Cisco MDS 9000 シリーズ IP サービス リリース 9.x 構成ガイド

最終更新：2025 年 5 月 19 日

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

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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 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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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)

© 2021–2025 Cisco Systems, Inc. All rights reserved.

目 次

Full Cisco Trademarks with Software License ?

はじめに：

はじめに xv

対象読者 xv

表記法 xv

マニュアルに関するフィードバック xvii

関連資料 xvii

通信、サービス、およびその他の情報 xvii

第 1 章

新機能および変更された機能に関する情報 1

新機能および変更された機能に関する情報 1

第 2 章

概要 3

概要 3

第 3 章

FCIP の設定 7

機能情報 7

FCIP の概要 8

FCIP の概念 9

FCIP ハイ アベイラビリティ ソリューション 11

ファイバ チャネル ポート チャネル 11

FSPF 12

FCIP の設定 13

FCIP の有効化 13

FCIP の基本構成 14
FCIP プロファイルの作成 15
FCIP プロファイル情報の表示 16
FCIP リンクの作成 17
FCIP MAC 統計情報の表示 18
FCIP プロファイルの詳細設定 19
TCP リスナー ポートの構成 19
TCP パラメータの構成 20
最小 再送信タイムアウト 20
Keepalive Timeout 21
最大再送信回数 21
OBFL ログの最大再送信しきい値 22
パス MTU 23
選択的確認応答 23
ウィンドウ管理 24
輻輳モニタリング 25
FCIP プロファイル情報の表示 26
FCIP インターフェイスの詳細構成 27
ピアの構成 27
ピア IP アドレス（IPv4）の割り当て 27
ピア IP アドレス（IPv6）の割り当て 28
TCP 接続数の設定 29
アクティブ接続の構成 30
タイム スタンプ制御の有効化 30
QoS 31
E ポートの構成 32
FCIP インターフェイス情報の表示 32
拡張 FCIP 機能 39
FCIP 書き込みアクセラレーション 39
FCIP 書き込みアクセラレーションの構成 42
書き込みアクセラレーションのアクティビティ情報の表示 42

FCIP テープ アクセラレーション 43
FCIP テープ アクセラレーションに関するテープ ライブラリ LUN マッピング 46
FCIP テープ アクセラレーションの構成 48
テープ アクセラレーションのアクティビティ情報の表示 49
FCIP圧縮 51
FCIP 圧縮の構成 52
FCIP 圧縮情報の表示 52
最大限のパフォーマンスを引き出すための FCIP リンクの構成 53
Cisco MDS 9250i スイッチでパフォーマンスを最大限に引き出すための FCIP リンクの構成 54
1 Gbps モードでの FCIP パフォーマンスの構成 54
10 Gbps モードでの FCIP パフォーマンスの構成 56
Cisco MDS 24/10 ポート SAN 拡張モジュールおよび M9220i スイッチで最大のパフォーマンスの FCIP リンクの構成 58
1 Gbps モードでの FCIP パフォーマンスの構成 58
10 Gbps モードでの FCIP パフォーマンスの構成 60
25 Gbps モードでの FCIP パフォーマンスの構成 61
40 Gbps モードでの FCIP パフォーマンスの構成 63
FCIP 構成の確認 65
FCIP パラメータのデフォルト設定 65

第 4 章 **SAN Extension Tuner の設定 67**
SAN Extension Tuner の概要 67
SAN Extension Tuner の設定 69
データ パターン 70
ライセンスの前提条件 70
SAN Extension Tuner の設定 70
FCIP リンクの調整 70
チューナーの有効化 71
nWWN の構成 71
仮想 N ポートの構成 71

SCSI ディスク読み取り/書き込み IO の生成 72
一度だけ SCSI ディスク読み取り/書き込み IO の生成 72
SCSI ディスク読み取り/書き込み IO の継続的な生成 73
SCSI の転送可能サイズ 74
SCSI テープ読み取り/書き込み IO の生成 75
一度だけ SCSI テープ読み取り/書き込み IO の生成 75
SCSI テープ読み取り/書き込み IO の継続的な生成 76
SCSI の転送可能サイズ 76
データ パターンの構成 77
SAN Extension Tuner 構成の確認 78
調整パラメータのデフォルト設定 79

第 5 章 **iSCSI の構成 81**
iSCSI の概要 82
iSCSI の設定制限 85
iSCSI の構成 85
iSCSI のイネーブル化 85
仮想ファイバ チャネル ホストとしての iSCSI ホストの提示 86
iSCSI インターフェイスの作成 86
iSCSI ターゲットとしてのファイバ チャネル ターゲットの提示 92
ダイナミック マッピング 93
スタティック マッピング 94
iSCSI 仮想ターゲットをアドバタイズするインターフェイスを構成する 95
仮想ファイバ チャネル ホストとしての iSCSI ホストの提示 96
イニシエータ識別モードの指定 96
iSCSI 仮想ターゲットの設定例 96
発信側提供モード 98
アイドル タイムアウトを構成する 100
iSCSI イニシエータへの WWN の割り当て 101
iSCSI イニシエータの名 name プションを使用したダイナミック マッピングを構成する 102

iSCSI イニシエータの名 name プションを使用したスタティック マッピングを構成する 103

iSCSI イニシエータの名 IP アドレス プションを使用したスタティック マッピングを構成する 103

iSCSI イニシエータに対する WWN の割り当て 104

自動的に割り当てられた nWWN/pWWN マッピングの保存 105

WWN の競合の確認と削除 105

プロキシ イニシエータ モード 106

プロキシ イニシエータの構成 108

iSCSI の VSAN メンバーシップ 108

iSCSI ホストの VSAN メンバーシップの割り当て 109

iSCSI インターフェイスのデフォルト ポート VSAN の設定 109

iSCSI デバイスの VSAN メンバーシップ 110

iSCSI のアクセス コントロール 111

iSCSI ユーザーの AAA 認証の構成 117

iSCSI の認証 メカニズムの構成 117

インターフェイスで iSCSI セッションの認証メカニズムの構成 118

ローカル認証の構成 118

iSCSI イニシエータ認証の制限 118

相互 CHAP 認証の設定 119

認証用のイニシエータごとの iSCSI ターゲット ユーザ名とパスワードの構成 120

iSCSI 即時データ機能および割り込みデータ機能 121

Cisco MDS スイッチ向け iSCSI インターフェイスの拡張機能 122

QoS 値の設定 125

iSCSI 情報の表示 125

iSLB の構成 135

iSLB の設定制限 136

iSLB 構成の前提条件 137

iSLB イニシエータ 137

iSLB イニシエータの構成 138

iSLB イニシエータの構成 138

iSLB イニシエータ IP アドレスの構成 138

iSLB 発信側への WWN の割り当て 139

iSLB イニシエータへの VSAN メンバーシップの割り当て 142

ロード バランシングのメトリック設定 143

iSLB イニシエータ構成の確認 144

iSLB イニシエータ ターゲットの構成 144

iSLB 発信側および発信側ターゲット用のゾーンの設定およびアクティブ化 145

iSLB ゾーン分割設定の確認 147

iSLB セッション認証の設定 147

iSLB イニシエータ認証の制限 148

相互 CHAP 認証 148

iSLB ゾーン認証設定の確認 149

VRRP を使用するロード バランシング 150

ギガビット イーサネット インターフェイスを選択する VRRP ロード バランシング アルゴリズム 151

VRRP を使用したロード バランシングの構成 154

ロード バランシング用の VRRP の有効化 155

iSLB VRRP ロード バランシング構成の確認 155

iSLB VRRP 情報の表示 155

CFS を使用した iSLB 構成の配信 156

CFS を使用した iSLB 構成の配信 157

iSLB 構成配信の有効化 157

ファブリックのロック 157

ファブリックへの変更のコミット 158

保留中の変更の廃棄 158

ファブリックのロックのクリア 159

CFS マージ プロセス 159

保留中の iSLB 設定変更の表示 160

iSLB CFS ステータスの表示 160

iSLB CFS マージ ステータスの矛盾 161

iSCSI ハイ アベイラビリティ 161

透過型ターゲット フェールオーバー 161

スタティック iSCSI 仮想ターゲットの作成 164
スタティック iSCSI 仮想ターゲットのトレスパス機能を有効にする 165
同じ IP ネットワークに接続された複数の IPS ポート 166
VRRP ベースのハイ アベイラビリティ 166
イーサネット ポート チャネル ベースのハイ アベイラビリティ 167
iSCSI 認証設定時の注意事項およびシナリオ 168
認証なしの構成 168
ローカル パスワード データベースを使用した CHAP の構成 169
外部 RADIUS サーバを使用した CHAP の構成 169
iSCSI トランスペアレント モード イニシエータ 171
iSCSI の構成シナリオ 1 171
iSCSI の構成シナリオ 2 175
iSCSI の構成シナリオ 1 180
iSCSI の構成シナリオ 2 185
Internet Storage Name Service の概要 190
iSNS クライアント機能の概要 190
iSNS クライアント プロファイルの作成 191
インターフェイスにプロファイルをタグ付け 192
iSNS クライアント構成の確認 192
iSNS サーバ機能 194
iSNS サーバの構成 196
iSNS サーバの有効化 196
iSNS の構成配信 196
ESI 再試行カウントの設定 197
登録期間の設定 198
iSNS クライアントの登録および登録解除 198
iSNS サーバ構成の確認 199
iSNS Cloud Discovery 205
クラウド検出 205
iSNS クラウド検出の設定 206
デフォルト設定 209

第 6 章 IP サービスの設定 211

トラフィック管理サービス 212

Management Interface Configuration 212

IPv4 の mgmt0 イーサネット インターフェイスの構成 213

IPv6 の mgmt0 イーサネット インターフェイスの構成 214

デフォルト ゲートウェイ 214

デフォルト ゲートウェイの設定 215

デフォルト ゲートウェイの構成の確認 215

IPv4 デフォルト ネットワークの構成 215

IP over Fibre Channel 217

IPFC 設定 217

VSAN での IPv4 アドレスの構成 218

VSAN インターフェイスの構成の確認 218

IPv4 ルーティングの有効化 218

IPFC の構成例 219

IPv4 スタティックルート 222

IPv4 スタティック ルートの設定 222

IPv4 スタティック ルート情報の確認 223

ARP の表示とクリア 223

オーバーレイ VSAN 224

オーバーレイ VSAN の設定 224

複数の VSAN の構成 226

DNS の設定 229

DNS ホスト情報の表示 230

DNS 機能のデフォルト設定 231

第 7 章 IP ストレージ サービスの設定 233

機能情報 234

サポート対象ハードウェア 234

FCIP および iSCSI インターフェイスのアップグレード 234

Cisco MDS 9220i スイッチでの IPS ポートの構成 234
Cisco MDS 24/10 ポート SAN 拡張モジュールでの 40 Gbps 速度の構成 235
IPv4 の IP ストレージ インターフェイスの構成 236
基本 IPStorage 構成 237
IPS ポート コア ダンプを備えたファイバ チャネル モジュール 237
IPStorage の VLAN について 239
インターフェイス サブネットの要件 240
IPStorage 接続の確認 240
IPStorage IPv4-ACL のガイドライン 241
IPStorage ハイ アベイラビリティの構成 242
iSCSI および FCIP サービスの VRRP 242
IP ストレージ インターフェイスの VRRP の構成 243
CDP の設定 244
IPStorage インターフェイスでのリンク速度の変更 245
Cisco MDS 9250i マルチ サービス ファブリック スイッチのリンク速度の変更 245
IPStorage インターフェイスで 1 Gbps リンク速度を構成する 245
IPStorage インターフェイスで 10 Gbps リンク速度を構成する 246
Cisco MDS 9220i スイッチのリンク速度の変更 247
IPStorage インターフェイスでの 1 Gbps リンク速度の構成 247
IPStorage インターフェイスで 10 Gbps リンク速度を構成する 248
IPStorage インターフェイスでの 25 Gbps リンク速度の構成 248
IPStorage インターフェイスでの 40 Gbps リンク速度の構成 249
Cisco MDS 24/10 ポート SAN 拡張モジュールでリンク速度の変更 250
IPStorage インターフェイスでの 1 Gbps リンク速度の構成 250
IPStorage インターフェイスで 10 Gbps リンク速度を構成する 251
IPStorage インターフェイスでの 40 Gbps リンク速度の構成 251
統計の表示 252
イーサネット MAC 統計情報の表示 253
TCP 統計情報の表示 254
IPStorage サービス パラメータのデフォルト設定 256

第 8 章 ギガビット イーサネット インターフェイスでの IPv4 の構成 257

IPv4 の概要 257

IPv4 の基本的なギガビット イーサネット構成 258

自動ネゴシエーションの設定 259

MTU フレーム サイズの設定 260

無差別モードの構成 261

ギガビット イーサネット接続の確認 262

Cisco MDS NX-OS での VLAN サポート 262

ギガビット イーサネットの VLAN 262

VLAN サブインターフェイスの構成 263

インターフェイス サブネットの要件 263

スタティック IPv4 ルーティングの構成 264

IPv4 ルート テーブルの表示 265

IPv4：アクセス コントロール リスト 265

ギガビット イーサネットの注意事項 265

ギガビット イーサネット インターフェイスへの適用 266

Address Resolution Protocol キャッシュ 266

ARP キャッシュの表示 267

ARP キャッシュのクリア 267

IPv4 統計情報の表示 267

IPv4 パラメータのデフォルト設定 268

第 9 章 IPv6 の設定 269

IPv6 の概要 269

IPv6 アドレス空間の拡張による一意アドレスの確保 270

IPv6 アドレス形式 270

IPv6 アドレス プレフィックスの形式 271

IPv6 アドレスタイプ：ユニキャスト 271

グローバル アドレス 271

リンクローカル アドレス 272

IPv6 アドレスタイプ：マルチキャスト 273
IPv6 の ICMP 274
IPv6 のパス MTU ディスカバリ 275
IPv6 ネイバー探索 275
IPv6 ネイバー送信要求メッセージおよびアドバタイズ メッセージ 275
ルーター発見 278
IPv6 ステートレス自動設定 278
IPv4 と IPv6 の二重プロトコル スタック 278
IPv6 用の基本的な接続の設定 279
IPv6 アドレッシングの設定と IPv6 ルーティングの有効化 280
IPv4 および IPv6 プロトコル アドレスの構成 281
IPv6 基本接続の設定と動作の確認 282
ネイバー探索パラメータの構成の確認 284
重複アドレス検出試行回数 284
到達可能性時間 284
再送信時間 285
ネイバー探索パラメータの構成の確認 286
IPv6 スタティック ルート 286
IPv6 スタティック ルートの設定 286
IPv6 スタティック ルートの設定と動作の確認 287
ギガビット イーサネットの IPv6-ACL に関する注意事項 288
IPv4 から IPv6 への移行 289
IPv6 の表示 289
デフォルト設定 290

はじめに

ここでは、『Cisco MDS 9000 Series Configuration Guideを使用している対象読者、構成、および表記法について説明します。また、関連マニュアルの入手方法についても説明します。次のセクションを含んでいます：

- 対象読者 （xv ページ）
- 表記法 （xv ページ）
- マニュアルに関するフィードバック （xvii ページ）
- 関連資料 （xvii 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 MDS 9000 シリーズ スイッチの設置、構成、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

コマンドの説明では、次の表記法を使用しています。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	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、角カッコで囲み、縦棒で区切って示しています。

表記法	説明
{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。
[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。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

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

このマニュアルでは、次の表記法を使用しています。

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

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

警告 安全上の重要事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

これらの注意事項を保管しておいてください。

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、mds-docfeedback@cisco.comよりご連絡ください。ご協力をよろしくお願いいたします。

関連資料

Cisco MDS 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/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/series.html

ドキュメント ロードマップ

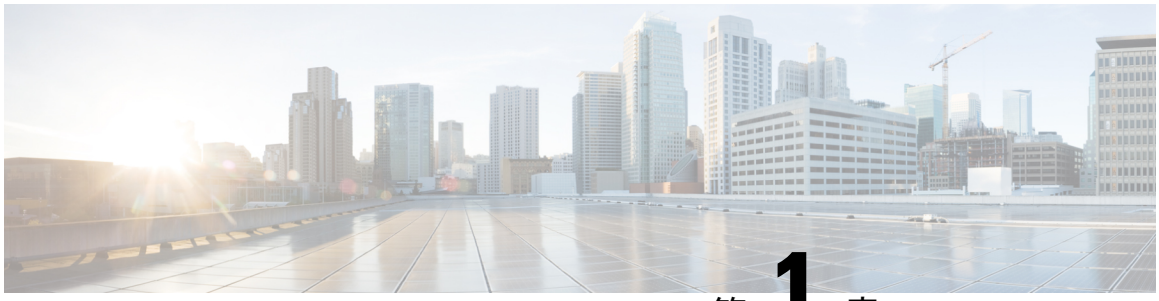
https://www.cisco.com/c/en/us/td/docs/storage/san_switches/mds9000/roadmaps/rel90.html

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。
- 重要な技術によって求めるビジネス成果を得るには、Cisco Services [英語] 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 [英語] 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ク、トレーニング、認定関連の出版物を入手するには、Cisco Press [英語] 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。

シスコのバグ検索ツール

Cisco 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 Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。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。



第 1 章

新機能および変更された機能に関する情報

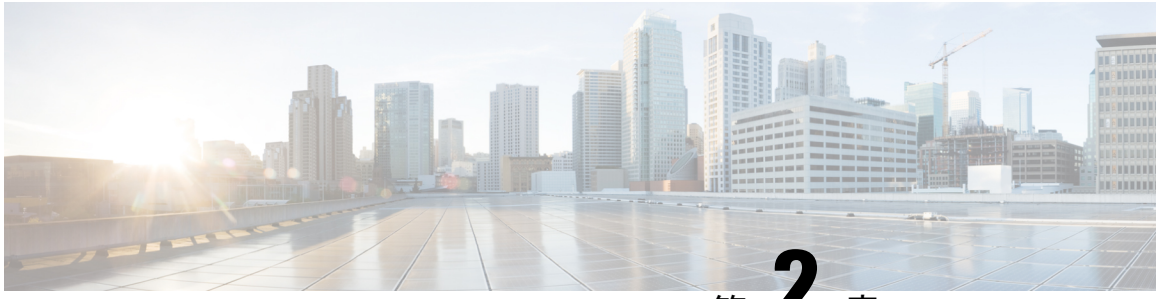
• 新機能および変更された機能に関する情報 （1 ページ）

新機能および変更された機能に関する情報

機能名	リリース	説明	参照先
FCIP XRC 統計情報	9.4(3)	FCIP に使用される IP ストレージ インターフェイスのイーサネット MAC 統計情報を追加	FCIP リンクの構成
tcp min-retransmit-time *milliseconds*	9.4（2）	デフォルトの TCP 最小再送信時間が 200 ミリ秒から 50 ミリ秒に変更されました。 TCP 最小再送信時間の範囲が、200 ～ 5000 ミリ秒から 50 ～ 5000 ミリ秒に変更されました。	FCIP リンクの構成
単一の FCIP トンネルでの最大スループット。	9.3(1)	単一の FCIP トンネルでの最大スループット • Cisco MDS 9220i では 10Gbps です。 • 40 Gbps IPS ポートの場合、4 つの FCIP トンネルが個別の VLAN サブインターフェイスに作成されている場合、最大スループットは 34.6 Gbps です。 • は 7 Gbps です。最大のパフォーマンスを得るには、10 Gbps IPS ポートで 2 つの fcip トンネルを作成します。	Cisco MDS 24/10 ポート SAN 拡張モジュールおよび M9220i スイッチで最大のパフォーマンスの FCIP リンクの構成

新機能および変更された機能に関する情報

機能名	リリース	説明	参照先
Cisco MDS 9220i の 25 Gbps IPS ポート速度のサポートが導入されました。	9.3(1)	25 Gbps の速度は、Cisco MDS NX-OS リリース 9.3(1) でサポートされます。	Cisco MDS 9220i スイッチでの IPS ポートの構成



第 2 章

概要

Cisco MDS 9000 NX-OS ソフトウェアは、FCIP、ストレージエリア ネットワーク（SAN）拡張チューナ、iSCSI、IP ストレージ、IPv4、および IPv6 などの機能を単一プラットフォームに搭載しています。これらの IP サービスは、ストレージ ネットワーク内の全スイッチに設定情報を配信することによって、SANプロビジョニングを簡素化します。仮想ルータ冗長プロトコル（VRRP）は、あるポートから別のポートへの接続のフェールオーバーを可能にすることによって、iSCSI および FCIP 接続の IP ネットワークの可用性を増大させます。IP ネットワークの可用性の増大により、ある IP サービス ポートから、ローカルまたは別の Cisco MDS 9000 スイッチにある別の IP サービス ポートへ、iSCSI ボリュームのフェールオーバーを容易に行うことができます。

- 概要 （3 ページ）

概要

この章は、次の項で構成されています。

- Fibre Channel over IP プロトコル （3 ページ）
- SAN 拡張チューナー （4 ページ）
- Internet Small Computer Systems Interface （4 ページ）
- IP サービス （4 ページ）
- IP ストレージ （4 ページ）
- IPv4 と IPv6 （5 ページ）

Fibre Channel over IP プロトコル

Fibre Channel over IP Protocol（FCIP）は、ローカル ストレージ エリア ネットワーク（SAN）からリモート SAN（SAN アイランド）にファイバ チャネル データを転送することによって、リモート SAN アイランドを透過的に接続します。FCIP 接続の IP ネットワーク可用性は、仮想ルータ冗長プロトコル（VRRP）や Quality of Service（QoS）などの機能を使用することによって増大させることができます。FCIP は、順序が乱れた配信の問題への対応、ジャンボ フレー

ムのサポート、トラフィック シェーピングの実行、TCP 最適化の実行を行う拡張を通じて、ワイヤ パフォーマンスに対して最適化することができます。

FCIP の構成の詳細については、FCIP の設定 （7 ページ） を参照してください。

SAN 拡張チューナー

SAN 拡張チューナー（SET）機能は、Small Computer System Interface（SCSI）入出力コマンドを生成しトラフィックを特定の仮想ターゲットに振り分けることにより、FCIP パフォーマンスの最適化を図ります。SET は、入出力/秒および入出力遅延の結果を報告します。この情報は、最大限の FCIP スループットを達成するために必要な同時入出力数を決定するのに役立ちます。

SAN 拡張チューナの設定の詳細については、SAN Extension Tuner の設定 （67 ページ）を参照してください。

Internet Small Computer Systems Interface

Internet Small Computer Systems Interface（iSCSI）機能により、IP ホストがファイバ チャネル ストレージにアクセスすることができます。この機能を使用して、IP ネットワーク内の iSCSI ホストとファイバ チャネル SAN 内のファイバ チャネル ストレージ装置との間の iSCSI 要求および応答をルーティングすることができます。ファイバ チャネル ストレージ デバイスは、Cisco MDS 9000 ファミリ スイッチのファイバ チャネル インターフェイスからアクセス可能です。

iSCSI の構成の詳細については、iSCSI の構成 （81 ページ） を参照してください。

IP サービス

IP サービス モジュールにより、イーサネット インフラストラクチャを使用してストレージ ネットワークを拡張できます。Cisco MDS 9000 ファミリ スイッチは、イーサネットおよびファイバ チャネル インターフェイス間の IP トラフィックをルーティングします。VSAN 間でトラフィックをルーティングするには、IP スタティック ルーティング機能を使用します。Fabric Manager および Device Manager を使用した IP ルート。NX-OS リリース 4.2(1) 以降、新規 IP ルート作成中の選択に CPP インターフェイスも使用できます。

IP サービスの設定の詳細については、IP サービスの設定 （211 ページ）を参照してください。

IP ストレージ

IP ストレージ（IPS）サービス モジュールにより、オープン規格の FCIP プロトコルを使用して、超長距離の SAN アイランドの相互接続が可能になります。IPS ポートを搭載したファイバ チャネル モジュールおよび MSM-18/4 モジュールにより、FCIP および iSCSI 機能が使用できるようになります。両方のモジュールは、Cisco MDS 9000 ファミリにシームレスに統合され、VSAN、セキュリティ、トラフィック管理など、他のスイッチング モジュールで使用可能なフルレンジの機能をサポートしています。

IP ストレージの設定の詳細については、IP ストレージ サービスの設定 （233 ページ）を参照してください。

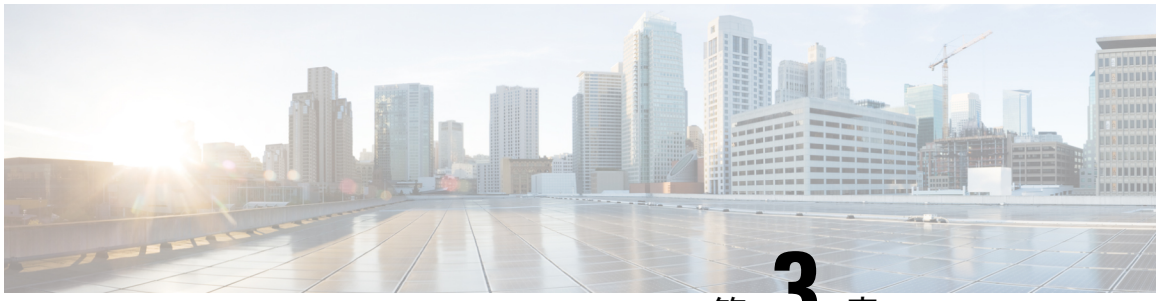
IPv4 と IPv6

Cisco MDS 9000 NX-OS ソフトウェアは、ギガビット イーサネット インターフェイス上で IP バージョン 4（IPv4）および IP バージョン 6（IPv6）プロトコルをサポートしています。IPv6 のアーキテクチャは、エンドツーエンドのセキュリティ、Quality Of Service（QoS）、およびグローバルに一意なアドレスなどのサービスを提供すると同時に、既存の IPv4 ユーザーが簡単に IPv6 へ移行できるように設計されています。IPv4 および IPv6 のデュアル スタック方法により、Cisco MDS 9000 ファミリ スイッチは旧来の IP ネットワーク、両バージョンの移行期のネットワーク、および IPv6 データ ネットワークに接続することができます。

