



## **Cisco Nexus 9000 Series NX-OS SAN Switching Configuration Guide, Release 10.5(x)**

**First Published:** 2024-07-26

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at <https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html>. Cisco product warranty information is available at <https://www.cisco.com/c/en/us/products/warranty-listing.html>. US Federal Communications Commission Notices are found here <https://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

© 2024–2024 Cisco Systems, Inc. All rights reserved.



## CONTENTS

### Trademarks ?

---

#### PREFACE

##### はじめに xv

対象読者 xv

表記法 xv

Cisco Nexus 9000 シリーズ スイッチの関連資料 xvi

マニュアルに関するフィードバック xvi

通信、サービス、およびその他の情報 xvii

Cisco バグ検索ツール xvii

マニュアルに関するフィードバック xvii

---

#### CHAPTER 1

##### New and Changed Information 1

New and Changed Information 1

---

#### CHAPTER 2

##### SAN スイッチングのハードウェア サポート 3

SAN スイッチングのハードウェア サポート 3

---

#### CHAPTER 3

##### 概要 5

ライセンス要件 5

SAN スイッチングの概要 5

SAN スイッチングの一般的な注意事項と制限事項 10

---

#### CHAPTER 4

##### FC/FCoE スイッチ モードの有効化 13

FCoE 機能を有効にする 13

FC スイッチング モードに関する注意事項と制限事項 13

|                          |    |
|--------------------------|----|
| FC/FCoE の有効化             | 14 |
| FC/FCoE の無効化             | 15 |
| FCoE リンクの LAN トラフィックの無効化 | 16 |
| FC-Map の設定               | 17 |
| ファブリック プライオリティの設定        | 18 |
| ジャンボ MTU の設定             | 19 |
| アドバタイズメント間隔の設定           | 19 |

---

**CHAPTER 5****FCoE の設定 21**

|                                       |    |
|---------------------------------------|----|
| FCoE のトポロジ                            | 21 |
| 直接接続された CNA のトポロジ                     | 21 |
| リモート接続された CNA のトポロジ                   | 22 |
| FCoE のベスト プラクティス                      | 22 |
| 直接接続された CNA のベスト プラクティス               | 22 |
| リモート接続された CNA のベスト プラクティス             | 23 |
| ガイドラインと制約事項                           | 25 |
| FC/FCoE の構成                           | 26 |
| TCAM カービングの実行                         | 26 |
| LLDP の設定                              | 27 |
| デフォルトQoSの設定                           | 27 |
| ユーザー定義の QoS の構成                       | 28 |
| トラフィック シェーピングの設定                      | 30 |
| vPC を伴う FCoE の設定例                     | 30 |
| Cisco Nexus 9000 シリーズ スイッチの vPC の設定例  | 31 |
| Cisco Nexus 9000 シリーズ スイッチの FCoE の設定例 | 36 |
| QoS の設定                               | 41 |
| TCAM カービングに関する情報                      | 42 |
| ユーザー定義テンプレートに関する情報                    | 44 |
| ユーザー定義テンプレートの作成                       | 47 |
| ユーザー定義テンプレートに関する情報                    | 48 |
| ユーザー定義テンプレートの変更                       | 51 |

|                    |    |
|--------------------|----|
| ユーザー定義テンプレートに関する情報 | 53 |
| ユーザー定義テンプレートのコミット  | 57 |
| ユーザー定義テンプレートに関する情報 | 59 |
| テンプレートの削除          | 62 |
| ユーザー定義テンプレートに関する情報 | 63 |
| TCAM カービング設定の確認    | 67 |
| FCoE 設定の確認         | 67 |

---

|                  |   |           |
|------------------|---|-----------|
| <b>CHAPTER 6</b> | <b>Configuring Long-distance Over FCoE</b>                      | <b>69</b> |
|                  | Configuring Long-distance Over FCoE                             | 69        |
|                  | Configurations for Different Types of Policies                  | 70        |
|                  | Configuration Examples of Policy Applied to Ethernet Interfaces | 72        |
|                  | Verifying Configuration of Long-Distance Over FCoE              | 72        |

---

|                  |                             |           |
|------------------|-----------------------------|-----------|
| <b>CHAPTER 7</b> | <b>ファイバチャネル インターフェイスの構成</b> | <b>73</b> |
|                  | ファイバチャネル インターフェイスについて       | 73        |
|                  | ファイバチャネル インターフェイスについて       | 73        |
|                  | 仮想ファイバチャネル インターフェイス         | 73        |
|                  | VF ポート                      | 74        |
|                  | VE ポート                      | 74        |
|                  | VNP ポート                     | 76        |
|                  | インターフェイス モード                | 76        |
|                  | E ポート                       | 76        |
|                  | F ポート                       | 77        |
|                  | NP ポート                      | 77        |
|                  | TE ポート                      | 77        |
|                  | TF ポート                      | 77        |
|                  | TNP ポート                     | 78        |
|                  | SD ポート                      | 78        |
|                  | auto モード                    | 78        |
|                  | インターフェイスの状態                 | 78        |
|                  | 管理ステート                      | 78        |

|                              |     |
|------------------------------|-----|
| 動作ステート                       | 79  |
| 理由コード                        | 79  |
| バッファツールバッファ クレジット            | 82  |
| ファイバチャネルのライセンス要件             | 83  |
| ファイバチャネルポートライセンスの有効化         | 83  |
| ファイバチャネルの QoS 要件             | 84  |
| QoS の構成による no-drop のサポート     | 84  |
| 物理ファイバチャネル インターフェイス          | 95  |
| 長距離 ISL                      | 95  |
| ファイバチャネル インターフェイスの構成         | 96  |
| ファイバチャネル インターフェイスの構成         | 96  |
| ファイバチャネル インターフェイスの範囲の構成      | 97  |
| インターフェイスの管理状態の設定             | 98  |
| インターフェイス モードの設定              | 98  |
| インターフェイスの説明の構成               | 100 |
| ユニファイド ポートの設定                | 101 |
| ポート速度の設定                     | 104 |
| トランク モードの構成                  | 105 |
| コメント                         | 106 |
| 自動検知                         | 106 |
| ブレイクアウトによる FC ポートの変換         | 107 |
| ブレイクアウト インターフェイスでの速度の変更      | 108 |
| SD ポート フレーム カプセル化の設定         | 108 |
| 受信データ フィールド サイズの構成           | 108 |
| ビット エラーしきい値を理解する             | 109 |
| バッファ間クレジットの構成                | 111 |
| 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 | 112 |
| スイッチ ポート属性のデフォルト値の構成         | 112 |
| N ポート識別子仮想化について              | 113 |
| N ポート識別子仮想化のイネーブル化           | 114 |
| ポート チャネルの設定例                 | 115 |

|                           |     |
|---------------------------|-----|
| ファイバチャネル インターフェイスの確認      | 115 |
| SFP トランスミッタ タイプの確認        | 115 |
| インターフェイス情報の検証             | 116 |
| BB_Credit 情報の確認           | 117 |
| ファイバチャネル インターフェイスのデフォルト設定 | 118 |
| ファイバチャネル インターフェイスの構成0     | 119 |

---

**CHAPTER 8**

|                            |            |
|----------------------------|------------|
| <b>VSAN の設定と管理</b>         | <b>121</b> |
| VSAN の設定と管理                | 121        |
| VSAN に関する情報                | 121        |
| VSAN トポロジ                  | 122        |
| VSAN の利点                   | 123        |
| VSAN とゾーン                  | 123        |
| VSAN の注意事項と制限事項            | 124        |
| VSAN の作成について               | 125        |
| VSAN の静的な作成                | 126        |
| ポート VSAN メンバーシップ           | 127        |
| スタティック ポート VSAN メンバーシップの概要 | 127        |
| VSAN スタティック メンバーシップの表示     | 128        |
| デフォルト VSAN                 | 129        |
| 独立 VSAN                    | 129        |
| 分離された VSAN メンバーシップの概要      | 130        |
| VSAN の動作ステート               | 130        |
| スタティック VSAN の削除            | 130        |
| スタティック VSAN の削除            | 131        |
| ロード バランシングの概要              | 132        |
| ロード バランシングの設定              | 132        |
| interop モード                | 133        |
| スタティック VSAN 設定の表示          | 133        |
| VSAN のデフォルト設定              | 134        |

## CHAPTER 9

## SAN ポート チャネルの設定 135

## SAN ポート チャネルの設定 135

## SAN ポートチャネルに関する情報 135

## ポートチャネルと VSAN トランキングの理解 136

## ロード バランシングを理解する 137

## SAN ポート チャネルの設定 138

## SAN ポート チャネルの設定時の注意事項 138

## SAN ポート チャネルの作成 140

## ポートチャネル モードについて 141

## SAN ポート チャネルの削除について 143

## SAN ポート チャネルのインターフェイス 144

## 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 144

## SAN ポート チャネルへのインターフェイスの追加 145

## インターフェイスの強制追加 146

## 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 147

## SAN ポート チャネルからのインターフェイスの削除 148

## SAN ポートチャネルプロトコル 148

## チャンネル グループの作成について 149

## 自動作成の注意事項 150

## 自動作成の有効化および構成 151

## 手動設定チャンネル グループについて 152

## 手動構成チャンネル グループへの変更 152

## ポート チャネルの設定例 152

## SAN ポート チャネル構成の確認 153

## SAN ポート チャネルのデフォルト設定 154

## CHAPTER 10

## ファイバチャネル ドメイン パラメータの構成 157

## ドメイン パラメータに関する情報 157

## ファイバチャネル ドメイン 157

## ドメインの再起動 158

|                                 |     |
|---------------------------------|-----|
| ドメインの再起動                        | 158 |
| ドメイン マネージャの高速再起動                | 159 |
| ドメイン マネージャの高速再起動の有効化            | 159 |
| スイッチの優先度                        | 160 |
| スイッチ優先順位の構成                     | 160 |
| fcdomain の開始について                | 161 |
| fcdomain の無効化または再有効化            | 161 |
| ファブリック名の構成                      | 162 |
| 着信 RCF                          | 162 |
| 着信 RCF の拒否                      | 163 |
| マージされたファブリックの自動再構成              | 163 |
| 自動再構成の有効化                       | 164 |
| ドメイン ID                         | 165 |
| ドメイン ID - 注意事項                  | 165 |
| スタティック ドメイン ID または優先ドメイン ID の設定 | 166 |
| 許可ドメイン ID リスト                   | 167 |
| 許可ドメイン ID リストの構成                | 168 |
| 許可ドメイン ID リストの CFS 配信           | 168 |
| 配信のイネーブル化                       | 169 |
| ファブリックのロック                      | 169 |
| 変更のコミット                         | 170 |
| 変更の破棄                           | 170 |
| ファブリックのロックのクリア                  | 171 |
| CFS 配信ステータスの表示                  | 171 |
| 保留中の変更の表示                       | 171 |
| セッション ステータスの表示                  | 172 |
| 連続ドメイン ID の割り当て                 | 172 |
| 連続ドメイン ID 割り当ての有効化              | 172 |
| FC ID                           | 173 |
| 永続的 FC ID                       | 174 |
| 永続的 FC ID 機能の有効化                | 174 |

|                          |     |
|--------------------------|-----|
| 永続的 FC ID 設定時の注意事項       | 175 |
| 永続的 FC ID の構成            | 175 |
| HBA に対する一意のエリア FC ID     | 176 |
| HBA に対する一意のエリア FC ID の設定 | 177 |
| 固定的 FC ID の選択消去          | 178 |
| 永続的 FC ID の消去            | 179 |
| fcdomain 構成の確認           | 179 |
| ファイバチャネル ドメインのデフォルト設定    | 180 |

**CHAPTER 11****FCoE の VLAN および仮想インターフェイスの設定 183**

|  |     |
|--|-----|
| 仮想インターフェイスの概要                          | 183 |
| FCoE VLAN および仮想インターフェイスに関する注意事項および制約事項 | 184 |
| 仮想インターフェイスの設定                          | 186 |
| VSAN から VLAN へのマッピング                   | 186 |
| 仮想ファイバチャネルインターフェイスの作成                  | 187 |
| vFC インターフェイスの構成                        | 189 |
| 仮想ファイバチャネルインターフェイスと VSAN との関連付け        | 190 |
| 暗黙的仮想ファイバチャネルポートチャネルインターフェイスの作成        | 191 |
| 仮想ファイバチャネルの設定: ポートチャネルインターフェイス         | 193 |
| 仮想インターフェイスの確認                          | 194 |
| VSAN から VLAN へのマッピングの設定例               | 197 |
| FCoE over Enhanced vPC                 | 199 |
| FCoE over Enhanced vPC の設定             | 200 |
| vPC による SAN ブート                        | 203 |
| vPC による SAN ブートの設定例                    | 203 |

**CHAPTER 12****FLOGI、ネームサーバー、および RSCN データベースの管理 205**

|                                  |     |
|----------------------------------|-----|
| FLOGI、ネームサーバー、および RSCN データベースの管理 | 205 |
| ファブリック ログイン                      | 205 |
| ネームサーバープロキシ                      | 206 |
| ネームサーバプロキシの登録について                | 206 |

|                        |     |
|------------------------|-----|
| 名前サーバープロキシの登録          | 206 |
| 重複 pWWN の拒否            | 207 |
| 重複 pWWN の拒否            | 207 |
| 名前サーバーデータベース エントリ      | 208 |
| 名前サーバーのデータベース エントリの表示  | 208 |
| FDMI                   | 210 |
| FDMI の表示               | 211 |
| RSCN                   | 213 |
| RSCN 情報の概要             | 213 |
| RSCN 情報の表示             | 213 |
| multi-pid オプション        | 214 |
| [multi-pid] オプションの設定   | 215 |
| 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          | 216 |
| RSCN タイマーの設定           | 216 |
| RSCN タイマー設定の確認         | 218 |
| RSCN タイマー設定の配布         | 218 |
| RSCN のデフォルト設定          | 221 |

## CHAPTER 13

## DDAS 223

## DDAS 223

|   |     |
|---|-----|
| デバイスエイリアスについての情報                          | 223 |
| デバイスエイリアスの機能                              | 223 |
| デバイスエイリアスの前提条件                            | 224 |
| ゾーンエイリアスとデバイスエイリアスの比較                     | 224 |
| デバイスエイリアス データベース                          | 225 |
| デバイスエイリアスの作成                              | 225 |
| デバイスエイリアスのモード                             | 226 |
| デバイスエイリアス サービスに対するデバイスエイリアスのモードの注意事項と制限事項 | 227 |
| デバイスエイリアス モードの設定                          | 228 |
| デバイスエイリアスの配布                              | 229 |

|                              |     |
|------------------------------|-----|
| ファブリックのロック                   | 229 |
| 変更のコミット                      | 229 |
| 変更の破棄                        | 230 |
| ファブリック ロックの上書き               | 231 |
| 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 | 232 |
| レガシー ゾーン エイリアスの構成            | 233 |
| ゾーン エイリアスのインポート              | 233 |
| デバイス エイリアス データベースの結合の注意事項    | 234 |
| デバイス エイリアス構成の確認              | 234 |
| デバイス エイリアス サービスのデフォルト設定      | 235 |

## CHAPTER 14

## ゾーンの設定と管理 237

|                        |     |
|------------------------|-----|
| ゾーンに関する情報              | 237 |
| ゾーン分割に関する情報            | 237 |
| ゾーン分割の特徴               | 237 |
| ゾーン分割の例                | 239 |
| ゾーン実装                  | 240 |
| アクティブおよびフル ゾーン セット     | 240 |
| ゾーンの設定                 | 241 |
| 設定例                    | 242 |
| ゾーン セット                | 244 |
| ゾーン セットのアクティブ化         | 244 |
| デフォルト ゾーン              | 245 |
| デフォルト ゾーン のアクセス権限の設定   | 245 |
| FC エイリアスの作成            | 246 |
| FC エイリアスの作成            | 247 |
| ゾーン セットの作成とメンバ ゾーン の追加 | 249 |
| ゾーンの実行                 | 250 |
| ゾーン セットの配信             | 251 |
| フル ゾーン セットの配信のイネーブル化   | 251 |
| ワンタイム配信のイネーブル化         | 252 |

|  |     |
|--|-----|
| リンクの分離からの回復                                  | 252 |
| ゾーンセットのインポートおよびエクスポート                        | 253 |
| ゾーンセットの複製                                    | 253 |
| ゾーンセットのコピー                                   | 254 |
| ゾーン、ゾーンセット、およびエイリアスの名前の変更                    | 254 |
| ゾーンのクローニング、ゾーンセットと FC エイリアス                  | 255 |
| ゾーン サーバー データベースのクリア                          | 256 |
| ゾーン設定の確認                                     | 257 |
| 拡張ゾーン分割                                      | 257 |
| 拡張ゾーン分割                                      | 257 |
| 基本ゾーン分割から拡張ゾーン分割への変更                         | 259 |
| 拡張ゾーン分割から基本ゾーン分割への変更                         | 259 |
| 拡張ゾーン分割のイネーブル化                               | 260 |
| ゾーン データベースの変更                                | 260 |
| ゾーン データベース ロックの解除                            | 261 |
| 拡張ゾーン情報の確認                                   | 262 |
| データベースのマージ                                   | 262 |
| ゾーン マージ制御ポリシーの設定                             | 263 |
| デフォルトのゾーン ポリシー                               | 264 |
| システムのデフォルト ゾーン分割設定値の設定                       | 264 |
| スマート ゾーン分割の概要                                | 266 |
| スマート ゾーン分割のメンバー設定                            | 266 |
| VSAN でのスマート ゾーン分割の有効化                        | 267 |
| スマート ゾーン分割のデフォルト値の設定                         | 267 |
| スマート ゾーン分割へのゾーンの自動変換                         | 268 |
| ゾーン メンバーのデバイス タイプの設定                         | 269 |
| スマート ゾーン分割設定の削除                              | 269 |
| 基本ゾーン分割モードにおけるゾーン レベルでのスマート ゾーン分割の無効化        | 270 |
| 拡張ゾーン分割モードの VSAN に対するゾーン レベルでのスマート ゾーン分割の無効化 | 271 |
| ゾーン データベースの圧縮                                | 271 |

ゾーンおよびゾーン セットの分析 272

ゾーンのデフォルト設定 272

---

**CHAPTER 15****拡張ファイバ チャネル機能 275**

拡張ファイバ チャネル機能および概念 275

ファイバチャネル タイムアウト値 275

すべての VSAN のタイマー設定 275

VSAN ごとのタイマー設定 276

fctimer の配布 277

fctimer の配布の有効化と無効化 278

fctimer 設定変更のコミット 278

fctimer 設定変更の廃棄 279

ファブリック ロックの上書き 279

ファブリック データベースの結合の注意事項 280

構成された fctimer 値の確認 280

World Wide Names (WWN) 281

WWN 設定の確認 281

リンク初期化 WWN の使用方法 282

セカンダリ MAC アドレスの設定 282

HBA の FC ID 割り当て 283

デフォルトの企業 ID リスト 283

企業 ID の設定の確認 284

スイッチの相互運用性 285

Interop モードの概要 285

interop モード 3 の設定 287

相互運用ステータスの確認 289

高度なファイバチャネル機能のデフォルト設定 293



## はじめに

この前書きは、次の項で構成されています。

- [対象読者](#) (xv ページ)
- [表記法](#) (xv ページ)
- [Cisco Nexus 9000 シリーズ スイッチの関連資料](#) (xvi ページ)
- [マニュアルに関するフィードバック](#) (xvi ページ)
- [通信、サービス、およびその他の情報](#) (xvii ページ)

## 対象読者

このマニュアルは、Cisco Nexus スイッチの設置、設定、および維持に携わるネットワーク管理者を対象としています。

## 表記法

コマンドの説明には、次のような表記法が使用されます。

| 表記法           | 説明   |
|---------------|--|
| <b>bold</b>   | 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。                     |
| <i>italic</i> | イタリック体の文字は、ユーザが値を指定する引数です。                               |
| [x]           | 省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。                     |
| [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、角かっこで囲み、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、波かっこで囲み、縦棒で区切って示しています。 |

| 表記法         | 説明  |
|-------------|---|
| [x {y   z}] | 角かっこまたは波かっこ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。角かっこ内の波かっこと縦棒は、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。イタリック体を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ないでください。引用符を使用すると、その引用符も含めて string と見なされます。                          |

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、スクリーン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。 |

## Cisco Nexus 9000 シリーズ スイッチの関連資料

Cisco Nexus 9000 シリーズ スイッチ全体のマニュアルセットは、次の URL にあります。

[https://www.cisco.com/en/US/products/ps13386/tsd\\_products\\_support\\_series\\_home.html](https://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.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。ご協力をお願いいたします。

## 通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、[Cisco Services](#) にアクセスしてください。
- サービス リクエストを送信するには、[Cisco Support](#) にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco DevNet \[英語\]](#) にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。

## Cisco バグ検索ツール

[シスコバグ検索ツール](#) (BST) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

## マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。





# CHAPTER 1

## New and Changed Information

---

- [New and Changed Information](#), on page 1

## New and Changed Information

*Table 1: New and Changed Features*

| Feature | Description                            | Changed in Release | Where Documented |
|---------|--|--------------------|------------------|
| NA      | No new features added in this release. | 10.5(1)F           | NA               |





## 第 2 章

# SAN スイッチングのハードウェア サポート

- [SAN スイッチングのハードウェア サポート \(3 ページ\)](#)

## SAN スイッチングのハードウェア サポート

次の表に、SAN スイッチングをサポートする Cisco Nexus 9000 シリーズ ハードウェアを示します。

表 2: Cisco Nexus 9300 シリーズスイッチ: サポートするハードウェア

| モデル (PID)        | FC E ポート | FCoE E ポート | FC エッジ ポート | FCoE エッジ ポート | FEX サポート |
|------------------|----------|------------|------------|--------------|----------|
| N9K-C9336C-FX2-E | ○        | はい         | はい         | はい           | いいえ      |
| N9K-C93180YC-FX  | はい       | はい         | はい         | はい           | いいえ      |
| N9K-C93360YC-FX2 | はい       | はい         | はい         | はい           | いいえ      |



(注) Cisco NX-OS リリース 10.2(3)F 以降、FCoE E ポートがサポートされています。

次の FC SFP がサポートされています。

- DS-SFP-4X32G-SW は N9K-C9336C-FX2-E でのみサポートされます
- DS-SFP-FC8G-SW は N9K-C93180YC-FX および N9K-C93360YC-FX2 でのみサポートされます
- DS-SFP-FC16G-SW は N9K-C93180YC-FX および N9K-C93360YC-FX2 でのみサポートされます
- DS-SFP-FC32G-SW は N9K-C93180YC-FX および N9K-C93360YC-FX2 でのみサポートされます
- DS-SFP-FC32G LW は長距離 ISL でのみサポートされます (N9K-C93180YC-FX でサポート)





## CHAPTER 3

### 概要

---

この章は、次の内容で構成されています。

- [ライセンス要件](#) (5 ページ)
- [SAN スイッチングの概要](#) (5 ページ)
- [SAN スイッチングの一般的な注意事項と制限事項](#) (10 ページ)

## ライセンス要件

Cisco NX-OS ライセンス方式の推奨の詳細と、ライセンスの取得および適用の方法については、『[Cisco NX-OS ライセンス ガイド](#)』および『[Cisco NX-OS ライセンス オプション ガイド](#)』を参照してください。

## SAN スイッチングの概要

この章では、Cisco Nexus 9000 デバイスの SAN スイッチングの概要について説明します。この章は、次の項で構成されています。

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。

### ドメインパラメータ

ファイバチャネルドメイン (fcdomain) 機能では、FC-SW-2 標準で記述されているように、主要スイッチ選択、ドメイン ID 配信、FC ID 割り当て、ファブリック再設定機能が実行されます。ドメインは VSAN 単位で設定されます。ドメイン ID を設定しない場合、ローカルスイッチはランダムな ID を使用します。

### N ポート仮想化

Cisco NX-OS ソフトウェアは業界標準の N ポート ID バーチャライゼーション (NPIV) をサポートします。NPIV を使用すると、単一の物理ファイバチャネルリンクで複数の N ポートファブリックが同時にログインできます。NPIV をサポートする HBA では、ホスト上の各仮想マシン (OS パーティション) についてゾーン分割とポートセキュリティを個別に設定できるようにす

ることで、SAN セキュリティを改善できます。NPIV はサーバ接続に有効だけでなく、コアおよびエッジの SAN スイッチ間の接続にも有効です。

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

N ポート バーチャライザ (NPV) は、コアエッジ SAN のファイバチャネル ドメイン ID 数を減らすことができる補完的な機能です。NPV モードで動作する Cisco Nexus 9000 シリーズ 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。

### 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 チャンネル

ポートチャンネルは、ファイバチャネル トラフィックについて、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) をポートチャン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、特定のプライマリ 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、ポートチャン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ンネル設定情報を交換するときにはプロトコルを使用するので、ポートチャン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 でのポートチャン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、チャンネル 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。

ポートチャンネルでは、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。ポートチャン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 のスケーラビリティ、アベイラビリティ、管理性、およびネットワーク セキュリティを高めることができます。

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 内にファブリックの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ために役立ちます。VSAN は、アベイラビリティを低下させることなく、分離された SAN アイランドを共通のインフラストラクチャに容易に統合できるようにすることで、コスト削減に貢献します。

ユーザーは、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 に対するユーザー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 のトランッキングも実装します。トランッキングでは、ISL (スイッチ間リンク) によって、同じ物理リンク上で複数の VSAN のトラフィックを伝送できます。

### ゾーン分割

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

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

- **LUNゾーン分割:** Nポートゾーン分割と組み合わせて使用すると、論理ユニット番号 (LUN) ゾーン分割は、特定のホストだけがLUNにアクセスできるようにし、異種ストレージサブシステム アクセスを管理するための単一制御点を提供します。
- **読み取り専用ゾーン:** 属性を設定して、任意のゾーンタイプでのI/O操作をSCSI読み取り専用コマンドに制限できます。この機能は、バックアップ、データ ウェアハウジングなど、サーバー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ーに制限できます。

厳密なネットワーク セキュリティを実現するため、入力スイッチで適用されるアクセス コントロールリスト (ACL) を使用して、ゾーン分割はフレームごとに常に適用されます。すべてのゾーン分割ポリシーはハードウェアで適用され、パフォーマンスの低下を引き起こすことはありません。拡張ゾーン分割セッション管理機能では、一度に1人のユーザー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、ネームサーバーに論理ユニット番号 (LUN) を登録しません。SCSI LUN 検出機能は、CLI (コマンドライン インターフェイス) またはSNMP (簡易ネットワーク管理プロトコル) を通して、オンデマンドで開始されます。近接スイッチがCisco Nexus デバイスに属する場合、この情報は近接スイッチとも同期されます。

### 拡張ファイバ チャネル機能

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

単一のスイッチに WWN を一意に関連付ける必要があります。主要スイッチを選択するとき、およびドメイン ID を割り当てるときは、WWN を使用します。Cisco Nexus デバイスは、3 つの Network Address Authority (NAA) アドレス フォーマットをサポートします。

ファイバチャネル標準では、任意のスイッチの F ポートに接続された N ポートに、一意の FC ID を割り当てする必要があります。使用する FC ID 番号を節約するために、Cisco Nexus デバイスでは特殊な割り当て方式を使用しています。

### FC-SP および DHCHAP

Fibre Channel Security Protocol (FC-SP) は、スイッチ間およびホストとスイッチ間で認証を実行して、企業全体のファブリックに関するセキュリティ問題を解決します。Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP) は、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 の使用により、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っ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。

### ファブリック構成サーバー

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設定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。

## SAN スイッチングの一般的な注意事項と制限事項

次に、SAN スイッチングの一般的な注意事項と制限事項を示します。

- SAN スイッチングは、Cisco Nexus C93180YC-FX および C93360YC-FX2 スイッチでのみサポートされます。Cisco NX-OS リリース 10.2(2)F 以降、SAN スイッチングはCisco N9K-C9336C-FX2-E プラットフォーム スイッチでもサポートされています。
- VE ポートまたは仮想拡張ポート (ISL) は、Cisco NX-OS リリース 10.2(3)F からサポートされています。
- ダイナミック ポート VLAN メンバーシップ (DPVM) はサポートされていません。
- スイッチ モードのファブリック エクステンダ (FEX) はサポートされていません
- IP over Fibre Channel (IPFC) 機能はサポートされていません。
- Inter VSAN Routing (IVR) はサポートされていません
- CLI の XML および DME はサポートされていません。
- OBFL (show logging onboard) 機能のサポートは、エラー統計に限定されています。



(注) OBFL の詳細については、*Cisco Nexus 9000 シリーズ NX-OS* トラブルシューティング ガイド、リリース 9.3(x) を参照してください。

- 8G サーバーおよびターゲット ポートはサポートされていません。
- 8G ISL の場合、ピア スイッチでフィル パターンを IDLE に設定する必要があります。
- Cisco NX-OS リリース 10.2(2) 以降、Cisco Nexus N9K-C9336C-FX2-E プラットフォーム スイッチの動作速度と san-po へのメンバーの追加には、次の制限が課されています。
  - **fc-bo の速度変更:**
    - デフォルトの速度は 32G です。
    - 速度変更は、単一の fc-bo インターフェイス レベルでは実行できません。
    - fc-bo の速度変更は、fc-bo インターフェイス レベルの範囲で行われます。
      - 範囲には、フロント パネルのポートに対応する fc-bo のフルセットが含まれている必要があります。



(注) 範囲の一部を指定すると、速度設定で **ERR\_01** エラーが表示されます。

- san-po の一部である fc-bo を範囲に含めないでください。



(注) 範囲に **san-po** メンバーが含まれている場合、速度設定は **ERR\_02** エラーを表示します。

- 範囲には、複数の前面パネルポートに対応する **fc-bo** ポートを設定できます。

- **san-po** の速度変更:

- **san-po** のデフォルトの速度は 32G です。
- **san-po** の速度変更は、そのメンバーにフロントパネルのポートに対応するすべての **fc-bo** ポートが含まれている場合にのみ許可されます。



(注) **san-po** がフロントパネルポートに対応する **fc-bo** ポートを部分的に設定している場合、速度変更により **ERR\_03** エラーが表示されます。

- **san-po** の速度を変更するには、**san-po** インターフェイスの範囲を指定します。

- 実行中の構成の速度設定:

- 速度設定（デフォルトではない）は、**fc-bo** インターフェイスの範囲レベルで表示されます。 **sh runn** コマンドの個々の **fc-breakout** インターフェイスの下には表示されません。
- 速度設定（デフォルトではない）は、**show interface fc<int no>** コマンドで表示されます。

- **san-po** へのメンバーの追加 (**channel-group x**) :

- インターフェイスの範囲には、フロントパネルのポートに対応する **fc-bo** のフルセットが含まれている必要があります。



(注) チャンネルの追加は成功しますが、一部の範囲に対して **WARN\_01** 警告メッセージが表示されます。

- 範囲には、複数の前面パネルポートに対応する **fc-bo** ポートを設定できます。

```
ERR_01 : if-range contains partial set of fc1/18/1-4 fc-bo ports
ERR_02 : if-range contains fc1/21/1-4 ports; some are part sanpo
ERR_03 : san-port-channel21 does not contain full set of fc1/22/1-4 fc-bo ports
WARN_01 : Warning: if-range contains partial set of fc1/22/1-4 fc-bo ports
```

- Cisco NX-OS リリース 10.2(3)F 以降、ファイバチャネルフォワーダ（FCF）間の仮想 E ポート（VE ポート）接続は、Cisco N9K-C93180YC-FX、N9K-C9336C-FX2-E、および N9K-C93360YC-FX2 プラットフォーム スイッチでサポートされます。



## 第 4 章

# FC/FCoE スイッチ モードの有効化

この章は、次の内容で構成されています。

Cisco Nexus 9000 シリーズスイッチで FC/FCoE スイッチ モードを有効にするには、**feature-set fcoe** を設定する必要があります。



(注) Cisco Nexus 9000 シリーズスイッチで NPV モードを有効にする方法の詳細については、[cisco.com](http://cisco.com) の *Cisco Nexus 9000 Series NX-OS FC-NPV and FCoE-NPV Configuration Guide* を参照してください。

- FCoE 機能を有効にする (13 ページ)
- FC スイッチング モードに関する注意事項と制限事項 (13 ページ)
- FC/FCoE の有効化, on page 14
- FC/FCoE の無効化, on page 15
- FCoE リンクの LAN トラフィックの無効化 (16 ページ)
- FC-Map の設定, on page 17
- ファブリック プライオリティの設定, on page 18
- ジャンボ MTU の設定 (19 ページ)
- アドバタイズメント間隔の設定, on page 19

## FCoE 機能を有効にする

## FC スイッチング モードに関する注意事項と制限事項

- リリース 10.1(1) 以降、FC スイッチモードは Cisco Nexus 93360YC-FX2 でサポートされます。
- リリース 10.2(2) 以降、FC スイッチモードは Cisco Nexus C9336C-FX2-E でサポートされます。
- FC/FCoE 構成はロールバックをサポートしていません。FC/FCoE 構成が存在する場合は、ベストエフォート オプションを使用します。他のすべての構成は成功しますが、FC/FCoE 構成ではエラー メッセージが表示されます。

## FC/FCoE の有効化

スイッチで FC/FCoE をイネーブルにできますが、VLAN 1 で FCoE をイネーブルにすることはできません。



**Note** または、Cisco NX-OS セットアップユーティリティに含まれている FC セットアップスクリプトを使用して、FC/FCoE を有効にすることもできます。詳細については、対応するバージョンの *Cisco Nexus 9000* シリーズ NX-OS 基本設定ガイドを参照してください。 [cisco.com](http://cisco.com) に掲載されています。



**Note** Cisco Nexus デバイスのファイバチャネル機能はすべて、FC プラグインにパッケージ化されています。FC/FCoE を有効にすると、スイッチソフトウェアにより SAN\_ENTERPRISE\_PKG FC\_FEATURES\_PKG ライセンスのチェックが行われます。ライセンスが検出されると、ソフトウェアによりプラグインがロードされます。FC ポート ライセンスを有効にするには、パッケージ FC\_PORT\_ACTIVATION\_PKG が必要です。

FC プラグインのロード後は、次の 2 つが使用可能となります。

- ファイバチャネルおよび FCoE に関するすべての CLI
- インストールされている拡張モジュールのファイバチャネルインターフェイス。

180 日が経過すると、有効なライセンスが消失し、FC プラグインは無効となります。スイッチの次回リブート時に、すべての FC/FCoE コマンドが CLI から削除され、FC/FCoE 設定が消去されます。

### Before you begin

FC\_FEATURES\_PKG (N5010SS または N5020SS) ライセンスがインストールされていることが必要です。次の表に、SAN スイッチングのライセンス要件に関する詳細情報を示します。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **install feature-set fcoe**
3. switch(config)# **feature-set fcoe**

## DETAILED STEPS

## Procedure

|        | Command or Action                               | Purpose                    |
|--------|---|----------------------------|
| Step 1 | switch# <b>configure terminal</b>               | 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。 |
| Step 2 | switch(config)# <b>install feature-set fcoe</b> | 機能セット FCoE をインストールします。     |
| Step 3 | switch(config)# <b>feature-set fcoe</b>         | FC/FCoE 機能を有効にします。         |

## Example

次の例は、スイッチで FC/FCoE を有効にする方法を示しています。

```
switch# configure terminal
switch(config)# install feature-set fcoe
switch(config)# feature-set fcoe
```

## FC/FCoE の無効化

FC/FCoE を無効にすると、すべての FC/FCoE コマンドが CLI から削除され、FC/FCoE 構成が削除されます。



**Note** スイッチに FC ポートがある場合、コマンド **no feature-set fcoe** は許可されません。スイッチに FC ポートがある場合は、このコマンドを発行する前に、それらをイーサネットポートに変換する必要があります。Cisco Nexus C93180YC-FX、C9336C-FX2-E、および C93360YC-FX2 スイッチでは、機能セット **fcoe** を無効にした後にスイッチをリロードする必要があります。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no feature-set fcoe**
3. switch(config)# **no install feature-set fcoe**

## DETAILED STEPS

## Procedure

|        | Command or Action                                  | Purpose                    |
|--------|--|----------------------------|
| Step 1 | switch# <b>configure terminal</b>                  | 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。 |
| Step 2 | switch(config)# <b>no feature-set fcoe</b>         | FC/FCoE 機能を無効にします。         |
| Step 3 | switch(config)# <b>no install feature-set fcoe</b> | 機能セット FCoE をアンインストールします。   |

## Example

次の例は、スイッチの FCoE を無効にする方法を示したものです。

```
switch# configure terminal
switch(config)# no feature-set fcoe
switch(config)# no install feature-set fcoe
```

## FCoE リンクの LAN トラフィックの無効化

FCoE リンクの LAN トラフィックを無効にできます。

DCBXを使用すると、スイッチから、直接接続された CNA へ LAN 論理リンク ステータス (LLS) メッセージを送信できます。CNA へ LLS ダウン メッセージを送信する場合は、**shutdown lan** コマンドを入力します。このコマンドにより、インターフェイスの VLAN のうち、FCoE に対応していないすべての VLAN をダウンできます。インターフェイスの VLAN のうち FCoE に対応している VLAN では、中断されることなくそのまま SAN トラフィックを伝送できます。

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet slot/port**
3. switch(config-if)# **shutdown lan**
4. (任意) switch(config-if)# **no shutdown lan**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                      | 目的                         |
|--------|-----------------------------------|----------------------------|
| Step 1 | switch# <b>configure terminal</b> | グローバルコンフィギュレーションモードを開始します。 |

|        | コマンドまたはアクション  | 目的  |
|--------|---|---|
| Step 2 | switch(config)# <b>interface ethernet slot/port</b> | 設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。<br><br>(注)<br>これが 10G ブレイクアウト ポートの場合、 <i>slot/port</i> 構文は <i>QSFP-module/port</i> になります。 |
| Step 3 | switch(config-if)# <b>shutdown lan</b>              | インターフェイス上のイーサネット トラフィックをシャットダウンします。インターフェイスが FCoE VLAN の一部である場合は、シャットダウンを実行しても、その FCoE トラフィックに影響はありません。                                   |
| Step 4 | (任意) switch(config-if)# <b>no shutdown lan</b>      | インターフェイス上のイーサネット トラフィックを再び有効にします。   |

## FC-Map の設定



**Note** ファブリックの分離を維持し、FC-MAP のデフォルトを残すには、[VLAN への VSAN のマッピング方式](#)を使用することをお勧めします。

対象となる Cisco Nexus デバイスのファイバチャネル ファブリックを識別するための FC-Map を設定することにより、ファブリック間の通信に伴うデータの破損を防ぐことができます。FC-Map が設定されると、現在のファブリックの一部ではない MAC アドレスがスイッチによって廃棄されます。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **fcoe fcmmap fabric-map**
3. (Optional) switch(config)# **no fcoe fcmmap fabric-map**

### DETAILED STEPS

#### Procedure

|        | Command or Action                 | Purpose                     |
|--------|-----------------------------------|-----------------------------|
| Step 1 | switch# <b>configure terminal</b> | 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。 |

|               | Command or Action   | Purpose  |
|---------------|---|--|
| <b>Step 2</b> | switch(config)# <b>fcoe fcmmap fabric-map</b>               | グローバルFC-Mapを設定します。デフォルト値は、0E.FC.00です。有効な範囲は、0E.FC.00～0E.FC.FFです。 |
| <b>Step 3</b> | (Optional) switch(config)# <b>no fcoe fcmmap fabric-map</b> | グローバルFC-Mapをデフォルト値の0E.FC.00にリセットします。                             |

### Example

次に示すのは、グローバルFC-Mapの設定例です。

```
switch# configure terminal
switch(config)# fcoe fcmmap 0x0efc2a
```

## ファブリック プライオリティの設定

Cisco Nexus デバイスはプライオリティをアドバタイズします。ファブリック内のCNAでは、このプライオリティを基に、接続先として最適なスイッチが決定されます。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **fcoe fcf-priority fabric-priority**
3. (Optional) switch(config)# **no fcoe fcf-priority fabric-priority**

### DETAILED STEPS

#### Procedure

|               | Command or Action  | Purpose   |
|---------------|--|---|
| <b>Step 1</b> | switch# <b>configure terminal</b>                                      | 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。                                    |
| <b>Step 2</b> | switch(config)# <b>fcoe fcf-priority fabric-priority</b>               | グローバルファブリックプライオリティを設定します。デフォルト値は128です。有効な範囲は、0（高い）～255（低い）です。 |
| <b>Step 3</b> | (Optional) switch(config)# <b>no fcoe fcf-priority fabric-priority</b> | グローバルファブリックプライオリティをデフォルト値である128にリセットします。                      |

**Example**

次に示すのは、グローバル ファブリック プライオリティの設定例です。

```
switch# configure terminal
switch(config)# fcoe fcf-priority 42
```

## ジャンボ MTU の設定

次の例は、ジャンボ MTU をサポートするようにデフォルトのイーサネット システム クラスを設定する方法を示しています。

```
switch(config)# policy-map type network-qos jumbo
switch(config-pmap-nq)# class type network-qos class-fcoe
switch(config-pmap-c-nq)# pause no-drop
switch(config-pmap-c-nq)# mtu 2158
switch(config-pmap-nq)# class type network-qos class-default
switch(config-pmap-c-nq)# mtu 9216
switch(config-pmap-c-nq)# exit
switch(config-pmap-nq)# exit
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 jumbo
```

## アドバタイズメント間隔の設定

スイッチ上で、ファイバチャネル ファブリックのアドバタイズメント間隔を設定できます。

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config)# **fcoe fka-adv-period interval**
3. (Optional) switch(config)# **no fcoe fka-adv-period interval**

**DETAILED STEPS****Procedure**

|               | Command or Action                                   | Purpose   |
|---------------|---|---|
| <b>Step 1</b> | switch# <b>configure terminal</b>                   | 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。                                |
| <b>Step 2</b> | switch(config)# <b>fcoe fka-adv-period interval</b> | ファブリックのアドバタイズメント間隔を設定します。デフォルト値は 8 秒です。有効な範囲は 4 ~ 60 秒です。 |

|               | Command or Action   | Purpose                                  |
|---------------|---|--|
| <b>Step 3</b> | (Optional) <code>switch(config)# no fcoe fka-adv-period interval</code> | ファブリックのアドバタイズメント間隔を、デフォルト値の 8 秒にリセットします。 |

### Example

次の例は、ファブリックのアドバタイズメント間隔を設定する方法を示したものです。

```
switch# configure terminal  
switch(config)# fcoe fka-adv-period 42
```



## 第 5 章

# FCoE の設定

この章は、次の内容で構成されています。

- FCoE のトポロジ (21 ページ)
- FCoE のベストプラクティス (22 ページ)
- ガイドラインと制約事項 (25 ページ)
- FC/FCoE の構成 (26 ページ)
- FCoE 設定の確認, on page 67

## FCoE のトポロジ

### 直接接続された CNA のトポロジ

Cisco Nexus デバイスは、次の図のようにファイバチャネルフォワーダ (FCF) として配置できます。

図 1: 直接接続された FCF



FCF が FCoE ノード (ENode) と他の FCF との間の中継に使用されないようにするため、FIP フレームは次のルールに従って処理されます。この処理により、異なるファブリック内の ENode と FCF との間のログインセッションも回避されます。

- CNA から受信された FIP の送信要求フレームおよびログイン フレームは FCF により処理され、転送されません。
- FCF が他の FCF からインターフェイスを介して送信要求およびアドバタイズメントを受信すると、次のような処理が実行されます。
  - フレーム内の FC-MAP 値が FCF の FC-MAP 値と一致する (FCF が同一のファブリック内にある) 場合、これらのフレームは無視され、廃棄されます。
  - FIP フレーム内の FC-MAP 値が FCF の FC-MAP 値と一致しない (FCF が異なるファブリック内にある) 場合、インターフェイスが「FCoE 孤立」状態になります。

中継用の Cisco Nexus FCF を経由した場合に限って到達可能な FCF については、CNA から検出することもログインすることもできません。ハードウェアの制約上、Cisco Nexus デバイスでは、CNA と他の FCF との間の FCoE 中継機能は実行できません。

Cisco Nexus FCF では FCoE 中継機能が実行できないため、FCoE VLAN のアクティブな Spanning Tree Protocol (STP) パスが必ず CNA と FCF の間の直接接続されたリンクを経由するようにネットワーク トポロジを設計する必要があります。FCoE VLAN は、直接接続されたリンクに対してだけ設定するようにしてください。

## リモート接続された CNA のトポロジ

Cisco Nexus デバイスは、次の図のようにリモート接続された CNA に対する FCF としては配置できませんが、FIP スヌーピングブリッジとしては配置できません。

図 2: リモート接続された FCF



FCF が ENode と他の FCF との間の中継に使用されないようにするため、FIP フレームは次のルールに従って処理されます。この処理により、異なるファブリック内の ENode と FCF との間のログインセッションも回避されます。

- CNA から受信された FIP の送信要求フレームおよびログインフレームは FCF により処理され、転送されません。
- FCF が他の FCF からインターフェイスを介して送信要求およびアドバタイズメントを受信すると、次のような処理が実行されます。
  - フレーム内の FC-MAP 値が FCF の FC-MAP 値と一致する (FCF が同一のファブリック内にある) 場合、これらのフレームは無視され、廃棄されます。
  - FIP フレーム内の FC-MAP 値が FCF の FC-MAP 値と一致しない (FCF が異なるファブリック内にある) 場合、インターフェイスが「FCoE 孤立」状態になります。

Cisco Nexus FCF では FCoE 中継機能が実行できないため、FCoE VLAN のアクティブな STP パスが必ず CNA と FCF の間の直接接続されたリンクを経由するようにネットワーク トポロジを設計する必要があります。FCoE VLAN は、直接接続されたリンクに対してだけ設定するようにしてください。

## FCoE のベスト プラクティス

### 直接接続された CNA のベスト プラクティス

次の図は、直接接続された CNA と Cisco Nexus デバイスを使用したアクセス ネットワークのベスト プラクティス トポロジを示したものです。

図 3: 直接接続された CNA



上図の配置トポロジに対する設定のベスト プラクティスは次のとおりです。

1. SAN 内の仮想ファブリック (VSAN) ごとにトラフィックを送送できるよう、それぞれの統合アクセススイッチに一意的専用 VLAN を設定する必要があります (VSAN 1 用に VLAN 1002、VSAN 2 用に VLAN 1003 など)。マルチスパンニングツリー (MST) を有効にした場合は、FCoE VLAN に対して別個の MST インスタンスを使用する必要があります。
2. ユニファイドファブリック (UF) リンクをトランクポートとして設定する必要があります。ネイティブ VLAN として FCoE VLAN を設定しないでください。仮想ファイバチャネルインターフェイスの VF\_Port トランッキングおよび VSAN 管理を拡張できるように、すべての FCoE VLAN を UF リンクのメンバとして設定する必要があります。



(注) イーサネットトラフィックおよび FCoE トラフィックはどちらも、統合ワイヤにより伝送されません。

3. UF リンクをスパンニングツリーエッジポートとして設定する必要があります。
4. FCoE トラフィックの伝送用として指定されていないイーサネットリンクのメンバとして FCoE VLAN を設定しないでください。これは、FCoE VLAN に使用する STP のスコープを UF リンクに限定する必要があるためです。
5. LAN の代替パス用に (同一または別の SAN ファブリックにある) 統合アクセススイッチをイーサネットリンク経由で相互に接続する必要がある場合は、すべての FCoE VLAN をメンバーシップから除外することを、これらのリンクに対して明示的に設定する必要があります。この設定により、FCoE VLAN に使用する STP のスコープが UF リンクに限定されます。
6. SAN-A および SAN-B の FCoE に対してはそれぞれ別々の FCoE VLAN を使用する必要があります。



(注) 直接接続されたトポロジでは、すべての Gen-1 (pre-FIP) CNA および Gen-2 (FIP) CNA がサポートされています。

## リモート接続された CNA のベスト プラクティス

次の図は、リモート接続された CNA と Cisco Nexus デバイスを使用したアクセスネットワークのベストプラクティストポロジを示したものです。

図 4: リモート接続された CNA



上図の配置トポロジに対する設定のベスト プラクティスは次のとおりです。

1. SAN 内の仮想ファブリック (VSAN) ごとにトラフィックを伝送できるよう、それぞれの統合アクセススイッチに一意の専用 VLAN を設定する必要があります (VSAN1 用に VLAN 1002、VSAN2 用に VLAN 1003 など)。MST を有効にした場合は、FCoE VLAN に対して別個の MST インスタンスを使用する必要があります。
2. ユニファイドファブリック (UF) リンクをトランク ポートとして設定する必要があります。ネイティブ VLAN として FCoE VLAN を設定しないでください。仮想ファイバチャネルインターフェイスの VF\_Port トランッキングおよび VSAN 管理を拡張できるよう、すべての FCoE VLAN を UF リンクのメンバとして設定する必要があります。




---

(注) イーサネットトラフィックおよび FCoE トラフィックはどちらも、ユニファイドファブリックリンクにより伝送されます。

---

3. CNA およびブレードスイッチを、スパニングツリーエッジポートとして設定する必要があります。
4. 新しいリンクやブレードスイッチのプロビジョニングなど、さまざまなイベントに伴って実行される STP の再コンバージェンスの際に障害が発生しないよう、各ブレードスイッチは、(できれば EtherChannel を介して) ただ 1 つの Cisco Nexus 統合アクセススイッチに接続される必要があります。
5. Cisco Nexus 統合アクセススイッチには、それに接続されているブレードスイッチよりも高い STP プライオリティを設定する必要があります。そうすることで、統合アクセススイッチがスパニングツリーのルートであり、かつそれに接続されているすべてのブレードスイッチがダウンストリーム ノードとなるような FCoE VLAN のアイランドを作成できます。
6. FCoE トラフィックの伝送用として指定されていないイーサネットリンクのメンバとして FCoE VLAN を設定しないでください。これは、FCoE VLAN に使用する STP のスコープを UF リンクに限定する必要があるためです。
7. LAN の代替パス用に、統合アクセススイッチやブレードスイッチをイーサネットリンク経由で相互に接続する必要がある場合は、これらのリンクに対してすべての FCoE VLAN をメンバーシップから除外することを、明示的に設定する必要があります。この設定により、FCoE VLAN に使用する STP のスコープが UF リンクに限定されます。
8. SAN-A および SAN-B の FCoE に対してはそれぞれ別々の FCoE VLAN を使用する必要があります。




---

(注) リモート接続されたトポロジは、Gen-2、Gen-3、Gen-4 (FIP) CNA に限ってサポートされます。

---

## ガイドラインと制約事項

FC/FCoE には、次のガイドラインと制約事項があります。

- Cisco Nexus デバイスの FCoE は、Gen-1 (pre-FIP) CNA および Gen-2 (FIP) CNA 2 をサポートします。Cisco Nexus 2232PP ファブリック エクステンダ (FEX) の FCoE では、Gen-2 CNA に限りサポートされています。
- VLAN 1 では FCoE をイネーブルにできません。
- LLDP はデフォルトでは有効になっていないため、FCoE を有効にするには、**feature lldp** を使用して LLDP 機能を有効にする必要があります。
- 同一の FEX に対して、ストレート型とアクティブ-アクティブを組み合わせたトポロジはサポートされていません。
- FCoE は、銅線 SFP ではサポートされていません。
- FC/FCoE 構成はロールバックをサポートしていません。FC/FCoE 構成が存在する場合は、ベストエフォートオプションを使用します。他のすべての構成は成功しますが、FC/FCoE 構成ではエラーメッセージが表示されます。
- FCoE は 10 ギガビット、25 ギガビット、40 ギガビットおよび 100 ギガビットイーサネットインターフェイスでサポートされます。100G ブレイクアウト (4x25G) および 40G ブレイクアウト (4x10G) は、FCoE インターフェイスでサポートされています。
- Cisco Nexus デバイス インターフェイスのポート チャネルでは、複数のインターフェイスが設定されている場合、直接接続 FCoE (つまりバインドインターフェイスを介して CNA に直接接続された FCoE) はサポートされていません。単一リンクのポート チャネル上では、直接接続 FCoE がサポートされています。これにより、1 つの 10/25/40/100 GB リンクを持つ仮想ポート チャネル (vPC) を介して各アップストリーム スイッチに接続された CNA からの FCoE を実現できます。



- (注) FC/FCoE のデフォルトの Quality of Service (QoS) ポリシーの説明については、ご使用のデバイスの Quality of Service についてのガイドを参照してください。ご使用の Nexus ソフトウェア リリース版を参照してください。このマニュアルの入手可能なバージョンは、次のサイトから取得できます: <https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-installation-and-configuration-guides-list.html>

