄

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

- 有効なデータベースの内容は影響を受けません。

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

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。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **device-alias abort**

手順の詳細

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

廃棄操作のステータスの表示

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

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

ファブリックのロックの上書き

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

スイッチを再起動した場合、変更はvolatileディレクトリでだけ使用でき、また廃棄される場合もあります。

管理者の権限を使用して、ロックされたデバイス エイリアス セッションを解除するには、EXEC モードで **clear device-alias session** コマンドを使用します。

```
switch# clear device-alias session
```

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

```
switch# show device-alias status
Fabric Distribution: Enabled
Database:- Device Aliases 24
Status of the last CFS operation issued from this switch:
==========================================================
Operation: Clear Session<--------------------Lock released by administrator
Status: Success<-----------------------------Successful status of the operation
```

デバイス エイリアスの配布のディセーブル化とイネーブル化

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

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **no device-alias distribute**
3. switch(config)# **device-alias distribute**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **no device-alias distribute**	配布をディセーブルにします。
ステップ 3	switch(config)# **device-alias distribute**	配布をイネーブルにします（デフォルト）。

Viewing the Status of Device Alias Distribution

デバイス エイリアス配布のステータスを表示するには、**show device-alias status** コマンドを使用します。 次に、配布がイネーブルな場合のデバイス エイリアスの表示例を示します。

```
switch# show device-alias status
Fabric Distribution: Enabled <-------------------------------Distribution is enabled

Database:-Device Aliases 24

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

Pending Database:- Device Aliases 24

Status of the last CFS operation issued from this switch:

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

Operation: Enable Fabric Distribution

Status: Success
```

次に、配布がディセーブルな場合のデバイス エイリアスの表示例を示します。

```
switch# show device-alias status
Fabric Distribution: Disabled
```

```
Database:- Device Aliases 24

Status of the last CFS operation issued from this switch:

-----------------------------------------------------------

Operation: Disable Fabric Distribution

Status: Success
```

レガシー ゾーン エイリアスの設定について

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

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

名前または定義の競合が存在する場合、ゾーン エイリアスはインポートされません。

設定に応じて、必要とされるゾーン エイリアスをデバイス エイリアス データベースにコピーしてください。

インポート操作が終了し、**commit** 操作を行うと、変更されたエイリアスデータベースが物理ファブリック内のほかのすべてのスイッチに配布されます。 ファブリック内のほかのスイッチに設定を配布したくない場合、**abort** 操作を行うと、結合の変更内容が完全に廃棄されます。

ゾーン エイリアスのインポート

特定の VSAN のゾーン エイリアスをインポートする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **device-alias import fcalias vsan** *vlan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **device-alias import fcalias vsan** *vlan-id*	指定された VSAN の fcalias 情報をインポートします。

デバイス エイリアス データベースの結合の注意事項

2 つのデバイス エイリアス データベースを結合する場合は、次の注意事項に従ってください。

- 名前が異なる 2 つのデバイス エイリアスが同一の pWWN にマッピングされていないことを確認します。
- 2 つの同一の pWWN が 2 つの異なるデバイス エイリアスにマッピングされていないことを確認します。
- 両方のデータベースのデバイス エイリアスの合計数が、Cisco MDS SAN-OS Release 3.0（x）以前が稼働しているファブリックでは 8K（8191 個のデバイス エイリアス）、Cisco MDS SAN-OS Release 3.1（x）以降が稼働しているファブリックでは 20K を超えていないことを確認します。

両方のデータベースのデバイス エントリの合計数がサポートされる設定制限値を超えた場合、結合は失敗します。 たとえば、データベース *N* に 6000 個のデバイス エイリアス、データベース *M* に 2192 個のデバイス エイリアスがあり、SAN-OS Release 3.0(x) 以前が稼働している場合、この結合操作は失敗します。 デバイス エイリアス モードが一致していない場合も、結合操作は失敗します。

追加情報については、『*Cisco Nexus 5000 Series System Management Configuration Guide*』の「CFS Merge Support」を参照してください。

デバイス エイリアス設定の確認

デバイス エイリアス情報を表示するには、次のいずれかの作業を実行します。

手順の概要

1. switch# **show zoneset** [**active**]
2. switch# **show device-alias database** [**pending** | **pending-diffs**]
3. switch# **show device-alias** {**pwwn** *pwwn-id* | **name** *device-name* } [**pending**]
4. switch# **show flogi database** [**pending**]
5. switch# **show fcns database** [**pending**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **show zoneset** [**active**]	ゾーン セット情報のデバイス エイリアスを表示します。
ステップ 2	switch# **show device-alias database** [**pending** | **pending-diffs**]	デバイス エイリアス データベースを表示します。

	コマンドまたはアクション	目的
ステップ 3	switch# **show device-alias** {**pwwn** *pwwn-id* | **name** *device-name* } [**pending**]	指定された pWWN またはエイリアスのデバイス エイリアス情報を表示します。
ステップ 4	switch# **show flogi database** [**pending**]	FLOGI データベースのデバイス エイリアス情報を表示します。
ステップ 5	switch# **show fcns database** [**pending**]	FCNS データベースのデバイス エイリアス情報を表示します。

デバイス エイリアス設定の確認例

次に、ゾーン セット内のデバイス エイリアス情報を表示する例を示します。

```
switch# show zoneset
zoneset name s1 vsan 1
  zone name z1 vsan 1
    pwwn 21:01:00:e0:8b:2e:80:93 [x] <---------------Device alias displayed for each pWWN.
    pwwn 21:00:00:20:37:39:ab:5f [y]
  zone name z2 vsan 1
    pwwn 21:00:00:e0:8b:0b:66:56 [SampleName]
    pwwn 21:00:00:20:37:39:ac:0d [z]
```

次に、デバイス エイリアス データベース内の保留中の変更内容を表示する例を示します。

```
switch# show device-alias database pending
```

次に、デバイス エイリアス データベース内の特定の pWWN を表示する例を示します。

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

次に、保留中のデバイス エイリアス データベースと有効なデバイス エイリアス データベースの相違点を表示する例を示します。

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

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

デフォルトのデバイス エイリアス設定

次の表に、デバイス エイリアス パラメータのデフォルト設定を示します。

表 *26*：デフォルトのデバイス エイリアス パラメータ

パラメータ	デフォルト
デバイス エイリアスの配布	イネーブル

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

第 12 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

この章の内容は、次のとおりです。

- ファイバ チャネル ルーティング サービスおよびプロトコルの設定，187 ページ

ファイバ チャネル ルーティング サービスおよびプロトコルの設定

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、Cisco SAN 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。 特殊な考慮事項を必要とする設定を除き、FSPF サービスを設定する必要はありません。 FSPF はファブリック内の任意の 2 つのスイッチ間の最適パスを自動的に計算します。 FSPF は次の機能を提供します。

- 任意の 2 つのスイッチ間に最短で最速のパスを確立して、ファブリック全体で動的にルートを計算します。
- 特定のパスに障害が発生したときに代替パスを選択します。 FSPF は複数のパスをサポートし、障害リンクを迂回する代替パスを自動的に計算します。 同等な 2 つのパスが使用可能な場合は、推奨ルートが提供されます。

FSPF に関する情報

FSPF は、ファイバ チャネル ネットワーク内でのルーティング用として、T11 委員会によって現在標準化されているプロトコルです。 FSPF プロトコルには、次の特性および特徴があります。

- 複数パスのルーティングをサポートします。
- パス ステータスはリンク ステート プロトコルによって決まります。

- ドメイン ID だけに基づいて、ホップ単位ルーティングを行います。
- FSPF が稼働するポートは E ポートまたは TE ポートに限られていて、トポロジはループ フリーです。
- VSAN 単位で稼働します。 ファブリック内の各 VSAN では、この VSAN に設定されたスイッチとの接続が保証されます。
- トポロジ データベースを使用して、ファブリック内のすべてのスイッチのリンク ステートを追跡し、各リンクにコストを対応付けます。
- トポロジが変更された場合、迅速な再コンバージェンスを保証します。 標準ダイクストラ アルゴリズムを使用します。ただし、より強固で、効率的な差分ダイクストラ アルゴリズムを静的に、あるいは動的に選択することができます。 VSAN 単位でルートが計算されるため、再コンバージェンス タイムは高速かつ効率的です。

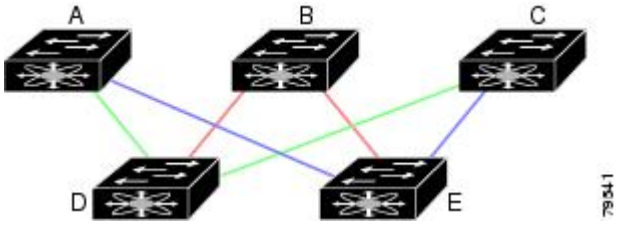
（注） FSPF 機能は任意のトポロジで使用できます。

FSPF の例

フォールト トレラント ファブリックの例

次の図は、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部分でリンク ダウンが発生しても、各スイッチはファブリック内の他のすべてのスイッチと通信できます。 同様に、どのスイッチがダウンしても、ファブリックの残りの接続は維持されます。

図 *36*： フォールト トレラント ファブリック



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

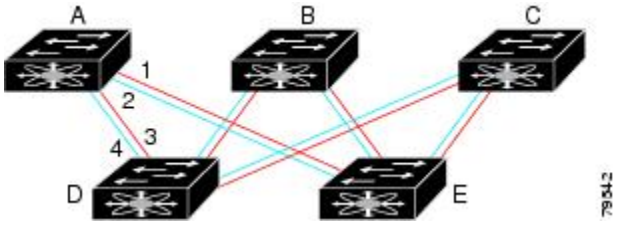
冗長リンクの例

トポロジを改善するには、任意のスイッチペア間の接続をそれぞれ複製します。スイッチペア間には複数のリンクを設定できます。 次の図は、この調整例を示します。 Cisco SAN スイッチは

SAN 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ペアをそれぞれ単一の論理リンクとして認識できます。

物理リンク ペアをバンドルすると、データベース サイズおよびリンク更新頻度が減るため、FSPF の効率が大幅に向上します。物理リンクが集約されると、障害は単一リンクでなく、SANポートチャネル全体に対応付けられます。この設定により、ネットワークの復元力も向上します。SAN ポートチャネル内にリンク障害が発生してもルートが変更されないため、ルーティングループ、トラフィックの消失、またはルート再設定によるファブリック ダウンタイムが生じるリスクが軽減されます。

図 *37*：冗長リンクを持つフォールト トレラント ファブリック



たとえば、すべてのリンク速度が等しく、SAN ポート チャネルが存在しない場合、FSPF は A ～ C の 4 つの同等のパス（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は、これらのパスは 2 つに減ります。

FSPF のグローバル設定

デフォルトでは、FSPF は Cisco SAN スイッチでイネーブルです。

一部の FSPF 機能は、各 VSAN でグローバルに設定できます。 VSAN 全体に機能を設定すると、コマンドごとにVSAN番号を指定する必要がなくなります。 このグローバル設定機能を使用すると、タイプ ミスや、その他の軽微な設定エラーが発生する可能性も低減されます。

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

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

SPF 計算ホールド タイムの概要

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

Link State Records の概要

ファブリックに新しいスイッチが追加されるたびに、Link State Record（LSR）が近接スイッチに送信されて、ファブリック全体にフラッディングされます。

次の表に、スイッチの応答のデフォルト設定を表示します。

表 *27*：*LSR* のデフォルト設定

LSR のオプション	デフォルト	説明
ACK インターバル（RxmtInterval）	5 秒	再送信するまで、スイッチが LSR からの ACK を待機する期間
リフレッシュ タイム（LSRefreshTime）	30 分	LSR リフレッシュを送信するまで、スイッチが待機する期間
最大エージング（MaxAge）	60 分	データベースから LSR を削除するまで、スイッチが待機する期間

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

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

VSAN での FSPF の設定

VSAN 全体に FSPF 機能を設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fspf config vsan** *vsan-id*
3. switch-config-(fspf-config)# **spf static**
4. switch-config-(fspf-config)# **spf hold-time** *value*
5. switch-config-(fspf-config)# **region** *region-id*

手順の詳細

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

FSPF のデフォルト設定へのリセット

FSPF VSAN グローバル設定を工場出荷時のデフォルト設定に戻す手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **no fspf config vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **no fspf config vsan** *vsan-id*	指定された VSAN の FSPF 設定を削除します。

FSPF のイネーブル化またはディセーブル化

FSPF ルーティング プロトコルをイネーブルまたはディセーブルにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fspf enable vsan** *vsan-id*
3. switch(config)# **no fspf enable vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fspf enable vsan** *vsan-id*	指定された VSAN 内で FSPF ルーティング プロトコルをイネーブルにします。
ステップ 3	switch(config)# **no fspf enable vsan** *vsan-id*	指定された VSAN 内で FSPF ルーティング プロトコルをディセーブルにします。

VSAN の FSPF カウンタのクリア

VSAN 全体の FSPF 統計情報カウンタをクリアする手順は、次のとおりです。

手順の概要

1. switch# **clear fspf counters vsan** *vsan-id*

手順の詳細

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

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

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対応付け、コストが最小なパスを選択します。インターフェイスに関連付けられたコストを管理上変更して、FSPF ルート選択を実行できます。 コストは、1 ～ 65,535 の整数値で指定できます。 1 Gbps のデフォルト コストは 1000 であり、2 Gbps では 500 です。

FSPF リンク コストの設定

FSPF リンク コストを設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **interface fc** *slot*/*port*
3. switch(config-if)# **fspf cost** *value* **vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface fc** *slot*/*port*	指定されたインターフェイスを設定します。すでに設定されている場合は、指定されたインターフェイスに対してコンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **fspf cost** *value* **vsan** *vsan-id*	指定された VSAN 内の選択されたインターフェイスにコストを設定します。

hello タイム インターバルの概要

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

（注） この値は、ISL の両端のポートで同じでなければなりません。

hello タイム インターバルの設定

FSPF hello タイム インターバルを設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **interface fc** *slot*/*port*
3. switch(config-if)# **fspf hello-interval** *value* **vsan** *vsan-id*

手順の詳細

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

デッド タイム インターバルの概要

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

（注） この値は、ISL の両端のポートで同じでなければなりません。

注意 設定されたデッド タイム インターバルが hello タイム インターバルより小さい場合は、コマンド プロンプトにエラーが報告されます。

デッド タイム インターバルの設定

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。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **interface fc** *slot*/*port*
3. switch(config-if)# **fspf dead-interval** *value* **vsan** *vsan-id*

手順の詳細

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

再送信インターバルの概要

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

（注） この値は、インターフェイスの両端のスイッチで同じでなければなりません。

再送信インターバルの設定

FSPF 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。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **interface fc** *slot*/*port*
3. switch(config-if)# **fspf retransmit-interval** *value* **vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **interface fc** *slot*/*port*	指定されたインターフェイスを設定します。すでに設定されている場合は、指定されたインターフェイスに対してコンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **fspf retransmit-interval** *value* **vsan** *vsan-id*	指定された VSAN の未確認応答リンク ステート アップデートの再送信タイム インターバルを指定します。 デフォルトは 5 秒です。

インターフェイス単位での FSPF のディセーブル化

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

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

特定のインターフェイスに対する FSPF のディセーブル化

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

特定のインターフェイスで FSPF をディセーブルにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **interface fc** *slot*/*port*
3. switch(config-if)# **fspf passive vsan** *vsan-id*
4. switch(config-if)# **no fspf passive vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **interface fc** *slot*/*port*	指定されたインターフェイスを設定します。すでに設定されている場合は、指定されたインターフェイスに対してコンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **fspf passive vsan** *vsan-id*	指定された VSAN 内の特定のインターフェイスに対して FSFP プロトコルをディセーブルにします。
ステップ 4	switch(config-if)# **no fspf passive vsan** *vsan-id*	指定された VSAN 内の特定のインターフェイスに対して FSFP プロトコルを再度イネーブルにします。

インターフェイスの FSPF カウンタのクリア

インターフェイスの FSPF 統計情報カウンタをクリアする手順は、次のとおりです。

手順の概要

1. switch# **clear fspf counters vsan** *vsan-id* **interface fc** *slot*/*port*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **clear fspf counters vsan** *vsan-id* **interface fc** *slot*/*port*	指定された VSAN 内の指定インターフェイスの FSPF 統計情報カウンタをクリアします。

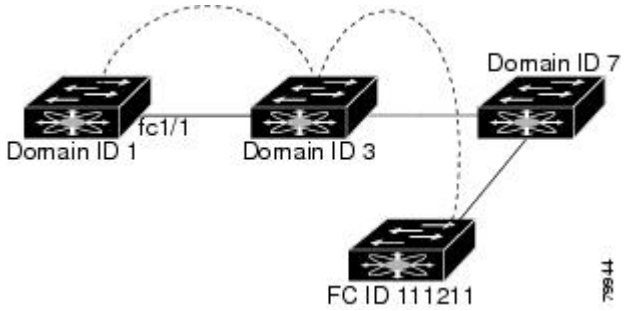
FSPF ルート

FSPF は、FSPF データベース内のエントリに基づいて、ファブリックを経由するトラフィックをルーティングします。 これらのルートは動的に学習させるか、または静的に設定することもできます。

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 を使用して、ドメイン ID が 1 のスイッチに、指定されたルート（FC ID 111211 やドメイン ID 3 など）を設定できます（次の図を参照）。

図 *38*：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

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。

手順の概要

1. switch# **configuration terminal**
2. switch(config)#**fcroute** *fcid* **interface fc** *slot*/*port* **domain** *domain-id* **vsan** *vsan-id*
3. switch(config)#**fcroute** *fcid* **interface san-port-channel** *port* **domain** *domain-id* **vsan** *vsan-id*
4. switch(config)# **fcroute** *fcid* **interface fc** *slot*/*port* **domain** *domain-id* **metric** *value* **vsan** *vsan-id*
5. switch(config)#**fcroute** *fcid* **interface fc** *slot*/*port* **domain** *domain-id* **metric** *value* **remote vsan** *vsan-id*
6. switch(config)#**fcroute** *fcid netmask* **interface fc** *slot*/*port* **domain** *domain-id* **vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)#**fcroute** *fcid* **interface fc** *slot*/*port* **domain** *domain-id* **vsan** *vsan-id*	指定されたファイバ チャネル インターフェイスおよびドメインに対応するルートを設定します。 この例では、指定されたインターフェイスに FC ID、およびネクスト ホップ スイッチに対するドメイン ID が割り当てられます。
ステップ 3	switch(config)#**fcroute** *fcid* **interface san-port-channel** *port* **domain** *domain-id* **vsan** *vsan-id*	指定された SAN ポート チャネル インターフェイスおよびドメインに対応するルートを設定します。 この例では、インターフェ

	コマンドまたはアクション	目的
		イス san-port-channel 1 に FC ID（0x111211）、およびネクスト ホップ スイッチに対するドメイン ID が割り当てられます。
ステップ 4	switch(config)# **fcroute** *fcid* **interface fc** *slot*/*port* **domain** *domain-id* **metric** *value* **vsan** *vsan-id*	特定の FC ID およびネクスト ホップ ドメイン ID に対応するスタティック ルートを設定し、ルートのコストも割り当てます。 リモートの宛先オプションを指定しない場合、デフォルトは direct です。
ステップ 5	switch(config)#**fcroute** *fcid* **interface fc** *slot*/*port* **domain** *domain-id* **metric** *value* **remote vsan** *vsan-id*	RIB にスタティック ルートを追加します。 このルートがアクティブ ルートであり、転送情報ベース（FIB）レコードに空きがある場合は、FIB にもこのルートが追加されます。 ルートのコスト（メトリック）を指定しない場合、デフォルトは 10 です。
ステップ 6	switch(config)#**fcroute** *fcid netmask* **interface fc** *slot*/*port* **domain** *domain-id* **vsan** *vsan-id*	インターフェイス（またはSAN ポート チャネル）に指定されたルートのネットマスクを設定します。 3 つのルート（ドメインだけに一致する 0xff0000、ドメインおよびエリアに一致する 0xffff00、およびドメイン、エリア、ポートに一致する 0xffffff）のいずれかを指定できます。