次のテーブルに、Cisco MDS 9250i マルチサービス ファブリック スイッチ IPS の機能と、以前のプラットフォーム（SSN16 および 18+4）を示します。

ライン カード	物理ポート速度	物理ポート数	FCIP トンネルの数	各 IPS/ギガビット イーサネット インターフェイスに対する FCIP トンネル バウンドの数	iSCSI ポートの数
Cisco MDS 24/10 SAN 拡張モジュールのポート	1/10 Gbps	8	24	3	該当なし
Cisco MDS 9250i マルチサービス ファブリック スイッチ	1/10 Gbps	2	12	6	2
SSN-16	1 Gbps	16	48	3	16
18+4	1 Gbps	4	12	3	4

概要



第 3 章

FCIP の設定

Cisco MDS 9000 ファミリの IP ストレージ（IPS）サービスは、オープン規格の IP ベース テクノロジーを使用することによって、ファイバ チャネル SAN の到達距離を延長します。スイッチは Fibre Channel over IP（FCIP）を使用して、別々の SAN アイランドを接続できます。

（注） FCIP は、Cisco MDS 9700 シリーズ スイッチの Cisco 24/10 ポート SAN 拡張モジュール、MDS 9250i マルチサービス ファブリック スイッチ、および MDS 9220i ファブリック スイッチの IPS ポートを備えたファイバ チャネル モジュールでサポートされます。

この章は、次の項で構成されています。

- 機能情報 （7 ページ）
- FCIP の概要 （8 ページ）
- FCIP の設定 （13 ページ）
- FCIP プロファイルの詳細設定 （19 ページ）
- FCIP インターフェイスの詳細構成 （27 ページ）
- 拡張 FCIP 機能 （39 ページ）
- 最大限のパフォーマンスを引き出すための FCIP リンクの構成 （53 ページ）
- FCIP 構成の確認 （65 ページ）
- FCIP パラメータのデフォルト設定 （65 ページ）

機能情報

このセクションには、リリースの新機能と更新機能が一時的にについて説明します。

表 *1 :* 機能情報の表

機能	リリース	説明
FCIP XRC 統計情報	9.4(3)	FCIP に使用される IP ストレージ インターフェイスのイーサネット MAC 統計情報を追加

機能	リリース	説明
tcp min-retransmit-time *milliseconds*	9.4（2）	デフォルトの TCP 最小再送信時間が 200 ミリ秒から 50 ミリ秒に変更されました。 TCP 最小再送信時間の範囲が、200 ～ 5000 ミリ秒から 50 ～ 5000 ミリ秒に変更されました。
FCIP	8.5(1)	Cisco MDS 9220i ファブリック スイッチにサポートが追加されました。
show interface fcip *fcip-id*	8.4（2）	show interface fcip *fcip-id* コマンドの出力が、各 TCP 接続の RTT 統計情報をサポートするように変更されました。
OBFL ログの最大再送信しきい値	8.4(1)	TCP 再送信レートを OBFL にロギングするためのしきい値を構成するために、次のコマンドが導入されました。 **tcp logging onboard tcp-retransmission-threshold** 次の新しいコマンドが導入されました。**tcp obfl max-retransmissions_pkt_thresh** *value*
OBFL ログの最大再送信しきい値	8.2(1)	この機能では、用 OBFL にログインして TCP 再送信速度しきい値を構成することができます。 次の新しいコマンドが導入されました。**tcp obfl max-retransmissions_pkt_thresh** *value*

FCIP の概要

Fibre Channel over IP Protocol（FCIP）は、地理的に分散したファイバ チャネル SAN アイランドの IP ローカルエリア ネットワーク（LAN）、メトロポリタンエリア ネットワーク（MAN）、およびワイドエリア ネットワーク（WAN）を介して透過的に接続するトンネリング プロトコルです。スイッチは Fibre Channel over IP（FCIP）を使用して、別々の SAN アイランドを接続できます。（次の図を参照してください）。

図 *1: FCIP* によって接続されたファイバ チャネル *SAN*

FCIP はネットワーク層トランスポートとして TCP を使用します。TCP ヘッダーに DF ビットが設定されます。

FCIP プロトコルの詳細については、http://www.ietf.org にアクセスして IP ストレージに関する IETF 規格を参照してください。さらに、http://www.t11.org にアクセスして、スイッチ バックボーン接続に関するファイバ チャネル規格を参照してください（FC-BB-2 を参照）。

このセクションは、次のトピックで構成されています。

FCIP の概念

FCIP 用の IPS ポートを搭載した ファイバ チャネルを構成するには、以下の概念の基本的な理解が必要です。

- FCIP および VE ポート （9 ページ）
- FCIP リンク （10 ページ）
- FCIP Profiles （10 ページ）
- FCIP インターフェイス （11 ページ）

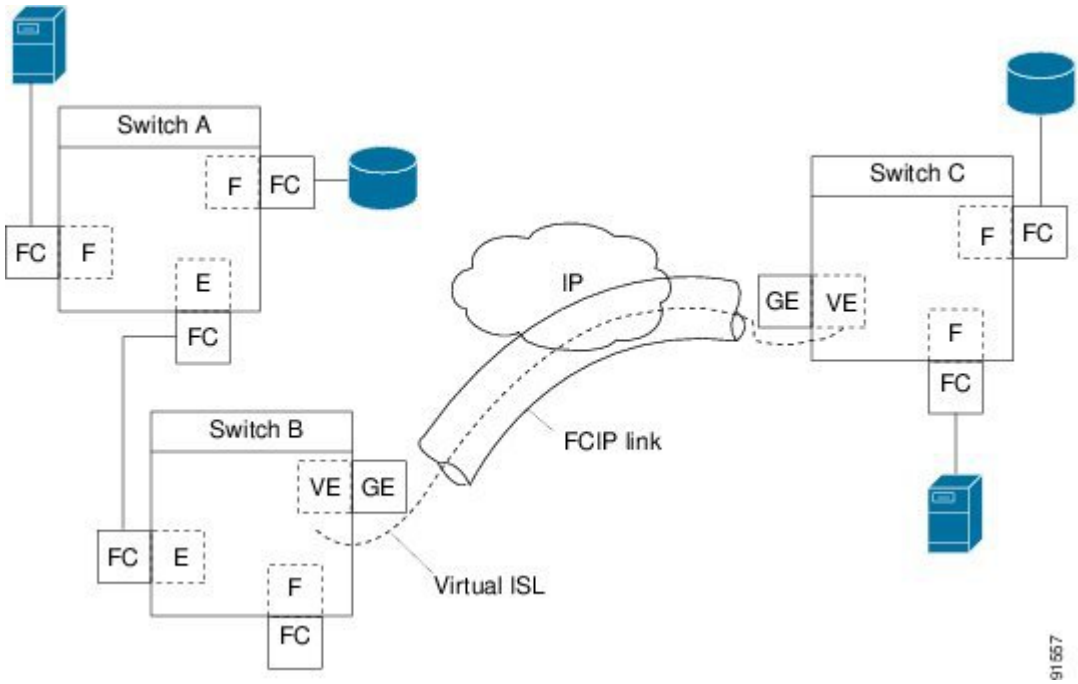
FCIP および VE ポート

下の図に、ファイバ チャネル Inter-Switch Link（ISL）および Cisco の拡張 ISL（EISL）に関する FCIP の内部モデルを示します。

FCIP 仮想 E（VE）ポートは、ファイバチャネルではなく FCIP を介して転送される点を除き、標準ファイバ チャネル E ポートとまったく同様に機能します。唯一の要件は、VE ポートの他端を別の VE ポートにすることです。

仮想 ISL は FCIP リンクを介して確立され、ファイバ チャネル トラフィックを転送します。対応する各仮想 ISL は、両端に E ポートまたは TE ポートが接続されたファイバ チャネル ISL と似ています（下の図を参照）。

図 *2 : FCIP* リンクおよび仮想 *ISL*



詳細については、E ポートの構成 （32 ページ）を参照してください。

FCIP リンク

（注） 順序どおり配信（IOD）は 、WA および TA が有効になっている FCIP ISL ではサポートされません。

FCIP リンクは、2 つの FCIP リンク エンドポイントを結ぶ 1 つまたは複数の TCP 接続で構成されます。各リンクはカプセル化されたファイバ チャネル フレームを伝達します。

FCIP リンクが起動すると、FCIP リンクの両端の VE ポートは仮想ファイバ チャネル（E）ISL を作成し、E ポート プロトコルを開始して（E）ISL を起動します。

デフォルトでは、どの Cisco MDS 9000 ファミリ スイッチの FCIP 機能も、FCIP リンクごとに TCP 接続を 2 つ作成します。

- 一方の接続はデータ フレーム用です。
- もう一方の接続はファイバ チャネル制御フレーム、つまりスイッチ/スイッチ プロトコル フレーム（すべてクラス F）専用です。これにより、すべての制御フレームの遅延が軽減されます。

IPS ポートを搭載したファイバチャネル モジュールで FCIP を有効にするには、FCIP プロファイルおよび FCIP インターフェイス（インターフェイス FCIP）を構成する必要があります。

2 つのピア間に FCIP リンクが確立されます。VE ポート初期化動作は、通常の E ポートと同じです。この動作はリンクが FCIP であるか、または純粋なファイバ チャネルであるかに関係なく、E ポート検出プロセス（ELP、ESC）に基づいて決まります。

FCIP リンクが確立されると、すべてのスイッチ間通信（ドメイン管理、ゾーン、VSAN など）で、VE ポートの動作が E ポートの動作と同じになります。ファイバ チャネル レイヤでは、VE および E ポートの動作はすべて同じです。

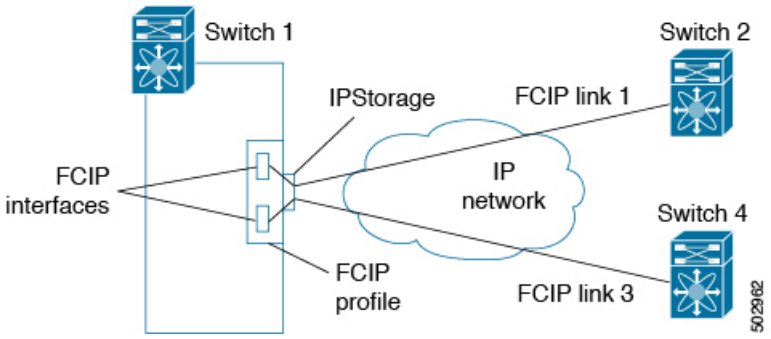
FCIP Profiles

FCIP プロファイルには、ローカル IP アドレスおよび TCP パラメータに関する情報が含まれます。プロファイルで定義される情報は、次のとおりです。

- ローカル接続ポイント（IP アドレスおよび TCP ポート番号）
- このプロファイルを使用するすべての FCIP リンクの基礎となる TCP 接続の動作

FCIP リンクが終端する IPStorage ポートは、FCIP プロファイルのローカル IP アドレスによって決まります（下の図を参照）。

図 *3* : *FCIP* プロファイルおよび *FCIP* リンク



FCIP インターフェイス

FCIP インターフェイスは FCIP リンクおよび VE ポート インターフェイスのローカル エンド ポイントです。すべての FCIP および E ポート パラメータは、FCIP インターフェイスに対するコンテキスト内で設定されます。

FCIP パラメータの構成は次のとおりです。

- FCIP プロファイルでは、FCIP リンクを開始する IPStorage ポートを判別し、TCP 接続動作を定義します。
- ピア情報。
- FCIP リンクの TCP 接続数。
- E ポート パラメータ：トランキング モードおよびトランク許可 VSAN リスト。

FCIP ハイ アベイラビリティ ソリューション

FCIP 設定で使用できるハイ アベイラビリティ ソリューションは、次のとおりです。

ファイバ チャネル ポート チャネル

FCIP インターフェイスで構成されるポート チャネルは、ファイバ チャネル ポート チャネルと同じように動作します。ファイバ チャネル スイッチ間のリンク冗長性の利点は、ネイティブ FC ポート チャネルと同じです。FCIP レベルより下位で、FCIP リンクは IPStorage ポート上で動作できます。リンクはファイバ チャネル レイヤに対して完全に透過的です。

ファイバチャネル ポート チャネル（FCIP リンクが属する場合もある）では、互換性チェックが正常である限り、ファイバチャネル ポート チャネル内で組み合わせられる（E）ISL リンクに制約はありません。

（注） Cisco MDS 48 ポート 64 Gbps ファイバチャネル スイッチング モジュール（DS-X9748-3072K9）のメンバーでポート チャネルが構成されている場合、IOD が構成され、ポート チャネルのメンバーが追加、削除、またはフラップされます。

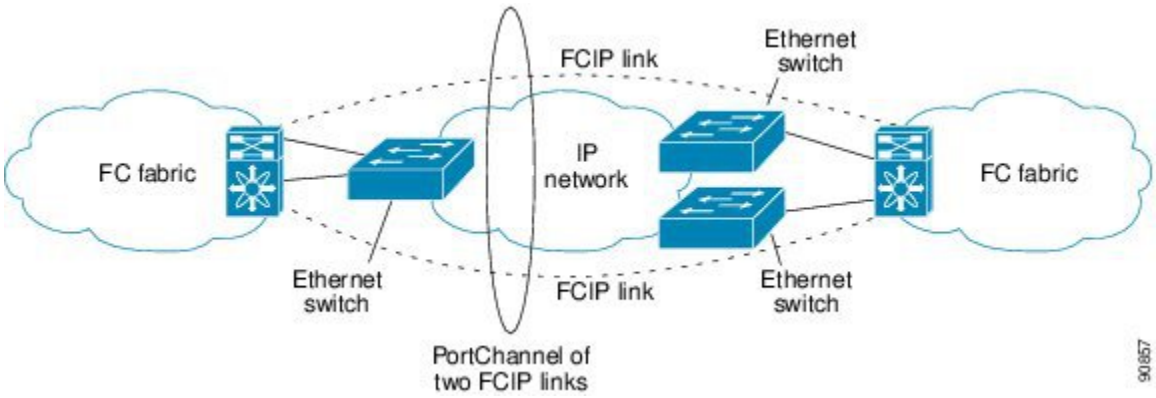
詳細については、「Cisco Fabric Manager インターフェイス構成ガイド」および「Cisco MDS 9000 シリーズ NX-OS インターフェイス構成ガイド」を参照してください。

ファイバ チャネル ポート チャネルに組み込むことのできるファイバ チャネル ポートの最大数は 16 です。

ファイバ チャネル ポート チャネルを構成するには、『Cisco MDS 9000 ファミリ NX-OS インターフェイス構成ガイド』および『Cisco Fabric Manager インターフェイス構成ガイド』を参照してください。

次の図に、ポート チャネルベース のロード バランシング構成例を示します。この設定を実行するには、SAN アイランドごとに 2 つの IP アドレスが必要です。このソリューションにより、リンク障害が解決されます。

図 *4:* ポート チャネル ベースのロード バランシング



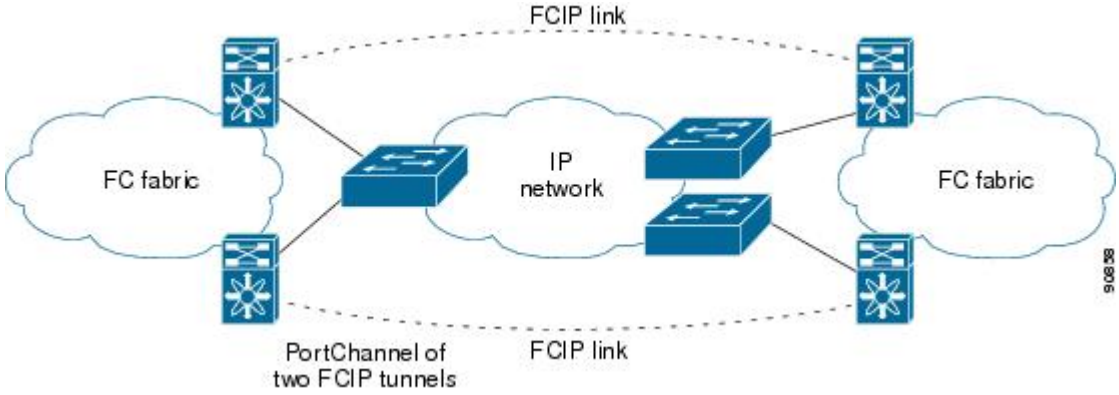
ファイバ チャネル ポート チャネル ソリューションは、次の特性によって他のソリューションから区別されます。

- バンドル全体が 1 つの論理（E）ISL リンクになります。
- ポート チャネル内のすべての FCIP リンクが、2 つの同じスイッチ間に終端配置されている必要があります。
- ファイバ チャネル トラフィックはポート チャネル内の FCIP リンク間でロード バランシングされます。

FSPF

下の図では、 FPSF ベース ロード バランシング構成例を示します。この設定では、SAN アイランドごとに 2 つの IP アドレスが必要です。この設定により、IP および FCIP リンクの障害が解決されます。

図 *5 : FSPF* ベースのロード バランシング



FSPF ソリューションは、次の特性によって他のソリューションから区別されます。

- 各 FCIP リンクは、それぞれ異なる（E）ISL です。
- FCIP リンクは、2 つの SAN アイランド間の複数のスイッチに接続できます。
- ファイバ チャネル トラフィックは FCIP リンク間でロード バランシングされます。

FCIP の設定

ここでは、FCIP の設定方法について説明します。

FCIP の有効化

Fibre Channel over IP Protocol（FCIP）は、地理的に分散したファイバ チャネル SAN アイランドの IP ローカルエリア ネットワーク（LAN）、メトロポリタンエリア ネットワーク（MAN）、およびワイドエリア ネットワーク（WAN）を介して透過的に接続するトンネリング プロトコルです。

FCIP 機能の設定を開始するには、ファブリック内の目的のスイッチ上で FCIP を明示的にイネーブルにする必要があります。デフォルトでは、この機能は Cisco MDS 9000 ファミリのすべてのスイッチでディセーブルになっています。

FCIP 機能に関する構成および確認の操作コマンドを実行できるのは、スイッチ上で FCIP が有効になっている場合のみです。この機能をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

デフォルトで、Cisco MDS 9700 シリーズ スイッチ、MDS 9220i スイッチ、および 9220i スイッチには SAN Extension over IP パッケージ ライセンスが同梱されています。

参加させるスイッチの FCIP を有効にするには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	構成モードに入ります。
ステップ 2	switch(config)# **feature fcip**	スイッチ上で FCIP を有効にします。
ステップ 3	（任意） switch(config)# **no feature fcip**	スイッチ上の FCIP を無効にします（デフォルト）。

FCIP の基本構成

FCIP Wizard を使用して FCIP リンクを作成したあと、これらのリンクのパラメータを変更することが必要となる場合があります。変更が必要なのは、FCIP プロファイル、FCIP リンク パラメータなどです。

- Cisco MDS 9220i スイッチの場合、各 1 Gbps または 10 Gbps IPStorage インターフェイスには一度に 3 つの FCIP リンクを構成でき、40 Gbps IPStorage インターフェイスには一度に 4 つの FCIP リンクを構成できます。
- Cisco MDS 9250i スイッチ間では、各 IPStorage インターフェイスに FCIP リンクを一度に 6 つ構成できます。
- Cisco MDS 24/10 ポート SAN 拡張モジュールの場合、各 1 Gbps または 10 Gbps IPStorage インターフェイスには一度に 3 つの FCIP リンクを構成でき、40 Gbps IPStorage インターフェイスには一度に 4 つの FCIP リンクを構成できます。

（注） IPsec および IKE を使用する場合、IPS ポートを使用するファイバ チャネル モジュールの各 IPStorage インターフェイスは、独自の IP サブネットで構成する必要があります。同じ IP サブネットの IP アドレスまたはネットワークマスクで複数の IPStorage インターフェイスが構成される場合、IKE パケットは正しい IPS ポートに送信されず、IPSec リンクは起動しません。

（注） Cisco MDS 9220i スイッチでは、IPsec および NAT を使用して FCIP を構成できます。

FCIP リンクを構成するには、両方のスイッチで次の手順を実行します。

手順

ステップ 1 IPStorage インターフェイスを構成します。

『*Cisco MDS 9000* ファミリ *NX-OS IP* サービス構成ガイド』を参照してください。

ステップ 2 FCIP プロファイルを作成してから、IPStorage インターフェイスの IP アドレスをプロファイルに割り当てます。

ステップ 3 FCIP インターフェイスを作成し、インターフェイスにプロファイルを割り当てます。

ステップ 4 FCIP インターフェイスのピア IP アドレスを設定します。

ステップ 5 インターフェイスをイネーブルにします。

FCIP プロファイルの作成

FCIP プロファイルを作成するには、IPStorage インターフェイスまたはサブインターフェイスのローカル IP アドレスを FCIP プロファイルに割り当てる必要があります。インターフェイスには IPv4 または IPv6 のアドレスを割り当てることができます。下の図に、構成例を示します。

図 *6* : 各 *IPStorage* インターフェイスへのプロファイルの割り当て

手順

ステップ 1 上の図のスイッチ 1 の FCIP プロファイルを作成するには、次のステップに従います。

a) switch1# **configure terminal**

コンフィギュレーション モードに入ります。

b) switch1(config)# **fcip profile 10**

FCIP 接続のプロファイルを作成します。有効な範囲は 1 ～ 255 です。

c) switch1(config-profile)# **ip address 10.100.1.25**

プロファイル（10）に IPStorage インターフェイス（3/1）の IPv4 アドレスを関連付けます。

d) switch1# **show fcip profile**

FCIP プロファイル情報を表示します。

ステップ 2 上の図のスイッチ 2 の FCIP プロファイルを作成するには、次のステップに従います。

a) switch2# **configure terminal**

構成モードに入ります。

b) switch2(config)# **fcip profile 20**

FCIP 接続のプロファイルを作成します。

c) switch2(config-profile)# **ip address 10.1.1.1**

プロファイル（20）に IPStorage インターフェイスの IPv4 アドレスを関連付けます。

d) switch2# **show fcip profile**

FCIP プロファイル情報を表示します。

FCIP プロファイル情報の表示

FCIP プロファイルの概要の表示

```
switch# show fcip profile

-------------------------------------------------------------------------------
ProfileId Ipaddr   TcpPort
-------------------------------------------------------------------------------
1         20.1.1.1 3225
2         20.1.1.1 2000
3         20.1.1.1 3000
4         20.1.1.1 4000
5         20.1.1.1 5000
6         20.1.1.1 6000
7         30.1.1.1 3225
8         31.1.1.1 3225
9         32.1.1.1 3225
10        33.1.1.1 3225
11        34.1.1.1 3225
12        35.1.1.1 3225
```

詳細な FCIP プロファイル情報の表示

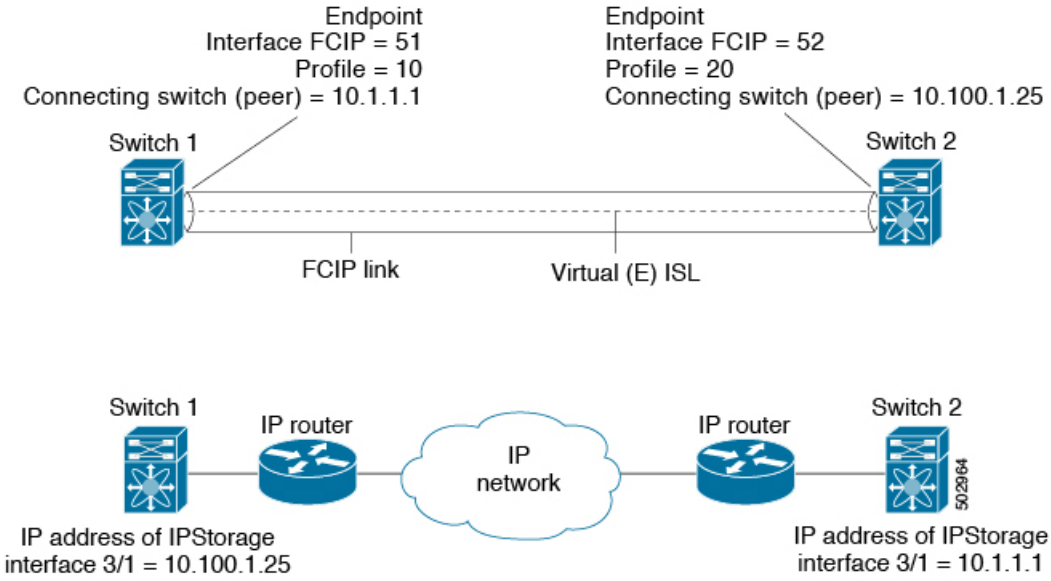
```
switch# show fcip profile 1
FCIP Profile 1
Internet Address is 20.1.1.1 (interface IPStorage1/1)
Tunnels Using this Profile: fcip1
Listen Port is 3225
TCP parameters
SACK is enabled
PMTU discovery is enabled, reset timeout is 3600 sec
Keep alive is 60 sec
Minimum retransmission timeout is 200 ms
Maximum number of re-transmissions is 4
Send buffer size is 16384 KB
Maximum allowed bandwidth is 5000000 kbps
Minimum available bandwidth is 4000000 kbps
Configured round trip time is 1000 usec
Congestion window monitoring is enabled, burst size is 50 KB
Auto jitter detection is enabled
```

FCIP リンクの作成

FCIP リンクのエンドポイントを 2 つ作成すると、2 つの IPS ポート間に FCIP リンクが確立されます。ピア IP アドレスによって、リモート FCIP エンドポイントのアドレスを指定します。これにより、FCIP インターフェイスが有効になると、そのピア スイッチへの FCIP リンクを作成できます。