# FC/FCoE の構成

## TCAM カービングの実行

ここでは、TCAM カービングの実行方法について説明します。

### 手順の概要

1. 機能 FCoE をインストールします。
2. fcoe が完全に機能するように、次のコマンドを設定します（まだ設定されていない場合）。
3. TCAM カービングを実行します。
4. 設定された TCAM リージョンサイズを確認するには、**show hardware access-list tcam region** コマンドを使用します。
5. 構成を保存し、コマンド **reload** を使用して、スイッチをリロードします。

### 手順の詳細

#### 手順

**Step 1** 機能 FCoE をインストールします。

```
switch(config)# install feature-set fcoe
switch(config)# switch(config)# feature-set fcoe
```

**Step 2** fcoe が完全に機能するように、次のコマンドを設定します（まだ設定されていない場合）。

```
hardware access-list tcam region ing-ifacl 256
hardware access-list tcam region ing-redirect 256
```

256 は、FC/FCoE の ing-ifacl および ing-redirect リージョンに必要な最小 tcam スペースです。

（注）

現在の tcam の構成を確認するには、show hardware access-list tcam region コマンドを使用します。

必要な tcam スペースが使用できない場合は、hardware access-list tcam region ing-racl 1536 コマンドを使用して ing-racl リージョンを縮小できます。

**Step 3** TCAM カービングを実行します。

例:

```
Switch(config)# hardware access-list tcam region ing-racl 1536
Switch(config)# hardware access-list tcam region ing-ifacl 256
Switch(config)# hardware access-list tcam region ing-redirect 256
```

**Step 4** 設定された TCAM リージョンサイズを確認するには、**show hardware access-list tcam region** コマンドを使用します。

例:

```
Switch(config)# show hardware access-list tcam region
Switch(config)#
```

**Step 5** 構成を保存し、コマンド **reload** を使用して、スイッチをリロードします。

例:

```
Switch(config)# reload
Switch(config)#
```

---

### 次のタスク

TCAM のカービング後には、スイッチをリロードする必要があります。

## LLDP の設定

ここでは、LLDP の設定方法について説明します。

### 手順の概要

1. **configure terminal**
2. **[no] feature lldp**

### 手順の詳細

#### 手順

---

**Step 1** **configure terminal**

グローバル設定モードを開始します。

**Step 2** **[no] feature lldp**

デバイス上で LLDP をイネーブルまたはディセーブルにします。LLDP はデフォルトでディセーブルです。

---

## デフォルト QoS の設定

FCoE のデフォルト ポリシーには、ネットワーク QoS、出力キューイング、入力キューイング、QoS の 4 種類があります。FCoE デフォルトポリシーを有効にするには、**feature-set fcoe command** コマンドを使用して FCoE NPV 機能を有効にします。デフォルトの QoS 入力ポリシーである **default-fcoe-in-policy** は、すべての FC および SAN ポート チャネル インターフェイスに暗黙的に付加され、FC から FCoE へのトラフィックを可能にします。これは、**show interface {fc slot/port}**

`san-port-channel <no>} all` を使用して確認できます。デフォルトの QoS ポリシーは、すべての FC および FCoE トラフィックに CoS3 および Q1 を使用します。

## ユーザー定義の QoS の構成

FCoE トラフィックに別のキューまたは CoS 値を使用するには、ユーザー定義のポリシーを作成します。トラフィックが異なるキューまたは CoS を使用できるようにするには、ユーザー定義の QoS 入力ポリシーを作成し、FC インターフェイスと FCoE インターフェイスの両方に明示的にアタッチする必要があります。ユーザー定義の QoS ポリシーを作成し、システム全体の QoS に対してアクティブにする必要があります。



- (注) FCoE をサポートするには、イーサネットまたはポートチャネルインターフェイスを MTU 9216 (または使用可能な最大 MTU サイズ) で構成する必要があります。

次の例は、すべての FC および FCoE トラフィックに CoS3 および Q2 を使用するユーザー定義の QoS ポリシーを設定し、アクティブにする方法を示しています。

- ユーザー定義のネットワーク QoS ポリシーの設定:

```
switch(config)# policy-map type network-qos fcoe_nq
switch(config-pmap-nqos)# class type network-qos c-nq1
switch(config-pmap-nqos-c)# mtu 1500
switch(config-pmap-nqos-c)# class type network-qos c-nq2
switch(config-pmap-nqos-c)# mtu 9216
switch(config-pmap-nqos-c)# pause pfc-cos 3
switch(config-pmap-nqos-c)# class type network-qos c-nq3
switch(config-pmap-nqos-c)# mtu 1500
switch(config-pmap-nqos-c)# class type network-qos c-nq-default
switch(config-pmap-nqos-c)# mtu 1500
switch(config-pmap-nqos-c)# exit
switch(config-pmap-nqos)# exit
switch(config)#
```

- ユーザー定義の入力キューイング ポリシーの作成:

```
switch(config)# policy-map type queuing fcoe-in-policy
switch(config-pmap-que)# class type queuing c-in-q2
switch(config-pmap-c-que)# bandwidth percent 50
switch(config-pmap-c-que)# class type queuing c-in-q-default
switch(config-pmap-c-que)# bandwidth percent 50
switch(config-pmap-c-que)# exit
switch(config-pmap-que)# exit
switch(config)#
```

- ユーザー定義の出力キューイング ポリシーの作成:

```
switch(config)# policy-map type queuing fcoe-out-policy
switch(config-pmap-que)# class type queuing c-out-q3
switch(config-pmap-c-que)# priority level 1
switch(config-pmap-c-que)# class type queuing c-out-q-default
switch(config-pmap-c-que)# bandwidth remaining percent 50
switch(config-pmap-c-que)# class type queuing c-out-q1
switch(config-pmap-c-que)# bandwidth remaining percent 0
switch(config-pmap-c-que)# class type queuing c-out-q2
```

```
switch(config-pmap-c-que)# bandwidth remaining percent 50
switch(config-pmap-c-que)# exit
switch(config-pmap-que)# exit
switch(config)#
```

- ユーザー定義の QoS 入力ポリシーの作成:

```
switch(config)# class-map type qos match-any fcoe
switch(config-cmap-qos)# match protocol fcoe
switch(config-cmap-qos)# match cos 3
switch(config-cmap-qos)# exit
switch(config)#
switch(config)# policy-map type qos fcoe_qos_policy
switch(config-pmap-qos)# class fcoe
switch(config-pmap-c-qos)# set cos 3
switch(config-pmap-c-qos)# set qos-group 2
switch(config-pmap-c-qos)# exit
switch(config-pmap-qos)# exit
switch(config)#
```

- ユーザー定義のシステム QoS ポリシーのアクティブ化:

```
switch(config)# system qos
switch(config-sys-qos)# service-policy type queuing input fcoe-in-policy
switch(config-sys-qos)# service-policy type queuing output fcoe-out-policy
switch(config-sys-qos)# service-policy type network-qos fcoe_nq
switch(config-sys-qos)# exit
switch(config)#
```

- FC または FCoE インターフェイスへの QoS 入力ポリシーの適用:

```
switch# conf
switch(config)# interface {fc <slot>/<port> | ethernet <slot>/<port> | san-port-channel
<no> | port-channel <no>}
switch(config-if)# service-policy type qos input fcoe_qos_policy
```

- FC または FCoE インターフェイスからの QoS 入力ポリシーの削除:

```
switch# conf
switch(config)# interface {fc <slot>/<port> | ethernet <slot>/<port> | san-port-channel
<no> | port-channel <no>}
switch(config-if)# no service-policy type qos input fcoe_qos_policy
```

- FC または FCoE インターフェイスに適用される QoS 入力ポリシーの確認:

```
switch# show running-config interface {fc <slot>/<port> | interface <slot>/<port> |
san-port-channel <no> | port-channel <no>} all
```



(注)

- ユーザー定義の QoS ポリシーを使用する場合、同じ QoS 入力ポリシーをスイッチ内のすべての FC および FCoE インターフェイスに適用する必要があります。
- FCoE トラフィックは単一の CoS でのみサポートされるため、複数の QoS クラス マップで **match protocol fcoe** を設定しないでください。

## トラフィック シェーピングの設定

トラフィック シェーピングにより、使用可能な帯域幅へのアクセスの制御、および送信されたトラフィックがリモートのターゲットインターフェイスのアクセス速度を超える場合に発生する輻輳を回避するために、トラフィックのフローを規制できます。トラフィック シェーピングはデータの伝送レートを制限するため、このコマンドは必要な場合にのみ使用できます。

次の例は、トラフィック シェーパの構成方法を示しています。

- 次のコマンドは、すべての FC インターフェイスのデフォルトのシステム レベル設定を表示します。

```
switch(config)# show running-config all | i i rate
hardware qos fc rate-shaper
switch(config)#
```

- 次の例は、レートシェーパの構成方法を示しています。このコマンドは、すべての FC インターフェイスに適用されます。



- (注) まれに、4G、8G、16G、または 32G インターフェイスのいずれかで入力廃棄が発生することがあります。レートシェーブを設定するには、*hardware qos fc rate-shaper [low]* コマンドを使用します。これはシステムレベルの設定であるため、すべての FC ポートに適用され、すべての FC ポートのレートが低下します。*hardware qos fc rate-shaper* コマンドのデフォルト オプションは、すべての FC インターフェイスに適用できません。

```
switch(config)# hardware qos fc rate-shaper low
switch(config)#
switch(config)#end
```

## vPC を伴う FCoE の設定例

Cisco NX-OS リリース 9.3(5) 以降、Cisco Nexus N9K-93180YC-FX デバイスは vPC をサポートし、Cisco NX-OS リリース 10.1(1) 以降、Cisco Nexus N9K-C93360YC-FX2 デバイスも vPC をサポートします。Cisco Nexus N9K-93180YC-FX、N9K-C9336C-FX2-E、および N9K-C93360YC-FX2 デバイスは vPC をサポートします。vPCscan は、帯域幅を増やし、イーサネット ファブリックへのロードバランシングを強化するように設定できます。次に、Cisco Nexus 9000 シリーズスイッチで vPC を使用するとき FCoE を設定する方法を説明する設定例を示します。

図 5: ホスト vPC での FCoE トラフィック フロー



図 6: Nexus 9000 FCoE および vPC ラボ トポロジ



---

(注) FCoE VLAN は、vPC ピア リンク間でトランキングしないでください。

---



---

(注) コア スイッチに接続する Cisco Nexus N9K-93180YC-FX スイッチ (スイッチモード) では、FC アップリンクのみがサポートされます。

---

設定例では、次のパラメータが含まれています。

```
switchname: tme-switch-1
switchname: tme-switch-2
mgmt ip: 172.25.182.66
mgmt ip: 172.25.182.67
```

設定例には、次のハードウェアが含まれています。

- Dell サーバ PE2950
- Emulex CNA または CISCO CNA
- Cisco NX-OS リリース 9.3(5)10.2(1)F 以降のリリースを実行している 2 つの Cisco Nexus 9000 スイッチ。

設定例は次の考慮事項と要件を含んでいます。

- DCBX をサポートする第 2 世代 CNA が必要です。
- 別のスイッチへの単一のホスト CNA ポート チャンネル接続。単一スイッチのポート チャンネルで、ポート チャンネルまたは vPC に複数のメンバー ポートが含まれている場合、FCoE インターフェイスは機能しません。
- Cisco NX-OS リリース 9.3(5) 10.2(1)F 以降のリリース。
- FCoE を実行するには、FC 機能パッケージが必要です。これがインストールされていない場合、90 日持続する一時ライセンスがあります。

## Cisco Nexus 9000 シリーズ スイッチの vPC の設定例

この例では、基本設定 (IP アドレス (mgmt0)、スイッチ名、管理者のパスワードなど) がスイッチで完了していると仮定します。



---

(注) 設定は、vPC トポロジの両方のピア スイッチで実行する必要があります。

---

## 手順の概要

1. feature vpc
2. vPC domain
3. vpc peer-link
4. show vpc peer-keepalive
5. int po
6. vpc
7. show vpc statistics

## 手順の詳細

## 手順

|               | コマンドまたはアクション  | 目的  |
|---------------|---|---|
| <b>Step 1</b> | <b>feature vpc</b><br>例:<br><pre>tme-switch-1# conf t Enter configuration commands, one per line. End with CNTL/Z. tme-switch-1(config)# feature vpc tme-switch-1(config)#  tme-switch-2# conf t Enter configuration commands, one per line. End with CNTL/Z. tme-switch-2(config)# feature vpc tme-switch-2(config)#</pre> | 両方のピア スイッチで vPC 機能をイネーブルにしま           す。  |
| <b>Step 2</b> | <b>vPC domain</b><br>例:<br><pre>tme-switch-1(config)# vpc domain 2 tme-switch-1(config-vpc-domain)# peer-keepalive destination 192.165.200.230  tme-switch-2(config)# vpc domain 2 tme-switch-2(config-vpc-domain)# peer-keepalive destination 192.165.200.229</pre>  | vPC ドメインおよびピアのキープアライブの宛先を           設定します。<br>(注)<br>この設定では、スイッチ tme-switch-1 の管理 IP アド           レスは 192.165.200.229、スイッチ tme-switch-2 の管           理 IP アドレスは 192.165.200.230 です。 |
| <b>Step 3</b> | <b>vpc peer-link</b><br>例:<br><pre>tme-switch-1(config)# int port-channel 1 tme-switch-1(config-if)# vpc peer-link</pre> (注)<br>vPC ピアリンクでは、スパニングツリー ポート タ           イプは、ネットワーク ポート タイプに変更されま           す。これにより、STP ブリッジ保証 (デフォルトで  | vPC ピアリンクとして使用するポート チャネルイン           ターフェイスを設定します。  |

|               | コマンドまたはアクション   | 目的   |
|---------------|--|--|
|               | <p>イネーブル) がディセーブルでなければ、vPC ピアリンクの STP ブリッジ保証がイネーブルになります。</p> <pre>tme-switch-2(config)# int port-channel 1 tme-switch-2(config-if)# vpc peer-link</pre>  |  |
| <b>Step 4</b> | <p><b>show vpc peer-keepalive</b></p> <p>例:</p> <pre>tme-switch-1(config)# show vpc peer-keepalive vPC keep-alive status : peer is alive --Destination : 172.25.182.167 --Send status : Success --Receive status : Success --Last update from peer : (0) seconds, (975) msec tme-switch-1(config)#  tme-switch-2(config)# show vpc peer-keepalive --PC keep-alive status : peer is alive --Destination : 172.25.182.166 --Send status : Success --Receive status : Success --Last update from peer : (0) seconds, (10336) msec tme-switch-2(config)#</pre>   | ピアキープアライブに到達できることを確認します。                               |
| <b>Step 5</b> | <p><b>int po</b></p> <p>例:</p> <pre>tme-switch-1(config-if-range)# int po 1 tme-switch-1(config-if)# switchport mode trunk tme-switch-1(config-if)# no shut tme-switch-1(config-if)# exit tme-switch-1(config)# int eth 1/39-40 tme-switch-1(config-if-range)# switchport mode trunk tme-switch-1(config-if-range)# channel-group 1 tme-switch-1(config-if-range)# no shut tme-switch-1(config-if-range)#  tme-switch-2(config-if-range)# int po 1 tme-switch-2(config-if)# switchport mode trunk tme-switch-2(config-if)# no shut tme-switch-2(config-if)# exit tme-switch-2(config)# int eth 1/39-40 tme-switch-2(config-if-range)# switchport mode trunk tme-switch-2(config-if-range)# channel-group 1 tme-switch-2(config-if-range)# no shut tme-switch-2(config-if-range)#  tme-switch-1(config-if-range)# show int po1 port-channel 1 is up Hardware: Port-Channel, address: 000d.ecde.a92f (bia 000d.ecde.a92f) MTU 1500 bytes, BW 20000000 Kbit, DLY 10 usec,</pre> | vPC ピアリンク ポートチャネルにメンバーポートを追加し、このポートチャネルインターフェイスを起動します。 |

|               | コマンドまたはアクション   | 目的  |
|---------------|--|---|
|               | <pre> reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA Port mode is trunk full-duplex, 10 Gb/s Beacon is turned off Input flow-control is off, output flow-control is off Switchport monitor is off Members in this channel: Eth1/39, Eth1/40 Last clearing of "show interface" counters never 1 minute input rate 1848 bits/sec, 0 packets/sec 1 minute output rate 3488 bits/sec, 3 packets/sec tme-switch-1(config-if-range)#  tme-switch-2(config-if-range)# show int po1 port-channell1 is up Hardware: Port-Channel, address: 000d.ecdf.5fae (bia 000d.ecdf.5fae) MTU 1500 bytes, BW 20000000 Kbit, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA Port mode is trunk full-duplex, 10 Gb/s Beacon is turned off Input flow-control is off, output flow-control is off Switchport monitor is off Members in this channel: Eth1/39, Eth1/40 Last clearing of "show interface" counters never minute input rate 1848 bits/sec, 0 packets/sec minute output rate 3488 bits/sec, 3 packets/sec tme-switch-2(config-if-range)# </pre> |   |
| <b>Step 6</b> | <p><b>vpc</b></p> <p><b>例:</b></p> <pre> tme-switch-1(config)# int po 11 tme-switch-1(config-if)# vpc 11 tme-switch-1(config-if)# switchport mode trunk tme-switch-1(config-if)# no shut tme-switch-1(config-if)# int eth 1/1 tme-switch-1(config-if)# switchport mode trunk tme-switch-1(config-if)# channel-group 11 tme-switch-1(config-if)# spanning-tree port type edge trunk tme-switch-1(config-if)# </pre> <p><b>警告</b></p> <p>エッジポートタイプ (PortFast) は、単一のホストに接続されているポートだけでイネーブルにする必要があります。エッジポートタイプ (PortFast) がイネーブルの場合、このインターフェイスにハブ、コンセントレータ、スイッチ、ブリッジなどの一部のデバイスを接続すると、一時的なブリッジングループが発生することがあります。このタイプの設定は、慎重に行う必要があります。</p>  | <p>vPC を作成し、メンバー インターフェイスを追加します。</p> <p>(注)</p> <p>vPC トポロジを介した FCoE を実行するには、ポートチャンネルは単一のメンバー インターフェイスだけを持っている必要があります。</p> <p>(注)</p> <p>ポート チャンネル インターフェイスの下に設定された vPC 番号は、両方の Nexus 9000 スイッチで一致する必要があります。ポートチャンネル インターフェイス番号が両方のスイッチで一致している必要はありません。</p> |

|               | コマンドまたはアクション  | 目的                                  |
|---------------|---|-------------------------------------|
|               | <pre>tme-switch-2(config)# int po 11 tme-switch-2(config-if)# vpc 11 tme-switch-2(config-if)# switchport mode trunk tme-switch-2(config-if)# no shut tme-switch-2(config-if)# int eth 1/1 tme-switch-2(config-if)# switchport mode trunk tme-switch-2(config-if)# channel-group 11 tme-switch-2(config-if)# spanning-tree port type edge trunk</pre> <p><b>警告</b><br/>エッジポートタイプ (PortFast) は、単一のホストに接続されているポートだけでイネーブルにする必要があります。エッジポートタイプ (PortFast) がイネーブルの場合、このインターフェイスにハブ、コンセントレータ、スイッチ、ブリッジなどの一部のデバイスを接続すると、一時的なブリッジングループが発生することがあります。このタイプの設定は、慎重に行う必要があります。</p>  |                                     |
| <b>Step 7</b> | <p><b>show vpc statistics</b></p> <p>例:</p> <pre>tme-switch-1(config-if)# show vpc statistics vpc 11 port-channell1 is up vPC Status: Up, vPC number: 11 Hardware: Port-Channel, address: 000d.ecde.a908 (bia 000d.ecde.a908) MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA Port mode is trunk full-duplex, 10 Gb/s Beacon is turned off Input flow-control is off, output flow-control is off Switchport monitor is off Members in this channel: Eth1/1 Last clearing of "show interface" counters never minute input rate 4968 bits/sec, 8 packets/sec minute output rate 792 bits/sec, 1 packets/sec tme-switch-1(config-if)#</pre> <pre>tme-switch-2(config-if)# show vpc statistics vpc 11 port-channell1 is up vPC Status: Up, vPC number: 11 Hardware: Port-Channel, address: 000d.ecdf.5fae (bia 000d.ecdf.5fae) MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA Port mode is trunk full-duplex, 10 Gb/s Beacon is turned off Input flow-control is off, output flow-control is</pre> | vPC インターフェイスが起動していて、動作していることを確認します。 |

|  | コマンドまたはアクション   | 目的 |
|--|--|----|
|  | <pre> off Switchport monitor is off Members in this channel: Eth1/1 Last clearing of "show interface" counters never minute input rate 4968 bits/sec, 8 packets/sec minute output rate 792 bits/sec, 1 packets/sec tme-switch-1(config-if)# </pre> |    |

## Cisco Nexus 9000 シリーズ スイッチの FCoE の設定例

2つの Nexus 9000 スイッチ間に vPC をセットアップしたら、FCoE トポロジを設定できます。この手順では、IP アドレス (mgmt0)、スイッチ名、パスワード、管理者などを指定する基本設定が Nexus 9000 スイッチ上で実施済みであり、前のセクションに従って vPC 設定が完了していると想定しています。次の手順では、vPC トポロジとともに FCoE トポロジをセットアップするために必要な FCoE の基本設定を行います。

### 手順の概要

1. **install feature-set fcoe**
2. **feature-set fcoe**
3. **vsan database**
4. **interface port-channel**
5. **int vfc**
6. **show int brief**
7. **show flogi database**
8. **show vpc statistics**

### 手順の詳細

#### 手順

|               | コマンドまたはアクション  | 目的  |
|---------------|---|---|
| <b>Step 1</b> | <b>install feature-set fcoe</b>   | FCoE 機能をインストールします。  |
| <b>Step 2</b> | <b>feature-set fcoe</b><br><br>例:<br><br><pre> tme-switch-1(config)# feature-set fcoe Please configure the following for fcoe to be fully functional: - hardware access-list tcam region ing-racl TCAM size - hardware access-list tcam region ing-ifacl TCAM size - hardware access-list tcam region ing-redirect TCAM size tme-switch-1(config)#  tme-switch-2(config)# feature-set fcoe </pre> | Cisco Nexus 9000 スイッチで FCoE を有効にします。<br><br>(注)<br>これが完了するまでに数分かかることがあります。この手順を実行する前に、TCAM カービングを完了する必要があります。TCAM カービングの完了後には、スイッチをリロードする必要があります。 |

|               | コマンドまたはアクション   | 目的   |
|---------------|--|--|
|               | <pre>Please configure the following for fcoe to be fully functional: - hardware access-list tcam region ing-racl TCAM size - hardware access-list tcam region ing-ifacl TCAM size - hardware access-list tcam region ing-redirect TCAM size tme-switch-2 (config) #</pre>  |  |
| <b>Step 3</b> | <p><b>vsan database</b></p> <p>例:</p> <pre>tme-switch-1 (config) # vsan database tme-switch-1 (config-vsan-db) # vsan 100 tme-switch-1 (config-vsan-db) # exit tme-switch-1 (config) # vlan 100 tme-switch-1 (config-vlan) # fcoe vsan 100 tme-switch-1 (config-vlan) # show vlan fcoe VLAN VSAN Status ----- 100 100 Operational tme-switch-1 (config-vlan) #  tme-switch-2 (config) # vsan database tme-switch-2 (config-vsan-db) # vsan 101 tme-switch-2 (config-vsan-db) # exit tme-switch-2 (config) # vlan 101 tme-switch-2 (config-vlan) # fcoe vsan 101 tme-switch-2 (config-vlan) # show vlan fcoe VLAN VSAN Status ----- 101 101 Operational tme-switch-2 (config) #</pre> | <p>VSANを構築して、FCoEトラフィックの伝送用として指定されている VLAN にマッピングします。</p> <p>(注)<br/>VLAN 番号と VSAN 番号が同じである必要はありません。</p> |
| <b>Step 4</b> | <p><b>interface port-channel</b></p> <p>例:</p> <pre>tme-switch-1 (config) # interface port-channel 11 tme-switch-1 (config-if) # switchport trunk allowed vlan 1, 100 tme-switch-1 (config-if) # mtu 9216 tme-switch-1 (config-if) # service-policy type qos input default-fcoe-in-policy tme-switch-1 (config-if) # show int trunk  Port Native Status Port ----- Eth1/1 1 trnk-bndl Pol1 Eth1/39 1 trnk-bndl Pol Eth1/40 1 trnk-bndl Pol Pol 1 trunking -- Pol1 1 trunking --  Port Vlans Allowed on Trunk ----- Eth1/1 1,100 Eth1/39 1-3967,4048-4093 Eth1/40 1-3967,4048-4093</pre>  | <p>vPC リンクの通過を許可される VLAN を設定します。</p>   |

| コマンドまたはアクション  | 目的 |
|---|----|
| <pre>Po1 1-3967,4048-4093 Po11 1,100</pre>  |    |
| <hr/> Port Vlans Err-disabled on Trunk  |    |
| <pre>Eth1/1 none Eth1/39 100 Eth1/40 100 Po1 100 Po11 none</pre>  |    |
| <hr/> Port STP Forwarding   |    |
| <pre>Eth1/1 none Eth1/39 none Eth1/40 none Po1 1 Po11 1,100 tme-switch-1(config-if)#  tme-switch-2(config)# int po 11 tme-switch-2(config-if)# switchport trunk allowed vlan 1, 101 tme-switch-1(config-if)# mtu 9216 tme-switch-1(config-if)# service-policy type qos input default-fcoe-in-policy tme-switch-2(config-if)# show int trunk</pre> |    |
| <hr/> Port Native Status Port   |    |
| <pre>Eth1/1 1 trnk-bndl Po11 Eth1/39 1 trnk-bndl Po1 Eth1/40 1 trnk-bndl Po1 Po1 1 trunking -- Po11 1 trunking --</pre>   |    |
| <hr/> Port Vlans Allowed on Trunk   |    |
| <pre>Eth1/1 1,101 Eth1/39 1-3967,4048-4093 Eth1/40 1-3967,4048-4093 Po1 1-3967,4048-4093 Po11 1,101</pre>   |    |
| <hr/> Port Vlans Err-disabled on Trunk  |    |
| <pre>Eth1/1 none Eth1/39 101 Eth1/40 101 Po1 101 Po11 none</pre>  |    |
| <hr/> Port STP Forwarding   |    |
| <pre>Eth1/1 none Eth1/39 none Eth1/40 none</pre>  |    |

|               | コマンドまたはアクション  | 目的  |
|---------------|---|---|
|               | <pre>Pol 1 Pol1 1,101 tme-switch-2(config-if)#</pre>  |   |
| <b>Step 5</b> | <p><b>int vfc</b></p> <p>例:</p> <pre>tme-switch-1(config)# int vfc 1 tme-switch-1(config-if)# bind interface poll tme-switch-1(config-if)# no shut tme-switch-1(config-if)#  tme-switch-2(config)# int vfc 1 tme-switch-2(config-if)# bind interface poll tme-switch-2(config-if)# no shut tme-switch-2(config-if)#  tme-switch-1(config)# vsan database tme-switch-1(config-vsan-db)# vsan 100 interface vfc 1 tme-switch-1(config)# show vsan membership vsan 1 interfaces: fc2/1 fc2/2 fc2/3 fc2/4 fc2/5 fc2/6 fc2/7 fc2/8  vsan 100 interfaces: vfc1  vsan 4079(evfp_isolated_vsan) interfaces:  vsan 4094(isolated_vsan) interfaces: tme-switch-1(config)#  tme-switch-2(config)# vsan database tme-switch-2(config-vsan-db)# vsan 101 interface vfc 1 tme-switch-2(config)# show vsan membership vsan 1 interfaces: fc2/1 fc2/2 fc2/3 fc2/4 fc2/5 fc2/6 fc2/7 fc2/8  vsan 101 interfaces: vfc1  vsan 4079(evfp_isolated_vsan) interfaces:  vsan 4094(isolated_vsan) interfaces: tme-switch-2(config)#</pre> | <p>仮想ファイバチャネルインターフェイス (vfc) を構築し、前のステップで構築した VSAN に追加します。</p> |
| <b>Step 6</b> | <p><b>show int brief</b></p> <p>例:</p> <pre>tme-switch-1(config-if)# show int brief</pre> <hr/> <pre>Ethernet VLAN Type Mode Status Reason Speed -----</pre> <pre>Eth1/1 1 eth trunk up none 10G(D) Eth1/2 1 eth access up none 10G(D) Eth1/38 1 eth access down SFP not inserted 10G(D)</pre>  | <p>vfc が起動し、動作していることを確認します。</p>                               |

|               | コマンドまたはアクション   | 目的   |
|---------------|--|--|
|               | <pre> Eth1/39 1 eth trunk up none 10G(D) Eth1/40 1 eth trunk up none 10G(D)  -----  Port-channel VLAN Type Mode Status Reason Speed  -----  Po1 1 eth trunk up none a-10G(D) none Po11 1 eth trunk up none a-10G(D) none  -----  Port VRF Status IP Address Speed MTU  -----  mgmt0 -- up 172.25.182.166 1000 1500  -----  Interface Vsan Admin Admin Status SFP Oper Oper Port  -----  vfc1 100 F on up -- F auto -- tme-switch-1(config-if)#  tme-switch-2(config-if)# show int brief  -----  Ethernet VLAN Type Mode Status Reason Speed Port  -----  Eth1/1 1 eth trunk up none 10G(D) 11 Eth1/2 1 eth access up none 10G(D) -- Eth1/38 1 eth access down SFP not inserted 10G(D) -- Eth1/39 1 eth trunk up none 10G(D) 1 Eth1/40 1 eth trunk up none 10G(D) 1  -----  Port-channel VLAN Type Mode Status Reason Speed Protocol  -----  Po1 1 eth trunk up none a-10G(D) none Po11 1 eth trunk up none a-10G(D) none  -----  Port VRF Status IP Address Speed MTU  -----  mgmt0 -- up 172.25.182.167 1000 1500  -----  Interface Vsan Admin Admin Status SFP Oper Oper  -----  vfc1 101 F on up -- F auto -- tme-switch-2(config-if)# </pre> |  |
| <b>Step 7</b> | <pre> <b>show flogi database</b>  例: tme-switch-1# show flogi database  -----  INTERFACE VSAN FCID PORT NAME NODE NAME  -----  vfc1 100 0x540000 21:00:00:c0:dd:11:2a:01 20:00:00:c0:dd:11:2a:01 </pre>  | <p>仮想ファイバチャネルインターフェイスがファブリックにログインしたことを確認します。</p> |

|               | コマンドまたはアクション  | 目的                       |
|---------------|---|--------------------------|
|               | <pre>Total number of flogi = 1. tme-switch-2# show flogi database</pre> <hr/> <pre>INTERFACE VSAN FCID PORT NAME NODE NAME</pre> <hr/> <pre>vfc1 101 0x540000 21:00:00:c0:dd:11:2a:01 20:00:00:c0:dd:11:2a:01</pre> <pre>Total number of flogi = 1.</pre>   |                          |
| <b>Step 8</b> | <p><b>show vpc statistics</b></p> <p>例:</p> <pre>tme-switch-1(config-if)# show vpc statistics vpc 11 port-channel11 is up vPC Status: Up, vPC number: 11 Hardware: Port-Channel, address: 000d.ecde.a908 (bia 000d.ecde.a908) MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA Port mode is trunk full-duplex, 10 Gb/s Beacon is turned off Input flow-control is off, output flow-control is off Switchport monitor is off Members in this channel: Eth1/1 Last clearing of "show interface" counters never 1 minute input rate 4968 bits/sec, 8 packets/sec 1 minute output rate 792 bits/sec, 1 packets/sec</pre> <pre>tme-switch-2(config-if)# show vpc statistics vpc 11 port-channel11 is up vPC Status: Up, vPC number: 11 Hardware: Port-Channel, address: 000d.ecdf.5fae (bia 000d.ecdf.5fae) MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA Port mode is trunk full-duplex, 10 Gb/s Beacon is turned off Input flow-control is off, output flow-control is off Switchport monitor is off Members in this channel: Eth1/1 Last clearing of "show interface" counters never 1 minute input rate 4968 bits/sec, 8 packets/sec 1 minute output rate 792 bits/sec, 1 packets/sec</pre> | vPC が起動し、動作していることを確認します。 |

## QoS の設定

QoS を設定するには、システム サービス ポリシーをアタッチする必要があります。 **service-policy** コマンドは、システムのサービスポリシーとしてシステムクラスポリシーマップを指定します。

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **system qos**
3. switch(config-sys-qos)# **service-policy type {network-qos | qos | queuing} [input | output] fcoe default policy-name**

## 手順の詳細

## 手順

|               | コマンドまたはアクション   | 目的   |
|---------------|--|--|
| <b>Step 1</b> | switch# <b>configure terminal</b>  | 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。   |
| <b>Step 2</b> | switch(config)# <b>system qos</b>  | システム QoS 構成 モードを開始します。   |
| <b>Step 3</b> | switch(config-sys-qos)# <b>service-policy type {network-qos   qos   queuing} [input   output] fcoe default policy-name</b> | <p>デフォルトの FCoE ポリシーマップをシステムのサービスポリシーとして使用するよう指定します。FCoE には次の4つの定義済みポリシーマップがあります。</p> <ul style="list-style-type: none"> <li>• service-policy type queuing input<br/>fcoe-default-in-policy</li> <li>• service-policy type queuing output<br/>fcoe-default-out-policy</li> <li>• service-policy type qos input fcoe-default-in-policy</li> <li>• service-policy type network-qos fcoe-default-nq-policy</li> </ul> <p>(注)<br/>Cisco Nexus デバイスで FCoE をイネーブルにする前に、事前定義された FCoE ポリシーマップをタイプ qos、タイプ network-qos、およびタイプ queuing の各ポリシーマップに追加する必要があります。</p> |

## TCAM カービングに関する情報

3 値連想メモリ (TCAM) カービング機能では、TCAM のデフォルトリージョンサイズの変更を可能にするテンプレートベースの手段を使用します。スイッチが起動すると、他のどんなテンプレートも設定していなければ、このデフォルトテンプレートが表示されます。次の表に、テンプレート内のさまざまなリージョンの種類とサイズを示します。

表 3: 事前定義済み組み込みデフォルトテンプレート

| [リージョン<br>(Region) ] | サイズ (エントリ<br>数) | サイズ (ブロック数) | 特長   |
|----------------------|-----------------|-------------|--|
| Vacl                 | 1024            | 16          | 入力 VLAN アクセス<br>コントロール リスト<br>(VACL)、出力<br>VACL  |
| Ifacl                | 1152            | 18 日        | 入力インターフェイ<br>ス ACL、入力レイヤ<br>3 物理ポート/サブイ<br>ンターフェイス<br>RACL、すべての<br>ポートの出力<br>RACL、デフォルトの<br>コントロール プレー<br>ン ポリシング<br>(CoPP)                            |
| QoS                  | 448             | 7           | 入力 vlan-qos、入力<br>system-qos、入力<br>interface-qos   |
| Rbacl                | 1152            | 18 日        | 入力レイヤ 3 スイッ<br>チ仮想インターフェ<br>イス、入力レイヤ 3<br>ポートチャネル/ポー<br>トチャネルサブイン<br>ターフェイス ルータ<br>アクセス コントロー<br>ル リスト<br>(RACL)、出力<br>Cisco Trusted Security<br>(CTS) |
| スパン                  | 64              | 1           | スパン  |
| Sup                  | 256             | 4           | Sup-rdt  |
| 合計                   | <b>4096</b>     | <b>64</b>   |  |

## ユーザー定義テンプレートに関する情報

デフォルトテンプレートに加えて最大 16 個のテンプレートを作成できます（つまり、同時に 17 個のテンプレートを保持できるということです）。希望の 3 値連想メモリ（TCAM）リージョンにどんなサイズでも設定できます。

各テンプレートで、次の操作を実行できます。

- 作成（Create）
- 変更
- 削除
- Commit

各テンプレートは、次のうちのいずれかのステータスになっています。

- 保存済み
- コミット型

### 作成（Create）

テンプレートを作成する場合、TCAM リージョンのサイズはデフォルト値に初期化されます。テンプレートを作成する場合、テンプレートはデフォルトでは保存済みステータスになっています。テンプレートを作成すると、これを変更してどの TCAM リージョンのサイズも変更できます。各 TCAM ブロックのサイズは 64 エントリのため、リージョンのサイズは 64 の倍数で設定する必要があります。入力した値が 64 の倍数でなかった場合、値を再入力するように求めるエラーメッセージが表示されます。

### 変更

すべての保存済みテンプレートを編集してどの TCAM リージョンのサイズでも変更できますが、どの TCAM のリージョンのサイズも 0 に設定することはできません。編集中、入力したサイズが 64 の境界線にあるかがソフトウェアによってチェックされます。テンプレートを変更する場合、すべての TCAM リージョンのサイズの合計が 4096 エントリより小さくなる必要があります。変更中は、4096 エントリ未満なのはソフトウェアではチェックされません。

テンプレートは、保存済みステータスのときのみ変更できます。テンプレートをコミットした後は編集できません。

コミット済みのユーザー定義テンプレートは、別のユーザー定義テンプレートまたはデフォルトテンプレートを提供することによって作成済みステータスに変更できます。

別のユーザー定義テンプレートを提供するには、次のコマンドを入力します。

**hardware profile tcam resource service-template user-defined-template**

デフォルトテンプレートを提供するには、次のコマンドを入力します。

**no hardware profile tcam resource service-template currently-committed-template**

## 削除

どの保存済みテンプレートも削除できます。テンプレートを削除した後では、そのテンプレートに関するすべての情報が失われます。コミットしたテンプレートは削除できません。

コミット済みのユーザー定義テンプレートは、別のユーザー定義テンプレートまたはデフォルトテンプレートを提供することによって作成済みステートに変更できます。

別のユーザー定義テンプレートを提供するには、次のコマンドを入力します。

**hardware profile tcam resource service-template user-defined-template**

デフォルトテンプレートを提供するには、次のコマンドを入力します。

**no hardware profile tcam resource service-template currently-committed-template**

## Commit

自分のユーザー定義テンプレートまたはソフトウェアで提供されているデフォルトテンプレートはどれでもコミットできます。テンプレートをコミットするには、**commit** コマンドを入力し、スイッチの再起動を行います。**commit** コマンドを入力すると、ソフトウェアによってテンプレートが検証されます。検証が成功すると、スイッチを再起動するか確認するメッセージが表示されます。テンプレート（ユーザー定義またはデフォルト）は、再起動後に適用されます。再起動を選択しなかった場合、TCAM リージョンへの変更は行われず、コミットされるテンプレートはありません。

Cisco NX-OS リリース 9.3(3) 以降では、テンプレートをコミットすると、実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーしてスイッチをリブートするかどうかを確認するプロンプトが表示されます。続行に同意すると、次のことが行われます。

- コミットしたテンプレート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。
- スイッチが再起動します。
- コミットしたテンプレートがソフトウェアによって使用されます。
- テンプレートが実行中ステートに移行します。



- (注) Cisco NX-OS リリース 9.3(3) より前では、テンプレートをコミットした後、システムは自動では再起動せず **commit** コマンドの出力にメッセージが表示され、コミットしたテンプレートを有効にするためにスイッチを再起動するか尋ねられます。

コミットされていないTCAMプロファイルを含むバックアップコンフィギュレーションから、書き込み消去、リロード、および実行コンフィギュレーションのコピーを実行すると、次のことが発生します。

1. TCAM プロファイルがコミットされると、スイッチはプロンプトなしで自動的にリロードします。
2. TCAM カービング CLI の後の設定は適用されません。

3. コミットされた TCAM プロファイルで設定を復元するには、バックアップ コンフィギュレーションを実行コンフィギュレーションに再度コピーする必要があります。ただし、TCAM カービング プロファイルはすでにコミットされているため、スイッチのリロードはありません。

新しいコミットされた TCAM プロファイルが原因でスイッチがリロードされると、**show system reset-reason** コマンドは、次に示すようにリロードの理由を表示します。

```
switch# show system reset-reason
----- reset reason for Supervisor-module 1 (from Supervisor in slot 1) ---
1) At 302777 usecs after Sun Jan 20 22:02:37 2019
   Reason: Reload due to change in TCAM service-template
   Service:
   Version: 9.3(3)

2) At 314447 usecs after Sun Jan 20 21:52:58 2019
   Reason: Reset Requested by CLI command reload
   Service:
   Version: 9.3(3)

3) At 20142 usecs after Sun Jan 20 21:27:33 2019
   Reason: Reset Requested by CLI command reload
   Service:
   Version: 9.3(3)
```

スイッチを再起動後、コミットされたテンプレートが Cisco Nexus サーバー上のすべての ASIC に適用されます。Cisco Nexus デバイス上の別の ASIC に別のテンプレートをコミットできません。各テンプレートの各リージョンのサイズを指定したすべての保存済みテンプレートおよびコミット済みテンプレートは実行コンフィギュレーションに表示されます。

テンプレートがコミットされたとき、以下がチェックされます。

1. TCAM 内のすべてのリージョンの合計サイズは 4096 エントリです。
2. 各リージョンのサイズは TCAM 内に収まります。どの時点でも、TCAM リージョンに対して常に実行サイズがあります。実行サイズ（ハードウェア TCAM 内の現在のサイズ）は、コミットされ実行テンプレートとして現在使用されているデフォルトまたはユーザー定義テンプレートのどちらかによって定義されます。現在コミットされているテンプレート内のリージョンのサイズを現在の実行サイズから増やす場合は、リージョンのサイズを増やすために使用可能な現在のリージョンの外部に未使用のエントリ（他のどのリージョンにも割り当てられていないエントリ）が十分にあるかチェックされます。現在コミットされているテンプレート内のリージョンのサイズを現在の実行サイズから減らす場合は、TCAM リージョンのサイズを減らすために開放できるエントリがリージョン内に十分にあるか判断するためにチェックされます。テンプレート内のリージョンのサイズを減らすすべての変更は、そのテンプレート内のリージョンのサイズを増やす変更の前に完了します。
3. sup-region のすべての機能をサポートするためにソフトウェアで 256 エントリを必要とするため、スーパーバイザ リージョンのサイズは 256 エントリより小さく変更できません。
4. 256 エントリが使用可能でも、スーパーバイザ リージョンのデフォルト サイズは 128 エントリです。TCAM カービングにより、128 エントリをさらに使用できます。sup-region の値を 128、192、または 256 に変更するには、CLI で **sup** キーワードを使用できます。
5. スーパーバイザ リージョンおよびスパン リージョンではハードウェアは 256 エントリより多くはサポートしません。このチェックは検査過程で実施されます。

これらすべてのチェックを通過した場合、そのテンプレートをコミットでき、再起動してテンプレートを適用するかを確認するプロンプトが表示されます。

これらのチェックが失敗した場合、コミットが失敗しテンプレートは保存済み状態に戻ります。コミットが失敗した場合、**commit** コマンドの出力に失敗の原因が表示されます。

デフォルト テンプレートは変更または削除できません。このテンプレートは、保存済みからコミット済み、コミット済みから保存済みへ移行のみが可能です。デフォルト テンプレートがコミットされた場合、実行コンフィギュレーションには表示されません。デフォルト テンプレートを適用するには、現在の実行テンプレートを使用して **no commit** コマンドを入力してください。このコマンドを入力すると、テンプレートをコミットするときに実行されるのと同じ検証チェックが実行されます。すべての検証が成功すると、スイッチを再起動するか確認するメッセージが表示されます。再起動に同意すると、テンプレートがスタートアップコンフィギュレーションに保存されシステムが再起動します。再起動後、デフォルトテンプレートが適用されます。スタートアップコンフィギュレーションには、再起動前にコミットしたコミット済みテンプレートがあります。再起動後に、スタートアップコンフィギュレーションのテンプレートが使用されます。スタートアップコンフィギュレーションにコミット済みテンプレートがない場合、デフォルトテンプレートが使用されます。

テンプレート管理コマンドを入力して、TCAM カービングテンプレートを作成および管理できます。このテンプレート ベース TCAM カービング CLI は **config-sync** でサポートされます。テンプレートの作成のみが **config-sync** 内部でサポートされます。テンプレート コミットは、**config-sync** コンテキストの外部でスイッチごとに別々に実施する必要があります。

## ユーザー定義テンプレートの作成

### 手順の概要

1. **switch# configure terminal**
2. **switch(config)# hardware profile tcam resource template *template-name***

### 手順の詳細

#### 手順

|               | コマンドまたはアクション  | 目的  |
|---------------|---|---|
| <b>Step 1</b> | <b>switch# configure terminal</b>   | 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。  |
| <b>Step 2</b> | <b>switch(config)# hardware profile tcam resource template <i>template-name</i></b> | デフォルトリージョンサイズで新しいテンプレートを作成します。最大16個のテンプレート（加えてデフォルトテンプレート）を作成できます。<br><i>template-name</i> 引数には最大64文字を指定できます。 |

## 例

次に、qos-template という名前のユーザー定義テンプレートを作成する例を示します。

```
switch# configure terminal
switch(config)# hardware profile tcam resource template qos-template
```

## ユーザー定義テンプレートに関する情報

デフォルトテンプレートに加えて最大 16 個のテンプレートを作成できます（つまり、同時に 17 個のテンプレートを保持できるということです）。希望の 3 値連想メモリ（TCAM）リージョンにどんなサイズでも設定できます。

各テンプレートで、次の操作を実行できます。

- 作成（Create）
- 変更
- 削除
- Commit

各テンプレートは、次のうちのいずれかのステータスになっています。

- 保存済み
- コミット型

### 作成（Create）

テンプレートを作成する場合、TCAM リージョンのサイズはデフォルト値に初期化されます。テンプレートを作成する場合、テンプレートはデフォルトでは保存済みステータスになっています。テンプレートを作成すると、これを変更してどの TCAM リージョンのサイズも変更できます。各 TCAM ブロックのサイズは 64 エントリのため、リージョンのサイズは 64 の倍数で設定する必要があります。入力した値が 64 の倍数でなかった場合、値を再入力するように求めるエラーメッセージが表示されます。

### 変更

すべての保存済みテンプレートを編集してどの TCAM リージョンのサイズでも変更できますが、どの TCAM のリージョンのサイズも 0 に設定することはできません。編集中、入力したサイズが 64 の境界線にあるかがソフトウェアによってチェックされます。テンプレートを変更する場合、すべての TCAM リージョンのサイズの合計が 4096 エントリより小さくなる必要があります。変更中は、4096 エントリ未満なのはソフトウェアではチェックされません。

テンプレートは、保存済みステータスのときにのみ変更できます。テンプレートをコミットした後は編集できません。

コミット済みのユーザー定義テンプレートは、別のユーザー定義テンプレートまたはデフォルトテンプレートを提供することによって作成済みステータスに変更できます。

別のユーザー定義テンプレートを提供するには、次のコマンドを入力します。

**hardware profile tcam resource service-template user-defined-template**

デフォルトテンプレートを提供するには、次のコマンドを入力します。

**no hardware profile tcam resource service-template currently-committed- template**

### 削除

どの保存済みテンプレートも削除できます。テンプレートを削除した後では、そのテンプレートに関するすべての情報が失われます。コミットしたテンプレートは削除できません。

コミット済みのユーザー定義テンプレートは、別のユーザー定義テンプレートまたはデフォルトテンプレートを提供することによって作成済みステートに変更できます。

別のユーザー定義テンプレートを提供するには、次のコマンドを入力します。

**hardware profile tcam resource service-template user-defined-template**

デフォルトテンプレートを提供するには、次のコマンドを入力します。

**no hardware profile tcam resource service-template currently-committed- template**

### Commit

自分のユーザー定義テンプレートまたはソフトウェアで提供されているデフォルトテンプレートはどれでもコミットできます。テンプレートをコミットするには、**commit** コマンドを入力し、スイッチの再起動を行います。**commit** コマンドを入力すると、ソフトウェアによってテンプレートが検証されます。検証が成功すると、スイッチを再起動するか確認するメッセージが表示されます。テンプレート（ユーザー定義またはデフォルト）は、再起動後に適用されます。再起動を選択しなかった場合、TCAM リージョンへの変更は行われず、コミットされるテンプレートはありません。

Cisco NX-OS リリース 9.3(3) 以降では、テンプレートをコミットすると、実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーしてスイッチをリブートするかどうかを確認するプロンプトが表示されます。続行に同意すると、次のことが行われます。

- コミットしたテンプレート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。
- スイッチが再起動します。
- コミットしたテンプレートがソフトウェアによって使用されます。
- テンプレートが実行中ステートに移行します。



(注) Cisco NX-OS リリース 9.3(3) より前では、テンプレートをコミットした後、システムは自動では再起動せず **commit** コマンドの出力にメッセージが表示され、コミットしたテンプレートを有効にするためにスイッチを再起動するか尋ねられます。

コミットされていない TCAM プロファイルを含むバックアップコンフィギュレーションから、書き込み消去、リロード、および実行コンフィギュレーションのコピーを実行すると、次のことが発生します。

1. TCAM プロファイルがコミットされると、スイッチはプロンプトなしで自動的にリロードします。
2. TCAM カービング CLI の後の設定は適用されません。
3. コミットされた TCAM プロファイルで設定を復元するには、バックアップコンフィギュレーションを実行コンフィギュレーションに再度コピーする必要があります。ただし、TCAM カービングプロファイルはすでにコミットされているため、スイッチのリロードはありません。

新しいコミットされた TCAM プロファイルが原因でスイッチがリロードされると、**show system reset-reason** コマンドは、次に示すようにリロードの理由を表示します。

```
switch# show system reset-reason
----- reset reason for Supervisor-module 1 (from Supervisor in slot 1) ---
1) At 302777 usecs after Sun Jan 20 22:02:37 2019
   Reason: Reload due to change in TCAM service-template
   Service:
   Version: 9.3(3)

2) At 314447 usecs after Sun Jan 20 21:52:58 2019
   Reason: Reset Requested by CLI command reload
   Service:
   Version: 9.3(3)

3) At 20142 usecs after Sun Jan 20 21:27:33 2019
   Reason: Reset Requested by CLI command reload
   Service:
   Version: 9.3(3)
```

スイッチを再起動後、コミットされたテンプレートが Cisco Nexus サーバー上のすべての ASIC に適用されます。Cisco Nexus デバイス上の別の ASIC に別のテンプレートをコミットできません。各テンプレートの各リージョンのサイズを指定したすべての保存済みテンプレートおよびコミット済みテンプレートは実行コンフィギュレーションに表示されます。

テンプレートがコミットされたとき、以下がチェックされます。

1. TCAM 内のすべてのリージョンの合計サイズは 4096 エントリです。
2. 各リージョンのサイズは TCAM 内に収まります。どの時点でも、TCAM リージョンに対して常に実行サイズがあります。実行サイズ（ハードウェア TCAM 内の現在のサイズ）は、コミットされ実行テンプレートとして現在使用されているデフォルトまたはユーザー定義テンプレートのどちらかによって定義されます。現在コミットされているテンプレート内のリージョンのサイズを現在の実行サイズから増やす場合は、リージョンのサイズを増やすために使用可能な現在のリージョンの外部に未使用のエントリ（他のどのリージョンにも割り当てられていないエントリ）が十分にあるかチェックされます。現在コミットされているテンプレート内のリージョンのサイズを現在の実行サイズから減らす場合は、TCAM リージョンのサイズを減らすために開放できるエントリがリージョン内に十分にあるか判断するためにチェックされます。テンプレート内のリージョンのサイズを減らすすべての変更は、そのテンプレート内のリージョンのサイズを増やす変更の前に完了します。

3. `sup-region` のすべての機能をサポートするためにソフトウェアで 256 エントリを必要とするため、スーパーバイザ リージョンのサイズは 256 エントリより小さく変更できません。
4. 256 エントリが使用可能でも、スーパーバイザ リージョンのデフォルト サイズは 128 エントリです。TCAM カービングにより、128 エントリをさらに使用できます。`sup-region` の値を 128、192、または 256 に変更するには、CLI で `sup` キーワードを使用できます。
5. スーパーバイザ リージョンおよびスパン リージョンではハードウェアは 256 エントリより多くはサポートしません。このチェックは検査過程で実施されます。

これらすべてのチェックを通過した場合、そのテンプレートをコミットでき、再起動してテンプレートを適用するかを確認するプロンプトが表示されます。

これらのチェックが失敗した場合、コミットが失敗しテンプレートは保存済み状態に戻りません。コミットが失敗した場合、`commit` コマンドの出力に失敗の原因が表示されます。

デフォルト テンプレートは変更または削除できません。このテンプレートは、保存済みからコミット済み、コミット済みから保存済みへ移行のみが可能です。デフォルト テンプレートがコミットされた場合、実行コンフィギュレーションには表示されません。デフォルトテンプレートを適用するには、現在の実行テンプレートを使用して `no commit` コマンドを入力してください。このコマンドを入力すると、テンプレートをコミットするときに実行されるのと同じ検証チェックが実行されます。すべての検証が成功すると、スイッチを再起動するか確認するメッセージが表示されます。再起動に同意すると、テンプレートがスタートアップコンフィギュレーションに保存されシステムが再起動します。再起動後、デフォルトテンプレートが適用されます。スタートアップコンフィギュレーションには、再起動前にコミットしたコミット済みテンプレートがあります。再起動後に、スタートアップコンフィギュレーションのテンプレートが使用されます。スタートアップコンフィギュレーションにコミット済みテンプレートがない場合、デフォルトテンプレートが使用されます。