順序どおりの配信

データ フレームに関して In-Order Delivery（IOD; 順序どおりの配信）を行うと、送信元が送信した順番で宛先にフレームが配信されることが保証されます。

一部のファイバチャネルプロトコルまたはアプリケーションでは、順序外のフレーム配信を処理できません。 このような場合、Cisco SAN スイッチはフレーム フロー内のフレーム順序を保持します。 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 に対応したスイッチでは、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すべてのフレームは、常に受信された順番で配信されます。

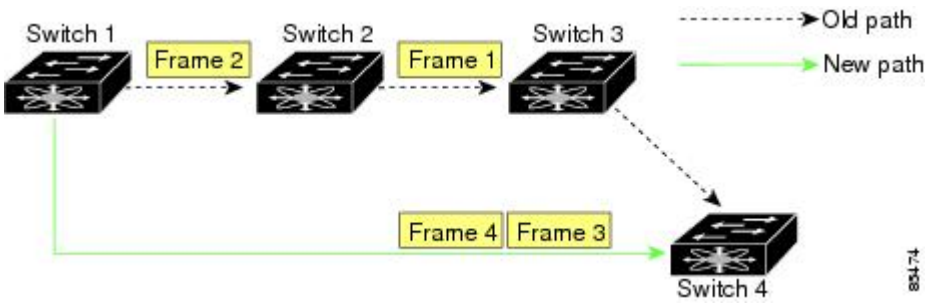
IOD を使用するのは、順序外のフレーム配信をサポートできない環境の場合だけにしてください。

順序どおりの配信機能をイネーブルにすると、グレースフル シャットダウン機能は実行されません。

ネットワーク フレーム順序の再設定の概要

ネットワーク内でルートが変更されると、新しく選択されたパスが元のルートよりも高速になったり、輻輳が軽減されたりすることがあります。

図 *39*： ルート変更の配信



上の図では、スイッチ 4 からスイッチ 1 への新しいパスの方が高速です。 したがって、フレーム 3 およびフレーム 4 は、フレーム 1 およびフレーム 2 よりも先に配信されることがあります。

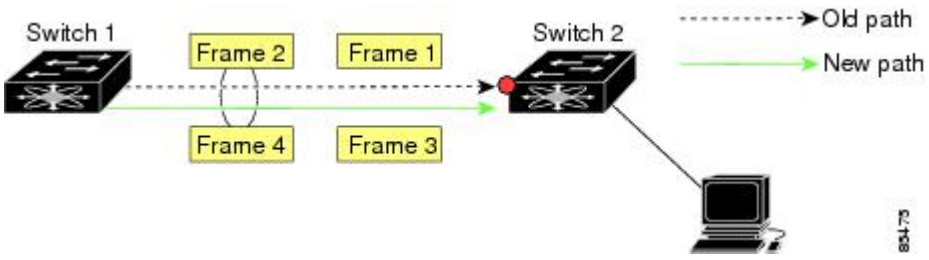
順序保証機能がイネーブルの場合、ネットワーク内のフレームは次のように配信されます。

- ネットワーク内のフレームは送信された順番で配信されます。
- ネットワーク遅延ドロップ期間内に順番どおりに配信できないフレームは、ネットワーク内でドロップされます。

SAN ポート チャネル フレームの順序変更について

SANポートチャネル内でリンクが変更されると、同じ交換または同じフローに対応するフレームが、より高速なパスに切り替わることがあります。

図 *40*： リンクが輻輳している場合の配信



上の図では、古いパス（赤点）のポートが輻輳しています。 したがって、フレーム 3 およびフレーム 4 は、フレーム 1 およびフレーム 2 よりも先に配信されることがあります。

順序どおりの配信機能がイネーブルになっている場合、ポート チャネル リンクに変更が生じると、その SAN ポート チャネルを通過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が配信されてから、新しいフレームが許可されます。
- 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消去されてから、新しいパスを通して配信されます。

古いパスを経由するフレームをネットワーク遅延ドロップ期間内に順番どおりに配信できない場合は、これらのフレームはドロップされます。

関連トピック

ドロップ遅延時間の設定, （203 ページ）

順序どおりの配信のイネーブル化の概要

順序どおりの配信機能は、特定の VSAN またはスイッチ全体に対してイネーブルにできます。 デフォルトでは、順序どおりの配信は、Cisco SAN 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のは、順序に従わないフレームを処理できないデバイスがスイッチに搭載されている場合に限定してください。 スイッチ内のロードバランシングアルゴリズムを使用すると、通常のファブリック処理中に、フレームを順序どおりに配信できます。 送信元FC ID、宛先 FC ID、および交換 ID に基づくロードバランシング アルゴリズムをハードウェアで実行しても、パフォーマンスは低下しません。 ただし、順序どおりの配信機能がイネーブルの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中断され、順序に従わずに転送される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、回復が遅れます。

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上のすべての VSAN で統一されるように保証するには、順序どおりの配信をグローバルにイネーブルにします。

順序どおりの配信をグローバルにイネーブルにするのは、ファブリック全体にこの機能が必要な場合だけにしてください。 そうでない場合は、この機能を必要とする VSAN に対してだけ IOD をイネーブルにします。

スイッチで順序どおりの配信をイネーブルにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **in-order-guarantee**
3. switch(config)# **no in-order-guarantee**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **in-order-guarantee**	スイッチ内で順序どおりの配信をイネーブルにします。
ステップ 3	switch(config)# **no in-order-guarantee**	スイッチを出荷時の設定に戻し、順序どおりの配信機能をディセーブルにします。

特定の VSAN に対する順序どおりの配信のイネーブル化

VSAN を新しく作成すると、グローバルな順序保証値が自動的に継承されます。 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設定することにより、このグローバル値を変更できます。

マルチキャスト ツリーの計算に最下位ドメイン スイッチを使用する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **in-order-guarantee vsan** *vsan-id*
3. switch(config)# **no in-order-guarantee vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **in-order-guarantee vsan** *vsan-id*	指定された VSAN 内で順序どおりの配信をイネーブルにします。
ステップ 3	switch(config)# **no in-order-guarantee vsan** *vsan-id*	スイッチを出荷時のデフォルト設定に戻し、指定された VSAN の順序どおりの配信機能をディセーブルにします。

順序どおりの配信のステータスの表示

現在の設定ステータスを表示するには、**show in-order-guarantee** コマンドを使用します。

```
switch# show in-order-guarantee
global inorder delivery configuration:guaranteed
VSAN specific settings
vsan 1 inorder delivery:guaranteed
vsan 101 inorder delivery:not guaranteed
vsan 1000 inorder delivery:guaranteed
vsan 1001 inorder delivery:guaranteed
vsan 1682 inorder delivery:guaranteed
vsan 2001 inorder delivery:guaranteed
vsan 2009 inorder delivery:guaranteed
vsan 2456 inorder delivery:guaranteed
vsan 3277 inorder delivery:guaranteed
vsan 3451 inorder delivery:guaranteed
vsan 3452 inorder delivery:guaranteed
```

ドロップ遅延時間の設定

ネットワーク、ネットワーク内の指定された VSAN、またはスイッチ全体のデフォルトの遅延時間を変更できます。

ネットワークおよびスイッチのドロップ遅延時間を設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcdroplatency network** *value*
3. switch(config)# **fcdroplatency network** *value* **vsan** *vsan-id*
4. switch(config)# **no fcdroplatency network** *value*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcdroplatency network** *value*	ネットワークのネットワーク ドロップ遅延時間を設定します。 有効値は 0 ～ 60000 ミリ秒です。 デフォルトは 2000 ミリ秒です。 （注） ネットワークのドロップ遅延時間は、ネットワーク内の最長パスのすべてのスイッチ遅延の合計として計算する必要があります。
ステップ 3	switch(config)# **fcdroplatency network** *value* **vsan** *vsan-id*	指定された VSAN のネットワーク ドロップ遅延時間を設定します。

	コマンドまたはアクション	目的
ステップ 4	switch(config)# **no fcdroplatency network** *value*	現在の fcdroplatency ネットワーク設定を削除し、スイッチを出荷時の設定に戻します。

遅延情報の表示

show fcdroplatency コマンドを使用して、設定された遅延パラメータを表示できます。次に、ネットワーク遅延情報を表示する例を示します。

```
switch# show fcdroplatency
switch latency value:500 milliseconds
global network latency value:2000 milliseconds
VSAN specific network latency settings
vsan 1 network latency:5000 milliseconds
vsan 2 network latency:2000 milliseconds
vsan 103 network latency:2000 milliseconds
vsan 460 network latency:500 milliseconds
```

フロー統計情報の設定

フロー統計情報は、集約統計情報テーブル内の入力トラフィックをカウントします。 次の 2 種類の統計情報を収集できます。

- 集約フロー統計（VSAN のトラフィックをカウント）。
- VSAN 内の送信元/宛先 ID ペアに対応するトラフィックをカウントするフロー統計情報。

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、集約フロー統計情報およびフロー統計情報に対して、最大 1000 エントリをイネーブルにできます。 使用されていないフロー インデックスを、各新規フローに割り当てるようにしてください。フローインデックスの番号の間は、集約フロー統計情報とフロー統計情報間で共有します。

集約フロー統計情報のカウント

VSAN の集約フロー統計情報をカウントする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcflow stats aggregated index** *value* **vsan** *vsan-id*
3. switch(config)# **no fcflow stats aggregated index** *value* **vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcflow stats aggregated index** *value* **vsan** *vsan-id*	集約フロー カウンタをイネーブルにします。
ステップ 3	switch(config)# **no fcflow stats aggregated index** *value* **vsan** *vsan-id*	集約フロー カウンタをディセーブルにします。

個々のフロー統計情報のカウント

VSAN 内の送信元および宛先 FC ID のフロー統計情報をカウントする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcflow stats index** *value dest-fcid source-fcid netmask* **vsan** *vsan-id*
3. switch(config)# **no fcflow stats aggregated index** *value* **vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcflow stats index** *value dest-fcid source-fcid netmask* **vsan** *vsan-id*	フロー カウンタをイネーブルにします。 （注） ソース ID および宛先 ID は、16 進形式の FC ID（0x123aff など）で指定します。 使用できるマスクは、0xff0000 または 0xffffff のどちらかです。
ステップ 3	switch(config)# **no fcflow stats aggregated index** *value* **vsan** *vsan-id*	フロー カウンタをディセーブルにします。

FIB 統計情報のクリア

集約フロー カウンタをクリアするには、**clear fcflow stats**コマンドを使用します。 次に、集約フロー カウンタをクリアする例を示します。

```
switch# clear fcflow stats aggregated index 1
```

次に、送信元および宛先 FC ID に対応するフロー カウンタをクリアする例を示します。

```
switch# clear fcflow stats index 1
```

フロー統計情報の表示

フロー統計情報を表示するには、**show fcflow stats** コマンドを使用します。 次に、集約フロー概要を表示する例を示します。

```
switch# show fcflow stats aggregated
Idx       VSAN     frames
---------- ---------- ----------
         6          1      42871
```

次に、フロー統計情報を表示する例を示します。

```
switch# show fcflow stats
```

次に、フロー インデックスの使用状況を表示する例を示します。

```
switch# show fcflow stats usage
2 flows configured
Configured flows : 3,7
```

次に、特定の VSAN のグローバル FSPF 情報を表示する例を示します。

```
switch# show fspf vsan 1
```

次に、指定された VSAN の FSPF データベースの概要を表示する例を示します。 追加のパラメータを指定しない場合、データベース内のすべての LSR が表示されます。

```
switch# show fspf database vsan 1
```

次に、FSPF インターフェイス情報を表示する例を示します。

```
switch# show fspf vsan 1 interface fc2/1
```

FSPF のデフォルト設定値

次の表に、FSPF 機能のデフォルト設定を示します。

表 *28*： *FSPF* のデフォルト設定値

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です。
SPF 計算	ダイナミック
SPF ホールド タイム	0.
バックボーン リージョン	0.
ACK インターバル（RxmtInterval）	5 秒
リフレッシュ タイム（LSRefreshTime）	30 分
最大エージング（MaxAge）	60 分

パラメータ	デフォルト
hello 間隔	20 秒
デッド間隔	80 秒
配信ツリー情報	主要スイッチ（ルート ノード）から取得します。
ルーティング テーブル	FSPF は指定された宛先への等コスト パスを 16 まで格納します。
ロード バランシング	複数の等コスト パスの宛先 ID およびソース ID に基づきます。
順序どおりの配信	ディセーブル。
ドロップ遅延	ディセーブル。
スタティック ルート コスト	ルートのコスト（メトリック）を指定しない場合、デフォルトは 10 です。
リモート宛先スイッチ	リモート宛先スイッチを指定しない場合、デフォルトは、direct です。
マルチキャスト ルーティング	主要スイッチを使用してマルチキャスト ツリーを計算します。

第 13 章

FLOGI、ネーム サーバ、FDMI、および RSCN データベースの管理

この章の内容は、次のとおりです。

- FLOGI、ネーム サーバ、FDMI、および RSCN データベースの管理，209 ページ

FLOGI、ネーム サーバ、FDMI、および RSCN データベースの管理

ファブリック ログインに関する情報

ファイバ チャネル ファブリックでは、ホストまたはディスクごとに FC ID が必要です。 FLOGI テーブルにストレージデバイスが表示されるかどうかを確認するには、次の例のように **show flogi** コマンドを使用します。 必要なデバイスが FLOGI テーブルに表示されていれば、FLOGI が正常に行われます。 ホスト HBA および接続ポートに直接接続されているスイッチ上の FLOGI データベースを検査します。

次に、FLOGI テーブルのストレージ デバイスを確認する例を示します。

```
switch# show flogi database
--------------------------------------------------------------------------------
INTERFACE  VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
fc2/3      1     0xb200e2  21:00:00:04:cf:27:25:2c  20:00:00:04:cf:27:25:2c
fc2/3      1     0xb200e1  21:00:00:04:cf:4c:18:61  20:00:00:04:cf:4c:18:61
fc2/3      1     0xb200d1  21:00:00:04:cf:4c:18:64  20:00:00:04:cf:4c:18:64
fc2/3      1     0xb200ce  21:00:00:04:cf:4c:16:fb  20:00:00:04:cf:4c:16:fb
fc2/3      1     0xb200cd  21:00:00:04:cf:4c:18:f7  20:00:00:04:cf:4c:18:f7
vfc3/1     2     0xb30100  10:00:00:05:30:00:49:63  20:00:00:05:30:00:49:5e
Total number of flogi = 6.
```

次に、特定のインターフェイスに接続されたストレージ デバイスを確認する例を示します。

```
switch# show flogi database interface vfc1/1
INTERFACE  VSAN    FCID           PORT NAME               NODE NAME
```

```
--------------------------------------------------------------------------------
vfc1/1     1     0x870000  20:00:00:1b:21:06:58:bc  10:00:00:1b:21:06:58:bc
Total number of flogi = 1.
```

次に、VSAN（仮想 SAN）1 に関連付けられたストレージ デバイスを確認する例を示します。

```
switch# show flogi database vsan 1
```

ネーム サーバ プロキシ

ネーム サーバ機能は、各 VSAN 内のすべてのホストおよびストレージ デバイスの属性が格納されたデータベースをメンテナンスします。 ネームサーバでは、情報を最初に登録したデバイスによるデータベース エントリの変更が認められます。

プロキシ機能は、別のデバイスによって登録されたデータベース エントリの内容を変更（更新または削除）する必要がある場合に役立ちます。

ネーム サーバ プロキシ登録の概要

ネーム サーバ登録要求はすべて、パラメータが登録または変更されたポートと同じポートから発信されます。 同一ポートから送られない場合、要求は拒否されます。

この許可を使用すると、WWN が他のノードに代わって特定のパラメータを登録できるようになります。

ネーム サーバ プロキシの登録

ネーム サーバ プロキシを登録する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)#**fcns proxy-port** *wwn-id* **vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)#**fcns proxy-port** *wwn-id* **vsan** *vsan-id*	指定した VSAN のプロキシ ポートを設定します。

重複 pWWN の拒否について

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

重複 pWWN の拒否

重複 pWWN を拒否する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcns reject-duplicate-pwwn vsan** *vsan-id*
3. switch(config)# **no fcns reject-duplicate-pwwn vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcns reject-duplicate-pwwn vsan** *vsan-id*	pWWN がすでに存在する場合は、デバイスがファブリックにログインする際に、デバイスをログアウトします。
ステップ 3	switch(config)# **no fcns reject-duplicate-pwwn vsan** *vsan-id*	同一の pWWN を持つ新しいデバイスでネーム サーバ データベースにある最初のデバイスのエントリを上書きします（デフォルト）。

ネーム サーバ データベース エントリの概要

ネーム サーバはすべてのホストのネーム エントリを FCNS データベースに保管しています。 ネーム サーバを使用すると、Nx ポートで（ネーム サーバへの）PLOGI 中に属性を登録し、その他のホストの属性を取得できます。 Nx ポートが明示的または暗黙的にログアウトする時点で、これらの属性は登録解除されます。

マルチスイッチ ファブリック構成では、各スイッチ上で稼働するネーム サーバ インスタンスが分散型データベースで情報を共有します。 スイッチごとに 1 つのネーム サーバ プロセスのインスタンスが実行されます。

ネーム サーバのデータベース エントリの表示

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

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

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

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

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

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

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

次に、指定された VSAN のネーム サーバ データベースおよび統計情報を表示する例を示します。

```
switch# show fcns database vsan 1
VSAN 1:
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x030001    N     10:00:00:05:30:00:25:a3 (Cisco)         ipfc
0x030101    NL    10:00:00:00:77:99:60:2c (Interphase)
0x030200    N     10:00:00:49:c9:28:c7:01
0xec0001    NL    21:00:00:20:37:a6:be:14 (Seagate)       scsi-fcp
Total number of entries = 4
```

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

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

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

```
switch# show fcns statistics
```

FDMI

Cisco SAN スイッチは、FC-GS-4 規格で記述されている Fabric-Device 管理インターフェイス（FDMI）機能をサポートしています。 FDMI を使用すると、ファイバ チャネル HBA などのデバイスをインバンド通信によって管理できます。 この機能を追加することにより、既存のファイバ チャネル ネーム サーバおよび管理サーバの機能を補完します。

FDMI 機能を使用すると、独自のホスト エージェントをインストールしなくても、スイッチ ソフトウェアによって接続先 HBA およびホスト オペレーティング システムに関する次のような管理情報を抽出できます。

- 製造元、モデル、およびシリアル番号
- ノード名およびノードのシンボリック名
- ハードウェア、ドライバ、およびファームウェアのバージョン
- ホスト オペレーティング システム（OS）の名前およびバージョン番号

FDMI エントリはすべて永続ストレージに保存され、FDMI プロセスを起動した時点で取り出されます。

FDMI の表示

次に、指定された VSAN のすべての HBA の詳細情報を表示する例を示します。

```
switch# show fdmi database detail vsan 1
```

RSCN

Registered State Change Notification（RSCN）は、ファブリック内で行われた変更について各ホストに通知するためのファイバ チャネル サービスです。 ホストは、（State Change Registration（SCR）要求によって）ファブリック コントローラに登録することにより、この情報を受信できます。 次のいずれかのイベントが発生した場合、適宜通知されます。

- ファブリックへのディスクの加入または脱退
- ネーム サーバの登録変更
- 新しいゾーンの実施
- IP アドレスの変更
- ホストの動作に影響する、その他の同様なイベント

RSCN 情報の概要

スイッチ RSCN（SW-RSCN）は、登録されたホストおよびファブリック内の到達可能なすべてのスイッチに送信されます。

（注） スイッチは RSCN を送信して、登録済みのノードに変更が発生したことを通知します。 ネーム サーバに再度クエリーを発行して新しい情報を取得するのは、各ノードの責任範囲です。 スイッチが各ノードに送信する RSCN には、変更に関する詳細情報は含まれていません。