下の図に、FCIP リンクの構成例を示します。

図 *7*: 各 *IPStorage* インターフェイスへのプロファイルの割り当て



手順

ステップ 1 スイッチ 1 の FCIP リンク エンドポイントを作成するには、次のステップを実行します。

a) switch1# **configure terminal**

コンフィギュレーション モードに入ります。

b) switch1(config)# **interface fcip 51**

FCIP インターフェイス（51）を作成します。

c) switch1(config-if)# **use-profile 10**

FCIP インターフェイスにプロファイル（10）を割り当てます。

d) switch1(config-if)# **peer-info ipaddr 10.1.1.1**

ピアの IPv4 アドレス情報（スイッチ 2 の場合は 10.1.1.1）を FCIP インターフェイスへ割り当てます。

e) switch1(config-if)# **no shutdown**

インターフェイスを有効にします。

ステップ 2 スイッチ 2 の FCIP リンク エンドポイントを作成するには、次のステップを実行します。

a) switch2# **configure terminal**

構成モードに入ります。

b) switch2(config)# **interface fcip 52**

FCIP インターフェイス（52）を作成します。

c) switch2(config-if)# **use-profile 20**

FCIP インターフェイスにプロファイル（20）を割り当てます。

d) switch2(config-if)# **peer-info ipaddr 10.100.1.25**

ピアの IPv4 アドレス情報（スイッチ 1 の場合は 10.100.1.25）を FCIP インターフェイスへ割り当てます。

e) switch2(config-if)# **no shutdown**

インターフェイスをイネーブルにします。

FCIP MAC 統計情報の表示

次に、Cisco MDS 9000 NX-OS リリース 9.4(3) から FCIP に使用される IP ストレージ インターフェイスのイーサネット MAC 統計情報を表示する例を示します。

```
switch# show interface IPStorage 1/1 counters detailed
IPStorage1/1
Rate Stats:
Rx 5 minutes input rate bits/sec: 0
Rx 5 minutes input rate bytes/sec: 0
Rx 5 minutes input rate packets/sec: 0
Tx 5 minutes input rate bits/sec: 0
Tx 5 minutes input rate bytes/sec: 0
Tx 5 minutes input rate packets/sec: 0
Total Stats:

Rx packets input: 0
Rx bytes: 0
Rx multicast frames: 0
Rx broadcast frames: 0
Rx errors: 0
Rx queue drops: 0
Rx if-down drops: 0
Rx RED drops: 0
Rx bad ether type drops: 0
Rx bad protocol drops: 0
Tx packets output: 0
Tx bytes: 0
Tx underruns: 0
Tx multicast frames: 0
Tx broadcast frames: 0
Tx errors: 0
Tx collisions: 0
Tx ARP drops: 0
Tx if-down drops: 0
```

```
MAC Error Stats
Rx packets with FCS or align errors: 0
Rx packets with length < min: 0
Rx packets with length < min & FCS error: 0
Rx packets with length > max: 0
Rx packets with length > max & FCS error: 0
Rx packets with PCI error: 0
Rx packets with GMX/SPX/PCI error: 0
Rx packets dropped by RED buffer exhaustion: 0
Rx free buffers went below RED threshold count: 0
Rx L2 multicast packets: 0
Rx L2 broadcast packets: 0
Rx packets dropped by dest MAC filter: 0
Rx packets dropped due to a full receive FIFO: 0
Rx total MAC errors: 0
Tx packets dropped in PKO queue: 0
Tx packets sent with single collision: 0
Tx packets sent with multiple collisions: 0
Tx packets dropped due to excessive collisions: 0
Tx packets delayed count: 0
Tx total MAC errors: 0
```

FCIP プロファイルの詳細設定

FCIP の基本設定では、ローカル IP アドレスを使用して FCIP プロファイルを設定します。FCIP プロファイルの構成の一部として、ローカル IP アドレスおよびローカル ポート以外に、その他の TCP パラメータを指定できます。

ここでは、次の内容について説明します。

（注） FCIP 構成オプションには、`switch (config-` profile`)#` サブモード プロンプトからアクセスできます。

TCP リスナー ポートの構成

手順

ステップ 1 TCP リスナー ポートを構成するには、次のステップを実行します。

a) switch# **configure terminal**

構成モードに入ります。

b) switch(config)# **fcip profile 20**

プロファイルがまだ存在していない場合はプロファイルを作成し、プロファイル コンフィギュレーション サブモードを開始します。有効な範囲は 1 ～ 511 です。

FCIP のデフォルト TCP ポートは 3225 です。このポートを変更するには、**port** コマンドを使用します。

ステップ 2 デフォルト FCIP ポート番号（3225）を変更するには、次の手順を実行します。

a) switch(config-profile)# **port 5000**

ローカル ポート番号（5000）にプロファイルを関連付けます。

b) switch(config-profile)# **no port**

デフォルトの 3225 ポートに戻します。

TCP パラメータの構成

このセクションで説明された TCP パラメータを設定することにより、スイッチ内の TCP 動作を制御できます。

（注） FCIP を WAN リンクを介して伝送する場合、デフォルトの TCP 設定が適さないことがあります。このような場合は、TCP パラメータ（具体的には、帯域幅、往復時間、および CWM バースト サイズ）を変更することによって、FCIP WAN リンクを調整することを推奨します。

このセクションは、次のトピックで構成されています。

最小 再送信タイムアウト

再送信を行うまでに TCP が待機する最小時間を制御できます。デフォルトでは、Cisco MDS NX-OS リリース 9.4(2) 以降のリリースでは、値は 50 ミリ秒であり、Cisco MDS NX-OS リリース 9.4(2) より前では値は 200 ミリ秒です。

最小再送信時間を構成するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config-profile)# **tcp min-retransmit-time 500**	TCP 接続の最小 TCP 再送信時間を 500 ミリ秒に指定します。 Cisco MDS NX-OS リリース 9.4(2) 以降のリリースでは、デフォルトは 50 ミリ秒で、範囲は 50 ～ 5000 ミリ秒です。 Cisco MDS NX-OS リリース 9.4(2) より前では、デフォルト値は 200 ミリ秒で、範囲は 200 ～ 5000 ミリ秒です。
ステップ 2	（任意） switch(config-profile)# **no tcp min-retransmit-time 500**	最小 TCP 再送信時間を工場出荷時のデフォルトに戻します。

	コマンドまたはアクション	目的
		Cisco MDS NX-OS リリース 9.4(2) 以降のリリースでは、工場出荷時のデフォルトは 50 ミリ秒です。 Cisco MDS NX-OS リリース 9.4(2) より前では、工場出荷時のデフォルト値は 200 ミリ秒です。

Keepalive Timeout

FCIP リンクが動作しているかどうかを TCP 接続で確認するインターバルを設定できます。この確認によって、トラフィックがない場合でも、FCIP リンク障害が迅速に検出されます。

TCP接続のアイドル状態が指定の時間を超えると、接続がアクティブかどうかを確認するために、キープアライブ タイムアウト パケットが送信されます。キープアライブ タイムアウト機能では、FCIP リンク障害の検出にかかる時間を調整できます。

接続のアイドル状態が続く最初のインターバルを設定できます（60秒がデフォルト）。構成されたインターバルの間、接続がアイドル状態だった場合は、8つのキープアライブ プローブが 1 秒間隔で送信されます。8 つのプローブに応答がなく、その間も接続のアイドル状態が続いた場合は、FCIP リンクが自動的に終了します。

（注） 変更できるのは、（接続がアイドル状態である）最初のインターバルだけです。

最初のキープアライブ タイムアウト インターバルを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config-profile)# **tcp keepalive-timeout 120**	TCP 接続のキープアライブ タイムアウト インターバルを秒単位で指定します（120）。範囲は1～7200秒です。
ステップ 2	（任意） switch(config-profile)# **no tcp keepalive-timeout 120**	キープアライブ タイムアウトインターバルをデフォルトの 60 秒に戻します。

最大再送信回数

TCP が接続終了を決定するまでに、パケットを再送信する最大回数を指定できます。

最大再送信回数を構成するには、次のステップを実行します。

手順

ステップ 1 switch(config-profile)# **tcp max-retransmissions 6**

最大再送信回数（6）を指定します。指定できる再送信回数の範囲は 1 ～ 8 回です。

ステップ 2 （任意） switch(config-profile)# **no tcp max-retransmissions 6**

デフォルトの 4 回の再送信に戻します。

OBFL ログの最大再送信しきい値

FCIP リンクは、ピア ツー ピア TCP セッションを使用します。中継ネットワークが無損失ではなく、フレームをドロップする可能性があるイーサネットであることがよくあります。これらは、TCP の送信者によって自動的に再送信します。エンドのアプリケーションは、ある程度の再送信による遅延を許容できる必要があります。ただし、一部のアプリケーションには、その他のよりも再送信の低い許容値があります。過剰な TCP 再送信のイベントは、トラブルシューティングに役立つOBFLにログインした可能性があります。ロギングをトリガする再送信レートのしきい値を構成できます。この再送信レートは、FCIP プロファイルごとに測定されます。

FCIP プロファイルごとの OBFL 再送信レートを構成するには、次のステップに従います。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **fcip profile** *profile_id*	プロファイルがまだない場合はプロファイルを作成し、プロファイル コンフィギュレーション サブモードを開始します。範囲は 1 ～ 255 です。
ステップ 3	• `switch(config-profile)# tcp obfl max-retransmissions_pkt_thresh value` • `switch(config-profile)# tcp logging onboard tcp-retransmission-threshold value`	1 分ごとの測定 10000 パケットごとに OBFL、パケットの数は、TCP 再送信速度が再送信のロギングのしきい値を指定します。範囲は 5 ～ 10 です。デフォルト値は 5 です。 Cisco MDS リリース 8.4(1) 以降、 **tcp obfl max-retransmissions_pkt_thresh** *value* コマンドは廃止されました。**tcp logging onboard tcp-retransmission-threshold** *value* コマンドを使用して、OBFL への TCP 再送信レートを構成します。指定できる範囲は 0.01 ～ 0.10 です。デフォルト値は 0.05% です。
ステップ 4	switch# **show logging onboard error-stats**	過剰な FCIP 再送信ログを表示します。

パス MTU

Path MTU（PMTU）は、IP ネットワークにおける FCIP リンクの 2 つのエンドポイント間の最小 MTU です。PMTU ディスカバリは、TCP が PMTU をダイナミックに学習し、最大 TCP セグメントを相応に調整するメカニズムです（RFC 1191）。

デフォルトでは、PMTUディスカバリはすべてのスイッチでイネーブルになり、タイムアウトは 3600 秒です。PMTU の変更によって TCP の最大セグメント サイズを引き下げる場合は、時間がどれだけ経過したら TCP が元の MTU を試行するのか、その時間を reset-timeout で指定します。

PMTU を構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config-profile)# **no tcp pmtu-enable**	PMTU ディスカバリを無効にします。
ステップ 2	switch(config-profile)# **tcp pmtu-enable**	デフォルト値の 3600 秒で PMTU ディスカバリをイネーブル（デフォルト）にします。
ステップ 3	switch(config-profile)# **tcp pmtu-enable reset-timeout 90**	PMTU リセット タイムアウトを 90 秒に指定します。値の範囲は 60 ～ 3600 秒です。
ステップ 4	switch(config-profile)# **no tcp pmtu-enable reset-timeout 600**	PMTU ディスカバリを有効な状態のままにしますが、タイムアウトをデフォルトの 3600 秒に戻します。

選択的確認応答

1 つのウィンドウ内で複数のパケットが失われると、TCP のパフォーマンスが低下する可能性があります。累積確認応答から取得できる情報は限定されているため、TCP の送信側が学習できるのは、1 往復について 1 つの消失パケットに関する情報だけになります。選択的確認応答（SACK）メカニズムによって、TCP伝送時の複数の消失パケットに伴う制限を克服できます。

受信側 TCP は、送信側に SACK アドバタイズメントを送り返します。送信側はその後、欠落したデータ セグメントだけを再送信できます。Cisco MDS 9000 ファミリ スイッチ上では、SACK はデフォルトでイネーブルです。

SACK を構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config-profile)# **no tcp sack-enable**	SACK を無効にします。
ステップ 2	switch(config-profile)# **tcp sack-enable**	SACK を有効にします（デフォルト）。

ウィンドウ管理

最大帯域幅パラメータ、最小使用可能帯域幅パラメータ、および動的に測定されるラウンドトリップ時間（RTT）を使用して、最適な TCP ウィンドウ サイズが自動的に計算されます。

（注） 設定された round-trip-time パラメータによって、TCP 接続のウィンドウ倍率が決まります。このパラメータは、近似値にすぎません。計測された RTT 値によって、ウィンドウ管理のラウンドトリップ時間パラメータが上書きされます。構成された round-trip-time が計測された RTT に対して小さすぎる場合は、ウィンドウ倍率が小さすぎるために、リンクがフルに利用されていない可能性があります。

min-available-bandwidth パラメータと計測された RTT の組み合わせに基づいてしきい値が決定され、このしきい値を下回ると、最小限利用可能な帯域幅で送信できるだけのウィンドウサイズを TCP が積極的に維持します。

max-bandwidth-mbps パラメータと計測された RTT の組み合わせによって、最大ウィンドウサイズが決まります。

（注） 物理リンクで最悪の場合に利用可能な帯域幅と一致するよう最大帯域幅を設定します。このリンクを通過する他のトラフィック（たとえば、他の FCIP リンク、WAN 制限）に注意してください。最大帯域幅とは、総帯域幅からこのリンクを通過する他のトラフィックを引いたものです。

（注） Cisco MDS 9250i マルチサービス ファブリック スイッチでは、TCP 最大帯域幅として最大 5 Gbps まで構成できます。使用可能な最小帯域幅が最大帯域幅の 80% になるようにすることを推奨します。

ウィンドウ管理を構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config-profile)# **tcp max-bandwidth-mbps 900 min-available-bandwidth-mbps 300 round-trip-time-ms 10**	使用可能な最大帯域幅を 900 Mbps に構成し、最小低速開始しきい値を 300 Mbps に構成し、RTT を 10 ミリ秒に構成します。
ステップ 2	（任意） switch(config-profile)# **no tcp max-bandwidth-mbps 900 min-available-bandwidth-mbps 300 round-trip-time-ms 10**	工場出荷時のデフォルトに戻します。FCIP のデフォルトは、最大帯域幅が 1 Gbps、使用可能な最小帯域幅が 500 Mbps、RTT が 1 ミリ秒です。

	コマンドまたはアクション	目的
ステップ 3	switch(config-profile)# **tcp max-bandwidth-kbps 2000 min-available-bandwidth-kbps 2000 round-trip-time-us 200**	使用可能な最大帯域幅を 2000 Kbps に構成し、使用可能な最小帯域幅を 2000 Kbps に構成し、RTT を 200 ミリ秒に構成します。

輻輳モニタリング

輻輳ウィンドウモニタリング（CWM）パラメータを有効にすると、各アイドル期間経過後の輻輳が TCP によってモニタされるようにできます。CWM パラメータによって、アイドル期間経過後の最大許容バーストサイズも決まります。このパラメータはデフォルトでイネーブルになり、バーストサイズは 50 KB です。

次に、帯域幅パラメータと CWM の相互作用、および結果としての TCP 動作について簡単に説明します。

- 前の RTT におけるファイバチャネルトラフィックの平均レートが min-available-bandwidth に RTT を乗じた値に満たない場合、TCP ドロップが発生しないかぎり、バースト全体が min-available-bandwidth レートでただちに送信されます。
- ファイバチャネルトラフィックの平均レートが min-available-bandwidth に RTT を乗じた値よりも大きく、max-bandwidth に RTT を乗じた値よりも小さい場合で、かつ、ファイバチャネルトラフィックが設定された CWM 値よりも小さいバーストサイズで伝送される場合、バースト全体が FCIP によって max-bandwidth レートでただちに送信されます。
- ファイバチャネルトラフィックの平均レートが min-available-bandwidth に RTT を乗じた値よりも大きく、バーストサイズが CWM 値より大きい場合は、バーストの一部分だけが即時送信されます。残りは次の RTT で送信されます。

ソフトウェアでは標準の TCP ルールを使用して、min-available-bandwidth の維持に必要な値よりウィンドウを拡大し、max-bandwidth に近づけます。

ヒント 最適なパフォーマンスを実現するために、この機能は有効のままにしておくことを推奨します。CWM バーストサイズを大きくすると、IP ネットワークでのパケットドロップが増え、TCP パフォーマンスが影響を受ける可能性があります。IP ネットワークに十分なバッファリングがある場合にかぎり、CWM バーストサイズをデフォルトより大きくして、送信遅延の軽減を図ってください。

CWM デフォルト値を変更するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config-profile)# **no tcp cwm**	輻輳モニタリングを無効にします。

	コマンドまたはアクション	目的
ステップ 2	switch(config-profile)# **tcp cwm**	輻輳のモニタリングをイネーブルにし、デフォルトサイズにバーストサイズを設定します。デフォルトのバースト サイズは 50 KB です。
ステップ 3	switch(config-profile)# **tcp cwm burstsize 30**	バーストサイズを 30 KB に変更します。有効な値の範囲は 10 ～ 100 KB です。
ステップ 4	（任意） switch(config-profile)# **no tcp cwm burstsize 25**	CWM 機能を有効な状態のままにし、バースト サイズを工場出荷時のデフォルトに変更します。

FCIP プロファイル情報の表示

Cisco MDS 9250i マルチサービス ファブリック スイッチの FCIP プロファイル情報を表示するには、**show fcip profile** コマンドを使用します。

```
switch# show fcip profile 1
Internet address is 209.165.200.226 (interface IPStorage5/4.101)
Listen Port is 3225
TCP parameters
SACK is enabled
PMTU discovery is enabled, reset timeout is 3600 sec
Keep alive is 60 sec
Minimum retransmission timeout is 200 ms
Maximum number of re-transmissions is 4
Maximum number of obfl re-transmission Thresh is 5
Maximum allowed bandwidth is 5000000 kbps
Minimum available bandwidth is 4000000 kbps
Configured round trip time is 1000 usec
Congestion window monitoring is enabled, burst size is 50 KB
Auto jitter detection is enabled
```

24/10 ポート SAN 拡張モジュールの FCIP プロファイル情報を表示するには、**show fcip profile** コマンドを使用します。

```
switch# show fcip profile 41
FCIP Profile 41
Internet Address is 209.165.200.225 (interface IPStorage5/4.101)
Listen Port is 3225
TCP parameters
SACK is enabled
PMTU discovery is enabled, reset timeout is 3600 sec
Keep alive is 60 sec
Minimum retransmission timeout is 200 ms
Maximum number of re-transmissions is 4
Maximum number of obfl re-transmission Thresh is 6
Maximum allowed bandwidth is 10000000 kbps
Minimum available bandwidth is 8000000 kbps
Configured round trip time is 1000 usec
Congestion window monitoring is enabled, burst size is 50 KB
Auto jitter detection is enabled
```

FCIP インターフェイスの詳細構成

ここでは、ピアとの接続を確立するために、FCIP インターフェイス上で設定できるオプションについて説明します。

ピアの構成

すべての FCIP および E ポート パラメータは、FCIP インターフェイスに対するコンテキスト内で設定されます。FCIP リンクを作成するには、FCIP インターフェースにプロファイルを割り当て、FCIP リンクの両端にある 2つのスイッチでピア情報を構成します。ピア IP スイッチ情報によって、スイッチはそのピア スイッチとの FCIP リンクを開始します。FCIP の基本構成では、ピア IP アドレスを使用してピア情報を構成します。ピア IP アドレス オプションを使用して、ピアと FCI Pリンクを確立できます。このオプションは、FCIP リンクの両端を設定します。IP アドレスとともに、ピア TCP ポートを使用することもできます。

`config-if` サブモードを開始するには、次のステップを実行します。

始める前に

ピア接続を確立するには、まず FCIP インターフェイスを作成し、`config-if` サブモードを開始します。

手順

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **interface fcip 100**

FCIP インターフェイス（100）を作成します。

（注）
各 IPStorage インターフェイスには、FCIP リンクを一度に 3 つ構成できます。Cisco MDS 9250i では、各 IPStorage ポートに FCIP リンクを一度に 6 つ構成できます。Cisco MDS 24/10 ポートの SAN 拡張モジュールでは、各 IPStorage ポートは、時に設定された 3 つの FCIP リンクを持つことができます。

ピア IP アドレス（IPv4）の割り当て

IPv4 アドレスおよびポート番号に基づいてピア情報を割り当てる手順は、次のとおりです。

手順

ステップ 1 switch(config-if)# **peer-info ipaddr 10.1.1.1**

ピア情報を設定するため IPv4 アドレスを割り当てます。ポートが指定されていないため、デフォルトのポート番号（3225）が使用されます。

ステップ 2 switch(config-if)# **peer-info ipaddr 10.1.1.1 port 3000**

IPv4 アドレスを割り当て、ピア TCP ポートを 3000 に設定します。有効なポート番号は 0 ～ 65535 です。

ステップ 3 switch(config-if)# **no shutdown**

インターフェイスをイネーブルにします。

ピア IP アドレス（IPv6）の割り当て

IPv6 アドレスおよびポート番号に基づいてピア情報を割り当てる手順は、次のとおりです。

手順

ステップ 1 switch(config-if)# **peer-info ipaddr**

ピア情報を設定するため IPv6 アドレスを割り当てます。ポートが指定されていないため、デフォルトのポート番号（3225）が使用されます。

ステップ 2 switch(config-if)# **peer-info ipaddr 2001:0db8:800:200c::417a port 3000**

IPv6 アドレスを割り当て、ピア TCP ポートを 3000 に設定します。有効なポート番号は 0 ～ 65535 です。

ステップ 3 switch(config-if)# **no shutdown**

インターフェイスを有効にします。

ステップ 4 switch(config-if)# **interface IPStorage slot-number/plot-number**

IPStorage インターフェイス コンフィギュレーション モードを開始します。

ステップ 5 switch(config-if)# **shutdown**

インターフェイスを無効にします。

ステップ 6 switch(config-if)# **ipv6 enable**

インターフェイスで IPv6 処理をイネーブルにします。

ステップ 7 switch(config-if)# **no shutdown**

インターフェイスをイネーブルにします。

TCP 接続数の設定

FCIP リンクに使用する TCP 接続の数を 2 または 5 に指定できます。デフォルトでは、各リンクに対して 2 つの接続を使用します。接続 0 は FCIP 制御接続です。残りの 1 つまたは 4 つの TCP 接続はデータに使用されます。

（注） ピア スイッチ FCIP リンクでも同じ数の TCP 接続が構成されていることを確認してください。このように構成されていない場合は、FCIP リンクが稼働しません。

（注） Cisco MDS プラットフォームでは、10 Gb IPStorage ポートには 1 Gb イーサーネット ポートとは異なるパフォーマンス特性があります。MDS 10 Gb IPStorage ポートを使用して FCIP リンクで最大限のスループットを達成するには、これらのリンクで TCP 接続の数を 5 に設定します。

TCP 接続の試行回数を指定するには、次のステップを実行します。

手順

ステップ 1 switch# **configure terminal**

グローバル コンフィギュレーション モードを開始します。

ステップ 2 switch(config)# **interface fcip 4**

FCIP インターフェイス コンフィギュレーション モードを開始します。

ステップ 3 switch(config-if)# **shutdown**

インターフェイスをディセーブルにします。

ステップ 4 switch(config-if)# **tcp-connection 5**

TCP 接続の数を指定します。有効な値は、2 または 5 です。

（注）
TCP 接続の数を変更するには、 最初に FCIP インターフェイスがシャットダウンされていることを確認します。

ステップ 5 （任意） switch(config-if)# **no tcp-connection**

FCIP インターフェイスごとに 2 つの TCP セッションの工場出荷時のデフォルト設定に戻します。

ステップ 6 switch(config-if)# **no shutdown**

インターフェイスをイネーブルにします。

アクティブ接続の構成

TCP接続を開始するためにモードを構成できます。IP接続を能動的に試行するアクティブモードは、デフォルトで有効です。パッシブ モードをイネーブルにする場合、スイッチは TCP 接続を開始せず、ピアが接続してくるのを待機します。デフォルトで、スイッチは各 FCIP リンクに対して 2 つの TCP 接続を試行します。

（注） FCIP リンクの両端をパッシブ モードに設定しないでください。両端がパッシブに設定されていると、接続は開始されません。

パッシブ モードを構成にするには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config-if)# **passive-mode**	TCP接続試行時にパッシブ モードを有効にします。
ステップ 2	switch(config-if)# **no passive-mode**	工場出荷時のデフォルト設定（TCP接続試行時にアクティブ モードを使用する）に戻します。
ステップ 3	switch(config-if)# **no shutdown**	インターフェイスをイネーブルにします。

タイム スタンプ制御の有効化

指定期間範囲外のパケットを廃棄するように、スイッチを構成できます。イネーブルの場合、この機能はパケットが受け入れられる期間を指定します。パケットがこのオプションで指定された範囲内に到着した場合、そのパケットは受け入れられます。そうでない場合、パケットはドロップされます。

デフォルトでは、タイムスタンプ制御は Cisco MDS 9000 ファミリのすべてのスイッチでディセーブルです。有効にすると、パケットがネットワーク時間から 2000 ミリ秒間隔（+ または -2000 ミリ秒）以内に到着した場合、そのパケットは受け入れられます。

（注） **[time-stamp]** オプションが有効な場合、両方のスイッチでNTPを構成してください（詳細については、『 Cisco NX-OS 基本構成ガイド 』を参照してください）。

ヒント　テープ アクセラレーションまたは書き込みアクセラレーションが構成されている FCIP インターフェイスでは、タイムスタンプ制御を有効にしないでください。

タイム スタンプ制御を有効または無効にするには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config-if)# **time-stamp**`Please enable NTP with a common time source on both MDS Switches that are on either side of the FCIP link`	デフォルトの許容時間差（2000 ミリ秒）を使用して受信パケットのタイム スタンプ チェックを有効にします。
ステップ 2	（任意） switch(config-if)# **no time-stamp**	タイム スタンプを無効にします（デフォルト）。
ステップ 3	switch(config-if)# **time-stamp acceptable-diff 4000**	パケット許容時間を設定します。有効な範囲は 500 ～ 10,000 ミリ秒です。
ステップ 4	（任意） switch(config-if)# **no time-stamp acceptable-diff 500**	設定された時間差を削除し、工場出荷時のデフォルトに戻します。デフォルトの時間差は、ネットワーク時刻から 2000 ミリ秒です。
ステップ 5	switch(config-if)# **no shutdown**	インターフェイスをイネーブルにします。