テンプレート管理コマンドを入力して、TCAM カービングテンプレートを作成および管理できます。このテンプレート ベース TCAM カービング CLI は `config-sync` でサポートされます。テンプレートの作成のみが `config-sync` 内部でサポートされます。テンプレート コミットは、`config-sync` コンテキストの外部でスイッチごとに別々に実施する必要があります。

## ユーザー定義テンプレートの変更

### 手順の概要

1. `switch# configure terminal`
2. `switch(config)# hardware profile tcam resource template template-name`
3. `switch(config-tmpl)# {vacl vacl-region | ifacl ifacl-region | qos qos-region | rbacl rbacl-region | span span-region}`
4. `switch(config-tmpl)# {vacl vacl-region | ifacl ifacl-region | qos qos-region | rbacl rbacl-region | span span-region iracl iracl-region eracl eracl-region sup sup-region iracl iracl-region eracl eracl-region sup sup-region }`

## 手順の詳細

## 手順

|               | コマンドまたはアクション   | 目的  |
|---------------|--|---|
| <b>Step 1</b> | switch# <b>configure terminal</b>  | 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。  |
| <b>Step 2</b> | switch(config)# <b>hardware profile tcam resource template template-name</b>   | デフォルトリージョンサイズで新しいテンプレートを作成します。最大 16 個のテンプレート（加えてデフォルトテンプレート）を作成できます。このコマンドは、テンプレートモードを開始するために使用します。   |
| <b>Step 3</b> | switch(config-templ)# { <b>vacl vacl-region</b>   <b>ifacl ifacl-region</b>   <b>qos qos-region</b>   <b>rbacl rbacl-region</b>   <b>span span-region</b> }  | リージョンブロックサイズを設定します。 <ul style="list-style-type: none"> <li>• <b>vacl-region:</b> このリージョンのブロックサイズは 64 ~ 3584 です。</li> <li>• <b>ifacl-region:</b> このリージョンのブロックサイズは 320 ~ 3584 です。</li> <li>• <b>qos-region:</b> このリージョンのブロックサイズは 64 ~ 3584 です。</li> <li>• <b>rbacl-region:</b> このリージョンのブロックサイズは 64 ~ 3584 です。</li> <li>• <b>span-region:</b> このリージョンのブロックサイズは 64 ~ 256 です。</li> </ul> <p>(注)<br/>リージョンのサイズをゼロには設定できません。ブロックサイズは 64 の倍数にする必要があります。</p> |
| <b>Step 4</b> | switch(config-templ)# { <b>vacl vacl-region</b>   <b>ifacl ifacl-region</b>   <b>qos qos-region</b>   <b>rbacl rbacl-region</b>   <b>span span-region</b>   <b>iracl iracl-region eracl eracl-region sup sup-region iracl iracl-region eracl eracl-region sup sup-region</b> } | リージョンブロックサイズを設定します。 <ul style="list-style-type: none"> <li>• <b>vacl-region:</b> このリージョンのブロックサイズは 64 ~ 3584 です。</li> <li>• <b>ifacl-region:</b> このリージョンのブロックサイズは 320 ~ 3584 です。</li> <li>• <b>qos-region:</b> このリージョンのブロックサイズは 64 ~ 3584 です。</li> <li>• <b>rbacl-region:</b> このリージョンのブロックサイズは 64 ~ 3584 です。</li> </ul>  |

|  | コマンドまたはアクション | 目的   |
|--|--------------|--|
|  |              | <ul style="list-style-type: none"> <li>• <i>span-region</i>: このリージョンのブロックサイズは 64 ~ 256 です。</li> <li>• <i>iracl-region</i>: このリージョンのブロックサイズは 64 ~ 3648 です。</li> <li>• <i>eracl-region</i>: このリージョンのブロックサイズは 64 ~ 3648 です。</li> <li>• <i>sup-region</i>: このリージョンのブロックサイズは 64 ~ 256 です。</li> </ul> <p>(注)<br/>リージョンのサイズをゼロには設定できません。ブロックサイズは 64 の倍数にする必要があります。<br/><i>iracl</i> と <i>eracl</i> のブロックサイズを合計すると 3712 になります。</p> |

## 例

次に、ユーザー定義 QoS テンプレートを変更する例を示します。

```
switch# configure terminal
switch(config)# hardware profile tcam resource template qos-template
switch(config-tmpl) qos 64
```

## ユーザー定義テンプレートに関する情報

デフォルトテンプレートに加えて最大 16 個のテンプレートを作成できます（つまり、同時に 17 個のテンプレートを保持できるということです）。希望の 3 値連想メモリ (TCAM) リージョンにどんなサイズでも設定できます。

各テンプレートで、次の操作を実行できます。

- 作成 (Create)
- 変更
- 削除
- Commit

各テンプレートは、次のうちのいずれかのステータスになっています。

- 保存済み
- コミット型

## 作成 (Create)

テンプレートを作成する場合、TCAM リージョンのサイズはデフォルト値に初期化されます。テンプレートを作成する場合、テンプレートはデフォルトでは保存済みステートになっています。テンプレートを作成すると、これを変更してどの TCAM リージョンのサイズも変更できます。各 TCAM ブロックのサイズは 64 エントリのため、リージョンのサイズは 64 の倍数で設定する必要があります。入力した値が 64 の倍数でなかった場合、値を再入力するように求めるエラーメッセージが表示されます。

## 変更

すべての保存済みテンプレートを編集してどの TCAM リージョンのサイズでも変更できますが、どの TCAM のリージョンのサイズも 0 に設定することはできません。編集時、入力したサイズが 64 の境界線にあるかがソフトウェアによってチェックされます。テンプレートを変更する場合、すべての TCAM リージョンのサイズの合計が 4096 エントリより小さくなる必要があります。変更中は、4096 エントリ未満なのはソフトウェアではチェックされません。

テンプレートは、保存済みステートのときにのみ変更できます。テンプレートをコミットした後は編集できません。

コミット済みのユーザー定義テンプレートは、別のユーザー定義テンプレートまたはデフォルトテンプレートを提供することによって作成済みステートに変更できます。

別のユーザー定義テンプレートを提供するには、次のコマンドを入力します。

**hardware profile tcam resource service-template user-defined-template**

デフォルトテンプレートを提供するには、次のコマンドを入力します。

**no hardware profile tcam resource service-template currently-committed- template**

## 削除

どの保存済みテンプレートも削除できます。テンプレートを削除した後では、そのテンプレートに関するすべての情報が失われます。コミットしたテンプレートは削除できません。

コミット済みのユーザー定義テンプレートは、別のユーザー定義テンプレートまたはデフォルトテンプレートを提供することによって作成済みステートに変更できます。

別のユーザー定義テンプレートを提供するには、次のコマンドを入力します。

**hardware profile tcam resource service-template user-defined-template**

デフォルトテンプレートを提供するには、次のコマンドを入力します。

**no hardware profile tcam resource service-template currently-committed- template**

## Commit

自分のユーザー定義テンプレートまたはソフトウェアで提供されているデフォルトテンプレートはどれでもコミットできます。テンプレートをコミットするには、**commit** コマンドを入力し、スイッチの再起動を行います。**commit** コマンドを入力すると、ソフトウェアによってテンプレートが検証されます。検証が成功すると、スイッチを再起動するか確認するメッセージが表示されます。テンプレート（ユーザー定義またはデフォルト）は、再起動後に適用されます。再起動を選択し

なかった場合、TCAM リージョンへの変更は行われず、コミットされるテンプレートはありません。

Cisco NX-OS リリース 9.3(3) 以降では、テンプレートをコミットすると、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーしてスイッチをリブートするかどうかを確認するプロンプトが表示されます。続行に同意すると、次のことが行われます。

- コミットしたテンプレートがスタートアップ コンフィギュレーションに保存されます。
- スイッチが再起動します。
- コミットしたテンプレートがソフトウェアによって使用されます。
- テンプレートが実行中ステートに移行します。



- (注) Cisco NX-OS リリース 9.3(3) より前では、テンプレートをコミットした後、システムは自動では再起動せず **commit** コマンドの出力にメッセージが表示され、コミットしたテンプレートを有効にするためにスイッチを再起動するか尋ねられます。

コミットされていない TCAM プロファイルを含むバックアップ コンフィギュレーションから、書き込み消去、リロード、および実行コンフィギュレーションのコピーを実行すると、次のことが発生します。

1. TCAM プロファイルがコミットされると、スイッチはプロンプトなしで自動的にリロードします。
2. TCAM カービング CLI の後の設定は適用されません。
3. コミットされた TCAM プロファイルで設定を復元するには、バックアップ コンフィギュレーションを実行コンフィギュレーションに再度コピーする必要があります。ただし、TCAM カービング プロファイルはすでにコミットされているため、スイッチのリロードはありません。

新しいコミットされた TCAM プロファイルが原因でスイッチがリロードされると、**show system reset-reason** コマンドは、次に示すようにリロードの理由を表示します。

```
switch# show system reset-reason
----- reset reason for Supervisor-module 1 (from Supervisor in slot 1) -----
1) At 302777 usecs after Sun Jan 20 22:02:37 2019
   Reason: Reload due to change in TCAM service-template
   Service:
   Version: 9.3(3)

2) At 314447 usecs after Sun Jan 20 21:52:58 2019
   Reason: Reset Requested by CLI command reload
   Service:
   Version: 9.3(3)

3) At 20142 usecs after Sun Jan 20 21:27:33 2019
   Reason: Reset Requested by CLI command reload
   Service:
   Version: 9.3(3)
```

スイッチを再起動後、コミットされたテンプレートが Cisco Nexus サーバー上のすべての ASIC に適用されます。Cisco Nexus デバイス上の別の ASIC に別のテンプレートをコミットできません。各テンプレートの各リージョンのサイズを指定したすべての保存済みテンプレートおよびコミット済みテンプレートは実行コンフィギュレーションに表示されます。

テンプレートがコミットされたとき、以下がチェックされます。

1. TCAM 内のすべてのリージョンの合計サイズは 4096 エントリです。
2. 各リージョンのサイズは TCAM 内に収まります。どの時点でも、TCAM リージョンに対して常に実行サイズがあります。実行サイズ（ハードウェア TCAM 内の現在のサイズ）は、コミットされ実行テンプレートとして現在使用されているデフォルトまたはユーザー定義テンプレートのどちらかによって定義されます。現在コミットされているテンプレート内のリージョンのサイズを現在の実行サイズから増やす場合は、リージョンのサイズを増やすために使用可能な現在のリージョンの外部に未使用のエントリ（他のどのリージョンにも割り当てられていないエントリ）が十分にあるかチェックされます。現在コミットされているテンプレート内のリージョンのサイズを現在の実行サイズから減らす場合は、TCAM リージョンのサイズを減らすために開放できるエントリがリージョン内に十分にあるか判断するためにチェックされます。テンプレート内のリージョンのサイズを減らすすべての変更は、そのテンプレート内のリージョンのサイズを増やす変更の前に完了します。
3. sup-region のすべての機能をサポートするためにソフトウェアで 256 エントリを必要とするため、スーパーバイザ リージョンのサイズは 256 エントリより小さく変更できません。
4. 256 エントリが使用可能でも、スーパーバイザ リージョンのデフォルト サイズは 128 エントリです。TCAM カービングにより、128 エントリをさらに使用できます。sup-region の値を 128、192、または 256 に変更するには、CLI で **sup** キーワードを使用できます。
5. スーパーバイザ リージョンおよびスパン リージョンではハードウェアは 256 エントリより多くはサポートしません。このチェックは検査過程で実施されます。

これらすべてのチェックを通過した場合、そのテンプレートをコミットでき、再起動してテンプレートを適用するかを確認するプロンプトが表示されます。

これらのチェックが失敗した場合、コミットが失敗しテンプレートは保存済みステートに戻ります。コミットが失敗した場合、**commit** コマンドの出力に失敗の原因が表示されます。

デフォルトテンプレートは変更または削除できません。このテンプレートは、保存済みからコミット済み、コミット済みから保存済みへ移行のみが可能です。デフォルトテンプレートがコミットされた場合、実行コンフィギュレーションには表示されません。デフォルトテンプレートを適用するには、現在の実行テンプレートを使用して **no commit** コマンドを入力してください。このコマンドを入力すると、テンプレートをコミットするときに実行されるのと同じ検証チェックが実行されます。すべての検証が成功すると、スイッチを再起動するか確認するメッセージが表示されます。再起動に同意すると、テンプレートがスタートアップコンフィギュレーションに保存されシステムが再起動します。再起動後、デフォルトテンプレートが適用されます。スタートアップコンフィギュレーションには、再起動前にコミットしたコミット済みテンプレートがあります。再起動後に、スタートアップコンフィギュレーションのテンプレートが使用されます。スタートアップコンフィギュレーションにコミット済みテンプレートがない場合、デフォルトテンプレートが使用されます。

テンプレート管理コマンドを入力して、TCAM カービングテンプレートを作成および管理できます。このテンプレートベース TCAM カービング CLI は config-sync でサポートされます。テンプレートの作成のみが config-sync 内部でサポートされます。テンプレート コミットは、config-sync コンテキストの外部でスイッチごとに別々に実施する必要があります。

## ユーザー定義テンプレートのコミット

ユーザー定義テンプレートをコミットできます。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **hardware profile tcam resource service-template *template-name***
3. (任意) switch# **show hardware profile tcam resource template**

### 手順の詳細

#### 手順

|               | コマンドまたはアクション  | 目的  |
|---------------|---|---|
| <b>Step 1</b> | 必須: switch# <b>configure terminal</b>   | 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。  |
| <b>Step 2</b> | switch(config)# <b>hardware profile tcam resource service-template <i>template-name</i></b> | 事前定義済みのテンプレートを実行イメージでコミットします。テンプレートをコミットすると、実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーしてスイッチをリブートするかどうかを確認するプロンプトが表示されます。続行に同意すると、指定したテンプレートが再起動後に適用されます。それ以外の場合、TCAM リージョンは変更されず、テンプレートもコミットされません。 |
| <b>Step 3</b> | (任意) switch# <b>show hardware profile tcam resource template</b>                            | すべてのテンプレートを表示します。<br><br>(注)<br>スイッチのリロード後、このコマンドを使用して、コミットされたテンプレートを表示します。   |

#### 例

次の例では、ユーザー定義テンプレートをコミットする方法を示します。

```
switch# configure terminal
switch(config)# hardware profile tcam resource service-template templ

Details of the templ template you are trying to commit are as follows:
```

```
-----
Template name: temp1
Current state: Created

Region  Features  Size-allocated  Current-size  Current-usage  Available/free
-----
Vacl   Vacl         1024            1024          15              1009
Ifacl  Ifacl        1152            1152          209             943
Rbacl  Rbacl        1152            1152          3               1149
Qos    Qos          448             448           30              418
Span   Span         64              64            2               62
Sup    Sup          256             256           58              198
-----
```

To finish committing the template, the system will do the following:

- 1> Save running config : "copy running-config startup-config"
- 2> Reboot the switch : "reload"

```
-----
Do you really want to continue with RELOAD ? (y/n) [no] yes
```

```
System is still initializing
Configuration mode is blocked until system is ready
switch(config)# [16152.925385] Shutdown Ports..
[16152.959744] writing reset reason 9
[snip]
```

/AFTER SWITCH RELOADS/

```
switch# show hardware profile tcam resource template
-----
Template  Type      State   Vacl  Ifacl  Rbacl  Qos   Span  Sup    TOTAL
-----
default  system   Created 1024  1152  1152   448   64    256   4096
temp1    user     Committed 1024  1152  1152   448   64    256   4096
temp2    user     Created  1024  1152  1152   448   64    256   4096
-----
```

次に、レイヤ 3 カード側 UPC に対して、ユーザー定義のテンプレートをコミットし、適用する例を示します。

```
switch# configure terminal
switch(config)# hardware profile tcam resource service-template temp1
```

Details of the temp1 template you are trying to commit are as follows:

```
-----
Template name: temp1
Current state: Created

Region  Features  Size-allocated  Current-size  Current-usage  Available/free
-----
Vacl   Vacl         1984            2048          11              2037
Ifacl  Ifacl        1216            1152          26              1126
Rbacl  Rbacl        128             128           3               125
Qos    Qos          448             448           9               439
Span   Span         64              64            3               61
Sup    Sup          256             128           81              47
ERacl  ERacl        1920            0              0               0
IRacl  IRacl        1792            0              0               0
-----
```

```
To finish committing the template, the system will do the following:
 1> Save running config : "copy running-config startup-config"
 2> Reboot the switch   : "reload"
```

```
-----
Do you really want to continue with RELOAD ? (y/n) [no] yes
System is still initializing
Configuration mode is blocked until system is ready
5548(config)# [166850.680711] Shutdown Ports..
[166850.716114] writing reset reason 9,
[snip]
```

```
/AFTER SWITCH RELOADS/
```

```
switch# show hardware profile tcam resource template
-----
Template   Type      State      ERacl  Ifacl  IRacl  Qos  Span  Sup    TOTAL
-----
default   system   Created    2048   64    1664   64   64    64    4096
temp1     user     Committed  1920   64    1792   64   64    64    4096
temp2     user     Created    2048   64    1664   64   64    64    4096
-----
```

## ユーザー定義テンプレートに関する情報

デフォルトテンプレートに加えて最大 16 個のテンプレートを作成できます（つまり、同時に 17 個のテンプレートを保持できるということです）。希望の 3 値連想メモリ（TCAM）リージョンにどんなサイズでも設定できます。

各テンプレートで、次の操作を実行できます。

- 作成（Create）
- 変更
- 削除
- Commit

各テンプレートは、次のうちのいずれかのステータスになっています。

- 保存済み
- コミット型

### 作成（Create）

テンプレートを作成する場合、TCAM リージョンのサイズはデフォルト値に初期化されます。テンプレートを作成する場合、テンプレートはデフォルトでは保存済みステータスになっています。テンプレートを作成すると、これを変更してどの TCAM リージョンのサイズも変更できます。各 TCAM ブロックのサイズは 64 エントリのため、リージョンのサイズは 64 の倍数で設定する必要があります。入力した値が 64 の倍数でなかった場合、値を再入力するように求めるエラーメッセージが表示されます。

## 変更

すべての保存済みテンプレートを編集してどの TCAM リージョンのサイズでも変更できますが、どの TCAM のリージョンのサイズも 0 に設定することはできません。編集中、入力したサイズが 64 の境界線にあるかがソフトウェアによってチェックされます。テンプレートを変更する場合、すべての TCAM リージョンのサイズの合計が 4096 エントリより小さくなる必要があります。変更中は、4096 エントリ未満なのはソフトウェアではチェックされません。

テンプレートは、保存済みステータスのときのみ変更できます。テンプレートをコミットした後は編集できません。

コミット済みのユーザー定義テンプレートは、別のユーザー定義テンプレートまたはデフォルトテンプレートを提供することによって作成済みステータスに変更できます。

別のユーザー定義テンプレートを提供するには、次のコマンドを入力します。

**hardware profile tcam resource service-template user-defined-template**

デフォルトテンプレートを提供するには、次のコマンドを入力します。

**no hardware profile tcam resource service-template currently-committed- template**

## 削除

どの保存済みテンプレートも削除できます。テンプレートを削除した後では、そのテンプレートに関するすべての情報が失われます。コミットしたテンプレートは削除できません。

コミット済みのユーザー定義テンプレートは、別のユーザー定義テンプレートまたはデフォルトテンプレートを提供することによって作成済みステータスに変更できます。

別のユーザー定義テンプレートを提供するには、次のコマンドを入力します。

**hardware profile tcam resource service-template user-defined-template**

デフォルトテンプレートを提供するには、次のコマンドを入力します。

**no hardware profile tcam resource service-template currently-committed- template**

## Commit

自分のユーザー定義テンプレートまたはソフトウェアで提供されているデフォルトテンプレートはどれでもコミットできます。テンプレートをコミットするには、**commit** コマンドを入力し、スイッチの再起動を行います。**commit** コマンドを入力すると、ソフトウェアによってテンプレートが検証されます。検証が成功すると、スイッチを再起動するか確認するメッセージが表示されます。テンプレート（ユーザー定義またはデフォルト）は、再起動後に適用されます。再起動を選択しなかった場合、TCAM リージョンへの変更は行われず、コミットされるテンプレートはありません。

Cisco NX-OS リリース 9.3(3) 以降では、テンプレートをコミットすると、実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーしてスイッチをリブートするかどうかを確認するプロンプトが表示されます。続行に同意すると、次のことが行われます。

- コミットしたテンプレート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。
- スイッチが再起動します。

- コミットしたテンプレートがソフトウェアによって使用されます。
- テンプレートが実行中ステートに移行します。



- (注) Cisco NX-OS リリース 9.3(3) より前では、テンプレートをコミットした後、システムは自動では再起動せず **commit** コマンドの出力にメッセージが表示され、コミットしたテンプレートを有効にするためにスイッチを再起動するか尋ねられます。

コミットされていない TCAM プロファイルを含むバックアップ コンフィギュレーションから、書き込み消去、リロード、および実行コンフィギュレーションのコピーを実行すると、次のことが発生します。

1. TCAM プロファイルがコミットされると、スイッチはプロンプトなしで自動的にリロードします。
2. TCAM カービング CLI の後の設定は適用されません。
3. コミットされた TCAM プロファイルで設定を復元するには、バックアップ コンフィギュレーションを実行コンフィギュレーションに再度コピーする必要があります。ただし、TCAM カービング プロファイルはすでにコミットされているため、スイッチのリロードはありません。

新しいコミットされた TCAM プロファイルが原因でスイッチがリロードされると、**show system reset-reason** コマンドは、次に示すようにリロードの理由を表示します。

```
switch# show system reset-reason
----- reset reason for Supervisor-module 1 (from Supervisor in slot 1) -----
1) At 302777 usecs after Sun Jan 20 22:02:37 2019
   Reason: Reload due to change in TCAM service-template
   Service:
   Version: 9.3(3)

2) At 314447 usecs after Sun Jan 20 21:52:58 2019
   Reason: Reset Requested by CLI command reload
   Service:
   Version: 9.3(3)

3) At 20142 usecs after Sun Jan 20 21:27:33 2019
   Reason: Reset Requested by CLI command reload
   Service:
   Version: 9.3(3)
```

スイッチを再起動後、コミットされたテンプレートが Cisco Nexus サーバー上のすべての ASIC に適用されます。Cisco Nexus デバイス上の別の ASIC に別のテンプレートをコミットできません。各テンプレートの各リージョンのサイズを指定したすべての保存済みテンプレートおよびコミット済みテンプレートは実行コンフィギュレーションに表示されます。

テンプレートがコミットされたとき、以下がチェックされます。

1. TCAM 内のすべてのリージョンの合計サイズは 4096 エントリです。
2. 各リージョンのサイズは TCAM 内に収まります。どの時点でも、TCAM リージョンに対して常に実行サイズがあります。実行サイズ（ハードウェア TCAM 内の現在のサイズ）は、コミットされ実行テンプレートとして現在使用されているデフォルトまたはユーザー定義テンプレート

のどちらかによって定義されます。現在コミットされているテンプレート内のリージョンのサイズを現在の実行サイズから増やす場合は、リージョンのサイズを増やすために使用可能な現在のリージョンの外部に未使用のエントリ（他のどのリージョンにも割り当てられていないエントリ）が十分にあるかチェックされます。現在コミットされているテンプレート内のリージョンのサイズを現在の実行サイズから減らす場合は、TCAM リージョンのサイズを減らすために開放できるエントリがリージョン内に十分にあるか判断するためにチェックされます。テンプレート内のリージョンのサイズを減らすすべての変更は、そのテンプレート内のリージョンのサイズを増やす変更の前に完了します。

3. `sup-region` のすべての機能をサポートするためにソフトウェアで 256 エントリを必要とするため、スーパーバイザ リージョンのサイズは 256 エントリより小さく変更できません。
4. 256 エントリが使用可能でも、スーパーバイザ リージョンのデフォルト サイズは 128 エントリです。TCAM カービングにより、128 エントリをさらに使用できます。`sup-region` の値を 128、192、または 256 に変更するには、CLI で `sup` キーワードを使用できます。
5. スーパーバイザ リージョンおよびスパン リージョンではハードウェアは 256 エントリより多くはサポートしません。このチェックは検査過程で実施されます。

これらすべてのチェックを通過した場合、そのテンプレートをコミットでき、再起動してテンプレートを適用するかを確認するプロンプトが表示されます。

これらのチェックが失敗した場合、コミットが失敗しテンプレートは保存済み状態に戻ります。コミットが失敗した場合、`commit` コマンドの出力に失敗の原因が表示されます。

デフォルトテンプレートは変更または削除できません。このテンプレートは、保存済みからコミット済み、コミット済みから保存済みへ移行のみが可能です。デフォルトテンプレートがコミットされた場合、実行コンフィギュレーションには表示されません。デフォルトテンプレートを適用するには、現在の実行テンプレートを使用して `no commit` コマンドを入力してください。このコマンドを入力すると、テンプレートをコミットするときに実行されるのと同じ検証チェックが実行されます。すべての検証が成功すると、スイッチを再起動するか確認するメッセージが表示されます。再起動に同意すると、テンプレートがスタートアップコンフィギュレーションに保存されシステムが再起動します。再起動後、デフォルトテンプレートが適用されます。スタートアップコンフィギュレーションには、再起動前にコミットしたコミット済みテンプレートがあります。再起動後に、スタートアップコンフィギュレーションのテンプレートが使用されます。スタートアップコンフィギュレーションにコミット済みテンプレートがない場合、デフォルトテンプレートが使用されます。

テンプレート管理コマンドを入力して、TCAM カービングテンプレートを作成および管理できます。このテンプレートベース TCAM カービング CLI は `config-sync` でサポートされます。テンプレートの作成のみが `config-sync` 内部でサポートされます。テンプレート コミットは、`config-sync` コンテキストの外部でスイッチごとに別々に実施する必要があります。

## テンプレートの削除

テンプレートを作成後、そのテンプレートを削除できます。削除は、そのテンプレートに関するすべての情報をソフトウェアから取り除きます。

## 手順の概要

1. `switch# configure terminal`
2. `switch(config)# no hardware profile tcam resource template template-name`

## 手順の詳細

## 手順

|               | コマンドまたはアクション   | 目的   |
|---------------|--|--|
| <b>Step 1</b> | <code>switch# configure terminal</code>  | 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。   |
| <b>Step 2</b> | <code>switch(config)# no hardware profile tcam resource template <i>template-name</i></code> | ユーザー定義テンプレートを削除します。<br><br>保存済みのテンプレートだけが削除できます。コミット済み/実行中のテンプレートは削除できません。実行コンフィギュレーションに記述されているテンプレートは（スタートアップコンフィギュレーションも同様）削除できません。他のどんなユーザー定義テンプレートも保存済みのステータスにあれば削除できます。デフォルトテンプレートは削除できません。 |

## 例

次に、テンプレートを削除する例を示します

```
switch# configure terminal
switch(config)# no hardware profile tcam resource template qos-template
```

## ユーザー定義テンプレートに関する情報

デフォルトテンプレートに加えて最大 16 個のテンプレートを作成できます（つまり、同時に 17 個のテンプレートを保持できるということです）。希望の 3 値連想メモリ（TCAM）リージョンにどんなサイズでも設定できます。

各テンプレートで、次の操作を実行できます。

- 作成（Create）
- 変更
- 削除
- Commit

各テンプレートは、次のうちのいずれかのステータスになっています。

- 保存済み

- コミット型

### 作成 (Create)

テンプレートを作成する場合、TCAM リージョンのサイズはデフォルト値に初期化されます。テンプレートを作成する場合、テンプレートはデフォルトでは保存済みステートになっています。テンプレートを作成すると、これを変更してどの TCAM リージョンのサイズも変更できます。各 TCAM ブロックのサイズは 64 エントリのため、リージョンのサイズは 64 の倍数で設定する必要があります。入力した値が 64 の倍数でなかった場合、値を再入力するように求めるエラーメッセージが表示されます。

### 変更

すべての保存済みテンプレートを編集してどの TCAM リージョンのサイズでも変更できますが、どの TCAM のリージョンのサイズも 0 に設定することはできません。編集時、入力したサイズが 64 の境界線にあるかがソフトウェアによってチェックされます。テンプレートを変更する場合、すべての TCAM リージョンのサイズの合計が 4096 エントリより小さくなる必要があります。変更中は、4096 エントリ未満なのはソフトウェアではチェックされません。

テンプレートは、保存済みステートのときにのみ変更できます。テンプレートをコミットした後は編集できません。

コミット済みのユーザー定義テンプレートは、別のユーザー定義テンプレートまたはデフォルトテンプレートを提供することによって作成済みステートに変更できます。

別のユーザー定義テンプレートを提供するには、次のコマンドを入力します。

**hardware profile tcam resource service-template user-defined-template**

デフォルトテンプレートを提供するには、次のコマンドを入力します。

**no hardware profile tcam resource service-template currently-committed- template**

### 削除

どの保存済みテンプレートも削除できます。テンプレートを削除した後では、そのテンプレートに関するすべての情報が失われます。コミットしたテンプレートは削除できません。

コミット済みのユーザー定義テンプレートは、別のユーザー定義テンプレートまたはデフォルトテンプレートを提供することによって作成済みステートに変更できます。

別のユーザー定義テンプレートを提供するには、次のコマンドを入力します。

**hardware profile tcam resource service-template user-defined-template**

デフォルトテンプレートを提供するには、次のコマンドを入力します。

**no hardware profile tcam resource service-template currently-committed- template**

### Commit

自分のユーザー定義テンプレートまたはソフトウェアで提供されているデフォルトテンプレートはどれでもコミットできます。テンプレートをコミットするには、**commit** コマンドを入力し、ス

スイッチの再起動を行います。**commit** コマンドを入力すると、ソフトウェアによってテンプレートが検証されます。検証が成功すると、スイッチを再起動するか確認するメッセージが表示されます。テンプレート（ユーザー定義またはデフォルト）は、再起動後に適用されます。再起動を選択しなかった場合、TCAM リージョンへの変更は行われず、コミットされるテンプレートはありません。

Cisco NX-OS リリース 9.3(3) 以降では、テンプレートをコミットすると、実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーしてスイッチをリブートするかどうかを確認するプロンプトが表示されます。続行に同意すると、次のことが行われます。

- コミットしたテンプレート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。
- スイッチが再起動します。
- コミットしたテンプレートがソフトウェアによって使用されます。
- テンプレートが実行中ステートに移行します。



(注) Cisco NX-OS リリース 9.3(3) より前では、テンプレートをコミットした後、システムは自動では再起動せず **commit** コマンドの出力にメッセージが表示され、コミットしたテンプレートを有効にするためにスイッチを再起動するか尋ねられます。

コミットされていないTCAMプロファイルを含むバックアップコンフィギュレーションから、書き込み消去、リロード、および実行コンフィギュレーションのコピーを実行すると、次のことが発生します。

1. TCAM プロファイルがコミットされると、スイッチはプロンプトなしで自動的にリロードします。
2. TCAM カービング CLI の後の設定は適用されません。
3. コミットされた TCAM プロファイルで設定を復元するには、バックアップコンフィギュレーションを実行コンフィギュレーションに再度コピーする必要があります。ただし、TCAM カービングプロファイルはすでにコミットされているため、スイッチのリロードはありません。

新しいコミットされた TCAM プロファイルが原因でスイッチがリロードされると、**show system reset-reason** コマンドは、次に示すようにリロードの理由を表示します。

```
switch# show system reset-reason
----- reset reason for Supervisor-module 1 (from Supervisor in slot 1) -----
1) At 302777 usecs after Sun Jan 20 22:02:37 2019
   Reason: Reload due to change in TCAM service-template
   Service:
   Version: 9.3(3)

2) At 314447 usecs after Sun Jan 20 21:52:58 2019
   Reason: Reset Requested by CLI command reload
   Service:
   Version: 9.3(3)

3) At 20142 usecs after Sun Jan 20 21:27:33 2019
   Reason: Reset Requested by CLI command reload
```

```
Service:
Version: 9.3(3)
```

スイッチを再起動後、コミットされたテンプレートが Cisco Nexus サーバー上のすべての ASIC に適用されます。Cisco Nexus デバイス上の別の ASIC に別のテンプレートをコミットできません。各テンプレートの各リージョンのサイズを指定したすべての保存済みテンプレートおよびコミット済みテンプレートは実行コンフィギュレーションに表示されます。

テンプレートがコミットされたとき、以下がチェックされます。

1. TCAM 内のすべてのリージョンの合計サイズは 4096 エントリです。
2. 各リージョンのサイズは TCAM 内に収まります。どの時点でも、TCAM リージョンに対して常に実行サイズがあります。実行サイズ（ハードウェア TCAM 内の現在のサイズ）は、コミットされ実行テンプレートとして現在使用されているデフォルトまたはユーザー定義テンプレートのどちらかによって定義されます。現在コミットされているテンプレート内のリージョンのサイズを現在の実行サイズから増やす場合は、リージョンのサイズを増やすために使用可能な現在のリージョンの外部に未使用のエントリ（他のどのリージョンにも割り当てられていないエントリ）が十分にあるかチェックされます。現在コミットされているテンプレート内のリージョンのサイズを現在の実行サイズから減らす場合は、TCAM リージョンのサイズを減らすために開放できるエントリがリージョン内に十分にあるか判断するためにチェックされます。テンプレート内のリージョンのサイズを減らすすべての変更は、そのテンプレート内のリージョンのサイズを増やす変更の前に完了します。
3. sup-region のすべての機能をサポートするためにソフトウェアで 256 エントリを必要とするため、スーパーバイザ リージョンのサイズは 256 エントリより小さく変更できません。
4. 256 エントリが使用可能でも、スーパーバイザ リージョンのデフォルト サイズは 128 エントリです。TCAM カービングにより、128 エントリをさらに使用できます。sup-region の値を 128、192、または 256 に変更するには、CLI で **sup** キーワードを使用できます。
5. スーパーバイザ リージョンおよびスパン リージョンではハードウェアは 256 エントリより多くはサポートしません。このチェックは検査過程で実施されます。

これらすべてのチェックを通過した場合、そのテンプレートをコミットでき、再起動してテンプレートを適用するかを確認するプロンプトが表示されます。

これらのチェックが失敗した場合、コミットが失敗しテンプレートは保存済みステートに戻ります。コミットが失敗した場合、**commit** コマンドの出力に失敗の原因が表示されます。

デフォルトテンプレートは変更または削除できません。このテンプレートは、保存済みからコミット済み、コミット済みから保存済みへ移行のみが可能です。デフォルトテンプレートがコミットされた場合、実行コンフィギュレーションには表示されません。デフォルトテンプレートを適用するには、現在の実行テンプレートを使用して **no commit** コマンドを入力してください。このコマンドを入力すると、テンプレートをコミットするときに実行されるのと同じ検証チェックが実行されます。すべての検証が成功すると、スイッチを再起動するか確認するメッセージが表示されます。再起動に同意すると、テンプレートがスタートアップコンフィギュレーションに保存されシステムが再起動します。再起動後、デフォルトテンプレートが適用されます。スタートアップコンフィギュレーションには、再起動前にコミットしたコミット済みテンプレートがあります。再起動後に、スタートアップコンフィギュレーションのテンプレートが使用されます。

スタートアップコンフィギュレーションにコミット済みテンプレートがない場合、デフォルトテンプレートが使用されます。

テンプレート管理コマンドを入力して、TCAM カービングテンプレートを作成および管理できます。このテンプレートベース TCAM カービング CLI は `config-sync` でサポートされます。テンプレートの作成のみが `config-sync` 内部でサポートされます。テンプレートコミットは、`config-sync` コンテキストの外部でスイッチごとに別々に実施する必要があります。

## TCAM カービング設定の確認

TCAM カービングの設定情報を表示するには、次のいずれかのコマンドを入力します。

| コマンド  | 目的                  |
|---|---------------------|
| <code>show hardware profile tcam resource template</code>                           | すべてのテンプレートを表示します。   |
| <code>show hardware profile tcam resource template name <i>template-name</i></code> | ユーザー定義テンプレートを表示します。 |
| <code>show hardware profile tcam resource template default</code>                   | デフォルトテンプレートを表示します。  |

## FCoE 設定の確認

FCoE の設定情報を確認するには、次のうちいずれかの作業を行います。

| コマンド   | 目的  |
|--|---|
| <code>switch# show fcoe</code>   | FCoE がスイッチでイネーブルになっているかどうかを表示します。             |
| <code>switch# show fcoe database</code>                                  | FCoE データベースの内容を表示します。                         |
| <code>switch# show interface [<i>interface number</i>] fcoe</code>       | 個々のインターフェイスまたはすべてのインターフェイスに関する FCoE 設定を表示します。 |
| <code>switch# show queuing interface [<i>interface slot/port</i>]</code> | キューの設定および統計情報を表示します。                          |
| <code>switch# show policy-map interface [<i>interface number</i>]</code> | 1 つまたはすべてのインターフェイスのポリシー マップ設定を表示します。          |

次の例は、FCoE 機能が有効になっているかどうかを確認する方法を示したものです。

```
switch# show fcoe
Global FCF details
      FCF-MAC is 00:0d:ec:6d:95:00
      FC-MAP is 0e:fc:00
```

```
FCF Priority is 128
```

```
FKA Advertisement period for FCF is 8 seconds
```

次に、FCoE データベースを表示する例を示します。

```
switch# show fcoe database
```

```
-----  
INTERFACE          FCID          PORT NAME          MAC ADDRESS  
-----  
vfc3                0x490100      21:00:00:1b:32:0a:e7:b8 00:c0:dd:0e:5f:76
```

次の例は、あるインターフェイスの FCoE 設定を表示する方法を示したものです。

```
switch# show interface ethernet 1/37 fcoe
```

```
Ethernet1/37 is FCoE UP
```

```
  vfc3 is Up
```

```
    FCID is 0x490100
```

```
    PWWN is 21:00:00:1b:32:0a:e7:b8
```

```
    MAC addr is 00:c0:dd:0e:5f:76
```



## CHAPTER 6

# Configuring Long-distance Over FCoE

- [Configuring Long-distance Over FCoE, on page 69](#)
- [Configurations for Different Types of Policies, on page 70](#)
- [Configuration Examples of Policy Applied to Ethernet Interfaces, on page 72](#)
- [Verifying Configuration of Long-Distance Over FCoE, on page 72](#)

## Configuring Long-distance Over FCoE

N9K-C93180YC-FX supports long distance (up to 10 kilometers) on FCoE ISLs. The support is applicable on 10G, 25G, and 40G speeds. For line rate traffic without drops, the ingress buffer sizes and pause/resume thresholds need to be increased on long-distance ISLs. This can be achieved by applying custom long-distance FCoE policies to the ISL ports. The default FCoE-related system level network-qos and queuing policies allocate fixed ingress buffer sizes and pause/resume thresholds to all Ethernet ports. To facilitate the increase of ingress buffer allocation for long-distance ISLs, it may be required to decrease the ingress buffer allocation for a few Ethernet ports by using custom short distance FCoE policies.



**Note** It is recommended to use FCoE long distance ISLs only for SAN traffic.

**Table 4: FCoE Long Distance Across Different Speeds**

| Speed | Distance |
|-------|----------|
| 10G   | 10 Km    |
| 25G   | 10 Km    |
| 40G   | 10 Km    |

**Note**

- Ingress buffer allocation for Ethernet ports that are not bound to VFC or for Ethernet ports bound to VFC (with short distance requirements, that is less than 100 meters) can be decreased by using the custom short distance FCoE policies.
- When policy is changed on ports running traffic, there will be momentary drop in traffic.
- If ingress buffer allocation failure happens for an Ethernet port, shut/no shut has to be executed on the port after the ingress buffer is made available for the Ethernet port to come up.

## Configurations for Different Types of Policies

Configurations vary for different types of policies, that is, default system level policy and interface level custom policies for different speeds, as follows:

- **Default System Level Policy for FCoE**

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

The default settings for system level policy for FCoE are as follows:

- Buffer-size - 104000
- Pause-threshold - 20800
- Resume-threshold - 19136

- **Interface Level Custom Policies for Different Speeds**

Custom policies for long distance that need to be applied to Ethernet port/port channel bound to VFC/VFC-PO ISLs with long distance support are as follows:

- **Long Distance Policy for 10G ISLs**

```
switch(config)# policy-map type queuing ld_10G_fcoe_in_que_policy
switch(config-pmap-que)# class type queuing c-in-q1
switch(config-pmap-c-que)# bandwidth percent 90
switch(config-pmap-c-que)# pause buffer-size 166400 pause-threshold 20800
resume-threshold 19136
switch(config-pmap-c-que)# class type queuing c-in-q-default
switch(config-pmap-c-que)# bandwidth percent 10
switch(config-pmap-c-que)
```

```
switch(config)# policy-map type queuing ld_10G_fcoe_in_que_policy
switch(config-pmap-que)# class type queuing c-in-q1
switch(config-pmap-c-que)# bandwidth percent 90
switch(config-pmap-c-que)# pause buffer-size 291200 pause-threshold 145600
resume-threshold 143936
switch(config-pmap-c-que)# class type queuing c-in-q-default
switch(config-pmap-c-que)# bandwidth percent 10
```

- **Long Distance Policy for 25G ISLs**

```
switch(config)# policy-map type queuing ld_25G_fcoe_in_que_policy
switch(config-pmap-que)# class type queuing c-in-q1
```

```

switch(config-pmap-c-que)# bandwidth percent 90
switch(config-pmap-c-que)# pause buffer-size 384800 pause-threshold 20800
resume-threshold 19136
switch(config-pmap-c-que)# class type queuing c-in-q-default
switch(config-pmap-c-que)# bandwidth percent 10
switch(config-pmap-c-que)#

switch(config)# policy-map type queuing ld_25G_fcoe_in_que_policy
switch(config-pmap-que)# class type queuing c-in-ql
switch(config-pmap-c-que)# bandwidth percent 90
switch(config-pmap-c-que)# pause buffer-size 728000 pause-threshold 364000
resume-threshold 362336
switch(config-pmap-c-que)# class type queuing c-in-q-default
switch(config-pmap-c-que)# bandwidth percent 10
switch(config-pmap-c-que)#

```

#### • Long Distance Policy for 40G ISLs

```

switch(config)# policy-map type queuing ld_40G_fcoe_in_que_policy
switch(config-pmap-que)# class type queuing c-in-ql
switch(config-pmap-c-que)# bandwidth percent 90
switch(config-pmap-c-que)# pause buffer-size 728000 pause-threshold 78208
resume-threshold 76544
switch(config-pmap-c-que)# class type queuing c-in-q-default
switch(config-pmap-c-que)# bandwidth percent 10
switch(config-pmap-c-que)#

switch(config)# policy-map type queuing ld_40G_fcoe_in_que_policy
switch(config-pmap-que)# class type queuing c-in-ql
switch(config-pmap-c-que)# bandwidth percent 90
switch(config-pmap-c-que)# pause buffer-size 1299584 pause-threshold 649792
resume-threshold 648128
switch(config-pmap-c-que)# class type queuing c-in-q-default
switch(config-pmap-c-que)# bandwidth percent 10
switch(config-pmap-c-que)#

```

### Custom Policy for Ingress Buffer Size and Pause/Resume Thresholds

If sufficient buffers are not available to bring up long-distance ports, then fine tuning the buffers allocated to any 10G/25G Ethernet ports (with short distance requirements, that is, less than 100 meters) using default policies is required. If sufficient buffers are not available to bring up long-distance ports, a buffer allocation failure message appears. A sample buffer allocation failure message is as follows:

```

switch(config-if)# interface ethernet1/8
switch(config-if)# service-policy type queuing input ld_10G_fcoe_in_que_policy
switch(config-if)# no shutdown
2022 Oct 31 07:39:21 HW1 %$ VDC-1 %$ %ACLQOS-SLOT1-2-ACLQOS_FAILED: ACLQOS failure: Ingress
buffer allocation failed for interface Ethernet1/8

```

Create a custom policy to free up the required buffers and apply it to the existing Ethernet ports or to Ethernet ports bound for VFC that is used for short distance connectivity.

```

switch(config)# policy-map type queuing 100m_fcoe_in_que_policy
switch(config-pmap-que)# class type queuing c-in-ql
switch(config-pmap-c-que)# bandwidth percent 50
switch(config-pmap-c-que)# pause buffer-size 41600 pause-threshold 20800 resume-threshold
19136
switch(config-pmap-c-que)# class type queuing c-in-q-default
switch(config-pmap-c-que)# bandwidth percent 50
switch(config-pmap-c-que)#

```

### Required number of Ethernet Ports to Reduce Ingress Buffers on per Long Distance FCoE ISL

The following table displays the number of Ethernet ports needing an ingress buffer size reduction to accommodate a single long distance FCoE ISL of a given speed.