RSCN 情報の表示

次に、登録済みデバイス情報を表示する例を示します。

```
switch# show rscn scr-table vsan 1
```

（注） SCR テーブルは設定不可能です。 ホストが RSCN 情報と一緒に SCR フレームを送信する場合にかぎり、入力されます。 ホストが RSCN 情報を受信しない場合、**show rscn scr-table** コマンドはエントリを返しません。

[multi-pid] オプションの概要

RSCN の multi-pidオプションをイネーブルに設定すると、登録済み Nx ポートに対して生成される RSCN に、影響を受けた複数のポート ID が含まれる場合があります。 この場合、ゾーン分割ルールを適用してから、影響を受けた複数のポート ID が 1 つの RSCN にまとめられます。 このオプションをイネーブルにすることによって、RSCN の数を減らすことができます。 たとえば、スイッチ 1 に 2 つのディスク（D1、D2）および 1 台のホスト（H）が接続されていると仮定します。 ホスト H は、RSCN を受信するように登録済みです。 D1、D2、および H は、同じゾーンに属しています。 ディスク D1 および D2 が同時にオンラインである場合、次のどちらかの処理が適用されます。

- スイッチ 1 の multi-pid オプションがディセーブル：ホスト H に対して、2 つの RSCN（ディスク D1 とディスク D2 に関して 1 つずつ）が生成されます。
- スイッチ 1 の multi-pid オプションがイネーブル：ホスト H に対して単一の RSCN が生成されます。RSCN ペイロードには、影響を受けたポート ID が一覧表示されます（この場合は、D1 と D2 の両方）。

（注） Nx ポートには、multi-pid RSCN ペイロードをサポートしないものがあります。 その場合は、RSCN multi-pid オプションをディセーブルにしてください。

[multi-pid] オプションの設定

multi-pid オプションを設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **rscn multi-pid vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **rscn multi-pid vsan** *vsan-id*	指定された VSAN の RSCN を multi-pid フォーマットで送信します。

ドメイン フォーマット SW-RSCN の抑制

ドメイン フォーマット SW-RSCN は、ローカル スイッチ名またはローカル スイッチ管理 IP アドレスが変更されるとすぐに送信されます。 この SW-RSCN は、ISL を介して、他のすべてのドメインおよびスイッチに送信されます。 リモート スイッチから、ドメイン フォーマット SW-RSCN を開始したスイッチに対して GMAL コマンドおよび GIELN コマンドを発行すると、変更内容を判別できます。 ドメイン フォーマット SW-RSCN によって、一部の他社製の SAN スイッチで問題が発生することがあります。

これらの SW-RSCN の ISL を介した送信を抑制する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **rscn suppress domain-swrscn vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **rscn suppress domain-swrscn vsan** *vsan-id*	指定された VSAN のドメイン フォーマット SW-RSCN の送信を抑制します。

RSCN 統計情報のクリア

カウンタをクリアしたあとに、それらのカウンタを別のイベントに関して表示することができます。 たとえば、特定のイベント（ONLINE または OFFLINE イベントなど）で生成された RSCN または SW-RSCN の個数を追跡できます。 このような統計情報を利用して、VSAN 内で発生する各イベントへの応答を監視できます。

次に、指定された VSAN の RSCN 統計情報をクリアする例を示します。

```
switch# clear rscn statistics vsan 1
```

RSCN 統計情報をクリアした後、**show rscn statistics** コマンドを入力してクリアされたカウンタを表示できます。

```
switch# show rscn statistics vsan 1
```

RSCN タイマーの設定

RSCN は、VSAN 単位のイベント リスト キューを維持します。RSCN イベントは、生成されると、このキューに入れられます。 最初の RSCN イベントがキューに入ると、VSAN 単位のタイマーが始動します。 タイムアウトになると、すべてのイベントがキューから出され、結合 RSCN が登録済みユーザに送信されます。 デフォルトのタイマー値の場合に、登録済みユーザに送信される結

合 RSCN の数が最小になります。 配置によっては、ファブリック内の変更を追跡するために、イベント タイマー値をさらに小さくする必要が生じることがあります。

（注） RSCN タイマー値は、VSAN 内のすべてのスイッチで同一にする必要があります。

（注） ダウングレードを実行する場合は、事前に、ネットワーク内の RSCN タイマー値をデフォルト値に戻してください。 デフォルト値に戻しておかないと、VSAN およびその他のデバイスを経由するリンクがディセーブルになります。

RSCN タイマーを設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **rscn distribute**
3. switch(config)# **rscn event-tov** *timeout* **vsan** *vsan-id*
4. switch(config)# **no rscn event-tov** *timeout* **vsan** *vsan-id*
5. switch(config)# **rscn commit vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **rscn distribute**	RSCN タイマーの設定の配布をイネーブルにします。
ステップ 3	switch(config)# **rscn event-tov** *timeout* **vsan** *vsan-id*	指定した VSAN のイベント タイムアウト値（ミリ秒）を設定します。 有効値は 0 ～ 2000 ミリ秒です。 値をゼロ（0）に設定すると、タイマーはディセーブルになります。
ステップ 4	switch(config)# **no rscn event-tov** *timeout* **vsan** *vsan-id*	デフォルト値（ファイバ チャネル VSAN の場合、2000 ミリ秒）に戻します。
ステップ 5	switch(config)# **rscn commit vsan** *vsan-id*	配布する RSCN タイマー設定を指定された VSAN 内のスイッチにコミットします。

RSCN タイマー設定の確認

RSCN タイマー設定を確認するには、**show rscn event-tov vsan** コマンドを使用します。 次に、VSAN 10 の RSCN 統計情報をクリアする例を示します。

```
switch# show rscn event-tov vsan 10
Event TOV : 1000 ms
```

RSCN タイマー設定の配布

各スイッチのタイムアウト値は、手動で設定されるため、異なるスイッチが別々の時間にタイムアウトになると、誤設定が生じます。 つまり、ネットワーク内の異なる N ポートが別々の時間に RSCN を受信してしまうことがあります。 Cisco Fabric Service（CFS）インフラストラクチャでは、RSCN タイマー設定情報をファブリック内のすべてのスイッチに自動的に配布することで、この状況を解消します。 また、SW-RSCN の数も削減します。

RSCN は、配布と非配布の 2 つのモードをサポートしています。 配布モードでは、RSCN は CFS を使用して、ファブリック内のすべてのスイッチに設定を配布します。 非配布モードでは、影響を受けるのはローカル スイッチに対するコンフィギュレーション コマンドだけです。

（注） すべてのコンフィギュレーション コマンドが配布されるわけではありません。 配信されるのは、**rscn event-tov tov vsan vsan** コマンドのみです。

注意 RSCN タイマー設定だけが配布されます。

RSCN タイマーは、初期化およびスイッチオーバーの実行時に CFS に登録されます。 ハイ アベイラビリティを実現するため、RSCN タイマー配布がクラッシュし再起動する場合、またはスイッチオーバーが発生した場合には、クラッシュまたはスイッチオーバーが発生する前の状態から、通常の機能が再開されます。

追加情報については、『*Cisco Nexus 5000 Series System Management Configuration Guide*』の「Using Cisco Fabric Services」を参照してください。

RSCN タイマー設定の配布のイネーブル化

RSCN タイマー設定の配布をイネーブルにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **rscn distribute**
3. switch(config)# **no rscn distribute**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **rscn distribute**	RSCN タイマーの設定の配布をイネーブルにします。
ステップ 3	switch(config)# **no rscn distribute**	RSCN タイマーの配布をディセーブル（デフォルト）にします。

ファブリックのロック

データベースを変更するときの最初のアクションによって、保留中のデータベースが作成され、VSAN 内の機能がロックされます。 ファブリックがロックされると、次のような状況になります。

- 他のユーザがこの機能の設定に変更を加えることができなくなります。
- コンフィギュレーションデータベースのコピーが、最初のアクティブ変更と同時に保留中のデータベースになります。

RSCN タイマー設定の変更のコミット

アクティブ データベースに加えられた変更をコミットする場合、ファブリック内のすべてのスイッチに設定がコミットされます。 コミットが正常に行われると、設定の変更がファブリック全体に適用され、ロックが解除されます。

RSCN タイマー設定の変更をコミットする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **rscn commit vsan** *timeout*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **rscn commit vsan** *timeout*	RSCN タイマーの変更をコミットします。

RSCN タイマー設定の変更の廃棄

保留中のデータベースに加えられた変更を廃棄（中断）する場合、コンフィギュレーション データベースは影響を受けないまま、ロックが解除されます。

RSCN タイマー設定の変更をコミットする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **rscn abort vsan** *timeout*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **rscn abort vsan** *timeout*	RSCN タイマーの変更を廃棄し、保留中のコンフィギュレーション データベースをクリアします。

ロック済みセッションのクリア

RSCN タイマー設定を変更したが、変更をコミットまたは廃棄してロックを解除するのを忘れた場合、管理者はファブリック内の任意のスイッチからロックを解除できます。 管理者がこの操作を行うと、ユーザによる保留データベースの変更は廃棄され、ファブリックのロックは解除されます。

保留中のデータベースは揮発性ディレクトリでだけ有効で、スイッチが再起動されると廃棄されます。

管理者の特権を使用して、ロックされた RSCN セッションを解除するには、EXEC モードで **clear rscn session** コマンドを使用します。 次に、VSAN 10 の RSCN セッションをクリアする例を示します。

```
switch# clear rscn session vsan 10
```

RSCN 設定の配布情報の表示

次に、RSCN 設定の配布の登録ステータスを表示する例を示します。

```
switch# show cfs application name rscn
 Enabled        : Yes
 Timeout        : 5s
 Merge Capable  : Yes
 Scope          : Logical
```

（注） 結合対象のファブリックの RSCN タイマー値が異なる場合、結合は失敗します。

次に、設定のコミット時に有効な一連のコンフィギュレーション コマンドを表示する例を示します。

（注） 保留中のデータベースには、既存設定と変更された設定の両方が含まれます。

```
switch# show rscn pending
rscn event-tov 2000 ms vsan 1
rscn event-tov 2000 ms vsan 2
rscn event-tov 300 ms vsan 10
```

次に、保留中の設定とアクティブな設定の違いを表示する例を示します。

```
switch# show rscn pending-diff vsan 10
- rscn event-tov 2000 ms vsan 10
+ rscn event-tov 300 ms vsan 10
```

デフォルトの RSCN 設定値

次の表に、RSCN のデフォルト設定を示します。

表 *29*：デフォルトの *RSCN* 設定値

パラメータ	デフォルト
RSCN タイマー値	2000 ミリ秒（ファイバ チャネル VSAN）
RSCN タイマー設定の配布	ディセーブル

第 14 章

SCSI ターゲットの検出

この章の内容は、次のとおりです。

- SCSI ターゲットの検出，221 ページ

SCSI ターゲットの検出

SCSI LUN 検出に関する情報

SCSI ターゲットにはディスク、テープ、およびその他のストレージ デバイスが含まれます。 これらのターゲットは、ネーム サーバに論理ユニット番号（LUN）を登録しません。

ネーム サーバには、次の理由により、LUN 情報が必要となります。

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

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

SCSI LUN 検出機能は、CLI（コマンドライン インターフェイス）または SNMP（簡易ネットワーク管理プロトコル）を通して、オンデマンドで開始されます。 近接スイッチが Cisco Nexus 5000 シリーズに属する場合、この情報は近接スイッチとも同期されます。

SCSI LUN 検出の開始について

SCSI LUN 検出はオンデマンドで実行されます。

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

SCSI LUN 検出の開始

SCSI LUN 検出を開始する手順は、次のとおりです。

手順の概要

1. switch# **discover scsi-target** {**custom-list** | **local** | **remote** | **vsan** *vsan-id* **fcid** *fc-id*} **os** {**aix** | **hpux** | **linux** | **solaris** | **windows**} [**lun** | **target**]

手順の詳細

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

SCSI LUN 検出を開始する例

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

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

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

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

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

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

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

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

カスタマイズ検出の開始について

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

カスタマイズ検出の開始

カスタマイズ検出を開始する手順は、次のとおりです。

手順の概要

1. switch# **discover custom-list add vsan** *vsan-id* **domain** *domain-id*
2. switch# **discover custom-list delete vsan** *vsan-id* **domain** *domain-id*

手順の詳細

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

SCSI LUN 情報の表示

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

次に、検出されたターゲットを表示する例を示します。

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

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

次に、FCNS データベースを表示する例を示します。

```
switch# show fcns database
```

次に、SCSI ターゲット ディスクを表示する例を示します。

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

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

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

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

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

第 15 章

拡張ファイバ チャネル機能および概念

この章の内容は、次のとおりです。

- 拡張ファイバ チャネル機能および概念，225 ページ

拡張ファイバ チャネル機能および概念

ファイバ チャネルのタイムアウト値

ファイバ チャネル プロトコルに関連するスイッチのタイマー値を変更するには、次の Time Out 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。

すべての VSAN のタイマー設定

ファイバ チャネル プロトコルに関連するスイッチのタイマー値を変更できます。

注意 D_S_TOV、E_D_TOV、およびR_A_TOV の値は、スイッチのすべての VSAN が一時停止されていないかぎりグローバルに変更できません。

（注） タイマー値を変更するときに VSAN を指定しない場合は、変更された値がスイッチ内のすべての VSAN に適用されます。

すべての VSAN にファイバ チャネル タイマーを設定する手順は、次のとおりです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **fctimer R_A_TOV** *timeout*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fctimer R_A_TOV** *timeout*	すべてのVSANのR_A_TOVタイムアウト値を設定します。単位はミリ秒です。 このタイプの設定は、すべての VSAN が一時停止されていないかぎり、許可されません。

VSAN ごとのタイマー設定

指定された VSAN に fctimer を発行して、ファイバ チャネルなどの特殊なリンクを含む VSAN に別の TOV 値を設定することもできます。 VSAN ごとに異なる E_D_TOV、R_A_TOV、および D_S_TOV 値を設定できます。 アクティブ VSAN のタイマー値を変更すると、VSAN は一時停止されてからアクティブになります。

（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させる必要があります。 ファブリック内のすべてのスイッチに同じ値を設定してください。

VSAN 単位の FC タイマーを設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config#)# **fctimer D_S_TOV** *timeout* **vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config#)# **fctimer D_S_TOV** *timeout* **vsan** *vsan-id*	指定された VSAN の D_S_TOV タイムアウト値（ミリ秒）を設定します。 VSAN が一時的に停止します。 必要に応じて、このコマンドを終了することもできます。

次に、VSAN 2 のタイマー値を設定する例を示します。

```
switch(config#)# fctimer D_S_TOV 6000 vsan 2
Warning: The vsan will be temporarily suspended when updating the timer value This
configuration would impact whole fabric. Do you want to continue? (y/n) y
Since this configuration is not propagated to other switches, please configure the same
value in all the switches
```

fctimer 配信の概要

ファブリック内のすべての Cisco SAN スイッチに対して、VSAN 単位での fctimer のファブリック配布をイネーブルにできます。 fctimer の設定を実行して、配布をイネーブルにすると、ファブリック内のすべてのスイッチにその設定が配布されます。

スイッチの配布をイネーブルにしたあとで最初のコンフィギュレーション コマンドを入力すると、ファブリック全体のロックを自動的に取得します。 fctimer アプリケーションは、有効データベースと保留データベース モデルを使用し、使用中のコンフィギュレーションに基づいてコマンドを格納またはコミットします。

追加情報については、『*Cisco Nexus 5000 Series System Management Configuration Guide*』の「Using Cisco Fabric Services」を参照してください。

fctimer の配布のイネーブル化とディセーブル化

fctimer のファブリック配布をイネーブルまたはディセーブルにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fctimer distribute**
3. switch(config)# **no fctimer distribute**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fctimer distribute**	ファブリック内のすべてのスイッチに対する fctimer 設定の配布をイネーブルにします。 ファブリックのロックを取得して、その後の設定変更をすべて保留データベースに格納します。
ステップ 3	switch(config)# **no fctimer distribute**	ファブリック内のすべてのスイッチに対する fctimer 設定の配布をディセーブル（デフォルト）にします。

fctimer 設定変更のコミット

fctimer の設定変更をコミットすると、有効データベースは保留データベースの設定変更によって上書きされ、ファブリック内のすべてのスイッチが同じ設定を受け取ります。 セッション機能を実行せずに fctimer の設定変更をコミットすると、fctimer 設定は物理ファブリック内のすべてのスイッチに配布されます。

fctimer の設定変更をコミットする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fctimer commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fctimer commit**	ファブリック内のすべてのスイッチに対して fctimer の設定変更を配布し、ロックを解除します。 保留データベースに対する変更を有効データベースに上書きします。

fctimer 設定変更の廃棄

設定変更を加えたあと、変更内容をコミットする代わりに廃棄すると、この変更内容を廃棄できます。 いずれの場合でも、ロックは解除されます。

fctimer の設定変更を廃棄する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fctimer abort**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fctimer abort**	保留データベースの fctimer の設定変更を廃棄して、ファブリックのロックを解除します。

ファブリックのロックの上書き

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

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

管理者特権を使用して、ロックされた fctimer セッションを解除するには、**clear fctimer session** コマンドを使用します。

```
switch# clear fctimer session
```

FABRIC データベースの結合の注意事項

2 つのファブリックを結合する場合は、次の注意事項に従ってください。

- 次の結合条件を確認します。
  - fctimer 値を配布する結合プロトコルが実行されない。 ファブリックを結合する場合、fctimer 値を手動で結合する必要があります。
  - VSAN 単位の fctimer 設定は物理ファブリック内で配布される。
  - fctimer 設定は、変更された fctimer 値を持つ VSAN が含まれるスイッチだけに適用される。
  - グローバルな fctimer 値は配布されない。
- 配布がイネーブルになっている場合は、グローバル タイマーの値を設定しないでください。

（注） 保留できるfctimer設定操作の回数は15回以内です。 15回を超えて設定操作を行う場合には、保留設定をコミットするか、中止する必要があります。

追加情報については、『*Cisco Nexus 5000 Series System Management Configuration Guide*』の「CFS Merge Support」を参照してください。

設定された fctimer 値の確認

設定された fctimer 値を表示するには、**show fctimer** コマンドを使用します。 次の例では、設定されたグローバル TOV が表示されています。

```
switch# show fctimer
F_S_TOV   D_S_TOV   E_D_TOV   R_A_TOV
----------------------------------------
5000 ms   5000 ms   2000 ms   10000 ms
```

（注） **show fctimer** コマンドの出力には、（設定されていない場合でも）F_S_TOV 定数が表示されます。

次の例では、VSAN 10 の設定済み TOV が表示されています。

```
switch# show fctimer vsan 10
vsan no.  F_S_TOV   D_S_TOV   E_D_TOV   R_A_TOV
-------------------------------------------------
10        5000 ms   5000 ms   3000 ms   10000 ms
```

World Wide Names（WWN）

スイッチの World Wide Name（WWN）は、イーサネットの MAC アドレスに相当します。 MAC アドレスと同様に、デバイスごとに WWN を一意に対応付ける必要があります。 主要スイッチを選択するとき、およびドメイン ID を割り当てるときは、WWN を使用します。

Cisco SAN スイッチは、3 つの Network Address Authority（NAA）アドレス フォーマットをサポートします （次の表を参照）。

表 *30*：標準化された *NAA WWN* フォーマット

NAA アドレス	NAA タイプ	WWN フォーマット	
IEEE 48 ビット アドレス	タイプ 1 = 0001b	000 0000 0000b	48 ビット MAC アドレス
IEEE 拡張	タイプ 2 = 0010b	ローカルに割り当て	48 ビット MAC アドレス
IEEE 登録	タイプ 5 = 0101b	IEEE 企業 ID：24 ビット	VSID：36 ビット

注意　WWN の変更は、管理者または、スイッチの操作に精通した担当者が実行してください。

WWN 情報の確認

WWN 設定のステータスを表示するには、**show wwn** コマンドを使用します。 次に、すべての WWN のステータスを表示する例を示します。

```
switch# show wwn status
Type    Configured     Available    Resvd.  Alarm State
----    ----------  --------------  ------  -----------
   1           64        48 ( 75%)      16    NONE
 2,5       524288    442368 ( 84%)   73728    NONE
```