QoS

Quality of Service（QoS）パラメータでは、すべての IP パケットをマーク付けする DiffServ コードポイント（DSCPDSCP）値を指定します（タイプ オブ サービス：IP ヘッダーの TOS フィールド）。

- 制御 DSCP 値は、制御 TCP 接続のすべての FCIP フレームに適用されます。
- データ DSCP 値は、データ接続のすべての FCIP フレームに適用されます。

FCIP リンクの TCP 接続が 1 つだけの場合は、その接続のすべてのパケットにデータ DSCP 値が適用されます。

QoS 値を設定するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config-if)# **qos control 24 data 26**	その DSCP 値ですべてのパケットをマークするように制御 TCP 接続およびデータ接続を設定します。制御とデータの値の範囲は 0 ～ 63 です。

	コマンドまたはアクション	目的
ステップ 2	switch(config-if)# **no qos control 24 data 26**	スイッチを工場出荷時のデフォルトに戻します（すべての制御パケットおよびデータ パケットを DCSP 値 0 でマーク）。

E ポートの構成

FC (T)E インターフェイスを構成するのと同じ方法で、FCIP インターフェイスを構成します。特に、次の機能が FCIP インターフェイスで利用できます。

- FCIP インターフェイスは任意の VSAN のメンバーにすることができます。

  詳細については、『Cisco MDS 9000 シリーズ ファブリック構成ガイド』を参照してください。

- トランク モードおよびトランク許可 VSAN

  詳細については、『Cisco MDS 9000 シリーズ インターフェイス構成ガイド』を参照してください。

- ポート チャネル
  - 複数の FCIP リンクを 1 つのファイバ チャネル ポート チャネルにバンドルできます。
  - FCIP リンクとファイバ チャネル リンクを 1 つのポート チャネルにまとめることはできません。

  詳細については、『Cisco MDS 9000 シリーズ ファブリック構成ガイド』を参照してください。

- FSPF

  詳細については、『Cisco MDS 9000 シリーズ ファブリック構成ガイド』を参照してください。

- 隣接スイッチからのゾーン データベースのインポートとエクスポート

  詳細については、『Cisco MDS 9000 シリーズ NX-OS システム管理構成ガイド』を参照してください。

FCIP インターフェイス情報の表示

FCIP リンクの概要、カウンタ、説明、およびステータスを表示するには、**show interface** コマンドを使用します。これらのコマンドの出力を使用して、管理モード、インターフェイス ステータス、動作モード、関連 VSAN ID、および使用されるプロファイルを確認できます。

FCIP の概要の表示

```
switch# show fcip summary
--------------------------------------------------------------------------------
Tun prof IPS-if peer-ip Status T W T Enc Comp Bandwidth rtt
E A A max/min (us)
--------------------------------------------------------------------------------
1 1 IPS1/1 20.1.1.2 TRNK Y N N N A 5000M/4000M 1000
2 2 IPS1/1 20.1.1.2 TRNK Y N N N A 1000M/800M 1000
3 3 IPS1/1 20.1.1.2 DOWN N N N N N 1000M/800M 1000
4 4 IPS1/1 20.1.1.2 DOWN N N N N N 1000M/800M 1000
5 5 IPS1/1 20.1.1.2 DOWN N N N N N 1000M/800M 1000
6 6 IPS1/1 20.1.1.2 DOWN N N N N N 1000M/800M 1000
7 7 IPS1/2.1 30.1.1.2 TRNK Y N N N M2 1000M/800M 1000
8 8 IPS1/2.2 31.1.1.2 TRNK Y N N N M2 1000M/800M 1000
9 9 IPS1/2.3 32.1.1.2 DOWN N N N N N 1000M/800M 1000
10 10 IPS1/2.4 33.1.1.2 DOWN N N N N N 1000M/800M 1000
11 11 IPS1/2.5 34.1.1.2 DOWN N N N N N 1000M/800M 1000
12 12 IPS1/2.6 35.1.1.2 DOWN N N N N N 1000M/800M 1000
```

指定したインターフェイスのカウンタの FCIP インターフェイス概要の表示

```
switch# show interface fcip 1
fcip1 is trunking
Hardware is IPStorage
Port WWN is 20:2b:00:2a:6a:1b:60:70
Peer port WWN is 20:62:8c:60:4f:73:d7:80
Admin port mode is auto, trunk mode is on
snmp link state traps are enabled
Port mode is TE
Port vsan is 1
Operating Speed is 5 Gbps
Trunk vsans (admin allowed and active) (1)
Trunk vsans (up) (1)
Trunk vsans (isolated) ()
Trunk vsans (initializing) ()
Interface last changed at Wed Nov 27 15:12:25 2019

Using Profile id 1 (interface IPStorage1/1)
Peer Information
Peer Internet address is 10.1.1.6 and port is 3225
Write acceleration mode is configured off
Tape acceleration mode is configured off
Tape Accelerator flow control buffer size is automatic
FICON XRC Accelerator is configured off
Ficon Load Balancer configured off for all vsans
Ficon Tape acceleration configured off for all vsans
IP Compression is enabled and set for mode2
Maximum number of TCP connections is 5
QOS control code point is 0
QOS data code point is 0
TCP Connection Information
5 Active TCP connections
27 Attempts for active connections, 2 close of connections
Path MTU 1500 bytes
Current retransmission timeout is 6400 ms
Current Send Buffer Size: 87080 KB, Requested Send Buffer Size: 62500 KB
CWM Burst Size: 50 KB
CONN<0>
Data connection: Local 10.1.1.12:65489, Remote 10.1.1.6:3225
TCP Parameters
```

```
Advertized window: Current: 24580 KB, Maximum: 24580 KB, Scale: 6
Peer receive window: Current: 8191 KB, Maximum: 8191 KB, Scale: 7
Congestion window: Current: 7372 KB, Slow start threshold: 8094 KB
Measured RTT : 500000 us Min RTT: 500000 us Max RTT: 0 us
Round trip time: Smoothed 0 ms, Variance: 100 Jitter: 150 us
TCP Connection Rate
Input Bytes: 0.00 MB/sec, Output Bytes: 0.00 MB/sec
Input Frames: 0/sec, Output Frames: 0/sec
CONN<1>
Data connection: Local 10.1.1.12:65487, Remote 10.1.1.6:3225
TCP Parameters
Advertized window: Current: 487 KB, Maximum: 24580 KB, Scale: 6
Peer receive window: Current: 8191 KB, Maximum: 8191 KB, Scale: 7
Congestion window: Current: 870 KB, Slow start threshold: 8094 KB
Measured RTT : 500000 us Min RTT: 7573 us Max RTT: 0 us
Round trip time: Smoothed 8 ms, Variance: 4 Jitter: 150 us
TCP Connection Rate
Input Bytes: 0.00 MB/sec, Output Bytes: 0.00 MB/sec
Input Frames: 0/sec, Output Frames: 0/sec
CONN<2>
Data connection: Local 10.1.1.12:65485, Remote 10.1.1.6:3225
TCP Parameters
Advertized window: Current: 477 KB, Maximum: 24580 KB, Scale: 6
Peer receive window: Current: 8191 KB, Maximum: 8191 KB, Scale: 7
Congestion window: Current: 853 KB, Slow start threshold: 8094 KB
Measured RTT : 500000 us Min RTT: 7419 us Max RTT: 0 us
Round trip time: Smoothed 8 ms, Variance: 4 Jitter: 150 us
TCP Connection Rate
Input Bytes: 0.00 MB/sec, Output Bytes: 0.00 MB/sec
Input Frames: 0/sec, Output Frames: 0/sec
CONN<3>
Data connection: Local 10.1.1.12:65483, Remote 10.1.1.6:3225
TCP Parameters
Advertized window: Current: 488 KB, Maximum: 24580 KB, Scale: 6
Peer receive window: Current: 8191 KB, Maximum: 8191 KB, Scale: 7
Congestion window: Current: 872 KB, Slow start threshold: 8094 KB
Measured RTT : 500000 us Min RTT: 7590 us Max RTT: 0 us
Round trip time: Smoothed 8 ms, Variance: 4 Jitter: 150 us
TCP Connection Rate
Input Bytes: 0.00 MB/sec, Output Bytes: 0.00 MB/sec
Input Frames: 0/sec, Output Frames: 0/sec
CONN<4>
Control connection: Local 10.1.1.12:65481, Remote 10.1.1.6:3225
TCP Parameters
Advertized window: Current: 335 KB, Maximum: 24580 KB, Scale: 6
Peer receive window: Current: 8125 KB, Maximum: 8125 KB, Scale: 7
Congestion window: Current: 50 KB, Slow start threshold: 8069 KB
Measured RTT : 18 us Min RTT: 18 us Max RTT: 23 us
Round trip time: Smoothed 1 ms, Variance: 1 Jitter: 150 us
TCP Connection Rate
Input Bytes: 0.00 MB/sec, Output Bytes: 0.00 MB/sec
Input Frames: 0/sec, Output Frames: 0/sec
5 minutes input rate 208 bits/sec, 26 bytes/sec, 0 frames/sec
5 minutes output rate 272 bits/sec, 34 bytes/sec, 0 frames/sec
1658 frames input, 174756 bytes
1658 Class F frames input, 174756 bytes
0 Class 2/3 frames input, 0 bytes
0 Reass frames
0 Error frames timestamp error 0
1663 frames output, 202836 bytes
1663 Class F frames output, 202836 bytes
0 Class 2/3 frames output, 0 bytes
0 Error frames
```

指定したインターフェイスのカウンタの FCIP インターフェイス概要の表示

```
switch# show interface fcip 1
fcip1 is trunking
Hardware is IPStorage
Port WWN is 20:62:8c:60:4f:73:d7:80
Peer port WWN is 20:2b:00:2a:6a:1b:60:70
Admin port mode is auto, trunk mode is on
snmp link state traps are enabled
Port mode is TE
Port vsan is 1
Operating Speed is 10000 Mbps
Trunk vsans (admin allowed and active) (1)
Trunk vsans (up) (1)
Trunk vsans (isolated) ()
Trunk vsans (initializing) ()
Interface last changed at Tue Nov 26 15:16:55 2019

Using Profile id 1 (interface IPStorage2/3)
Peer Information
Peer Internet address is 10.1.1.12 and port is 3225
Write acceleration mode is configured off
Tape acceleration mode is configured off
Tape Accelerator flow control buffer size is automatic
FICON XRC Accelerator is configured off
Ficon Load Balancer configured off for all vsans
Ficon Tape acceleration configured off for all vsans
IP Compression is enabled and set for mode2
Maximum number of TCP connections is 5
QOS control code point is 0
QOS data code point is 0
TCP Connection Information
5 Active TCP connections
23 Attempts for active connections, 5 close of connections
Path MTU 1500 bytes
Current retransmission timeout is 200 ms
Current Send Buffer Size: 149580 KB, Requested Send Buffer Size: 125000 KB
CWM Burst Size: 50 KB
CONN<0>
Data connection: Local 10.1.1.6:3225, Remote 10.1.1.12:65489
TCP Parameters
Advertized window: Current: 24580 KB, Maximum: 24580 KB, Scale: 7
Peer receive window: Current: 4095 KB, Maximum: 4095 KB, Scale: 6
Congestion window: Current: 3686 KB, Slow start threshold: 3998 KB
Measured RTT : 500000 us Min RTT: 500000 us Max RTT: 0 us
Round trip time: Smoothed 24 ms, Variance: 12 Jitter: 150 us
TCP Connection Rate
Input Bytes: 0.00 MB/sec, Output Bytes: 0.00 MB/sec
Input Frames: 0/sec, Output Frames: 0/sec
CONN<1>
Data connection: Local 10.1.1.6:3225, Remote 10.1.1.12:65487
TCP Parameters
Advertized window: Current: 24580 KB, Maximum: 24580 KB, Scale: 7
Peer receive window: Current: 487 KB, Maximum: 487 KB, Scale: 6
Congestion window: Current: 438 KB, Slow start threshold: 462 KB
Measured RTT : 500000 us Min RTT: 500000 us Max RTT: 0 us
Round trip time: Smoothed 24 ms, Variance: 12 Jitter: 150 us
TCP Connection Rate
Input Bytes: 0.00 MB/sec, Output Bytes: 0.00 MB/sec
Input Frames: 0/sec, Output Frames: 0/sec
CONN<2>
Data connection: Local 10.1.1.6:3225, Remote 10.1.1.12:65485
TCP Parameters
```

```
Advertized window: Current: 24580 KB, Maximum: 24580 KB, Scale: 7
Peer receive window: Current: 477 KB, Maximum: 477 KB, Scale: 6
Congestion window: Current: 429 KB, Slow start threshold: 453 KB
Measured RTT : 500000 us Min RTT: 500000 us Max RTT: 0 us
Round trip time: Smoothed 24 ms, Variance: 12 Jitter: 150 us
TCP Connection Rate
Input Bytes: 0.00 MB/sec, Output Bytes: 0.00 MB/sec
Input Frames: 0/sec, Output Frames: 0/sec
CONN<3>
Data connection: Local 10.1.1.6:3225, Remote 10.1.1.12:65483
TCP Parameters
Advertized window: Current: 24580 KB, Maximum: 24580 KB, Scale: 7
Peer receive window: Current: 488 KB, Maximum: 488 KB, Scale: 6
Congestion window: Current: 439 KB, Slow start threshold: 463 KB
Measured RTT : 500000 us Min RTT: 500000 us Max RTT: 0 us
Round trip time: Smoothed 24 ms, Variance: 12 Jitter: 150 us
TCP Connection Rate
Input Bytes: 0.00 MB/sec, Output Bytes: 0.00 MB/sec
Input Frames: 0/sec, Output Frames: 0/sec
CONN<4>
Control connection: Local 10.1.1.6:3225, Remote 10.1.1.12:65481
TCP Parameters
Advertized window: Current: 8123 KB, Maximum: 24580 KB, Scale: 7
Peer receive window: Current: 334 KB, Maximum: 334 KB, Scale: 6
Congestion window: Current: 50 KB, Slow start threshold: 373 KB
Measured RTT : 19 us Min RTT: 20 us Max RTT: 25 us
Round trip time: Smoothed 1 ms, Variance: 1 Jitter: 150 us
TCP Connection Rate
Input Bytes: 0.00 MB/sec, Output Bytes: 0.00 MB/sec
Input Frames: 0/sec, Output Frames: 0/sec
5 minutes input rate 288 bits/sec, 36 bytes/sec, 0 frames/sec
5 minutes output rate 224 bits/sec, 28 bytes/sec, 0 frames/sec
1130 frames input, 137324 bytes
1130 Class F frames input, 137324 bytes
0 Class 2/3 frames input, 0 bytes
0 Reass frames
0 Error frames timestamp error 0
1132 frames output, 119060 bytes
1132 Class F frames output, 119060 bytes
0 Class 2/3 frames output, 0 bytes
0 Error frames
```

詳細 FCIP インターフェイス標準カウンタ情報の表示

```
switch# show interface fcip 1 counters
fcip1
TCP Connection Information
5 Active TCP connections
27 Attempts for active connections, 2 close of connections
Path MTU 1500 bytes
Current retransmission timeout is 6400 ms
Current Send Buffer Size: 87080 KB, Requested Send Buffer Size: 62500 KB
CWM Burst Size: 50 KB
CONN<0>
Data connection: Local 10.1.1.12:65489, Remote 10.1.1.6:3225
TCP Parameters
Advertized window: Current: 24580 KB, Maximum: 24580 KB, Scale: 6
Peer receive window: Current: 8191 KB, Maximum: 8191 KB, Scale: 7
Congestion window: Current: 7372 KB, Slow start threshold: 8094 KB
Measured RTT : 500000 us Min RTT: 500000 us Max RTT: 0 us
Round trip time: Smoothed 0 ms, Variance: 100 Jitter: 150 us
TCP Connection Rate
```

```
Input Bytes: 0.00 MB/sec, Output Bytes: 0.00 MB/sec
Input Frames: 0/sec, Output Frames: 0/sec
CONN<1>
Data connection: Local 10.1.1.12:65487, Remote 10.1.1.6:3225
TCP Parameters
Advertized window: Current: 487 KB, Maximum: 24580 KB, Scale: 6
Peer receive window: Current: 8191 KB, Maximum: 8191 KB, Scale: 7
Congestion window: Current: 870 KB, Slow start threshold: 8094 KB
Measured RTT : 500000 us Min RTT: 7573 us Max RTT: 0 us
Round trip time: Smoothed 8 ms, Variance: 4 Jitter: 150 us
TCP Connection Rate
Input Bytes: 0.00 MB/sec, Output Bytes: 0.00 MB/sec
Input Frames: 0/sec, Output Frames: 0/sec
CONN<2>
Data connection: Local 10.1.1.12:65485, Remote 10.1.1.6:3225
TCP Parameters
Advertized window: Current: 477 KB, Maximum: 24580 KB, Scale: 6
Peer receive window: Current: 8191 KB, Maximum: 8191 KB, Scale: 7
Congestion window: Current: 853 KB, Slow start threshold: 8094 KB
Measured RTT : 500000 us Min RTT: 7419 us Max RTT: 0 us
Round trip time: Smoothed 8 ms, Variance: 4 Jitter: 150 us
TCP Connection Rate
Input Bytes: 0.00 MB/sec, Output Bytes: 0.00 MB/sec
Input Frames: 0/sec, Output Frames: 0/sec
CONN<3>
Data connection: Local 10.1.1.12:65483, Remote 10.1.1.6:3225
TCP Parameters
Advertized window: Current: 488 KB, Maximum: 24580 KB, Scale: 6
Peer receive window: Current: 8191 KB, Maximum: 8191 KB, Scale: 7
Congestion window: Current: 872 KB, Slow start threshold: 8094 KB
Measured RTT : 500000 us Min RTT: 7590 us Max RTT: 0 us
Round trip time: Smoothed 8 ms, Variance: 4 Jitter: 150 us
TCP Connection Rate
Input Bytes: 0.00 MB/sec, Output Bytes: 0.00 MB/sec
Input Frames: 0/sec, Output Frames: 0/sec
CONN<4>
Control connection: Local 10.1.1.12:65481, Remote 10.1.1.6:3225
TCP Parameters
Advertized window: Current: 333 KB, Maximum: 24580 KB, Scale: 6
Peer receive window: Current: 8122 KB, Maximum: 8122 KB, Scale: 7
Congestion window: Current: 50 KB, Slow start threshold: 8069 KB
Measured RTT : 500000 us Min RTT: 18 us Max RTT: 0 us
Round trip time: Smoothed 1 ms, Variance: 1 Jitter: 150 us
TCP Connection Rate
Input Bytes: 0.00 MB/sec, Output Bytes: 0.00 MB/sec
Input Frames: 0/sec, Output Frames: 0/sec
5 minutes input rate 224 bits/sec, 28 bytes/sec, 0 frames/sec
5 minutes output rate 288 bits/sec, 36 bytes/sec, 0 frames/sec
1686 frames input, 177260 bytes
1686 Class F frames input, 177260 bytes
0 Class 2/3 frames input, 0 bytes
0 Reass frames
0 Error frames timestamp error 0
1691 frames output, 206072 bytes
1691 Class F frames output, 206072 bytes
0 Class 2/3 frames output, 0 bytes
0 Error frames
IP compression statistics
83360 rxbytes
55942 rxbytes compressed, 0 rxbytes non-compressed
1.49 rx compression ratio
99132 txbytes
64015 txbytes compressed, 1152 txbytes non-compressed
1.52 tx compression ratio
```

```
IP compression flow control statistics
0 bytes queued for hw compression
0 queued for hardware compression
0 queued for hardware decompression
0 slowed tcp flow control
0 accelerated tcp flow control
0 side band flow control ON
2346 side band flow control OFF
IP compression hung statistics
0 times compression engine hung detected
0 jobs replayed for hardware compression
0 jobs replayed for hardware decompression
0 compression jobs not processed during compression engine reset
0 compression response job not processed during compression engine reset
0 decompression jobs not processed during decompression engine reset
0 decompression response job not processed during decompression engine reset
```

FCIP インターフェイスの説明の表示

```
switch# show interface fcip 51 description
FCIP51
Sample FCIP interface
```

合計 *txbytes* カウンタに表示される送信バイト数は、圧縮前のデータ量です。圧縮後は、圧縮された *txbytes* バイトが圧縮されて送信され、圧縮されていない *txbytes* バイトが圧縮なしで送信されます。パケットは、圧縮後により大きくなる場合に圧縮なしで送信されることもあります。

簡単な FCIP インターフェイス カウンタ情報の表示（Cisco MDS 9250i マルチサービス ファブリック スイッチ）

```
switch# show interface fcip 1-12 counters brief
--------------------------------------------------------------------------------
Interface Input (rate is 5 min avg) Output (rate is 5 min avg)
------------------------------ ------------------------------
Rate Total Rate Total
MB/s Frames MB/s Frames
--------------------------------------------------------------------------------
fcip1 191 1155974124 225 1363537690
fcip2 173 1046686124 227 1372311228
fcip3 0 0 0 0
fcip4 0 0 0 0
fcip5 0 0 0 0
fcip6 0 0 0 0
fcip7 189 1143612956 221 1339130294
fcip8 194 1167499884 218 1317700800
fcip9 0 0 0 0
fcip10 0 0 0 0
fcip11 0 0 0 0
fcip12 0 0 0 0
```

簡単な FCIP インターフェイス カウンタの情報を表示する (10/24 ポート SAN 拡張モジュール)

```
switch# show interface fcip 41 counters brief
--------------------------------------------------------------------------------
```

```
Interface Input (rate is 5 min avg) Output (rate is 5 min avg)
---------------------------- ----------------------------
Rate Total Rate Total
MB/s Frames MB/s Frames
-------------------------------------------------------------------------------
fcip41 191 1155974124 225 1363537690
```

拡張 FCIP 機能

FCIP インターフェイスに関する次のオプションを 1 つ以上設定すると、アプリケーション機能を大幅に向上させることができます。

FCIP 書き込みアクセラレーション

FCIP 書き込みアクセラレーション機能によって、FCIP を使用して WAN 上でストレージ トラフィックをルーティングする場合のアプリケーション書き込みパフォーマンスを大幅に改善できます。FCIP 書き込みアクセラレーションが有効になっている場合、送信側からの書き込みフレームをより近い FCIP スイッチで確認することで WAN のスループットが最大化されます。これにより、書き込み操作の WAN 遅延の影響が排除されます。書き込みアクセラレーション機能はデフォルトで無効であり、FCIP リンクの両側で有効にする必要があります。

（注） 書き込みアクセラレーション（WA）を使用する FCIP リンクでは、すべての高速フローが 1 つの FCIP リンクル（またはポート チャネル）を必ず通過する必要があります。これは、両方の方向でコマンドと応答の両方に適用されます。このようにしないと、FCIP WA は失敗します。その結果、コマンドと応答が異なるパスをたどる可能性があるため、FCIP WA を FSPF 等コスト パスに使用できなくなります。

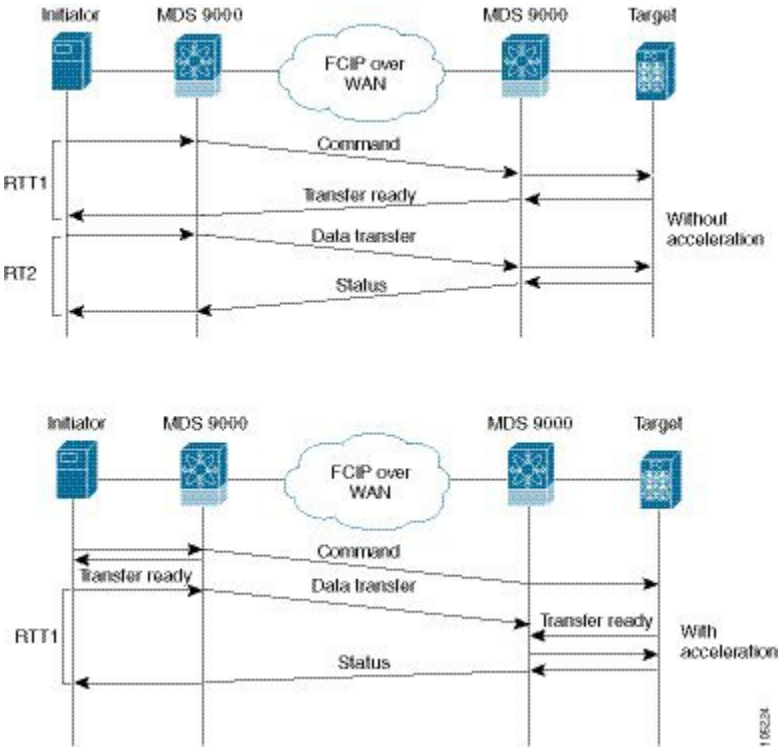
（注） ポート チャネル内のすべての FCIP リンクに、2 または 5 接続、WA、TA などの同じ属性が設定されていることを確認します。そうしないと、アップグレード中に望ましくない結果が発生します。

（注） FCIP 書き込みアクセラレーション機能は、FC 標準準拠の SCSI WRITE コマンド のみを高速化します。

（注） IBM Peer-to-Peer Remote Copy（PPRC）は、FCIP 書き込みアクセラレーションではサポートされません。

下の図で、書き込みアクセラレーションを使用せずに書き込みコマンドを実行する場合は、ラウンドトリップ トランスファー（RTT）が2つ必要ですが、書き込みアクセラレーションを使用して SCSI 書き込みコマンドを実行する場合に必要な RTT は 1 つのみです。最大サイズの Transfer Ready が FCIP リンクのホスト側からホストに戻されたあとで、 SCSI 書き込みコマンドがターゲットに到達します。これにより、ホストは FCIP リンク上で WRITE コマンドおよび Transfer Ready を長時間待機しなくても、SCSI 書き込みデータ送信を開始できます。また、FCIP リンクを経由して交換する場合には複数の Transfer Ready が必要ですが、これによる遅延もなくなります。