**Table 5: Recommendation to Reduce Ingress Buffer Size**

| Speed                 | Recommendation                                      |
|-----------------------|---|
| 10G long distance ISL | Apply 100m_fcoe_in_que_policy on one 10G/25G port   |
| 25G long distance ISL | Apply 100m_fcoe_in_que_policy on five 10G/25G ports |
| 40G long distance ISL | Apply 100m_fcoe_in_que_policy on nine 10G/25G ports |

## Configuration Examples of Policy Applied to Ethernet Interfaces

The following section includes configuration examples of policy applied to Ethernet interfaces for enabling 10G, 25G and 40G FCoE long distance ISLs.

```
switch(config)# interface ethernet 1/1
switch(config-if)# service-policy type queuing input ld_10G_fcoe_in_que_policy
switch(config-if)#
```

```
switch(config)# interface ethernet 1/2
switch(config-if)# service-policy type queuing input ld_25G_fcoe_in_que_policy
switch(config-if)#
```

```
switch(config)# interface ethernet 1/3
switch(config-if)# service-policy type queuing input ld_40G_fcoe_in_que_policy
switch(config-if)#
```

```
switch(config)# interface ethernet 1/4
switch(config-if)# service-policy type queuing input 100m_fcoe_in_que_policy
switch(config-if)#
```

## Verifying Configuration of Long-Distance Over FCoE

To display configuration information about long-distance over FCoE, perform one of the following tasks:

| Command   | Purpose   |
|---|---|
| <b>show queuing interface eth</b> <i>eth port</i>             | Displays the allocated ingress buffer availability and pause/resume thresholds. |
| <b>show running-config interface ethernet</b> <i>eth port</i> | Displays the information about configuration.                                   |



## 第 7 章

# ファイバチャネル インターフェイスの構成 0

この章は、次の内容で構成されています。

- [ファイバチャネル インターフェイスについて \(73 ページ\)](#)
- [ファイバチャネル インターフェイスについて \(73 ページ\)](#)
- [ファイバチャネル インターフェイスの構成0 \(96 ページ\)](#)
- [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 \(112 ページ\)](#)
- [ファイバチャネル インターフェイスの確認 \(115 ページ\)](#)
- [ファイバチャネル インターフェイスのデフォルト設定, on page 118](#)
- [ファイバチャネル インターフェイスの構成0 \(119 ページ\)](#)

## ファイバチャネル インターフェイスについて

## ファイバチャネル インターフェイスについて

## 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 デバイスでは、FCoE 対応の物理イーサネット インターフェイスは、1 つの仮想のファイバチャネル (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。

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 宛先を 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)
- 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

vFC インターフェイスは、常にトランク モードで実行されます。それ以外では、どのモードでも動作しません。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。

160 vFC インターフェイスのサポートが含まれます。

Cisco Nexus デバイスは、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 インターフェイス経由の VF ポートのサポートは、各ファブリック エクステンダが Cisco Nexus デバイスに直接接続する、Cisco Nexus ファブリック エクステンダストレート型トポロジでのみサポートされます。

## 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ーです。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 トランッキングは、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 モードで有効になります。

VE ポート上に複数の VSAN を構成できます。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構成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 上で無効になります。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、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、**VE ポート構成制限**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。
- FCoE ペイロードサイズが 2112 より大きい場合、VE ポートは輻輳中にフラップする可能性があります。

### FSPF パラメータ

FSPF は、VSAN で起動されると、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ー 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         |                  |                 |         |
|---|------------------|------------------|-----------------|---------|
|   | N9K-C9336C-FX2-E | N9K-C93360YC-FX2 | N9K-C93180YC-FX | FEX     |
| 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ている vFC (VE および VF) ポート | 8 (最大値)          | 8 (最大値)          | 8 (最大値)         | サポート対象外 |

## 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せん。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ーです。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 アドレスが付いた複数の 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、および TF モードおよび TNP 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 ポートまたは F 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 F モード、または SD モードで動作しません。NPモード、Fモード、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 E モードまたは F モードで設定できます。

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ています。

- 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、管理モードで設定できる各種の属性があります。
- 動作ステータスは、インターフェイス速度のような指定された属性の現在のステータスを表します。このステータスは変更できず、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。

## 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。

### Related Topics

[SAN ポート チャネルの設定](#), on page 135

## 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。このポートは、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。

### Related Topics

[N ポート バーチャライゼーションの設定](#)

## 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 デバイス 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 デバイスでは 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。

### Related Topics

[VSAN トランキングの設定](#)

## 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送信できます。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 デバイスでは VSAN トランッ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

トランッキング 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ッキング拡張ポートとして機能します。トランッキングされた F ポート (TF ポート) に TNP ポートを接続して、NPV スイッチからコア NPIV スイッチへのリンクを作成することができます。

## 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監視します。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、TE ポート、および TF ポート、NP ポートおよび 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 デバイス 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。

### Related Topics

[VSAN トランッキングの設定](#)

## インターフェイスの状態

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。

Table 6: 管理ステート

| 管理状態 | 説明   |
|------|--|
| アップ  | インターフェイスはイネーブルです。  |
| 下へ   | 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。

Table 7: 動作ステート

| 動作状態       | 説明   |
|------------|--|
| アップ        | 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、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。 |
| 下へ         | 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<br>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。

Table 8: インターフェイスステートの理由コード

| 管理設定 | 運用ステータス       | 理由コード   |
|------|---------------|---|
| アップ  | アップ           | なし。   |
| Down | Down          | 管理上ダウンされています。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。 |
| アップ  | ダウン<br>(Down) | 次の表を参照してください。   |

管理ステータスが **up** で、動作ステータスが **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、動作不能ステータスの理由コードを示します。



**Note** 表に示されている理由コードは一部だけです。

**Table 9:** 動作不能ステータスの理由コード

| 理由コード（長いバージョン）                 | 説明   | 適用可能なモード |
|--------------------------------|--|----------|
| リンク障害または未接続                    | 物理層リンクが正常に動作していません。  | すべて（All） |
| SFPがありません                      | Small Form-Factor Pluggable（SFP）ハードウェアが接続されていません。  | すべて（All） |
| 初期化中                           | 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。   | すべて（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。  |          |
| 非アクティブ                         | インターフェイス VSAN が削除されているか、suspended ステータスにあります。<br><br>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。   |          |
| ハードウェア障害（Hardware failure）     | ハードウェア障害が検出されました。  |          |
| エラー ディセーブル化                    | 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。<br><br><ul style="list-style-type: none"> <li>• 設定障害。</li> <li>• 互換性のない BB_credit 設定</li> </ul><br>インターフェイスを正常に動作させるには、まずこのステータス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して、さらにまたは、インターフェイスをイネーブルにします。 |          |

| 理由コード (長いバージョン)  | 説明  | 適用可能なモード              |
|--|---|-----------------------|
| 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。                |                       |
| ELPが失敗したため、隔離されました   | 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       |
| ESCが失敗したため、隔離されました   | ポート ネゴシエーションが失敗しました。  |                       |
| ドメインの重複により隔離されました  | 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。  |                       |
| ファブリック再構成が無効なため、隔離されました                                      | ファブリックの再設定によりポートが分離されました。   |                       |
| ドメインマネージャが無効なため、隔離されました                                      | fcdomain 機能がディセーブルです。   |                       |
| ゾーンのマージが失敗したため、隔離されました                                       | 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 |
| 速度に互換性がないため、中断しました   | 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。                                |                       |
| モードに互換性がないため、中断しました  | 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。                               |                       |
| リモートスイッチ WWNに互換性がないため、中断しました                                 | 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のスイッチ ペアに接続されている必要があります。 |                       |

| 理由コード（長いバージョン）                         | 説明  | 適用可能なモード             |
|--|---|----------------------|
| 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 |

## バッファツーバッファ クレジット

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。

BB\_credit メカニズムは仮想ファイバチャネルインターフェイスではなく、ファイバチャネルインターフェイスで使用されます。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 (fcrxbbcredit) 値を各ファイバチャネルインターフェイスに設定できます。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、プライオリティフロー制御と呼ばれるクラスベースの一時停止メカニズムに基づいたフロー制御を提供します。プライオリティフロー制御



### Note

- バッファ間（B2B）クレジットは構成できません。
- 8G リンクのフィルパターンはIDLEでなければなりません。両方のピアで、8G リンクのフィルパターンを IDLE に設定する必要があります。コマンド **switchport fill-pattern IDLE speed speed** を使用して、Cisco Nexus 9000 スイッチでフィルパターンを IDLE に設定します。

```
switch (config)# interface fc1/1
switch (config-if)# switchport fill-pattern IDLE speed 8000
```



**Note** 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64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。

受信 B2B クレジット値は、N9K-C93180YC-FX では64、N9K-C93360YC-FX2 および N9K-C9336C-FX2-E では32です。これは、両方のプラットフォームのすべてのポートモード(F、E)に適用され、変更できません。

## ファイバチャネルのライセンス要件

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、正しいライセンスがインストールされていることを確認します。ライセンスの詳細については、このガイドのFC/FCoEの有効化の章を参照してください。



**Note** 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せんが、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。

## ファイバチャネルポートライセンスの有効化

ここでは、SAN スイッチングのライセンスを有効にする方法について説明します。

### 始める前に

ポートライセンスを有効にするには、ファイバチャネル (FC) ポートをシャットダウンする必要があります。



(注) FC ポートへの変換については、[ユニファイドポートの設定](#)を参照してください。

### 手順の概要

1. ポートライセンスを有効にします。

### 手順の詳細

#### 手順

ポートライセンスを有効にします。

例:

```
Switch(config)# int fc1/1
Switch(config-if)# port-license acquire
```

## ファイバチャネルの QoS 要件

次のタイプのインターフェイスが使用されている場合は、FCoE QoS を設定する必要があります。

- ネイティブ FC - FC の場合
- FCoE - vFC の場合
- FC および FCoE - FC および vFC の場合

スイッチでイーサネットが設定されていない場合でも、FCoE QoS を追加する必要があります。

次のコマンドは、ネイティブ FC または FCoE、または FC と FCoE 用に構成する必要があるデフォルトの QoS 構成を有効にします。

```
switch(config)# system qos
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 qos input fcoe-default-in-policy
switch(config-sys-qos)# service-policy type network-qos fcoe-default-nq-policy
```

## QoS の構成による no-drop のサポート

ingress FC/FCoE フレームをマークするには、qos ingress ポリシーが使用されます。qos ingress ポリシーは、FC/FCoE トラフィックを処理するインターフェイスに適用する必要があります（vFC にバインドされるすべてのイーサネット/ポートチャネルインターフェイスなど）。



(注)

ポート qos 領域にハードウェア TCAM スペースが予約されていることを確認します。入力 PACL TCAM しきい値が syslog に表示される場合は常に、TCAM サイズを増やし、スイッチをリロードします。

この手順は、FCoE NPV が機能するために必須です。

- ポートの ACL 領域用に、TCAM スペースを予約します。  
他の領域用に予約された TCAM スペースを取得することが必要な場合があります。
- 設定を保存します。
- ラインカードまたはスイッチをリロードします。  
スイッチをリロードします。
- ACL 領域の TCAM スペースを確認します。
- N9K-C93180YC-FX、N9K-C93360YC-FX2、および N9K-C9336C-FX2-E での TCAM カービングの例:

```
hardware access-list tcam region ing-racl 1536
hardware access-list tcam region ing-ifacl 256
hardware access-list tcam region ing-redirect 256
```

- N9K-C92160YC-X、N9K-C9272Q、N9K-C93236C、N9K-C93180YC-EX、または N9K-C93180YC-FX での TCAM カービングの例

```
hardware access-list tcam region ing-racl 1536
hardware access-list tcam region ing-redirect 256
```

例:

```
switch# show hardware access-list tcam region | i i ifacl
Ingress PACL [ing-ifacl] size = 256
switch# config

switch(config)# hardware access-list tcam region ing-racl 1536
switch(config)# hardware access-list tcam region ing-ifacl 256
switch(config)# hardware access-list tcam region ing-redirect 256

switch# copy running-config startup-config
switch# reload

switch# show hardware access-list tcam region | i i ifacl
Ingress PACL [ing-ifacl] size = 256

switch# show hardware access-list tcam region | i "IPV4 Port QoS \[qos\] size"
Ingress PACL [ing-ifacl] size = 256
switch# config

switch(config)# hardware access-list tcam region ing-racl 1536
switch(config)# hardware access-list tcam region ing-ifacl 256
```

```
switch(config)# hardware access-list tcam region ing-redirect 256

switch# copy running-config startup-config

switch# reload

switch# show hardware access-list tcam region | i "IPv4 Port QoS \[qos\] size"
Ingress PACL [ing-ifacl] size = 256
```

### FCoE QoS ポリシーの設定

- FCoE のデフォルト ポリシーには、network-qos、output queuing、input queuing の 4 種類があります。
- FCoE デフォルト ポリシーをアクティブにするには、**feature-set fcoe-npv** コマンドを使用して FCoE-NPV 機能を有効にし、**no feature-set fcoe-npv** コマンドを実行して FCoE デフォルト ポリシーを削除します。
- **no feature-set fcoe-npv** を入力する前に、インターフェイスおよびシステム レベルからすべての FCoE ポリシーを削除します。**no feature-set fcoe-npv** コマンドは、FC ポートが設定されていない場合にのみ使用できます。



- (注) FCoE のデフォルト ポリシーを使用することを推奨します。適用されるすべてのポリシーは、同じタイプ (4q または 8q モード) である必要があります。システムおよびインターフェイス レベルで明示的に適用または削除する必要があります。



- (注) Active/Active FEX トポロジをサポートするのは、次のものだけです。
- N2K-C2232PP
  - N2K-C2348UPQ
  - NB22HP
  - NB22IBM
- FCoE トラフィックに異なるキューまたは cos 値を使用するには、ユーザー定義のポリシーを作成します。

## FC/FCoE の QoS ポリシーの構成

- FC/FCoE のデフォルトポリシーには、network-qos、output queuing、input queuing、および qos の 4 種類があります。
- FC/FCoE トラフィックに別のキューまたは cos 値を使用するには、ユーザー定義のポリシーを作成します。
- これらの方法の 1 つに従って QoS ポリシーを構成できます。
  - 定義済みポリシー：要件に合わせて事前定義されたネットワーク QoS ポリシー（**default-fcoe-in-policy**）を適用できます。



- (注)
- デフォルトでは、FCoE に適用されるポリシーはありません。
  - QOS ポリシーの下での **no-stats** コマンドの使用は、ネイティブなファイバチャネルポートがある場合にのみ必須で、コマンドは N9K-C93180YC-FX プラットフォームにのみ適用されます。
  - ユーザー定義のポリシー：システム定義ポリシーの 1 つに準拠する QoS ポリシーを作成できます。

## システム全体の QoS ポリシーの設定



- (注) FC/FCoE トラフィックを伝送するすべてのインターフェイスについて、ネットワーク QoS ポリシーと出力/入力キューイングポリシーをシステムレベルで適用し、qos ポリシーをインターフェイスレベルで適用する必要があります。

```
switch(config)# system qos
switch(config-sys-qos)# service-policy type queuing input default-fcoe-in-que-policy
switch(config-sys-qos)# service-policy type queuing output { default-fcoe-8q-out-policy |
default-fcoe-out-policy }
switch(config-sys-qos)# service-policy type network-qos { default-fcoe-8q-nq-policy |
default-fcoe-nq-policy }
```

### ユーザー定義ポリシーの設定例

```
switch(config)# policy-map type network-qos fcoe_nq
switch(config-pmap-nqos)# class type network-qos c-nq1
switch(config-pmap-nqos-c)# pause pfc-cos 3
switch(config-pmap-nqos-c)# mtu 9216
switch(config-pmap-nqos-c)# class type network-qos c-nq2
switch(config-pmap-nqos-c)# mtu 1500
switch(config-pmap-nqos-c)# class type network-qos c-nq3
switch(config-pmap-nqos-c)# mtu 1500
switch(config-pmap-nqos-c)# class type network-qos c-nq-default
switch(config-pmap-nqos-c)# mtu 1500
switch(config-pmap-nqos-c)# exit
switch(config-pmap-nqos)# exit
```

```

switch(config)#
switch(config)# policy-map type queuing fcoe-in-policy
switch(config-pmap-que)# class type queuing c-in-q1
switch(config-pmap-c-que)# bandwidth percent 50
switch(config-pmap-c-que)# class type queuing c-in-q-default
switch(config-pmap-c-que)# bandwidth percent 50
switch(config-pmap-c-que)# exit
switch(config)
switch(config)# policy-map type queuing fcoe-out-policy
switch(config-pmap-que)# class type queuing c-out-q3
switch(config-pmap-c-que)# priority level 1
switch(config-pmap-c-que)# class type queuing c-out-q-default
switch(config-pmap-c-que)# bandwidth remaining percent 50
switch(config-pmap-c-que)# class type queuing c-out-q1
switch(config-pmap-c-que)# bandwidth remaining percent 50
switch(config-pmap-c-que)# class type queuing c-out-q2
switch(config-pmap-c-que)# bandwidth remaining percent 0
switch(config-pmap-c-que)# exit
switch(config)#
switch(config)# class-map type qos match-any fcoe
switch(config-cmap-qos)# match protocol fcoe
switch(config-cmap-qos)# match cos 3
switch(config-cmap-qos)# exit
switch(config)#
switch(config)# policy-map type qos fcoe_qos_policy
switch(config-pmap-qos)# class fcoe
switch(config-pmap-c-qos)# set cos 3
switch(config-pmap-c-qos)# set qos-group 1
switch(config-pmap-c-qos)# exit
switch(config-pmap-qos)# exit
switch(config)#
switch(config)# system qos
switch(config-sys-qos)# service-policy type queuing input fcoe-in-policy
switch(config-sys-qos)# service-policy type queuing output fcoe-out-policy
switch(config-sys-qos)# service-policy type network-qos fcoe_nq

```



(注) QOS ポリシーでの **set cos 3** コマンドは、ネイティブファイバチャネルポートがある場合にのみ必須で、N9K-C93180YC-FX プラットフォーム、N9K-C93360YC-FX2 プラットフォーム、および N9K-C9336C-FX2-Eにのみ適用されます。他のすべての Cisco Nexus 9000 プラットフォームスイッチでは、この手順はオプションです。



(注) FEX が接続されている場合:

- システム レベルおよび HIF ポートに QoS ポリシーを適用して、FCoE トラフィックのポーズフレームを受け入れます。
- FEX がオンラインの場合、8q ポリシーはサポートされません。

```

switch(config)# system qos
switch(config-sys-qos)# service-policy type queuing input policy-name
switch(config-sys-qos)# service-policy type queuing output policy-name
switch(config-sys-qos)# service-policy type network-qos policy-name
switch(config-sys-qos)# service-policy type qos input policy-name

```

FC/FCoE の VFC インターフェイスにバインドされている個々のイーサネット/ポートチャネルインターフェイスに対し、ingress QoS ポリシーを適用します。

```
switch(config)# interface ethernet 2/1
switch(config-if)# switchport mode trunk
switch(config-if)# mtu 9216 /* Or maximum allowed value */
switch(config-if)# service-policy type qos input { default-fcoe-in-policy | fcoe_qos_policy
) no-stats
switch(config-if)# exit
switch(config)#
```



(注) QoS ポリシーは、HIF インターフェイスまたは HIF インターフェイスのポート チャネルにアタッチする必要があります。

- HIF インターフェイス

```
interface "HIF port"
service-policy type qos input policy-name
```

- HIF インターフェイスのポート チャネル

```
interface port-channel
)
service-policy type qos input policy-name
```



(注) 次のプラットフォームは 8q ポリシーをサポートしていません。

- Cisco Nexus 9332PQ スイッチ
- Cisco Nexus C9372PX スイッチ
- Cisco Nexus C9396PX switch
- Cisco Nexus C9372PX-E スイッチ
- Cisco Nexus X9536C-S ラインカード
- Cisco Nexus X9564PX ラインカード

- FC/FCoE QoS ポリシーの設定

- FC/FCoE のデフォルトポリシーには、ネットワーク QoS、出力キューイング、入力キューイング、QoS の 4 種類があります。
- FCoE デフォルトポリシーをアクティブにするには、**feature-set fcoe-npv** コマンドを使用して FCoE-NPV 機能を有効にし、**no feature-set fcoe-npv** コマンドを実行して FCoE デフォルトポリシーを削除します。

- **no feature-set fcoe-npv** を入力する前に、インターフェイスおよびシステム レベルからすべての FCoE ポリシーを削除します。



---

(注) FCoE のデフォルト ポリシーを使用することを推奨します。適用されるすべてのポリシーは、同じタイプ (4q または 8q モード) である必要があります。システムおよびインターフェイス レベルで明示的に適用または削除する必要があります。

---

- FC/FCoE トラフィックに別のキューまたは cos 値を使用するには、ユーザー定義のポリシーを作成します。
- FC/FCoE のネットワーク QoS ポリシーの構成
  - これらの方法の 1 つに従ってネットワーク QoS ポリシーを設定できます。
    - 定義済みポリシー: 要件に合わせて事前定義されたネットワーク QoS ポリシーを適用できます。 **default-fcoe-8q-nq-policy** または **default-fcoe-nq-policy** を選択するオプションがあります。



---

(注) デフォルトでは、FC/FCoE に適用されるポリシーはありません。

---

- ユーザー定義のポリシー: システム定義ポリシーの 1 つに準拠するネットワークの QoS ポリシーを作成できます。
- FC/FCoE の出力キューイング ポリシーの構成
  - これらの方法の 1 つに従って、出力キューイング ポリシーを構成できます。
    - 定義済みポリシー: 要件に合わせて事前定義された出力キューイング ポリシーを適用できます。 **default-fcoe-8q-out-policy** または **default-fcoe-out-policy** を選択するオプションがあります。



---

(注) デフォルトでは、FC/FCoE に適用されるポリシーはありません。

---

- ユーザー定義のポリシー: システム定義ポリシーの 1 つに準拠する出力キューイング ポリシーを作成できます。
- FC/FCoE の入力キューイング ポリシーの構成
  - これらの方法の 1 つに従って、入力キューイング ポリシーを構成できます。
    - 定義済みポリシー: 定義済み入力キューイングポリシーを適用できます。 **default-fcoe-in-que-policy**



(注) デフォルトでは、FCoE に適用されるポリシーはありません。

- ユーザー定義のポリシー: システム定義ポリシーの1つに準拠する入力キューイングポリシーを作成できます。
- FCoE の QoS ポリシーの構成
  - これらの方法の1つに従って QoS ポリシーを構成できます。
  - 定義済みポリシー: 要件に合わせて事前定義されたネットワーク QoS ポリシー (**default-foe-in-policy**) を適用できます。



(注) • デフォルトでは、FCoE に適用されるポリシーはありません。

- **no-stats** を QoS ポリシーに適用することを推奨します。

- ユーザー定義のポリシー: システム定義ポリシーの1つに準拠する QoS ポリシーを作成できます。

- システム全体の QoS ポリシーの設定



(注) FCoE トラフィックを伝送するすべてのインターフェイスについて、ネットワーク QoS ポリシーと出力/入力キューイングポリシーをシステムレベルで適用し、qos ポリシーをインターフェイスレベルで適用する必要があります。

```
switch(config)# system qos
switch(config-sys-qos)# service-policy type queuing input default-foe-in-que-policy
switch(config-sys-qos)# service-policy type queuing output { default-foe-8q-out-policy
| default-foe-out-policy }
switch(config-sys-qos)# service-policy type network-qos { default-foe-8q-nq-policy |
default-foe-nq-policy }
```

- ユーザー定義ポリシーの設定例

```
switch(config)# policy-map type network-qos fcoe_nq
switch(config-pmap-nqos)# class type network-qos c-nq1
switch(config-pmap-nqos-c)# pause pfc-cos 3
switch(config-pmap-nqos-c)# mtu 9216
switch(config-pmap-nqos-c)# class type network-qos c-nq2
switch(config-pmap-nqos-c)# mtu 1500
switch(config-pmap-nqos-c)# class type network-qos c-nq3
switch(config-pmap-nqos-c)# mtu 1500
switch(config-pmap-nqos-c)# class type network-qos c-nq-default
switch(config-pmap-nqos-c)# mtu 1500
```

```
switch(config-pmap-nqos-c)# exit
switch(config-pmap-nqos)# exit
switch(config)#
switch(config)# policy-map type queuing fcoe-in-policy
switch(config-pmap-que)# class type queuing c-in-q1
switch(config-pmap-c-que)# bandwidth percent 50
switch(config-pmap-c-que)# class type queuing c-in-q-default
switch(config-pmap-c-que)# bandwidth percent 50
switch(config-pmap-c-que)# exit
switch(config)
switch(config)# policy-map type queuing fcoe-out-policy
switch(config-pmap-que)# class type queuing c-out-q3
switch(config-pmap-c-que)# priority level 1
switch(config-pmap-c-que)# class type queuing c-out-q-default
switch(config-pmap-c-que)# bandwidth remaining percent 50
switch(config-pmap-c-que)# class type queuing c-out-q1
switch(config-pmap-c-que)# bandwidth remaining percent 50
switch(config-pmap-c-que)# class type queuing c-out-q2
switch(config-pmap-c-que)# bandwidth remaining percent 0
switch(config-pmap-c-que)# exit
switch(config)#
switch(config)# class-map type qos match-any fcoe
switch(config-cmap-qos)# match protocol fcoe
switch(config-cmap-qos)# match cos 3
switch(config-cmap-qos)# exit
switch(config)#
switch(config)# policy-map type qos fcoe_qos_policy
switch(config-pmap-qos)# class fcoe
switch(config-pmap-c-qos)# set cos 3
switch(config-pmap-c-qos)# set qos-group 1
switch(config-pmap-c-qos)# exit
switch(config-pmap-qos)# exit
switch(config)#
switch(config)# system qos
switch(config-sys-qos)# service-policy type queuing input fcoe-in-policy
switch(config-sys-qos)# service-policy type queuing output fcoe-out-policy
switch(config-sys-qos)# service-policy type network-qos fcoe_nq
```



- 
- (注) QOS ポリシーでの **set cos 3** コマンドは、ネイティブファイバチャネルポートがある場合にのみ必須で、N9K-C93180YC-FX プラットフォームにのみ適用されます。他のすべての Cisco Nexus 9000 プラットフォームスイッチでは、この手順はオプションです。
-



(注) FEX が接続されている場合:

- システム レベルおよび HIF ポートに QoS ポリシーを適用して、FCoE トラフィックのポーズ フレームを受け入れます。
- FEX がオンラインの場合、8q ポリシーはサポートされません。

```
switch(config)# system qos
switch(config-sys-qos)# service-policy type queuing input
policy-name
switch(config-sys-qos)# service-policy type queuing output
policy-name
switch(config-sys-qos)# service-policy type network-qos
policy-name
switch(config-sys-qos)# service-policy type qos input policy-name
```

FCoE の VFC インターフェイスにバインドされている個々のイーサネット/ポートチャネルインターフェイスに対し、ingress QoS ポリシーを適用します。

```
switch(config)# interface ethernet 2/1
switch(config-if)# switchport mode trunk
switch(config-if)# mtu 9216 /* Or maximum allowed value */
switch(config-if)# service-policy type qos input { default-fcoe-in-policy |
fcoe_qos_policy }
switch(config-if)# exit
switch(config)#
```



(注) QoS ポリシーは、HIF インターフェイスまたは HIF インターフェイスのポートチャネルにアタッチする必要があります。

- HIF インターフェイス

```
interface "HIF port"
service-policy type qos input policy-name
```

- HIF インターフェイスのポートチャネル

```
interface port-channel
service-policy type qos input policy-name
```



(注) 次のプラットフォームは 8q ポリシーをサポートしていません。

- Cisco Nexus 9332PQ スイッチ
- Cisco Nexus C9372PX スイッチ
- Cisco Nexus C9396PX switch
- Cisco Nexus C9372PX-E スイッチ
- Cisco Nexus X9536C-S ライン カード
- Cisco Nexus X9564PX ライン カード



(注) Syslog にラベル割り当ての失敗が表示される場合は常に、FC/FCoE ACL がインターフェイスに適用されていない可能性があります。次に、QoS ポリシーがインターフェイスに `no-stats` で適用されているかどうかを確認する必要があります。

## 物理ファイバチャネル インターフェイス

Cisco Nexus C93180YC-FX および C93360YC-FX2 スイッチは、SAN ネットワークに接続されたアップリンクまたは（サーバーまたはターゲットに接続された）ダウンリンクとして、それぞれ最大 48 および 96 の物理ファイバチャネル（FC）インターフェイスをサポートします。Cisco Nexus N9K-C9336C-FX2-E スイッチには、SAN ネットワークに接続されたアップリンクまたはダウンリンク（サーバまたはターゲットに接続された）として、最大 112 個の物理ファイバチャネル（FC）ブレイクアウト インターフェイスを含めることができます。FC ブレイクアウトで変換できるのは、9 ～ 36 のポートのみです。

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、SD、TE、および TF および TNP のモードをサポートします。



**Note** NP および TNP は、機能 `fcoe-npv` でのみサポートされます。

## 長距離 ISL

Cisco NX-OS リリース 10.2(1)F 以降、Cisco Nexus N9K-C93180YC-FX および N9K-C93360YC-FX2 スイッチは、32 Gbps ファイバチャネルスイッチ間リンク（ISL）での長距離をサポートします。

長距離 ISL `BB_credit` を計算するための公式は、2 KB の一般的なファイバー チャネル フレームとインターフェイス速度を想定しています。新しいスイッチの固定（64）バッファ間クレジットは、

最大3キロメートルの距離にわたって32 Gbps ファイバチャネル ISL をサポートするようになりました。

表 10: さまざまな速度での FC 長距離

| スピード | ディスタンス |
|------|--------|
| 32G  | 3 km   |
| 16G  | 5 km   |
| 8G   | 10 km  |

表 11: さまざまな速度での FC 長距離

| スピード | ディスタンス | Throughput |
|------|--------|------------|
| 32G  | 3 km   | 25.45G     |
| 16G  | 5 km   | 13.35G     |
| 8G   | 10 km  | 6.67G      |

## ファイバチャネルインターフェイスの構成0

### ファイバチャネルインターフェイスの構成

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。



**Note** FC ポートの作成またはポート変換については、[ユニファイドポートの設定](#)セクションを参照してください。

#### SUMMARY STEPS

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

#### DETAILED STEPS

##### Procedure

|        | Command or Action                     | Purpose              |
|--------|---------------------------------------|----------------------|
| Step 1 | switch# <b>configuration terminal</b> | コンフィギュレーションモードに入ります。 |

|        | Command or Action  | Purpose   |
|--------|--|---|
| Step 2 | switch(config)# <b>interface</b> { <b>fc slot/port</b> } { <b>vfc vfc-id</b> } | <p>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。</p> <p><b>Note</b><br/>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状態がアップの場合、ファイバチャネル ID (FC ID) も割り当てられます。</p> <p><b>Note</b><br/>これが 10G ブレイクアウトポートの場合、<i>slot/port</i> 構文は <i>QSFP-module/port</i> になります。</p> <p><b>Note</b><br/>これが QSFP+ GEM またはブレイクアウトポートの場合、<i>port</i> 構文は <i>QSFP-module/port</i> になります。</p> |

## ファイバチャネル インターフェイスの範囲の構成

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。

### SUMMARY STEPS

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** ] }

### DETAILED STEPS

#### Procedure

|        | Command or Action  | Purpose   |
|--------|--|---|
| Step 1 | switch# <b>configuration terminal</b>  | コンフィギュレーションモードに入ります。  |
| Step 2 | switch(config)# <b>interface</b> { <b>fc slot/port - port</b> [ , <b>fc slot/port - port</b> ]   <b>vfc vfc-id - vfc-id</b> [ , <b>vfc vfc-id - vfc-id</b> ] } | <p>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。</p> <p><b>Note</b><br/>これが QSFP+ GEM またはブレイクアウトポートの場合、<i>port</i> 構文は <i>QSFP-module/port</i> になります。</p> |

## インターフェイスの管理状態の設定

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 フローを有効に無効にする手順は、次のとおりです。

### SUMMARY STEPS

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

### DETAILED STEPS

#### Procedure

|               | Command or Action  | Purpose   |
|---------------|--|---|
| <b>Step 1</b> | switch# <b>configuration terminal</b>                        | コンフィギュレーション モードに入ります。   |
| <b>Step 2</b> | switch(config)# <b>interface</b> {fc slot/port} {vfc vfc-id} | <p>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。</p> <p><b>Note</b><br/>これが 10G ブレイクアウト ポートの場合、<i>slot/port</i> 構文は <i>QSFP-module/port</i> になります。</p> <p><b>Note</b><br/>これが QSFP+ GEM またはブレイクアウト ポートの場合、<i>port</i> 構文は <i>QSFP-module/port</i> になります。</p> |
| <b>Step 3</b> | switch(config-if)# <b>shutdown</b>                           | 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

### SUMMARY STEPS

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

## DETAILED STEPS

## Procedure

|        | Command or Action  | Purpose  |
|--------|--|--|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                      | 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。   |
| Step 2 | <pre>switch(config) # interface vfc vfc-id}</pre> <b>Example:</b><br><pre>switch(config) # interface vfc 20 switch(config-if) #</pre>      | 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。   |
| Step 3 | <pre>switch(config-if) # switchport mode {F}</pre> <b>Example:</b><br><pre>switch(config-if) # switchport mode F switch(config-if) #</pre> | ポートモードを設定します。<br><br>vFC インターフェイスは F モードのみをサポートします。<br><br><b>Note</b><br>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。 |

## Example

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 F
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 F
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 1、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構成

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、任意の英数字の文字列を使用できます。

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。

### SUMMARY STEPS

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**

### DETAILED STEPS

#### Procedure

|               | Command or Action   | Purpose  |
|---------------|---|--|
| <b>Step 1</b> | switch# <b>configuration terminal</b>                         | コンフィギュレーションモードに入ります。   |
| <b>Step 2</b> | switch(config)# <b>interface</b> {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。<br><br><b>Note</b><br>これが 10G ブレイクアウト ポートの場合、slot/port 構文は <i>QSFP-module/port</i> になります。<br><br><b>Note</b><br>これが QSFP+ GEM またはブレイクアウト ポートの場合、port 構文は <i>QSFP-module/port</i> になります。 |
| <b>Step 3</b> | switch(config-if)# <b>switchport description cisco-HBA2</b>   | 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。  |
| <b>Step 4</b> | switch(config-if)# <b>no switchport description</b>           | インターフェイスの説明をクリアします。  |

## ユニファイドポートの設定

### 始める前に

サポートされる Cisco Nexus スイッチが存在することを確認します。ユニファイドポートは、Cisco Nexus C93180YC-FX スイッチ、N9K-C9336C-FX2-E、および C93360YC-FX2 スイッチで使用できます。

- Cisco Nexus 5672UP
- Cisco Nexus 5672UP-16G
- N56-M24UP2Q LEM を搭載した Cisco Nexus 56128P
- N5696-M20UP LEM を搭載した Cisco Nexus 5696Q



(注) C93180YC-FX、N9K-C9336C-FX2-E、または C93360YC-FX2 プラットフォームの詳細については、*Cisco Nexus 9000 Series Hardware Installation Guide* を参照してください。

ユニファイドポートをファイバチャネルまたはFCoEとして設定している場合は、**install feature-set fcoe** および **feature-set fcoe** コマンドをイネーブルにしていることを確認します。

### 手順

|               | コマンドまたはアクション  | 目的  |
|---------------|---|---|
| <b>Step 1</b> | switch# <b>configure terminal</b>                                 | 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。  |
| <b>Step 2</b> | switch(config)# <b>slot slot number</b>                           | スイッチ上のスロットを指定します。<br><br>(注)<br>これが QSFP+ GEM またはブレイクアウトポートの場合、 <i>port</i> 構文は <i>QSFP-module/port</i> になります。  |
| <b>Step 3</b> | switch(config-slot)# <b>port port number type {ethernet   fc}</b> | ユニファイドポートをネイティブファイバチャネルポートおよびイーサネットポートとして設定します。<br><br><ul style="list-style-type: none"> <li>• <b>type</b> : シャーシのスロット上で設定するポートのタイプを指定します。</li> <li>• <b>ethernet</b> : イーサネットポートを指定します。</li> <li>• <b>fc</b> : ファイバチャネル (FC) ポートを指定します。</li> <li>• <b>breakout</b> : ポートタイプをイーサネットポートから FC ポートに変更または分割します。ただ</li> </ul> |

|  | コマンドまたはアクション | 目的  |
|--|--------------|---|
|  |              | <p>し、このオプションは N9K-C9336C-FX2-E でのみサポートされます。</p> <p>(注)</p> <ul style="list-style-type: none"> <li>• 拡張モジュール上のユニファイドポートを変更するには、GEM カードの電源を再投入する必要があります。変更を有効にするためにスイッチ全体をリブートする必要はありません。</li> <li>• ユニファイドポートをファイバチャネルとして設定する場合、ファイバチャネルインターフェイスおよびVSANメンバーシップの既存の設定は影響を受けません。</li> <li>• N9K-C93180YC-FX スイッチでは、FC ポート範囲は 4 の倍数にする必要があります。不連続にすることもできます。変更を有効にするために、スイッチをリロードしてください。</li> <li>• N9K-C93360YC-FX2 スイッチでは、カラム内の 4 つの前面パネルポートすべてをまとめて FC/イーサネットに変換する必要があります。このスイッチでは、4 つのポートがポートグループを形成します。たとえば、最初のポートグループは、1、2、49、50 です。2 番目のポートグループは、3、4、51、52 になり、以下も同様です。</li> <li>• N9K-C9336C-FX2-E スイッチでは、ポートタイプ (9 ~ 36 など) を FC ブレークアウトポートとして変換できます。ポートは、連続した範囲 (たとえば、9 ~ 11)、非連続的な範囲 (たとえば、18、23、30)、または単一のポート (たとえば、36) の FC ブレークアウトポートとして変換することもできます。</li> </ul> <p>(注)</p> <p>N5672-16G で FC ポートを構成する場合、16G をサポートするには、ファブリックモードを 40G モードにする必要があります。ポートがイーサネットから FC に変更されると、次回のリロード時にファブリックモードが 40G に変更されます。初めてポートを FC に変更すると、次のメッセージが表示されます: 「ポートの種類が変更されました。ファブリックモードも変更されます。設定を保存して、スイッチをリロードしてください」。</p> |

|               | コマンドまたはアクション   | 目的   |
|---------------|--|--|
|               |  | 現在のファブリック モード設定を確認するために使用します。 <b>show fabric-mode</b><br><br>FC ポート範囲は 4 の倍数にする必要があります。不連続にすることもできます。変更を有効にするために、スイッチをリロードしてください。  |
| <b>Step 4</b> | <code>switch(config-slot)# copy running-config startup-config</code> | 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。   |
| <b>Step 5</b> | <code>switch(config-slot) # reload</code>                            | スイッチをリブートします。  |
| <b>Step 6</b> | <code>switch(config) # slot slot number</code>                       | スイッチ上のスロットを指定します。  |
| <b>Step 7</b> | <code>switch(config-slot) # no port port number type fc</code>       | <code>copy rs</code> を実行してスイッチをリロードした後、ポートをイーサネット ポートに戻します。<br><br>(注)<br>すべての FC ポートが削除されると、ファブリック モードは 10-G モードに変わります。すべてのポートをイーサネットに変更すると、次のメッセージが表示されます。「ポートの種類が変更されました。ファブリックモードも変更されます。設定を保存して、スイッチをリロードしてください」。 |

### 例

次の例は、C93180YC-FX 拡張モジュールでユニファイド ポートを設定する方法を示したものです。

```
switch# configure terminal
switch(config)# slot 1
switch(config-slot)# port 1-16 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
switch(config-slot)#
```



(注) N9K-C93180YC-FX および N9K-C93360YC-FX2 スイッチでは、個々のポートを FC ポートに変換できません。N5672UP-16G では、スロット 2 のみに UP ポートがあります。

```
switch# configure terminal
switch(config)# slot 1
switch(config-slot)# port 1-24 type fc
Port type is changed. ACTION REQUIRED: Please save configurations and reload the switch
switch(config-slot)#
```

または

```
switch# configure terminal
switch(config)# slot 2
switch(config-slot)# port 13-24 type fc
Port type is changed. Please power-off and no power-off the module
switch(config-slot)#
```

次の例は、スロット 1、10 ポートを Cisco N6004X-M20UP モジュールの FC ポートとして設定する方法を示しています。

```
switch# configure terminal
switch(config)# slot 1
switch(config-slot)# port 1-10 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
```

## ポート速度の設定

ポート速度は、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設定できます。サポートされるすべてのプラットフォームスイッチで、サポートされる最小速度は 4G で、最大速度は 32G です。ただし、N9K-C9336C-FX2-E スイッチでサポートされる最小速度は 8G であり、サポートされる最大速度は同じく 32G です。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。



**Note** 8G 速度はサーバーおよびターゲット インターフェイスに対してサポートされていません。



**Caution** 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。

### SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **interface fc slot/port**
3. switch(config-if)# **switchport speed 16000**
4. switch(config-if)# **no switchport speed**

### DETAILED STEPS

#### Procedure

|        | Command or Action                     | Purpose               |
|--------|---------------------------------------|-----------------------|
| Step 1 | switch# <b>configuration terminal</b> | コンフィギュレーション モードに入ります。 |

|        | Command or Action                                      | Purpose  |
|--------|--|--|
| Step 2 | <code>switch(config)# interface fc slot/port</code>    | <p>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。</p> <p><b>Note</b><br/>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。</p> <p><b>Note</b><br/>これが 10G ブレイクアウト ポートの場合、<i>slot/port</i> 構文は <i>QSFP-module/port</i> になります。</p> <p><b>Note</b><br/>これが QSFP+ GEM またはブレイクアウト ポートの場合、<i>port</i> 構文は <i>QSFP-module/port</i> になります。</p>  |
| Step 3 | <code>switch(config-if)# switchport speed 16000</code> | <p>インターフェイスのポート速度を 16 Mbps に構成します。</p> <p>数値は、Mbps 単位の速度を表します。4 Gbps インターフェイスには 4000 の速度、8 Gbps インターフェイスには 8000、16 Gbps インターフェイスには 16000、32 Gbps インターフェイスには 32000、または auto (デフォルト) を設定できます。</p> <p><b>Note</b><br/>16G ホストアダプタを Cisco Nexus 9000 スイッチの 32G SFP ポートに接続するときに、速度が自動速度として設定されている場合、またはデフォルトが 8G 速度に設定されているときにリンクがアップしない場合は、<b>switchport speed 16000</b> コマンドを使用して、ポートを手動で設定する必要があります。</p> |
| Step 4 | <code>switch(config-if)# no switchport speed</code>    | <p>インターフェイスの出荷時のデフォルト (auto) 管理速度に戻します。</p>  |

## トランク モードの構成

トランク モードを構成するには、次の作業を行います。

### 手順の概要

1. `switch# configuration terminal`
2. `switch(config)# interface fc slot/port`
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

#### 手順

|               | コマンドまたはアクション   | 目的  |
|---------------|--|---|
| <b>Step 1</b> | switch# <b>configuration terminal</b>                | コンフィギュレーション モードに入ります。                           |
| <b>Step 2</b> | switch(config)# <b>interface fc slot/port</b>        | 指定し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。 |
| <b>Step 3</b> | switch(config-if)# <b>switchport trunk mode on</b>   | 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)。       |
| <b>Step 4</b> | switch(config-if)# <b>switchport trunk mode off</b>  | 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。               |
| <b>Step 5</b> | switch(config-if)# <b>switchport trunk mode auto</b> | 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。      |

### コメント

トランキング モードがオンの FC ポートと SAN-PO リンクが 2 つのスイッチ間で起動するには、両方のスイッチを互いの OUI で構成する必要があります。

OUI 値がデフォルトで登録されていない場合にのみ、スイッチで OUI を構成します。OUI は次のように検出および構成されます。

```
N9K(config-if)# show wwn switch
Switch WWN is 20:00:2c:d0:2d:50:ea:64
N9K(config-if)#
```

スイッチでは、OUI (0x2cd02d) がすでに登録されている場合、次の出力が表示されます。

```
MDS9710(config-if)# sh wwn oui | i 2cd02d
0x2cd02d Cisco Default
MDS9710(config-if) #
If the OUI is not registered, configure it manually.
MDS9710(config-if)# wwn oui 0x2cd02d
```

Cisco NX-OS Release 7.3(0)D1(1) 以降では、Cisco MDS 9700 シリーズコアスイッチで OUI を構成できます。

### 自動検知

自動検知は、速度に関係なく、すべてのインターフェイスで有効になっています。8G Small Form-Factor Pluggable (SFP) が挿入されている場合、インターフェイスは 8G および 4G の速度で動作します。16G SFP が挿入されている場合、インターフェイスは 16G、8G、および 4G の速度でのみ動作し、32G SFP では、インターフェイスは 32G、16G、および 8G の速度で動作します。



**Note** Cisco Nexus C93180YC-FX スイッチは 10G SFP をサポートします。Cisco Nexus 2348UPQ では、16G は自動検知されません。16G 速度を明示的に設定するには、ファイバチャネル インターフェイスを使用した *Cisco Unified FEX Nexus 2348UPQ* の設定を参照してください。

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。

## ブレイクアウトによる FC ポートの変換

ファイバチャネル (FC) ポートのブレイクアウト インターフェイスポート オプションは、Cisco Nexus N9K-C9336C-FX2-E プラットフォーム スイッチ上の FC のインターフェイスでのみサポートされています。LCM コンポーネントは、FC ポートのブレイクアウトまたは変換をサポートしません。

FCoE ポートを FC ポートに変換するには、次の手順を実行します。

### SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **slot1**
3. switch(config-slot)# **port 9 type fc breakout**
4. switch(config-slot)# **reload**

### DETAILED STEPS

#### Procedure

|               | Command or Action                                   | Purpose  |
|---------------|---|--|
| <b>Step 1</b> | switch# <b>configuration terminal</b>               | コンフィギュレーション モードに入ります。  |
| <b>Step 2</b> | switch(config)# <b>slot1</b>                        | シャーシのスロットで事前プロビジョニングを有効にします。   |
| <b>Step 3</b> | switch(config-slot)# <b>port 9 type fc breakout</b> | ポートタイプを FCoE ポートからファイバー チャネル ポートに変更または分割します。<br><br><b>Note</b><br>ポートタイプ、たとえば 9 ~ 36 を、FC ブレイクアウトポートとして変換できます。ポートは、連続範囲 (たとえば、9 ~ 11)、非連続範囲 (たとえば、18、23、30)、または単一ポート (たとえば、36) の FC ブレイクアウト ポートとして変換できます。 |

|        | Command or Action                  | Purpose       |
|--------|------------------------------------|---------------|
| Step 4 | switch(config-slot)# <b>reload</b> | スイッチをリロードします。 |

スイッチがリロードされると、スイッチはFCブレイクアウトポート（fc1/9/1...fc1/9/4 など）でオンラインになります。

## ブレイクアウト インターフェイスでの速度の変更

各ブレイクアウト インターフェイスで速度を変更できます。ただし、すべてのブレイクアウトポートの速度が変更されます。

コマンドの例:

```
switch(config)# int fc1/9/1-4
switch(config-if)# switchport speed 32000
!!!WARNING! This command affects all interfaces of a breakout port!!!
switch(config-if)#
```



(注) FCブレイクアウトポートのデフォルトの速度は32Gです。

## 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。カプセル化を有効にすると、すべての発信フレームがカプセル化され、**show interface SD\_port\_interface** コマンドの出力には、カプセル化が EISL であることを示す新しい行が表示されます。

## 受信データ フィールド サイズの構成

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。

### SUMMARY STEPS

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

## DETAILED STEPS

## Procedure

|        | Command or Action                                    | Purpose  |
|--------|--|--|
| Step 1 | switch# <b>configuration terminal</b>                | コンフィギュレーション モードに入ります。  |
| Step 2 | switch(config)# <b>interface fc slot/port</b>        | 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。<br><br><b>Note</b><br>これが 10G ブレイクアウト ポートの場合、 <i>slot/port</i> 構文は <i>QSFP-module/port</i> になります。<br><br><b>Note</b><br>これが QSFP+ GEM またはブレイクアウト ポートの場合、 <i>port</i> 構文は <i>QSFP-module/port</i> になります。 |
| Step 3 | switch(config-if)# <b>switchport fcxbufsize 2000</b> | 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を理解する

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無効化します。

**shutdown/no shutdown** コマンドを順番に入力すると、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無効化されないようにスイッチを設定できます。



**Note** 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。

## SUMMARY STEPS

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**

## DETAILED STEPS

### Procedure

|               | Command or Action   | Purpose   |
|---------------|---|---|
| <b>Step 1</b> | switch# <b>configuration terminal</b>                     | コンフィギュレーションモードに入ります。  |
| <b>Step 2</b> | switch(config)# <b>interface fc slot/port</b>             | 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。<br><br><b>Note</b><br>これが 10G ブレイクアウトポートの場合、 <i>slot/port</i> 構文は <i>QSFP-module/port</i> になります。<br><br><b>Note</b><br>これが QSFP+GEM またはブレイクアウトポートの場合、 <i>port</i> 構文は <i>QSFP-module/port</i> になります。 |
| <b>Step 3</b> | switch(config-if)# <b>switchport ignore bit-errors</b>    | 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。   |
| <b>Step 4</b> | switch(config-if)# <b>no switchport ignore bit-errors</b> | 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。  |

## バッファ間クレジットの構成



### Caution

**switchport fcrxbbcredit** コマンドを使用してインターフェイスを設定すると、設定の変更がすぐに適用されるように、インターフェイスは自動的にフラップします。したがって、このような構成の計画は、スケジュールされたメンテナンス時間帯にのみ行い、運用環境へのそのような構成の影響を最小限に抑えることをお勧めします。

### SUMMARY STEPS

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. (Optional) switch(config-if)# **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|        | Command or Action   | Purpose  |
|--------|---|--|
| Step 1 | switch# <b>configure terminal</b>                         | 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。   |
| Step 2 | switch(config)# <b>interface fc slot/port</b>             | 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。<br><br><b>Note</b><br>これが 10G ブレイクアウト ポートの場合、 <i>slot/port</i> 構文は <i>QSFP-module/port</i> になります。<br><br><b>Note</b><br>これが QSFP+ GEM またはブレイクアウト ポートの場合、 <i>port</i> 構文は <i>QSFP-module/port</i> になります。 |
| Step 3 | switch(config-if)# <b>switchport fcrxbbcredit default</b> | 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。<br><br>デフォルト値は、ポート機能に応じて割り当てられます。  |

|        | Command or Action   | Purpose   |
|--------|---|---|
| Step 4 | switch(config-if)# <b>switchport fcrxbbcredit</b> <i>number mode</i><br>{ <b>E</b>   <b>F</b>   <b>TE</b> } | <p>選択したインターフェイスにバッファ間クレジット番号を割り当て、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。</p> <p><b>Note</b><br/>E、F、またはTEをmode用に指定すると、バッファ間クレジットの値は、ポートがその特定のモードに設定されている場合にのみ、適用されます。</p> <p>バッファ間クレジットの値の破には、1~240です。デフォルト値は16です。</p>  |
| Step 5 | switch(config-if)# <b>do show int fc</b> <i>slot/port</i>   | <p>送受信のバッファ間クレジットを、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。</p> <p><b>Note</b><br/>正しいバッファ間クレジット値は、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。</p> <p><b>Note</b><br/>これが10Gブレイクアウトポートの場合、<i>slot/port</i>構文は <i>QSFP-module/port</i> になります。</p> <p><b>Note</b><br/>これがQSFP+GEMまたはブレイクアウトポートの場合、<i>port</i> 構文は <i>QSFP-module/port</i> になります。</p> |
| Step 6 | (Optional) switch(config-if)# <b>copy running-config startup-config</b>                                     | <p>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、変更を継続的に保存します。</p>   |

## 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構成

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。

## SUMMARY STEPS

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**

## DETAILED STEPS

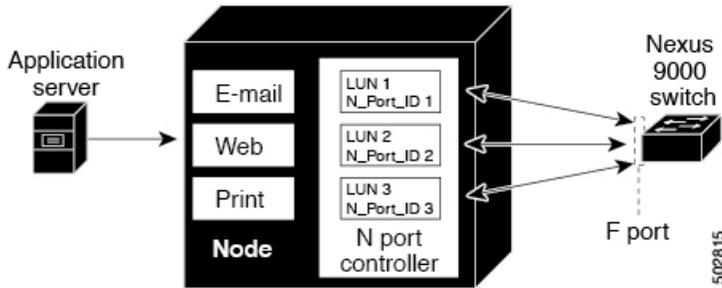
## Procedure

|        | Command or Action  | Purpose   |
|--------|--|---|
| Step 1 | switch# <b>configuration terminal</b>                            | コンフィギュレーション モードに入ります。   |
| Step 2 | switch(config)# <b>no system default switchport shutdown san</b> | <p>インターフェイス管理ステートのデフォルト設定を <b>up</b> に設定します（出荷時のデフォルト設定は <b>down</b> です）。</p> <p><b>Tip</b><br/>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。</p> |
| Step 3 | switch(config)# <b>system default switchport shutdown san</b>    | <p>インターフェイス管理ステートのデフォルト設定を <b>down</b> に設定します。これが出荷時のデフォルト設定です。</p> <p><b>Tip</b><br/>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。</p>           |
| Step 4 | switch(config)# <b>system default switchport trunk mode auto</b> | <p>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 <b>auto</b> に設定します。</p> <p><b>Note</b><br/>デフォルト設定のトランク モードは <b>on</b> です。</p>                                  |

## N ポート識別子仮想化について

N ポート識別子仮想化（NPIV）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。

Figure 7: NPIV の例



## N ポート識別子仮想化のイネーブル化

スイッチでNPIVをイネーブルまたはディセーブルにできます。**feature-set fcoe**が有効になっている場合、機能NPIVはデフォルトで有効になります。

### Before you begin

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。



**Note** すべてのNポートIDは同じVSAN内で割り当てられます。

### SUMMARY STEPS

1. **configure terminal**
2. **feature npiv**
3. **no feature npiv**

### DETAILED STEPS

#### Procedure

|               | Command or Action   | Purpose                        |
|---------------|---|--------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre> | コンフィギュレーションモードに入ります。           |
| <b>Step 2</b> | <b>feature npiv</b><br><b>Example:</b><br><pre>switch(config)# feature npiv</pre>                     | スイッチ上のすべてのVSANのNPIVをイネーブルにします。 |

|        | Command or Action  | Purpose                       |
|--------|--|-------------------------------|
| Step 3 | <b>no feature npiv</b><br><b>Example:</b><br>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。

### 例

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 san-po-channel 2
switch(config-if)# switchport mode F
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 32000
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。

Small Form-Factor Pluggable (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 に関して両方の値を表示します。

## インターフェイス情報の検証

**show interface** コマンドはインターフェイス構成を表示します。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** という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
```



**Note** 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-config** 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 configurationshow running-config
...
interface fc3/5
  switchport speed 200016000
...
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 fc3/5show running-config fc3/5
interface fc3/5
  switchport speed 200016000
  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 fc1/7
...
fc1/7 is up
Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
Port WWN is 20:07:2c:d0:2d:50:e5:24
Admin port mode is auto, trunk mode is off
snmp link state traps are enabled
Port mode is F, FCID is 0xe10280
Port vsan is 500
```

```

Operating Speed is 32 Gbps
Admin Speed is auto
Transmit B2B Credit is 12
Receive B2B Credit is 64
Receive data field Size is 2112
Beacon is turned off
fec state is enabled by default
5 minutes input rate 0 bits/sec,0 bytes/sec, 0 frames/sec
5 minutes output rate 0 bits/sec,0 bytes/sec, 0 frames/sec
16705 frames input,1225588 bytes
0 discards,0 errors
0 invalid CRC/FCS,0 unknown class
0 too long,0 too short
16714 frames output,1345676 bytes
0 discards,0 errors
0 input OLS,0 LRR,0 NOS,0 loop inits
7 output OLS,4 LRR, 0 NOS, 0 loop inits
Receive B2B Credit performance buffers is 0
12 transmit B2B credit remaining
0 low priority transmit B2B credit remaining
Interface last changed at Thu Nov 14 11:59:40 2019

```

## 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。

**Table 12:** 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                         |
| 管理状態          | 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、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。

Table 13: 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    | 該当なし                        |
| 管理状態          | Shutdown (初期設定時に変更された場合を除く) |
| トランク モード      | [オン (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    | 該当なし                        |
| データ フィールドサイズ  | n/a                         |

## ファイバチャネル インターフェイスの構成0





## 第 8 章

# VSAN の設定と管理

この章では、VSAN の設定と管理方法について説明します。

この章は、次の項で構成されています。

- [VSAN の設定と管理, on page 121](#)
- [VSAN に関する情報, on page 121](#)
- [VSAN の注意事項と制限事項, on page 124](#)
- [スタティック VSAN 設定の表示, on page 133](#)
- [VSAN のデフォルト設定, on page 134](#)

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

各 VSAN には最大 239 台のスイッチを組み込めます。それぞれの VSAN は、異なる VSAN で同じファイバチャネル ID（FC ID）を同時に使用できる独立したアドレス領域を持ちます。

## VSAN トポロジ

VSAN には次の特徴もあります。

- 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。

次の図は、各フロアに 1 つずつ、3 つのスイッチがあるファブリックを示しています。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。

Figure 8: 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る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ー 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。

Figure 9: 2 つの VSAN の例



このネットワーク内の 4 つのスイッチは、VSAN 2 と VSAN 7 の両方のトラフィックを伝送する VSAN トランクリンクによって相互接続されます。各 VSAN に異なるスイッチ間トポロジを設定できます。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 がもしまければ、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。前の図では、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
  - ユーザー 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、ユーザー 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 間でユーザーを追加、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 34 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) と `evfp isolated_vsan` (vsan 4079) です。ユーザー指定の VSAN ID 範囲は 4078 と 4080~4093 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。

Table 14: VSAN とゾーンの比較

| VSAN 特性   | ゾーン特性  |
|---|--|
| VSAN は、SAN とルーティング、ネーミング、およびゾーン分割プロトコルが同じです。                | ルーティング、ネーミング、およびゾーン分割プロトコルは、ゾーン単位で利用できません。   |
| VSAN は、ユニキャスト、マルチキャスト、およびブロードキャストトラフィックを制限します。              | ゾーンは、ユニキャストトラフィックを制限します。                     |
| メンバーシップは、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、一般的に 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ン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せん。                     |

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 とは別個のものであります。

Figure 10: VSAN とゾーン分割



## VSAN の注意事項と制限事項

VRF 設定時の注意事項と制限事項は次のとおりです。

- **VSAN ID:** VSAN ID は、デフォルト VSAN (VSAN 1)、ユーザー定義の VSAN (VSAN 2 ~ 4078 および 4080~4093)、evfp\_isolated\_vsan (VSAN 4079) および分離 VSAN (VSAN 4094) として、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 VSANID 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。



**Note** VSAN 名は一意である必要があります。

- ロードバランシング属性: これらの属性は、ロードバランシングパス選択に対する送信元/宛先 ID (src-dst-id) または Originator Exchange ID (OX ID) (デフォルトでは、src-dst-ox-id) の使用を示します。
- VSAN がアクティブの状態、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。
- Cisco Nexus 9300-FX および 9700-FX プラットフォーム スイッチでは、デフォルトの VSAN 1 を含む 32 の VSAN のみを作成できます。
- トランキング F ポート チャンネル機能を有効にするために f port-channel-trunk コマンドが実行される標準スイッチは、以下の予約済み VSAN と分離された VSAN の設定ガイドラインに従います。
  - いずれかのインターフェイスでトランク モードがオンであるか、NP ポート チャンネルが稼働している場合、予約済み VSAN は 3040～4078 であり、ユーザー設定には使用できません。
  - 分離 VSAN の 4094、および拡張仮想ファブリック プロトコル (EVFP) 分離 VSAN の 4079 は、ユーザー設定には使用できません。