次に、ブロック ID 51 の情報を表示する例を示します。

```
switch# show wwn status block-id 51
WWNs in this block: 21:00:ac:16:5e:52:00:03 to 21:ff:ac:16:5e:52:00:03
Num. of WWNs:: Configured: 256 Allocated:    0 Available: 256

Block Allocation Status: FREE
```

次に、特定のスイッチにおける WWN を表示する例を示します。

```
switch# show wwn switch
Switch WWN is 20:00:ac:16:5e:52:00:00
```

リンク初期化 WWN の使用方法

Exchange Link Protocol（ELP）および Exchange Fabric Protocol（EFP）は、リンク初期化の際に WWN を使用します。 ELP と EFP はどちらも、デフォルトでは、リンク初期化時に VSAN WWN を使用します。 ただし、ELP の使用方法はピア スイッチの使用方法に応じて変わります。

- ピア スイッチの ELP がスイッチの WWN を使用する場合、ローカル スイッチもスイッチの WWN を使用します。
- ピア スイッチの ELP が VSAN の WWN を使用する場合、ローカル スイッチも VSAN の WWN を使用します。

セカンダリ MAC アドレスの設定

セカンダリ MAC アドレスを割り当てる手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **wwn secondary-mac** *wwn-id* **range** *value*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **wwn secondary-mac** *wwn-id* **range** *value*	セカンダリ MAC アドレスを設定します。 このコマンドは元に戻せません。

次に、セカンダリ MAC アドレスを設定する例を示します。

```
switch(config)# wwn secondary-mac 00:99:55:77:55:55 range 64
This command CANNOT be undone.
Please enter the BASE MAC ADDRESS again: 00:99:55:77:55:55
Please enter the mac address RANGE again: 64
From now on WWN allocation would be based on new MACs. Are you sure? (yes/no) no
You entered: no. Secondary MAC NOT programmed
```

HBA の FC ID 割り当て

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

一部の Host Bus Adapter（HBA）は、ドメインとエリアが同じ FC ID を持つターゲットを検出しません。 スイッチ ソフトウェアは、この動作が発生しないテスト済みの企業 ID のリストを保持しています。 これらの HBA には単一の FC ID が割り当てられます。 HBA が同じドメインおよびエリア内のターゲットを検出できる場合、完全なエリアが割り当てられます。

多数のポートを持つスイッチのスケーラビリティを高めるため、スイッチ ソフトウェアは、同じドメインおよびエリア内のターゲットを検出できる HBA のリストを維持しています。 ファブリック ログインの間、pWWN で使用される企業 ID（Organizational Unique Identifier [OUI; 組織固有識別子] としても知られる）によってそれぞれの HBA が識別されます。 エリア全体が、リストされている企業 ID を持つ N ポートに割り当てられ、残りには、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（エリア全体または単一）に関係なく、FC ID エントリは永続的です。

デフォルトの企業 ID リスト

すべての Cisco SAN スイッチには、エリア割り当てが必要な企業 ID のデフォルト リストが含まれています。 この企業 ID を使用すると、設定する永続的 FC ID エントリの数が少なくなります。 これらのエントリは、CLI を使用して設定または変更できます。

注意 永続的エントリは、企業 ID の設定よりも優先されます。HBA がターゲットを検出しない場合は、HBA とターゲットが同じスイッチに接続され、FC ID のエリアが同じであることを確認してから、次の手順を実行します。

1. HBA に接続されているポートをシャットダウンします。
2. 永続的 FC ID エントリをクリアします。
3. ポート WWN から企業 ID を取得します。
4. エリア割り当てを必要とするリストに企業 ID を追加します。
5. ポートをアップにします。

企業 ID のリストには、次の特性があります。

- 永続的 FC ID の設定は常に企業 ID リストよりも優先されます。 エリアを受け取るように企業 ID が設定されている場合でも、永続的 FC ID の設定によって単一の FC ID が割り当てられます。
- 後続のリリースに追加される新規の企業 ID は、既存の企業 ID に自動的に追加されます。
- 企業 ID のリストは、実行コンフィギュレーションおよび保存されたコンフィギュレーションの一部として保存されます。
- 企業 ID のリストが使用されるのは、fcinterop の FC ID 割り当て方式が auto モードの場合だけです。 変更されないかぎり、interop の FC ID 割り当ては、デフォルトで auto に設定されています。

  ヒント fcinterop の FC ID 割り当て方式を auto に設定し、企業 ID リストと永続的 FC ID 設定を使用して、FC ID のデバイス割り当てを行うことをお勧めします。

  FC ID の割り当てを変更するには、**fcinterop FCID allocation auto** コマンドを使用し、現在割り当てられているモードを表示するには、**show running-config** コマンドを使用します。
- **write erase** を入力すると、リストは該当するリリースに付属している企業 ID のデフォルトリストを継承します。

企業 ID を割り当てる手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcid-allocation area company-id** *value*
3. switch(config)# **no fcid-allocation area company-id** *value*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcid-allocation area company-id** *value*	デフォルト リストに新しい企業 ID を追加します。
ステップ 3	switch(config)# **no fcid-allocation area company-id** *value*	デフォルト リストから企業 ID を削除します。

次に、デフォルト リストに新しい企業 ID を追加する例を示します。

```
switch(config)# fcid-allocation area company-id 0x003223
```

企業 ID の設定の確認

設定された企業 ID を表示するには、**show fcid-allocation area** コマンドを使用します。 最初にデフォルトエントリが表示され、次にユーザによって追加されたエントリが表示されます。エントリがデフォルト リストの一部で、あとで削除された場合でも、エントリは表示されます。

次に、デフォルトおよび設定された企業 ID のリストを表示する例を示します。

```
switch# show fcid-allocation area
FCID area allocation company id info:
00:50:2E <--------------- Default entry
00:50:8B
00:60:B0
00:A0:B8
00:E0:69
00:30:AE + <------------- User-added entry
00:32:23 +
00:E0:8B * <------------- Explicitly deleted entry (from the original default list)
Total company ids: 7
+ - Additional user configured company ids.
* - Explicitly deleted company ids from default list.
```

削除済みエントリの印が付いていない企業IDのリストを組み合わせると、特定のリリースに付属するデフォルト エントリを暗黙的に導き出すことができます。

また、**show fcid-allocation company-id-from-wwn** コマンドを使用すると、特定の WWN の企業 ID を表示または取得することもできます。 一部の WWN 形式では、企業 ID がサポートされていません。 この場合、FC ID の永続的エントリを設定する必要があります。

次に、指定された WWN の企業 ID を表示する例を示します。

```
switch# show fcid-allocation company-id-from-wwn 20:00:00:05:30:00:21:60
Extracted Company ID: 0x000530
```

スイッチの相互運用性

相互運用性を使用すると、複数ベンダーによる製品の間で相互に通信することができます。 ファイバ チャネル標準規格では、ベンダーに対して共通の外部ファイバ チャネル インターフェイスを使用することを推奨しています。

同じ方法で標準規格に準拠していないベンダーもあるため、相互運用モードが必要になります。ここでは、これらのモードの基本的な概念について簡単に説明します。

各ベンダーには標準モード、および同等の相互運用モードがあります。相互運用モードでは拡張機能または独自の機能が無効になり、標準に準拠した実装が可能になります。

（注） Cisco Nexus 5000 シリーズスイッチでの相互運用性の設定方法に関する詳細は、『*Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*』を参照してください。

Interop モードの概要

ソフトウェアは、次の 4 つの interop モードをサポートします。

- モード 1：標準ベースの interop モード。ファブリック内の他のベンダー製品もすべて interop モードになっている必要があります。
- モード 2：Brocade ネイティブ モード（Core PID 0）
- モード 3：Brocade ネイティブ モード（Core PID 1）
- モード 4：McData ネイティブ モード

interop モード 2、3、および 4 の設定方法については、次から入手できる『*Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*』を参照してください。http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/interoperability/guide/intopgd.html

次の表に、相互運用性モードを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 Cisco Nexus 5000 シリーズ スウィッチに固有の変更点です。

表 *31*：相互運用モードがイネーブルの場合のスイッチ動作の変更点

スイッチ機能	相互運用モードがイネーブルの場合の変更点
ドメイン ID	一部のベンダーは、ファブリック内の 239 のドメインを完全には使用できません。 ドメイン ID は 97 ～ 127 の範囲に制限されます。これは、McData の公称制限をこの範囲内に収めるためです。 ドメイン ID は Static または Preferred に設定できます。それぞれの動作は次のとおりです。 • Static：シスコ スイッチは 1 つのドメイン ID だけを受け入れ、そのドメイン ID を取得できない場合には、ファブリックから隔離します。 • Preferred：スイッチが要求したドメイン ID を取得できない場合、割り当てられた任意のドメインを受け入れます。
タイマー	ISL（スイッチ間リンク）を確立するときにファイバ チャネル タイマー値が E ポートで交換されるので、すべてのスイッチでこれらのタイマーをすべて同じにする必要があります。 タイマーには、F_S_TOV、D_S_TOV、E_D_TOV、および R_A_TOV があります。
F_S_TOV	Fabric Stability TOV タイマーが正確に一致するかどうかを確認してください。
D_S_TOV	Distributed Services TOV タイマーが正確に一致するかどうかを確認してください。
E_D_TOV	Error Detect TOV タイマーが正確に一致するかどうかを確認してください。
R_A_TOV	Resource Allocation TOV タイマーが正確に一致するかどうかを確認してください。
トランキング	2 つの異なるベンダー製のスイッチ間では、トランキングはサポートされません。 この機能はポート単位、またはスイッチ単位でディセーブルに設定できます。

スイッチ機能	相互運用モードがイネーブルの場合の変更点
デフォルト ゾーン	ゾーンのデフォルトの許可動作（すべてのノードから他のすべてのノードを認識可能）または拒否動作（明示的にゾーンに配置されていないすべてのノードが隔離される）は変更できます。
ゾーン分割属性	ゾーンを pWWN に制限したり、その他の独自のゾーン分割方式（物理ポート番号）を除去することができます。 （注） Brocade スイッチでは、**cfgsave**コマンドを使用して、ファブリック全体のゾーン分割設定を保存します。 このコマンドは、同じファブリックに属する Cisco SAN スイッチには影響しません。 各 Cisco SAN スイッチで明示的に設定を保存する必要があります。
ゾーンの伝播	一部のベンダーは、他のスイッチに完全なゾーン設定を受け渡さないで、アクティブ ゾーンセットだけを受け渡します。 ファブリック内の他のスイッチにアクティブ ゾーンセットまたはゾーン設定が正しく伝播されたかどうかを確認してください。
VSAN	interop モードは、指定された VSAN にだけ有効です。 （注） interop モードは、FICON 対応の VSAN で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 スイッチと Cisco SAN 以外のスイッチを接続する場合は、TE ポートおよび SAN ポート チャネルを使用できません。 Cisco SAN 以外のスイッチに接続できるのは、Eポートだけです。interop モードの場合でも、TE ポートおよび SAN ポート チャネルを使用すると、シスコ スイッチをほかの Cisco SAN スイッチに接続することができます。
FSPF	interop モードにしても、ファブリック内のフレームのルーティングは変更されません。 スイッチは引き続き src-id、dst-id、および ox-id を使用して、複数の ISL リンク間でロードバランスします。

スイッチ機能	相互運用モードがイネーブルの場合の変更点
ドメインの中断再設定	これは、スイッチ全体に影響するイベントです。 Brocade および McData では、ドメイン ID を変更するときにスイッチ全体をオフライン モードにしたり、再起動したりする必要があります。
ドメインの非中断再設定	これは、関連する VSAN に限定されるイベントです。 Cisco SAN スイッチには、スイッチ全体ではなく、影響を受ける VSAN のドメイン マネージャ プロセスのみを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かを確認してください。

interop モード 1 の設定

Cisco SAN スイッチの interop モード 1 のイネーブル化は、中断を伴うかまたは中断を伴わずに行うことができます。

（注） Brocade スイッチから Cisco SAN スイッチまたは McData スイッチに接続する前に、Brocade の **msplmgmtdeactivate** コマンドを明示的に実行する必要があります。 このコマンドは Brocade 独自のフレームを使用して、Cisco SAN スイッチまたは McData スイッチが認識しないプラットフォーム情報を交換します。 これらのフレームを拒否すると、一般的な E ポートが隔離されます。

interop モード 1 を設定するには、次の作業を行います。

手順の概要

1. 他ベンダー製スイッチに接続する E ポートの VSAN を相互運用モードにします。
2. 97（0x61）～ 127（0x7F）の範囲でドメイン ID を割り当てます。
3. FC タイマーを変更します（システム デフォルトから変更された場合）。
4. ドメインを変更するときに、変更された VSAN のドメイン マネージャ機能の再起動が必要な場合と、不要な場合があります。

手順の詳細

ステップ 1 他ベンダー製スイッチに接続する E ポートの VSAN を相互運用モードにします。

```
switch# configuration terminal
switch(config)# vsan database
switch(config-vsan-db)# vsan 1 interop 1
switch(config-vsan-db)# exit
```

ステップ 2 97（0x61）～ 127（0x7F）の範囲でドメイン ID を割り当てます。

（注） これは、McData スイッチに適用される制限です。

Cisco SAN スイッチの場合、デフォルトでは、主要スイッチから ID が要求されます。 Preferred オプションを使用した場合、Cisco SAN スイッチは固有の ID を要求しますが、主要スイッチから別の ID が割り当てられた場合もファブリックに加入します。 Static オプションを使用した場合、要求された ID を主要スイッチが承認して、これを割り当てない限り、Cisco SAN スイッチはファブリックに参加しません。

（注） ドメイン ID を変更すると、N ポートに割り当てられた FC ID も変更されます。

ステップ 3 FC タイマーを変更します（システム デフォルトから変更された場合）。

（注） Cisco SAN スイッチ、Brocade、McData FC Error Detect（ED_TOV）、および Resource Allocation（RA_TOV）の各タイマーは、同じ値にデフォルト設定されています。 これらの値は、必要に応じて変更できます。 RA_TOV のデフォルト値は 10 秒、ED_TOV のデフォルト値は 2 秒です。 FC-SW2 標準に基づく場合、これらの値は、ファブリック内の各スイッチで一致している必要があります。

```
switch(config)# fctimer e_d_tov ?
  <1000-100000> E_D_TOV in milliseconds(1000-100000)

switch(config)# fctimer r_a_tov ?
  <5000-100000> R_A_TOV in milliseconds(5000-100000)
```

ステップ 4 ドメインを変更するときに、変更された VSAN のドメイン マネージャ機能の再起動が必要な場合と、不要な場合があります。

- **disruptive** オプションを使用して、ファブリックを強制的に再設定する場合は次のようになります。

```
switch(config)# fcdomain restart disruptive vsan 1
```

または

- ファブリックを強制的に再設定しない場合は次のようになります。

```
switch(config# fcdomain restart vsan 1
```

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、相互運用モードで稼働していることを確認するためのコマンドについて説明します。

Cisco Nexus 5000 シリーズの任意のスイッチで相互運用性コマンドを入力した場合のステータスを確認する手順は、次のとおりです。

手順の概要

1. ソフトウェア バージョンを確認します。
2. インターフェイスの状態が使用中の設定に必要な状態になっているかどうかを確認します。
3. 目的のコンフィギュレーションが稼働しているかどうかを確認します。
4. 相互運用性モードがアクティブであるかどうかを確認します。
5. ドメイン ID を確認します。
6. ローカル主要スイッチのステータスを確認します。
7. スイッチのネクスト ホップおよび宛先を確認します。
8. ネーム サーバ情報を確認します。

手順の詳細

ステップ 1 ソフトウェア バージョンを確認します。

例：

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software

TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2008, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.

Some parts of this software are covered under the GNU Public

License. A copy of the license is available at

http://www.gnu.org/licenses/gpl.html.

Software
  BIOS:      version 1.2.0
  loader:    version N/A
  kickstart: version 4.0(1a)N1(1)
  system:    version 4.0(1a)N1(1)
  BIOS compile time:       06/19/08
  kickstart image file is: bootflash:/n5000-uk9-kickstart.4.0.1a.N1.latest.bin
  kickstart compile time:  11/25/2008 6:00:00 [11/25/2008 14:17:12]
  system image file is:    bootflash:/n5000-uk9.4.0.1a.N1.latest.bin
  system compile time:     11/25/2008 6:00:00 [11/25/2008 14:59:49]
Hardware
  cisco Nexus5020 Chassis ("40x10GE/Supervisor")
  Intel(R) Celeron(R) M CPU with 2074308 kB of memory.
  Processor Board ID JAB120900PJ
  Device name: switch
  bootflash: 1003520 kB
```

```
Kernel uptime is 0 day(s), 1 hour(s), 29 minute(s), 55 second(s)

Last reset at 510130 usecs after Wed Nov 26 18:12:23 2008
  Reason: Reset Requested by CLI command reload
  System version: 4.0(1a)N1(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin
```

ステップ 2 インターフェイスの状態が使用中の設定に必要な状態になっているかどうかを確認します。

例：

```
switch# show interface brief

--------------------------------------------------------------------------------

Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port

                  Mode   Trunk                          Mode  Speed  Channel

                         Mode                                 (Gbps)

--------------------------------------------------------------------------------

fc3/1      1      E      on      trunking        swl    TE      2    --

fc3/2      1      auto   on      sfpAbsent       --     --           --

fc3/3      1      E      on      trunking        swl    TE      2    --

fc3/4      1      auto   on      sfpAbsent       --     --           --

fc3/5      1      auto   auto    notConnected    swl    --           --

fc3/6      1      auto   on      sfpAbsent       --     --           --

fc3/7      1      auto   auto    sfpAbsent       --     --           --

fc3/8      1      auto   auto    sfpAbsent       --     --           --
```

ステップ 3 目的のコンフィギュレーションが稼働しているかどうかを確認します。

例：

```
switch# show running-config

Building Configuration...

 interface fc2/1

no shutdown

 interface fc2/2

no shutdown

 interface fc2/3

 interface fc2/4
```

<省略>

```
interface mgmt0

ip address 6.1.1.96 255.255.255.0

switchport encap default
```

```
no shutdown
vsan database
vsan 1 interop
boot system bootflash:/nx5000-system-23e.bin
boot kickstart bootflash:/nx5000-kickstart-23e.bin
callhome
fcdomain domain 100 preferred vsan 1
ip route 6.1.1.0 255.255.255.0 6.1.1.1
ip routing
line console
  databits 5
  speed 110
logging linecard
ssh key rsa 512 force
ssh server enable
switchname switch
username admin password 5 $1$Li8/fBYX$SNc72.xt4nTXpSnR9OUFB/ role network-admin
```

ステップ 4 相互運用性モードがアクティブであるかどうかを確認します。

例：

```
switch# show vsan 1
vsan 1 information
         name:VSAN0001  state:active
         interoperability mode:yes <---------------------- verify mode
         loadbalancing:src-id/dst-id/oxid
         operational state:up
```

ステップ 5 ドメイン ID を確認します。

例：

```
switch# show fcdomain vsan 1
The local switch is a Subordinated Switch.
Local switch run time information:
        State: Stable
        Local switch WWN:    20:01:00:05:30:00:51:1f
        Running fabric name: 10:00:00:60:69:22:32:91
        Running priority: 128
```

```
        Current domain ID: 0x64(100) <---------------verify domain id
Local switch configuration information:
        State: Enabled
        Auto-reconfiguration: Disabled
        Contiguous-allocation: Disabled
        Configured fabric name: 41:6e:64:69:61:6d:6f:21
        Configured priority: 128
        Configured domain ID: 0x64(100) (preferred)
Principal switch run time information:
        Running priority: 2
Interface               Role          RCF-reject
----------------    -------------    ------------
fc2/1               Downstream       Disabled
fc2/2               Downstream       Disabled
fc2/4               Upstream         Disabled
----------------    -------------    ------------
```

ステップ 6 ローカル主要スイッチのステータスを確認します。

例：