図 *8 : FCIP* リンク書き込みアクセラレーション



ヒント 「channel mode active」を構成したポート チャネルに FCIP リンクが含まれている場合は、複数の FCIP リンクに対して FCIP 書き込みアクセラレーション（WA）を有効にできます。これらは、ポート チャネル プロトコル（PCP）を使用して作成されたポート チャネルです。FCIP 環境における複数の FSPF 等コスト パスにわたって書き込みアクセラレーションを使用することはできません。ネイティブ ファイバ チャネル書き込みアクセラレーションは、ポート チャネルで使用できます。channel mode active が構成されたポート チャネル、またはポート チャネル プロトコル（PCP）で構成されたポート チャネルでも、FCIP 書き込みアクセラレーションを使用できます。イニシエータとターゲット ポート間に、コストの等しい複数の非ポート チャネル FCIP リンクが存在している場合、FCIP WA は機能しません。この設定では、SCSI 検出に失敗したり、WRITE または READ 処理が失敗したりすることがあります。FCIP WA を使用すると、FSPF ルーティングにより、単一 FCIP ポート チャネルまたは ISL が常に、イニシエータとターゲット ポート間のパスに存在することが確実になります。

書き込みアクセラレーションが構成された Cisco MDS 9700 シリーズ スイッチで構成されている FCIPs 上で VSAN あたり 1 つだけの FCIP ポート チャネルはサポートされます。

ヒント　書き込みアクセラレーションが構成された FCIP インターフェイス上では、タイムスタンプ制御を有効にしないでください。

（注）　Cisco MDS NX-OS リリース 7.3(1)DY(1) 以降では、Cisco MDS 9250i スイッチと Cisco MDS 9700 Director の Cisco MDS 24/10 ポート SAN 拡張モジュールの間に FCIP ポート チャネルが構成されている場合に、FCIP 書き込みアクセラレーションを有効にできます。

書き込みアクセラレーションを有効にする前に、次の前提条件が満たされていることを確認してください。

- FCIP ポート用の新しいポート チャネルの作成時に、Cisco MDS 9220i および MDS 9250i スイッチで **fcip enhanced** コマンドを使用している。ポート チャネルの作成の詳細については、『Cisco MDS 9000 シリーズ インターフェイス構成ガイド』の「ポート チャネルの構成」の章を参照してください。**fcip-enhanced** コマンドの詳細については、「Cisco MDS 9000 ファミリ コマンド リファレンス」を参照してください。
- Cisco MDS 9250i と MDS 9700 スイッチ間で FCIP ポートチャネルを構成し、FCIP ポートで書き込みアクセラレーションが有効になっている場合は、Cisco MDS 9250i スイッチで **fcip-enhanced** コマンドを使用して、FCIP ポートチャネルで書き込みアクセラレーションを有効にしてください。 ポート チャネルの作成の詳細については、『Cisco MDS 9000 シリーズ インターフェイス構成ガイド』の「ポート チャネルの構成」の章を参照してください。**fcip-enhanced** コマンドの詳細については、「Cisco MDS 9000 ファミリ コマンド リファレンス」を参照してください。
- **show port-channel database** コマンドを使用して、FCIP インターフェイスのみがポート チャネルのメンバーであることを確認します。
- Cisco MDS 9700 Director の Cisco MDS 24/10 SAN 拡張モジュールで FCIP 作成された FCIP インターフェイスで **passive-mode** を有効にしています。パッシブ モードのイネーブル化の詳細については、アクティブ接続の構成 （30 ページ）の項を参照してください。

ヒント　Cisco MDS NX-OS リリース 8.1(1) 以降では、次の条件下で、Cisco MDS 24/10 ポート SAN 拡張モジュールを搭載した 2 台の MDS 9700 シリーズ スイッチ間で FCIP ポート チャネルの書き込みアクセラレーションを構成しないでください。

- トラフィックが FCIP ポート チャネルを介して FCoE ポートと FC ポートの間を流れる場合。
- トラフィックが 2 つの連続する FCIP ポート チャネルを順番に通過します 。

このセクションは、次のトピックで構成されています。

FCIP 書き込みアクセラレーションの構成

書き込みアクセラレーションを有効にするには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch1# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch1(config)# **interface fcip 51**	FCIP インターフェイス（51）を作成します。
ステップ 3	switch1(config-if)# **write-accelerator**	書き込みアクセラレーションを有効にします。

書き込みアクセラレーションのアクティビティ情報の表示

以下に書き込みアクセラレーション アクティビティの情報を表示する方法を示します。

指定したホストエンド FCIP リンクで書き込みアクセラレーションによって処理される交換の表示

```
switch# show fcip host-map 100

MAP TABLE (5 entries TOTAL entries 5)

OXID | RXID | HOST FCID| TARG FCID| VSAN | Index
------+------+----------+----------+------+---------
0xd490|0xffff|0x00690400|0x00620426|0x0005|0x0000321f
0xd4a8|0xffff|0x00690400|0x00620426|0x0005|0x00003220
0xd4c0|0xffff|0x00690400|0x00620426|0x0005|0x00003221
0xd4d8|0xffff|0x00690400|0x00620426|0x0005|0x00003222
0xd4f0|0xffff|0x00690400|0x00620426|0x0005|0x00003223
```

指定したターゲットエンド FCIP リンクで書き込みアクセラレーションによって処理される交換の表示

```
switch# show fcip target-map 100

MAP TABLE (3 entries TOTAL entries 3)

OXID | RXID | HOST FCID| TARG FCID| VSAN | Index
------+------+----------+----------+------+---------
0xc308|0xffff|0x00690400|0x00620426|0x0005|0x00003364
0xc320|0xffff|0x00690400|0x00620426|0x0005|0x00003365
0xc338|0xffff|0x00690400|0x00620426|0x0005|0x00003366
```

詳細な FCIP インターフェイス書き込みアクセラレーション カウンタ情報の表示

```
switch# show interface fcip 4 counters
fcip4
```

```
TCP Connection Information
...
Write Accelerator statistics
6091 packets in 5994 packets out
0 frames dropped 0 CRC errors
0 rejected due to table full
0 ABTS sent 0 ABTS received
0 tunnel synchronization errors
37 writes recd 37 XFER_RDY sent (host)
0 XFER_RDY rcvd (target)
37 XFER_RDY rcvd (host)
0 XFER_RDY not proxied due to flow control (host)
0 bytes queued for sending
0 estimated bytes queued on the other side for sending
0 times TCP flow ctrl(target)
0 bytes current TCP flow ctrl(target)
```

FCIP テープ アクセラレーション

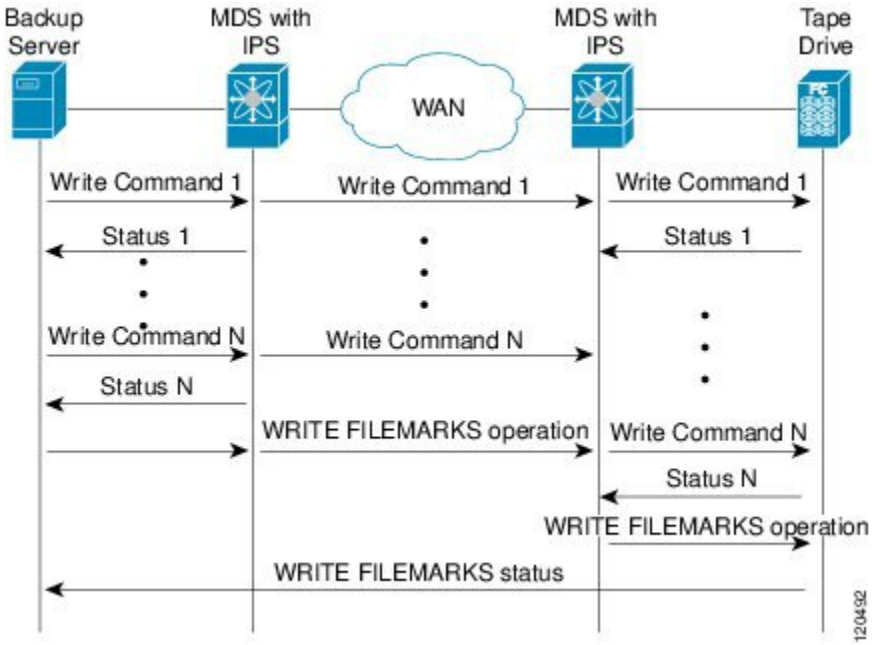
FCIP テープ アクセラレーション機能によって、FCIP を使用して WAN 上でストレージ トラフィックをルーティングする場合のアプリケーション書き込みパフォーマンスを大幅に改善できます。FCIP テープ アクセラレーションが有効になっている場合、送信側からのフレームをより近い FCIP スイッチで確認することで WAN のスループットが最大化されます。これにより、書き込み操作の WAN 遅延の影響が排除されます。FCIP テープ アクセラレーション機能はデフォルトで無効であり、FCIP リンクの両側で有効にする必要があります。

テープはユーザー データを順番に格納して検索するストレージ デバイスです。Cisco MDS NX-OS は、テープ書き込みアクセラレーションと読み取りアクセラレーションの両方を提供します。

テープ デバイスにアクセスするアプリケーションでは通常、未処理状態になる SCSI WRITE または READ 動作は 1 つだけです。このシングル コマンド プロセスにより、長距離 WAN リンク上で FCIP リンクを使用する場合は、テープ アクセラレーション機能の利点が制限されます。ホストがテープ ドライブから正常なステータス応答を受信しないかぎり、各 SCSI WRITE または READ 処理が完了しないため、バックアップおよびのパフォーマンスが低下します。FCIPテープアクセラレーション機能は、この問題の解消に有効です。この機能はホストとテープ ドライバ間で、WAN リンクを介して送信されるデータ ストリーミングを高速化することにより、テープのバックアップ、アーカイブ、および復元処理を改善します。

書き込み処理に関するテープ アクセラレーションの例では、 下の図のバックアップ サーバがテープ ライブラリのドライブに書き込み処理を発行します。ローカル Cisco MDS スイッチはリモート テープ ドライブのプロキシとして動作することにより、Transfer Ready を代行し、ホストにデータ送信の開始を伝えます。すべてのデータを受信してから、ローカルCisco MDS スイッチはSCSI WRITE 処理の正常完了を代行して通知します。この応答により、ホストは次の SCSI WRITE 処理を開始できます。このプロキシ方式を使用すると、プロキシを使用しないでデータを送信する場合に比べて、同じ期間内に FCIP リンクを介して多くのデータを送信できます。プロキシ方式により、WAN リンクのパフォーマンスが向上します。

図 *9 : FCIP* リンクのテープ アクセラレーション（書き込み処理の場合）



FCIP リンクのテープ側にあるもう片方の Cisco MDS スイッチでは、受信したコマンドおよびデータをバッファに格納します。その後、テープ ドライブからの Transfer Ready を待ち受けてデータを転送することにより、テープ ドライブのバックアップ サーバーとして機能します。

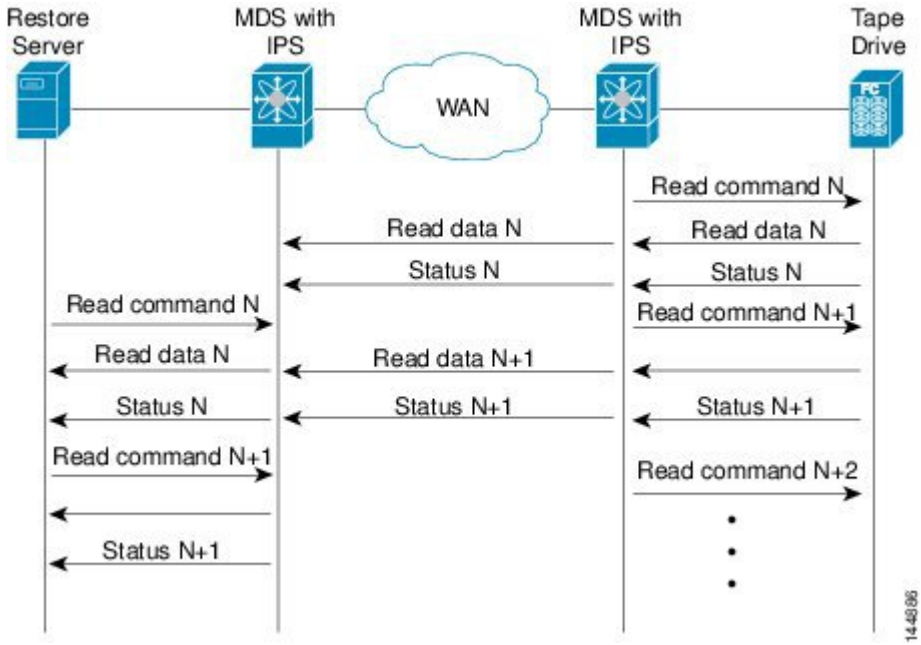
（注） 制御 LUN またはメディア チェンジャが LUN 0 として、テープ ドライブがその他の LUN としてエクスポートされるテープ ライブラリ環境において、リンクのアップ/ダウンが短時間で繰り返されるような状況（FCIP リンク、Server/Tape Port リンク）では、テープ アクセラレーションでテープ セッションが検出されず、これらのセッションが高速化されない可能性があります。リンクをイネーブルにする前に数分間、FCIP リンクをディセーブルにする必要があります。これは、テープ ドライブが直接 FC 接続されているか、LUN 0 としてエクスポートされたテープ環境には適用されません。

Cisco NX-OS は、WAN 上の TCP/IP によって、リモート テープ ドライブに確実にデータを配信します。プロキシに頼らずにエンドツーエンドで WRITE FILEMARKS 処理を完了させることによって、書き込みデータの完全性が維持されます。WRITE FILEMARKS 処理は、テープ ライブラリ データとバッファ データの同期を通知します。テープ メディア エラーがエラー処理のためにバックアップ サーバーに戻されると、Cisco NX-OS ソフトウェアが自動的にテープ ビジー エラーを再試行します。

読み取り処理に関するテープ アクセラレーションの例では、下の図のリストア サーバがテープ ライブラリのドライブに読み取り処理を発行します。復元プロセスでは、テープ側のリモート Cisco MDS スイッチは、ホストからさらに SCSI 読み取り処理が要求されることを予測して、テープ ドライブに SCSI 読み取り処理を独自に送信します。先取りの読み取りデータはローカル Cisco MDS スイッチでキャッシュに格納されます。ホストから SCSI 読み取り処理を

受信したローカルCisco MDS スイッチは、キャッシュのデータを送信します。この方式を使用すると、テープに読み取りアクセラレーションを使用しないでデータを送信する場合に比べて、同じ期間内にFCIP リンクを介して多くのデータを送信できます。その結果、WAN リンク上でのテープ読み取りパフォーマンスが向上します。

図 *10 : FCIP* リンクのテープ アクセラレーション（読み取り処理の場合）



Cisco NX-OS は、WAN 上の TCP/IP によって、復元アプリケーションに確実にデータを配信します。読み取り処理中のテープ メディア エラーは、エラー処理のためにリストア サーバーに戻されますが、それ以外のエラーは Cisco NX-OS ソフトウェアで回復されます。

（注） FCIP テープ アクセラレーション機能はデフォルトでディセーブルであり、FCIP リンクの両側でイネーブルにする必要があります。FCIP リンクの片側だけで有効にした場合、テープ アクセラレーション機能は処理時にオフになります。

ヒント FCIP ポートがポート チャネルに属している場合、またはイニシエータとターゲット ポートの間に複数のパスが存在する場合、FCIP テープ アクセラレーションは機能しません。このような設定では、SCSI 検出に失敗したり、読み書き処理が中断されたりすることがあります。

FCIP インターフェイスでテープ アクセラレーションがイネーブルの場合、このインターフェイスでは FICON VSAN をイネーブルにできません。同様に、FICON VSAN で FCIP インターフェイスが起動している場合は、このインターフェイス上でテープ アクセラレーションをイネーブルにできません。

（注） FCIP リンクに対してテープアクセラレーション機能を有効にすると、リンクが再初期化され、書き込みおよび読み取りアクセラレーション機能も自動的に有効になります。

書き込みのテープ アクセラレーションでは、リモート Cisco MDS スイッチで一定量のデータがバッファに格納されたあとで、Transfer Ready の代行によってではなく、ローカル Cisco MDS スイッチによって、ホストからの書き込み処理がフロー制御されます。書き込み処理が完了し、一部のデータ バッファが解放されると、ローカル Cisco MDS スイッチがプロキシ処理を再開します。同様に、読み取りのテープ アクセラレーションでは、ローカルの Cisco MDS スイッチに一定量のデータがバッファリングされると、さらに読み取りを発行するのではなく、リモートの Cisco MDS スイッチによって、テープ ドライブへの読み取り操作がフロー制御されます。書き込み処理が完了し、一部のデータバッファが解放されると、リモート Cisco MDS スイッチが読み取りの発行を再開します。

デフォルトのフロー制御バッファリングでは、**automatic** オプションを使用します。このオプションでは、WAN 遅延およびテープ速度を考慮して、最適なパフォーマンスが確保されます。ユーザー側でフロー制御バッファ サイズを指定することもできます（最大バッファ サイズは 12 MB）。

フロー制御バッファリングには、デフォルト オプションの使用を推奨します。

（注） FCIP テープ アクセラレーションは、5 つの TCP 接続で機能します。

ヒント テープ アクセラレーションが設定された FCIP インターフェイス上では、タイムスタンプ制御をイネーブルにしないでください。

このセクションは、次のトピックで構成されています。

FCIP テープ アクセラレーションに関するテープ ライブラリ LUN マッピング

テープ ライブラリが論理ユニット（LU）マッピングを行い、FCIP テープ アクセラレーションがイネーブルの場合は、ターゲット ポートからアクセスできる各物理テープ ドライブに、固有の論理ユニット番号（LUN）を割り当てる必要があります。

次の図に、単一ターゲット ポートからスイッチ 2 に接続されたテープ ドライブを示します。テープ ライブラリが LUN マッピングを行う場合は、4 つすべてのテープ ドライブに固有の LUN を割り当てる必要があります。

図 *11 : FCIP LUN* マッピング

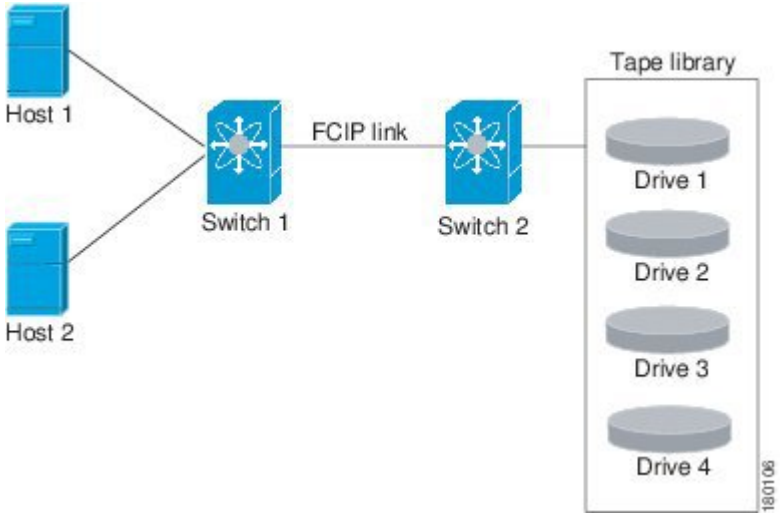


表 2 : 単一ホスト アクセスで有効な LUN マッピングの例 （47 ページ） および表 3 : 単一ホスト アクセスで無効な LUN マッピングの例 （48 ページ） に示したマッピングの場合、ホスト 1 はドライブ 1 およびドライブ 2 に、ホスト 2 はドライブ 3 およびドライブ 4 にアクセスできます。

次のテーブルに、有効なテープ ライブラリ LUN マッピングを示します。

表 *2 :* 単一ホスト アクセスで有効な *LUN* マッピングの例

ホスト	LUN マッピング	ドライブ
ホスト 1	LUN 1	ドライブ 1
	LUN 2	ドライブ 2
ホスト 2	LUN 3	ドライブ 3
	LUN 4	ドライブ 4

次のテーブルに、無効なテープ ライブラリ LUN マッピングを示します。

表 *3:* 単一ホスト アクセスで無効な *LUN* マッピングの例

ホスト	LUN マッピング	ドライブ
ホスト 1	LUN 1	ドライブ 1
	LUN 2	ドライブ 2
ホスト 2	LUN 1	ドライブ 3
	LUN 2	ドライブ 4

次に、1 つのテープ ポートを介して、複数のホストでテープ ドライブを共有する場合の設定例を示します。この例では、ホスト 1 がドライブ 1 およびドライブ 2 にアクセスでき、ホスト 2 がドライブ 2、ドライブ 3、およびドライブ 4 にアクセスできます。以下のテーブルに、この設定で有効な LUN マッピングを示します。

表 *4:* 複数のホスト アクセスで有効な論理 *LUN* マッピングの例

ホスト	LUN マッピング	ドライブ
ホスト 1	LUN 1	ドライブ 1
	LUN 2	ドライブ 2
ホスト 2	LUN 2	ドライブ 2
	LUN 3	ドライブ 3
	LUN 4	ドライブ 4

FCIP テープ アクセラレーションの構成

（注） FCIP テープ アクセラレーション リンクでは、TA 対応リンクでトランク モードが **on** の場合には、トランク モード許可 VSAN で、各 VSAN のトラフィックが 1 つのリンクだけを通過するように構成されている必要があります。トラフィックが複数のリンクを通過する場合には、トラフィックのエラーが発生する可能性があります。

FCIP テープ アクセラレーションを有効にする手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch1# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch1(config)# **interface fcip 5**	FCIP インターフェイス（5）を作成します。
ステップ 3	switch1(config-if)# **write-accelerator tape-accelerator**	テープアクセラレーション（およびまだ有効になっていない場合は書き込みアクセラレーション）を有効にします。
ステップ 4	switch1(config-if)# **write-accelerator tape-accelerator flow-control-buffer-size auto**	自動フロー制御を使用したテープアクセラレーションを有効にします（デフォルト）。
ステップ 5	switch1(config-if)# **write-accelerator tape-accelerator flow-control-buffer-size 2048**	テープ アクセラレーション フロー制御バッファのサイズを 2 MB に設定します。
ステップ 6	（任意） switch1(config-if)# **no write-accelerator tape-accelerator**	テープ アクセラレーションを無効にし（デフォルト）、FCIP リンクをリセットします。 （注） 書き込みアクセラレーション機能は引き続き有効です。
ステップ 7	（任意） switch1(config-if)# **no write-accelerator tape-accelerator flow-control-buffer-size 2048**	フロー制御バッファのサイズをデフォルト値 automatic に設定します。テープアクセラレーション機能と書き込みアクセラレーション機能は引き続き有効です。このコマンドは、FCIP リンクをリセットしません。
ステップ 8	（任意） switch1(config-if)# **no write-accelerator**	書き込みアクセラレーション機能とテープアクセラレーション機能の両方を無効にし、FCIP リンクをリセットします。

テープ アクセラレーションのアクティビティ情報の表示

以下にテープ アクセラレーション アクティビティの情報を表示する方法を示します。

交換にテープ アクセラレーションが適用されているテープに関する情報の表示

```
switch# show fcip tape-session summary

--------------------------------------------------------------------------------
Tunnel Tunnel End host-fcid tape-fcid lun vsan TCP Connection
--------------------------------------------------------------------------------

16 host-end 0x7c0006 0x390006 0x0000 3000 0
16 host-end 0x7c0004 0x390004 0x0000 3000 0
16 host-end 0x7c0003 0x390003 0x0000 3000 0
```

```
16 host-end 0x7c0007 0x390007 0x0000 3000 0
16 host-end 0x7c0005 0x390005 0x0000 3000 0
16 host-end 0x7c0000 0x390000 0x0000 3000 0
16 host-end 0x7c0002 0x390002 0x0000 3000 0
```

ホスト エンド FCIP リンクで交換にテープ アクセラレーションが適用されているテープに関する情報の表示

```
switch# show fcip tape-session tunnel 1 host-end

HOST TAPE SESSIONS (1 entries TOTAL entries 1)

Host Tape Session #1
FCID 0xEF0001, VSAN 1, LUN 0x0002
Outstanding Exchanges 0, Outstanding Writes 0
Target End Write Buffering 0 Bytes, Auto Max Writes 3
Flags 0x0, FSM state Non TA Mode
Cached Reads 0
First index 0xfffffff7, Last index 0xfffffff7, RA index 0x0000f99a
Current index=0xfffffffe, Els Oxid 0xfff7
Hosts 1
FCID 0x770100
```

ターゲット エンド FCIP リンクで交換にテープ アクセラレーションが適用されているテープに関する情報の表示

```
switch# show fcip tape-session tunnel 1 targ-end

TARGET TAPE SESSIONS (1 entries TOTAL entries 1)

Target Tape Session #1
FCID 0xEF0001, VSAN 1, LUN 0x0002
Outstanding Exchanges 0, Outstanding Writes 0
Host End Read Buffering 0 Bytes, Auto Max Read Blocks 3
Flags 0x800, Timer Flags 0x0
FSM State Default, Prev FSM State Bypass
Relative Block offset 0
First index 0xfffffff7, Last index 0xfffffff7, RA index 0x0000f99a
Current index=0xfffffffe, Els Oxid 0xfff7
Hosts 1
FCID 0x770100
```