## VSAN の作成について

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

## VSAN の静的な作成

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

### SUMMARY STEPS

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

### DETAILED STEPS

#### Procedure

|               | Command or Action  | Purpose   |
|---------------|--|---|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br>switch# configure terminal<br>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。                                      |
| <b>Step 2</b> | <b>vsan database</b><br><b>Example:</b><br>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。 |
| <b>Step 3</b> | <b>vsan vsan-id</b><br><b>Example:</b><br>switch(config-vsan-db)# vsan 360   | VSAN が存在しない場合は、指定された ID で VSAN を作成します。                          |
| <b>Step 4</b> | <b>vsan vsan-id name name</b><br><b>Example:</b><br>switch(config-vsan-db)# vsan 360 name test                           | 割り当てられた名前でも VSAN をアップデートします。                                    |
| <b>Step 5</b> | <b>vsan vsan-id suspend</b><br><b>Example:</b><br>switch(config-vsan-db)# vsan 470 suspend                               | 選択された VSAN を中断します。  |
| <b>Step 6</b> | <b>switch(config-vsan-db)# no vsan vsan-id suspend</b><br><b>Example:</b><br>switch(config-vsan-db)# no vsan 470 suspend | 前のステップで入力した <b>suspend</b> コマンドを無効にします。                         |
| <b>Step 7</b> | <b>switch(config-vsan-db)# end</b><br><b>Example:</b>  | EXEC モードに戻ります。  |

|  | Command or Action                        | Purpose |
|--|--|---------|
|  | <code>switch(config-vsan-db)# end</code> |         |

## ポート VSAN メンバーシップ

スイッチのポート VSAN メンバーシップは、ポート単位で割り当てられます。デフォルトでは、各ポートはデフォルト VSAN に属します。ポートに VSAN メンバーシップを静的に（ポートに VSAN を割り当てて）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。この方式は、Dynamic Port VSAN Membership (DPVM) と呼ばれます。Cisco Nexus デバイスは DPVM をサポートしていません。

VSAN トランキンング 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。

## スタティック ポート VSAN メンバーシップの概要

インターフェイス ポートの VSAN メンバーシップをスタティックに割り当てることができます。

### SUMMARY STEPS

1. **configure terminal**
2. **vsan database**
3. **vsan vsan-id**
4. **switch(config-vsan-db)# vsan vsan-id interface vfc vfc-id**
5. **vsan vsan-id interface vfc vfc-id**
6. **switch(config-vsan-db)# vsan vsan-id vfc vfc-id**
7. **vsan vsan-id vfc vfc-id}**

### DETAILED STEPS

#### Procedure

|               | Command or Action   | Purpose                    |
|---------------|---|----------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><code>switch# configure terminal</code><br><code>switch(config)#</code>       | 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。 |
| <b>Step 2</b> | <b>vsan database</b><br><b>Example:</b><br><code>switch(config)# vsan database</code><br><code>switch(config-vsan-db)#</code> | VSAN に対するデータベースを設定します。     |

|        | Command or Action  | Purpose   |
|--------|--|---|
| Step 3 | <b>vsan vsan-id</b><br><b>Example:</b><br>switch(config-vsantdb)# vsan 50                                      | VSAN が存在しない場合は、指定された ID で VSAN を作成します。  |
| Step 4 | switch(config-vsantdb)# <b>vsan vsan-id interface vfc vfc-id</b>   | 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。  |
| Step 5 | <b>vsan vsan-id interface vfc vfc-id</b><br><b>Example:</b><br>switch(config-vsantdb)# vsan 34 interface vfc 5 | 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。  |
| Step 6 | switch(config-vsantdb)# <b>vsan vsan-id vfc vfc-id</b>   | 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。<br><br><b>Note</b><br>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。 |
| Step 7 | <b>vsan vsan-id vfc vfc-id}</b><br><b>Example:</b><br>switch(config-vsantdb)# vsan 10 vfc 3                    | 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。<br><br><b>Note</b><br>vFC インターフェイスの VSAN メンバーシップを削除するには、別の VSAN にそのインターフェイスの VSAN メンバーシップを割り当てます。VSAN 1 に割り当てることを推奨します。        |

## VSAN スタティックメンバーシップの表示

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

次に、指定された VSAN のメンバーシップ情報を表示する例を示します。

```
switch # show vsan 1 membership
vsan 1 interfaces:
    vfc21    vfc22    vfc23    vfc24
    san-port-channel 3 vfc1/1
```



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

次に、すべての VSAN のメンバーシップ情報を表示する例を示します。

```
switch # show vsan membership
vsan 1 interfaces:
    vfc21   vfc22   vfc23   vfc24
    san-port-channel 3   vfc31
vsan 2 interfaces:
    vfc23 vfc41
vsan 7 interfaces:
vsan 100 interfaces:
vsan 4094(isolated vsan) interfaces:
```

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

```
switch # show vsan membership interface vfc21
vfc21
    vsan:1
    allowed list:1-4093
```

## デフォルト VSAN

Cisco SAN スイッチの出荷時の設定では、デフォルトの VSAN 1 のみが有効です。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。



**Note** VSAN 1 は削除できませんが、中断できます。

最大 34 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) と `evfp isolated_vsan` (vsan 4079) です。ユーザー指定の VSAN ID 範囲は 4078 と 4080~4093 です。

## 独立 VSAN

VSAN 4094 は独立 VSAN です。VSAN を削除すると、すべての非ランキング 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)。



**Note** 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。



**Caution** 独立 VSAN を使用してポートを設定しないでください。



**Note** 最大 34 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) と `evfp isolated_vsan` (`vsan 4079`) です。ユーザー指定の VSAN ID 範囲は 4078 と 4080~4093 です。

## 分離された VSAN メンバーシップの概要

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

## VSAN の動作ステート

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

## スタティック VSAN の削除

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

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

Figure 11: 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 サーバー)、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。



**Note** 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。

### Related Topics

[VSAN トランキングの設定](#)

## スタティック VSAN の削除

VSAN およびその各種属性を削除できます。

### SUMMARY STEPS

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

### DETAILED STEPS

#### Procedure

|               | Command or Action   | Purpose                        |
|---------------|---|--------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>             | 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。     |
| <b>Step 2</b> | <b>vsan database</b><br><b>Example:</b><br><pre>switch(config)# vsan database switch(config-vsan-db)#</pre>       | VSAN データベースを設定します。             |
| <b>Step 3</b> | <b>vsan vsan-id</b><br><b>Example:</b><br><pre>switch(config-vsan-db)# vsan 2</pre>                               | VSAN コンフィギュレーションモードを開始します。     |
| <b>Step 4</b> | <b>switch(config-vsan-db)# no vsan vsan-id</b><br><b>Example:</b><br><pre>switch(config-vsan-db)# no vsan 5</pre> | データベースおよびスイッチから VSAN 5 を削除します。 |
| <b>Step 5</b> | <b>switch(config-vsan-db)# end</b><br><b>Example:</b><br><pre>switch(config-vsan-db)# end</pre>                   | EXEC モードに戻ります。                 |

## ロードバランシングの概要

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

## ロードバランシングの設定

既存の VSAN でロードバランシングを設定できます。

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

### SUMMARY STEPS

1. **configure terminal**
2. **vsan database**
3. **vsan vsan-id**
4. **vsan vsan-id loadbalancing src-dst-id**
5. **no vsan vsan-id loadbalancing src-dst-id**
6. **vsan vsan-id loadbalancing src-dst-ox-id**
7. **vsan vsan-id suspend**
8. **no vsan vsan-id suspend**
9. **end**

### DETAILED STEPS

#### Procedure

|               | Command or Action   | Purpose                              |
|---------------|---|--------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>       | 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。           |
| <b>Step 2</b> | <b>vsan database</b><br><b>Example:</b><br><pre>switch(config)# vsan database switch(config-vsan-db)#</pre> | 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。 |
| <b>Step 3</b> | <b>vsan vsan-id</b><br><b>Example:</b><br><pre>switch(config-vsan-db)# vsan 15</pre>                        | 既存の VSAN を指定します。                     |

|        | Command or Action  | Purpose  |
|--------|--|--|
| Step 4 | <b>vsan vsan-id loadbalancing src-dst-id</b><br><b>Example:</b><br><pre>switch(config-vsan-db)# vsan 15 loadbalancing src-dst-id</pre>       | 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。 |
| Step 5 | <b>no vsan vsan-id loadbalancing src-dst-id</b><br><b>Example:</b><br><pre>switch(config-vsan-db)# no vsan 15 loadbalancing src-dst-id</pre> | 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。                         |
| Step 6 | <b>vsan vsan-id loadbalancing src-dst-ox-id</b><br><b>Example:</b><br><pre>switch(config-vsan-db)# vsan 15 loadbalancing src-dst-ox-id</pre> | 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。                           |
| Step 7 | <b>vsan vsan-id suspend</b><br><b>Example:</b><br><pre>switch(config-vsan-db)# vsan 23 suspend</pre>   | 選択された VSAN を中断します。   |
| Step 8 | <b>no vsan vsan-id suspend</b><br><b>Example:</b><br><pre>switch(config-vsan-db)# no vsan 23 suspend</pre>                                   | 前のステップで入力した <b>suspend</b> コマンドを無効にします。                                  |
| Step 9 | <b>end</b><br><b>Example:</b><br><pre>switch(config-vsan-db)# end</pre>  | EXEC モードに戻ります。   |

## interop モード

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

### Related Topics

[スイッチの相互運用性](#), on page 285

## スタティック VSAN 設定の表示

次に、特定の VSAN に関する情報を表示する例を示します。

```
switch# show vsan 100
```

次に、VSAN 使用状況を表示する例を示します。

```
switch# show vsan usage
```

```

4 vsan configured
configured vsans:1-4
vsans available for configuration:5-4093

```

次に、すべての VSAN を表示する例を示します。

```
switch# show vsan
```

## VSAN のデフォルト設定

次の表に、設定されたすべての VSAN のデフォルト設定を示します。

**Table 15:** 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   |
| 状態           | active ステート  |
| 名前           | VSAN と VSAN ID を表す 4 桁のストリングを連結したものです。たとえば、VSAN 3 は VSAN0003 です。 |
| ロード バランシング属性 | OX ID (src-dst-ox-id)  |



## 第 9 章

# SAN ポート チャンネルの設定

この章は、次の内容で構成されています。

- [SAN ポート チャンネルの設定, on page 135](#)

## SAN ポート チャンネルの設定

ストレージエリア ネットワーク (SAN) ポート チャンネルは、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 9000 スイッチでは、SAN ポート チャンネルは物理ファイバチャンネルインターフェイスを含むことができます。ただし、仮想ファイバーチャンネルインターフェイスはサポートされていません。SAN ポート チャンネルは、最大 16 のファイバチャンネルインターフェイスを含むことができます。

## SAN ポートチャンネルに関する情報

### E および TE ポートチャンネルについて

E ポートチャンネルは、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、より高度な集約帯域幅、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。ポートチャン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することができるため、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ンネルのリンクがダウンすることはありません。Cisco Nexus デバイスは FC スイッチモードで最大 4 つのポートチャンネルをサポートしています。これには E/TE ポートのポートチャンネルが含まれます。

SAN ポート チャンネルには、次の機能があります。

- ISL (スイッチ間リンク) (E ポート) または EISL (TE ポート) を介してポイントツーポイントで接続できます。複数のリンクを SAN ポート チャンネルに結合できます。
- チャン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、上位層プロトコル (ULP) 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。

Cisco Nexus デバイスは、最大 4 つの SAN ポートチャネル (ポートチャネルあたり 8 つのインターフェイス) をサポートします。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。

### 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 デバイス NPV モードで最大 4 つの SAN ポートチャネル (ポートチャネルあたり 8 つのインターフェイス) をサポートします。つまり、NPV モードでは、Cisco Nexus デバイスで最大 4 x NP のポートチャネルをサポートします。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 Nexus 9000 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透過型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 プロトコルを使用します。Cisco Nexus デバイスは F/TF ポートチャネルを含む FC スイッチモードで最大 4 つの SAN ポートチャネルをサポートします。



**Note** ファイバチャネルトラフィックに対し、すべてのリンクがポートチャネルで使用できるように、**port-channel load-balance ethernet source-dest-port** コマンドを入力して、ポートチャネルのロードバランシングを「source-dest-port」に設定します。この設定では、「source-destination-oxid」ロードバランシングがファイバチャネルトラフィックに使用されます。

## ポートチャネルと VSAN トランキングの理解

Cisco Nexus デバイスは、次のように VSAN トランキングとポートチャネルを実装します。

- 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。
- 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ます。スイッチ間リンク (ISL) と呼ばれます (下の図の左側を参照)。

- 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。

Figure 12: 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 チャンネルを作成できます。この設定では、ポート チャンネルは論理 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 チャンネルを作成できます。この設定では、ポート チャンネルは論理 EISL（複数の VSAN のトラフィックを伝送する）を実装します。

Figure 13: ポート チャンネルと VSAN トランキング



- ポート チャンネル 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。
- ポート チャンネルと トランキングは、TE ports over EISL 間で使用できます。

## ロード バランシングを理解する

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テンジで選択されたリンクが、後続のすべてのエクステンジで使用されます。
- エクステンジ ベース: エクステンジの最初のフレームがリンクに割り当てられ、エクステ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、後続のエクステンジは、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、さらに各エクステ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ています。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。

**Figure 14: 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、エクステ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ています。エクステ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。その特定のエクステンジにある残りすべてのフレームが同一のリンクに送信されます。エクステンジ 1 では、リンク 2 を使用するフレームはありません。次のエクステンジでは、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。ここではエクステンジ 2 のすべてのフレームが、リンク 2 を使用します。

**Figure 15: SID1、DID1、およびエクステ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。

次の図は、有効な SAN ポートチャネルの設定例を示しています。

**Figure 16: 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ています。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。

**Figure 17: 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。

- ポートチャネルモードはデフォルトでアクティブです。ポートチャネル **ON** モードはサポートされていません。
- 異なるポートグループのファイバチャネルポートを使用して、SAN ポートチャネルを構成します。
- 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信した場合、エラーが検出されたため、ポートチャネルの物理リンクはディセーブルになります。

- 次の要件を満たしていない場合に、SAN ポート チャンネルのエラーが検出されます。
  - SAN ポート チャン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 チャンネルを設定したあとで、SAN ポート チャンネルのリンクを変更できません。ポートチャン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ン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。
- SAN ポートチャンネルのメンバーの最大数は 16 です。
- Cisco Nexus N9K-C93180YC-FX スイッチは、実質的に暗黙の 1:1.6 オーバーサブスクリプションモデルに従います。したがって、24UP ポートのうち、すべてのポートが同時に 16-G FC ライン レートを取得できるわけではありません。
- Cisco Nexus 5672UP-16G スイッチを別の Cisco Nexus 5672UP-16G スイッチに接続する場合は、ポート グループ全体を同じポート タイプに接続します。ポート グループ内のポートは、次のいずれかのシナリオと同じタイプである必要があります。
  - 4 つの F ポートはすべて同じポート グループ内にある必要があります
  - 4 つの E ポートはすべて同じポート グループ内にある必要があります
  - 同じポート チャンネルの 4 つのポートはすべて、同じポート グループ内にある必要があります。

たとえば、Cisco Nexus 5672UP-16G スイッチのポート FC2/1 ~ 4 は、別の Cisco Nexus 5672UP-16G スイッチのポートタイプのポート 1 ~ 4、ポート 5 ~ 8、またはポート 9 ~ 12 に接続できます。

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

## F および TF ポート チャンネルの注意事項

F および TF ポート チャン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 ポートチャン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。
- ダイナミックポートVSANメンバーシップ(DPVM)を使ってポートチャネルのポートVSANを設定することはできません。
- Fポートチャネルを設定する前に、スイッチでfport-channel-trunk機能が有効になっていることを確認してください。
- いずれかのインターフェイスでトランキングが設定されているNPVスイッチ、またはトランキングFポートチャネル機能を有効にするためにfport-channel-trunkコマンドが実行される標準スイッチは、以下の予約済みVSANと分離されたVSANの設定ガイドラインに従います。
  - いずれかのインターフェイスでトランクモードがオンであるか、NPポートチャネルが稼働している場合、予約済みVSANは3040～4078であり、ユーザー設定には使用できません。
  - Exchange Virtual Fabric Protocol (EVFP) 分離VSANは4079であり、ユーザー設定には使用できません。

## 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。

### SUMMARY STEPS

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

### DETAILED STEPS

#### Procedure

|        | Command or Action  | Purpose  |
|--------|--|--|
| Step 1 | switch# <b>configure terminal</b>  | 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。   |
| Step 2 | switch(config)# <b>interface san-port-channel</b><br><i>channel-number</i> | 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。<br><br><b>Note</b><br>未使用のチャンネル番号を入力して、新しいSANポートチャネルを作成します（ファイバチャネルポート用）。使用済みと未使用のチャンネル番号の範囲を |

|  | Command or Action | Purpose  |
|--|-------------------|--|
|  |                   | 表示するには、 <b>show san-port-channel usage</b> コマンドを使用します。 |

## ポートチャンネル モードについて

チャンネルグループモードパラメータを使用して各 SAN ポート チャンネルを設定し、このチャン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ンネルプロトコルの動作を指定できます。チャン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 チャン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、ポートチャンネルプロトコルは起動されません。ただし、ポートチャン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ンネルでは、ポートチャン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、各端のポートチャン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**: ピアポートのチャン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ンネルプロトコルネゴシエーションを開始します。チャン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ン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ンネルモードでは、各端でポートチャン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。



**Note** F ポートチャン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。

**Table 16:** チャン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ン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 ポートチャン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 ポートチャン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。 |

| オン モード   | アクティブ モード  |
|--|--|
| ポート チャンネルのメンバ ポートの設定を追加または変更する場合、各端でポート チャンネルのメンバ 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。 | ポートチャンネルインターフェイスを追加または変更すると、SAN ポートチャン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、チャン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。  | ポートチャン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 チャンネルの設定

アクティブ モードを設定する手順は、次のとおりです。

### SUMMARY STEPS

1. switch# **configure 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**

### DETAILED STEPS

#### Procedure

|               | Command or Action  | Purpose   |
|---------------|--|---|
| <b>Step 1</b> | switch# <b>configure terminal</b>  | 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。  |
| <b>Step 2</b> | switch(config)# <b>interface san-port-channel</b><br><i>channel-number</i> | 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ンネルを設定します。SAN ポートチャンネル番号の範囲は、1 ~ 256 です。 |
| <b>Step 3</b> | switch(config-if)# <b>channel mode active</b>                              | アクティブ モードを設定します。  |
| <b>Step 4</b> | switch(config-if)# <b>no channel mode active</b>                           | 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。

### Related Topics

[インターフェイスの管理状態の設定](#), on page 98

## 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。

### SUMMARY STEPS

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

### DETAILED STEPS

#### Procedure

|        | Command or Action   | Purpose  |
|--------|---|--|
| Step 1 | switch# <b>configure terminal</b>   | 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。   |
| Step 2 | switch(config)# <b>no interface san-port-channel</b><br><i>channel-number</i> | 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。



**Note** 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。

Cisco Nexus N9K-C9336C-FX2-E プラットフォーム スイッチの SAN ポート チャネルにファイバ チャネル (FC) ブレイクアウト (BO) インターフェイスを追加するには、[SAN スイッチングの一般的なガイドラインと制限事項](#)を参照してください。

### 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、および許可 VSAN）
- 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。

**channel-group force** コマンドを使用して、ポートをチャネル グループへ強制的に追加できるようにした場合、パラメータは次のように処理されます。

- インターフェイスがポート チャンネルに追加されると、次のパラメータは削除され、代わってポート チャンネルに関する値が指定されます。ただしこの変更は、インターフェイスに関する実行コンフィギュレーションには反映されません。

- 帯域幅
- 遅延
- サービス ポリシー
- ACL

インターフェイスがポートチャンネルに追加またはポートチャンネルから削除されても、次のパラメータはそのまま維持されます。

- ビーコン
- 説明
- LACP ポート プライオリティ
- Debounce
- シャットダウン
- SNMP トラップ

## 中断および隔離ステート

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 チャンネルへのインターフェイスの追加

SAN ポート チャン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。

### SUMMARY STEPS

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

## DETAILED STEPS

## Procedure

|        | Command or Action  | Purpose   |
|--------|--|---|
| Step 1 | switch# <b>configure terminal</b>                              | 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。  |
| Step 2 | switch(config)# <b>interface</b> <i>type slot/port/BO port</i> | 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。<br><br><b>Note</b><br>これが 10G ブレイクアウト ポートの場合、 <i>slot/port</i> 構文は <i>QSFP-module/port</i> になります。<br><br><b>Note</b><br>これが QSFP+ GEM またはブレイクアウト ポートの場合、 <i>port</i> 構文は <i>QSFP-module/port</i> になります。 |
| Step 3 | switch(config-if)# <b>channel-group</b> <i>channel-number</i>  | ファイバチャンネルインターフェイスを指定されたチャンネルグループに追加します。チャン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する  |

## 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 チャン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 チャン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、ポートチャンネルのポートは追加から自動的に復旧します。



**Note** SAN ポート チャンネルが 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。

ファイバチャンネル (FC) インターフェイスのブレイクアウト (BO) ポートオプションは、Cisco Nexus N9K-C9336C-FX2-E プラットフォーム スイッチにのみ必要です。

メンバーの強制追加後、使用するモード (Active および On) に関係なく、片側のポートは正常にダウンします。これは、インターフェイスがダウンしてもフレームが失われないことを示します。

SAN ポート チャン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。

## SUMMARY STEPS

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

## DETAILED STEPS

## Procedure

|        | Command or Action   | Purpose   |
|--------|---|---|
| Step 1 | switch# <b>configure terminal</b>                                   | 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。  |
| Step 2 | switch(config)# <b>interface</b> <i>type slot/port /BO port</i>     | 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。<br><br><b>Note</b><br>これが 10G ブレイクアウト ポートの場合、 <i>slot/port</i> 構文は <i>QSFP-module/port</i> になります。<br><br><b>Note</b><br>これが QSFP+ GEM またはブレイクアウト ポートの場合、 <i>port</i> 構文は <i>QSFP-module/port</i> になります。 |
| Step 3 | switch(config-if)# <b>channel-group</b> <i>channel-number force</i> | 指定されたチャンネル 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 チャン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 チャンネルから削除された場合は、チャンネル 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 チャン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 チャンネルからインターフェイスを削除すると、SAN ポート チャンネルのチャンネル 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 チャン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。

### SUMMARY STEPS

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

### DETAILED STEPS

#### Procedure

|               | Command or Action  | Purpose   |
|---------------|--|---|
| <b>Step 1</b> | switch# <b>configure terminal</b>                                | 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。  |
| <b>Step 2</b> | switch(config)# <b>interface</b> <i>type slot/port/BO port</i>   | 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。<br><br><b>Note</b><br>これが 10G ブレイクアウト ポートの場合、 <i>slot/port</i> 構文は <i>QSFP-module/port</i> になります。<br><br><b>Note</b><br>これが QSFP+ GEM またはブレイクアウト ポートの場合、 <i>port</i> 構文は <i>QSFP-module/port</i> になります。 |
| <b>Step 3</b> | switch(config-if)# <b>no channel-group</b> <i>channel-number</i> | 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構成できます。チャネルグループは同じ機能と構成パラメータを持ちます。関連付けられた SAN ポート チャネル インターフェイスに適用される構成の変更は、チャネルグループ内のすべてのメンバーに伝播されます。

SAN ポート チャネルの設定を交換するプロトコルが Cisco SAN スイッチで使用できます。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。

ポートチャンネルプロトコルは、Cisco SAN スイッチのポートチャンネル機能モデルを拡張します。ポートチャンネルプロトコルは、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 ポートチャン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 ポートチャン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ンネルに属させます。

ポートチャンネルプロトコルは、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 ポートチャン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 ポートチャン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 ポートチャンネルに自動的に集約します。

## チャンネルグループの作成について

チャン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ンネルグループに自動的に設定できます。次の図に、チャン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、ポートチャンネルプロトコルは、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ンネルグループ 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 はチャンネルグループ（およびポートチャンネル）に参加できます。リンク A4-B4 はチャン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。

Figure 18: チャンネルグループの自動作成



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

チャン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ン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、ユーザー設定のチャンネルグループと自動設定のチャンネルグループの相違点を示します。

Table 17: チャンネルグループ設定の相違点

| ユーザ設定のチャンネルグループ | 自動設定のチャンネルグループ  |
|-----------------|---|
| 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ン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）。 |

| ユーザ設定のチャンネル グループ  | 自動設定のチャンネル グループ   |
|---|---|
| メンバ ポートはチャンネル 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、ユーザ設定のチャンネル グループのメンバにはなりません。   |
| チャンネル 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。 | チャンネル 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 ポートはチャンネル 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、チャンネル 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、チャンネル 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。このチャンネル グループは、必要に応じて明示的に変更できます。 |
| 任意のチャンネル グループの削除およびチャンネル グループへのメンバの追加が可能です。   | チャンネル グループは削除できません。チャンネル 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、チャンネル 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 チャンネルからすべてのメンバが削除されると、チャンネルは自動的に削除され、チャン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 チャンネルは、再起動後は存在しません。自動作成された SAN ポート チャン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 チャン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、チャン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ン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ン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。



**Tip** Cisco Nexus デバイス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 チャン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。

## 自動作成の有効化および構成

自動チャンネル グループを設定する手順は、次のとおりです。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface vfc vfc-id**
3. switch(config- if)# **channel-group auto**
4. switch(config- if)# **no channel-group auto**

### DETAILED STEPS

#### Procedure

|        | Command or Action                           | Purpose                              |
|--------|---|--------------------------------------|
| Step 1 | switch# <b>configure terminal</b>           | 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。         |
| Step 2 | switch(config)# <b>interface vfc vfc-id</b> | 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。 |

|        | Command or Action                               | Purpose   |
|--------|---|---|
| Step 3 | switch(config-if)# <b>channel-group auto</b>    | 選択したインターフェイスでチャンネル グループを自動作成します。  |
| Step 4 | switch(config-if)# <b>no channel-group auto</b> | 現在のインターフェイスのチャンネル 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、自動チャンネル グループを設定する例を示します。

```
switch(config)# interface vfc23
switch(config-if)# channel-group auto
```

## 手動設定チャンネル グループについて

ユーザによって設定されたチャンネルグループを自動作成チャン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ンネルグループから手動チャン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。チャン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ンネルグループのプロパティに従って動作します。また、チャン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。

## 手動構成チャンネル グループへの変更

自動作成されたチャンネルグループをユーザ設定チャンネルグループに変更するには、**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。

### 例

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 san-po-channel 2
switch(config-if)# switchport mode F
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 32000
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 チャネル構成の確認

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、**show san-port-channel database cli** のアスタリスク（\*）でも識別されます。

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。

### SUMMARY STEPS

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 vfc vfc/idt**

### DETAILED STEPS

#### Procedure

|        | Command or Action  | Purpose                      |
|--------|--|------------------------------|
| Step 1 | switch# <b>show san-port-channel summary   database   consistency [ details ]   usage   compatibility-parameters</b> | SAN ポート チャネルの情報を表示します。       |
| Step 2 | switch# <b>show san-port-channel database interface san-port-channel channel-number</b>                              | 指定された SAN ポート チャネルの情報を表示します。 |

|        | Command or Action  | Purpose                                    |
|--------|--|--|
| Step 3 | switch# switch# <b>show interface vfc</b> <i>vfc/idt</i> | 指定されたファイバ チャンネル 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 チャン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 チャン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 チャン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 チャンネルは、手動で作成された SAN ポート チャン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 チャンネルを表示する例を示します。

```
switch# show interface vfc21
vfc21 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
  Port-channel auto creation is enabled

Belongs to port-channel 123
...
```

## SAN ポート チャンネルのデフォルト設定

次の表に、SAN ポートチャンネルのデフォルト設定を示します。

Table 18: 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 10 章

# ファイバチャネルドメインパラメータの構成

この章では、ファイバチャネルドメインパラメータの設定方法について説明します。

この章は、次の項で構成されています。

- [ドメインパラメータに関する情報, on page 157](#)

## ドメインパラメータに関する情報

ファイバチャネルドメイン（fcdomain）機能では、FC-SW-2 標準で記述されているように、主要スイッチ選択、ドメイン ID 配信、FC ID 割り当て、ファブリック再設定機能が実行されます。ドメインは VSAN 単位で設定されます。ドメイン ID を設定しない場合、ローカルスイッチはランダムな ID を使用します。



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

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

## ファイバチャネルドメイン

fcdomain は、4つのフェーズで構成されます。

- **主要スイッチの選択:** このフェーズでは、ファブリック内で一意の主要スイッチを選択できます。
- **ドメインIDの配信:** このフェーズでは、ファブリック内のスイッチごとに、一意のドメインIDを取得できます。

- **FC ID の割り当て:** このフェーズでは、ファブリック内の対応するスイッチに接続された各デバイスに、一意の FC ID を割り当てることができます。
- **ファブリックの再設定:** このフェーズでは、ファブリック内のすべてのスイッチを再同期化して、新しい主要スイッチ選択フェーズを同時に再開できるようにします。

次の図は、`fcdomain` の構成例を示します。

Figure 19: `fcdomain` の構成例



## ドメインの再起動

ファイバチャネルドメインは、中断を伴う方法または中断を伴わない方法で起動できます。中断再起動を実行した場合は、**Reconfigure Fabric (RCF)** フレームがファブリック内のその他のスイッチに送信され、**VSAN** (リモートでセグメント化された ISL を含む) 内のすべてのスイッチでデータトラフィックは中断されます。非中断再起動を実行した場合は、**Build Fabric (BF)** フレームがファブリック内のその他のスイッチに送信され、該当スイッチでだけデータトラフィックは中断されます。

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。



**Note** 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、次の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。



**Note** 中断を伴うファブリックの再起動再設定 (RCF) は、Cisco Nexus C93180YC-FX スイッチではサポートされていません。

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 オプションはサポートされていません。

## ドメインの再起動

ファブリックの中断再起動または非中断再起動を実行できます。

## SUMMARY STEPS

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

## DETAILED STEPS

## Procedure

|        | Command or Action  | Purpose   |
|--------|--|---|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>  | 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。                            |
| Step 2 | <b>fcdomain restart vsan vsan-id</b><br><b>Example:</b><br><pre>switch (config)# fcdomain restart vsan 100</pre>                                       | トラフィックを中断しないで再設定するようにVSANを設定します。VSAN IDの範囲は、1～4093です。 |
| Step 3 | <b>switch(config)# fcdomain restart disruptive vsan vsan-id</b><br><b>Example:</b><br><pre>switch (config)# fcdomain restart disruptive vsan 101</pre> | データトラフィックを中断して再設定するようにVSANを設定します。                     |

## ドメイン マネージャの高速再起動

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

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

## ドメイン マネージャの高速再起動の有効化

ドメイン マネージャの高速再起動をイネーブルに設定できます。

## SUMMARY STEPS

1. **configure terminal**
2. **fcdomain optimize fast-restart vsan** *vsan-id*
3. **no fcdomain optimize fast-restart vsan** *vsan-id*

## DETAILED STEPS

## Procedure

|               | Command or Action  | Purpose   |
|---------------|--|---|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br>switch# configure terminal<br>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。  |
| <b>Step 2</b> | <b>fcdomain optimize fast-restart vsan</b> <i>vsan-id</i><br><b>Example:</b><br>switch(config)# fcdomain optimize fast-restart vsan<br>1       | 指定された VSAN でドメインマネージャの高速再起動をイネーブルにします。VSAN ID の範囲は、1 ~ 4093 です。         |
| <b>Step 3</b> | <b>no fcdomain optimize fast-restart vsan</b> <i>vsan-id</i><br><b>Example:</b><br>switch(config)# no fcdomain optimize fast-restart<br>vsan 1 | 指定された VSAN でドメインマネージャの高速再起動をディセーブル（デフォルト）にします。VSAN ID の範囲は、1 ~ 4093 です。 |

## スイッチの優先度

デフォルトでは、プライオリティは 128 に設定されます。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 WideName (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 の再起動の実行時に適用されます。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。

## スイッチ優先順位の構成

主要スイッチにプライオリティを設定できます。

## SUMMARY STEPS

1. **configure terminal**
2. **fcdomain priority** *number* **vsan** *vsan-id*

### 3. no fcdomain priority *number vsan vsan-id*

#### DETAILED STEPS

##### Procedure

|        | Command or Action  | Purpose  |
|--------|--|--|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                  | 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。   |
| Step 2 | <b>fcdomain priority <i>number vsan vsan-id</i></b><br><b>Example:</b><br><pre>switch(config)# fcdomain priority 12 vsan 1</pre>       | 指定された VSAN 内のローカルスイッチに指定されたプライオリティを設定します。fcdomain プライオリティの範囲は、1～254 です。VSAN ID の範囲は、1～4093 です。 |
| Step 3 | <b>no fcdomain priority <i>number vsan vsan-id</i></b><br><b>Example:</b><br><pre>switch(config)# no fcdomain priority 12 vsan 1</pre> | 指定された VSAN のプライオリティを出荷時の設定（128）に戻します。fcdomain プライオリティの範囲は、1～254 です。VSAN ID の範囲は、1～4093 です。     |

#### fcdomain の開始について

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 の無効化または再有効化

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。

#### SUMMARY STEPS

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

#### DETAILED STEPS

##### Procedure

|        | Command or Action                 | Purpose                    |
|--------|-----------------------------------|----------------------------|
| Step 1 | switch# <b>configure terminal</b> | 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。 |

|               | Command or Action   | Purpose                                |
|---------------|---|--|
| <b>Step 2</b> | <code>switch(config)# no fcdomain vsan vsan-id - vsan-id</code> | 指定された VSAN 範囲で fcdomain 設定をディセーブルにします。 |
| <b>Step 3</b> | <code>switch(config)# fcdomain vsan vsan-id</code>              | 指定された VSAN で fcdomain 設定をイネーブルにします。    |

## ファブリック名の構成

無効化された fcdomain にファブリック名の値を構成できます。

### SUMMARY STEPS

1. `configure terminal`
2. `fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan vsan-id`
3. `no fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan vsan-id`

### DETAILED STEPS

#### Procedure

|               | Command or Action   | Purpose   |
|---------------|---|---|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><code>switch# configure terminal</code><br><code>switch(config)#</code>   | 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。  |
| <b>Step 2</b> | <b>fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan vsan-id</b><br><b>Example:</b><br><code>switch(config)# fcdomain fabric-name</code><br><code>20:1:ac:16:5e:0:21:01 vsan 1</code>       | 指定された VSAN に設定済みファブリック名の値を割り当てます。VSAN ID の範囲は、1 ~ 4093 です。                                  |
| <b>Step 3</b> | <b>no fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan vsan-id</b><br><b>Example:</b><br><code>switch(config)# no fcdomain fabric-name</code><br><code>20:1:ac:16:5e:0:21:01 vsan 1</code> | VSAN 3010 のファブリック名の値を出荷時のデフォルト設定 (20:01:00:05:30:00:28:df) に変更します。VSAN ID の範囲は、1 ~ 4093 です。 |

## 着信 RCF

rcf-reject オプションはインターフェイス単位、VSAN 単位で設定できます。rcf-reject オプションはデフォルトで無効になっています (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。



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

## 着信 RCF の拒否

着信 RCF 要求フレームを拒否できます。

### SUMMARY STEPS

1. **configure terminal**
2. **interface vfc vfc-id**
3. switch(config)# **interface vfc vfc-id**
4. **fcdomain rcf-reject vsan vsan-id**
5. **no fcdomain rcf-reject vsan vsan-id**

### DETAILED STEPS

#### Procedure

|               | Command or Action  | Purpose   |
|---------------|--|---|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br>switch# configure terminal<br>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。  |
| <b>Step 2</b> | <b>interface vfc vfc-id</b><br><b>Example:</b><br>switch(config)# interface vfc 20                                 | 指定されたインターフェイスを設定します。仮想インターフェイスの ID 範囲は、1 ~ 8192 です。                               |
| <b>Step 3</b> | switch(config)# <b>interface vfc vfc-id</b>  | 指定されたインターフェイスを設定します。  |
| <b>Step 4</b> | <b>fcdomain rcf-reject vsan vsan-id</b><br><b>Example:</b><br>switch(config-if)# fcdomain rcf-reject vsan 10       | 指定された VSAN 内の指定されたインターフェイス上で RCF フィルタをイネーブルにします。VSAN ID の範囲は、1 ~ 4093 です。         |
| <b>Step 5</b> | <b>no fcdomain rcf-reject vsan vsan-id</b><br><b>Example:</b><br>switch(config-if)# no fcdomain rcf-reject vsan 10 | 指定された VSAN 内の指定されたインターフェイス上で RCF フィルタをディセーブル（デフォルト）にします。VSAN ID の範囲は、1 ~ 4093 です。 |

## マージされたファブリックの自動再構成

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

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

`autoreconfigure` オプションは実行時に即座に有効になります。 `fcdomain` を再起動する必要はありません。ドメインが重複によって現在隔離されており、後で両方のスイッチの `autoreconfigure` オプションをイネーブルにする場合は、ファブリックは隔離状態のままです。ファブリックを接続する前に両方のスイッチで `autoreconfigure` オプションをイネーブルにした場合、中断再設定 (RCF) が発生します。中断再設定が発生すると、データトラフィックが影響を受けることがあります。 `fcdomain` に非中断再設定を行うには、重複リンク上の設定済みドメインを変更し、ドメインの重複を排除します。

## 自動再構成の有効化

特定の VSAN（または VSAN 範囲）で自動再構成を有効化できます。

### SUMMARY STEPS

1. `configure terminal`
2. `fcdomain auto-reconfigure vsan vsan-id`
3. `no fcdomain auto-reconfigure vsan vsan-id`

### DETAILED STEPS

#### Procedure

|               | Command or Action   | Purpose  |
|---------------|---|--|
| <b>Step 1</b> | <code>configure terminal</code><br><b>Example:</b><br>switch# <code>configure terminal</code><br>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。   |
| <b>Step 2</b> | <code>fcdomain auto-reconfigure vsan vsan-id</code><br><b>Example:</b><br>switch(config)# <code>fcdomain auto-reconfigure vsan 1</code>       | 指定された VSAN で自動再設定オプションをイネーブルにします。VSAN ID の範囲は、1 ~ 4093 です。                 |
| <b>Step 3</b> | <code>no fcdomain auto-reconfigure vsan vsan-id</code><br><b>Example:</b><br>switch(config)# <code>no fcdomain auto-reconfigure vsan 1</code> | 指定された VSAN で自動再設定オプションをディセーブルにし、出荷時のデフォルト設定に戻します。VSAN ID の範囲は、1 ~ 4093 です。 |

## ドメイン ID

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

### ドメイン ID - 注意事項

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。



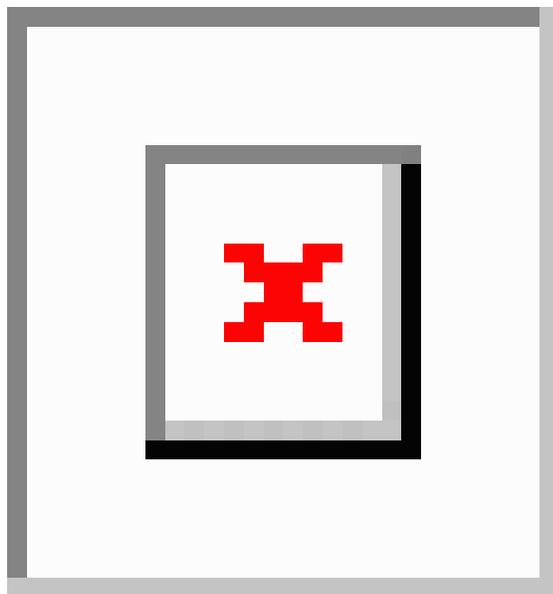
**Note** 値 0（ゼロ）を設定できるのは、優先オプションを使用した場合だけです。

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。

**Figure 20:** 優先オプションを使用した設定プロセス



下位スイッチの動作は、次の 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）。
  - 設定タイプが **preferred** の場合、ローカルスイッチは主要スイッチによって割り当てられたドメイン ID を受け入れ、割り当てられた ID が実行時ドメイン 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。



**Caution** 設定したドメインの変更をランタイム ドメインに適用する場合は、`fcdomain` コマンドを入力する必要があります。



**Note** 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。

#### Related Topics

[許可ドメイン ID リスト](#), on page 167

## スタティック ドメイン ID または優先ドメイン ID の設定

スタティック ドメイン ID または優先ドメイン ID を指定できます。

### SUMMARY STEPS

1. **configure terminal**
2. **fcdomain domain *domain-id* static vsan *vsan-id***
3. **no fcdomain domain *domain-id* static vsan *vsan-id***
4. **fcdomain domain *domain-id* preferred vsan *vsan-id***
5. **no fcdomain domain *domain-id* preferred vsan *vsan-id***

## DETAILED STEPS

## Procedure

|        | Command or Action   | Purpose   |
|--------|---|---|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>   | 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。  |
| Step 2 | <b>fcdomain domain domain-id static vsan vsan-id</b><br><b>Example:</b><br><pre>switch(config)# fcdomain domain 1 static vsan 3</pre>             | 特定の値だけを受け入れるように指定の VSAN 内のスイッチを設定し、要求されたドメイン ID が許可されない場合は、指定の VSAN 内のローカルインターフェイスを隔離ステートに移行します。ドメイン ID の範囲は 1 ~ 239 です。VSAN ID の範囲は、1 ~ 4093 です。 |
| Step 3 | <b>no fcdomain domain domain-id static vsan vsan-id</b><br><b>Example:</b><br><pre>switch(config)# no fcdomain domain 1 static vsan 3</pre>       | 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。  |
| Step 4 | <b>fcdomain domain domain-id preferred vsan vsan-id</b><br><b>Example:</b><br><pre>switch(config)# fcdomain domain 1 preferred vsan 5</pre>       | preferred ドメイン ID 3 を要求するために指定の VSAN 内のスイッチを設定し、主要スイッチによって割り当てられた値をすべて受け入れます。ドメイン ID の範囲は 1 ~ 239 です。VSAN ID の範囲は、1 ~ 4093 です。                    |
| Step 5 | <b>no fcdomain domain domain-id preferred vsan vsan-id</b><br><b>Example:</b><br><pre>switch(config)# no fcdomain domain 1 preferred vsan 5</pre> | 指定の VSAN 内の設定済みドメイン ID を 0 (デフォルト) にリセットします。設定済みドメイン ID は 0 preferred になります。  |

## 許可ドメイン ID リスト

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

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

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

## 許可ドメイン ID リストの構成

許可ドメイン ID リストを設定できます。

### SUMMARY STEPS

1. **configure terminal**
2. **fcdomain allowed** *domain-id range vsan vsan-id*
3. **no fcdomain allowed** *domain-id range vsan vsan-id*

### DETAILED STEPS

#### Procedure

|               | Command or Action  | Purpose  |
|---------------|--|--|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br>switch# configure terminal<br>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。   |
| <b>Step 2</b> | <b>fcdomain allowed</b> <i>domain-id range vsan vsan-id</i><br><b>Example:</b><br>switch(config)# fcdomain allowed 3 vsan 10       | 指定の VSAN でドメイン ID 範囲を持つスイッチを許可するようにリストを設定します。ドメイン ID の範囲は 1 ~ 239 です。VSAN ID の範囲は、1 ~ 4093 です。 |
| <b>Step 3</b> | <b>no fcdomain allowed</b> <i>domain-id range vsan vsan-id</i><br><b>Example:</b><br>switch(config)# no fcdomain allowed 3 vsan 10 | 指定の VSAN でドメイン ID 1 ~ 239 のスイッチを許可する出荷時のデフォルト設定に戻します。  |

## 許可ドメイン ID リストの CFS 配信

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

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。



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

追加情報については、ご使用のデバイスの『System Management Configuration Guide』の「Using Cisco Fabric Services」を参照してください。

## 配信のイネーブル化

許可ドメイン ID リスト設定の配信をイネーブル（またはディセーブル）に設定できます。

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

### Before you begin

CFS の前提条件は、次のとおりです。

CFS はデフォルトでイネーブルです。ファブリック内のすべてのデバイスで CFS をイネーブルに設定しないと配信は受信されません。アプリケーションに対して CFS がディセーブルになっていると、そのアプリケーションからコンフィギュレーションは配信されず、ファブリック内の他のデバイスからの配信も受け取ることができません。CFS を有効にするには、**cfs distribute** コマンドを使用します。

### SUMMARY STEPS

1. **configure terminal**
2. **fcdomain distribute**
3. **no fcdomain distribute**

### DETAILED STEPS

#### Procedure

|        | Command or Action   | Purpose                      |
|--------|---|------------------------------|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br>switch# configure terminal<br>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。   |
| Step 2 | <b>fcdomain distribute</b><br><b>Example:</b><br>switch(config)# fcdomain distribute          | ドメイン設定の配信をイネーブルにします。         |
| Step 3 | <b>no fcdomain distribute</b><br><b>Example:</b><br>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。

- 他のユーザーがこの機能の設定に変更を加えることができなくなります。

- アクティブな設定をコピーすると保留中の設定が作成されます。以降の変更は保留中の設定に行われ、アクティブな設定（およびファブリック内の他のスイッチ）への変更をコミットまたは廃棄するまでそのままです。

## 変更のコミット

保留中のドメイン設定変更をコミットして、ロックを解除できます。

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

### SUMMARY STEPS

1. **configure terminal**
2. **fcdomain commit vsan** *vsan-id*

### DETAILED STEPS

#### Procedure

|               | Command or Action   | Purpose                    |
|---------------|---|----------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>               | 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。 |
| <b>Step 2</b> | <b>fcdomain commit vsan</b> <i>vsan-id</i><br><b>Example:</b><br><pre>switch(config)# fcdomain commit vsan 45</pre> | 保留中のドメイン設定変更をコミットします。      |

## 変更の破棄

保留中のドメイン設定変更を破棄して、ロックを解放できます。

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

### SUMMARY STEPS

1. **configure terminal**
2. **fcdomain abort vsan** *vsan-id*

## DETAILED STEPS

## Procedure

|        | Command or Action  | Purpose                    |
|--------|--|----------------------------|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>      | 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。 |
| Step 2 | <b>fcdomain abort vsan vsan-id</b><br><b>Example:</b><br><pre>switch(config)# fcdomain abort vsan 30</pre> | 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

保留中の構成変更は **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せん。

```
switch# show fcdomain session-status vsan 1
Last Action Time Stamp : None
Last Action : None
Last Action Result : None
Last Action Failure Reason : none
```

## 連続ドメイン ID の割り当て

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

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

## 連続ドメイン ID 割り当ての有効化

特定の VSAN（または VSAN 範囲）で連続ドメインをイネーブルに設定できます。

### SUMMARY STEPS

1. **configure terminal**
2. **fcdomain contiguous-allocation vsan vsan-id**
3. **no fcdomain contiguous-allocation vsan vsan-id**

## DETAILED STEPS

## Procedure

|        | Command or Action   | Purpose   |
|--------|---|---|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>   | 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。  |
| Step 2 | <b>fcdomain contiguous-allocation vsan vsan-id</b><br><b>Example:</b><br><pre>switch(config)# fcdomain contiguous-allocation vsan 22-30</pre>   | 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。<br><b>Note</b><br><b>contiguous-allocation</b> 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。 |
| Step 3 | <b>no fcdomain contiguous-allocation vsan vsan-id</b><br><b>Example:</b><br><pre>switch(config)# no fcdomain contiguous-allocation vsan 7</pre> | 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、固定の FC ID 機能はイネーブルです。この機能がディセーブルの場合は、次のようになります。

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

## 永続的 FC ID

永続的 FC ID がイネーブルの場合は、次のようになります。

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



**Note** 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。



**Note** 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。

## 永続的 FC ID 機能の有効化

永続的 FC ID 機能をイネーブルに設定できます。

### SUMMARY STEPS

1. **configure terminal**
2. **fcdomain fcid persistent vsan *vsan-id***
3. **no fcdomain fcid persistent vsan *vsan-id***

### DETAILED STEPS

#### Procedure

|        | Command or Action   | Purpose                                  |
|--------|---|--|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                 | 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。               |
| Step 2 | <b>fcdomain fcid persistent vsan <i>vsan-id</i></b><br><b>Example:</b><br><pre>switch(config)# fcdomain fcid persistent vsan 78</pre> | 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。 |

|        | Command or Action   | Purpose                              |
|--------|---|--------------------------------------|
| Step 3 | <b>no fcdomain fcid persistent vsan</b> <i>vsan-id</i><br><b>Example:</b><br><pre>switch(config)# no fcdomain fcid persistent vsan 33</pre> | 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、FCID のポートフィールドが 0（ゼロ）であることを確認します。

## 永続的 FC ID の構成

永続的 FC ID を構成設定できます。

### SUMMARY STEPS

1. **configure terminal**
2. **fcdomain fcid database**
3. **vsan** *vsan-id* **wwn** *33:e8:00:05:30:00:16:df* **fcid** *fcid*
4. **vsan** *vsan-id* **wwn** *11:22:11:22:33:44:33:44* **fcid** *fcid* **dynamic**
5. **vsan** *vsan-id* **wwn** *11:22:11:22:33:44:33:44* **fcid** *fcid* **area**

### DETAILED STEPS

#### Procedure

|        | Command or Action   | Purpose                    |
|--------|---|----------------------------|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre> | 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。 |

## HBA に対する一意のエリア FC ID

|               | Command or Action   | Purpose  |
|---------------|---|--|
| <b>Step 2</b> | <b>fcdomain fcid database</b><br><b>Example:</b><br>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。  |
| <b>Step 3</b> | <b>vsan vsan-id wwn 33:e8:00:05:30:00:16:df fcid fcid</b><br><b>Example:</b><br>switch(config-fcid-db)# vsan 26 wwn<br>33:e8:00:05:30:00:16:df fcid 4                 | 指定の VSAN のデバイス WWN (33:e8:00:05:30:00:16:df) に FC ID 0x070128 を設定します。<br><b>Note</b><br>重複 FC ID の割り当てを回避するには、 <b>show fcdomain address-allocation vsan</b> コマンドを使用して、使用中の FC ID を表示します。 |
| <b>Step 4</b> | <b>vsan vsan-id wwn 11:22:11:22:33:44:33:44 fcid fcid dynamic</b><br><b>Example:</b><br>switch(config-fcid-db)# vsan 13 wwn<br>11:22:11:22:33:44:33:44 fcid 6 dynamic | ダイナミック モードで、指定の VSAN のデバイス WWN (11:22:11:22:33:44:33:44) に FC ID 0x070123 を設定します。  |
| <b>Step 5</b> | <b>vsan vsan-id wwn 11:22:11:22:33:44:33:44 fcid fcid area</b><br><b>Example:</b><br>switch(config-fcid-db)# vsan 88 wwn<br>11:22:11:22:33:44:33:44 fcid 4 area       | 指定の VSAN のデバイス WWN (11:22:11:22:33:44:33:44) に FC ID 0x070100 ~ 0x0701FF を設定します。<br><b>Note</b><br>この fcdomain のエリア全体を保護するには、FC ID の末尾 2 文字に 00 を割り当てます。                                 |

## HBA に対する一意のエリア FC ID



**Note** ここに記載された説明は、ホストバスアダプタ (HBA) ポートとストレージポートが同じスイッチに接続されている場合にのみお読みください。

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 以外の値を構成できます。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構成する必要があります。

Cisco SAN スイッチでは、FC ID の永続性機能によって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 に対する一意のエリア FC ID の設定

HBA ポートに異なるエリア ID を設定できます。

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

### Procedure

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

```
switch# show flogi database
-----
INTERFACE VSAN FCID PORT NAME NODE NAME
-----
vfc20 3 0x6f7703 50:05:08:b2:00:71:c8:c2 50:05:08:b2:00:71:c8:c0
vfc23 3 0x6f7704 50:06:0e:80:03:29:61:0f 50:06:0e:80:03:29:61:0f
```

#### Note

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。

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

```
switch# configure terminal
switch(config)# interface vfc 20
switch(config-if)# shutdown
switch(config-if)# end
```

**Step 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 3
...
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。

**Step 4** SAN スイッチで永続的 FC ID をイネーブルにします。

```
switch# configure terminal
switch(config)# fcdomain fcid persistent vsan 3
switch(config)# end
```

**Step 5** 異なるエリアアロケーションの新しい FC ID を割り当てます。この例では、77 を ee に置き換えます。

## ■ 固定的 FC ID の選択消去

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

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

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

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

```
switch# show flogi database
-----
INTERFACE VSAN  FCID      PORT NAME                               NODE NAME
-----
vfc20      3    0x6fee00    50:05:08:b2:00:71:c8:c2    50:05:08:b2:00:71:c8:c0
vfc23      3    0x6f7704    50:06:0e:80:03:29:61:0f    50:06:0e:80:03:29:61:0f
```

### Note

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

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。

**Table 19:** 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        | 利用中             | 削除されません |
| スタティック        | 使用しない           | 削除されません |
| ダイナミック        | 利用中             | 削除されません |
| ダイナミック        | 使用しない           | Deleted |