```
switch# show fcdomain domain-list vsan 1
Number of domains: 5
Domain ID              WWN
---------    ------------------------
 0x61(97)    10:00:00:60:69:50:0c:fe
 0x62(98)    20:01:00:05:30:00:47:9f
 0x63(99)    10:00:00:60:69:c0:0c:1d
0x64(100)    20:01:00:05:30:00:51:1f [Local]
0x65(101)    10:00:00:60:69:22:32:91 [Principal]
---------    ------------------------
```

ステップ 7 スイッチのネクスト ホップおよび宛先を確認します。

例：

```
switch# show fspf internal route vsan 1
FSPF Unicast Routes
---------------------------
 VSAN Number  Dest Domain   Route Cost    Next hops
```

```
-----------------------------------------------
           1     0x61(97)          500      fc2/2
           1     0x62(98)         1000      fc2/1
                                            fc2/2
           1     0x63(99)          500      fc2/1
           1    0x65(101)         1000      fc2/4
```

ステップ 8 ネーム サーバ情報を確認します。

例：

```
switch# show fcns data vsan 1

VSAN 1:

-----------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR) FC4-TYPE:FEATURE
-----------------------------------------------------------------------
0x610400    N     10:00:00:00:c9:24:3d:90 (Emulex)     scsi-fcp
0x6105dc    NL    21:00:00:20:37:28:31:6d (Seagate)    scsi-fcp
0x6105e0    NL    21:00:00:20:37:28:24:7b (Seagate)    scsi-fcp
0x6105e1    NL    21:00:00:20:37:28:22:ea (Seagate)    scsi-fcp
0x6105e2    NL    21:00:00:20:37:28:2e:65 (Seagate)    scsi-fcp
0x6105e4    NL    21:00:00:20:37:28:26:0d (Seagate)    scsi-fcp
0x630400    N     10:00:00:00:c9:24:3f:75 (Emulex)     scsi-fcp
0x630500    N     50:06:01:60:88:02:90:cb              scsi-fcp
0x6514e2    NL    21:00:00:20:37:a7:ca:b7 (Seagate)    scsi-fcp
0x6514e4    NL    21:00:00:20:37:a7:c7:e0 (Seagate)    scsi-fcp
0x6514e8    NL    21:00:00:20:37:a7:c7:df (Seagate)    scsi-fcp
0x651500    N     10:00:00:e0:69:f0:43:9f (JNI)

Total number of entries = 12
```

（注） シスコ スイッチ ネーム サーバにはローカル エントリおよびリモート エントリが表示され、エントリはタイムアウトしません。

拡張機能のデフォルト設定値

次の表に、この章で説明した機能のデフォルト設定を示します。

表 *32*：拡張機能のデフォルト設定値

パラメータ	デフォルト
CIM サーバ	ディセーブル
CIM サーバ セキュリティ プロトコル	HTTP
D_S_TOV	5,000 ミリ秒
E_D_TOV	2,000 ミリ秒
R_A_TOV	10,000 ミリ秒
fctrace を呼び出すタイムアウト時間	5 秒
fcping 機能によって送信されるフレーム数	5 フレーム
リモート キャプチャ接続プロトコル	TCP
リモート キャプチャ接続モード	パッシブ
ローカル キャプチャ フレーム制限	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

第 16 章

FC-SP および DHCHAP の設定

この章の内容は、次のとおりです。

- FC-SP および DHCHAP の設定，247 ページ

FC-SP および DHCHAP の設定

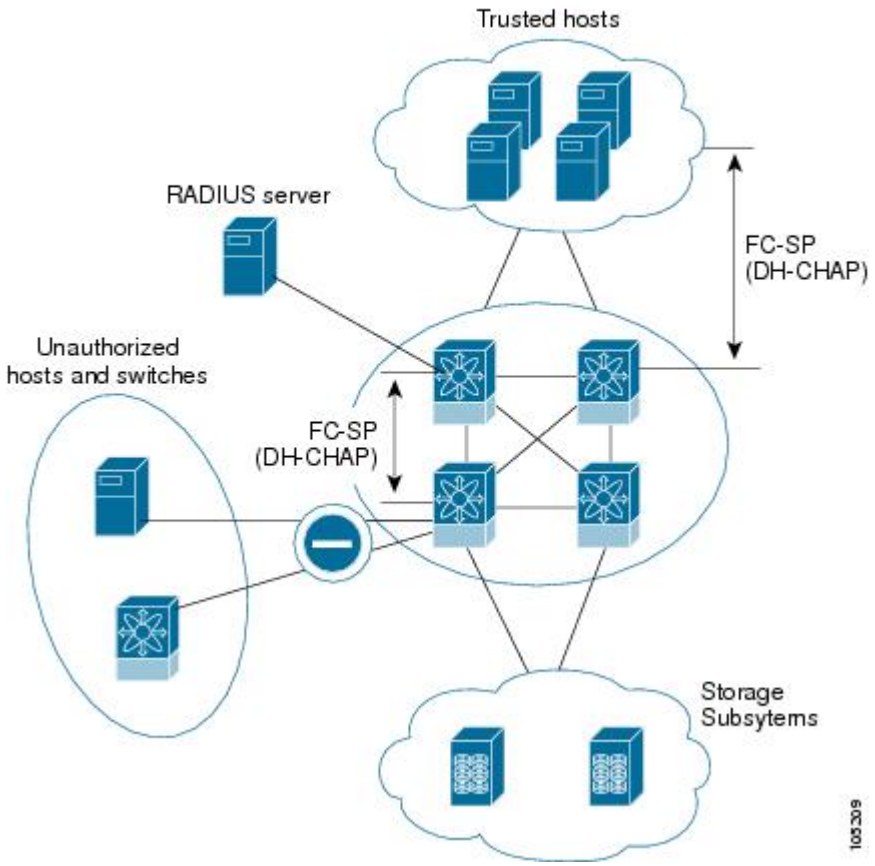
Fibre Channel Security Protocol（FC-SP）機能は、スイッチとスイッチ間およびホストとスイッチ間で認証を実行して、企業全体のファブリックに関するセキュリティ問題を解決します。Diffie-Hellman チャレンジハンドシェイク認証プロトコル（DHCHAP）は、Cisco SAN スイッチとその他のデバイス間で認証を行う FC-SP プロトコルです。 DHCHAP は、CHAP プロトコルと Diffie-Hellman 交換を組み合わせて構成されています。

ファブリック認証に関する情報

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

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

図 *41*： スイッチおよびホストの認証



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

DHCHAP

DHCHAP は、スイッチに接続している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 という用語を共通の意味で使用しています。

DHCHAP は、必須のパスワードに基づくキー交換による認証プロトコルであり、スイッチ間およびホスト スイッチ間の認証をサポートします。 DHCHAP はハッシュ アルゴリズムおよび DH グループをネゴシエートしてから、認証を実行します。 また、MD5 および 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する DHCHAP 認証の設定手順は、次のとおりです。

手順の概要

1. DHCHAP をイネーブルにします。
2. DHCHAP 認証モードを識別して設定します。
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。
4. ローカル スイッチおよびファブリックの他のスイッチの DHCHAP パスワードを設定します。
5. 再認証の DHCHAP タイムアウト値を設定します。
6. DHCHAP の設定を確認します。

手順の詳細

ステップ 1 DHCHAP をイネーブルにします。
ステップ 2 DHCHAP 認証モードを識別して設定します。
ステップ 3 ハッシュ アルゴリズムおよび DH グループを設定します。
ステップ 4 ローカル スイッチおよびファブリックの他のスイッチの DHCHAP パスワードを設定します。
ステップ 5 再認証の DHCHAP タイムアウト値を設定します。
ステップ 6 DHCHAP の設定を確認します。

ファイバ チャネル機能と DHCHAP の互換性

ここでは、DHCHAP 機能を既存の Cisco NX-OS 機能と一緒に設定した場合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 レベルではなく、物理インターフェイス レベルで実行されます。
- ポート セキュリティまたはファブリック バインディング：ファブリック バインディング ポリシーは、DHCHAP によって認証される ID に基づいて実行されます。
- VSAN：DHCHAP 認証は、VSAN 単位では実行されません。

DHCHAP イネーブル化の概要

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

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

DHCHAP のイネーブル化

Cisco Nexus 5000 シリーズ スイッチ用の DHCHAP をイネーブルにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcsp enable**
3. switch(config)# **no fcsp enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcsp enable**	このスイッチ上でDHCHAP をイネーブルにします。
ステップ 3	switch(config)# **no fcsp enable**	このスイッチ上でDHCHAP をディセーブル（デフォルト）にします。

DHCHAP 認証モードの概要

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

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

- On：接続元デバイスがDHCHAP認証をサポートしている場合、スイッチ初期化中に認証シーケンスが実行されます。 接続元デバイスが DHCHAP 認証をサポートしていない場合には、リンクが分離状態になります。
- auto-Active：接続元デバイスがDHCHAP認証をサポートしている場合、スイッチ初期化中に認証シーケンスが実行されます。 接続元デバイスが DHCHAP 認証をサポートしていない場合には、ソフトウェアにより、初期化シーケンスの残りが実行されます。

- auto-Passive（デフォルト）：スイッチは DHCHAP 認証を開始しませんが、接続元デバイスが DHCHAP 認証を開始すれば、DHCHAP 認証に参加します。
- Off：スイッチは DHCHAP 認証をサポートしません。 このモードでポートに認証メッセージが送信された場合、開始元スイッチにエラー メッセージが戻されます。

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

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

表 *33*：*2* 台の *SAN* スイッチ間の *DHCHAP* 認証ステータス

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

DHCHAP モードの設定

特定のインターフェイスの DHCHAP モードを設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **interface fc** *slot*/*port* - *slot*/*port*
3. switch(config-if)# **fcsp on**
4. switch(config-if)# **no fcsp on**
5. switch(config-if)# **fcsp auto-active 0**
6. switch(config-if)# **fcsp auto-active** *timeout-period*
7. switch(config-if)# **fcsp auto-active**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface fc** *slot*/*port* - *slot*/*port*	インターフェイスの範囲を選択し、インターフェイス コンフィギュレーション モードに入ります。
ステップ 3	switch(config-if)# **fcsp on**	選択したインターフェイスの DHCHAP モードを on ステートに設定します。
ステップ 4	switch(config-if)# **no fcsp on**	これら 3 つのインターフェイスを出荷時デフォルトの auto-passive に戻します。
ステップ 5	switch(config-if)# **fcsp auto-active 0**	選択したインターフェイスの DHCHAP 認証モードを auto-active に変更します。 0 は、ポートが再認証を実行しないことを表します。 （注） 再許可インターバル設定は、デフォルトの動作と同じです。
ステップ 6	switch(config-if)# **fcsp auto-active** *timeout-period*	選択したインターフェイスの DHCHAP 認証モードを auto-active に変更します。タイムアウト期間の値（分）では、最初の認証後の再認証の頻度を設定します。
ステップ 7	switch(config-if)# **fcsp auto-active**	選択したインターフェイスの DHCHAP 認証モードを auto-active に変更します。 再認証はディセーブルになります（デフォルト）。 （注） 再許可インターバル設定は、0 に設定した場合と同じです。

DHCHAP ハッシュ アルゴリズムの概要

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

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

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

DHCHAP ハッシュ アルゴリズムの設定

ハッシュ アルゴリズムを設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcsp dhchap hash** [**md5**] [**sha1**]
3. switch(config)# **no fcsp dhchap hash sha1**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcsp dhchap hash** [**md5**] [**sha1**]	MD5 または SHA-1 ハッシュ アルゴリズムを使用するように設定します。
ステップ 3	switch(config)# **no fcsp dhchap hash sha1**	出荷時デフォルトのハッシュ アルゴリズム プライオリティ リスト（最初に MD5、次に SHA-1）に戻します。

DHCHAP グループ設定の概要

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

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

DHCHAP グループの設定

DH グループの設定を変更する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcsp dhchap dhgroup** [**0** | **1** | **2** | **3** | **4**]
3. switch(config)# **no fcsp dhchap dhgroup** [**0** | **1** | **2**| **3** | **4**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcsp dhchap dhgroup** [**0** | **1** | **2** | **3** | **4**]	DH グループを設定された順序で使用するようにプライオリティ リスト化します。
ステップ 3	switch(config)# **no fcsp dhchap dhgroup** [**0** | **1** | **2**| **3** | **4**]	DHCHAP の出荷時デフォルトの順序（0、4、1、2、3）に戻します。

DHCHAP パスワードの概要

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

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

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

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

ローカル スイッチの DHCHAP パスワードの設定

ローカル スイッチの DHCHAP パスワードを設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcsp dhchap password** [**0** | **7**] *password* [**wwn** *wwn-id*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcsp dhchap password** [**0** | **7**] *password* [**wwn** *wwn-id*]	ローカル スイッチのクリアテキスト パスワードを設定します。

リモート デバイスのパスワード設定の概要

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 やデバイス WWN といったデバイス名で表されます。 パスワードは 64 文字に制限され、クリア テキスト（0）または暗号化テキスト（7）で指定できます。

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

リモート デバイスの DHCHAP パスワードの設定

ファブリック内の他のスイッチのリモート DHCHAP パスワードをローカル側で設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcsp dhchap devicename** *switch-wwn* **password** *password*
3. switch(config)# **no fcsp dhchap devicename** *switch-wwn* **password** *password*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcsp dhchap devicename** *switch-wwn* **password** *password*	スイッチWWNデバイス名で表される、ファブリック上の他のスイッチのパスワードを設定します。
ステップ 3	switch(config)# **no fcsp dhchap devicename** *switch-wwn* **password** *password*	ローカル認証データベースから、このスイッチのパスワード エントリを削除します。

DHCHAP タイムアウト値の概要

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

タイムアウト値を変更する場合には、次の要因について考慮してください。

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

DHCHAP タイムアウト値の設定

DHCHAP タイムアウト値を設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcsp timeout** *timeout*
3. switch(config)# **no fcsp timeout** *timeout*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcsp timeout** *timeout*	再認証タイムアウトを指定された値に設定します。単位は秒です。

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

DHCHAP AAA 認証の設定

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

プロトコル セキュリティ情報の表示

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

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

```
switch# show fcsp interface fc2/4
fc2/4:
        fcsp authentication mode:SEC_MODE_ON
        Status: Successfully authenticated
```

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

```
switch# show fcsp interface fc2/4 statistics
```

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

```
switch# show fcsp interface fc2/1 wwn
```

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