詳細な FCIP インターフェイス テープ アクセラレーション カウンタ情報の表示（有効な場合）

```
switch# show interface fcip 1 counters
fcip1
TCP Connection Information
....
Tape Accelerator statistics
1 Host Tape Sessions
0 Target Tape Sessions
Host End statistics
Received 31521 writes, 31521 good status, 0 bad status
Sent 31517 proxy status, 4 not proxied
Estimated Write buffer 0 writes 0 bytes
Received 31526 reads, 10 status
```

```
Sent 31516 cached reads
Read buffer 0 reads, 0 bytes
Host End error recovery statistics
Sent REC 0, received 0 ACCs, 0 Rejects
Sent ABTS 0, received 0 ACCs
Received 31 RECs, sent 2 ACCs, 0 Rejects
Received 0 SRRs, sent 0 ACCs, 0 Rejects
Received 0 TMF commands
Target End statistics
Received 0 writes, 0 good status, 0 bad status
Write Buffer 0 writes, 0 bytes
Received 0 reads, 0 good status, 0 bad status
Sent 0 reads, received 0 good status, 0 bad status
Sent 0 rewinds, received 0 good status, 0 bad status
Estimated Read buffer 0 reads, 0 bytes
Target End error recovery statistics
Sent REC 0, received 0 ACCs, 0 Rejects
Sent SRR 0, received 0 ACCs
Sent ABTS 0, received 0 ACCs
Received 0 TMF commands
```

FCIP圧縮

FCIP圧縮オプションを使用すると、IPパケットをFCIPリンクで圧縮できます。このオプションは、FCIPリンクごとに有効になります。FCIPの最大帯域幅構成は、FCフレームのサイズに基づいて計算されます。圧縮はIPレイヤで行われ、FCはIPレイヤの上にあるため、圧縮を有効にしても、FCIPインターフェイスはそれを使用しない場合と比べて多くのデータを送信しません（つまり、FCスループットは増加しません）。むしろ、IPネットワークを介して送信されるIPトラフィックの量を減らすのに役立ちます（つまり、IPの負荷を軽減します）。デフォルトでは、FCIP圧縮は無効です。圧縮モードを指定せずに有効にすると、（FCIPプロファイルのTCPパラメータで構成された）FCIPサービス エンジンとリンク速度に適した圧縮アルゴリズムが自動的に使用されます。

（注） FCIP圧縮機能の主な目的は、最大帯域幅使用率に達している低帯域幅IP接続のスループットを向上させることです。使用するIPサービス スイッチまたはモジュールによっては、組み込みIP圧縮エンジンのパフォーマンスがIPストレージ ポートの最大ライン レートよりも大幅に低下する場合があります。したがって、高帯域幅リンクでFCIP圧縮を構成すると、アプリケーション レベルの全体的なパフォーマンスが低下する可能性があります。

Cisco MDS 9250iスイッチおよびCisco 24/10ポートSAN拡張モジュールは、Auto、Mode1、およびMode2圧縮モードをサポートしています。これらのモードはすべて、モジュール内部でハードウェア圧縮エンジンを内部的に使用します。Autoモードがデフォルトで有効になっています。Mode2では圧縮にAutoモードよりも大きなバッチ サイズを使用するため、高い圧縮スループットが実現します。ただしMode2では圧縮スループットによって多少遅延が生じます。高いスループットが重要な導入環境では、Mode2を使用できます。Mode1は他のモードと比較して最高の圧縮率を実現します。圧縮率が最も重要である導入環境では、Mode1を使用できます。

（注） FCIP リンクの両側で Cisco MDS NX-OS リリース 8.1(1) 以降が動作しており、かつ、FCIP リンクの片側で圧縮を有効にした場合は、リンクの反対側でも必ず有効にしてください。

（注） FCIP 圧縮を使用する場合、FCIP プロファイルの **tcp max-bandwidth-xxxx** および **min-available-bandwidth-xxxx** で指定されるレートは圧縮バイト数単位です。

このセクションは、次のトピックで構成されています。

FCIP 圧縮の構成

FCIP 圧縮を有効にするには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface fcip 51**	FCIP インターフェイス（51）を作成します。
ステップ 3	switch(config-if)# **ip-compression mode2**	高い圧縮を有効にします。
ステップ 4	（任意） switch(config-if)# **ip-compression auto**	デフォルトで**自動**モードを使用します。
ステップ 5	（任意） switch(config-if)# **no ip-compression**	FCIP圧縮機能をディセーブル（デフォルト）にします。

FCIP 圧縮情報の表示

以下の例に、FCIP 圧縮情報を表示する方法を示します。

詳細な FCIP インターフェイス圧縮情報の表示（有効な場合）

```
switch# show interface fcip 4 counters
fcip4
TCP Connection Information
...
IP compression statistics
208752 rxbytes, 208752 rxbytes compressed
5143584 txbytes
0 txbytes compressed, 5143584 txbytes non-compressed
1.00 tx compression ratio
```

9250i の圧縮エンジン統計情報の表示

```
switch# (config-vsan-db)# show ips stats hw-comp interface IPStorage 1/1
HW Compression statistics for port IPStorage1/1
Compression stats
10444189094728 input bytes, 2822607905236 output compressed bytes
85952406 input pkts, 85952065 output compressed pkts
Decompression stats
8596899248 input compressed bytes, 27669956608 output bytes
45879853 input compressed pkts, 45879669 output pkts
Passthru stats
0 input bytes, 0 output bytes
0 input pkts, 0 output pkts
Miscellaneous stats
0 min input pktlen, 638570 max input pktlen
0 min output pktlen, 185641 max output pktlen
0 len mismatch, 0 incomplete processing
0 invalid result, 0 invalid session drop
0 comp expanded
Errors stats
0 decomp tx error, 0 post comp error
0 post decomp error, 0 comp packets expanded
```

10/24 ポート SAN 拡張モジュールの圧縮エンジンの統計情報の表示

```
switch# show ips stats hw-comp interface iPStorage 5/1

HW Compression statistics for port IPStorage5/1
Compression stats
53280732 input bytes, 44561835 output compressed bytes
544700 input pkts, 544700 output compressed pkts
Decompression stats
41760802 input compressed bytes, 49574684 output bytes
511886 input compressed pkts, 511886 output pkts
Passthru stats
0 input bytes, 0 output bytes
0 input pkts, 0 output pkts
Miscellaneous stats
0 min input pktlen, 3816 max input pktlen
0 min output pktlen, 1485 max output pktlen
0 len mismatch, 0 incomplete processing
0 invalid result, 0 invalid session drop
0 comp expanded
Errors stats
0 decomp tx error, 0 post comp error
0 post decomp error, 0 comp packets expanded
```

最大限のパフォーマンスを引き出すための FCIP リンクの構成

ここでは、2 つの Cisco MDS 9250i スイッチ間または 24/10 ポート SAN 拡張モジュール間で最適なパフォーマンスを実現するための FCIP リンクの構成方法について説明します。両側で

FCIP プロファイルの最大帯域幅および最小帯域幅パラメータの設定を同一にしておくことが推奨されます。

（注）

- **tcp max-bandwidth-mbps** が 33 Mbps 以下の FCIP リンクでは、FSPF コストは 30000 になります。これは、ため、インターフェイスを使用できなくなります。Cisco MDS NX-OS リリース 8.2(1) から開始して、このような低帯域幅 FCIP リンクの FSPF コストは、28999 に設定されます。この値は 30000 の FSPF 最大コストよりも低いであるため、インターフェイス経由でルーティングへのトラフィックができます。また、エンドツーエンドのパスで (FCIP ホップを含む)、追加の FC または FCoE ホップもできます。これらの追加ホップの合計 FSPF コストは、1000 を超えないパスは使用できないため、します。28999 の FSPF コストが特定のトポロジの適用されない場合は、これは手動で設定するを使用して、 **fspf コスト** インターフェイスのコンフィギュレーション コマンド。インターフェイスの FSPF コストを確認するを使用して、 **fspf インターフェイスを show** コマンド。

  FSPF コストの詳細については、『Cisco MDS Fabric Configuration Guide』を参照してください。

- FSPF 等コストマルチパス（ECMP）を使用して、さまざまなタイプの ISL 間でトラフィックをロードバランシングすることはできません。つまり、2 つのスイッチ間でタイプが異なる複数の等コスト ISL（FCIP + FC、または FCIP + FCoE など）はサポートされません。

- Cisco MDS 24/10 ポート SAN 拡張モジュールでは、同じ VSAN 内の FCIP メンバーを持つ複数の ECMP ポート チャネルを構成することは有効な構成ではありません。これが構成されている場合、トラフィックは 1 つのポート チャネルだけを通過します。

- FCIP TCP エンドポイント間でパケット損失がなく、最大の FCIP パフォーマンスが実現されます。FCIP は、TCP 再送信レートが 0.05% を下回る場合に最高のパフォーマンスを発揮します。TCP 再送信レートが 0.05% を超えているかどうかを確認するには、**show logging onboard error-stats** コマンドを使用して、60 秒間隔の時間間隔を表示します。この場合、TCP 再送信レートは、FCIP インターフェイスごとおよび TCP 接続ごとに 0.05% を超えています。

このセクションは、次のトピックで構成されています。

Cisco MDS 9250i スイッチでパフォーマンスを最大限に引き出すための FCIP リンクの構成

このセクションは、次のトピックで構成されています。

1 Gbps モードでの FCIP パフォーマンスの構成

1 Gbps モードで FCIP のパフォーマンスを最大限に引き出すには、次の設定が推奨されます。

1. IPStorage ポートに FCIP リンクを作成します。

（注） 1 つ以上の FCIP リンクを 1 Gbps で 1 つの IPStorage インターフェイスにバインドしている場合は、そのインターフェイスにバインドしているすべてのトンネルの合計最大帯域幅が 1 Gbps を超えないようにする必要があります。

2. TCP 最大帯域幅を 1000 Mbps に、最小帯域幅を 800 Mbps に設定します。

（注） TCP 最大帯域幅が設定されている場合は最大 1000 Mbps 値のいずれかに 5 つの TCP 接続の数を設定することをお勧めします。

3. 各 FCIP リンクで 2 つの TCP 接続を構成します。
4. IPStorage ポートで MTU サイズを 2500 に設定します。
5. 各 FCIP リンクで圧縮を有効にします。

1 Gbps モードで FCIP のパフォーマンスを最大限に引き出すには、次の構成ステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **fcip profile***profile-id*	FCIP プロファイルを設定し、FCIP プロファイル コンフィギュレーション モードを開始します。
ステップ 3	switch(config-profile)# **ip address**ip-address	IP アドレスを FCIP プロファイルに割り当てます。IPv4 アドレスまたは IPv6 アドレスを割り当てることができます。
ステップ 4	switch(config-profile)# **tcp max-bandwidth-mbps** *1000* **min-available-bandwidth-mbps** *800* **round-trip-time-ms** *milliseconds*	FCIP リンクの使用可能な最大帯域幅を 1000 Mbps に、最小帯域幅を 800 Mbps に設定し、ラウンドトリップ時間をミリ秒単位で構成します。
ステップ 5	switch(config-profile)# **exit**	FCIP プロファイル コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	switch(config)# **interface fcip** *interface-number*	FCIP インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	switch(config-if)# **use-profile** *profile-id*	指定されたプロファイルを FCIP リンクにバインドします。

	コマンドまたはアクション	目的
ステップ 8	switch(config-if)# **peer-info ipaddr** *ip-address*	ピア IP アドレス（IPv4 または IPv6）を設定します。
ステップ 9	switch(config-if)# **tcp-connections** *2*	TCP 接続の数を 2 に設定します。この値はピア側と同じにする必要があります。
ステップ 10	switch(config-if)# **ip-compression mode2**	インターフェイスの圧縮アルゴリズムを **mode2** に設定します。その他に設定できるモードは **auto** と **mode1** です。
ステップ 11	switch(config-if)# **no shutdown**	FCIP インターフェイスを有効にします。
ステップ 12	switch (config-if)# **exit**	FCIP 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、グローバル コンフィギュレーション モードに戻ります。
ステップ 13	switch(config)# **interface IPStorage** *slot-number/port-number*	IPStorage インターフェイス コンフィギュレーション モードを開始します。
ステップ 14	switch(config-if)# ip address *ip-address subnet-mask*	インターフェイスに IP アドレスを割り当てます。
ステップ 15	switch(config-if)# **switchport mtu 2500**	インターフェイスの MTU サイズを 2500 に設定します。MTU の有効な範囲は 576 ～ 9216 です。
ステップ 16	switch(config-if)# **no shutdown**	インターフェイスを有効にします。
ステップ 17	switch(config-if)# **end**	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、特権 EXEC モードに戻ります。

10 Gbps モードでの FCIP パフォーマンスの構成

10 Gbps モードで FCIP のパフォーマンスを最大限に引き出すには、次の設定が推奨されます。

1. IPStorage ポートに FCIP リンクを作成します。

   2 つ以上の FCIP リンクを 10 Gbps で 1 つの IPStorage インターフェイスにバインドしている場合は、そのインターフェイスにバインドしているすべてのトンネルの合計最大帯域幅が 10 Gbps を超えないようにする必要があります。

2. TCP 最大帯域幅を 5000 Mbps に、最小帯域幅を 4000 Mbps に設定します（デフォルト値）。
3. 各 FCIP リンクで 5 つの TCP 接続を構成します。
4. IPStorage ポートで MTU サイズを 2500 に設定します。

10 Gbps モードで FCIP のパフォーマンスを最大限に引き出すには、次の構成ステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **fcip profile** *profile-id*	FCIP プロファイルを設定し、FCIP プロファイル コンフィギュレーション モードを開始します。
ステップ 3	switch(config-profile)# **ip address** *ip-address*	IP アドレスを FCIP プロファイルに割り当てます。IPv4 アドレスまたは IPv6 アドレスを割り当てることができます。
ステップ 4	switch(config-profile)# **tcp max-bandwidth-mbps***5000***min-available-bandwidth-mbps***4000** **round-trip-time-ms***milliseconds*	FCIP リンクの使用可能な最大帯域幅を 5000 Mbps に、最小帯域幅を 4000 Mbps に設定し、ラウンドトリップ時間をミリ秒単位で構成します。
ステップ 5	switch(config-profile)# **exit**	FCIP プロファイル コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	switch(config)# **interface fcip interface-number**	FCIP インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	switch(config-if)# **use-profile***profile-id*	指定されたプロファイルを FCIP リンクにバインドします。
ステップ 8	switch(config-if)# **peer-info ipaddr***ip-address*	ピア IP アドレス（IPv4 または IPv6）を設定します。
ステップ 9	switch(config-if)# **tcp-connections***5*	TCP 接続の数を 5 に設定します。この値はピア側と同じにする必要があります。
ステップ 10	switch(config-if)# **no shutdown**	FCIP インターフェイスを有効にします。
ステップ 11	switch(config-if)# **exit**	FCIP 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、グローバル コンフィギュレーション モードに戻ります。
ステップ 12	switch(config)# **interface IPStorage***slot-number/port-number*	IPStorage インターフェイス コンフィギュレーション モードを開始します。
ステップ 13	switch(config-if)# **ip address***ip-address subnet-mask*	インターフェイスに IP アドレスを割り当てます。
ステップ 14	switch(config-if)# **switchport mtu 2500**	インターフェイスの MTU サイズを 2500 に設定します。MTU の有効な範囲は 576 ～ 9216 です。
ステップ 15	switch(config-if)# **no shutdown**	インターフェイスを有効にします。

	コマンドまたはアクション	目的
ステップ 16	switch(config-if)# **end**	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、特権 EXEC モードに戻ります。

Cisco MDS 24/10 ポート SAN 拡張モジュールおよび M9220i スイッチで最大のパフォーマンスの FCIP リンクの構成

このセクションは、次のトピックで構成されています。

1 Gbps モードでの FCIP パフォーマンスの構成

1 Gbps モードで FCIP のパフォーマンスを最大限に引き出すには、次の設定が推奨されます。

1. IPStorage ポートに FCIP リンクを作成します。

（注） 1 つ以上の FCIP リンクを 1 Gbps で 1 つの IPStorage インターフェイスにバインドしている場合は、そのインターフェイスにバインドしているすべてのトンネルの合計最大帯域幅が 1 Gbps を超えないようにする必要があります。

2. TCP 最大帯域幅を 1000 Mbps に、最小帯域幅を 800 Mbps に設定します。

（注） TCP 最大帯域幅は、複数の 1000 Mbps にある値に設定されている場合は、5 つには、TCP 接続の数を設定することをお勧めします。

3. 各 FCIP リンクで 2 つの TCP 接続を構成します。
4. IPStorage ポートで MTU サイズを 2500 に設定します。

1 Gbps モードで FCIP のパフォーマンスを最大限に引き出すには、次の構成ステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **fcip profile** *profile-id*	FCIP プロファイルを設定し、FCIP プロファイル 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
ステップ 3	switch(config-profile)# **ip address** *ip-address*	IP アドレスを FCIP プロファイルに割り当てます。IPv4 アドレスまたは IPv6 アドレスを割り当てることができます。
ステップ 4	switch(config-profile)# **tcp max-bandwidth-mbps** *1000* **min-available-bandwidth-mbps** *800* **round-trip-time-ms** *milliseconds*	FCIP リンクの使用可能な最大帯域幅を 1000 Mbps に、最小帯域幅を 800 Mbps に設定し、ラウンドトリップ時間をミリ秒単位で構成します。
ステップ 5	switch(config-profile)# **exit**	FCIP プロファイル コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	switch(config)# **interface fcip** *interface-number*	FCIP インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	switch(config-if)# **use-profile** *profile-id*	指定されたプロファイルを FCIP リンクにバインドします。
ステップ 8	switch(config-if)# **peer-info ipaddr** *ip-address*	ピア IP アドレス（IPv4 または IPv6）を設定します。
ステップ 9	switch(config-if)# **tcp-connections** *2*	TCP 接続の数を 2 に設定します。この値はピア側と同じにする必要があります。
ステップ 10	switch(config-if)# **ip-compression** *mode2*	インターフェイスの圧縮アルゴリズムを **mode2** に設定します。その他に設定できるモードは **auto** と **mode1** です。
ステップ 11	switch (config-if)# **no shutdown**	FCIP インターフェイスを有効にします。
ステップ 12	switch (config-if)# **exit**	FCIP 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、グローバル コンフィギュレーション モードに戻ります。
ステップ 13	switch(config)# **interface IPStorage** *slot-number/port-number*	IPStorage インターフェイス コンフィギュレーション モードを開始します。
ステップ 14	switch(config-if)# **ip address** *ip-address subnet-mask*	インターフェイスに IP アドレスを割り当てます。
ステップ 15	switch(config-if)# **switchport mtu** *2500*	インターフェイスの MTU サイズを 2500 に設定します。MTU の有効な範囲は 576 ～ 9216 です。
ステップ 16	switch(config-if)# **no shutdown**	インターフェイスを有効にします。
ステップ 17	switch(config-if)# **end**	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、特権 EXEC モードに戻ります。

10 Gbps モードでの FCIP パフォーマンスの構成

10 Gbps モードで FCIP のパフォーマンスを最大限に引き出すには、次の設定が推奨されます。

Cisco MDS NX-OS リリース 9.3(1) より前のリリースでは、単一の FCIP トンネルの最大スループットは 7 Gbps です。最大のパフォーマンスを得るには、10 Gbps IPS ポートで 2 つの fcip トンネルを作成します。

1. IPStorage ポートに FCIP リンクを作成します。

   2 つ以上の FCIP リンクを 10 Gbps で 1 つの IPStorage インターフェイスにバインドしている場合は、そのインターフェイスにバインドしているすべてのトンネルの合計最大帯域幅が 10 Gbps を超えないようにする必要があります。

2. TCP 最大帯域幅を 10000 Mbps に、最小帯域幅を 8000 Mbps に設定します（デフォルト値）。
3. 各 FCIP リンクで 5 つの TCP 接続を構成します。
4. IPStorage ポートで MTU サイズを 2500 に設定します。

10 Gbps モードで FCIP のパフォーマンスを最大限に引き出すには、次の構成ステップを実行します。

手順

ステップ 1 switch# **configure terminal**

グローバル コンフィギュレーション モードを開始します。

ステップ 2 switch(config)# **fcip profile** *profile-id*

FCIP プロファイルを設定し、FCIP プロファイル コンフィギュレーション モードを開始します。

ステップ 3 switch(config-profile)# **ip address** *ip-address*

IP アドレスを FCIP プロファイルに割り当てます。IPv4 アドレスまたは IPv6 アドレスを割り当てることができます。

ステップ 4 switch(config-profile)# **tcp max-bandwidth-mbps** *10000* **min-available-bandwidth-mbps** *8000* **round-trip-time-ms** *milliseconds*

FCIP リンクの使用可能な最大帯域幅を 10000 Mbps に、最小帯域幅を 8000 Mbps に設定し、ラウンドトリップ時間をミリ秒単位で構成します。

ステップ 5 switch(config-profile)# **exit**

FCIP プロファイル コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

ステップ 6 switch(config)# **interface fcip** *interface-number*

FCIP インターフェイス コンフィギュレーション モードを開始します。

ステップ 7 switch(config-if)# **use-profile** *profile-id*

指定されたプロファイルを FCIP リンクにバインドします。

ステップ 8 switch(config-if)# **peer-info ipaddr** *ip-address*

ピア IP アドレス（IPv4 または IPv6）を設定します。

ステップ 9 switch(config-if)# **tcp-connections***5*

TCP 接続の数を 5 に設定します。この値はピア側と同じにする必要があります。

ステップ 10 switch(config-if)# **no shutdown**

FCIP インターフェイスを有効にします。

ステップ 11 switch(config-if)# **exit**

FCIP 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、グローバル コンフィギュレーション モードに戻ります。

ステップ 12 switch(config)# **interface IPStorage** *slot-number/port-number*

IPStorage インターフェイス コンフィギュレーション モードを開始します。

ステップ 13 switch(config-if)# **ip address** *ip-address subnet-mask*

インターフェイスに IP アドレスを割り当てます。

ステップ 14 switch(config-if)# **switchport mtu 2500**

インターフェイスの MTU サイズを 2500 に設定します。MTU の有効な範囲は 576 ～ 9216 です。

ステップ 15 switch(config-if)# **no shutdown**

インターフェイスを有効にします。

ステップ 16 switch(config-if)# **end**

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、特権 EXEC モードに戻ります。

25 Gbps モードでの FCIP パフォーマンスの構成

25 Gbps モードで FCIP のパフォーマンスを最大限に引き出すには、次の設定が推奨されます。

FCIP トンネルの最大帯域幅は 10 Gbps です。したがって、25 Gbps IPS ポートごとに 2 つの FCIP トンネルを構成します。

（注） 最大のパフォーマンスを得るには、25 Gbps IPStorage ポートごとに 2 つの VLAN サブインターフェイスを作成します。各 VLAN サブインターフェイスで、FCIP トンネルを作成します。

1. 25 Gbps IPStorage ポートに VLAN サブインターフェイスを作成します。
2. 各 VLAN サブインターフェイスに FCIP リンクを作成します。
3. TCP 最大帯域幅を 10000 Mbps（10 Gbps）に、最小帯域幅を 8000 Mbps（8Gbps）に設定します（デフォルト値）。
4. 各 FCIP リンクで 5 つの TCP 接続を構成します。
5. IPStorage ポートで MTU サイズを 2500 に設定します。

25 Gbps モードで FCIP のパフォーマンスを最大限に引き出すには、次の構成ステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface IPStorage** *slot-number/port-number VLAN-ID*	25Gbps IPStorage ポートでの VLAN サブインターフェイス（VLAN ID）を構成します。
ステップ 3	switch(config-if)# **ip address** *ip-address subnet-mask*	VLAN サブインターフェイスに IP アドレスを割り当てます。
ステップ 4	switch(config-if)# **switchport mtu** *2500*	VLAN サブインターフェイスの MTU サイズを 2500 に設定します。MTU の有効な範囲は 576 ～ 9216 です。
ステップ 5	switch(config-if)# **no shutdown**	VLAN サブインターフェイスを有効にします。
ステップ 6	switch(config-if)# **end**	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、特権 EXEC モードに戻ります。
ステップ 7	switch(config)# **fcip profile** *profile-id*	FCIP プロファイルを設定し、FCIP プロファイル コンフィギュレーション モードを開始します。
ステップ 8	switch(config-profile)# **ip address** *ip-address*	ステップ 3 で構成した VLAN サブインターフェイスの IP アドレスを FCIP プロファイルに割り当てます。
ステップ 9	switch(config-profile)# **tcp max-bandwidth-mbps** *10000* **min-available-bandwidth-mbps** *8000* **round-trip-time-ms** *milliseconds*	FCIP リンクの使用可能な最大帯域幅を 10000 Mbps に、最小帯域幅を 8000 Mbps に設定し、ラウンドトリップ時間をミリ秒単位で構成します。
ステップ 10	switch(config-profile)# **exit**	FCIP プロファイル コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 11	switch(config)# **interface fcip** *interface-number*	FCIP インターフェイス コンフィギュレーション モードを開始します。
ステップ 12	switch(config-if)# **use-profile** *profile-id*	指定されたプロファイルを FCIP リンクにバインドします。
ステップ 13	switch(config-if)# **peer-info ipaddr** *ip-address*	ピア IP アドレス（IPv4 または IPv6）を設定します。
ステップ 14	switch(config-if)# **tcp-connections** *5*	TCP 接続の数を 5 に設定します。この値はピア側と同じにする必要があります。
ステップ 15	switch(config-if)# **no shutdown**	FCIP インターフェイスを有効にします。
ステップ 16	switch(config-if)# **exit**	FCIP 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、グローバル コンフィギュレーション モードに戻ります。