## 永続的 FC ID の消去

永続的 FC ID を消去できます。

### SUMMARY STEPS

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

### DETAILED STEPS

#### Procedure

|        | Command or Action   | Purpose                                 |
|--------|---|---|
| Step 1 | <b>purge fcdomain fcid vsan</b> <i>vsan-id</i><br><b>Example:</b><br>switch# <b>purge fcdomain fcid vsan</b> 667    | 指定の VSAN の未使用のダイナミック FC ID をすべて消去します。   |
| Step 2 | <b>purge fcdomain fcid vsan</b> <i>vsan-id</i><br><b>Example:</b><br>switch# <b>purge fcdomain fcid vsan</b> 50-100 | 指定の VSAN 範囲の未使用のダイナミック FC ID をすべて消去します。 |

## fcdomain 構成の確認



**Note** 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: 0
Number of times Local Switch was Principal: 0
Number of non disruptive reconfigurations: 0
Number of disruptive 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。

**Table 20:** デフォルト **fcdomain** パラメータ

| パラメータ       | デフォルト           |
|-------------|-----------------|
| fcdomain 機能 | [有効 (Enabled) ] |

| パラメータ                       | デフォルト                   |
|-----------------------------|-------------------------|
| 設定済みドメイン ID                 | 0 (ゼロ)                  |
| 設定済みドメイン                    | 優先 (Preferred)          |
| auto-reconfigure オプション      | ディセーブル                  |
| contiguous-allocation オプション | ディセーブル                  |
| プライオリティ                     | 128                     |
| 許可リスト                       | 1 ~ 239                 |
| ファブリック名                     | 20:01:00:05:30:00:28:df |
| rcf-reject                  | ディセーブル                  |
| 固定的 FC ID                   | [有効 (Enabled)]          |
| 許可ドメイン ID リスト設定の配信          | ディセーブル                  |





## 第 11 章

# FCoE の VLAN および仮想インターフェイスの設定

この章は、次の内容で構成されています。

- [仮想インターフェイスの概要, on page 183](#)
- [FCoE VLAN および仮想インターフェイスに関する注意事項および制約事項, on page 184](#)
- [仮想インターフェイスの設定 \(186 ページ\)](#)
- [仮想インターフェイスの確認, on page 194](#)
- [VSAN から VLAN へのマッピングの設定例 \(197 ページ\)](#)
- [FCoE over Enhanced vPC \(199 ページ\)](#)
- [vPC による SAN ブート \(203 ページ\)](#)

## 仮想インターフェイスの概要

Cisco Nexus デバイスでは、Fibre Channel over Ethernet (FCoE) がサポートされています。これにより、スイッチとサーバーの間の同じ物理イーサネット接続上でファイバチャネルおよびイーサネットトラフィックを伝送できます。

FCoE のファイバチャネル部分は、仮想ファイバチャネルインターフェイスとして設定されます。論理ファイバチャネル機能（インターフェイスモードなど）は、仮想ファイバチャネルインターフェイスで設定できます。

仮想ファイバチャネルインターフェイスは、いずれかのインターフェイスにバインドしたうえで使用する必要があります。バインド先は、コンバージドネットワークアダプタ (CNA) が Cisco Nexus デバイスに直接接続されている場合は物理イーサネットインターフェイス、CNA がレイヤ 2ブリッジにリモート接続されている場合は MAC アドレス、CNA が仮想ポートチャネル (vPC) を介してファイバチャネルフォワーダ (FCF) に接続されている場合は EtherChannel となります。

## VE ポート

仮想拡張 (VE) ポートは、FCoE ネットワークで拡張ポートとして機能します。VE ポートは、ネットワーク内の複数の FCoE スイッチを接続できます。VE ポートは、物理イーサネットポートまたはポート チャンネルにバインドできます。

Cisco Nexus 9000 シリーズ スイッチでは、VE\_Port がバインドされるポート チャンネルのメンバー間のトラフィックは、SID、DID、および OXID に基づいてロード バランシングされます。

FCoE トラフィックに対し、すべてのリンクがポートチャンネルで使用できるように、**port-channel load-balance ethernet source-dest-port** コマンドを入力して、ポートチャンネルのロードバランシングを「source-dest-port」に設定します。この設定では、「source-destination-oxid」ロードバランシングが FCoE トラフィックに使用されます。

# FCoE VLAN および仮想インターフェイスに関する注意事項および制約事項

FCoE VLAN と仮想ファイバチャンネル (vFC) インターフェイスには、以下の注意事項と制約事項があります。

- それぞれの vFC インターフェイスは、FCoE 対応イーサネットインターフェイス、EtherChannel インターフェイス、またはリモート接続されたアダプタの MAC アドレスにバインドする必要があります。FCoE は 10 ギガビット、25 ギガビット 40 ギガビット、および 100 ギガビットイーサネットインターフェイスでサポートされます。
- 仮想ファイバチャンネルインターフェイスは、いずれかのインターフェイスにバインドしたうえで使用する必要があります。バインド先は、物理イーサネットインターフェイス (コンバージドネットワーク アダプタ (CNA) が Cisco Nexus デバイスに直接接続されている場合)、MAC アドレス (CNA がレイヤ 2 ブリッジにリモート接続されている場合)、または EtherChannel です。
- vFC インターフェイスにバインドするイーサネットインターフェイスまたは EtherChannel インターフェイスを設定する際は、次の点に注意してください。
  - イーサネットまたは EthernetChannel インターフェイスは、トランクポートにする必要があります (**switchport mode trunk** コマンドを使用します)。
  - vFC の VSAN に対応する FCoE VLAN は、許可 VLAN リストに含まれている必要があります。
  - インターフェイスに MTU 9216 および QoS ポリシーを設定します。デフォルト (サービス ポリシー タイプ qos input default-fcoe-in-policy) またはカスタム QoS ポリシーを使用できます。
  - FCoE VLAN をトランクポートのネイティブ VLAN として設定しないでください。



---

**Note** トランク上のデフォルトの VLAN はネイティブ VLAN です。タグなしフレームはいずれも、ネイティブ VLAN トラフィックとしてトランクを通過します。

---

- FCoE には FCoE VLAN だけを使用する必要があります。
- デフォルト VLAN の VLAN1 を FCoE VLAN として使用しないでください。
- イーサネットインターフェイスは、PortFast として設定する必要があります (**spanning-tree port type edge trunk** コマンドを使用します)。



---

**Note** スイッチインターフェイスのトランキングが有効に設定されている場合でも、サーバインターフェイスにトランキングを設定する必要はありません。サーバから送信される FCoE 以外のトラフィックはすべて、ネイティブ VLAN 上を通過します。

---

- vFC インターフェイスは、FCoE Initialization Protocol (FIP) スヌーピングブリッジに接続された複数のメンバポートを持つイーサネットポートチャンネルにバインドできます。
- 各 vFC インターフェイスは、ただ 1 つの VSAN に対応付けられます。
- vFC インターフェイスに関連付けられた VSAN は、専用の FCoE 対応 VLAN にマッピングする必要があります。
- プライベート VLAN では、FCoE はサポートされません。
- LAN の代替パス用に (同一または別の SAN ファブリックにある) 統合アクセススイッチをイーサネットリンク経由で相互に接続する必要がある場合は、すべての FCoE VLAN をメンバーシップから除外することを、これらのリンクに対して明示的に設定する必要があります。
- SAN-A および SAN-B ファブリックの FCoE に対してはそれぞれ別々の FCoE VLAN を使用する必要があります。
- vPC を介した pre-FIP CNA への FCoE 接続はサポートされていません。
- ポートチャンネルにバインド可能な vFCs の最大数は 48 です。
- ポートチャンネルにバインド可能な vFC の最大数は 48 (Nexus 6001 の場合は 24) です。



---

**Note** 仮想インターフェイスは、管理状態がダウンに設定された状態で作成されます。仮想インターフェイスを動作させるためには、管理状態を明示的に設定する必要があります。

---

# 仮想インターフェイスの設定

## VSAN から VLAN へのマッピング

SAN 内の VSAN ごとにトラフィックを伝送できるよう、それぞれの統合アクセス スイッチには一意の専用 VLAN を設定する必要があります（VSAN 1 用に VLAN 1002、VSAN 2 用に VLAN 1003 など）。マルチ スパニング ツリーが有効に設定されている場合、FCoE VLAN には別個の MST インスタンスを使用する必要があります。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vlan vlan-id**
3. switch(config-vlan)# **fcoe [vsan vsan-id]**
4. switch(config-vlan)# **exit**
5. (Optional) switch(config)# **show vlan fcoe**
6. (Optional) switch(config-if)# **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|               | Command or Action   | Purpose   |
|---------------|---|---|
| <b>Step 1</b> | switch# <b>configure terminal</b>                                       | 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。  |
| <b>Step 2</b> | switch(config)# <b>vlan vlan-id</b>                                     | VLAN コンフィギュレーション モードを開始します。VLAN 番号の有効範囲は 1 ~ 4,096 です。  |
| <b>Step 3</b> | switch(config-vlan)# <b>fcoe [vsan vsan-id]</b>                         | 指定された VLAN で FCoE をイネーブルにします。VSAN 番号を指定しない場合は、対象の VLAN から番号が同じ VSAN へマッピングが作成されます。対象の VLAN から指定した VSAN へのマッピングを設定します。 |
| <b>Step 4</b> | switch(config-vlan)# <b>exit</b>  | VLAN コンフィギュレーション モードを終了します。Cisco Nexus デバイスで設定されたコマンドを実行するには、このモードを終了する必要があります。                                       |
| <b>Step 5</b> | (Optional) switch(config)# <b>show vlan fcoe</b>                        | VLAN の FCoE 設定に関する情報を表示します。   |
| <b>Step 6</b> | (Optional) switch(config-if)# <b>copy running-config startup-config</b> | 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、変更を継続的に保存します。   |

**Example**

次の例は、VLAN 200 を VSAN 2 にマッピングする方法を示したものです。

```
switch(config)# vlan 200
switch(config-vlan)# fcoe vsan 2
```

## 仮想ファイバチャネルインターフェイスの作成

仮想ファイバチャネルインターフェイスを作成できます。仮想ファイバチャネルインターフェイスは、いずれかの物理インターフェイスにバインドしたうえで使用する必要があります。

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config)# **interface vfc vfc-id**
3. switch(config-if)# **bind {interface {ethernet slot/port | port-channel channel-number} | mac-address MAC-address}**
4. (Optional) switch(config-if)# **no bind {interface {ethernet slot/port | port-channel channel-number} | mac-address MAC-address}**
5. (Optional) switch(config)# **no interface vfc vfc-id**

**DETAILED STEPS****Procedure**

|               | Command or Action   | Purpose   |
|---------------|---|---|
| <b>Step 1</b> | switch# <b>configure terminal</b>   | 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。  |
| <b>Step 2</b> | switch(config)# <b>interface vfc vfc-id</b>   | 仮想ファイバチャネルインターフェイスがまだ存在していない場合、それを作成し、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。<br><br>仮想ファイバチャネルインターフェイス ID の有効範囲は、1 ~ 8192 です。        |
| <b>Step 3</b> | switch(config-if)# <b>bind {interface {ethernet slot/port   port-channel channel-number}   mac-address MAC-address}</b>               | 指定されたインターフェイスに仮想ファイバチャネルインターフェイスをバインドします。<br><br><b>Note</b><br>これが 10G ブレイクアウトポートの場合、slot/port 構文は QSFP-module/port になります。 |
| <b>Step 4</b> | (Optional) switch(config-if)# <b>no bind {interface {ethernet slot/port   port-channel channel-number}   mac-address MAC-address}</b> | 指定されたインターフェイスに対する仮想ファイバチャネルインターフェイスのバインドを解除します。   |

|               | Command or Action   | Purpose  |
|---------------|---|--|
|               |   | <b>Note</b><br>これが 10G ブレイクアウト ポートの場合、 <i>slot/port</i> 構文は <i>QSFP-module/port</i> になります。 |
| <b>Step 5</b> | (Optional) switch(config)# <b>no interface vfc vfc-id</b> | 仮想ファイバチャネルインターフェイスを削除します。  |

### Example

次の例は、イーサネットインターフェイスに仮想ファイバチャネルインターフェイスをバインドする方法を示したものです。

```
switch# configure terminal
switch(config)# interface vfc 4
switch(config-if)# bind interface ethernet 1/4
```

次の例は、Cisco Nexus 2232PP ファブリック エクステンダ (FEX) イーサネットインターフェイスに仮想ファイバチャネルインターフェイスをバインドする方法を示したものです。

```
switch# configure terminal
switch(config)# interface vfc 1001
switch(config-if)# bind interface ethernet 100/1/1
```

次の例は、ポートチャネルに仮想ファイバチャネルインターフェイスをバインドする方法を示したものです。

```
switch# configure terminal
switch(config)# interface vfc 3
switch(config-if)# bind interface port-channel 1
```

次の例は、Nexus デバイス 2232PP FEX 上の仮想ファイバチャネルインターフェイスをバインドして vPC を作成する方法を示したものです。

```
switch# configure terminal
switch(config)# interface vfc 1001
switch(config-if)# bind interface ethernet 100/1/1
```



**Note** FCoE をサポートしていない Cisco Nexus FEX にインターフェイスをバインドしようとすると、エラーメッセージが表示されます。

次の例は、MAC アドレスに仮想ファイバチャネルインターフェイスをバインドする方法を示したものです。

```
switch# configure terminal
switch(config)# interface vfc 2
switch(config-if)# bind mac-address 00:0a:00:00:00:36
```

次の例は、Cisco Nexus 2232PP FEX の MAC アドレスに仮想ファイバチャネル インターフェイスをバインドする方法を示したものです。

```
switch# configure terminal
switch(config)# interface vfc 1001
switch(config-if)# bind mac-address 00:01:0b:00:00:02
```

次の例は、仮想ファイバチャネル インターフェイスを削除する方法を示したものです。

```
switch# configure terminal
switch(config)# no interface vfc 4
```

次の例は、イーサネット インターフェイスから仮想ファイバチャネル インターフェイスをバインド解除する方法を示したものです。

```
switch# configure terminal
switch(config)# int vfc17
switch(config-if)# no bind interface ethernet 1/17
switch(config-if)# exit
```

## vFC インターフェイスの構成

次の手順は、マルチメンバー ポート チャネルのメンバー ポートへの vPC インターフェイスを設定する方法を示しています。



(注) 4 ポート vPC の設定を解除できるのは、ポートチャネルからメンバー ポートを削除した後だけです。単一のメンバー ポート チャネルでのみ設定を解除できます。

### 手順の概要

1. マルチメンバー ポート チャネルを作成します。
2. 個々のメンバー ポートをマルチメンバー ポート チャネルに追加します。
3. マルチメンバー ポート チャネルのメンバー ポートに vPC を関連付けます。

### 手順の詳細

#### 手順

##### Step 1

マルチメンバー ポート チャネルを作成します。

```
switch(config-vlan)# interface port-channel 500
switch(config-vlan)# [no]fcoe multi-vfc
```

##### Step 2

個々のメンバー ポートをマルチメンバー ポート チャネルに追加します。

```
switch(config-vlan)# interface ethernet 100/1/1
switch(config-vlan)# channel-group 500
```

## 仮想ファイバチャネルインターフェイスと VSAN との関連付け

```
switch (config)# interface ethernet 100/1/2
switch(config-if)# channel-group 500
```

**Step 3** マルチメンバー ポート チャネルのメンバー ポートに vPC を関連付けます。

```
switch(config)# interface vfc 10011
switch(config-vlan)# bind interface ethernet 100/1/1
switch(config-vlan)# interface vfc 10012
switch (config)# bind interface ethernet 100/1/2
```

## 仮想ファイバチャネルインターフェイスと VSAN との関連付け

SAN 内の仮想ファブリック (VSAN) ごとにトラフィックを伝送できるよう、それぞれの統合アクセス スイッチには一意の専用 VLAN を設定する必要があります (VSAN 1 用に VLAN 1002、VSAN 2 用に VLAN 1003 など)。MST が有効に設定されている場合、FCoE VLAN には別個の MST インスタンスを使用する必要があります。

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **vsan database**
3. switch(config-vsan)# **vsan vsan-id interface vfc vfc-id**
4. (任意) switch(config-vsan)# **no vsan vsan-id interface vfc vfc-id**

## 手順の詳細

## 手順

|               | コマンドまたはアクション  | 目的   |
|---------------|---|--|
| <b>Step 1</b> | switch# <b>configure terminal</b>                                     | 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。   |
| <b>Step 2</b> | switch(config)# <b>vsan database</b>                                  | VSAN コンフィギュレーションモードを開始します。   |
| <b>Step 3</b> | switch(config-vsan)# <b>vsan vsan-id interface vfc vfc-id</b>         | VSAN と仮想ファイバチャネルインターフェイスの関連付けを設定します。<br><br>VSAN 番号は、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物理イーサネットインターフェイスの上の VLAN にマッピングする必要があります。 |
| <b>Step 4</b> | (任意) switch(config-vsan)# <b>no vsan vsan-id interface vfc vfc-id</b> | VSAN と仮想ファイバチャネルインターフェイスの関連付けを解除します。   |

### 例

次の例は、仮想ファイバチャネルインターフェイスを VSAN に関連付ける方法を示したものです。

```
switch# configure terminal
switch(config)# vsan database
switch(config-vsan)# vsan 2 interface vfc 4
```

## 暗黙的仮想ファイバチャネルポートチャネルインターフェイスの作成

仮想ファイバチャネル (vFC) を構築し、1つのコマンドを使用してそれをイーサネットインターフェイスまたはポートチャネルに暗黙的にバインドすることができます。このためには、vFC 識別子がイーサネットインターフェイスまたはポートチャネル識別子とマッチする必要があります。イーサネットインターフェイスは、モジュール (スロットまたはポート) インターフェイス (スロット/QSFP-モジュール/ポート) にすることができます。



**Note** ブレイクアウトポートに暗黙的な vFC を構築することはできません。

### 仮想ファイバチャネルインターフェイスの設定

#### Before you begin

- FCoE の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。
- FCoE がイネーブルになっていることを確認します。

### Procedure

**Step 1** 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。

```
switch# configure terminal
```

**Step 2** vFC を構築します (まだ存在しない場合)。

さらに、*vfc slot/port* は、vFC をイーサネット スロット/ポート インターフェイスにバインドします。vFC スロット/QSFP モジュール/ポートは、vFC をブレイクアウト インターフェイスにバインドします。

```
switch(config) # interface vfc {id | slot/port | slot/QSFP-module/port }
```

**Step 3** vFC インターフェイスを起動します。

```
switch(config-if) # no shutdown
```

**Step 4** Required: インターフェイス コンフィギュレーション モードを終了します。

```
switch(config-if) # exit
```

### 仮想ファイバチャネル インターフェイスの設定

次の例は、イーサネット インターフェイスに仮想ファイバチャネル インターフェイスを暗黙的にバインドする方法を示したものです。

```
switch# configure terminal
switch(config)# interface eth1/11
switch(config-if)# switchport mode trunk
switch(config-if)# mtu 9216
switch(config-if)# service-policy type qos input default-fcoe-in-policy
switch(config-if)# no shutdown

switch(config)# interface vfcl/11
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)#

switch(config)# vsan database
switch(config-vsan-db)# vsan 10
switch(config-vsan-db)# exit
switch(config)#

switch(config)# vlan 10
switch(config-vlan)# fcoe vsan 10
switch(config-vlan)# exit
switch(config)#

switch(config)# vsan database
switch(config-vsan-db)# vsan 10 interface vfcl/11
switch(config-vsan-db)# exit
switch(config)#
switch(config)# show interface vfcl/11
vfcl/11 is trunking (Not all VSANs UP on the trunk)
Bound interface is Ethernet1/11
Hardware is Ethernet
Port WWN is 20:0b:00:de:fb:9d:0e:a0
Admin port mode is F, trunk mode is on
snmp link state traps are enabled
Port mode is TF
Port vsan is 10
Operating Speed is 10 Gbps
Admin Speed is auto
Trunk vsans (admin allowed and active) (1,10)
Trunk vsans (up) (10)
Trunk vsans (isolated) ()
Trunk vsans (initializing) (1)
11 fcoe in packets
1692 fcoe in octets
0 fcoe out packets
0 fcoe out octets
Interface last changed at Mon Dec 16 09:03:33 2019

switch(config)#
```

## 仮想ファイバチャネルの設定: ポート チャネル インターフェイス

### Procedure

- 
- Step 1** 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。  
switch# **configure terminal**
- Step 2** 番号に基づいてイーサネット ポート チャネルに暗黙的にバインドする vFC を構築します。  
ポート番号の範囲は 1 ~ 4096 です。  
switch(config) # **interface vfc-port-channel** *port number*
- Step 3** vFC ポートを起動します。  
switch(config-if) # **no shutdown**
- Step 4** Required: 現在のインターフェイス コンフィギュレーション モードを終了します。  
switch(config-if) # **exit**
- 

### 仮想ファイバチャネルの設定: ポート チャネル インターフェイス

この例は、イーサネット ポート チャネルに暗黙的にバインドする vFC ポート チャネルを構築する方法を示しています。

```
switch# configure terminal
switch(config)# interface port-channel 10
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# mtu 9216
switch(config-if)# service-policy type qos input default-fcoe-in-policy
switch(config-if)# no shutdown
switch(config-if)# exit

switch(config)# interface eth1/49
switch(config-if)# channel-group 10 force
switch(config-if)# no shutdown
switch(config-if)# exit

switch# configure terminal
switch(config)# interface vfc-port-channel 10
switch(config-if)# no shutdown
switch(config-if)# exit

switch(config)# vlan 10
switch(config-vlan)# fcoe vsan 10
switch(config-vlan)# exit
switch(config)#

switch(config)# vsan database
switch(config-vsan-db)# vsan 10 interface vfc-port-channel 10
switch(config-vsan-db)# exit
```

```

switch(config)# show interface vfc-port-channel 10
vfc-po10 is trunking (Not all VSANs UP on the trunk)
Bound interface is port-channel10
Hardware is Ethernet
Port WWN is 25:1b:00:de:fb:9d:0e:a0
Admin port mode is F, trunk mode is on
snmp link state traps are enabled
Port mode is TF
Port vsan is 10
Operating Speed is 40 Gbps
Admin Speed is auto
Trunk vsans (admin allowed and active) (1,10)
Trunk vsans (up) (10)
Trunk vsans (isolated) ()
Trunk vsans (initializing) (1)
11 fcoe in packets
1236 fcoe in octets
0 fcoe out packets
0 fcoe out octets
Interface last changed at Mon Dec 16 08:56:13 2019

```

## 仮想インターフェイスの確認

仮想インターフェイスに関する設定情報を表示するには、次の作業のいずれかを行います。

| コマンド                                     | 目的                                 |
|--|------------------------------------|
| switch# <b>show interface vfc vfc-id</b> | 指定されたファイバチャネルインターフェイスの詳細な設定を表示します。 |
| switch# <b>show interface brief</b>      | すべてのインターフェイスのステータスが表示されます。         |
| switch# <b>show vlan fcoe</b>            | FCoE VLAN から VSAN へのマッピングを表示します。   |

次の例は、イーサネットインターフェイスにバインドされた仮想ファイバチャネルインターフェイスを表示する方法を示したものです。

```

switch# show interface vfc 11

vfc11 is trunking (Not all VSANs UP on the trunk)

Bound interface is Ethernet1/11
Hardware is Ethernet
Port WWN is 20:0a:00:de:fb:9d:0e:df
Admin port mode is F, trunk mode is on
snmp link state traps are enabled
Port mode is TF
Port vsan is 10
Operating Speed is 10 Gbps
Admin Speed is auto
Trunk vsans (admin allowed and active) (1,10)
Trunk vsans (up) (10)
Trunk vsans (isolated) ()
Trunk vsans (initializing) (1)
2 fcoe in packets
152 fcoe in octets

```

```

0 fcoe out packets
0 fcoe out octets
Interface last changed at Wed Dec 18 10:36:58 2019

```

次の例は、MAC アドレスにバインドされた仮想ファイバ チャンネル インターフェイスを表示する方法を示したものです。

```

switch# show interface vfc 11

vfc11 is trunking (Not all VSANs UP on the trunk)
Bound MAC is 0090.faf8.7513
Hardware is Ethernet
Port WWN is 20:0a:00:de:fb:9d:0e:df
Admin port mode is F, trunk mode is on
snmp link state traps are enabled
Port mode is TF
Port vsan is 10
Operating Speed is 10 Gbps
Admin Speed is auto
Trunk vsans (admin allowed and active) (1,10)
Trunk vsans (up) (10)
Trunk vsans (isolated) ()
Trunk vsans (initializing) (1)
3 fcoe in packets
228 fcoe in octets
0 fcoe out packets
0 fcoe out octets
Interface last changed at Mon Dec 16 09:09:02 2019

```

次の例は、スイッチ上のすべてのインターフェイスのステータスを表示する方法を示したものです（簡略化のため、出力の一部は省略）。

```

switch# show interface brief

-----
Port VRF Status IP Address Speed MTU
-----
mgmt0 -- up 9.9.9.9 1000 1500
-----

Ethernet VLAN Type Mode Status Reason Speed Port
Interface Ch #
-----
Eth1/1 1 eth trunk up none 100G(D) 1
Eth1/2 1 eth trunk up none 100G(D) 1
Eth1/3 -- eth routed down Administratively down auto(D) --
Eth1/4 -- eth routed down XCVR not inserted auto(D) --
Eth1/5 -- eth routed down Administratively down auto(D) --
Eth1/6 -- eth routed down Administratively down auto(D) --
Eth1/7 1 eth trunk up none 40G(D) 601
Eth1/8 -- eth routed down XCVR not inserted auto(D) --
Eth1/14 -- eth routed down XCVR not inserted auto(D) --
Eth1/16 -- eth routed down XCVR not inserted auto(D) --
Eth1/17 -- eth routed down XCVR not inserted auto(D) --
Eth1/18/1 1 eth trunk up none 10G(D) 181
Eth1/18/2 1 eth trunk up none 10G(D) 560
Eth1/18/3 1 eth trunk up none 10G(D) 560
Eth1/18/4 1 eth trunk up none 10G(D) 560
Eth1/19 -- eth routed down Administratively down auto(D) --
Eth1/20 -- eth routed down Administratively down auto(D) --
Eth1/21 -- eth routed down XCVR not inserted auto(D) --
Eth1/22 -- eth routed down XCVR not inserted auto(D) --
Eth1/23 -- eth routed down XCVR not inserted auto(D) --
Eth1/24 -- eth routed down XCVR not inserted auto(D) --

```

```

Eth1/25 1 eth trunk up none 100G(D) 2500
Eth1/26 1 eth trunk up none 40G(D) 26
Eth1/27 -- eth routed down XCVR not inserted auto(D) --
Eth1/28 -- eth routed down XCVR not inserted auto(D) --
Eth1/29 -- eth routed down XCVR not inserted auto(D) --
Eth1/31 1 eth trunk up none 40G(D) 559
Eth1/32 -- eth routed down XCVR not inserted auto(D) --
Eth1/33 -- eth routed down XCVR not inserted auto(D) --
Eth1/34 -- eth routed down XCVR not inserted auto(D) --
Eth1/35 -- eth routed down Administratively down auto(D) --
Eth1/36/1 -- eth routed down Administratively down auto(D) --
Eth1/36/2 -- eth routed down Administratively down auto(D) --
Eth1/36/3 -- eth routed down Administratively down auto(D) --
Eth1/36/4 -- eth routed down Administratively down auto(D) --

```

```

-----
Port-channel VLAN Type Mode Status Reason Speed Protocol
Interface
-----

```

```

Po1 1 eth trunk up none a-100G(D) lacp
Po26 1 eth trunk up none a-40G(D) none
Po181 1 eth trunk up none a-10G(D) none
Po559 1 eth trunk up none a-40G(D) none
Po560 1 eth trunk up none a-10G(D) none
Po601 1 eth trunk up none a-40G(D) none
Po2500 1 eth trunk up none a-100G(D) none

```

```

-----
Interface Vsan Admin Admin Status SFP Oper Oper Port
Mode Trunk Mode Speed Channel
Mode (Gbps)
-----

```

```

fc1/9/1 1 E on trunking swl TE 8 224
fc1/9/2 1 E on trunking swl TE 8 224
fc1/9/3 1 E on trunking swl TE 8 224
fc1/9/4 1 E on trunking swl TE 8 224
fc1/10/1 1 E on trunking swl TE 8 224
fc1/10/2 1 E on trunking swl TE 8 224
fc1/10/3 1 E on trunking swl TE 8 224
fc1/10/4 1 E on trunking swl TE 8 224
fc1/11/1 1 E on trunking swl TE 8 224
fc1/11/2 1 E on trunking swl TE 8 224
fc1/11/3 1 E on trunking swl TE 8 224
fc1/11/4 1 E on trunking swl TE 8 224
fc1/12/1 1 auto on down swl -- -- --
fc1/12/2 1 auto on down swl -- -- --
fc1/12/3 1 auto on down swl -- -- --
fc1/12/4 1 auto on down swl -- -- --
fc1/13/1 1 E on trunking swl TE 8 225
fc1/13/2 1 E on trunking swl TE 8 225
fc1/13/3 1 E on trunking swl TE 8 225
fc1/13/4 1 E on trunking swl TE 8 225
fc1/15/1 501 auto off up swl F 32 --
fc1/15/2 501 F on trunking swl TF 32 114
fc1/15/3 501 F off up swl F 32 --
fc1/15/4 1 F on trunking swl TF 32 118
fc1/30/1 1 E off notConnected swl -- -- --
fc1/30/2 1 E off notConnected swl -- -- --
fc1/30/3 1 E on trunking swl TE 32 --
fc1/30/4 1 E on notConnected swl -- -- --

```

```

-----
Interface Vsan Admin Status Oper Oper IP
Trunk Mode Speed Address
-----

```

```

Mode (Gbps)
-----
san-port-channel114 501 on trunking TF 32 --
san-port-channel118 1 on trunking TF 32 --
san-port-channel224 1 on trunking TE 88 --
san-port-channel225 1 on trunking TE 32 --

-----

Interface Vsan Admin Admin Status Bind Oper Oper
Mode Trunk Info Mode Speed
Mode (Gbps)
-----

vfc1 501 F on trunking Ethernet1/26 TF 40
vfc2 501 F on trunking e02f.6d08.cda9 TF auto
vfc560 1 F on trunking port-channel560 TF 30
vfc1/25 501 F on trunking Ethernet1/25 TF 100

-----

Interface Vsan Admin Admin Status Bind Oper Oper
Mode Trunk Info Mode Speed
Mode (Gbps)
-----

vfc-po559 1 F on trunking port-channel559 TF 40
vfc-po601 501 F on trunking port-channel601 TF 40

```

次の例は、スイッチにおける VLAN と VSAN とのマッピングを表示する方法を示したものです。

```

switch# show vlan fcoe

```

| VLAN | VSAN | Status          |
|------|------|-----------------|
| 15   | 15   | Operational     |
| 20   | 20   | Operational     |
| 25   | 25   | Operational     |
| 30   | 30   | Non-operational |

## VSAN から VLAN へのマッピングの設定例

次に示すのは、FCoE VLAN および仮想ファイバチャネルインターフェイスの設定例です。

### 手順の概要

1. 関連する VLAN を有効にし、その VLAN を VSAN へマッピングします。
2. 物理イーサネットインターフェイス上で VLAN を設定します。
3. 仮想ファイバチャネルインターフェイスを作成し、それを物理イーサネットインターフェイスにバインドします。
4. 仮想ファイバチャネルインターフェイスを VSAN に関連付けます。
5. (任意) VSAN のメンバーシップ情報を表示します。
6. (任意) 仮想ファイバチャネルインターフェイスに関するインターフェイス情報を表示します。

## 手順の詳細

## 手順

**Step 1** 関連する VLAN を有効にし、その VLAN を VSAN へマッピングします。

```
switch(config)# vlan 200
switch(config-vlan)# fcoe vsan 2
switch(config-vlan)# exit
```

**Step 2** 物理イーサネット インターフェイス上で VLAN を設定します。

```
switch(config)# interface eth1/11
switch(config)# spanning-tree port type edge trunk
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1,200
switch(config-if)# mtu 9216
switch(config-if)# service-policy type qos input default-fcoe-in-policy
switch(config-if)# exit
```

**Step 3** 仮想ファイバ チャンネル インターフェイスを作成し、それを物理イーサネット インターフェイスにバインドします。

```
switch(config)# interface vfc 11
switch(config-if)# bind interface ethernet 1/4
switch(config-if)# no shutdown
switch(config-if)# exit
```

(注)

デフォルトでは、仮想ファイバ チャンネル インターフェイスはすべて VSAN 1 上に存在します。VLAN から VSAN へのマッピングを VSAN 1 以外の VSAN に対して行う場合は、ステップ 4 へ進みます。

**Step 4** 仮想ファイバ チャンネル インターフェイスを VSAN に関連付けます。

```
switch(config)# vsan database
switch(config-vsan-db)# vsan 2
switch(config-vsan-db)# vsan 2 interface vfc 11
switch(config-vsan)# exit
```

**Step 5** (任意) VSAN のメンバーシップ情報を表示します。

```
switch# show vsan 2 membership
vsan 2 interfaces
    vfc 11
```

**Step 6** (任意) 仮想ファイバチャネル インターフェイスに関するインターフェイス情報を表示します。

```
switch# show interface vfc 11

vfc11 is trunking (Not all VSANs UP on the trunk)
Bound interface is Ethernet1/11
Hardware is Ethernet
Port WWN is 20:0a:00:de:fb:9d:0e:df
Admin port mode is F, trunk mode is on
snmp link state traps are enabled
Port mode is TF
Port vsan is 2
Operating Speed is 10 Gbps
Admin Speed is auto
Trunk vsans (admin allowed and active) (1-2,10)
Trunk vsans (up) (2)
Trunk vsans (isolated) ()
Trunk vsans (initializing) (1,10)
2 fcoe in packets
152 fcoe in octets
0 fcoe out packets
0 fcoe out octets
Interface last changed at Mon Dec 16 09:22:25 2019
```

## FCoE over Enhanced vPC

イーサネットトラフィックは、Enhanced vPC トポロジでは FEX とスイッチ ペア間でデュアルホーム接続されますが、FCoE トラフィックは、SAN 分離を維持するためにシングルホーム接続される必要があります。したがって、Enhanced vPC が FCoE をサポートする一方で、SAN 分離と高 FCoE 帯域幅が必要な場合は、シングルホーム接続の FEX トポロジの方が望ましいこともあります。

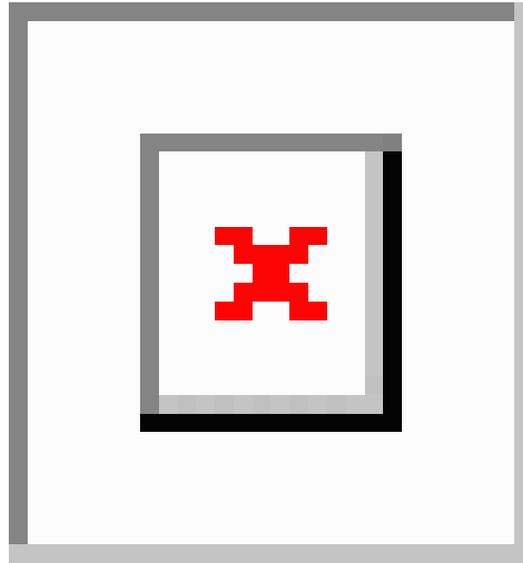
シングルホーム接続のトポロジに対する、Enhanced vPC のデメリットを考慮してください。

- 一般的な SAN ネットワークには、SAN A と SAN B という 2 つのファブリックがあり、その間のトラフィックは分離されています。Enhanced vPC トポロジでは、各スイッチは FEX によってペア化されており（シングルホーム）、1 つの FEX からの FCoE トラフィックが 1 つのスイッチにしか送信されないようになっています。一方、イーサネットトラフィックは、各 FEX と両方のスイッチ間でデュアルホーム接続されます。FEX からの FCoE トラフィックは 1 つのスイッチにしか送受信されず、イーサネットトラフィックは両方に送受信されるため、FEX アップリンクのトラフィック負荷は均等化されません。
- 8 つのアップリンクポートを持つ FEX では、イーサネットトラフィックは 8 ポートをすべて使用しますが、シングルホーム接続の FCoE トラフィックは、このトポロジでは 4 つのポートしか使用しないよう制限されているため、FCoE で使用可能な最大帯域幅も制限されます。さらに、共有リンクのデフォルトの QoS テンプレートは、FCoE トラフィックに対してリンク帯域幅の半分しか割り当てず、残りの半分はイーサネットトラフィックに割り当てられるという制限もあります。

- FEX を使用する Enhanced vPC トポロジでは、ホスト vPC は 2 ポートに制限されており、FEX あたり 1 ポートずつ使用します。

次の図は、それぞれ異なる Cisco Nexus デバイスに関連付けられた、2 つの Cisco Nexus 2000 FEX を使用するシステムの FCoE トラフィック フローを示します。

図 21: FCoE over Enhanced vPC



## FCoE over Enhanced vPC の設定

SAN 分離を維持するため、FCoE トラフィックはシングルホーム接続される必要があります。まず、FEX を 1 つのスイッチと関連付けます。FEX とスイッチが関連付けられると、仮想ファイバチャネル (vFC) インターフェイスを作成し、ポートにバインドします。

最初のピアで FEX とスイッチをペアリングすると、SAN トラフィックを分離できるよう別のポート番号を使用して 2 番目のピアでも同じ設定を繰り返します。設定が異なっても、整合性エラーが発生することはありません。これは、Enhanced vPC 設定の FCoE の部分は、vPC 整合性チェックの対象となっていないためです。

### 始める前に

FCoE over Enhanced vPC (199 ページ) の制限事項を確認してください。

### 手順の概要

1. switch# **configure terminal**
2. switch(config) # **fex fex-chassis\_ID**
3. switch(config-fex) # **fcoe**
4. switch(config-fex) # **interface vfc vfc-id**
5. switch(config-if) # **bind interface ethernet [fex-chassis-ID]/slot/port**
6. switch(config-if) # **no shutdown**

7. (任意) switch(config-if) # end
8. (任意) switch(config)# copy running-config startup-config

## 手順の詳細

## 手順

|               | コマンドまたはアクション  | 目的   |
|---------------|---|--|
| <b>Step 1</b> | switch# <b>configure terminal</b>   | 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。   |
| <b>Step 2</b> | switch(config) # <b>fex fex-chassis_ID</b>                                    | 指定された FEX のコンフィギュレーションモードを開始します。<br><br><i>fex-chassis_ID</i> の範囲は 100 ~ 199 です。   |
| <b>Step 3</b> | switch(config-fex) # <b>fcoe</b>  | このスイッチにのみ FCoE トラフィックを送信するよう、FEX を設定します。   |
| <b>Step 4</b> | switch(config-fex) # <b>interface vfc vfc-id</b>                              | 仮想ファイバチャネルインタフェースのコンフィギュレーションモードを開始します。インタフェースが存在しない場合は、このコマンドにより、インタフェースが作成されます。<br><br><i>vfc-id</i> の範囲は、1 ~ 8192 です。   |
| <b>Step 5</b> | switch(config-if) # <b>bind interface ethernet [fex-chassis-ID]/slot/port</b> | vFC インタフェースを指定された物理イーサネットインタフェースにバインドします。<br><br><i>fex-chassis_ID</i> の範囲は 100 ~ 199 です。 <i>slot</i> は 1 にする必要があります。FCoE では、 <i>port</i> の範囲は 1 ~ 32 です。<br><br>(注)<br>これが 10G ブレイクアウトポートの場合、 <i>slot/port</i> 構文は <i>QSFP-module/port</i> になります。 |
| <b>Step 6</b> | switch(config-if) # <b>no shutdown</b>  | インタフェースを、デフォルトの操作状態に戻します。  |
| <b>Step 7</b> | (任意) switch(config-if) # <b>end</b>   | 特権 EXEC モードに戻ります。  |
| <b>Step 8</b> | (任意) switch(config)# <b>copy running-config startup-config</b>                | 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、変更を継続的に保存します。   |

## 例

この例では、各FEXをFCoEトラフィックのスイッチにペアリングする方法を示します。

```
nexus5000-sanA# configure terminal
nexus5000-sanA(config) # fex 101
nexus5000-sanA(config-fex) # fcoe
nexus5000-sanA(config-fex) # interface vfc 1
nexus5000-sanA(config-if) # bind interface ethernet 101/1/1
nexus5000-sanA(config-if) # no shutdown
nexus5000-sanA(config-if) # end
nexus5000-sanA# copy running-config startup-config
nexus5000-sanA#
```

```
nexus5000-sanB# configure terminal
nexus5000-sanB(config) # fex 102
nexus5000-sanB(config-fex) # fcoe
nexus5000-sanB(config-fex) # interface vfc 1
nexus5000-sanB(config-if) # bind interface ethernet 102/1/1
nexus5000-sanB(config-if) # no shutdown
nexus5000-sanB(config-if) # end
nexus5000-sanB# copy running-config startup-config
nexus5000-sanB#
```

```
nexus5500-sanA# configure terminal
nexus5500-sanA(config) # fex 101
nexus5500-sanA(config-fex) # fcoe
nexus5500-sanA(config-fex) # interface vfc 1
nexus5500-sanA(config-if) # bind interface ethernet 101/1/1
nexus5500-sanA(config-if) # no shutdown
nexus5500-sanA(config-if) # end
nexus5500-sanA# copy running-config startup-config
nexus5500-sanA#
```

```
nexus5500-sanB# configure terminal
nexus5500-sanB(config) # fex 102
nexus5500-sanB(config-fex) # fcoe
nexus5500-sanB(config-fex) # interface vfc 1
nexus5500-sanB(config-if) # bind interface ethernet 102/1/1
nexus5500-sanB(config-if) # no shutdown
nexus5500-sanB(config-if) # end
nexus5500-sanB# copy running-config startup-config
nexus5500-sanB#
```

```
nexus6000-sanA# configure terminal
nexus6000-sanA(config) # fex 101
nexus6000-sanA(config-fex) # fcoe
nexus6000-sanA(config-fex) # interface vfc 1
nexus6000-sanA(config-if) # bind interface ethernet 101/1/1
nexus6000-sanA(config-if) # no shutdown
nexus6000-sanA(config-if) # end
nexus6000-sanA# copy running-config startup-config
nexus6000-sanA#
```

```
nexus6000-sanB# configure terminal
nexus6000-sanB(config) # fex 102
nexus6000-sanB(config-fex) # fcoe
nexus6000-sanB(config-fex) # interface vfc 1
nexus6000-sanB(config-if) # bind interface ethernet 102/1/1
nexus6000-sanB(config-if) # no shutdown
```

```
nexus6000-sanB(config-if) # end
nexus6000-sanB# copy running-config startup-config
nexus6000-sanB#
```

## vPC による SAN ブート

1 つの VFC インターフェイスが vPC メンバーにバインドされている場合、Cisco Nexus シリーズスイッチは SAN ブートを使用できます。複数のインターフェイスを複数のメンバにバインドすることはできません。

- vPC に割り当てられたポートを含む FEX が Nexus スイッチに関連付けられていること。
- vPC メンバには、1 つの VFC インターフェイスしかバインドされていないこと。複数のインターフェイスを複数のメンバにバインドすることはできません。



(注) 以前のすべての設定、および対応トポロジとの下位互換性を確保するには、Enhanced vPC を使用しないストレート-スルー FEX トポロジで FEX を設定する必要があります。

## vPC による SAN ブートの設定例

この例では、仮想ファイバチャネルインターフェイス 1 はファブリック A の物理イーサネットインターフェイス 101/1/1、およびファブリック B のインターフェイス 102/1/1 にバインドされています。インターフェイスはまた、両方のファブリックの仮想ポートチャンネル 1 にも関連付けられています。

```
nexus5000-sanA(config) # interface vfc 1
nexus5000-sanA(config-if) # bind interface eth 101/1/1
nexus5000-sanA(config) # interface eth 101/1/1
nexus5000-sanA(config-if) # channel-group 1 mode active
nexus5000-sanA(config-if) # interface port-channel 1
nexus5000-sanA(config-if) # vpc 1
nexus5000-sanA(config-if) #
```

```
nexus5000-sanB(config) # interface vfc 1
nexus5000-sanB(config-if) # bind interface eth 102/1/1
nexus5000-sanB(config) # interface eth 102/1/1
nexus5000-sanB(config-if) # channel-group 1 mode active
nexus5000-sanB(config-if) # interface port-channel 1
nexus5000-sanB(config-if) # vpc 1
nexus5000-sanB(config-if) #
```

```
nexus5500-sanA(config) # interface vfc 1
nexus5500-sanA(config-if) # bind interface eth 101/1/1
nexus5500-sanA(config) # interface eth 101/1/1
nexus5500-sanA(config-if) # channel-group 1 mode active
nexus5500-sanA(config-if) # interface port-channel 1
nexus5500-sanA(config-if) # vpc 1
nexus5500-sanA(config-if) #
```

```
nexus5500-sanB(config) # interface vfc 1
```

```
nexus5500-sanB(config-if) # bind interface eth 102/1/1
nexus5500-sanB(config) # interface eth 102/1/1
nexus5500-sanB(config-if) # channel-group 1 mode active
nexus5500-sanB(config-if) # interface port-channel 1
nexus5500-sanB(config-if) # vpc 1
nexus5500-sanB(config-if) #

nexus5600-sanA(config) # interface vfc 1
nexus5600-sanA(config-if) # bind interface eth 101/1/1
nexus5600-sanA(config) # interface eth 101/1/1
nexus5600-sanA(config-if) # channel-group 1 mode active
nexus5600-sanA(config-if) # interface port-channel 1
nexus5600-sanA(config-if) # vpc 1
nexus5600-sanA(config-if) #

nexus5600-sanB(config) # interface vfc 1
nexus5600-sanB(config-if) # bind interface eth 102/1/1
nexus5600-sanB(config) # interface eth 102/1/1
nexus5600-sanB(config-if) # channel-group 1 mode active
nexus5600-sanB(config-if) # interface port-channel 1
nexus5600-sanB(config-if) # vpc 1
nexus5600-sanB(config-if) #

nexus6000-sanA(config) # interface vfc 1
nexus6000-sanA(config-if) # bind interface eth 101/1/1
nexus6000-sanA(config) # interface eth 101/1/1
nexus6000-sanA(config-if) # channel-group 1 mode active
nexus6000-sanA(config-if) # interface port-channel 1
nexus6000-sanA(config-if) # vpc 1
nexus6000-sanA(config-if) #

nexus6000-sanB(config) # interface vfc 1
nexus6000-sanB(config-if) # bind interface eth 102/1/1
nexus6000-sanB(config) # interface eth 102/1/1
nexus6000-sanB(config-if) # channel-group 1 mode active
nexus6000-sanB(config-if) # interface port-channel 1
nexus6000-sanB(config-if) # vpc 1
nexus6000-sanB(config-if) #
```



## 第 12 章

# FLOGI、ネームサーバー、および RSCN データベースの管理

この章では、FLOGI、ネームサーバー、および RSCN データベースの設定と管理方法について説明します。

この章は、次の項で構成されています。

- [FLOGI、ネームサーバー、および RSCN データベースの管理（205 ページ）](#)

## FLOGI、ネームサーバー、および RSCN データベースの管理

### ファブリック ログイン

ファイバチャネルファブリックでは、ホストまたはディスクごとに FC ID が必要です。FLOGI テーブルにストレージデバイスが表示されるかどうかを確認するには、次の例のように **show flogi** コマンドを使用します。必要なデバイスが FLOGI テーブルに表示されていれば、FLOGI が正常に行われます。ホスト Host Bus Adapter (HBA) および接続ポートに直接接続されているスイッチ上の FLOGI データベースを検査します。ポートあたりの FLOGI または FDISC の最大数は 256 で、スイッチあたりの FLOGI または FDISC の最大数は 1000 です。

次に、FLOGI テーブルのストレージデバイスを確認する例を示します。

```
switch# show flogi database
-----
INTERFACE  VSAN    FCID          PORT NAME          NODE NAME
-----
vfc23      1       0xb200e2     21:00:00:04:cf:27:25:2c  20:00:00:04:cf:27:25:2c
vfc23      1       0xb200e1     21:00:00:04:cf:4c:18:61  20:00:00:04:cf:4c:18:61
vfc23      1       0xb200d1     21:00:00:04:cf:4c:18:64  20:00:00:04:cf:4c:18:64
vfc23      1       0xb200ce     21:00:00:04:cf:4c:16:fb  20:00:00:04:cf:4c:16:fb
vfc23      1       0xb200cd     21:00:00:04:cf:4c:18:f7  20:00:00:04:cf:4c:18:f7
vfc31      2       0xb30100     10:00:00:05:30:00:49:63  20:00:00:05:30:00:49:5e
Total number of flogi = 6.
```

次に、特定のインターフェイスに接続されたストレージデバイスを確認する例を示します。

```
switch# show flogi database interface vfc1/1
INTERFACE  VSAN      FCID          PORT NAME          NODE NAME
-----
vfc1/1     1       0x870000    20:00:00:1b:21:06:58:bc  10:00:00:1b:21:06:58:bc
Total number of flogi = 1.
```

次に、VSAN（仮想 SAN）1 に関連付けられたストレージ デバイスを確認する例を示します。

```
switch# show flogi database vsan 1
show flogi database vsan 1
-----
INTERFACE  VSAN  FCID  PORT NAME  NODE NAME
-----
fc1/17 1 0xee0000 21:00:00:24:ff:17:08:2e 20:00:00:24:ff:17:08:2e
fc1/18 1 0xee0020 10:00:00:90:fa:dc:0f:08 20:00:00:90:fa:dc:0f:08
fc1/37 1 0xee00ef 50:06:01:6a:08:60:7c:67 50:06:01:60:88:60:7c:67
Total number of flogi = 3.
```

## ネームサーバー プロキシ

ネームサーバー機能は、各 VSAN 内のすべてのホストおよびストレージ デバイスの属性を含むデータベースを維持します。ネームサーバーでは、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。

ネームサーバー登録要求はすべて、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。

### ネームサーバー プロキシの登録について

ネームサーバー登録要求はすべて、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。

### ネームサーバー プロキシの登録

ネームサーバー プロキシを登録できます。

#### SUMMARY STEPS

1. **configure terminal**
2. **fens proxy-port *wwn-id* vsan *vsan-id***

## DETAILED STEPS

## Procedure

|        | Command or Action   | Purpose                    |
|--------|---|----------------------------|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>   | 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。 |
| Step 2 | <b>fcns proxy-port <i>wwn-id vsan vsan-id</i></b><br><b>Example:</b><br><pre>switch(config)# fcns proxy-port 11:22:11:22:33:44:33:44 vsan 300</pre> | 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

FC 標準では、NX-OS は同一スイッチ、同一 VSAN、および同一 FC ドメインですでにログインしている pWWN の任意のインターフェイスでのログインを受け入れます。同じ pWWN が、異なるインターフェイスで同じスイッチにログインしないようにするには、ポートセキュリティ機能を使用します。

デフォルトでは、同一 VSAN の異なるスイッチでの（重複する pWWN による）今後の FLOGI はすべて拒否され、以前の FLOGI が維持されます。これは FC 標準に準拠していません。

このオプションを無効にすると、以前の FCNS エントリを削除することで、同一 VSAN の異なるスイッチでの（重複する pWWN による）今後の FLOGI はすべて許可されます。

## 重複 pWWN の拒否

FC 標準では、NX-OS は同一スイッチ、同一 VSAN、および同一 FC ドメインですでにログインしている pWWN の任意のインターフェイスでのログインを受け入れます。同じ pWWN が、異なるインターフェイスで同じスイッチにログインしないようにするには、ポートセキュリティ機能を使用します。

デフォルトでは、同一 VSAN の異なるスイッチでの（重複する pWWN による）今後の FLOGI はすべて拒否され、以前の FLOGI が維持されます。これは FC 標準に準拠していません。

このオプションを無効にすると、以前の FCNS エントリを削除することで、同一 VSAN の異なるスイッチでの（重複する pWWN による）今後の FLOGI はすべて許可されます。

重複 pWWN を拒否するには、次の手順を実行します。

## SUMMARY STEPS

1. **configure terminal**
2. **fcns reject-duplicate-pwwn vsan *vsan-id***
3. **no fcns reject-duplicate-pwwn vsan *vsan-id***

## DETAILED STEPS

## Procedure

|               | Command or Action  | Purpose  |
|---------------|--|--|
| <b>Step 1</b> | <b>configure terminal</b><br><br><b>Example:</b><br>switch# configure terminal<br>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。   |
| <b>Step 2</b> | <b>fcns reject-duplicate-pwwn vsan vsan-id</b><br><br><b>Example:</b><br>switch(config)# fcns reject-duplicate-pwwn vsan 100       | 異なるスイッチでの（重複するpWWNによる）今後のFLOGIはすべて拒否され、以前のFLOGIが維持されます（デフォルト）。   |
| <b>Step 3</b> | <b>no fcns reject-duplicate-pwwn vsan vsan-id</b><br><br><b>Example:</b><br>switch(config)# no fcns reject-duplicate-pwwn vsan 256 | 以前のFLOGIエントリを削除することで、異なるスイッチでの（重複するpWWNによる）今後のFLOGIはすべて許可されます。<br><br>ただし、他のスイッチのFLOGIデータベースには以前のエントリがまだ含まれています。 |