```
switch# show fcsp dhchap
```

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

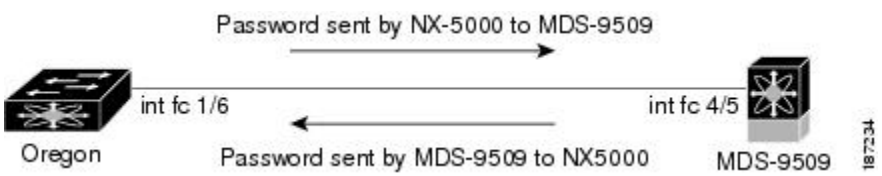
```
switch# show fcsp dhchap database
```

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

設定例

ここでは、次の図に示した例を設定するための手順について説明します。

図 *42* : *DHCHAP* 認証の例



認証を設定するには、次の作業を行います。

手順の概要

1. ファブリックの Cisco SAN スイッチのデバイス名を取得します。 ファブリックの Cisco SAN スイッチは、スイッチ WWN によって識別されます。
2. このスイッチで DHCHAP を明示的にイネーブルにします。
3. このスイッチのクリア テキスト パスワードを設定します。 このパスワードは、接続先デバイスで使用されます。
4. スイッチWWNデバイス名で表される、ファブリック上の他のスイッチのパスワードを設定します。
5. 必要なインターフェイスの DHCHAP モードをイネーブルにします。
6. DHCHAP ローカル パスワード データベースを表示して、このスイッチに設定されたプロトコル セキュリティ情報を確認します。
7. インターフェイスの DHCHAP 設定を表示します。
8. 接続スイッチでこれらの手順を繰り返します。

手順の詳細

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

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

ステップ 2 このスイッチで DHCHAP を明示的にイネーブルにします。

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

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

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

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

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

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

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

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

例：
```
switch(config)# interface fc2/4
switch(config-if)# fcsp on
```

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

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

ステップ 7 インターフェイスの DHCHAP 設定を表示します。

例：
```
switch# show fcsp interface fc2/4
fc2/4
        fcsp authentication mode:SEC_MODE_ON
        Status:Successfully authenticated
```

ステップ 8 接続スイッチでこれらの手順を繰り返します。

例：
```
MDS-9509# show wwn switch
Switch WWN is 20:00:00:05:30:00:38:5e
MDS-9509(config)# fcsp enable
MDS-9509(config)# fcsp dhchap password rtp9509
MDS-9509(config)# fcsp dhchap devicename 20:00:00:05:30:00:54:de password rtp9216
MDS-9509(config)# interface fc 4/5
MDS-9509(config-if)# fcsp on
MDS-9509# show fcsp dhchap database
DHCHAP Local Password:
        Non-device specific password:*******
Other Devices' Passwords:
        Password for device with WWN:20:00:00:05:30:00:54:de is *******
MDS-9509# show fcsp interface fc2/4
Fc2/4
        fcsp authentication mode:SEC_MODE_ON
        Status:Successfully authenticated
```

これで、設定例用の DHCHAP 認証が設定およびイネーブルにされました。

デフォルトのファブリック セキュリティ設定値

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

表 *34*：デフォルトのファブリック セキュリティ設定値

パラメータ	デフォルト
DHCHAP 機能	ディセーブル

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

第 17 章

ポート セキュリティの設定

この章の内容は、次のとおりです。

- ポート セキュリティの設定，261 ページ

ポート セキュリティの設定

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

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

ポート セキュリティについて

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

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

ポート セキュリティの実行

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

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

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

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

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

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

自動学習の概要

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

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

学習は、既存の設定済みのポートセキュリティ ポリシーを上書きしません。たとえば、インターフェイスが特定の pWWN を許可するように設定されている場合、自動学習がエントリを追加して、そのインターフェイス上の他の pWWN を許可することはありません。 他のすべての pWWN は、自動学習モードであってもブロックされます。

シャットダウン状態のポートについては、学習エントリは作成されません。

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

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

ポート セキュリティのアクティブ化

デフォルトでは、ポート セキュリティ機能はアクティブにされていません。

ポート セキュリティ機能をアクティブにすると、次のようになります。

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

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

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

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

ポート セキュリティの設定

自動学習と CFS 配信を使用するポート セキュリティの設定

自動学習とCFS配信を使用する場合にポート セキュリティを設定するには、次の手順に従ってください。

手順の概要

1. ポート セキュリティをイネーブルにします。
2. CFS 配信をイネーブルにします。
3. 各 VSAN で、ポート セキュリティをアクティブにします。
4. CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。
5. すべてのスイッチとすべてのホストが自動的に学習されるまで待ちます。
6. 各 VSAN で、自動学習をディセーブルにします。
7. CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。
8. 各VSANのコンフィギュレーションデータベースにアクティブ データベースをコピーします。
9. CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。
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。

手順の詳細

ステップ 1 ポート セキュリティをイネーブルにします。

ステップ 2 CFS 配信をイネーブルにします。

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

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

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

ステップ 6 各 VSAN で、自動学習をディセーブルにします。

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

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

ステップ 9 CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。
これで、ファブリック内の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が同一になります。

ステップ 10 ファブリック オプションを使用して、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

関連トピック

ポート セキュリティのアクティブ化, （267 ページ）
変更のコミット, （278 ページ）

ポート セキュリティ データベースのコピー, （285 ページ）
自動学習のディセーブル化, （271 ページ）
ポート セキュリティのイネーブル化, （266 ページ）
ポート セキュリティの配信のイネーブル化, （276 ページ）

自動学習を使用し、CFS 配信を使用しないポート セキュリティの設定

自動学習を使用し、CFS を使用しない場合にポート セキュリティを設定するには、次の手順に従ってください。

手順の概要

1. ポート セキュリティをイネーブルにします。
2. 各 VSAN で、ポート セキュリティをアクティブにします。デフォルトで自動学習が有効になります。
3. すべてのスイッチとすべてのホストが自動的に学習されるまで待ちます。
4. 各 VSAN で、自動学習をディセーブルにします。
5. 各VSANのコンフィギュレーションデータベースにアクティブデータベースをコピーします。
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。
7. ファブリック内のすべてのスイッチに対して上記の手順を繰り返します。

手順の詳細

ステップ 1 ポート セキュリティをイネーブルにします。

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

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

ステップ 4 各 VSAN で、自動学習をディセーブルにします。

ステップ 5 各 VSAN のコンフィギュレーション データベースにアクティブ データベースをコピーします。

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

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

関連トピック

ポート セキュリティのアクティブ化, （267 ページ）
ポート セキュリティ データベースのコピー, （285 ページ）

自動学習のディセーブル化, （271 ページ）
ポート セキュリティのイネーブル化, （266 ページ）

手動データベース設定によるポート セキュリティの設定

手動でポート セキュリティ データベースを設定する場合にポート セキュリティを設定するには、次の手順に従ってください。

手順の概要

1. ポート セキュリティをイネーブルにします。
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。
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。
4. 各 VSAN で、自動学習をディセーブルにします。
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。
6. ファブリック内のすべてのスイッチに対して上記の手順を繰り返します。

手順の詳細

ステップ 1 ポート セキュリティをイネーブルにします。

ステップ 2 各 VSAN の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。

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

ステップ 4 各 VSAN で、自動学習をディセーブルにします。

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

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

ポート セキュリティのイネーブル化

デフォルトでは、ポート セキュリティ機能はディセーブルです。

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。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **port-security enable**
3. switch(config)# **no port-security enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **port-security enable**	スイッチ上でポート セキュリティをイネーブルにします。
ステップ 3	switch(config)# **no port-security enable**	スイッチ上でポート セキュリティをディセーブル（デフォルト）にします。

ポート セキュリティのアクティブ化

ポート セキュリティのアクティブ化

ポート セキュリティをアクティブにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **port-security activate vsan** *vsan-id*
3. switch(config)# **port-security activate vsan** *vsan-id* **no-auto-learn**
4. switch(config)# **no port-security activate vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **port-security activate vsan** *vsan-id*	指定された VSAN のポート セキュリティ データベースをアクティブにし、自動的に自動学習をイネーブルにします。

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

データベースのアクティブ化の拒否

次の場合は、データベースをアクティブ化しようとしても、拒否されます。

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

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

ポート セキュリティの強制的なアクティブ化

ポートセキュリティアクティベーション要求が拒否された場合は、アクティベーションを強制できます。

（注） アクティベーションを強制すると、既存のデバイスがアクティブ データベースに違反したときに既存のデバイスがログアウトされます。

port-security database diff active vsan コマンドを使用して、欠落しているか矛盾するエントリを表示できます。

ポート セキュリティ データベースを強制的にアクティブにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **port-security activate vsan** *vsan-id* **force**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **port-security activate vsan** *vsan-id* **force**	矛盾がある場合でも、指定された VSAN のポート セキュリティ データベースを強制的にアクティブにします。

データベースの再アクティブ化

ヒント　自動学習がイネーブルの場合、force オプションを使用しないと、自動学習をディセーブルにするまでデータベースをアクティブにできません。

ポート セキュリティ データベースを再度アクティブにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **no no port-security auto-learn vsan** *vsan-id*
3. switch(config)# **exit**
4. switch# **port-security database copy vsan** *vsan-id*
5. switch# **configuration terminal**
6. switch(config)# **port-security activate vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **no no port-security auto-learn vsan** *vsan-id*	自動学習をディセーブルにし、スイッチにアクセスする新規デバイスをスイッチが学習しないように設定します。 この時点までに学習されたデバイスに基づいて、データベースの内容を処理します。
ステップ 3	switch(config)# **exit**	
ステップ 4	switch# **port-security database copy vsan** *vsan-id*	アクティブ データベースから設定済みデータベースにコピーします。

	コマンドまたはアクション	目的
ステップ 5	switch# **configuration terminal**	再びコンフィギュレーション モードを開始します。
ステップ 6	switch(config)# **port-security activate vsan** *vsan-id*	指定された VSAN のポート セキュリティ データベースをアクティブにし、自動的に自動学習をイネーブルにします。

自動学習

自動学習のイネーブル化について

自動学習設定の状態は、ポート セキュリティ機能の状態によって異なります。

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

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

自動学習のイネーブル化

自動学習をイネーブルにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **port-security auto-learn vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **port-security auto-learn vsan** *vsan-id*	自動学習をイネーブルにして、VSAN 1 へのアクセスが許可されたすべてのデバイスについて、スイッチが学習できるよ

	コマンドまたはアクション	目的
		うにします。 これらのデバイスは、ポート セキュリティ アクティブ データベースに記録されます。

自動学習のディセーブル化

自動学習をディセーブルにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **no port-security auto-learn vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **no port-security auto-learn vsan** *vsan-id*	自動学習をディセーブルにし、スイッチにアクセスする新規デバイスをスイッチが学習しないように設定します。 この時点までに学習されたデバイスに基づいて、データベースの内容を処理します。

自動学習デバイスの許可

次の表に、デバイス要求に対して接続が許可される条件をまとめます。

表 *35*：許可される自動学習デバイス要求

条件	デバイス（**pWWN**、**nWWN**、**sWWN**）	接続先	認証
1	1 つまたは複数のスイッチ ポートに設定されている場合	設定済みスイッチ ポート	許可
2		他のすべてのスイッチ ポート	拒否

条件	デバイス（pWWN、nWWN、sWWN）	接続先	認証
3	未設定	設定されていないスイッチ ポート	自動学習がイネーブルの場合は許可
4			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許可するスイッチ ポート	許可
6	任意のスイッチ ポートにログインするように設定されている場合	スイッチ上の任意のポート	許可
7	未設定	その他のデバイスが設定されたポート	拒否

許可される場合

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

- pWWN（P1）には、インターフェイス fc2/1（F1）からアクセスできます。
- pWWN（P2）には、インターフェイス fc2/2（F1）からアクセスできます。
- nWWN（N1）には、インターフェイス fc2/2（F2）からアクセスできます。
- インターフェイス vfc3/1（F3）からは、任意の WWN にアクセスできます。
- nWWN（N3）には、任意のインターフェイスからアクセスできる。
- pWWN（P3）には、インターフェイス fc2/4（F4）からアクセスできます。
- sWWN（S1）には、インターフェイス fc3/1 ～ 3（F10 ～ F13）からアクセスできます。
- pWWN（P10）には、インターフェイス vfc4/1（F11）からアクセスできます。

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

表 *36*：各シナリオの許可結果

デバイス接続要求	認証	条件	理由
P1、N2、F1	許可	1	競合しません。

デバイス接続要求	認証	条件	理由
P2、N2、F1	許可	1	競合しません。
P3、N2、F1	拒否	2	F1 が P1/P2 にバインドされています。
P1、N3、F1	許可	6	N3 に関するワイルドカード一致です。
P1、N1、F3	許可	5	F3 に関するワイルドカード一致です。
P1、N4、F5	拒否	2	P1 が F1 にバインドされています。
P5、N1、F5	拒否	2	N1 は F2 でだけ許可されます。
P3、N3、F4	許可	1	競合しません。
S1、F10	許可	1	競合しません。
S2、F11	拒否	7	P10 が F11 にバインドされています。
P4、N4、F5（自動学習が有効）	許可	3	競合しません。
P4、N4、F5（自動学習が無効）	拒否	4	一致しません。
S3、F5（自動学習が有効）	許可	3	競合しません。
S3、F5（自動学習が無効）	拒否	4	一致しません。
P1、N1、F6（自動学習が有効）	拒否	2	P1 が F1 にバインドされています。
P5、N5、F1（自動学習が有効）	拒否	7	P1 と P2 だけが F1 にバインドされています。
S3、F4（自動学習が有効）	拒否	7	P3 と F4 がペアになります。

デバイス接続要求	認証	条件	理由
S1、F3（自動学習が有効）	許可	5	競合しません。
P5、N3、F3	許可	6	F3 および N3 に関するワイルドカード（*）一致です。
P7、N3、F9	許可	6	N3 に関するワイルドカード（*）が一致しています。

関連トピック

自動学習デバイスの許可，（271 ページ）

ポート セキュリティの手動設定

ポート セキュリティを手動で設定するには、次の作業を行います。

手順の概要

1. 保護する必要があるポートの WWN を識別します。
2. 許可された nWWN または pWWN に対して fWWN を保護します。
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。
4. 設定を確認します。

手順の詳細

ステップ 1 保護する必要があるポートの WWN を識別します。
ステップ 2 許可された nWWN または pWWN に対して fWWN を保護します。
ステップ 3 ポート セキュリティ データベースをアクティブにします。
ステップ 4 設定を確認します。

WWN の識別に関する注意事項

ポート セキュリティを手動で設定する場合は、次に従い行ってください。

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

許可済みのポート ペアの追加

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

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

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

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **port-security database vsan** *vsan-id*
3. switch(config)# **no port-security database vsan** *vsan-id*
4. switch(config-port-security)# **swwn** *swwn-id* **interface san-port-channel 5**
5. switch(config-port-security)# **any-wwn interface fc** *slot*/*port* - **fc** *slot*/*port*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **port-security database vsan** *vsan-id*	指定された VSAN に対してポート セキュリティ データベース モードを開始します。
ステップ 3	switch(config)# **no port-security database vsan** *vsan-id*	指定された VSAN からポート セキュリティ コンフィギュレーション データベースを削除します。
ステップ 4	switch(config-port-security)# **swwn** *swwn-id* **interface san-port-channel 5**	SAN ポート チャネル 5 を介した場合だけログインするように、指定された sWWN を設定します。
ステップ 5	switch(config-port-security)# **any-wwn interface fc** *slot*/*port* - **fc** *slot*/*port*	指定されたインターフェイスを介してログインするようにすべての WWN を設定します。

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

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

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

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

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

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

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

```
switch(config-port-security)# any-wwn interface fc 3/2
```

ポート セキュリティ設定の配信

ポート セキュリティ機能は Cisco Fabric Services（CFS）インフラストラクチャを使用して効率的なデータベース管理を実現し、VSAN 内のファブリック全体に 1 つの設定を提供します。また、ファブリック全体でポート セキュリティ ポリシーを実行します。

追加情報については、『*Cisco Nexus 5000 Series System Management Configuration Guide*』の「Using Cisco Fabric Services」を参照してください。

ポート セキュリティの配信のイネーブル化

配信モードで実行されたすべての設定は保留中の（一時的な）データベースに保存されます。 設定を変更する場合、設定に対して保留中のデータベースの変更をコミットまたは廃棄する必要が

あります。その間、ファブリックはロックされた状態になります。保留中のデータベースへの変更は、変更をコミットするまで設定に反映されません。

（注） CFS配信がイネーブルの場合、ポートのアクティベーションまたは非アクティベーション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、CFSコミットを発行するまで有効になりません。 常にCFSコミットとこれらの処理のいずれかを使用して、正しい設定を確認してください。

たとえば、ポート セキュリティをアクティブにし、自動学習をディセーブルにし、最後に保留状態のデータベースに変更をコミットすると、**port-security activate vsan** *vsan-id* no-auto-learn コマンドを入力した場合と同じ結果になります。

ヒント ポート セキュリティをアクティブにし、自動学習をイネーブルにしたあとに、コミットを実行することを推奨します。

ポート セキュリティ データベースを再度アクティブにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **port-security distribute**
3. switch(config)# **no port-security distribute**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# **port-security distribute**	配信をイネーブルにします。
ステップ 3	switch(config)# **no port-security distribute**	配信をディセーブルにします。

関連トピック

アクティベーション設定と自動学習設定の配信, （279 ページ）

ファブリックのロック

既存の設定を変更するときの最初のアクションが実行されると、保留中のデータベースが作成され、VSAN内の機能がロックされます。 ファブリックがロックされると、次のような状況になります。

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

変更のコミット

設定に加えられた変更をコミットする場合、保留中のデータベースの設定が他のスイッチに配信されます。 コミットが正常に行われると、設定の変更がファブリック全体に適用され、ロックが解除されます。

指定された VSAN のポート セキュリティ設定の変更をコミットする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **port-security commit vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **port-security commit vsan** *vsan-id*	指定された VSAN のポート セキュリティの変更をコミットします。

変更の廃棄

保留中のデータベースに加えられた変更を廃棄（中断）する場合、設定は影響されないまま、ロックが解除されます。

指定された VSAN のポート セキュリティ設定の変更を廃棄する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **port-security abort vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **port-security abort vsan** *vsan-id*	指定された VSAN のポート セキュリティの変更を廃棄し、保留中のコンフィギュレーション データベースをクリアします。

アクティベーション設定と自動学習設定の配信

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

学習済みエントリは一時的なもので、ログインを許可するか否かを決定するロールを持ちません。そのため、学習済みエントリは配信に参加しません。 学習をディセーブルにし、保留中のデータベースの変更をコミットする場合、学習済みエントリはアクティブ データベース内のスタティック エントリになり、ファブリック内のすべてのスイッチに配信されます。 コミット後、すべてのスイッチのアクティブ データベースが同一になり、学習をディセーブルにできます。

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

表 *37* : 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	アクション	配信がオフの場合	配信がオンの場合
コンフィギュレーションデータベースにAおよびBが存在し、アクティベーションが行われておらず、デバイスCおよびDがログインされています。	1. ポートセキュリティデータベースをアクティブにし、自動学習をイネーブルにします。	コンフィギュレーションデータベース＝{A、B} アクティブデータベース＝{A、B、C[1]、D*}	コンフィギュレーションデータベース＝{A、B} アクティブデータベース＝{ヌル} 保留中のデータベース＝{A、B＋アクティベーション（イネーブル）}
	2. 新規のエントリEがコンフィギュレーションデータベースに追加されました。	コンフィギュレーションデータベース＝{A、B、E} アクティブデータベース＝{A、B、C*、D*}	コンフィギュレーションデータベース＝{A、B} アクティブデータベース＝{ヌル} 保留中のデータベース＝{A、B、E+アクティベーション（イネーブル）}
	3. コミットを行います。	N/A	コンフィギュレーションデータベース＝{A、B、E} アクティブデータベース＝{A、B、E、C*、D*} 保留中のデータベース＝空の状態

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

[1] *（アスタリスク）は学習されたエントリを意味します。

ポート セキュリティ データベース結合の注意事項

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）エントリの統合を指します。

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

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

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

追加情報については、『*Cisco Nexus 5000 Series System Management Configuration Guide*』の「CFS Merge Support」を参照してください。

データベースの相互作用

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

表 *38*：アクティブおよびコンフィギュレーション ポート セキュリティ データベース

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

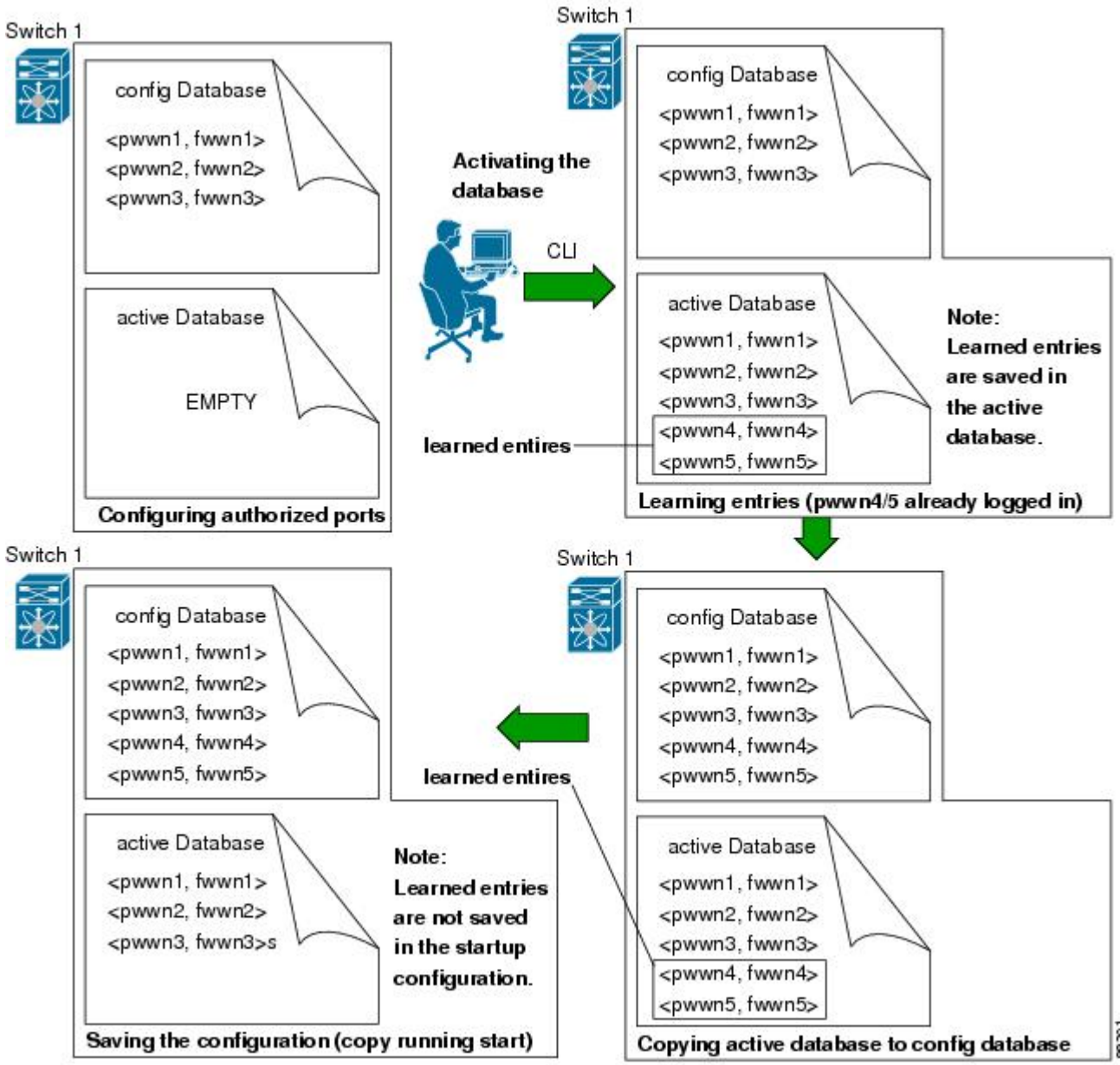
アクティブ データベース	コンフィギュレーション データベース
アクティブデータベースを設定済みデータベースで上書きするには、ポートセキュリティデータベースをアクティブ化します。 強制的にアクティブにすると、アクティブデータベースの設定済みエントリに違反が生じることがあります。	コンフィギュレーション データベースをアクティブ データベースで上書きできます。

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

データベースのシナリオ

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

図 *43*：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。 このアクションにより、コンフィギュレーションデータベースがアクティブデータベースと確実に同期化されます。配信がイネーブルの場合、このコマンドによってコンフィギュレーション データベースの一時的なコピーが作成され、結果としてファブリックがロックされます。 ファブリックがロックされた場合、すべてのスイッチのコンフィギュレーション データベースに変更をコミットする必要があります。

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

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

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

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

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

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

ポート セキュリティ データベースの削除

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

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

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

ポート セキュリティ データベースのクリア

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

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

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