40 Gbps モードでの FCIP パフォーマンスの構成

40 Gbps モードで FCIP のパフォーマンスを最大限に引き出すには、次の設定が推奨されます。

- FCIP トンネルの最大帯域幅は 10 Gbps です。したがって、40 Gbps IPS ポートに 4 つの FCIP トンネルを設定します。
- 最大のパフォーマンスを得るには、40 Gbps IP ストレージポートに 4 つの VLAN サブインターフェイスを作成します。各 VLAN サブインターフェイスで、FCIP トンネルを作成します。
  - Cisco MDS NX-OS Rel 9.3(1) より前のリリースでは、Cisco MDS 9220i の単一 FCIP トンネルの最大スループットは 7 Gbps です。40 Gbps IPS ポートでは、4 つの FCIP トンネルが個別の VLAN サブインターフェイスに作成されている場合、最大スループットは 28.5 Gbps です。
  - Cisco MDS NX-OS リリース 9.3(1) 以降、Cisco MDS 9220i の単一 FCIP トンネルの最大スループットは 10 Gbps です。40 Gbps IPS ポートでは、4 つの FCIP トンネルが個別の VLAN サブインターフェイスに作成されている場合、最大スループットは 34.6 Gbps です。

40 Gbps モードで FCIP のパフォーマンスを最大限に引き出すには、次の構成ステップを実行し、4 つの FCIP トンネルを構成します。

1. 40 Gbps IPStorage ポートに VLAN サブインターフェイスを作成します。
2. 各 VLAN サブインターフェイスに FCIP リンクを作成します。
3. TCP 最大帯域幅を 10000 Mbps（10 Gbps） に、最小帯域幅を 8000 Mbps（8Gbps）に設定します（デフォルト値）。

4. 各 FCIP リンクで 5 つの TCP 接続を構成します。
5. IPStorage ポートで MTU サイズを 2500 に設定します。

40 Gbps モードで FCIP のパフォーマンスを最大限に引き出すには、次の構成ステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface IPStorage** *slot-number/port-number VLAN-ID*	40 Gbps IPStorage ポートでの VLAN サブインターフェイス（VLAN ID）を構成します。
ステップ 3	switch(config-if)# **ip address** *ip-address subnet-mask*	VLAN サブインターフェイスに IP アドレスを割り当てます。
ステップ 4	switch(config-if)# **switchport mtu 2500**	VLAN サブインターフェイスの MTU サイズを 2500 に設定します。MTU の有効な範囲は 576 ～ 9216 です。
ステップ 5	switch(config-if)# **no shutdown**	VLAN サブインターフェイスを有効にします。
ステップ 6	switch(config-if)# **end**	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、特権 EXEC モードに戻ります。
ステップ 7	switch(config)# **fcip profile** *profile-id*	FCIP プロファイルを設定し、FCIP プロファイル コンフィギュレーション モードを開始します。
ステップ 8	switch(config-profile)# **ip address** *ip-address*	ステップ 3 で構成した VLAN サブインターフェイスの IP アドレスを FCIP プロファイルに割り当てます。
ステップ 9	switch(config-profile)# **tcp max-bandwidth-mbps** *10000* **min-available-bandwidth-mbps** *8000* **round-trip-time-ms** *milliseconds*	FCIP リンクの使用可能な最大帯域幅を 10000 Mbps に、最小帯域幅を 8000 Mbps に設定し、ラウンドトリップ時間をミリ秒単位で構成します。
ステップ 10	switch(config-profile)# **exit**	FCIP プロファイル コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	switch(config)# **interface fcip***interface-number*	FCIP インターフェイス コンフィギュレーション モードを開始します。
ステップ 12	switch(config-if)# **use-profile** *profile-id*	指定されたプロファイルを FCIP リンクにバインドします。

	コマンドまたはアクション	目的
ステップ 13	switch(config-if)# **peer-info ipaddr***ip-address*	ピア IP アドレス（IPv4 または IPv6）を設定します。
ステップ 14	switch(config-if)# **tcp-connections***5*	TCP 接続の数を 5 に設定します。この値はピア側と同じにする必要があります。
ステップ 15	switch(config-if)# **no shutdown**	FCIP インターフェイスを有効にします。
ステップ 16	switch(config-if)# **exit**	FCIP 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、グローバル コンフィギュレーション モードに戻ります。

FCIP 構成の確認

FCIP 構成を確認するには、次のコマンドを使用します。

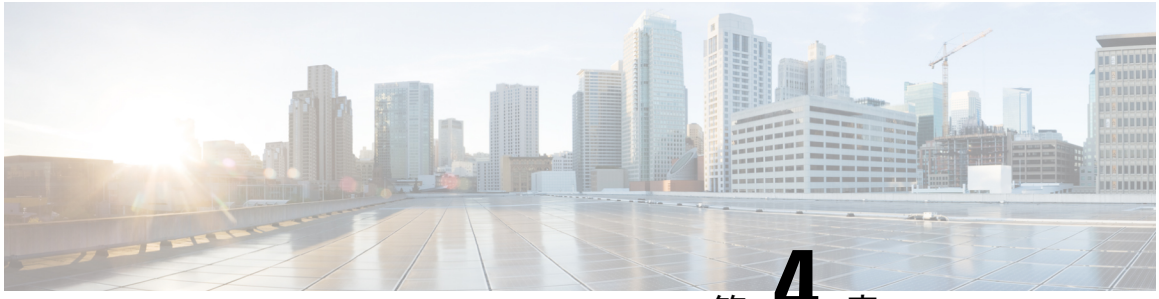
コマンド	目的
show fcip host-map *fcip-id*	指定したマップ情報を表示します。
show fcip profile *profile-id*	プロファイルの情報を表示します。
show fcip summary	概要を表示します。
show interface fcip	インターフェイスのステータスを表示します。
show interface fcip *fcip-id* **counters**	インターフェイス カウンタ情報を表示します。
show interface fcip *fcip-id* **counters brief**	インターフェイス カウンタの簡易な情報を表示します。
show interface fcip *fcip-id* **description**	インターフェイスの説明を表示します。
show fcip target-map	指定したターゲット マップ情報を表示します。
show fcip tape-session summary	テープ セッション情報を表示します。
show fcip tape-session tunnel 1 host-end	指定した FCIP リンク ID の情報を表示します。
show fcip tape-session tunnel 1 targ-end	ターゲット側の情報を表示します。
show ips stats hw-comp all	ハードウェア圧縮の統計情報を表示します。
show port-channel database	ポート チャネル データベースの情報を表示します。

FCIP パラメータのデフォルト設定

次の表に、FCIP パラメータのデフォルト設定を示します。

表 *5:* デフォルトの *FCIP* パラメータ

パラメータ	デフォルト
FCIP に対応するデフォルトの TCP ポート	3225
ピアへの TCP 接続のベース ポート	2
最小再送信時間	200 ミリ秒
キープアライブ タイムアウト	60 秒
最大再送信回数	4 回
PMTU ディスカバリ	イネーブル
PMTU enable reset timeout	3600 秒
SACK	イネーブル
最大帯域幅（Cisco MDS 24/10 ポート SAN の拡張モジュール）	10 Gbps
最大帯域幅（Cisco MDS 9220i ファブリック スイッチ）	10 Gbps
最大帯域幅（Cisco MDS 9250i マルチサービス ファブリック スイッチ）	5 Gbps
利用可能な最小帯域幅（Cisco MDS 24/10 ポート SAN の拡張モジュール）	8 Gbps
利用可能な最小帯域幅（Cisco MDS 9220i ファブリック スイッチ）	8 Gbps
利用可能な最小帯域幅（Cisco MDS 9250i マルチサービス ファブリック スイッチ）	4 Gbps
ラウンド トリップ時間	1 ミリ秒
バッファ サイズ	0 KB
制御 TCP およびデータ接続	パケットの送信なし
TCP 輻輳ウィンドウ モニタリング	イネーブル
バースト サイズ	50 KB
TCP 接続モード	アクティブ モード
FCIP タイムスタンプ	ディセーブル
パケットの許容差の範囲	+/– 2000 ミリ秒
B ポート キープアライブ応答	ディセーブル
書き込みアクセラレーション	無効化
テープ アクセラレーション	無効化



第 4 章

SAN Extension Tuner の設定

SAN Extension Tuner（SET）は、Cisco MDS 9000 ファミリ スイッチ固有の機能です。この機能は、直接アクセス（磁気ディスク）または順次アクセス（磁気テープ）SCSI 入出力コマンドを生成し、これらのトラフィックを特定の仮想ターゲットに振り分けることによって、FCIP パフォーマンスの最適化を図ります。テスト用入出力転送のサイズ、テスト中に生成する並行またはシリアル入出力の数を指定できます。SET からは、入出力/秒（IOPS）および入出力遅延の結果が報告されます。この情報は、FCIP スループットを最大にするために必要な、並行入出力の数を決定するときに役立ちます。

この章は、次の項で構成されています。

- SAN Extension Tuner の概要 （67 ページ）
- SAN Extension Tuner の設定 （69 ページ）
- データ パターン （70 ページ）
- ライセンスの前提条件 （70 ページ）
- SAN Extension Tuner の設定 （70 ページ）
- SAN Extension Tuner 構成の確認 （78 ページ）
- 調整パラメータのデフォルト設定 （79 ページ）

SAN Extension Tuner の概要

SAN Extension Tuner（SET）は、Cisco MDS 9000 ファミリ スイッチ固有の機能です。この機能は、直接アクセス（磁気ディスク）または順次アクセス（磁気テープ）SCSI 入出力コマンドを生成し、これらのトラフィックを特定の仮想ターゲットに振り分けることによって、FCIP パフォーマンスの最適化を図ります。リモート コピーおよびデータ バックアップなどのアプリケーションでは、IP ネットワーク上で FCIP を使用し、地理的に分散されている SAN を介して接続します。SET は IPS ポートで実装されます。この機能が有効の場合、この機能を使用して、構成されたオプションに基づいて、仮想ターゲットに対する SCSI 入出力コマンド（read および write）を生成できます。

（注） SAN 拡張チューナーは、HP c-Class Bladesystem 用シスコ ファブリック スイッチ、IBM BladeCenter 用シスコ ファブリック スイッチ、および 16 ポート ストレージ サービス ノード（SSN-16）ではサポートされていません。

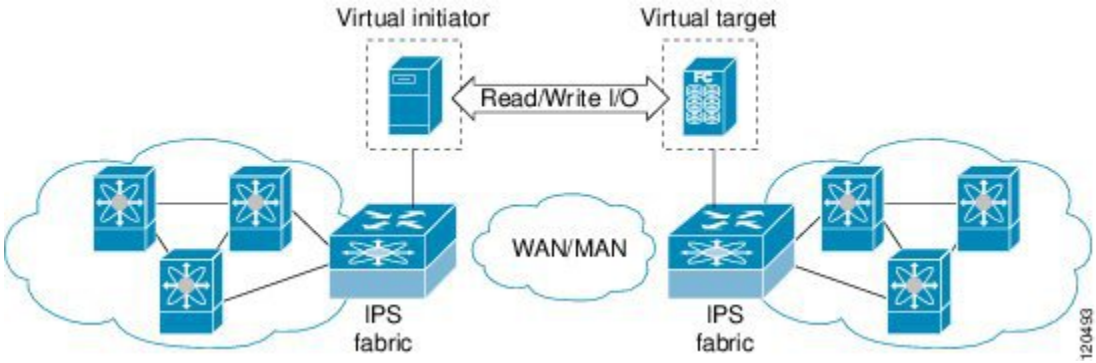
（注） Cisco MDS SAN-OS Release 3.3(1a) では、SAN Extension Tuner はマルチサービス モジュール（MSM）および Multiservice Modular スイッチでサポートされています。

リモート コピーおよびデータ バックアップなどのアプリケーションでは、IP ネットワーク上でFCIP を使用し、地理的に分散されている SAN を介して接続します。ファブリック全体で最大限のスループット パフォーマンスを実現するために、次の設定パラメータを調整できます。

- FCIP プロファイル用の TCP パラメータ（ウィンドウ管理 （24 ページ） を参照）
- アプリケーションが生成する並行 SCSI 入出力の数
- FCIP リンク上でアプリケーションが使用する転送サイズ

SET は IPS ポートで実装されます。この機能が有効の場合、この機能を使用することによって、構成されたオプションに基づいて、仮想ターゲットに対する SCSI 入出力コマンド（読み取りおよび書き込み）を生成できます（次の図を参照）。

図 *12 :* 仮想ターゲットに対する *SCSI* コマンドの生成



SET機能は、さまざまなSCSIトラフィック負荷を生成することによって、調整を支援します。さらに、FCIP リンク上の入出力ごとに、スループットおよび応答時間を測定します。

SAN ファブリックを調整する前に、次の注意事項を確認してください。

- 実装の詳細は次のとおりです。
  - 調整後の設定に持続性はありません。
  - 作成された仮想 N ポートはサポート対象の FC4 機能をネーム サーバーに登録しません。これは、SAN に含まれるホストがこれらの N ポートを通常の発信側またはターゲットとして検出しないようにするためです。

- SAN 内の他の発信側からのログイン要求は拒否されます。
- 仮想 N ポートは SCSI スイート全体を実装するのではなく、SCSI read および write コマンドだけを実装します。
- チューナーの発信側が通信できるのは、チューナーのターゲットだけです。

- 物理層でギガビット イーサネット インターフェイスがアップであることを確認します（GBIC とケーブルが接続されている、IP アドレスは不要）。
- スイッチ上で iSCSI をイネーブルにします（他の iSCSI 設定は不要）。
- インターフェイスを有効にします（その他の iSCSI インターフェイス構成は不要）
- ギガビット イーサネット インターフェイスで iSCSI インターフェイスを作成し、このインターフェイスを有効にします（その他の iSCSI インターフェイス設定は不要です）

  詳細については、「iSCSI インターフェイスの作成（86 ページ）」を参照してください。
- ネットワークの必要性に応じて、別個の VSAN またはゾーンで仮想 N ポートを構成します。
- 仮想 N ポートだけからなる独立した VSAN は、必須ではありませんが推奨します。ターゲットへのログインが拒否された場合に、一部のレガシー HBA が失敗する可能性があるからです。
- 同じギガビット イーサネット インターフェイスを使用して、仮想 N ポートと FCIP リンクを設定しないでください。それぞれ異なるギガビット イーサネット インターフェイスを使用してください。これは必須ではありませんが、推奨します。仮想Nポートによって発生したトラフィックが FCIP リンクのパフォーマンスに悪影響を与えることがあるからです。

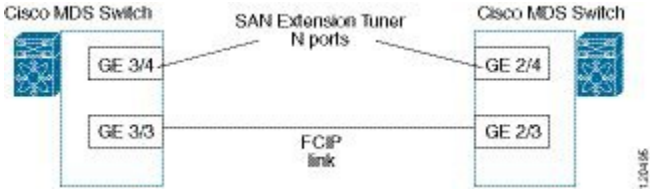
SAN Extension Tuner の設定

下の図に、スループットと遅延が測定される FCIP リンクには含まれないポート上で、仮想 N ポートを作成する物理設定の例を示します。

図 *13 :* ポート調整の物理構成例

下の図に、スループットと遅延が測定される FCIP リンクには含まれないポート上で、仮想 N ポートを作成する論理設定の例を示します。

図 *14 : FCIP* リンクに対応する *N* ポート調整の論理構成例



データ パターン

デフォルトでは、仮想Nポートが生成するデータのパターンとして、すべてゼロのパターンが使用されます。オプションとして、3 つの保存場所（bootflash: ディレクトリ、volatile: ディレクトリ、または slot0: ディレクトリ）のいずれかにあるデータ パターン ファイルを選択すると、生成されるデータ パターンとしてファイルを指定できます。このオプションは、FCIP リンク上での圧縮をテストする場合に特に便利です。ベンチマーク目的で、Canterbury 資料または人工資料ファイルも使用できます。

ライセンスの前提条件

SET を使用するには、SAN_EXTN_OVER_IP ライセンスが必要です（『*Cisco Family NX-OS Licensing Guide*』を参照）。

SAN Extension Tuner の設定

このセクションは、次のトピックで構成されています。

FCIP リンクの調整

所定の FCIP リンクを調整する手順は、次のとおりです。

手順

ステップ 1 スイッチ上の仮想 N ポートに nWWN を設定します。

ステップ 2 N ポートを作成するインターフェイス上で iSCSI をイネーブルにします。

ステップ 3 FCIP リンクの両側に仮想 N ポートを設定します。

ステップ 4 SAN内の実発信側が仮想Nポートを認識しないことを確認します。実際のイニシエータを分離するには、ゾーン分割（『Cisco MDS 9000 ファミリ NX-OS ファブリック構成ガイド』を参照）を使用します。

仮想 N ポートが相互に通信できるように、ゾーニング構成が設定されていることを確認します。

ステップ 5 SCSI の読み取りおよび書き込み入出力を開始します。

ステップ 6 必要に応じて、スイッチの他のギガビットイーサネットポートにNポートを追加し、最大限のスループットが得られるようにします。Nポートの追加が必要な状況としては、FCIP ポートチャネルを使用する場合などがあります。

チューナーの有効化

調整機能は、Cisco 9000 ファミリのすべてのスイッチについてデフォルトで無効になっています。この機能を有効にすると、調整はスイッチ全体でグローバルに有効になります。

調整機能を有効にするには、次のステップに従います。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	構成モードに入ります。
ステップ 2	switch(config)# **feature san-ext-tuner**	調整をイネーブルにします。
ステップ 3	switch(config)# **no feature san-ext-tuner**	現在適用されている調整の設定を削除し、調整を無効にします（デフォルト）。

nWWN の構成

このスイッチのチューナーに nWWN を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **san-ext-tuner**	SET コンフィギュレーション サブモードを開始します。
ステップ 2	switch(san-ext)# **nWWN 10:00:00:00:00:00:00:00**	SAN Extension Tuner の nWWN を設定します。

仮想 N ポートの構成

調整のために仮想 N ポートを設定するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	構成モードに入ります。
ステップ 2	switch(config)# **feature iscsi**	iSCSI をグローバルに有効にします。
ステップ 3	switch(config)# **iscsi enable module 1**	iSCSI を有効にし、次にモジュール 1 で有効にします。
ステップ 4	switch(config)# **interface iscsi 1/1**	iSCSI インターフェイスを作成し、インターフェイス コンフィギュレーション サブモードを開始します。
ステップ 5	switch(config-if)# **no shutdown**	iSCSI インターフェイスを有効にします。
ステップ 6	switch(config-if)# **end**	EXEC モードに戻ります。
ステップ 7	switch# **san-ext-tuner**	SET コンフィギュレーション サブモードを開始します。
ステップ 8	switch(san-ext)# **nport pWWN 12:00:00:00:00:00:00:56 vsan 200 interface gigabitethernet 1/1**	指定したギガビット イーサネット ポートおよび VSAN で仮想 N ポートを作成します。この N ポートはイニシエータまたはターゲットとして機能できます。
ステップ 9	（任意） switch(san-ext)# **no nport pWWN 22:34:56:78:90:12:34:56 vsan 200 interface gigabitethernet 1/1**	指定したギガビット イーサネット ポートおよび VSAN の仮想 N ポートを削除します。

SCSI ディスク読み取り/書き込み IO の生成

SCSI read および write コマンドは、一度だけ割り当てるか、または継続的に割り当てることができます。

このセクションは、次のトピックで構成されています。

一度だけ SCSI ディスク読み取り/書き込み IO の生成

SCSI read/write コマンドを一度だけ生成するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **san-ext-tuner**	SET コンフィギュレーション サブモードを開始します。

	コマンドまたはアクション	目的
ステップ 2	switch(san-ext)# **nport pWWN 12:00:00:00:00:00:00:56 vsan 200 interface gigabitethernet 1/1**	指定したギガビット イーサネット ポートおよび VSAN で仮想 N ポートを作成します。この N ポートはイニシエータまたはターゲットとして機能できます。
ステップ 3	switch(san-ext-nport)# **read command-id 100 target 22:22:22:22:22:22:22:22 transfer-size 512000 outstanding-ios 2 num-transactions 5000000**	**読み取り**コマンドで 2 つの未処理の I/O の転送サイズとして 512,000 バイトを指定します。I/O の合計は 5,000,000 バイトです。
ステップ 4	switch(san-ext-nport)# **write command-id 101 target 22:22:22:22:22:22:22:22 transfer-size 512000 outstanding-ios 2 num-transactions 5000000**	ターゲットが受信する**書き込み**コマンドで 2 つの未処理の I/O の転送サイズとして 512,000 バイトを指定します。I/O の合計は 5,000,000 バイトです。
ステップ 5	switch(san-ext-nport)# **stop command-id 100**	指定された ID のコマンドを停止します。
ステップ 6	（任意） switch(san-ext-nport)# **stop all**	未処理のコマンドをすべて停止します。
ステップ 7	switch(san-ext-nport)# **clear counters**	この N ポートに関連付けられているカウンタをクリアします。
ステップ 8	switch(san-ext-nport)# **end**	SAN Extension Tuner サブモードを終了します。

SCSI ディスク読み取り/書き込み IO の継続的な生成

SCSI 読み取り/書き込みコマンドを継続的に生成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **san-ext-tuner**	SET コンフィギュレーション サブモードを開始します。
ステップ 2	switch(san-ext)# **nport pWWN 12:00:00:00:00:00:00:56 vsan 200 interface gigabitethernet 1/1**	指定したギガビット イーサネット ポートおよび VSAN で仮想 N ポートを作成します。この N ポートはイニシエータまたはターゲットとして機能できます。
ステップ 3	switch(san-ext-nport)# **read command-id 100 target 22:22:22:22:22:22:22:22 transfer-size 512000 outstanding-ios 2 continuous**	SCSI コマンドが継続的に読み取られるように設定します。 **ヒント** 未処理の設定を停止するには **stop command-id** コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 4	switch(san-ext-nport)# **write command-id 100 target 22:22:22:22:22:22:22:22 transfer-size 512000 outstanding-ios 2 continuous**	SCSI コマンドが継続的に書き込まれるように設定します。
ステップ 5	switch(san-ext-nport)# **stop command-id 100**	指定された ID のコマンドを停止します。
ステップ 6	（任意） switch(san-ext-nport)# **stop command-id all**	未処理のコマンドをすべて停止します。
ステップ 7	（任意） switch(san-ext-nport)# **stop all**	未処理のコマンドをすべて停止します。
ステップ 8	switch(san-ext-nport)# **clear counters**	このNポートに関連付けられているカウンタをクリアします。
ステップ 9	switch(san-ext-nport)# **end**	SAN Extension Tuner サブモードを終了します。

SCSI の転送可能サイズ

SCSI 書き込みコマンドの転送可能サイズを指定するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **san-ext-tuner**	SET コンフィギュレーション サブモードを開始します。
ステップ 2	switch(san-ext)# **nport pWWN 12:00:00:00:00:00:00:56 vsan 200 interface gigabitethernet 1/1**	指定したギガビット イーサネット ポートおよび VSAN で仮想Nポートを作成します。このNポートはイニシエータまたはターゲットとして機能できます。
ステップ 3	switch(san-ext-nport)# **write command-id 100 target 22:22:22:22:22:22:22:22 transfer-size 512000 outstanding-ios 2 num-transactions 5000000**	ターゲットが受信する**書き込み**コマンドで 2 つの未処理の I/O の転送サイズとして 512,000 バイトを指定します。I/O の合計は 5,000,000 バイトです。
ステップ 4	switch(san-ext-nport)# **transfer-ready-size 512000**	SCSI write コマンドのターゲットとして最大転送可能サイズ 512,000 バイトを指定します。SCSI **書き込み**コマンドにこれよりも大きなサイズを指定すると、ターゲットは指定された転送サイズに基づいて複数の転送を実行します。
ステップ 5	switch(san-ext-nport)# **no transfer-ready-size 512000**	SCSI write コマンドに対して指定された転送可能サイズ設定を削除します。
ステップ 6	switch(san-ext-nport)# **stop command-id 100**	指定された ID のコマンドを停止します。
ステップ 7	switch(san-ext-nport)# **end**	SAN Extension Tuner サブモードを終了します。

SCSI テープ読み取り/書き込み IO の生成

SCSI tape read および write コマンドは、一度だけ割り当てるか、または継続的に割り当てることができます。

（注）
- 仮想Nポートが相互に通信できるように、ゾーニング構成が設定されていることを確認します。
- テープ動作をエミュレーションする仮想Nポートに対しては、未処理の入出力は一時点で 1 つだけです。

ここでは、次の内容について説明します。

一度だけ SCSI テープ読み取り/書き込み IO の生成

SCSI テープ読み取りまたは書き込みコマンドを一度だけ生成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **san-ext-tuner**	SET コンフィギュレーション サブモードを開始します。
ステップ 2	switch(san-ext)# **nport pWWN 12:00:00:00:00:00:00:56 vsan 200 interface gigabitethernet 1/1**	指定したギガビット イーサネット ポートおよび VSAN で仮想Nポートを作成します。このNポートはイニシエータまたはターゲットとして機能できます。
ステップ 3	switch(san-ext-nport)# **tape-read command-id 100 target 22:22:22:22:22:22:22:22 transfer-size 512000 num-transactions 5000000 filemark-frequency 32**	32 の SCSI read コマンドごとにファイルマーク上のスペースの転送サイズとして 512,000 バイトを指定します。I/O の合計は 5,000,000 バイトです。
ステップ 4	switch(san-ext-nport)# **tape-write command-id 101 target 22:22:22:22:22:22:22:22 transfer-size 512000 num-transactions 5000000 filemark-frequency 32**	転送サイズとして 512,000 バイトを指定し、ファイル マークが 32 個の SCSI write コマンドごとに書き込まれることを指定します。I/O の合計は 5,000,000 バイトです。
ステップ 5	switch(san-ext-nport)# **stop command-id 100**	指定された ID のコマンドを停止します。
ステップ 6	（任意） switch(san-ext-nport)# **stop all**	未処理のコマンドをすべて停止します。
ステップ 7	switch(san-ext-nport)# **clear counters**	このNポートに関連付けられているカウンタをクリアします。

	コマンドまたはアクション	目的
ステップ 8	switch(san-ext-nport)# **end**	SAN Extension Tuner サブモードを終了します。