## ネーム サーバー データベース エントリ

ネーム サーバー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 サーバーは、Nx ポートが他のホストの属性を取得するために（ネーム サーバーへの）PLOGI を実行するときに、Nx ポートによる属性の登録を許可します。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 サーバー 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 サーバー プロセスのインスタンスが実行されます。

## ネーム サーバーのデータベース エントリの表示

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

```
switch# show fcns database
```

```
VSAN 1:
```

```
-----
FCID          TYPE  PWWN                               (VENDOR)          FC4-TYPE:FEATURE
-----
0xe90000      N     20:00:00:6b:f1:70:08:ec (Cisco)           scsi-fcp:init fc-gs
0xec0020      N     21:00:00:24:ff:7f:37:05 (Company A)       scsi-fcp:target
0xec0040      N     50:08:01:60:01:59:49:33                scsi-fcp:init
0xec0060      N     20:12:00:11:0d:9d:06:00                scsi-fcp:init
0xec0080      N     50:08:01:60:08:df:19:11                scsi-fcp:init
0xec00a0      N     20:00:d8:b1:90:41:1d:d1 (Cisco)           scsi-fcp:init
0xec00ef      N     50:06:01:61:08:60:7a:ab (Company B)       scsi-fcp:both
0xee0000      N     50:08:01:60:08:df:19:10                scsi-fcp
0xee0020      N     20:13:00:11:0d:9d:07:00                scsi-fcp:target
-----
```

```

0xee0040 N 10:00:00:90:fa:d1:ef:12 (Company C) scsi-fcp:init
0xee0060 N 20:00:00:6b:f1:70:08:ed (Cisco) scsi-fcp:init fc-gs
0xef0020 N 50:08:01:60:01:59:49:32 scsi-fcp
0xef0040 N 20:11:00:11:0d:96:e7:00 scsi-fcp:init

```

Total number of entries = 13

VSAN 2:

| FCID     | TYPE | PWWN                    | (VENDOR) | FC4-TYPE:FEATURE |
|----------|------|-------------------------|----------|------------------|
| 0x5e0020 | N    | 25:6b:28:6f:7f:21:03:f6 | (Cisco)  | npv              |
| 0x5e0040 | N    | 25:6b:e0:0e:da:49:c2:2a | (Cisco)  | npv              |
| 0x5e0080 | N    | 21:ed:00:2a:10:7a:89:1d | (Cisco)  | npv              |
| 0x840000 | N    | 20:0f:2c:d0:2d:50:d3:48 | (Cisco)  | npv              |
| 0x840040 | N    | 25:52:2c:d0:2d:50:d3:48 | (Cisco)  | npv              |

Total number of entries = 5

次に、指定された VSAN のネーム サーバー 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    |
|----------|------|-------------------------|-------------|---------------------|
| 0xe90000 | N    | 20:00:00:6b:f1:70:08:ec | (Cisco)     | scsi-fcp:init fc-gs |
| 0xec0020 | N    | 21:00:00:24:ff:7f:37:05 | (Company A) | scsi-fcp:target     |
| 0xec0040 | N    | 50:08:01:60:01:59:49:33 |             | scsi-fcp:init       |
| 0xec0060 | N    | 20:12:00:11:0d:9d:06:00 |             | scsi-fcp:init       |
| 0xec0080 | N    | 50:08:01:60:08:df:19:11 |             | scsi-fcp:init       |
| 0xec00a0 | N    | 20:00:d8:b1:90:41:1d:d1 | (Cisco)     |                     |
| 0xec00ef | N    | 50:06:01:61:08:60:7a:ab | (Company B) | scsi-fcp:both       |
| 0xee0000 | N    | 50:08:01:60:08:df:19:10 |             | scsi-fcp            |
| 0xee0020 | N    | 20:13:00:11:0d:9d:07:00 |             | scsi-fcp:target     |
| 0xee0040 | N    | 10:00:00:90:fa:d1:ef:12 | (Company C) | scsi-fcp:init       |
| 0xee0060 | N    | 20:00:00:6b:f1:70:08:ed | (Cisco)     | scsi-fcp:init fc-gs |
| 0xef0020 | N    | 50:08:01:60:01:59:49:32 |             | scsi-fcp            |
| 0xef0040 | N    | 20:11:00:11:0d:96:e7:00 |             | scsi-fcp:init       |

Total number of entries = 13

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

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

```
show fcns database detail
```

```
-----
VSAN:200 FCID:0xee0000
-----
```

```

port-wwn (vendor) :21:00:00:24:ff:17:08:2e (Qlogic)
node-wwn :20:00:00:24:ff:17:08:2e
class :3
node-ip-addr :0.0.0.0
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features :scsi-fcp:init
symbolic-port-name :
symbolic-node-name :QLE2742 FW:v8.05.44 DVR:v2.1.73.0
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :20:11:00:de:fb:53:a3:a0
hard-addr :0x000000

```

```

permanent-port-wwn (vendor) :21:00:00:24:ff:17:08:2e (Qlogic)
connected interface :fc1/17
switch name (IP address) :sw (192.168.1.1)
-----
VSAN:200 FCID:0xee0020

```

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

```

switch# show fcns statistics

show fcns statistics
Name server statistics for vsan 1
=====
registration requests received = 0
deregistration requests received = 0
queries received = 0
queries sent = 0
reject responses sent = 0
RSCNs received = 0
RSCNs sent = 0

Name server statistics for vsan 200
=====
registration requests received = 18
deregistration requests received = 0
queries received = 78
queries sent = 0
reject responses sent = 0
RSCNs received = 0
RSCNs sent = 8

Name server statistics for vsan 201
=====
registration requests received = 0
deregistration requests received = 0
queries received = 0
queries sent = 0
reject responses sent = 0
RSCNs received = 0
RSCNs sent = 0

Name server statistics for vsan 202
=====
registration requests received = 0
deregistration requests received = 0
queries received = 0
queries sent = 0
reject responses sent = 0
RSCNs received = 0
RSCNs sent = 0

```

## FDMI

Cisco Nexus N9K-C93180YC-FX、N9K-C93360YC-FX2、および N9K-C9336C-FX2-E スイッチは、FC-GS-4 規格で説明されているように、ファブリック デバイス管理インターフェイス (FDMI) 機能をサポートします。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 サーバーおよび管理サーバー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
```

この例では、すべての VSAN の HBA リストを表示します。

```
switch# sh fdmi database
Registered HBA List for VSAN 10
 10:00:00:90:fa:c7:e1:f6
Registered HBA List for VSAN 108
 20:04:00:11:0d:dd:00:00
 20:05:00:11:0d:dd:00:00
```

この例では、特定の VSAN の HBA リストを表示します。

```
switch# sh fdmi database vsan 10
Registered HBA List for VSAN 10
 10:00:00:90:fa:c7:e1:f6
```

この例では、HBA リストのすべての詳細を表示します。

```
switch# sh fdmi database detail
Registered HBA List for VSAN 10
-----
HBA-ID: 10:00:00:90:fa:c7:e1:f6
-----
Node Name           :20:00:00:90:fa:c7:e1:f6
Manufacturer        :Emulex Corporation
Serial Num          :FC61659139
Model               :LPe32002-M2
Model Description   :Emulex LightPulse LPe32002-M2 2-Port 32Gb Fibre Channel Adapter
Hardware Ver        :0000000c
Driver Ver          :11.4.33.1
ROM Ver             :11.4.204.25
Firmware Ver        :11.4.204.25
OS Name/Ver         :VMware ESXi 6.7.0 Releasebuild-8169922
CT Payload Len      :245760
  Port-id: 10:00:00:90:fa:c7:e1:f6
    Supported FC4 types:1 scsi-fcp fc-gs
    Supported Speed   :8G 16G 32G
    Current Speed     :16G
    Maximum Frame Size :2048
    OS Device Name    :vmhba8
```

```

Host Name          :localhost
Registered HBA List for VSAN 108
-----
HBA-ID: 20:04:00:11:0d:dd:00:00
-----
Node Name          :20:04:00:11:0d:23:b4:00
Manufacturer       :QLogic Corporation
Serial Num         :RFD1743U70327
Model              :QLE2742
Model Description: Cisco QLE2742 Dual Port 32Gb FC to PCIe Gen3 x8 Adapter
Hardware Ver       :BK3210407-43 B
Driver Ver         :8.07.00.34.Trunk-SCST.18-k
ROM Ver            :3.60
Firmware Ver       :8.08.204 (785ad0)
  Port-id: 20:04:00:11:0d:dd:00:00
    Supported FC4 types:scsi-fcp 40 fc-av
    Supported Speed   :8G 16G 32G
    Current Speed     :32G
    Maximum Frame Size :2112
    OS Device Name    :qla2xxx:host7
    Host Name         :VirtuaLUN
-----
HBA-ID: 20:05:00:11:0d:dd:00:00
-----
Node Name          :20:05:00:11:0d:23:b5:00
Manufacturer       :QLogic Corporation
Serial Num         :RFD1743U70327
Model              :QLE2742
Model Description: Cisco QLE2742 Dual Port 32Gb FC to PCIe Gen3 x8 Adapter
Hardware Ver       :BK3210407-43 B
Driver Ver         :8.07.00.34.Trunk-SCST.18-k
ROM Ver            :3.60
Firmware Ver       :8.08.204 (785ad0)
  Port-id: 20:05:00:11:0d:dd:00:00
    Supported FC4 types:scsi-fcp 40 fc-av
    Supported Speed   :8G 16G 32G
    Current Speed     :32G
    Maximum Frame Size :2112
    OS Device Name    :qla2xxx:host8
    Host Name         :VirtuaLUN

```

この例では、特定の VSAN の HBA リストのすべての詳細を表示します。

```

switch# sh fDMI database detail vsan 10
Registered HBA List for VSAN 10
-----
HBA-ID: 10:00:00:90:fa:c7:e1:f6
-----
Node Name          :20:00:00:90:fa:c7:e1:f6
Manufacturer       :Emulex Corporation
Serial Num         :FC61659139
Model              :LPe32002-M2
Model Description: Emulex LightPulse LPe32002-M2 2-Port 32Gb Fibre Channel Adapter
Hardware Ver       :0000000c
Driver Ver         :11.4.33.1
ROM Ver            :11.4.204.25
Firmware Ver       :11.4.204.25
OS Name/Ver        :VMware ESXi 6.7.0 Releasebuild-8169922
CT Payload Len     :245760
  Port-id: 10:00:00:90:fa:c7:e1:f6
    Supported FC4 types:1 scsi-fcp fc-gs
    Supported Speed   :8G 16G 32G
    Current Speed     :16G
    Maximum Frame Size :2048

```

```
OS Device Name      :vmhba8
Host Name           :localhost
```

## RSCN

Registered State Change Notification (RSCN) は、ファブリック内で行われた変更について各ホストに通知するためのファイバチャネルサービスです。ホストは、(State Change Registration (SCR) 要求によって) ファブリック コントローラに登録することにより、この情報を受信できます。次のいずれかのイベントが発生した場合、適宜通知されます。

- ファブリックへのディスクの加入または脱退
- ネーム サーバの登録変更
- 新しいゾーンの実施
- IP アドレスの変更
- ホストの動作に影響する、その他の同様なイベント

スイッチ RSCN (SW-RSCN) は、登録されたホストおよびファブリック内の到達可能なすべてのスイッチに送信されます。



**Note** 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。ネームサーバーに再度クエリーを発行して新しい情報を取得するのは、各ノードの責任範囲です。スイッチが各ノードに送信する RSCN には、変更に関する詳細情報は含まれていません。

## RSCN 情報の概要

スイッチ RSCN (SW-RSCN) は、登録されたホストおよびファブリック内の到達可能なすべてのスイッチに送信されます。



**Note** 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。ネームサーバー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

show rscn scr-table vsan 1
SCR table for VSAN: 1
-----
FC-ID REGISTERED FOR
-----
0xee0000 fabric and nport detected rscns
```

```
0xee0020 fabric and nport detected rscns
0xee00ef fabric and nport detected rscns

Total number of entries = 3
```



**Note** SCR テーブルは設定不可能です。ホストが RSCN 情報と一緒に SCR フレームを送信する場合にかぎり、入力されます。ホストが RSCN 情報を受信しない場合、**show rscn scr-table** コマンドはエントリを返しません。

## multi-pid オプション

RSCN の **multi-pid** オプションがイネーブルな場合、登録済みの Nx ポートに対して生成された RSCN には、関連ポート ID を複数格納できます。この場合、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 で **multi-pid** オプションがディセーブルになります。ホスト H に対して 2 つの RSCN が生成されます (1 つはディスク D1 用、もう 1 つはディスク D2 用)。
- スイッチ 1 で **multi-pid** オプションがイネーブルになります。ホスト H に対して RSCN が 1 つ生成され、RSCN ペイロードによって関連ポート ID がリストされます (この場合は D1 および D2)。



**Note** 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 の **multi-pid** オプションをディセーブルにしてください。



**Note** PORT\_OFFLINE イベントの場合、**multi-pid** オプションが有効か無効かに関係なく、複数の RSCN が生成され (ポートの数に応じて)、すぐに送信されます。

PORT\_ONLINE イベントの場合、

- **multi-pid** オプションが有効になっていると、ポートの数に関係なく単一の RSCN が生成され、すぐに送信されます。この RSCN には、起動するすべてのポートに関する情報を含む複数のページが含まれています。
- **multi-pid** オプションが無効になっている場合、(ポートの数に応じて) 複数の RSCN が生成され、すぐに送信されます。

## [multi-pid] オプションの設定

**multi-pid** オプションを設定できます。

### SUMMARY STEPS

1. **configure terminal**
2. **rscn multi-pid vsan vsan-id**

### DETAILED STEPS

#### Procedure

|        | Command or Action   | Purpose                                     |
|--------|---|---|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>       | 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。                |
| Step 2 | <b>rscn multi-pid vsan vsan-id</b><br><b>Example:</b><br><pre>switch(config)# rscn multi-pid vsan 405</pre> | 指定された VSAN の RSCN を multi-pid フォーマットで送信します。 |

## ドメイン フォーマット SW-RSCN の抑制

ドメイン フォーマット SW-RSCN は、ローカル スイッチ名またはローカル スイッチ管理 IP アドレスが変更されるとすぐに送信されます。この SW-RSCN は、ISL を介して、他のすべてのドメインおよびスイッチに送信されます。リモート スイッチから、ドメイン フォーマット SW-RSCN を開始したスイッチに対して GMAL コマンドおよび GIELN コマンドを発行すると、変更内容を判別できます。ドメイン フォーマット SW-RSCN によって、一部の他社製の SAN スイッチで問題が発生することがあります。

これらの SW-RSCN の ISL を介した送信を抑制できます。

### SUMMARY STEPS

1. **configure terminal**
2. **rscn suppress domain-swrsn vsan vsan-id**

### DETAILED STEPS

#### Procedure

|        | Command or Action                            | Purpose                      |
|--------|--|------------------------------|
| Step 1 | <b>configure terminal</b><br><b>Example:</b> | 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。 |

|               | Command or Action   | Purpose                                   |
|---------------|---|---|
|               | switch# configure terminal<br>switch(config)#   |   |
| <b>Step 2</b> | <b>rscn suppress domain-swrsn vsan vsan-id</b><br><br><b>Example:</b><br>switch(config)# rscn suppress domain-swrsn vsan<br>250 | 指定された VSAN のドメインフォーマット SW-RSCN の送信を抑制します。 |

## RSCN 統計情報のクリア

カウンタをクリアしたあとに、それらのカウンタを別のイベントに関して表示することができます。たとえば、特定のイベント（ONLINE または OFFLINE イベントなど）で生成された RSCN または SW-RSCN の個数を追跡できます。このような統計情報を利用して、VSAN 内で発生する各イベントへの応答を監視できます。

次に、指定された VSAN の RSCN 統計情報をクリアする例を示します。

```
switch# clear rscn statistics vsan 1
```

RSCN 統計情報をクリアした後、**show rscn statistics** コマンドを使用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あります。



**Note** 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。



**Note** CFS はデフォルトでイネーブルです。ファブリック内のすべてのデバイスで CFS をイネーブルに設定しないと配信は受信されません。アプリケーションに対して CFS がディセーブルになっていると、そのアプリケーションからコンフィギュレーションは配信されず、ファブリック内の他のデバイスからの配信も受け取ることができません。CFS を有効にするには、**cfs distribute** コマンドを使用します。



**Note** ダウングレードを実行する場合は、事前に、ネットワーク内の RSCN タイマー値をデフォルト値に戻してください。デフォルト値に戻しておかないと、VSAN およびその他のデバイスを経由するリンクがディセーブルになります。

RSCN タイマーを設定できます。

## SUMMARY STEPS

1. **configure terminal**
2. **rscn distribute**
3. **rscn event-tov timeout vsan vsan-id**
4. **no rscn event-tov timeout vsan vsan-id**
5. **rscn commit vsan vsan-id**

## DETAILED STEPS

### Procedure

|               | Command or Action  | Purpose  |
|---------------|--|--|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                          | 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。   |
| <b>Step 2</b> | <b>rscn distribute</b><br><b>Example:</b><br><pre>switch(config)# rscn distribute</pre>  | RSCN タイマーの設定の配布をイネーブルにします。   |
| <b>Step 3</b> | <b>rscn event-tov timeout vsan vsan-id</b><br><b>Example:</b><br><pre>switch(config)# rscn event-tov 1000 vsan 501</pre>       | 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。 |
| <b>Step 4</b> | <b>no rscn event-tov timeout vsan vsan-id</b><br><b>Example:</b><br><pre>switch(config)# no rscn event-tov 1100 vsan 245</pre> | 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。   |
| <b>Step 5</b> | <b>rscn commit vsan vsan-id</b><br><b>Example:</b><br><pre>switch(config)# rscn commit vsan 25</pre>                           | 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。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。



**Note** 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。配布されるのは、**rscn event-tov vsan vsan** コマンドだけです。



**Caution** RSCN タイマー設定だけが配布されます。

RSCN タイマーは、初期化およびスイッチオーバーの実行時に CFS に登録されます。ハイアベイラビリティを実現するため、RSCN タイマー配布がクラッシュし再起動する場合、またはスイッチオーバーが発生した場合には、クラッシュまたはスイッチオーバーが発生する前の状態から、通常の機能が再開されます。

追加情報については、ご使用のデバイスの『System Management Configuration Guide』の「Using Cisco Fabric Services」を参照してください。

## RSCN タイマー設定の配布のイネーブル化

RSCN タイマー設定の配布をイネーブルに設定できます。

## SUMMARY STEPS

1. **configure terminal**
2. **rscn distribute**
3. **no rscn distribute**

## DETAILED STEPS

## Procedure

|        | Command or Action   | Purpose                         |
|--------|---|---------------------------------|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre> | 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。      |
| Step 2 | <b>rscn distribute</b><br><b>Example:</b><br><pre>switch(config)# rscn distribute</pre>               | RSCN タイマーの設定の配布をイネーブルにします。      |
| Step 3 | <b>no rscn distribute</b><br><b>Example:</b><br><pre>switch(config)# no rscn distribute</pre>         | 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。

- 他のユーザーがこの機能の設定に変更を加えることができなくなります。
- コンフィギュレーションデータベースのコピーが、最初のアクティブ変更と同時に保留中のデータベースになります。

## RSCN タイマー設定の変更のコミット

アクティブ データベースに加えられた変更をコミットする場合、ファブリック内のすべてのスイッチに設定がコミットされます。コミットが正常に行われると、設定の変更がファブリック全体に適用され、ロックが解除されます。

RSCN タイマー設定の変更をコミットできます。

## SUMMARY STEPS

1. **configure terminal**
2. **rscn commit vsan *timeout***

## RSCN タイマー設定の変更の廃棄

## DETAILED STEPS

## Procedure

|               | Command or Action  | Purpose                    |
|---------------|--|----------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>        | 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。 |
| <b>Step 2</b> | <b>rscn commit vsan <i>timeout</i></b><br><b>Example:</b><br><pre>switch(config)# rscn commit vsan 500</pre> | 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うまま、ロックが解除されます。

RSCN タイマー設定の変更を廃棄できます。

## SUMMARY STEPS

1. **configure terminal**
2. **rscn abort vsan *timeout***

## DETAILED STEPS

## Procedure

|               | Command or Action  | Purpose  |
|---------------|--|--|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>      | 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。                     |
| <b>Step 2</b> | <b>rscn abort vsan <i>timeout</i></b><br><b>Example:</b><br><pre>switch(config)# rscn abort vsan 800</pre> | 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、ユーザー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
```



**Note** 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。



**Note** 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 vsan 1
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
+ rscn event-tov 1001
```

## RSCN のデフォルト設定

次の表に、RSCN のデフォルト設定を示します。

**Table 21:** 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) |

| パラメータ          | デフォルト  |
|----------------|--------|
| RSCN タイマー設定の配布 | ディセーブル |



## 第 13 章

# DDAS

この章では、デバイス エイリアス サービスの配信方法について説明します。

この章は、次の項で構成されています。

- [DDAS, on page 223](#)

## 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 エイリアスについての情報

Cisco SAN のスイッチは、ファブリック規模単位で配信デバイス エイリアス サービス（デバイス エイリアス）をサポートします。

Cisco SAN スイッチで（ゾーン分割など）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、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。不適切なデバイス名は、予想外の結果を招くことがあります。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、協調型配布モードおよびファブリック規模の配布範囲を使用します。
- 基本および拡張および拡張モード。
- ゾーンを設定するために使用されたデバイス エイリアスは、それぞれの pWWN と一緒に、**show** コマンド出力に自動的に表示されます。

追加情報については、ご使用のデバイスの『System Management Configuration Guide』の「Using Cisco Fabric Services」を参照してください。

### Related Topics

[デバイス エイリアスのモード](#), on page 226

## 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。

**Table 22:** 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 に限定されません。 | VSAN 番号を指定せずにデバイス エイリアスを定義できます。また、同一の定義を何の制約もなく 1 つまたは複数の VSAN で使用できます。 |

| ゾーンベースのエイリアス  | デバイスエイリアス   |
|---|---|
| ゾーンエイリアスは、ゾーン分割設定の一部です。他の機能の設定にはエイリアスマッピングを使用できません。 | pWWNを使用するすべての機能にデバイスエイリアスを使用できます。   |
| エンドデバイスを指定するのにすべてのゾーンメンバタイプを使用できます。                 | pWWNだけがサポートされます。  |
| 設定はゾーンサーバデータベース内に含まれ、他の機能では使用できません。                 | デバイスエイリアスは、ゾーン分割に限定されていません。デバイスエイリアス設定はFCNS、ゾーン、および <code>fcping</code> 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応用されます。

## デバイスエイリアスの作成

保留データベースにデバイスエイリアスを作成できます。

### SUMMARY STEPS

1. `configure terminal`
2. `device-alias database`
3. `device-alias name device-name pwwn pwwn-id`
4. `no device-alias name device-name`
5. `device-alias rename old-device-name new-device-name`

## DETAILED STEPS

## Procedure

|               | Command or Action  | Purpose   |
|---------------|--|---|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>  | 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。  |
| <b>Step 2</b> | <b>device-alias database</b><br><b>Example:</b><br><pre>switch(config)# device-alias database switch(config-device-alias-db)#</pre>  | 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。   |
| <b>Step 3</b> | <b>device-alias name <i>device-name</i> pwwn <i>pwwn-id</i></b><br><b>Example:</b><br><pre>switch(config-device-alias-db)# device-alias name mydevice pwwn 21:01:00:e0:8b:2e:80:93</pre> | 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。 |
| <b>Step 4</b> | <b>no device-alias name <i>device-name</i></b><br><b>Example:</b><br><pre>switch(config-device-alias-db)# no device-alias name mydevice</pre>  | 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。  |
| <b>Step 5</b> | <b>device-alias rename <i>old-device-name</i> <i>new-device-name</i></b><br><b>Example:</b><br><pre>switch(config-device-alias-db)# device-alias rename mydevice mynewdevice</pre>       | 既存のデバイスエイリアスを新しい名前に変更します。   |

## 例

次に、デバイスエイリアス設定を表示する例を示します。

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

## デバイスエイリアスのモード

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。ユーザーは以前の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。



**Note** Cisco NX-OS Release 10 では、基本デバイス エイリアス モードと拡張デバイス エイリアス モードの両方がサポートされています。1(1) 2(1)F。

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、ゾーンサーバー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 スイッチで行われます。



**Note** 拡張モードまたはネイティブ デバイス エイリアス ベースの設定は、interop モードの VSAN では受け入れられません。対応するゾーンにネイティブ デバイス エイリアス ベースのメンバがある場合、IVR ゾーンセットのアクティベーションは interop モードの VSAN で失敗します。

## デバイス エイリアス サービスに対するデバイス エイリアスのモードの注意事項と制限事項

デバイス エイリアス サービス設定時の注意事項と制限事項は次のとおりです。

- 異なるデバイス エイリアス モードで稼働している 2 つのファブリックが結合されると、デバイス エイリアスの結合は失敗します。結合プロセス中、一方のモードまたは他方のモードに自動的に変換できません。このような状況では、どちらか一方のモードを選択する必要があります。
- 拡張モードから基本モードに変更する前に、最初にローカルスイッチとリモートスイッチの両方からすべてのネイティブ デバイス エイリアス ベースの設定を明示的に削除するか、またはすべてのデバイス エイリアス ベース設定のメンバを対応する pWWN に置き換える必要があります。
- デバイス エイリアス データベースからデバイス エイリアスを削除すると、すべてのアプリケーションは対応するデバイス エイリアスの実行を自動的に中止します。対応するデバイス エイリアスがアクティブなゾーンセットの一部である場合、その pWWN を出入りするすべてのトラフィ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

例えば、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、ゾーンサーバーは、新しいHBAのpWWNに基づいて自動的にゾーン分割を適用します。

## デバイスエイリアスモードの設定

拡張モードで動作するデバイスエイリアスを設定できます。

### SUMMARY STEPS

1. **configure terminal**
2. **device-alias mode enhanced**
3. **no device-alias mode enhance**

### DETAILED STEPS

#### Procedure

|               | Command or Action   | Purpose                     |
|---------------|---|-----------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>             | 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。  |
| <b>Step 2</b> | <b>device-alias mode enhanced</b><br><b>Example:</b><br><pre>switch(config)# device-alias mode enhanced</pre>     | 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。 |
| <b>Step 3</b> | <b>no device-alias mode enhance</b><br><b>Example:</b><br><pre>switch(config)# no device-alias mode enhance</pre> | 基本モードで動作するデバイスエイリアスを割り当てます。 |

#### 例

次に、現在のデバイスエイリアスモード設定を表示する例を示します。

```
switch# show device-alias status

Fabric Distribution: Enabled

Database:- Device Aliases 0 Mode: Basic

Locked By:- User "admin" SWWN 20:00:00:0d:ec:30:90:40

Pending Database:- Device Aliases 0 Mode: Basic
```

## デバイスエイリアスの配布

デフォルトでは、デバイスエイリアスの配布はイネーブルになっています。デバイスエイリアス機能はCFSを使用して、ファブリック内のすべてのスイッチに変更内容を配布します。

デバイスエイリアスの配布がディセーブルの場合、データベースの変更内容はファブリック内のスイッチに配布されません。ファブリック内のすべてのスイッチで同じ変更を手動で行い、デバイスエイリアスデータベースを最新の状態に維持する必要があります。すぐにデータベースの変更が行われるので、保留中のデータベースおよびコミットまたは中断の操作もありません。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。



**Note** CFSはデフォルトでイネーブルです。ファブリックのすべてのデバイスではCFSが有効になっている必要があります。そうでない場合、デバイスは配信を受け入れません。アプリケーションでCFS配信が無効にされている場合、そのアプリケーションは構成を配信せず、またファブリック内の他のデバイスからの配信も受け入れません。CFSを有効にするには、**cfs distribute** コマンドを使用します。

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。

- 他のユーザー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。保留データベースへの変更をコミットするかまたは破棄（**abort**）するまで、保留データベースは使用されます。

## 変更のコミット

変更をコミットできます。

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

- 有効なデータベースの内容が、保留中のデータベースの内容に上書きされます。

- 保留中のデータベースがファブリック内のスイッチに配布され、これらのスイッチの有効なデータベースが新しい変更内容に上書きされます。
- 保留中のデータベースの内容が空になります。
- ファブリック ロックがこの機能に対して解除されます。

## SUMMARY STEPS

1. **configure terminal**
2. **device-alias commit**

## DETAILED STEPS

### Procedure

|               | Command or Action   | Purpose                      |
|---------------|---|------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre> | 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。   |
| <b>Step 2</b> | <b>device-alias commit</b><br><b>Example:</b><br><pre>switch(config)# device-alias commit</pre>       | 現在アクティブなセッションに対する変更をコミットします。 |

## 変更の破棄

デバイス エイリアスのセッション変更を破棄できます。

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

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

## SUMMARY STEPS

1. **configure terminal**
2. **device-alias abort**

## DETAILED STEPS

## Procedure

|        | Command or Action   | Purpose                    |
|--------|---|----------------------------|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre> | 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。 |
| Step 2 | <b>device-alias abort</b><br><b>Example:</b><br><pre>switch(config)# device-alias abort</pre>         | 現在アクティブなセッションを廃棄します。       |

## 例

次に、破棄操作のステータスを表示する例を示します。

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

Fabric Distribution: Enabled
Database:- Device Aliases 2 Mode: Basic
Checksum: 0x22a1d11a2762bdb3cae50f16a21a1e1
Locked By:- User "CLI/SNMPv3:admin" SWWN 20:00:00:de:fb:9d:0e:a0
Pending Database:- Device Aliases 3 Mode: Basic
```

次に、中断操作のステータスを表示する例を示します。

```
switch(config)# device-alias abort
switch(config)#

switch(config)# show device-alias session status
Last Action Time Stamp : Mon Nov 4 09:10:11 2019
Last Action : Abort
Last Action Result : Success
Last Action Failure Reason : none
switch(config)#
```

## ファブリック ロックの上書き

ロック操作（クリア、コミット、中断）は、デバイスエイリアスの配布がイネーブルの場合にだけ使用できます。ユーザー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、ユーザー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があります。

管理者の権限を使用して、ロックされたデバイスエイリアスセッションを解除するには、EXEC モードで **clear device-alias session** コマンドを使用します。

```
switch# clear device-alias session
```

次に、クリア操作のステータスを表示する例を示します。

```
switch# show device-alias status

Fabric Distribution: Enabled

Database:- Device Aliases 24

Status of the last CFS operation issued from this switch:
=====
Operation: Clear Session<-----Lock released by administrator
Status: Success<-----Successful status of the operation
```

## デバイスエイリアスの配布のディセーブル化とイネーブル化

デバイスエイリアスの配布をディセーブルまたはイネーブルに設定できます。

### SUMMARY STEPS

1. **configure terminal**
2. **no device-alias distribute**
3. **device-alias distribute**

### DETAILED STEPS

#### Procedure

|               | Command or Action  | Purpose                    |
|---------------|--|----------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br>switch# configure terminal<br>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。 |
| <b>Step 2</b> | <b>no device-alias distribute</b><br><b>Example:</b><br>switch(config)# no device-alias distribute | 配布をディセーブルにします。             |
| <b>Step 3</b> | <b>device-alias distribute</b><br><b>Example:</b><br>switch(config)# device-alias distribute       | 配布をイネーブルにします（デフォルト）。       |

#### 例

次に、デバイスエイリアスの配布のステータスを表示する例を示します。

```
switch# show device-alias status

Fabric Distribution: Disabled
Database:- Device Aliases 3 Mode: Basic
```

```
Checksum: 0x284031ab5aade498a7e89cef1b04d7f
switch(config)#
```

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 3 Mode: Basic
Checksum: 0x284031ab5aade498a7e89cef1b04d7f
switch(config)#
```

## レガシー ゾーン エイリアスの構成

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。ファブリック内の他のスイッチに設定を配信する必要がない場合は、**abort** 処理を実行して、マージ変更内容をすべて破棄できます。

## ゾーン エイリアスのインポート

特定の VSAN のゾーン エイリアスをインポートできます。

### SUMMARY STEPS

1. **configure terminal**
2. **device-alias import fcalias vsan *vlan-id***

### DETAILED STEPS

#### Procedure

|        | Command or Action   | Purpose                           |
|--------|---|-----------------------------------|
| Step 1 | <b>configure terminal</b><br><br><b>Example:</b><br>switch# configure terminal<br>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。        |
| Step 2 | <b>device-alias import fcalias vsan <i>vlan-id</i></b><br><br><b>Example:</b>                     | 指定された VSAN の fcalias 情報をインポートします。 |

| Command or Action                                | Purpose |
|--|---------|
| switch(config)# device-alias import fcalias vsan |         |

## 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イリアスの総数が、20Kを超えていないことを確認してください。

両方のデータベースのデバイスエントリの合計数がサポートされる設定制限値を超えた場合、結合は失敗します。たとえば、データベース *N* に6000個のデバイスエイリアス、データベース *M* に2192個のデバイスエイリアスがあり、SAN-OS Release 3.0(x) 以前が稼働している場合、この結合操作は失敗します。デバイスエイリアスモードが一致していない場合も、結合操作は失敗します。

追加情報については、ご使用のデバイスの『System Management Configuration Guide』の「CFS Merge Support」を参照してください。

## デバイスエイリアス構成の確認

デバイスエイリアス情報を表示するには、次のいずれかの作業を実行します。

| コマンド  | 目的                                   |
|---|--------------------------------------|
| <b>show zoneset [active]</b>  | ゾーンセット情報のデバイスエイリアスを表示します。            |
| <b>show device-alias database [pending   pending-diffs]</b>           | デバイスエイリアス データベースを表示します。              |
| <b>show device-alias {pwwn pwwn-id   name device-name } [pending]</b> | 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。 |
| <b>show flogi database [pending]</b>                                  | 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。       |

| コマンド                                      | 目的                             |
|---|--------------------------------|
| <code>show fcns database [pending]</code> | FCNS データベースのデバイスエイリアス情報を表示します。 |

## デバイスエイリアスサービスのデフォルト設定

次の表に、デバイスエイリアスパラメータのデフォルト設定を示します。

**Table 23:** デフォルトのデバイスエイリアスパラメータ

| パラメータ                 | デフォルト                 |
|-----------------------|-----------------------|
| デバイスエイリアスの配布          | イネーブル                 |
| デバイスエイリアスのモード         | 基本 (Basic) :          |
| 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 14 章

# ゾーンの設定と管理

この章では、ゾーンの設定と管理方法について説明します。

この章は、次の項で構成されています。

- [ゾーンに関する情報, on page 237](#)

## ゾーンに関する情報

ゾーン分割により、ストレージデバイス間またはユーザーグループ間でアクセスコントロールの設定ができます。ファブリックで管理者権限を持つユーザーは、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。



**Note** Cisco NX-OS リリース 10.2(1) は、基本、拡張、およびスマートゾーニングをサポートします。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。

Cisco NX-OS リリース 9.3(5) は、拡張ゾーニングとスマートゾーニングをサポートします。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。

- ゾーンは、複数のゾーンメンバで構成されます。
  - 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。
  - VSAN 内で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 1000 です。
- ゾーン分割は、ファブリックの任意のスイッチから管理できます。
  - 任意のスイッチからゾーンをアクティブにした場合、ファブリックのすべてのスイッチがアクティブゾーンセットを受信します。また、ファブリック内のすべてのスイッチにフルゾーンセットが配布されます（送信元スイッチでこの機能が基本ゾーニングモードでイネーブルであり、拡張ゾーニングモードでデフォルトである場合）。
  - 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、次のデバイスエイリアスメンバー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。
- デバイスエイリアス: デバイスエイリアス名を指定します。
- FC エイリアス: FC エイリアスの名前を指定します。



**Note** 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、ログインデバイスのデバイスエイリアス、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。
- 最大 4000 のゾーン ACL エントリがサポートされています。
- ゾーン ACL エントリ数が 4000 を超えると、ゾーンはソフトゾーニングモードに移行する可能性があります。



**Note** インターフェイスベースゾーン分割は、Cisco SAN スイッチでのみ機能します。インターフェイスベースゾーン分割は、interop モードで設定された 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。

**Figure 22:** 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。

Figure 23: 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手動でディセーブルにすることはできません。
- ネーム サーバー 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。
- ゾーンの再アクティブ化（ゾーンセットがアクティブの状態、別のゾーンセットをアクティブ化する場合）しても、既存のトラフィックは中断しません。

必要に応じて、さらに次のゾーン機能を設定できます。

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

## アクティブおよびフルゾーンセット

ゾーンセットを設定する前に、次の注意事項について検討してください。

- 各 VSAN は、複数のゾーンセットを持つことができますが、アクティブにできるのは常に1つのゾーンセットだけです。
- ゾーンセットを作成すると、そのゾーンセットは、フルゾーンセットの一部となります。

- ゾーンセットがアクティブな場合は、フルゾーンセットからのゾーンセットのコピーがゾーン分割の実行に使用されます。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。



**Note** 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。

**Figure 24:** アクティブおよびフルゾーンセット



## ゾーンの設定

ゾーンを設定し、ゾーン名を割り当てることができます。

### SUMMARY STEPS

1. **configure terminal**
2. **zone name** *zone-name* **vsan** *vsan-id*
3. **member** *type value*

## DETAILED STEPS

## Procedure

|               | Command or Action   | Purpose  |
|---------------|---|--|
| <b>Step 1</b> | <b>configure terminal</b><br><br><b>Example:</b><br>switch# configure terminal<br>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。   |
| <b>Step 2</b> | <b>zone name zone-name vsan vsan-id</b><br><br><b>Example:</b><br>switch(config)# zone name test vsan 5 | 指定された VSAN にゾーンを設定します。<br><br><b>Note</b><br>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。   |
| <b>Step 3</b> | <b>member type value</b><br><br><b>Example:</b><br>switch(config-zone)# member interface 4              | 指定されたタイプ (pWWN、ファブリック pWWN、FC ID、FC エイリアス、デバイス 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。<br><br><b>Caution</b><br>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。<br><br><b>Tip</b><br>該当する表示コマンド (たとえば、 <b>show interface</b> または <b>show flogi database</b> コマンド) を使用して、必要な値を 16 進表記で取得します。 |

## 設定例



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

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 pwnn 10:00:00:23:45:67:89:ab
```

ファブリック pWWN の例:

```
switch(config-zone)# member fwnn 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
```

デバイス エイリアスの例:

```
switch(config-zone)# member device-alias finance
```

ドメイン ID の例:

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

Show WWN の例:

```
switch# show wwn switch
```

ローカル sWWN インターフェイスの例:

```
switch(config-zone)# member interface vfc 21
```

リモート sWWN インターフェイスの例:

```
switch(config-zone)# member interface vfc 21 swwn 20:00:00:05:30:00:4a:de
```

ドメイン ID インターフェイスの例:

```
switch(config-zone)# member interface vfc 21 domain-id 25
```



---

**Note** **system default zone default-zone permit** および **system default zone distribute full** などのゾーンのデフォルトシステム設定は、設定を手動で適用した後に、新しく作成された VSAN でのみ有効になります。これらの設定は、FC セットアップ スクリプトの一部として設定されている場合でも、VSAN 1 に適用されない場合があります。

---

次に、異なるタイプのメンバエイリアスを設定する例を示します。

```
switch(config)# fcalias name AliasSample vsan 3
```

pWWN の例:

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

fWWN の例:

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

FC ID の例:

```
switch(config-fcalias)# member fcid 0x222222
```

ドメイン ID の例:

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

デバイス エイリアスの例:

```
switch(config-fcalias)# member device-alias devName
```

## ゾーンセット

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

**Figure 25:** ゾーンセット、ゾーン、ゾーンメンバーの階層



ゾーンは、アクセス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。



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

## ゾーンセットのアクティブ化

既存のゾーンセットをアクティブまたは非アクティブにできます。

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

### SUMMARY STEPS

1. **configure terminal**
2. **zoneset activate name** *zoneset-name* **vsan** *vsan-id*
3. **no zoneset activate name** *zoneset-name* **vsan** *vsan-id*

### DETAILED STEPS

#### Procedure

|               | Command or Action   | Purpose                    |
|---------------|---|----------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>   | 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。 |
| <b>Step 2</b> | <b>zoneset activate name</b> <i>zoneset-name</i> <b>vsan</b> <i>vsan-id</i><br><b>Example:</b><br><pre>switch(config)# zoneset activate name test vsan 34</pre> | 指定されたゾーンセットをアクティブにします。     |
| <b>Step 3</b> | <b>no zoneset activate name</b> <i>zoneset-name</i> <b>vsan</b> <i>vsan-id</i><br><b>Example:</b>   | 指定されたゾーンセットを非アクティブにします。    |

|  | Command or Action                                     | Purpose |
|--|---|---------|
|  | switch(config)# no zoneset activate name test vsan 30 |         |

## デフォルトゾーン

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



**Note** 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。



**Note** 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。



**Note** 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** として設定される場合、またはゾーンセットがアクティブのとき、デフォルトゾーンメンバは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、アクティブゾーンセットを表示すると、このゾーンのメンバの一覧表示は明示されません。

## 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。

### SUMMARY STEPS

1. **configure terminal**
2. **zone default-zone permit vsan vsan-id**

### 3. no zone default-zone permit vsan vsan-id

#### DETAILED STEPS

##### Procedure

|               | Command or Action  | Purpose                              |
|---------------|--|--------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                | 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。           |
| <b>Step 2</b> | <b>zone default-zone permit vsan vsan-id</b><br><b>Example:</b><br><pre>switch(config)# zone default-zone permit vsan 13</pre>       | 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。        |
| <b>Step 3</b> | <b>no zone default-zone permit vsan vsan-id</b><br><b>Example:</b><br><pre>switch(config)# no zone default-zone permit vsan 40</pre> | デフォルトゾーンメンバへのトラフィックフローを拒否（デフォルト）します。 |

## FC エイリアスの作成

次の値を使用して、エイリアス名を割り当て、エイリアスメンバを設定できます。

- pWWN: N ポートの 16 進表記の WWN (10:00:00:23:45:67:89:ab など)
- fWWN: ファブリック ポートの 16 進表記の WWN (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。
- デバイスエイリアス: デバイスエイリアス名を指定します。



**Tip** 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

エイリアスを作成します。

### SUMMARY STEPS

1. **configure terminal**
2. エイリアス名 vsan-id **fcalias name vsan**
3. **member type value**

### DETAILED STEPS

#### Procedure

|        | Command or Action  | Purpose  |
|--------|--|--|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                  | 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。   |
| Step 2 | エイリアス名 vsan-id <b>fcalias name vsan</b><br><b>Example:</b><br><pre>switch(config)# fcalias name testname vsan 50</pre> | エイリアス名を設定します。名称は64文字以内の英数字のストリング（大文字と小文字を区別）で指定します。  |
| Step 3 | <b>member type value</b><br><b>Example:</b><br><pre>switch(config-fcalias)# member pwwn 20:00:20:94:00:00:01</pre>     | 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ーを設定します。<br><br><b>Note</b><br>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

**Table 24:** **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  | <b>member device-alias device-alias</b>       |
| ドメイン ID     | ドメイン ID 番号 <b>member domain-id portnumber</b> |
| FC ID       | <b>member fcid fcid</b>                       |
| ファブリック pWWN | <b>member fwwn fwwn-id</b>                    |

|                    |  |
|--------------------|--|
| ローカル sWWN インターフェイス | <b>member interface type slot/port</b><br><b>Note</b><br>これが QSFP+ GEM またはブレイクアウトポートの場合、 <i>port</i> 構文は <i>QSFP-module/port</i> になります。<br><b>Note</b><br>これが 10G ブレイクアウトポートの場合、 <i>slot/port</i> 構文は <i>QSFP-module/port</i> になります。                     |
| ドメイン ID インターフェイス   | <b>member interface type slot/port domain-id domain-id</b><br><b>Note</b><br>これが QSFP+ GEM またはブレイクアウトポートの場合、 <i>port</i> 構文は <i>QSFP-module/port</i> になります。<br><b>Note</b><br>これが 10G ブレイクアウトポートの場合、 <i>slot/port</i> 構文は <i>QSFP-module/port</i> になります。 |
| リモート sWWN インターフェイス | <b>member interface type slot/port swwn swwn-id</b><br><b>Note</b><br>これが QSFP+ GEM またはブレイクアウトポートの場合、 <i>port</i> 構文は <i>QSFP-module/port</i> になります。<br><b>Note</b><br>これが 10G ブレイクアウトポートの場合、 <i>slot/port</i> 構文は <i>QSFP-module/port</i> になります。        |
| pWWN               | <b>member pwwn pwwn-id</b>   |

次に、異なるタイプのメンバエイリアスを設定する例を示します。

```
switch(config)# fcalias name AliasSample vsan 3
```

pWWN の例:

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

fWWN の例:

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

FC ID の例:

```
switch(config-fcalias)# member fcid 0x222222
```

ドメイン ID の例:

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

ローカル sWWN インターフェイスの例:

```
switch(config-fcalias)# member interface vfc 21
```

リモート sWWN インターフェ이스の例:

```
switch(config-fcalias)# member interface vfc 21 swwn 20:00:00:05:30:00:4a:de
```

ドメイン ID インターフェ이스の例:

```
switch(config-fcalias)# member interface vfc21 domain-id 25
```

デバイス エイリアスの例:

```
switch(config-fcalias)# member device-alias devName
```

## ゾーンセットの作成とメンバゾーンの追加

ゾーンセットを作成して複数のメンバーゾーンを追加できます。

### SUMMARY STEPS

1. **configure terminal**
2. **zone set name** *zoneset-name* **vsan** *vsan-id*
3. **member** *name*
4. **zone name** *zone-name*
5. **member fcid** *fcid*

### DETAILED STEPS

#### Procedure

|               | Command or Action  | Purpose   |
|---------------|--|---|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>  | 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。  |
| <b>Step 2</b> | <b>zone set name</b> <i>zoneset-name</i> <b>vsan</b> <i>vsan-id</i><br><b>Example:</b><br><pre>switch(config)# zone set name new vsan 23</pre> | 設定したゾーンセット名でゾーンセットを設定します。<br><b>Tip</b><br>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。                              |
| <b>Step 3</b> | <b>member</b> <i>name</i><br><b>Example:</b><br><pre>switch(config-zoneset)# member new</pre>  | 以前指定したゾーンセットのメンバーとしてゾーンを追加します。<br><b>Tip</b><br>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。 |

|               | Command or Action   | Purpose   |
|---------------|---|---|
| <b>Step 4</b> | <b>zone name</b> <i>zone-name</i><br><b>Example:</b><br><pre>switch(config-zoneset)# zone name trial</pre>        | 指定されたゾーンセットにゾーンを追加します。<br><b>Tip</b><br>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。   |
| <b>Step 5</b> | <b>member fcid</b> <i>fcid</i><br><b>Example:</b><br><pre>switch(config-zoneset-zone)# member fcid 0x222222</pre> | 新しいゾーンに新しいメンバを追加します。<br><b>Tip</b><br>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。 |



**Tip** 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、フルゾーンセットを明示的に保存するには、実行コンフィギュレーションをスタートアップコンフィギュレーションにコピー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、ゾーン分割の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せん。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。



**Note** 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 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。

## ゾーンセットの配信

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。

**Table 25:** ゾーンセット配信の相違点

| 一時配信  | フルゾーンセット配信  |
|---|---|
| <b>zoneset distribute vsan</b> コマンド (EXEC モード)            | <b>zoneset distribute full vsan</b> 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。  |

## フルゾーンセットの配信のイネーブル化

すべての Cisco SAN スイッチは、新しい E ポート リンクが立ち上がったとき、または新しいゾーンセットが VSAN でアクティブにされたときに、アクティブゾーンセットを配信します。ゾーンセットの配信は、隣接スイッチへのマージ要求の送信時、またはゾーンセットのアクティブ化の際に行われます。

VSAN 単位で、VSAN 上のすべてのスイッチへのフルゾーンセットおよびアクティブゾーンセットの配信をイネーブルに設定できます。

### SUMMARY STEPS

1. **configure terminal**
2. **zoneset distribute full vsan vsan-id**

### DETAILED STEPS

#### Procedure

|        | Command or Action   | Purpose                               |
|--------|---|---------------------------------------|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br>switch# configure terminal<br>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。            |
| Step 2 | <b>zoneset distribute full vsan vsan-id</b><br><b>Example:</b>                                | 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。 |

| Command or Action                               | Purpose |
|---|---------|
| switch(config)# zoneset distribute full vsan 12 |         |

## 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。



**Note** Cisco Nexus 9000 では、相互運用モード 3 のみがサポートされています。

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

```
switch# show zone status vsan 3
```

```
VSAN: 3 default-zone: permit distribute: active only Interop: 100
```

```
mode:basic merge-control:allow
```

```
session:none
```

```
hard-zoning:enabled
```

```
Default zone:
```

```
qos:none broadcast:disabled ronly:disabled
```

```
Full Zoning Database :
```

```
Zonesets:0 Zones:0 Aliases: 0
```

```
Active Zoning Database :
```

```
Name: nozoneset Zonesets:1 Zones:2
```

```
Status: Zoneset distribution completed at 04:01:06 Aug 28 2010
```

## リンクの分離からの回復

ファブリックの2つのスイッチがTEポートまたはEポートを使用して結合される場合、アクティブゾーンセットのデータベースが2つのスイッチまたはファブリック間で異なると、このTEポートおよびEポートが分離する可能性があります。TEポートまたはEポートが分離した場合、次の3つのオプションのいずれかを使用して分離状態からポートを回復できます。

- 近接スイッチのアクティブゾーンセットのデータベースをインポートし、現在のアクティブゾーンセットと交換します（次の図を参照）。
- 現在のデータベースを近接スイッチにエクスポートします。

- フルゾーンセットを編集し、修正されたゾーンセットをアクティブにしてから、リンクを立ち上げることにより、手動で矛盾を解決します。

Figure 26: データベースのインポートとエクスポート



## ゾーンセットのインポートおよびエクスポート

ゾーンセット情報を隣接スイッチにエクスポート、または隣接スイッチからインポートできます。

### SUMMARY STEPS

- switch# **zoneset import interface vfc** *vfc-id* **vsan** *vsan-id*
- zoneset import interface** {**vfc** | **vfc-port-channel**} *if-number* **vsan** *vsan-id*
- zoneset export vsan** *vsan-id*

### DETAILED STEPS

#### Procedure

|        | Command or Action   | Purpose  |
|--------|---|--|
| Step 1 | switch# <b>zoneset import interface vfc</b> <i>vfc-id</i> <b>vsan</b> <i>vsan-id</i>  | VSAN または VSAN の範囲の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。 |
| Step 2 | <b>zoneset import interface</b> { <b>vfc</b>   <b>vfc-port-channel</b> } <i>if-number</i> <b>vsan</b> <i>vsan-id</i><br><br><b>Example:</b><br>switch# zoneset import interface 6 vsan 10 | VSAN または VSAN の範囲の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。 |
| Step 3 | <b>zoneset export vsan</b> <i>vsan-id</i><br><br><b>Example:</b><br>switch# zoneset export vsan 5   | 指定された VSAN または VSAN の範囲を介して接続された隣接スイッチにゾーンセットをエクスポートします。         |

## ゾーンセットの複製

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

- 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。



**Caution** 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。

### SUMMARY STEPS

1. `zone copy active-zoneset full-zoneset vsan vsan-id`
2. `zone copy vsan vsan-id active-zoneset scp://guest@myserver/tmp/active_zoneset.txt`

### DETAILED STEPS

#### Procedure

|               | Command or Action  | Purpose   |
|---------------|--|---|
| <b>Step 1</b> | <b>zone copy active-zoneset full-zoneset vsan vsan-id</b><br><b>Example:</b><br><pre>switch# zone copy active-zoneset full-zoneset vsan 301</pre>  | 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。       |
| <b>Step 2</b> | <b>zone copy vsan vsan-id active-zoneset scp://guest@myserver/tmp/active_zoneset.txt</b><br><b>Example:</b><br><pre>switch# zone copy vsan 55 active-zoneset scp://guest@myserver/tmp/active_zoneset.txt</pre> | SCP を使用して、指定された VSAN のアクティブゾーンをリモートロケーションにコピーします。 |

## ゾーン、ゾーンセット、およびエイリアスの名前の変更

ゾーン、ゾーンセット、FC エイリアス、またはゾーン属性グループの名前を変更できます。

### SUMMARY STEPS

1. `configure terminal`
2. `zoneset rename oldname newname vsan vsan-id`
3. `zone rename oldname newname vsan vsan-id`
4. `fcalias rename oldname newname vsan vsan-id`
5. `zone-attribute-group rename oldname newname vsan vsan-id`
6. `zoneset activate name newname vsan vsan-id`

## DETAILED STEPS

## Procedure

|        | Command or Action  | Purpose                                    |
|--------|--|--|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>  | 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。                 |
| Step 2 | <b>zoneset rename <i>oldname newname vsan vsan-id</i></b><br><b>Example:</b><br><pre>switch(config)# zoneset rename test myzoneset vsan 60</pre>                         | 指定された VSAN のゾーンセット名を変更します。                 |
| Step 3 | <b>zone rename <i>oldname newname vsan vsan-id</i></b><br><b>Example:</b><br><pre>switch(config)# zone rename test myzone vsan 50</pre>                                  | 指定された VSAN のゾーン名を変更します。                    |
| Step 4 | <b>fcalias rename <i>oldname newname vsan vsan-id</i></b><br><b>Example:</b><br><pre>switch(config)# fcalias rename test myfc vsan 200</pre>                             | 指定された VSAN の fcalias 名を変更します。              |
| Step 5 | <b>zone-attribute-group rename <i>oldname newname vsan vsan-id</i></b><br><b>Example:</b><br><pre>switch(config)# zone-attribute-group rename test mygroup vsan 12</pre> | 指定された VSAN のゾーン属性グループ名を変更します。              |
| Step 6 | <b>zoneset activate name <i>newname vsan vsan-id</i></b><br><b>Example:</b><br><pre>switch(config)# zoneset activate name myzone vsan 50</pre>                           | 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。 |

## ゾーンのクローニング、ゾーンセットと FC エイリアス

ゾーン、ゾーンセット、および FC エイリアスを複製できます。

## SUMMARY STEPS

1. **configure terminal**
2. **zoneset clone *oldname newname vsan vsan-id***
3. **zone clone *oldname newname vsan number***
4. **fcalias clone *oldname newname vsan vsan-id***
5. **zone-attribute-group clone *oldname newname vsan vsan-id***
6. **zoneset activate name *newname vsan vsan-id***

## DETAILED STEPS

## Procedure

|               | Command or Action   | Purpose                                    |
|---------------|---|--|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br>switch# configure terminal<br>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。                 |
| <b>Step 2</b> | <b>zoneset clone oldname newname vsan vsan-id</b><br><b>Example:</b><br>switch(config)# zoneset clone test myzoneset2 vsan 2                          | 指定された VSAN のゾーンセットをコピーします。                 |
| <b>Step 3</b> | <b>zone clone oldname newname vsan number</b><br><b>Example:</b><br>switch(config)# zone clone test myzone3 vsan 3                                    | 指定された VSAN 内のゾーンをコピーします。                   |
| <b>Step 4</b> | <b>fcalias clone oldname newname vsan vsan-id</b><br><b>Example:</b><br>switch(config)# fcalias clone test myfcalias vsan 30                          | 指定された VSAN の FC エイリアス名をコピーします。             |
| <b>Step 5</b> | <b>zone-attribute-group clone oldname newname vsan vsan-id</b><br><b>Example:</b><br>switch(config)# zone-attribute-group clone test mygroup2 vsan 10 | 指定された VSAN のゾーン属性グループをコピーします。              |
| <b>Step 6</b> | <b>zoneset activate name newname vsan vsan-id</b><br><b>Example:</b><br>switch(config)# zoneset activate name myzonetest1 vsan 3                      | ゾーンセットをアクティブにし、アクティブゾーンセット内の新しいゾーン名に更新します。 |

## ゾーン サーバー データベースのクリア

指定された VSAN のゾーン サーバー 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 サーバー 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
```