```
switch# clear port-security database auto-learn interface fc2/1 vsan 1
```

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

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

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

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

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

ポート セキュリティ設定の表示

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

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

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

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

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

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

次に、アクティブなデータベースを表示する例を示します。

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

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

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

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

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

次に、ポート セキュリティ統計情報を表示する例を示します。

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

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

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

ポート セキュリティのデフォルト設定

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

表 *39*：セキュリティのデフォルト設定値

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

第 18 章

ファブリック バインディングの設定

この章の内容は、次のとおりです。

- ファブリック バインディングの設定，289 ページ

ファブリック バインディングの設定

ファブリック バインディングについて

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

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

ファブリック バインディングのライセンス要件

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

ポート セキュリティとファブリック バインディングの比較

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

表 *40*：ファブリック バインディングとポート セキュリティの比較

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

xE ポートのポート レベル チェックは、次のように実行されます。

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

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

ファブリック バインディングの実行

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

ファブリック バインディングの設定

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

ファブリック バインディングの設定

ファブリック内の各スイッチにファブリック バインディングを設定する手順は、次のとおりです。

手順の概要

1. ファブリック設定機能をイネーブルにします。
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。
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。
4. ファブリック バインディング アクティブ データベースをファブリック バインディング設定データベースにコピーします。
5. ファブリック バインディング設定を保存します。
6. ファブリック バインディング設定を確認します。

手順の詳細

ステップ 1 ファブリック設定機能をイネーブルにします。
ステップ 2 ファブリックにアクセス可能なデバイスに sWWN のリスト、および対応するドメイン ID を設定します。
ステップ 3 ファブリック バインディング データベースをアクティブにします。
ステップ 4 ファブリック バインディング アクティブ データベースをファブリック バインディング設定データベースにコピーします。
ステップ 5 ファブリック バインディング設定を保存します。
ステップ 6 ファブリック バインディング設定を確認します。

ファブリック バインディングのイネーブル化

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

参加しているスイッチ上でファブリック バインディングをイネーブルにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fabric-binding enable**
3. switch(config)# **no fabric-binding enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fabric-binding enable**	現在のスイッチ上でファブリック バインディングをイネーブルにします。
ステップ 3	switch(config)# **no fabric-binding enable**	現在のスイッチ上でファブリック バインディングをディセーブル（デフォルト）にします。

スイッチの WWN リストの概要

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。 リストにない sWWN、または許可リストで指定されているドメイン ID と異なるドメイン ID を使用する sWWN がファブリックへの参加を試みると、スイッチとファブリック間の ISL が VSAN 内で自動的に隔離され、スイッチはファブリックへの参加を拒否されます。

スイッチ WWN リストの設定

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

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fabric-binding database vsan** *vsan-id*
3. switch(config)# **no fabric-binding database vsan** *vsan-id*
4. switch(config-fabric-binding)#**swwn** *swwn-id* **domain** *domain-id*
5. switch(config-fabric-binding)#**no swwn** *swwn-id* **domain** *domain-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fabric-binding database vsan** *vsan-id*	指定された VSAN のファブリック バインディング サブモードを開始します。
ステップ 3	switch(config)# **no fabric-binding database vsan** *vsan-id*	指定された VSAN のファブリック バインディング データベースを削除します。
ステップ 4	switch(config-fabric-binding)#**swwn** *swwn-id* **domain** *domain-id*	設定されたデータベース リストに、特定のドメイン ID 用の別のスイッチの sWWN を追加します。
ステップ 5	switch(config-fabric-binding)#**no swwn** *swwn-id* **domain** *domain-id*	設定されたデータベース リストから、スイッチの sWWN およびドメイン ID を削除します。

ファブリック バインディングのアクティベーションおよび非アクティベーション

ファブリック バインディング機能では、コンフィギュレーション データベース（config database）およびアクティブ データベースが維持されます。 config database は、実行された設定を収集する読み取りと書き込みのデータベースです。 これらの設定を実行するには、データベースをアク

ファブリック バインディングの設定

ティブにする必要があります。データベースがアクティブになると、アクティブデータベースがconfig databaseの内容で上書きされます。アクティブ データベースは、ログインを試みる各スイッチをチェックする読み取り専用データベースです。

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

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

ファブリック バインディングのアクティベーション

ファブリック バインディング機能をアクティブにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fabric-binding activate vsan** *vsan-id*
3. switch(config)# **no fabric-binding activate vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fabric-binding activate vsan** *vsan-id*	指定された VSAN のファブリック バインディング データベースをアクティブにします。
ステップ 3	switch(config)# **no fabric-binding activate vsan** *vsan-id*	指定された VSAN のファブリック バインディング データベースを非アクティブにします。

ファブリック バインディングの強制的なアクティベーション

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

ファブリック バインディング データベースを強制的にアクティブにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fabric-binding activate vsan** *vsan-id* **force**
3. switch(config)# **no fabric-binding activate vsan** *vsan-id* **force**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fabric-binding activate vsan** *vsan-id* **force**	指定されたVSANのファブリック バインディング データベースを、設定が許可されない場合でも、強制的にアクティブにします。
ステップ 3	switch(config)# **no fabric-binding activate vsan** *vsan-id* **force**	元の設定状態、または（状態が設定されていない場合は）出荷時の設定に戻します。

ファブリック バインディング設定のコピー

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

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

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

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

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

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

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

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

- 再起動後にファブリック バインディング設定データベースを使用できるように実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存するには、**copy running-config startup-config** コマンドを使用します。

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

ファブリック バインディング統計情報のクリア

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

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

ファブリック バインディング データベースの削除

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

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

ファブリック バインディング情報の確認

ファブリック バインディング情報を表示するには、次のいずれかの作業を実行します。

手順の概要

1. switch# **show fabric-binding database** [**active**]
2. switch# **show fabric-binding database** [**active**] [**vsan** *vsan-id*]
3. switch# **show fabric-binding statistics**
4. switch# **show fabric-binding status**
5. switch# **show fabric-binding violations**
6. switch# **show fabric-binding efmd** [**vsan** *vsan-id*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **show fabric-binding database** [**active**]	設定されたファブリック バインディング データベースを表示します。 キーワード active を含めて、アクティブなファブリック バインディング データベースだけを表示します。
ステップ 2	switch# **show fabric-binding database** [**active**] [**vsan** *vsan-id*]	指定された VSAN の設定済みファブリック バインディング データベースを表示します。

	コマンドまたはアクション	目的
ステップ 3	switch# **show fabric-binding statistics**	ファブリック バインディング データベースの統計情報を表示します。
ステップ 4	switch# **show fabric-binding status**	すべての VSAN のファブリック バインディング ステータスを表示します。
ステップ 5	switch# **show fabric-binding violations**	ファブリック バインディング違反を表示します。
ステップ 6	switch# **show fabric-binding efmd** [**vsan** *vsan-id*]	指定された VSAN の設定済みファブリック バインディング データベースを表示します。

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

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

次に、ファブリック バインディング違反を表示する例を示します。

```
switch# show fabric-binding violations
--------------------------------------------------------------------------------

VSAN Switch WWN [domain]     Last-Time             [Repeat count] Reason

--------------------------------------------------------------------------------

2    20:00:00:05:30:00:4a:1e [0xeb] Nov 25 05:46:14 2003   [2]    Domain mismatch

3    20:00:00:05:30:00:4a:1e [*] Nov 25 05:44:58 2003      [2]    sWWN not found

4    20:00:00:05:30:00:4a:1e [*] Nov 25 05:46:25 2003      [1]    Database mismatch
```

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

次に、VSAN 4 の EFMD 統計情報を表示する例を示します。

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

ファブリック バインディングのデフォルト設定

次の表に、ファブリック バインディング機能のデフォルト設定を示します。

表 *41*： ファブリック バインディングのデフォルト設定

パラメータ	デフォルト
ファブリック バインディング	ディセーブル

第 19 章

FCS の設定

この章の内容は、次のとおりです。

- FCS の設定，299 ページ

FCS の設定

FCS の概要

Fabric Configuration Server（FCS）を使用すると、トポロジ属性を検出したり、ファブリック要素のコンフィギュレーション情報リポジトリを維持したりすることができます。 通常、管理アプリケーションは N ポートを通してスイッチの FCS に接続されます。 FCS は次のオブジェクトに基づいて、ファブリック全体を表示します。

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

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

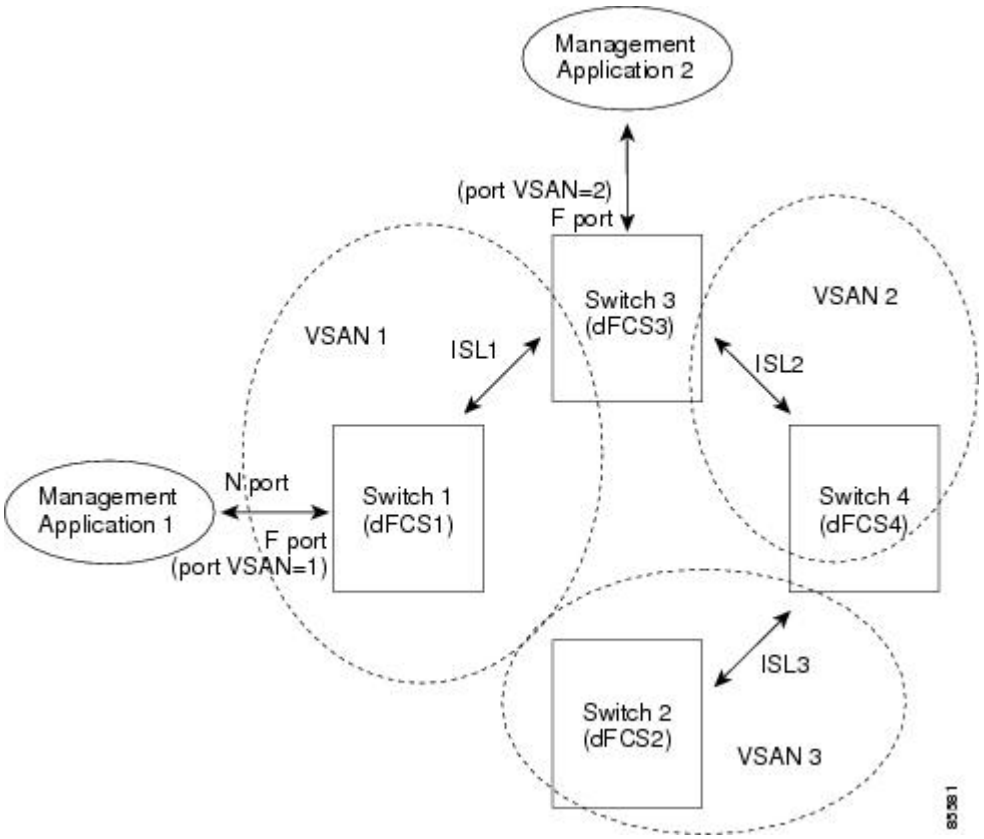
Cisco Nexus 5000 シリーズ スイッチ環境では、ファブリックは複数の VSAN で構成される場合があります。 VSAN ごとに FCS インスタンスが 1 つ存在します。

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

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

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

図 *44*： *VSAN* 環境における *FCS*



FCS の特性

FCS には次の特性があります。

- 次のようなネットワーク管理をサポートしています。

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

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

FCS 名の指定

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

（注） このコマンドのグローバル設定は、ファブリック内のすべてのスイッチがCisco MDS 9000ファミリまたはCisco Nexus 5000 シリーズ のスイッチである場合にかぎり実行してください。

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

プラットフォーム属性を登録する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcs plat-check-global vsan** *vsan-id*
3. switch(config)# **no fcs plat-check-global vsan** *vsan-id*

手順の詳細

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

FCS 情報の表示

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

次に、FCS ローカル データベースを表示する例を示します。

```
switch# show fcs database
```

次に、VSAN 1 のすべての IE のリストを表示する例を示します。

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

次に、特定のプラットフォームに関する情報を表示する例を示します。

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

次に、特定の pWWN のポート情報を表示する例を示します。

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

FCS のデフォルト設定

次の表に、FCS のデフォルト設定を示します。

表 *42* : *FCS* のデフォルト設定

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

第 20 章

ポート トラッキングの設定

この章の内容は、次のとおりです。

- ポート トラッキングの設定，303 ページ

ポート トラッキングの設定

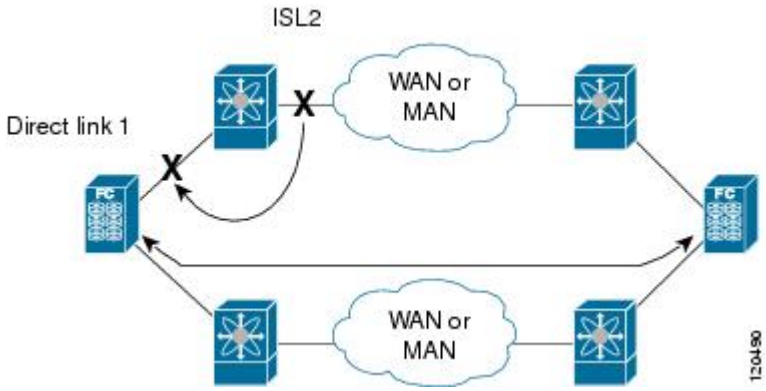
Cisco SAN スイッチは、（仮想ファイバ チャネル インターフェイスではなく）物理ファイバ チャネル インターフェイスでポート トラッキング機能を提供します。この機能はリンクの動作ステートに関する情報を利用して、エッジデバイスを接続するリンクの障害を引き起こします。この処理では、間接障害が直接障害に変換されるため、冗長リンクへの復旧処理が迅速化されます。ポート トラッキング機能がイネーブルになっている場合、この機能はリンク障害時に設定されたリンクをダウンにし、トラフィックを別の冗長リンクに強制的にリダイレクトします。

ポート トラッキングに関する情報

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

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

図 *45*：ポート トラッキングによるトラフィックの復旧



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

この章では次の用語を使用します。

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

ポート トラッキングには、次の機能があります。

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

関連トピック

RSCN 情報の概要, （213 ページ）
ファイバ チャネルのタイムアウト値, （225 ページ）

ポート トラッキングのデフォルト設定値

次の表に、ポート トラッキング パラメータのデフォルト設定を示します。

表 *43*：ポート トラッキング パラメータのデフォルト設定値

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

ポート トラッキングの設定

ポート トラッキングを設定する際、次の点に注意してください。

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

ポート トラッキングのイネーブル化

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

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

ポート トラッキングをイネーブルにするには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **port-track enable**
3. switch(config)# **no port-track enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **port-track enable**	ポート トラッキングをイネーブルにします。
ステップ 3	switch(config)# **no port-track enable**	現在適用されているポート トラッキング設定を削除し、ポート トラッキングをディセーブルにします。

リンク対象ポート設定の概要

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には、次の作業を行います。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface fc** *slot*/*port*
3. switch(config-if)# **port-track interface fc** *slot*/*port* | **san-port-channel** *port*
4. switch(config-if)# **no port-track interface fc** *slot*/*port* | **san-port-channel** *port*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。

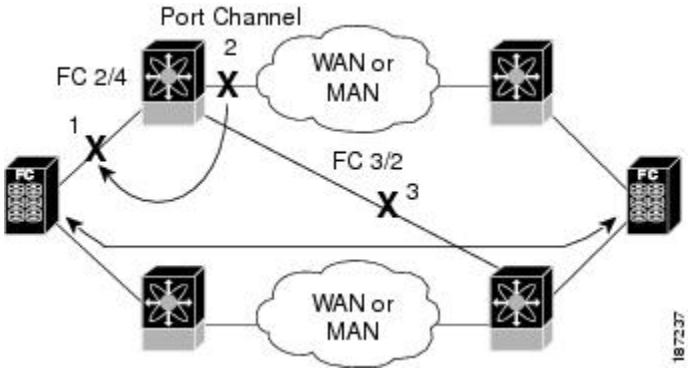
	コマンドまたはアクション	目的
ステップ 2	switch(config)# **interface fc** *slot*/*port*	リンク対象ポートでインターフェイス コンフィギュレーション モードを開始します。 これで、トラッキング対象ポートを設定できるようになります。
ステップ 3	switch(config-if)# **port-track interface fc** *slot*/*port* | **san-port-channel** *port*	トラッキング対象ポートを指定します。 トラッキング対象ポートがダウンすると、リンク対象ポートもダウンします。
ステップ 4	switch(config-if)# **no port-track interface fc** *slot*/*port* | **san-port-channel** *port*	インターフェイスに現在適用されているポート トラッキング設定を削除します。

複数ポート 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したときにかぎり、リンク対象ポートの動作ステートはダウンに設定されます。 トラッキング対象ポートが 1 つでもアップしている場合、リンク対象ポートはアップしたままになります。

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

図 *46*： ポート トラッキングによるトラフィックの復旧



複数ポートのトラッキング

複数のポートをトラッキングするには、次の作業を行います。

ポート トラッキングの設定

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **interface fc** *slot*/*port*
3. switch(config-if)# **port-track interface interface fc** *slot*/*port* | **san-port-channel** *port*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface fc** *slot*/*port*	指定されたインターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 これで、トラッキング対象ポートを設定できるようになります。
ステップ 3	switch(config-if)# **port-track interface interface fc** *slot*/*port* | **san-port-channel** *port*	指定されたインターフェイスのあるリンク対象ポートをトラッキングします。 トラッキング対象ポートがダウンすると、リンク対象ポートもダウンします。

VSAN 内のポートの監視の概要

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

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

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

VSAN 内のポートのモニタリングの概要

特定の VSAN でトラッキング対象ポートをモニタするには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **interface fc** *slot*/*port*
3. switch(config-if)# **port-track interface san-port-channel 1 vsan 2**
4. switch(config-if)# **no port-track interface san-port-channel 1 vsan 2**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface fc** *slot*/*port*	指定されたインターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 これで、トラッキング対象ポートを設定できるようになります。
ステップ 3	switch(config-if)# **port-track interface san-port-channel 1 vsan 2**	VSAN 2 で SAN ポート チャネルのトラッキングをイネーブルにします。
ステップ 4	switch(config-if)# **no port-track interface san-port-channel 1 vsan 2**	リンク対象ポートに対する VSAN の対応付けを削除します。 SAN ポート チャネル リンクは有効なままです。

強制シャットダウンの概要

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

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

トラッキング対象ポートの強制シャットダウン

トラッキング対象ポートを強制的にシャットダウンするには、次の作業を行います。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **interface fc** *slot*/*port*
3. switch(config-if)# **port-track force-shut**
4. switch(config-if)# **no port-track force-shut**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface fc** *slot*/*port*	指定されたインターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 これで、トラッキング対象ポートを設定できるようになります。
ステップ 3	switch(config-if)# **port-track force-shut**	トラッキング対象ポートを強制的にシャットダウンします。
ステップ 4	switch(config-if)# **no port-track force-shut**	トラッキング対象ポートのポート シャットダウン設定を解除します。

ポート トラッキング情報の表示

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

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

```
switch# show interface fc2/1
fc2/1 is down (Administratively down)
    Hardware is Fibre Channel, FCOT is short wave laser w/o OFC (SN)
    Port WWN is 20:01:00:05:30:00:0d:de
    Admin port mode is FX
    Port vsan is 1
    Receive data field Size is 2112
    Beacon is turned off
    Port tracked with interface fc2/2 (down)
    Port tracked with interface san-port-channel 1 vsan 2 (down)
5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
...
```

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

```
switch# show interface san-port-channel 1
port-channel 1 is down (No operational members)
    Hardware is Fibre Channel
    Port WWN is 24:01:00:05:30:00:0d:de
    Admin port mode is auto, trunk mode is on
    Port vsan is 2
    Linked to 1 port(s)
      Port linked to interface fc2/1
...
```

次に、ポート トラッキング モードを表示する例を示します。