**Note** **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構成が使用されるようにする必要があります。



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

## ゾーン設定の確認

ゾーン情報を表示するには、**show** コマンドを使用します。特定のオブジェクトの情報（たとえば、特定のゾーン、ゾーンセット、VSAN、エイリアス、または **brief** や **active** などのキーワード）を要求する場合、指定されたオブジェクトの情報だけが表示されます。

| コマンド                                     | 目的                     |
|--|------------------------|
| <b>show zone</b>                         | すべての VSAN のゾーン情報の表示    |
| <b>show zone vsan<br/>vsan-id</b>        | 特定の VSAN のゾーン情報の表示     |
| <b>show zoneset vsan<br/>vsan-id</b>     | VSAN 範囲に設定されたゾーンセットの表示 |
| <b>show zone name<br/>zone-name</b>      | 特定のゾーンのメンバの表示          |
| <b>show fcalias vsan<br/>vsan-id</b>     | fcalias 設定の表示          |
| <b>show zone member<br/>pwwn pwwn-id</b> | メンバが属しているすべてのゾーンの表示    |
| <b>show zone<br/>statistics</b>          | 他のスイッチと交換された制御フレーム数の表示 |
| <b>show zoneset active</b>               | アクティブゾーンセットの表示         |
| <b>show zone active</b>                  | アクティブゾーンの表示            |
| <b>show zone status</b>                  | ゾーンステータスの表示            |

## 拡張ゾーン分割

ゾーン分割機能は、FC-GS-4 および FC-SW-3 規格に準拠しています。どちらの規格も、前の項で説明した基本ゾーン分割機能と、この項で説明する拡張ゾーン分割機能をサポートしています。

### 拡張ゾーン分割

ゾーン分割機能は、FC-GS-4 および FC-SW-3 規格に準拠しています。どちらの規格も、前の項で説明した基本ゾーン分割機能と、この項で説明する拡張ゾーン分割機能をサポートしています。



**Note** 拡張ゾーンモードでスケールゾーン構成が再生される場合は、保存されたスケールゾーン構成を実行構成に適用する前に、ローカルゾーンデータベースを手動でクリアする必要があります。

次の表は、基本ゾーニングと拡張ゾーニングの違いを比較したものです。

**Table 26:** 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、そのサイズが重要になります。 |
| 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です。                         |
| ゾーン分割データベースを配信するには、同じゾーンセットを再度アクティブ化する必要があります。再度アクティブ化すると、ローカルスイッチおよびリモートスイッチのハードゾーン分割のハードウェア変更に影響することがあります。 | ゾーン分割データベースに対して変更を行い、再度アクティブ化することなく変更を配信します。                             | アクティブ化せずにゾーンセットを配信すると、スイッチのハードゾーン分割のハードウェア変更が回避されます。        |

| 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

基本ゾーンモードから拡張ゾーンモードに変更できます。

### Procedure

- 
- Step 1** ファブリック内のすべてのスイッチが拡張モードで動作可能であることを確認してください。
  - Step 2** 1つ以上のスイッチが拡張モードで動作できない場合、拡張モードへの変更要求は拒否されます。
  - Step 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。

### Procedure

- 
- Step 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。
  - Step 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。
  - Step 3** 動作モードを基本ゾーン分割モードに設定します。
-

## 拡張ゾーン分割のイネーブル化

VSAN 内で拡張ゾーン分割をイネーブルに設定できます。

デフォルトでは、拡張ゾーン分割機能は Cisco MDS 9000 スイッチはディセーブルです。

### SUMMARY STEPS

1. **configure terminal**
2. **zone mode enhanced vsan *vsan-id***
3. **no zone mode enhanced vsan *vsan-id***

### DETAILED STEPS

#### Procedure

|               | Command or Action  | Purpose                         |
|---------------|--|---------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br>switch# configure terminal<br>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。      |
| <b>Step 2</b> | <b>zone mode enhanced vsan <i>vsan-id</i></b><br><b>Example:</b><br>switch(config)# zone mode enhanced vsan 22       | 指定された VSAN で拡張ゾーン分割をイネーブルにします。  |
| <b>Step 3</b> | <b>no zone mode enhanced vsan <i>vsan-id</i></b><br><b>Example:</b><br>switch(config)# no zone mode enhanced vsan 30 | 指定された VSAN で拡張ゾーン分割をディセーブルにします。 |

## ゾーン データベースの変更

VSAN 内のゾーン分割データベースに対する変更をコミットまたは廃棄できます。

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

ファブリックが別のユーザー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。

## SUMMARY STEPS

1. **configure terminal**
2. **zone commit vsan vsan-id**
3. **switch(config)# zone commit vsan vsan-id force**
4. **switch(config)# no zone commit vsan vsan-id**
5. **no zone commit vsan vsan-id force**

## DETAILED STEPS

## Procedure

|        | Command or Action   | Purpose  |
|--------|---|--|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br>switch# configure terminal<br>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。                         |
| Step 2 | <b>zone commit vsan vsan-id</b><br><b>Example:</b><br>switch(config)# zone commit vsan 679                            | 拡張ゾーン データベースに変更を適用し、セッションをクローズします。                 |
| Step 3 | <b>switch(config)# zone commit vsan vsan-id force</b><br><b>Example:</b><br>switch(config)# zone commit vsan 34 force | 拡張ゾーン データベースに変更を強制的に適用し、別のユーザーが作成したセッションをクローズします。  |
| Step 4 | <b>switch(config)# no zone commit vsan vsan-id</b><br><b>Example:</b><br>switch(config)# no zone commit vsan 22       | 拡張ゾーン データベースへの変更を廃棄し、セッションをクローズします。                |
| Step 5 | <b>no zone commit vsan vsan-id force</b><br><b>Example:</b><br>switch(config)# no zone commit vsan 34 force           | 拡張ゾーン データベースへの変更を強制的に廃棄し、別のユーザーが作成したセッションをクローズします。 |

## ゾーン データベース ロックの解除

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

```
switch# configure terminal
switch(config)# no zone commit vsan 2
```

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

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



**Note** 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。

## 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
```

## 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。

**Table 27:** データベースのゾーン結合ステータス

| ローカル データベース   | 隣接データベース | 結合ステータス | 結合結果   |
|---|----------|---------|--|
| データベースには同じ名前のゾーンセットが含まれます。拡張ゾーン分割モードでは、interop モード3のアクティブゾーンセットには名前がありません。ゾーンセット名はフルゾーンセットにのみ存在しますが、異なるゾーン、エイリアス、属性グループになります。 |          | 成功      | データベース merge が成功した場合、ISL は分離されません。           |
| データベースには、同じ name1 を持つものの、異なるメンバーを持つゾーン、FC エイリアス、またはゾーン属性グループオブジェクトが含まれます。   |          | 失敗      | ローカル データベースには隣接データベースの情報が存在しません。ISL は分離されます。 |
| データなし   | データあり    | 成功      | ローカル データベースおよび隣接データベースが結合されます。               |
| データあり   | データなし    | 成功      | 隣接データベースにはローカルデータベースの情報が存在しません。              |

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（デフォルト ゾーニング：許可/拒否、スマート ゾーニング：有効/無効、マージポリシー - 許可/制限を含む）が異なる場合、ISL は分離されます。
- ゾーン結合オプションが同じである場合、結合制御設定に基づいて比較が行われます。
  - 設定が「制限」の場合、アクティブ ゾーンセットとフルゾーンセットが同じになる必要があります。これらが同じでない場合、リンクは分離されます。
  - 設定が「許可」の場合、結合規則を使用して結合が行われます。

## ゾーン マージ制御ポリシーの設定

マージ制御ポリシーを設定できます。

### SUMMARY STEPS

1. **configure terminal**
2. **zone merge-control restrict vsan vsan-id**
3. **no zone merge-control restrict vsan vsan-id**
4. **zone commit vsan vsan-id**

### DETAILED STEPS

#### Procedure

|        | Command or Action   | Purpose                            |
|--------|---|------------------------------------|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br>switch# configure terminal<br>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。         |
| Step 2 | <b>zone merge-control restrict vsan vsan-id</b><br><b>Example:</b><br>switch(config)# zone merge-control restrict vsan 24       | 現在の VSAN の結合制御設定を「制限」に設定します。       |
| Step 3 | <b>no zone merge-control restrict vsan vsan-id</b><br><b>Example:</b><br>switch(config)# no zone merge-control restrict vsan 33 | 現在の VSAN の結合制御設定をデフォルトの「許可」に設定します。 |
| Step 4 | <b>zone commit vsan vsan-id</b><br><b>Example:</b><br>switch(config)# zone commit vsan 20                                       | 指定された VSAN に対する変更をコミットします。         |

## デフォルトのゾーンポリシー

デフォルトゾーン内のトラフィックを許可または拒否できます。

### SUMMARY STEPS

1. **configure terminal**
2. **zone default-zone permit vsan** *vsan-id*
3. **no zone default-zone permit vsan** *vsan-id*
4. **zone commit vsan** *vsan-id*

### DETAILED STEPS

#### Procedure

|               | Command or Action   | Purpose                                 |
|---------------|---|---|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                       | 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。              |
| <b>Step 2</b> | <b>zone default-zone permit vsan</b> <i>vsan-id</i><br><b>Example:</b><br><pre>switch(config)# zone default-zone permit vsan 12</pre>       | 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。           |
| <b>Step 3</b> | <b>no zone default-zone permit vsan</b> <i>vsan-id</i><br><b>Example:</b><br><pre>switch(config)# no zone default-zone permit vsan 12</pre> | 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。 |
| <b>Step 4</b> | <b>zone commit vsan</b> <i>vsan-id</i><br><b>Example:</b><br><pre>switch(config)# zone commit vsan 340</pre>                                | 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。



**Note** system default zone default-zone permit および system default zone distribute full などのゾーンのデフォルトシステム設定は、設定を手動で適用した後に、新しく作成された VSAN でのみ有効になります。これらの設定は、FC セットアップスクリプトの一部として設定されている場合でも、VSAN 1 に適用されない場合があります。

FC スクリプトを使用してゾーン設定を構成することもできます。FC スクリプトを使用したデフォルトゾーン設定の構成の詳細については *Cisco Nexus 9000 シリーズ NX-OS 基本構成ガイド* を参照してください。

## SUMMARY STEPS

1. **configure terminal**
2. **system default zone default-zone permit**
3. **no system default zone default-zone permit**
4. **system default zone distribute full**
5. **no system default zone distribute full**

## DETAILED STEPS

### Procedure

|               | Command or Action  | Purpose   |
|---------------|--|---|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br>switch# configure terminal<br>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。                                  |
| <b>Step 2</b> | <b>system default zone default-zone permit</b><br><b>Example:</b><br>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。       |
| <b>Step 3</b> | <b>no system default zone default-zone permit</b><br><b>Example:</b><br>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。 |
| <b>Step 4</b> | <b>system default zone distribute full</b><br><b>Example:</b><br>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。           |
| <b>Step 5</b> | <b>no system default zone distribute full</b><br><b>Example:</b>   | 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          |

| Command or Action                                      | Purpose                           |
|--|-----------------------------------|
| switch(config)# no system default zone distribute full | ルト) にします。アクティブゾーンデータベースだけが配信されます。 |

## スマート ゾーン分割の概要

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

- デバイスに関して FC4 タイプが登録されていない。
- ゾーン変換時に、デバイスがファブリックにログインしていない。
- ゾーンは作成されているが、イニシエータとターゲットのいずれかまたは両方が指定されていない。

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



### Note

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

## スマート ゾーン分割のメンバー設定

次の表に、サポートされているスマートゾーン分割のメンバー設定を示します。

Table 28: スマートゾーン分割の設定

| 機能   | サポートあり |
|------|--------|
| PWWN | はい     |

| 機能        | サポートあり |
|-----------|--------|
| FCID      | はい     |
| FC エイリアス  | はい     |
| デバイスエイリアス | はい     |
| インターフェイス  | いいえ    |
| IP アドレス   | いいえ    |
| シンボル ノード名 | いいえ    |
| FWWN      | いいえ    |
| ドメイン ID   | いいえ    |

## VSAN でのスマート ゾーン分割の有効化

VSAN に対して **smart zoning** を設定するには、次の手順を実行します。

### Procedure

- 
- Step 1**    `switch# configure terminal`  
 コンフィギュレーション モードに入ります。
- Step 2**    `switch(config)# zone smart-zoning enable vsan 1`  
 VSAN でスマート ゾーン分割を有効にします。
- Step 3**    `switch(config)# no zone smart-zoning enable vsan 1`  
 VSAN でスマート ゾーン分割を無効にします。
- 

## スマート ゾーン分割のデフォルト値の設定

デフォルト値を設定するには、次の手順を実行します。

### Procedure

- 
- Step 1**    `switch# configure terminal`  
 コンフィギュレーション モードに入ります。

- Step 2**    `switch(config)# system default zone smart-zone enable`  
指定されたデフォルト値に基づいて作成された VSAN でスマート ゾーン分割を有効にします。
- Step 3**    `switch(config)# no system default zone smart-zone enable`  
VSAN でスマート ゾーン分割を無効にします。
- 

## スマート ゾーン分割へのゾーンの自動変換

ネームサーバーからデバイスタイプ情報を取得し、その情報をメンバーに追加するには、次の手順を実行します。これは、ゾーン、ゾーンセット、FC エイリアス、および VSAN のレベルで行えます。ゾーンセットがスマート ゾーン分割に変換されたら、ゾーンセットをアクティブにする必要があります。

### Procedure

---

- Step 1**    `switch# configure terminal`  
コンフィギュレーション モードに入ります。
- Step 2**    `switch(config)# zone convert smart-zoning fcalias name <alias-name> vsan <vsan no>`  
FC エイリアス メンバーのデバイス タイプ情報をネーム サーバーから取得します。
- Note**  
`zone convert` コマンドを実行すると、FC4 タイプは SCSI-FCP になります。SCSI-FCP には、デバイスがイニシエータかターゲットかを決定するビットがあります。イニシエータとターゲットの両方が設定されている場合、デバイスは両方として扱われます。
- Step 3**    `switch(config)# zone convert smart-zoning zone name <zone name> vsan <vsan no>`  
ゾーン メンバーのデバイス タイプ情報をネーム サーバーから取得します。
- Step 4**    `switch(config)# zone convert smart-zoning zoneset name <zoneset name> vsan <vsan no>`  
指定されたゾーンセットで、すべてのゾーンと FC エイリアス メンバーのデバイス タイプ情報をネーム サーバーから取得します。
- Step 5**    `switch(config)# zone convert smart-zoning vsan <vsan no>`  
VSAN 内に存在するすべてのゾーンセットのすべてのゾーンと FC エイリアス メンバーのデバイス タイプ情報をネーム サーバーから取得します。
- Step 6**    `switch(config)# show zone smart-zoning auto-conv status vsan 1`  
VSAN の以前の自動変換ステータスが表示されます。
- Step 7**    `switch(config)# show zone smart-zoning auto-conv log errors`

スマートゾーン分割自動変換のエラーログが表示されます。

### What to do next

デバイスがイニシエータ、ターゲット、またはその両方であるかどうかを確認するには、`show fcns database` コマンドを使用します。

```
switch# show fcns database
VSAN 1:
-----
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
-----
0x9c0000 N 21:00:00:e0:8b:08:96:22 (Company 1) scsi-fcp:init
0x9c0100 N 10:00:00:05:30:00:59:1f (Company 2) ipfc
0x9c0200 N 21:00:00:e0:8b:07:91:36 (Company 3) scsi-fcp:init
0x9c03d6 NL 21:00:00:20:37:46:78:97 (Company 4) scsi-fcp:target
```

## ゾーンメンバーのデバイスタイプの設定

ゾーンメンバーのデバイスタイプを設定するには、次の手順を実行します。

### Procedure

#### Step 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

#### Step 2 switch(config-zoneset-zone)# **member device-alias name both**

デバイスエイリアスメンバーのデバイスタイプを `both` として設定します。サポートされる各メンバータイプでは、`init`、`target`、および `both` がサポートされています。

#### Step 3 switch(config-zoneset-zone)# **member pwwn number target**

`pwwn` メンバーのデバイスタイプを `target` として設定します。サポートされる各メンバータイプでは、`init`、`target`、および `both` がサポートされています。

#### Step 4 switch(config-zoneset-zone)# **member fcid number**

`FCID` メンバーのデバイスタイプを設定します。設定されている特定のデバイスタイプがありません。サポートされる各メンバータイプでは、`init`、`target`、および `both` がサポートされています。

#### Note

ゾーンメンバーに対して特定のデバイスタイプが設定されていない場合は、バックエンドで、生成されたゾーンエントリがデバイスタイプ `both` として作成されます。

## スマートゾーン分割設定の削除

スマートゾーン分割設定を削除するには、次の手順を実行します。

## Procedure

- 
- Step 1** `switch(config)# clear zone smart-zoning fcalias name alias-name vsan number`  
指定された FC エイリアスのすべてのメンバーのデバイス タイプ設定を削除します。
- Step 2** `switch(config)# clear zone smart-zoning zone name zone name vsan number`  
指定されたゾーンのすべてのメンバーのデバイス タイプ設定を削除します。
- Step 3** `switch(config)# clear zone smart-zoning zoneset name zoneset name vsan number`  
指定されたゾーンセットの FC エイリアスとゾーンのすべてのメンバーのデバイス タイプ設定を削除します。
- Step 4** `switch(config)# clear zone smart-zoning vsan number`  
VSAN の指定されたゾーンセットの FC エイリアスとゾーンのすべてメンバーのデバイス タイプ設定を削除します。
- 

## 基本ゾーン分割モードにおけるゾーンレベルでのスマートゾーン分割の無効化

基本ゾーン分割モードの VSAN に対してゾーンレベルでスマートゾーン分割を無効にするには、次の手順を実行します。

## Procedure

- 
- Step 1** `switch# configure terminal`  
コンフィギュレーションモードに入ります。
- Step 2** `switch(config)# zone name zone1 vsan 1`  
ゾーン名を設定します。
- Step 3** `switch(config-zone)# attribute disable-smart-zoning`  
選択されたゾーンに対してスマートゾーン分割を無効にします。

### Note

このコマンドでは、選択されたゾーンのスマートゾーン分割が無効になるだけです。デバイス タイプ設定は削除されません。

---

## 拡張ゾーン分割モードの VSAN に対するゾーンレベルでのスマートゾーン分割の無効化

拡張ゾーン分割モードの VSAN に対してゾーンレベルでスマートゾーン分割を無効にするには、次の手順を実行します。

### Procedure

---

**Step 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**Step 2** switch(config)# **zone-attribute-group name disable-sz vsan 1**

拡張ゾーン セッションを作成します。

**Step 3** switch(config-attribute-group)#**disable-smart-zoning**

選択されたゾーンに対してスマートゾーン分割を無効にします。

**Note**

このコマンドでは、選択されたゾーンのスマートゾーン分割が無効になるだけです。デバイス タイプ設定は削除されません。

**Step 4** switch(config-attribute-group)# **zone name prod vsan 1**

ゾーン名を設定します。

**Step 5** switch(config-zone)# **attribute-group disable-sz**

選択されたゾーンのグループ属性名を割り当てるように設定します。

**Step 6** switch(config-zone)# **zone commit vsan 1**

選択された VSAN に対するゾーン分割の変更を確定します。

---

## 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。

**Note**

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。

---

### SUMMARY STEPS

1. **configure terminal**

2. **no zone name** *zone-name* **vsan** *vsan-id*
3. **zone compact** **vsan** *vsan-id*

## DETAILED STEPS

### Procedure

|               | Command or Action  | Purpose   |
|---------------|--|---|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>  | 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。                                |
| <b>Step 2</b> | <b>no zone name</b> <i>zone-name</i> <b>vsan</b> <i>vsan-id</i><br><b>Example:</b><br><pre>switch(config)# no zone name myzone vsan 35</pre> | ゾーンを削除し、ゾーン数を 2000 以下にします。                                |
| <b>Step 3</b> | <b>zone compact</b> <b>vsan</b> <i>vsan-id</i><br><b>Example:</b><br><pre>switch(config)# zone compact vsan 42</pre>                         | 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の確に管理するために、**show zone analysis** コマンドを使用して、ゾーン情報とゾーンセット情報を表示できます。

次に、フルゾーン分割の分析を表示する例を示します。

```
switch# show zone analysis vsan 1
```

次に、アクティブゾーニングの分析を表示する例を示します。

```
switch# show zone analysis active vsan 1
```

コマンド出力に表示される情報の詳細については、ご使用のデバイスの『Command Reference』を参照してください。

## ゾーンのデフォルト設定

次の表に、基本ゾーンパラメータのデフォルト設定を示します。

**Table 29:** 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 |

| パラメータ      | デフォルト           |
|------------|-----------------|
| フルゾーンセット配信 | フルゾーンセットは配信されない |
| 拡張ゾーン分割    | ディセーブル          |





## 第 15 章

# 拡張ファイバチャネル機能

この章では、拡張ファイバチャネル機能を設定する方法について説明します。

この章は、次の項で構成されています。

- [拡張ファイバチャネル機能および概念 \(275 ページ\)](#)

## 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、次のタイムアウト値 (TOV) を設定します。

- Distributed Services TOV (D\_S\_TOV) : 有効範囲は 5,000 ~ 10,000 ミリ秒です。
- Error Detect TOV (E\_D\_TOV) : 有効範囲は 1,000 ~ 4,000 ミリ秒です。デフォルトは 2,000 ミリ秒です。この値は、ポート初期化中に他端と比較されます。
- Resource Allocation TOV (R\_A\_TOV) : 有効範囲は 5,000 ~ 10,000 ミリ秒です。デフォルトは 10,000 ミリ秒です。この値は、ポート初期化中に他端と比較されます。



---

**Note** 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。



---

**Caution** D\_S\_TOV、E\_D\_TOV、および R\_A\_TOV 値をグローバルに変更するには、スイッチのすべての VSAN (仮想 SAN) を中断する必要があります。

---



**Note** 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 タイマーを設定できます。

## SUMMARY STEPS

1. **configure terminal**
2. **fctimer R\_A\_TOV timeout**

## DETAILED STEPS

### Procedure

|               | Command or Action   | Purpose   |
|---------------|---|---|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>   | 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。  |
| <b>Step 2</b> | <b>fctimer R_A_TOV timeout</b><br><b>Example:</b><br><pre>switch(config)# fctimer R_A_TOV 8008000</pre> | <p>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。</p> <p>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。</p> |

## 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。



**Note** 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 ファイバチャネル タイマーごとに設定できます。

## SUMMARY STEPS

1. **configure terminal**
2. **fctimer D\_S\_TOV timeout vsan vsan-id**

## DETAILED STEPS

### Procedure

|        | Command or Action  | Purpose  |
|--------|--|--|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                        | 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。   |
| Step 2 | <b>fctimer D_S_TOV timeout vsan vsan-id</b><br><b>Example:</b><br><pre>switch(config)# fctimer D_S_TOV 9009000 vsan 15</pre> | 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。 |

### 例

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 の配布

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。



**Note** CFS はデフォルトでイネーブルです。ファブリックのすべてのデバイスでは CFS が有効になっている必要があります。そうでない場合、デバイスは配信を受け入れません。アプリケーションで CFS 配信が無効にされている場合、そのアプリケーションは構成を配信せず、またファブリック内の他のデバイスからの配信も受け入れません。CFS を有効にするには、**cfs distribute** コマンドを使用します。

追加情報については、ご使用のデバイスの『System Management Configuration Guide』の「Using Cisco Fabric Services」を参照してください。

## fctimer の配布の有効化と無効化

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できます。

### SUMMARY STEPS

1. **configure terminal**
2. **fctimer distribute**
3. **no fctimer distribute**

### DETAILED STEPS

#### Procedure

|               | Command or Action   | Purpose  |
|---------------|---|--|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre> | 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。   |
| <b>Step 2</b> | <b>fctimer distribute</b><br><b>Example:</b><br><pre>switch(config)# fctimer distribute</pre>         | 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。 |
| <b>Step 3</b> | <b>no fctimer distribute</b><br><b>Example:</b><br><pre>switch(config)# no fctimer distribute</pre>   | 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。

### SUMMARY STEPS

1. **configure terminal**
2. **fctimer commit**

## DETAILED STEPS

## Procedure

|        | Command or Action   | Purpose  |
|--------|---|--|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre> | 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。   |
| Step 2 | <b>fctimer commit</b><br><b>Example:</b><br><pre>switch(config)# fctimer commit</pre>                 | 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。

## SUMMARY STEPS

1. **configure terminal**
2. **fctimer abort**

## DETAILED STEPS

## Procedure

|        | Command or Action   | Purpose  |
|--------|---|--|
| Step 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre> | 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。                     |
| Step 2 | <b>fctimer abort</b><br><b>Example:</b><br><pre>switch(config)# fctimer abort</pre>                   | 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 ロックの上書き

ユーザーが 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、ユーザー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
```

## ファブリック 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。



**Note** 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、ご使用のデバイスの『System Management Configuration Guide』の「CFS Merge Support」を参照してください。

## 構成された `fctimer` 値の確認

構成された `fctimer` 値を表示するには、`show fctimer` コマンドを使用します。次に、設定されているグローバルタイムアウト値 (TOV) を表示する例を示します。

```
switch# show fctimer
F_S_TOV   D_S_TOV   E_D_TOV   R_A_TOV
-----
5000 ms   5000 ms   2000 ms   10000 ms
```



**Note** `show fctimer` コマンドの出力には、(構成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 の構成済み 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 MAC アドレスと同等です。MAC アドレスと同様に、デバイスごとに WWN を一意に対応付ける必要があります。主要スイッチを選択するとき、およびドメイン ID を割り当てるときは、WWN を使用します。

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 (次の表を参照してください)。

Table 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    |



**Caution** 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 設定の確認

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、特定のスイッチの 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ことができます。

### SUMMARY STEPS

1. **configure terminal**
2. **wwn secondary-mac *wwn-id range value***

### DETAILED STEPS

#### Procedure

|               | Command or Action  | Purpose                              |
|---------------|--|--------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br>switch# configure terminal<br>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。           |
| <b>Step 2</b> | <b>wwn secondary-mac <i>wwn-id range value</i></b><br><b>Example:</b><br>switch(config)# wwn secondary-mac<br>33:e8:00:05:30:00:16:df range 55 | 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。 |

#### 例

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 番号を節約するために、Cisco SAN スイッチでは特殊な割り当て方式を使用しています。

一部の Host Bus Adapter (HBA) は、ドメインとエリアが同じ FC ID を持つターゲットを検出しません。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。各 HBA は、ファブリック ログイン時に pWWN で使用される会社 ID (組織固有識別子 (OUI) と呼ばれます) によって識別されます。リストされている会社 ID を持つ N ポートに完全な領域が割り当てられ、その他の場合は、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。



**Caution** 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 が割り当てられません。
- 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。



**Tip** `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 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、次にユーザー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 oui: 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。



**Note** Cisco Nexus デバイス 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、1つの相互運用モード（モード3—Brocade ネイティブ モード（コア PID 1））のみをサポートします。相互運用モードのモード3では、ネイティブ モードを変更することなく、コア PID 1（Brocade ネイティブ モード）の Brocade スイッチをシームレスに追加できます。その他すべての機能は同じままです。

- 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、次の URL にある *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](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有効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 デバイス スイッチに固有の変更点です。

Table 31: 相互運用モードが有効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  | <p>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。</p> <p>ドメイン ID は 97 ~ 127 の範囲に制限されます。これは、McData の公称制限をこの同じ範囲内に収めるためです。ドメイン ID は <b>Static</b> または <b>Preferred</b> に設定できます。それぞれの動作は次のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>Static:</b> 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。</li> <li>• <b>Preferred:</b> 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。</li> </ul> |
| 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無効にできます。   |
| デフォルトゾーン | ゾーンのデフォルトの許可動作 (すべてのノードから他のすべてのノードを認識可能) または拒否動作 (明示的にゾーンに配置されていないすべてのノードが隔離される) は変更できます。   |
| ゾーン分割属性  | <p>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。</p> <p><b>Note</b><br/>Brocade スイッチでは、<b>cfgsave</b> 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 スイッチには影響を及ぼしません。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。</p>  |

|                       |   |
|-----------------------|---|
| 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  |
| 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。<br><br>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。  |
| 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。  |
| 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、関連する VSAN のドメインマネージャプロセスだけを再起動する機能が組み込まれています。  |
| ネーム サーバー              | すべてのベンダーのネームサーバー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 3 の設定

Cisco SAN スイッチの interop モード 3 を中断または非中断に構成できます。



**Note** 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。

### Procedure

|        | Command or Action                         | Purpose   |
|--------|---|---|
| Step 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。 | <pre>switch# configuration terminal switch(config)# vsan database</pre> |

|               | Command or Action   | Purpose   |
|---------------|---|---|
|               |   | <pre>switch(config-vsantdb)# vsan 10 interop 3 switch(config-vsantdb)# exit</pre>   |
| <b>Step 2</b> | 97 (0x61) ~ 127 (0x7F) の範囲でドメイン ID を割り当てます。                 | <p><b>Note</b><br/>これは、McData スイッチに適用される制限です。</p> <p>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参加します。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かぎり、Cisco SAN スイッチはファブリックに参加しません。</p> <p><b>Note</b><br/>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。</p>   |
| <b>Step 3</b> | 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）。                          | <p><b>Note</b><br/>Cisco SAN スイッチ、Brocade、および McData の FC Error Detect (ED_TOV) と Resource Allocation (RA_TOV) のタイマーは、デフォルトで同一の値に設定されています。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。</p> <pre>switch(config)# fctimer e_d_tov ? &lt;1000-100000&gt; E_D_TOV in milliseconds(1000-100000) switch(config)# fctimer r_a_tov ? &lt;1000-4000&gt; E_D_TOV in milliseconds(1000-4000)</pre> |
| <b>Step 4</b> | 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。 | <ul style="list-style-type: none"> <li>• <b>disruptive</b> 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。 <pre>switch(config)# fcdomain restart disruptive vsan 1</pre> </li> </ul> <p>または</p>  |

|  | Command or Action | Purpose  |
|--|-------------------|--|
|  |                   | <ul style="list-style-type: none"> <li>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。</li> </ul> <pre>switch(config)# fcdomain restart vsan 10</pre> |

## 相互運用ステータスの確認

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。

任意の Cisco Nexus デバイス 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。

### SUMMARY STEPS

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。

### DETAILED STEPS

#### Procedure

**Step 1** ソフトウェアバージョンを確認します。

**Example:**

```
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

```

**Step 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。

**Example:**

```
switch# show interface brief
```

```

-----
Interface  Vsan    Admin  Admin  Status          SFP  Oper  Oper  Port
          Mode    Trunk
          Mode
          (Gbps)
-----
fc3/1      1        E      on     trunking        sw1  TE    2    --
fc3/2      1        auto   on     sfpAbsent       --   --    --   --
fc3/3      1        E      on     trunking        sw1  TE    2    --
fc3/4      1        auto   on     sfpAbsent       --   --    --   --
fc3/5      1        auto   auto   notConnected    sw1  --    --   --
fc3/6      1        auto   on     sfpAbsent       --   --    --   --
fc3/7      1        auto   auto   sfpAbsent       --   --    --   --
fc3/8      1        auto   auto   sfpAbsent       --   --    --   --

```

**Step 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。

**Example:**

```
switch# show running-config
Building Configuration...
  interface fc2/1
no shutdown
  interface fc2/2
no shutdown
  interface fc2/3
  interface fc2/4
<snip>
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
```

**Step 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。

**Example:**

```
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
```

**Step 5** ドメイン ID を確認します。

**Example:**

```
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
-----
```

**Step 6** ローカル主要スイッチのステータスを確認します。

**Example:**

```
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]
-----
```

**Step 7** スイッチのネクスト ホップおよび宛先を確認します。

**Example:**

```
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
```

**Step 8** ネーム サーバ情報を確認します。

**Example:**

```
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
```

**Note**

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。

## 高度なファイバチャネル機能のデフォルト設定

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。

Table 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 サーバー                | ディセーブル     |
| CIM サーバー 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         | Passive    |
| 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     |



## INDEX

- \* (アスタリスク) [153](#)
  - 最初の動作ポート[(アスタリスク)] [153](#)
    - 最初の動作ポート] [153](#)
- アクティブゾーンセット [240, 251](#)
  - 考慮事項 [240](#)
  - 配信のイネーブル化 [251](#)
- 宛先 ID [132, 137](#)
  - エクステンジベース [137](#)
  - パスの選択 [132](#)
  - フローベース [137](#)
- アドレス割り当てキャッシュ [179](#)
  - 説明 [179](#)
- 一意のエリア FC ID [176](#)
  - 設定 [176](#)
  - 説明 [176](#)
- インターフェイス [78, 100, 108, 115–116, 126–127, 144–145, 246](#)
  - FC エイリアス メンバの設定 [246](#)
  - SFP 情報の表示 [116](#)
  - SFP タイプ [115](#)
  - VSAN への割り当て [127](#)
  - VSAN メンバーシップ [126](#)
  - 隔離ステート [145](#)
  - 受信データ フィールド サイズの構成 [108](#)
  - 説明の構成 [100](#)
  - 中断ステート [145](#)
  - SAN ポートチャネルへの追加 [144–145](#)
- 永続的 FC ID [174, 177, 179](#)
  - 消去 [177](#)
  - 設定 [174](#)
  - 説明 [174](#)
  - 表示 [179](#)
  - イネーブル化 [174](#)
- 拡張ゾーン [257, 259–260, 264](#)
  - 基本ゾーンからの変更 [259](#)
  - 基本ゾーンの利点 [257](#)
  - スイッチ全体のデフォルト ゾーン ポリシーの設定 [264](#)
    - 説明 [257](#)
  - データベースの変更 [260](#)
  - デフォルトのフルデータベース配信の設定 [264](#)
  - デフォルト ポリシーの設定 [264](#)
- 拡張ポート モード [76](#)
- 確認 [67](#)
  - TCAM カービング設定 [67](#)
- 仮想ファイバチャネルインターフェイス [118, 128](#)
  - VSAN メンバーシップの表示 [128](#)
  - デフォルト設定 [118](#)
- 管理ステート [78](#)
  - 説明 [78](#)
- 管理速度 [104](#)
  - 設定 [104](#)
- 企業 ID [283](#)
  - FC ID の割り当て [283](#)
- 交換 ID [132](#)
  - パスの選択 [132](#)
- 交換リンクパラメータ [79](#)
- コミット [57](#)
  - ユーザー定義テンプレート [57](#)
- 作成 [47, 187, 191](#)
  - 仮想ファイバチャネルインターフェイス [187, 191](#)
  - ユーザー定義テンプレート [47](#)
- システム サービス ポリシー [41](#)
  - 付加 [41](#)
- 主要スイッチ [165, 167](#)
  - 設定 [167](#)
  - ドメイン ID の割り当て [165](#)
- 冗長性 [123](#)
  - VSANs [123](#)
- 概要 [42, 44, 48, 53, 59, 63](#)
  - デフォルトテンプレート [42](#)
  - ユーザー定義テンプレート [44, 48, 53, 59, 63](#)
- スイッチの優先順位 [160](#)
  - 説明 [160](#)
  - デフォルト [160](#)
- スイッチ ポート [112](#)
  - 属性のデフォルト値の設定 [112](#)
- スケラビリティ [123](#)
  - VSANs [123](#)
- ストレージ デバイス [237](#)
  - アクセス コントロール [237](#)
- スマートゾーン分割 [267](#)

- セカンダリ MAC アドレス 282
  - 設定 282
- 付加 41
  - システム サービス ポリシー 41
- 設定 19, 111, 200, 242
  - FCoE over Enhanced vPC 200
  - ジャンボ MTU 19
  - ゾーンの例 242
  - バッファ間クレジット 111
- zones 79, 123, 224, 237, 240, 244, 247, 253–255, 257, 271–272
  - FC エイリアスの設定 247
  - pWWN を使用したメンバーシップ 123
  - VSAN との比較 (表) 123
  - アクセス コントロール 244
  - エイリアスの設定 247
  - 機能 237, 240
  - コピー 255
  - 情報の表示 257
  - ダウングレード用の圧縮 271
  - データベースのインポート 253
  - データベースのエクスポート 253
  - デバイス エイリアスとの比較 224
  - デフォルト ポリシー 237
  - 名前の変更 254
  - バックアップ (手順) 254
  - 復元 (手順) 254
  - 分析 272
  - マージ障害 79
- ゾーンエイリアス 233
  - デバイス エイリアスへの変換 233
- ゾーン サーバー データベース 256
  - クリア 256
- ゾーンセット 237, 240, 244, 251–255, 257, 272
  - アクティブ化 244
  - 一時配信 252
  - インポート 253
  - エクスポート 253
  - 機能 237
  - 考慮事項 240
  - コピー 255
  - 作成 244
  - 情報の表示 257
  - 設定の配信 251
  - データベースのインポート 253
  - データベースのエクスポート 253
  - 名前の変更 254
  - 配信のイネーブル化 251
  - 分析 272
  - リンクの分離からの回復 252
- ゾーン属性グループ 255
  - コピー 255
- ゾーン データベース 256, 261
  - Cisco SAN 以外のデータベースの移行 256
  - ロックの解除 261
- ゾーン分割 237, 239–240
  - 実装 240
  - 説明 237
  - 例 239
- ゾーン メンバー 245
  - 情報の表示 245
- 相互運用性 133, 285, 289
  - interop モード 1 の設定 285
  - VSANs 133
  - ステータスの確認 289
  - 説明 285
- 送信元 ID 132, 137
  - エクステンジベース 137
  - パスの選択 132
  - フローベース 137
- 速度自動検知 106
- ソフトゾーン分割 250
  - 説明 250
- タイムアウト値 275
- デバイス エイリアス 223–226, 233–235
  - 拡張モード 226
  - 機能 223
  - 作成 225
  - 情報の表示 234
  - 説明 223
  - ゾーンエイリアスの変換 233
  - ゾーンセット情報の表示 234
  - ゾーンとの比較 224
  - データベースの変更 225
  - デフォルト設定 235
  - 要件 224
- デバイス エイリアス データベース 229–230, 232, 234
  - 結合 234
  - 配信のイネーブル化 232
  - 配信のディセーブル化 232
  - ファブリックのロック 229
  - 変更の破棄 230
- デフォルト VSAN 128
  - 説明 128
- デフォルトゾーン 245, 285
  - 説明 245
  - 相互運用性 285
  - ポリシー 245
- 動作ステート 79, 98
  - 説明 79

- 動作ステート (*continued*)
  - ファイバチャネル インターフェイスの構成 98
- 独立 VSAN 129–130
  - 説明 129
  - メンバーシップの表示 130
- ドメイン ID 79, 157, 165, 167–169, 172–173, 246, 285
  - CFS 配信の設定 168–169
  - FC エイリアス メンバの設定 246
  - Preferred 165
  - 許可リスト 167
  - 許可リストの設定 168
  - スタティック 165
  - 説明 165
  - 相互運用性 285
  - 配信 157
  - 隣接する割り当ての有効化 172–173
  - 連続割り当て 172
  - 割り当て障害 79
- ドメイン マネージャ 79, 159
  - 高速再起動機能 159
  - 分離 79
- トラフィックの分離 123
  - VSANs 123
- trunking 136, 285
  - 相互運用性 285
  - ポート チャネルとの比較 136
- トランキング E ポート モード 77
- トランキング ポート 127
  - VSAN に関連付けられた 127
- トランク モード 112
  - 管理デフォルト 112
- ネームサーバ 206, 208, 285
  - 相互運用性 285
  - データベース エントリの表示 208
  - プロキシ機能 206
  - プロキシの登録 206
- ノードプロキシ ポート モード 77
- ハードゾーン分割 250
  - 説明 250
- バッファ間クレジット 82, 111
  - 設定 111
- ビットエラー 109
  - 理由 109
- ビット エラーしきい値 109
  - 設定 109
  - 説明 109
- ファイバ チャネル 275
  - TOV 275
  - タイムアウト値 275
- ファイバチャネル インターフェイス 78–79, 82, 96–98, 100, 104, 108–109, 118
  - auto ポート モードの設定 98
  - BB\_credit 82
  - 管理ステート 78
  - 状態 78
  - 設定 96
  - 説明の構成 100
  - 速度の構成 104
  - デフォルト設定 118
  - 動作ステート 79
  - 範囲の設定 97
  - ビットエラーしきい値の設定 109
  - フレームのカプセル化の構成 108
  - ポートモードの設定 98
  - 理由コード 79
- ファイバチャネル ドメイン 157
- ファブリック 158
- ファブリック pWWN 237
  - ゾーン メンバーシップ 237
- ファブリック デバイス管理インターフェイス 210
- ファブリックの再構成 157
  - fcdomain フェーズ 157
  - セグメント分割 158
  - 説明 158
- ファブリック フレームの再設定 158
- ファブリック ポート モード 77
- ファブリック ログイン 205
- フルゾーンセット 240, 251
  - 考慮事項 240
  - 配信のイネーブル化 251
- フレームのカプセル化 108
  - 設定 108
- プロキシ 206
  - ネーム サーバーの登録 206
- 変更 51
  - ユーザー定義テンプレート 51
- ポート 126
  - VSAN メンバーシップ 126
- ポート速度 104
  - 設定 104
- ポート チャネル 79, 285
  - administratively down 79
  - 相互運用性 285
- ポート モード 78
  - auto 78
- ポート ワールドワイドネーム 237
- マージされたファブリック 163
  - 自動再構成済み 163
- 無効化 15
  - FCoE 15

ユーザー定義テンプレート **44, 47–48, 51, 53, 57, 59, 63**  
 コミット **57**  
 作成 **47**  
 概要 **44, 48, 53, 59, 63**  
 変更 **51**

ユニファイドポート **101**  
 設定 **101**

理由コード **79**  
 説明 **79**

レイヤ2 インターフェイス **101**  
 ユニファイドポート **101**

連続ドメイン ID の割り当て **172**  
 概要 **172**

ロード バランシング **124, 132, 135, 137**  
 SAN ポート チャネル **135**  
 VSAN の属性 **124**  
 設定 **132**  
 説明 **132, 137**  
 属性 **132**  
 保証 **132**

## A

auto ポート モード **78**  
 説明 **78**

auto モード **98**  
 設定 **98**

## B

BB\_credit **82, 117**  
 情報の表示 **117**  
 説明 **82**  
 理由コード **82**

Brocade **285**  
 ネイティブ interop モード **285**

## E

EISL **135**  
 SAN ポートチャネル リンク **135**

ELP **79**

Enhanced vPC **199–200**  
 FCoE **199**  
 FCoE の設定 **200**

E ポート **79, 98, 252**  
 設定 **98**  
 分離 **79**  
 リンクの分離からの回復 **252**

E ポートモード **76**  
 サービス クラス **76**

E ポート モード (*continued*)  
 説明 **76**

## F

FC ID **157, 172, 174, 246, 283**  
 FC エイリアス メンバの設定 **246**  
 persistent **174**  
 説明 **172**  
 デフォルトの企業 ID リストの割り当て **283**  
 割り当て **157**

fcdomain **79, 157, 159–165, 168–169, 179–180**  
 CFS 配信の設定 **168–169**  
 オーバーラップ分離 **79**  
 開始 **161**  
 restarts **157**  
 自動再構成の有効化 **164**  
 情報の表示 **179**  
 スイッチの優先順位 **160**  
 説明 **157**  
 着信 RCF **162**  
 デフォルト設定 **180**  
 統計情報の表示 **179**  
 ドメイン ID **165**  
 ドメイン マネージャの高速再起動 **159**  
 マージされたファブリックの自動再構成 **163**  
 無効化 **161**  
 イネーブル化 **161**

FCoE **15–16, 199**  
 Enhanced vPC 対応 **199**  
 LAN トラフィックの無効化 **16**  
 無効化 **15**

fctimer **280**  
 設定された値の表示 **280**

FC エイリアス **247, 254–255**  
 コピー **255**  
 作成 **247**  
 ゾーンの設定 **247**  
 名前の変更 **254**

FC ポート **107**  
 変換 **107**

FDMI **210–211**  
 説明 **210**  
 データベース情報の表示 **211**

FLOGI **205**  
 説明 **205**

FSPF **285**  
 相互運用性 **285**

fWWN **246**  
 FC エイリアス メンバの設定 **246**

Fx ポート [77, 123](#)  
     VSAN メンバーシップ [123](#)  
 F ポート [77, 98](#)  
     設定 [98](#)  
     説明 [77](#)  
 F ポート モード [77](#)  
     サービス クラス [77](#)  
     説明 [77](#)

**H**

HBA ポート [176](#)  
     エリア FCID の構成 [176](#)

**I**

interop モード [285, 293](#)  
     説明 [285](#)  
     デフォルト設定 [293](#)  
     モード 1 の設定 [285](#)  
 ISL [135](#)  
     SAN ポートチャネル リンク [135](#)

**M**

MAC アドレス [282](#)  
     セカンダリ の設定 [282](#)  
 McData [285](#)  
     ネイティブ interop モード [285](#)

**N**

N5K-M1008 拡張モジュール [95](#)  
 N5K-M1404 拡張モジュール [95](#)  
 NPIV [112–113](#)  
     説明 [112](#)  
     イネーブル化 [113](#)  
 NP ポート モード [77](#)  
 N ポート [237, 250](#)  
     ゾーンの実行 [250](#)  
     ゾーン メンバーシップ [237](#)  
     ハードゾーン分割 [250](#)  
 N ポート識別子仮想化 [112](#)

**P**

PLOGI [208](#)  
     ネームサーバ [208](#)  
 pWWN [237, 246](#)  
     FC エイリアス メンバの設定 [246](#)  
     ゾーン メンバーシップ [237](#)

**R**

RCF [158, 162–163](#)  
     説明 [158](#)  
     incoming [162](#)  
     着信の拒否 [163](#)  
 Registered State Change Notification. [213](#)  
 RSCN [213–215, 221](#)  
     情報の表示 [213](#)  
     スイッチ RSCN [213](#)  
     説明 [213](#)  
     デフォルト設定 [221](#)  
     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 [216, 218](#)  
     CFS を使用した設定の配信 [218](#)  
     設定 [216](#)

**S**

SAN ブート [203](#)  
     vPC による [203](#)  
     設定例 [203](#)  
 SAN ポートチャネル [135–138, 144–145, 153–154](#)  
     インターフェイス ステート [145](#)  
     インターフェイスの追加 [144–145](#)  
     構成誤りエラー検出 [138](#)  
     互換性チェック [144](#)  
     設定時の注意事項 [138](#)  
     設定の確認 [153](#)  
     説明 [135](#)  
     デフォルト設定 [154](#)  
     トランキングとの比較 [136](#)  
     ロードバランシング [137](#)  
 SAN ポートチャネルプロトコル [148–149](#)  
     自動作成 [149](#)  
     チャネルグループの作成 [148](#)  
 SAN ポートチャネルプロトコル [150](#)  
     自動作成のイネーブル化 [150](#)  
     自動作成の設定 [150](#)  
 SCR [213](#)  
     request [213](#)  
 SD ポート [98](#)  
     設定 [98](#)  
 SD ポートモード [78](#)  
     インターフェイスモード [78](#)  
     説明 [78](#)  
 SFP [115–116](#)  
     トランスミッタタイプ [115](#)  
     トランスミッタタイプの表示 [116](#)  
 SPAN 宛先ポートモード [78](#)

## T

- TE ポート [252, 285](#)
  - 相互運用性 [285](#)
  - リンクの分離からの回復 [252](#)
- TE ポート モード [77](#)
  - サービス クラス [77](#)
  - 説明 [77](#)
- TOV [275–276, 285, 293](#)
  - VSAN の設定 [276](#)
  - すべての VSAN の設定 [275](#)
  - 相互運用性 [285](#)
  - デフォルト設定 [293](#)
  - 範囲 [275](#)

## V

- vPC [203](#)
  - SAN ブート [203](#)
  - SAN ブートの例 [203](#)
- VSANs [77, 79, 121–130, 132–134, 165, 179, 206, 240, 275, 285](#)
  - FC ID [122](#)
  - interop モード [285](#)
  - TE ポート モード [77](#)
  - TOV [275](#)
  - 機能 [122](#)
  - キャッシュの内容 [179](#)
  - 削除 [130](#)
  - 使用状況の表示 [133](#)
  - 状態 [124](#)
  - 設定 [125](#)
  - 設定の表示 [133](#)
  - 説明 [121](#)
  - ゾーンとの比較 (表) [123](#)

## VSANs (continued)

- タイマー設定 [275](#)
- デフォルト VSAN [128](#)
- デフォルト設定 [134](#)
- 動作ステート [130](#)
- 独立 [129](#)
- ドメイン ID の自動再構成 [165](#)
- トラフィックの分離 [122](#)
- トランキング ポート [127](#)
- 名前 [124](#)
- ネームサーバ [206](#)
- 不一致 [79](#)
- 複数のゾーン [240](#)
- ポート メンバーシップ [126](#)
- メンバーシップの表示 [127](#)
- 利点 [122](#)
- ロード バランシング [132](#)
- ロード バランシング 属性 [124](#)
- VSAN ID [77, 123–124](#)
- VSAN メンバーシップ [123](#)
- 説明 [124](#)
- トラフィックの多重化 [77](#)
- range [123](#)

## W

- world wide names [281](#)
- WWN [79, 281–282](#)
  - 情報の表示 [281](#)
  - セカンダリ MAC アドレス [282](#)
  - 説明 [281](#)
  - 中断された接続 [79](#)
  - リンクの初期化 [282](#)

## 翻訳について

このドキュメントは、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。