```
switch# show interface fc 2/4
fc2/4 is up
    Hardware is Fibre Channel, FCOT is short wave laser
...
    Transmit B2B Credit is 64
    Receive B2B Credit is 16
    Receive data field Size is 2112
    Beacon is turned off
    Port track mode is force_shut <-- this port remains shut even if the tracked port is
back up
```

索 引

記号

* （アスタリスク） 122
  最初の動作ポート 122
    最初の動作ポート 122

A

AAA 257
  DHCHAP 認証 257
auto ポート モード 15
  説明 15
auto モード 22
  設定 22

B

BB_credit 19, 33
  情報の表示 33
  説明 19
  理由コード 19
Brocade 235
  ネイティブ interop モード 235
Buffer-to-Buffer credit 19, 27
  設定 27

D

DHCHAP 247, 248, 249, 250, 252, 253, 254, 257, 259
  AAA 認証 257
  AAA 認証の設定 257
  イネーブル化 250
  グループ設定 253
  セキュリティ情報の表示 257
  設定 248
  設定例 257
DHCHAP *(続き)*
  説明 248
  デフォルト設定 259
  認証モード 250
  ハッシュ アルゴリズム 252
  他の NX-OS 機能との互換性 249
  ローカル スイッチのパスワード 254
Diffie-Hellman チャレンジ ハンドシェイク認証プロトコル 247

E

EFMD 289, 291, 296
  統計情報の表示 296
  ファブリック バインディング 289
  ファブリック バインディングの開始 291
EISL 103
  SAN ポート チャネル リンク 103
ELP 16
Exchange Fabric Membership Data 289
Exchange Link Parameter 16
E ポート 16, 22, 96, 156, 187, 289, 299
  FCS のサポート 299
  FSPF トポロジ 187
  設定 22
  トランキング設定 96
  ファブリック バインディングの確認 289
  分離 16
  リンクの分離からの回復 156
E ポート モード 13
  サービス クラス 13
  説明 13

F

Fabric-Device 管理インターフェイス 212

Fabric Configuration Server 299
Fabric Shortest Path First 187
　ルーティング サービス 187
FC ID 35, 50, 51, 151, 232
　FC エイリアス メンバの設定 151
　固定 51
　説明 50
　デフォルトの企業 ID リストの割り当て 232
　割り当て 35
FC-SP 247, 250, 257
　ISL でのイネーブル化 257
　イネーブル化 250
　認証 247
fcdomain 16, 35, 38, 39, 40, 41, 42, 46, 47, 56, 57
　CFS 配信の設定 46, 47
　イネーブル化 39
　オーバーラップ分離 16
　開始 39
　restarts 35
　自動設定された、結合されたファブリック 41
　自動再設定のイネーブル化 42
　情報の表示 56
　スイッチ プライオリティ 38
　説明 35
　着信 RCF 40
　ディセーブル化 39
　デフォルト設定 57
　統計情報の表示 56
　ドメイン ID 42
　ドメイン マネージャの高速再起動 38
FCS 299, 300, 302
　情報の表示 302
　説明 299
　デフォルト設定 302
　特性 299
　名前の設定 300
fctimer 230
　設定された値の表示 230
FC エイリアス 152, 159
　コピー 159
　作成 152
　ゾーンの設定 152
　名前の変更 159
FDMI 212, 213
　説明 212
　データベース情報の表示 213
FLOGI 209
　説明 209
FSCN 223
　データベースの表示 223
FSPF 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 199, 206, 235
　hello タイム インターバルの設定 193
　Link State Record のデフォルト 190
　VSAN カウンタのクリア 191
　VSAN での設定 190
　イネーブル化 191
　インターフェイスでの設定 192
　インターフェイスでのディセーブル化 196
　カウンタのクリア 197
　グローバル情報の表示 206
　グローバル設定 189
　再コンバージェンス時間 187
　再送信インターバル 195
　順序どおりの配信 199
　冗長リンク 188
　設定のリセット 191
　説明 187
　相互運用性 235
　ディセーブル化 191
　データベース情報の表示 206
　デッド タイム間隔 194
　デフォルト設定 206
　デフォルトへのリセット 191
　トポロジの例 187
　フォールト トレラント ファブリック 187
　リンク コストの計算 193
　リンク コストの設定 193
　ルーティング サービス 187
　ルーティング プロトコルのディセーブル化 191
FSPF ルート 197, 198
　設定 198
　説明 197
fWWN 151
　FC エイリアス メンバの設定 151
Fx ポート 13, 128
　VSAN メンバーシップ 128
F ポート 13, 22
　設定 22
　説明 13
F ポート モード 13
　サービス クラス 13
　説明 13

H

HBA ポート 53
エリア FCID の設定 53
hello タイム インターバル 193
FSPF の設定 193
説明 193

I

interop モード 235, 244
説明 235
デフォルト設定 244
モード 1 の設定 235
IOD 199
ISL 103
SAN ポート チャネル リンク 103

L

LUN 223
検出された SCSI ターゲットの表示 223

M

MAC アドレス 231
セカンダリの設定 231
McData 235
ネイティブ interop モード 235

N

N5K-M1008 拡張モジュール 9
N5K-M1404 拡張モジュール 9
NPIV 28, 29
イネーブル化 29
説明 28
NPV 65, 66, 67, 69
NP インターフェイスの設定 66
イネーブル化 65
確認 69
サーバ インターフェイスの設定 67
NPV のイネーブル化 65
NPV の確認 69
NPV の設定 66, 67
NP ポート 59
NP ポート モード 13
NP リンク 61
N ポート 141, 154, 299
FCS のサポート 299
ゾーンの実行 154
ゾーン メンバーシップ 141
ハード ゾーン分割 154
N ポート識別子仮想化 28

P

PLOGI 211
ネーム サーバ 211
pWWN 141, 151
FC エイリアス メンバの設定 151
ゾーン メンバーシップ 141

R

RCF 36, 40, 41
説明 36
着信 40
着信の拒否 41
Registered State Change Notification 213
RSCN 213, 214, 215, 220
情報の表示 213
スイッチ RSCN 213
説明 213
デフォルト設定 220
ドメイン フォーマット SW-RSCN の抑制 215
複数のポート ID 214
RSCN タイマー 215, 217
CFS を使用した設定の配信 217
設定 215

S

SAN ポート チャネル 103, 104, 105, 109, 113, 114, 115, 122, 124
インターフェイス ステート 115
インターフェイスの追加 113, 115
互換性チェック 114
誤設定エラー検出 109
設定時の注意事項 109
設定の確認 122
説明 103

SAN ポート チャネル *(続き)*
デフォルト設定 **124**
トランキングとの比較 **104**
ロード バランシング **105**
SAN ポート チャネル プロトコル **117, 118, 119**
自動作成 **118**
自動作成のイネーブル化 **119**
自動作成の設定 **119**
チャネル グループの作成 **117**
SCR **213**
request **213**
SCSI **223**
LUN 検出結果の表示 **223**
SCSI LUN **221, 223**
カスタマイズ検出 **223**
検出の開始 **221**
情報の表示 **223**
ターゲットの検出 **221**
SD ポート **22**
設定 **22**
SD ポート モード **14**
インターフェイス モード **14**
説明 **14**
SFP **31**
トランスミッタ タイプ **31**
トランスミッタ タイプの表示 **31**
SPAN 宛先ポート モード **14**
SPF **190**
計算ホールド タイム **190**
sWWN **293**
ファブリック バインディングの設定 **293**

T

TE ポート **94, 156, 187, 235, 289, 299, 300**
FCS のサポート **299**
FSPF トポロジ **187**
相互運用性 **235**
トランキングの制約事項 **94**
ファブリック バインディングの確認 **289**
リンクの分離からの回復 **156**
TE ポート モード **13**
サービス クラス **13**
説明 **13**
TOV **225, 226, 235, 244**
VSAN の設定 **226**
すべての VSAN の設定 **225**
TOV *(続き)*
相互運用性 **235**
デフォルト設定 **244**
範囲 **225**

V

VSAN **13, 16, 42, 56, 94, 100, 125, 128, 130, 131, 132, 133, 134, 135, 137, 138, 139, 145, 187, 189, 190, 204, 210, 225, 235, 249, 299**
allowed-active リストの設定 **100**
DHCHAP との互換性 **249**
FC ID **125**
FCS のサポート **299**
FSPF **190**
FSPF 接続 **187**
FSPF の設定 **189**
interop モード **235**
TE ポート モード **13**
TOV **225**
機能 **125**
キャッシュの内容 **56**
許可アクティブ **94**
削除 **135**
使用状況の表示 **138**
ステート **130**
設定 **131**
設定の表示 **138**
説明 **125**
ゾーンとの比較（表） **128**
タイマー設定 **225**
デフォルト VSAN **133**
デフォルト設定 **139**
動作ステート **135**
独立 **134**
ドメイン ID の自動再設定 **42**
トラフィックの分離 **125**
トランキング ポート **132**
トランク許可 **94**
トランク許可リストの設定 **100**
名前 **130**
ネーム サーバ **210**
不一致 **16**
複数のゾーン **145**
フロー統計情報 **204**
ポート メンバーシップ **131**
メンバーシップの表示 **132**
利点 **125**

VSAN *(続き)*
ロード バランシング 137
ロード バランシング属性 130
VSAN ID 13, 101, 128, 130
VSAN メンバーシップ 128
許可リスト 101
説明 130
トラフィックの多重化 13
範囲 128

W

World Wide Name 230
WWN 16, 230, 231
情報の表示 231
セカンダリ MAC アドレス 231
説明 230
中断された接続 16
リンクの初期化 231

あ

アクティブ ゾーン セット 145, 155
考慮事項 145
配信のイネーブル化 155
宛先 ID 105, 137, 199
エクスチェンジ ベース 105
順序どおりの配信 199
パスの選択 137
フロー ベース 105
アドレス割り当てキャッシュ 56
説明 56

い

一意のエリア FC ID 53
設定 53
説明 53
インターフェイス 15, 23, 25, 31, 113, 115, 131, 132, 151
FC エイリアス メンバの設定 151
SAN ポート チャネルへの追加 113, 115
SFP 情報の表示 31
SFP タイプ 31
VSAN への割り当て 132
VSAN メンバーシップ 131
インターフェイス *(続き)*
隔離ステート 115
受信データ フィールド サイズの設定 25
説明の設定 23
中断ステート 115

え

永続的 FCID 51, 54, 56
イネーブル化 51
設定 51
説明 51
パージ 54
表示 56

か

拡張ゾーン 161, 163, 165, 168
基本ゾーンからの変更 163
基本ゾーンの利点 161
スイッチ全体のデフォルト ゾーン ポリシーの設定 168
説明 161
データベースの変更 165
デフォルトのフル データベース配信の設定 168
デフォルト ポリシーの設定 168
拡張ポート モード 13
仮想ファイバ チャネル インターフェイス 33
デフォルト設定 33
間接リンク障害 303
リカバリ 303
管理ステート 15
説明 15
管理速度 23
設定 23

き

企業 ID 232
FC ID の割り当て 232

け

結合されたファブリック 41
自動再構成された 41

こ

交換 ID 137, 199
順序どおりの配信 199
パスの選択 137
小型計算機システム インターフェイス 221

さ

再送信インターバル 195
FSPF の設定 195
説明 195

し

実行時チェック 198
スタティック ルート 198
主要スイッチ 42, 45
設定 45
ドメイン ID の割り当て 42
順序どおりの配信 200, 201, 202, 203
VSAN のイネーブル化 202
グローバルなイネーブル化 201
ステータスの表示 203
注意事項 201
ドロップ遅延時間の設定 203
ネットワーク フレームの順序変更 200
ポート チャネル フレームの順序変更 200
冗長構成 128
VSAN 128

す

スイッチ プライオリティ 38, 39
説明 38
デフォルト 39
スイッチ ポート 28
属性のデフォルト値の設定 28
スケーラビリティ 128
VSAN 128
スタティック ルート 198
実行時チェック 198
ストレージ デバイス 141
アクセス コントロール 141

せ

セカンダリ MAC アドレス 231
設定 231
設定 27
Buffer-to-Buffer credit 27

そ

相互運用性 138, 235, 240
interop モード 1 の設定 235
VSAN 138
ステータスの確認 240
説明 235
送信元 ID 105, 137, 199
エクスチェンジ ベース 105
順序どおりの配信 199
パスの選択 137
フロー ベース 105
ゾーン 16, 128, 141, 144, 149, 152, 157, 158, 159, 161, 169, 170, 174
FC エイリアスの設定 152
pWWN を使用したメンバーシップ 128
VSAN との比較（表） 128
アクセス コントロール 149
エイリアスの設定 152
機能 141, 144
コピー 159
情報の表示 161
ダウングレード用の圧縮 169
データベースのインポート 157
データベースのエクスポート 157
デバイス エイリアスとの比較 174
デフォルト ポリシー 141
名前の変更 159
バック アップ（手順） 158
復元（手順） 158
分析 170
マージ障害 16
ゾーン エイリアス 182
デバイス エイリアスへの変換 182
ゾーン サーバ データベース 160
クリア 160
ゾーン セット 141, 145, 149, 155, 156, 157, 159, 161, 170
アクティブ化 149
一時配信 156
インポート 157
エクスポート 157

ゾーン セット *(続き)*
機能 141
考慮事項 145
コピー 159
作成 149
情報の表示 161
設定の配信 155
データベースのインポート 157
データベースのエクスポート 157
名前の変更 159
配信のイネーブル化 155
分析 170
リンクの分離からの回復 156
ゾーン属性グループ 159
コピー 159
ゾーン データベース 160, 166
Cisco SAN 以外のデータベースの移行 160
ロックの解除 166
ゾーン分割 141, 143, 144
実装 144
説明 141
例 143
ゾーン メンバ 150
情報の表示 150
速度自動検知 24
ソフト ゾーン分割 154
説明 154

た

タイムアウト値 225

て

デッド タイム間隔 194
FSPF の設定 194
説明 194
デバイス エイリアス 173, 174, 175, 176, 182, 183, 184
拡張モード 176
機能 173
作成 175
情報の表示 183
説明 173
ゾーン エイリアスの変換 182
ゾーン セット情報の表示 183
デバイス エイリアス *(続き)*
ゾーンとの比較 174
データベースの変更 175
デフォルト設定 184
要件 174
デバイス エイリアス データベース 179, 181, 183
結合 183
配信のイネーブル化 181
配信のディセーブル化 181
ファブリックのロック 179
変更の破棄 179
デフォルト VSAN 133
説明 133
デフォルト ゾーン 150, 235
説明 150
相互運用性 235
ポリシー 150

と

動作ステート 15, 21
説明 15
ファイバ チャネル インターフェイスの設定 21
独立 VSAN 134, 135
説明 134
メンバーシップの表示 135
ドメイン ID 16, 35, 42, 45, 46, 47, 50, 151, 235
CFS 配信の設定 46, 47
FC エイリアス メンバの設定 151
preferred 42
static 42
許可リスト 45
許可リストの設定 46
説明 42
相互運用性 235
配信 35
隣接する割り当てのイネーブル化 50
連続割り当て 50
割り当て障害 16
ドメイン マネージャ 16, 37
高速再起動機能 37
分離 16
トラッキング対象ポート 306
動作バインディング 306
トラフィックの分離 128
VSAN 128

トランキング 93, 94, 96, 101, 104, 235
情報の表示 101
制限事項 93
設定時の注意事項 94
説明 93
相互運用性 235
デフォルト設定 101
トラフィックの結合 94
ポート チャネルとの比較 104
モードの設定 96
リンク ステート 96
トランキング E ポート モード 13
トランキング プロトコル 94, 95, 101
説明 95
デフォルト設定 101
デフォルトの状態 95
ポート独立の検出 94
トランキング ポート 132
VSAN に関連付けられた 132
トランク許可 VSAN リスト 98
説明 98
トランク ポート 101
情報の表示 101
トランク モード 28, 96, 97, 101
管理デフォルト 28
設定 96, 97
デフォルト設定 101
ドロップ遅延時間 203, 204
FSPF の順序どおりの配信の設定 203
情報の表示 204
設定 203

に

認証 247
ファブリック セキュリティ 247

ね

ネーム サーバ 210, 212, 221, 235
LUN 情報 221
相互運用性 235
データベース エントリの表示 212
プロキシ機能 210
プロキシの登録 210

の

ノード プロキシ ポート モード 13

は

ハード ゾーン分割 154
説明 154
パスワード 254
DHCHAP 254

ひ

ビット エラー 25
理由 25
ビット エラーしきい値 25
設定 25
説明 25

ふ

ファイバ チャネル 225, 293
TOV 225
タイムアウト値 225
ファブリック バインディング用の sWWN 293
ファイバ チャネル インターフェイス 15, 16, 19, 20, 21, 22, 23, 25, 33, 133
auto ポート モードの設定 22
BB_credit 19
VSAN メンバーシップの表示 133
管理ステート 15
ステート 15
設定 20
説明の設定 23
速度の設定 23
デフォルト設定 33
動作ステート 15
範囲の設定 21
ビット エラーしきい値の設定 25
フレームのカプセル化の設定 25
ポート モードの設定 22
理由コード 16
ファイバ チャネル セキュリティ プロトコル 247
ファイバ チャネル ドメイン 35
ファブリック 36

ファブリック pWWN 141
ゾーン メンバーシップ 141
ファブリック セキュリティ 247, 259
デフォルト設定 259
認証 247
ファブリックの再設定 35
fcdomain フェーズ 35
ファブリック バインディング 249, 289, 291, 292, 294, 295, 296, 297
DHCHAP との互換性 249
EFMD 289
EFMD 統計情報の表示（手順） 295
E ポートの確認 289
TE ポートの確認 289
アクティブ データベースの表示（手順） 295
イネーブル化 292
違反の表示（手順） 295
開始プロセス 291
強制 291
強制的なアクティベーション 294
強制的な非アクティベーション 294
コンフィギュレーション データベースの作成（手順） 295
コンフィギュレーションデータベースからの削除（手順） 295
コンフィギュレーション データベースへのコピー 294
コンフィギュレーション データベースへの保存 294
コンフィギュレーション ファイルへのコピー（手順） 295
ステータスの確認 292
説明 289
ディセーブル化 292
データベースの削除 296
デフォルト設定 297
統計情報のクリア 296
ポート セキュリティの比較 289
ライセンス要件 289
ファブリック フレームの再設定 36
ファブリック フレームの作成 36
説明 36
ファブリック ポート モード 13
ファブリック ログイン 209
フォールト トレラント ファブリック 188
例（図） 188
フル ゾーン セット 145, 155
考慮事項 145
配信のイネーブル化 155
フレームのカプセル化 25
設定 25
フロー統計情報 204, 205, 206
カウント 204
クリア 205
説明 204
表示 206
プロキシ 210
ネーム サーバの登録 210

ほ

ポート 131
VSAN メンバーシップ 131
ポート セキュリティ 249, 261, 262, 263, 266, 267, 268, 269, 274, 275, 286, 289
DHCHAP との互換性 249
アクティブ化 267
アクティブ化の拒否 268
アクティベーション 263
アクティベーションの強制 268
イネーブル化 266
違反の表示（手順） 269
許可済みのペアの追加 275
実行メカニズム 262
自動学習 262
自動学習を使用しない手動設定 274
設定の表示 286
設定の表示（手順） 269
ディセーブル化 266
デフォルト設定 286
統計情報の表示（手順） 269
非アクティブ化 267
ファブリック バインディングとの比較 289
不正アクセスの防止 261
ライセンス要件 261
ポート セキュリティ データベース 266, 269, 282, 284, 285, 286
クリーンアップ 285
結合の注意事項 282
コピー 285
コンフィギュレーションへのアクティブのコピー（手順） 269
再アクティブ化 269
削除 285
シナリオ 284
手動設定に関する注意事項 266

ポート セキュリティ データベース *(続き)*
設定の表示 286
相互作用 282
ポート セキュリティの自動学習 262, 263, 265, 270, 271, 276
CFS を使用しない設定に関する注意事項 265
CFS を使用する場合の設定に関する注意事項 263
イネーブル化 270
設定の配信 276
説明 262
ディセーブル化 271
デバイス許可 271
ポート速度 23
設定 23
ポート チャネル 16, 198, 200, 235, 249
DHCHAP との互換性 249
管理上のダウン 16
相互運用性 235
ファイバ チャネル ルートの設定 198
リンクの変更 200
ポート トラッキング 303, 305, 309, 310
イネーブル化 305
情報の表示 310
説明 303
注意事項 305
デフォルト設定 305
ポートの強制シャットダウン 309
ポート モード 15
auto 15
ポート ワールド ワイド ネーム 141

り

理由コード 16
説明 16
リンク コスト 193
FSPF の設定 193
説明 193
リンク障害 303
リカバリ 303

る

ルート コスト 193
計算 193

れ

連続ドメイン ID 割り当て 50
バージョン情報 50

ろ

ロード バランシング 103, 105, 130, 137
SAN ポート チャネル 103
VSAN の属性 130
設定 137
説明 105, 137
属性 137
保証 137
論理ユニット番号 221