SCSI テープ読み取り/書き込み IO の継続的な生成

SCSI テープ読み取りまたは書き込みコマンドを継続的に生成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **san-ext-tuner**	SET コンフィギュレーション サブモードを開始します。
ステップ 2	switch(san-ext)# **nport pWWN 12:00:00:00:00:00:00:56 vsan 200 interface gigabitethernet 1/1**	指定したギガビット イーサネット ポートおよび VSAN で仮想 N ポートを作成します。この N ポートはイニシエータまたはターゲットとして機能できます。
ステップ 3	switch(san-ext-nport)# **tape-read command-id 100 target 22:22:22:22:22:22:22:22 transfer-size 512000 continuous filemark-frequency 32**	SCSI tape read コマンドが継続的に発行されるように設定します。 ヒント 未処理の設定を停止するには **stop command-id** コマンドを使用します。
ステップ 4	switch(san-ext-nport)# **tape-write command-id 100 target 22:22:22:22:22:22:22:22 transfer-size 512000 continuous filemark-frequency 32**	SCSI tape write コマンドが継続的に発行されるように設定します。
ステップ 5	switch(san-ext-nport)# **stop command-id 100**	指定された ID のコマンドを停止します。
ステップ 6	（任意） switch(san-ext-nport)# **stop command-id all**	未処理のコマンドをすべて停止します。
ステップ 7	switch(san-ext-nport)# **clear counters**	この N ポートに関連付けられているカウンタをクリアします。
ステップ 8	switch(san-ext-nport)# **end**	SAN Extension Tuner サブモードを終了します。

SCSI の転送可能サイズ

SCSI 書き込みコマンドの転送可能サイズを指定するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **san-ext-tuner**	SET コンフィギュレーション サブモードを開始します。
ステップ 2	switch(san-ext)# **nport pWWN 12:00:00:00:00:00:00:56 vsan 200 interface gigabitethernet 1/1**	指定したギガビット イーサネット ポートおよび VSAN で仮想 N ポートを作成します。この N ポートはイニシエータまたはターゲットとして機能できます。
ステップ 3	switch(san-ext-nport)# **write command-id 100 target 22:22:22:22:22:22:22:22 transfer-size 512000 outstanding-ios 2 num-transactions 5000000**	ターゲットが受信する**書き込み**コマンドで 2 つの未処理の I/O の転送サイズとして 512,000 バイトを指定します。I/O の合計は 5,000,000 バイトです。
ステップ 4	switch(san-ext-nport)# **transfer-ready-size 512000**	SCSI write コマンドのターゲットとして最大転送可能サイズ 512,000 バイトを指定します。SCSI **書き込み**コマンドにこれよりも大きなサイズを指定すると、ターゲットは指定された転送サイズに基づいて複数の転送を実行します。
ステップ 5	switch(san-ext-nport)# **no transfer-ready-size 512000**	SCSI write コマンドに対して指定された転送可能サイズ設定を削除します。
ステップ 6	switch(san-ext-nport)# **stop command-id 100**	指定された ID のコマンドを停止します。
ステップ 7	switch(san-ext-nport)# **end**	SAN Extension Tuner サブモードを終了します。

データ パターンの構成

オプションで SCSI コマンドのデータ パターンを構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **san-ext-tuner**	SET コンフィギュレーション サブモードを開始します。
ステップ 2	switch(san-ext)# **nport pWWN 12:00:00:00:00:00:00:56 vsan 200 interface gigabitethernet 1/1**	指定したギガビット イーサネット ポートおよび VSAN で仮想 N ポートを作成します。この N ポートはイニシエータまたはターゲットとして機能できます。
ステップ 3	switch(san-ext-nport)# **data-pattern-file bootflash://DataPatternFile**	仮想 N ポートが読み取りコマンドのターゲットであり、かつ書き込みコマンドのイニシエータである場

	コマンドまたはアクション	目的
		合に、この仮想 N ポートにより送信されるデータ パターンを指定します。 **ヒント** このコマンドは、ターゲットでは read コマンドから戻されるデータを変更するように設定され、イニシエータでは write コマンド用に設定される必要があります。このコマンドは、特定のビット パターンを含むデータ セットまたは特定の圧縮率が設定されているデータ セットを定義するときに役立ちます。デフォルトのデータ セット（すべてゼロ）は非常に均一的であり圧縮率が高くなります。
ステップ 4	（任意） switch(san-ext-nport)# **no data-pattern-file**	SCSI read および write コマンドに対して指定されたデータ パターン設定を削除します。デフォルトでは、すべてゼロのデータ パターンが送信されます。
ステップ 5	switch(san-ext-nport)# **write command-id 100 target 22:22:22:22:22:22:22:22 transfer-size 512000 outstanding-ios 2 num-transactions 5000000**	2 つの未処理の I/O の転送サイズとして 512,000 バイトを指定します。I/O の合計は 5,000,000 バイトです。
ステップ 6	switch(san-ext-nport)# **stop command-id 100**	指定された ID のコマンドを停止します。
ステップ 7	switch(san-ext-nport)# **clear counters**	この N ポートに関連付けられているカウンタをクリアします。
ステップ 8	switch(san-ext-nport)# **end**	SAN Extension Tuner サブモードを終了します。

SAN Extension Tuner 構成の確認

Cisco MDS スイッチの現在の SAN Extension Tuner 設定を表示するには、**show** コマンドを使用します。

FLOGI データベースのエントリの表示

```
switch# show flogi database
--------------------------------------------------------------------------------
INTERFACE VSAN FCID     PORT NAME               NODE NAME
--------------------------------------------------------------------------------
iscsi1/1   200 0x050000 12:00:00:00:00:00:00:56 10:00:00:00:00:00:00:00
```

FLOGI データベースの VSAN エントリの詳細情報の表示

```
switch# show fcns database vsan 200
VSAN 200
```

```
--------------------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------------------
0x020000 N 22:22:22:22:22:22:22:22 scsi-fcp
0x050000 N 12:00:00:00:00:00:00:56 scsi-fcp
```

指定したインターフェイスで設定されているすべての仮想 N ポートの表示

```
switch# show san-ext-tuner interface gigabitethernet 3/4 nport pWWN 12:00:00:00:00:00:00:56
 vsan 200 counters
Statistics for nport
Node name 10:00:00:00:00:00:00:00 Port name 12:00:00:00:00:00:00:56
I/Os per second : 148
Read : 0%
Write : 100%
Ingress MB per second : 0.02 MBs/sec (Max -0.02 MBs/sec)
Egress MB per second : 73.97 MBs/sec (Max -75.47 MBs/sec))
Average Response time per I/O : Read - 0 us, Write - 13432 us
Maximum Response time per I/O : Read - 0 us, Write - 6953 us
Minimum Response time per I/O : Read - 0 us, Write - 19752 us
Errors : 0
```

指定したギガビットイーサネットインターフェイスで設定されている N ポートの表示

```
switch# show san-ext-tuner interface gigabitethernet 3/1
--------------------------------------------------------------------------------
Interface          NODE NAME               PORT                       NAME VSAN
--------------------------------------------------------------------------------
GigabitEthernet3/1 10:00:00:00:00:00:00:00 10:00:00:00:00:00:00:01 91
```

指定した N ポートに対して設定されている転送可能サイズの表示

```
switch# show san-ext-tuner interface gigabitethernet 3/1 nport pWWN 10:0:0:0:0:0:0:1
vsan 91
Node name : 10:00:00:00:00:00:00:00
Port name : 10:00:00:00:00:00:00:01
Transfer ready size : all
```

スイッチで設定されているすべての仮想 N ポートの表示

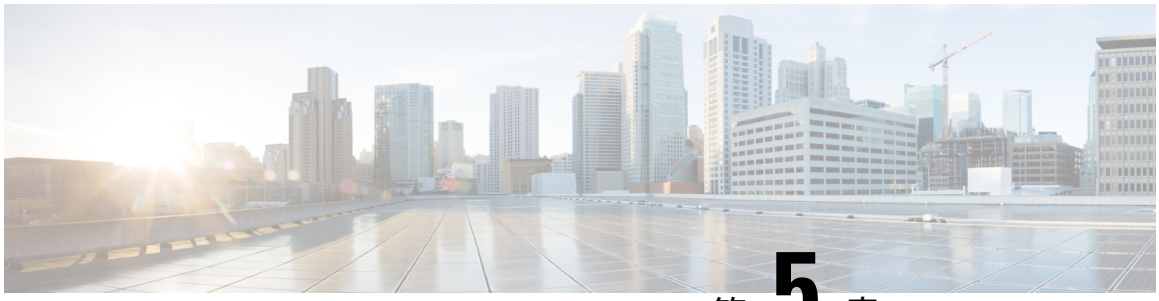
```
switch# show san-ext-tuner nports
--------------------------------------------------------------------------------
Interface          NODE NAME               PORT NAME                  VSAN
--------------------------------------------------------------------------------
GigabitEthernet3/1 10:00:00:00:00:00:00:00 10:00:00:00:00:00:00:01 91
```

調整パラメータのデフォルト設定

次の表に、調整パラメータのデフォルト設定を示します。

表 *6:* デフォルトの調整パラメータ

パラメータ	デフォルト
調整	ディセーブル
転送可能サイズ	SCSI **write** コマンドの転送サイズと同じ
未処理の入出力	1
トランザクション数	1
データ生成フォーマット	すべてゼロのフォーマット
ファイル マーキング頻度	0



第 5 章

iSCSI の構成

Cisco MDS 9000 ファミリの IP ストレージ（IPS）サービスは、オープン規格の IP ベース テクノロジーを使用することによって、ファイバ チャネル SAN の到達距離を延長します。IP ホストは Internet Small Computer Systems Interface（iSCSI）プロトコルを使用して、ファイバ チャネル ストレージにアクセスできます。

（注） iSCSI 機能は IPS ポートを搭載したファイバ チャネル モジュール固有で、Cisco MDS 9200 スイッチまたは Cisco MDS 9500 ディレクタで使用可能です。Cisco MDS NX-OS リリース 7.3(0)DY(1) 以降で iSCSI は 24/10 ポート SAN の拡張モジュールを搭載した Cisco MDS 9700 Director でサポートされていません。

Cisco MDS 9216i スイッチと 14/2 マルチプロトコル サービス（MPS-14/2）モジュールでは、ファイバ チャネル、FCIP、および iSCSI 機能も使用できます。MPS-14/2 モジュールは、Cisco MDS 9200 シリーズまたは Cisco MDS 9500 シリーズのすべてのスイッチで使用できます。

この章は、次の項で構成されています。

- iSCSI の概要 （82 ページ）
- **iSCSI の構成** （85 ページ）
- iSLB の構成 （135 ページ）
- VRRP を使用するロード バランシング （150 ページ）
- CFS を使用した iSLB 構成の配信 （156 ページ）
- CFS を使用した iSLB 構成の配信 （157 ページ）
- iSCSI ハイ アベイラビリティ （161 ページ）
- iSCSI 認証設定時の注意事項およびシナリオ （168 ページ）
- Internet Storage Name Service の概要 （190 ページ）
- デフォルト設定 （209 ページ）

iSCSI の概要

Cisco MDS 9000 ファミリの IP ストレージ（IPS）サービスは、オープン規格の IP ベース テクノロジーを使用することによって、ファイバ チャネル SAN の到達距離を延長します。iSCSI 機能は、IP ネットワーク内の iSCSI ホストと、Cisco MDS 9000 ファミリ スイッチの任意のファイバ チャネル インターフェイスからアクセス可能なファイバ チャネル SAN のファイバ チャネル ストレージ デバイス間で、iSCSI 要求および応答をルーティングします。iSCSI プロトコルを使用して、 iSCSI ドライバは、iSCSI ホストからの SCSI の要求と応答を IP ネットワークを介して転送できます。iSCSI 機能を使用するには、ファブリック内の目的のスイッチ上で iSCSI を明示的にイネーブルにする必要があります。

（注） iSCSI 機能は、Cisco Fabric Switch for HP c-Class Bladesystem および Cisco Fabric Switch for IBM BladeCenter ではサポートされません。

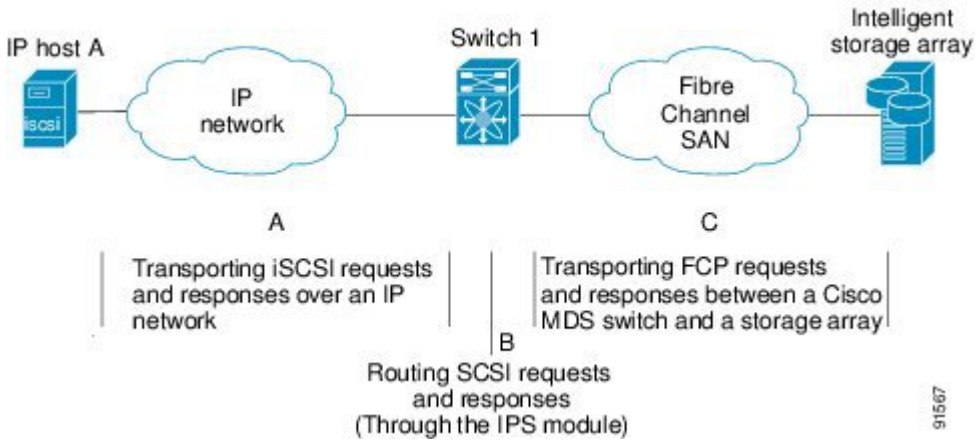
iSCSI 機能は、IP ネットワーク内の iSCSI ホストと、Cisco MDS 9000 ファミリ スイッチの任意のファイバ チャネル インターフェイスからアクセス可能なファイバ チャネル SAN のファイバ チャネル ストレージ デバイス間で、iSCSI 要求および応答をルーティングします。

IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールを介してストレージにアクセスする必要がある 各 iSCSI ホストには、互換性のある iSCSI ドライバをインストールしておく必要があります。iSCSI プロトコルを使用して、iSCSI ドライバは、iSCSI ホストからの SCSI の要求と応答を IP ネットワークを介して転送できます。ホストのオペレーティング システムの観点から、iSCSI ドライバは、ホスト内にファイバ チャネル ドライバに似た SCSI 転送ドライバであるように見えます。

IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールは、透過型 SCSI ルーティングを実行します。iSCSI プロトコルを使用する IP ホストは、ファイバ チャネル ネットワーク上のターゲットに透過的にアクセスできます。

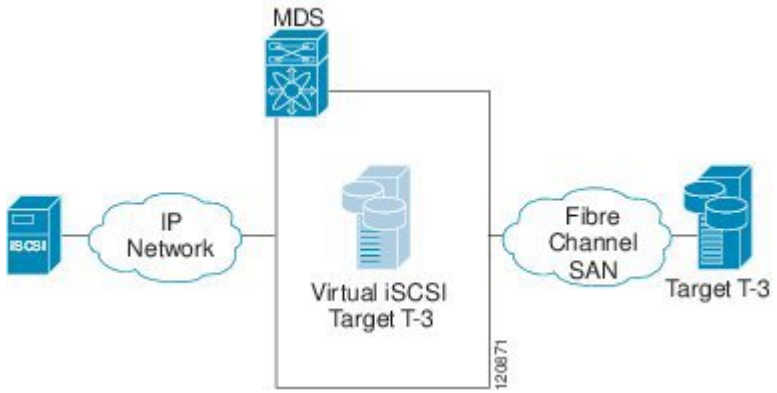
IP ネットワークを介して IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールに接続し、ファイバ チャネル SAN 上のファイバ チャネル ストレージにアクセスする、iSCSI ホストの一般的な構成例を示します（ 次の図を参照）。

図 *15 : iSCSI* 要求および応答の転送（透過型 *iSCSI* ルーティングの場合）



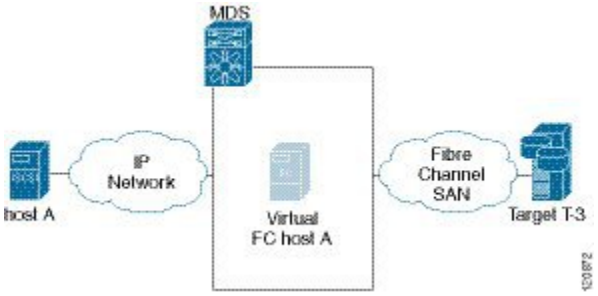
IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールは、独立した iSCSI SAN ビューおよびファイバ チャネル SAN ビューを作成します。iSCSI SAN ビューの場合、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールが iSCSI 仮想ターゲットを作成し、それをファイバ チャネル SAN で使用できる物理ファイバ チャネル ターゲットに対応付けます。これらのモジュールは、物理 iSCSI ターゲットが IP ネットワークに接続されているかのように、ファイバ チャネル ターゲットを IP ホストに提示します。

図 *16 : iSCSI SAN* ビュー：*iSCSI* 仮想ターゲット



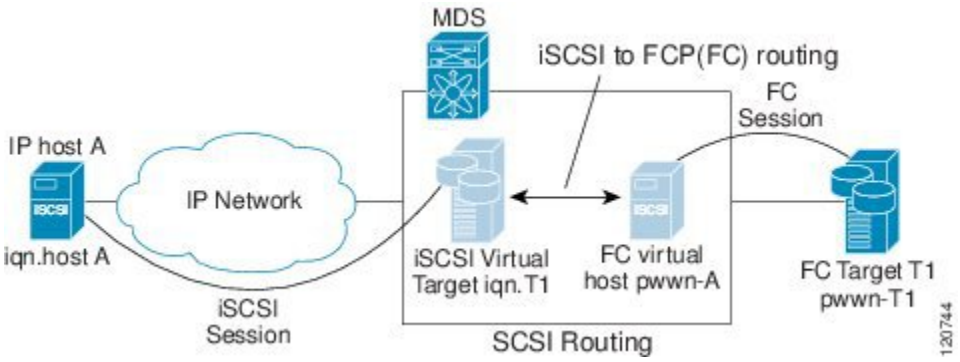
ファイバ チャネル SAN ビューの場合、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールが仮想ファイバ チャネル ホストとして iSCSI ホストを提示します。ストレージ デバイスは、実ファイバ チャネル ホストで実行される通信と同様に、仮想ファイバ チャネル ホストと通信します。

図 *17 :* ファイバ チャネル *SAN* ビュー：*HBA* としての *iSCSI* ホスト



IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールは、iSCSI 仮想ターゲットと仮想ファイバ チャネル ホスト間で、コマンドを透過的にマッピングします。

図 *18 : iSCSI* から *FCP*（ファイバ チャネル）へのルーティング



IP ホストからファイバ チャネル ストレージ デバイスへのルーティングでは、主に次の処理が実行されます。

- IP ネットワークを介して、ホストと IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュール間で iSCSI 要求および応答が転送されます。
- IP ネットワーク上のホストとファイバチャネル ストレージデバイス間で、SCSI 要求および応答がルーティングされます（iSCSI を FCP に変換したり、その逆の変換を行ったりします）。IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールで、この変換とルーティングを実行します。
- IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールとファイバ チャネル ストレージ デバイス間で、FCP 要求または応答が転送されます。

（注） iSCSI に相当するファイバ チャネル(FCP)は、ファイバ チャネル SAN を介して SCSI コマンドを伝送します。iSCSI プロトコルの詳細については、http://www.ietf.org で IP ストレージに関する IETF 標準規格を参照してください。

iSCSI の設定制限

iSCSI の設定に関しては、次の限度があります。

- ファブリックでサポートされる iSCSI および iSLB 発信側の最大数は 2000 です。
- サポートされる iSCSI および iSLB 発信側の最大数はポートごとに 200 です。
- 透過型またはプロキシイニシエータ モードで IPS ポートがサポートする iSCSI および iSLB セッションの最大数は 500 です。
- スイッチがサポートする iSCSI および iSLB セッションの最大数は 5000 です。
- ファブリックでサポートされる iSCSI および iSLB ターゲットの最大数は 6000 です。

iSCSI の構成

Cisco MDS 9000 ファミリの IP ストレージ（IPS）サービスは、オープン規格の IP ベース テクノロジーを使用することによって、ファイバ チャネル SAN の到達距離を延長します。IP ホストは Internet Small Computer Systems Interface（iSCSI）プロトコルを使用して、ファイバ チャネル ストレージにアクセスできます。

（注） iSCSI 機能は IPS ポートを搭載したファイバ チャネル モジュール固有で、Cisco MDS 9200 スイッチまたは Cisco MDS 9500 ディレクタで使用可能です。Cisco MDS NX-OS リリース 7.3(0)DY(1) 以降で iSCSI は 24/10 ポート SAN の拡張モジュールを搭載した Cisco MDS 9700 Director でサポートされていません。

Cisco MDS 9216i スイッチと 14/2 マルチプロトコル サービス（MPS-14/2）モジュールでは、ファイバ チャネル、FCIP、および iSCSI 機能も使用できます。MPS-14/2 モジュールは、Cisco MDS 9200 シリーズまたは Cisco MDS 9500 シリーズのすべてのスイッチで使用できます。

（注） ギガビット イーサネット インターフェイスの構成については、「IPv4 の基本的なギガビット イーサネット構成」のセクションを参照してください。

この章は、次の項で構成されています。

iSCSI のイネーブル化

iSCSI 機能を使用するには、ファブリック内の目的のスイッチ上で iSCSI を明示的に有効にする必要があります。別の方法として Fabric Manager または Device Manager を使用しても、必要なモジュールで直接 iSCSI の機能をイネーブルまたはディセーブルにできます。デフォルトでは、この機能は Cisco MDS 9000 ファミリのすべてのスイッチでディセーブルになっています。

参加させるスイッチの iSCSI を有効にするには、次のステップを実行します。

始める前に

この機能をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

手順

ステップ 1 構成コマンドを1行に1つずつ入力します。CNTL/Z で終了します

switch# **config terminalerminal**

ステップ 2 スイッチ上で iSCSI を有効にします。

switch(config)# **feature iscsi**

ステップ 3 現在のスイッチ上で iSCSI を無効（デフォルト）にします。

switch(config)# **no feature iscsi**

ステップ 4 スイッチ上で iSCSI モジュールを有効にします。

switch(config)# **iscsi enable module <x>**

（注）
SME と iSCSI を同一スイッチ上で使用可能にする新しいコマンドが追加されました。

ステップ 5 スイッチの iSCSI モジュールを無効にします。

switch(config)# **no iscsi enable module <x>**

仮想ファイバ チャネル ホストとしての iSCSI ホストの提示

IPS ポートまたは MPS-14/2 モジュールを搭載したファイバ チャネルは、iSCSI ホストの代わりにファイバ チャネル ストレージ デバイスに接続し、ストレージ デバイスにコマンドを送信し、ストレージデバイスと相互にデータを転送します。これらのモジュールでは、仮想ファイバ チャネル N ポートを使用して、iSCSI ホストに代わってファイバ チャネル ストレージ デバイスにアクセスします。iSCSI ホストは、iSCSI 修飾名（IQN）または IP アドレスにより識別されます。

iSCSI インターフェイスの作成

IPS ポートを搭載したファイバチャネルモジュール、MPS-14/2 モジュール、または Cisco MDS 9250i マルチサービス ファブリック スイッチの 1/10Gbps IP ストレージ ポートの各物理ギガビット イーサネット インターフェイスを使用すると、iSCSI 要求を変換してファイバ チャネル ターゲットにルーティングできます。反対方向では、応答を変換してルーティングできま

す。この機能をイネーブルにするには、対応する iSCSI インターフェイスがイネーブル ステートでなければなりません。

iSCSI インターフェイスを有効にするには、次のステップを実行します。

始める前に

tcp maximum-bandwidth-kbps および **tcp maximum-bandwidth-mbps** コマンドを使用して iSCSI の速度を構成し、**switchport speed** コマンドを使用して物理 IP ストレージ ポートの速度を 1Gbps または 10Gbps に設定します。Cisco MDS スイッチは、基盤となる物理ギガビット イーサネット ポートまたは IP ストレージ ポートの速度に基づいて iSCSI tcp maximum-bandwidth-kbps と maximum-bandwidth-mbps を制限しません。したがって、iSCSI **tcp maximum-bandwidth-kbps** および **tcp maximum-bandwidth-mbps** コマンドを、速度 1 Gbps で実行している物理 IP ストレージ ポートで 10Gbps に相当する速度に構成できてしまいます。TCP 最大帯域幅を構成するときには、物理 IP ストレージ ポートの最大速度を超えないようにしてください。

手順

ステップ 1 必要なギガビット イーサネット インターフェイスをイネーブルにします。

```
switch# config terminal
switch(config)# interface gigabitethernet 2/1
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)#
```

ステップ 2 必要な iSCSI インターフェイスを作成し、このインターフェイスを有効にします。

```
switch(config)# interface iscsi 2/1
switch(config-if)# no shutdown
```

iSCSI ターゲットとしてのファイバ チャネル ターゲットの提示

IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールは、物理ファイバ チャネル ターゲットを iSCSI 仮想ターゲットとして提示し、 iSCSI ホストからこれらへのアクセスを許可します。このモジュールは、これらのターゲットを次の 2 つのうちいずれかの方法で示します。

- ダイナミック マッピング：すべてのファイバ チャネル ターゲット デバイスまたはポートを iSCSI デバイスとして、自動的に対応付けます。このマッピングを使用して、自動 iSCSI ターゲット名が作成されます。

  。
- スタティック マッピング：手動で iSCSI ターゲット デバイスを作成し、ファイバ チャネル ターゲット ポート全体またはファイバ チャネル LUN のサブセットに対応付けます。このマッピングの場合は、ユーザー側で一意の iSCSI ターゲット名を指定する必要があります。

スタティック マッピングは、iSCSI ホストをファイバ チャネル ターゲット内の LU のサブセットに限定する必要がある場合、iSCSI アクセス コントロールが必要な場合、またはその両方が当てはまる場合に使用します（「iSCSI アクセス コントロール」を参照）。また、スタティック マッピングを使用すると、冗長ファイバ チャネル ポートがファイバ チャネル ターゲットの LU に到達可能な場合、透過的なフェールオーバを構成できます（「透過的なフェールオーバ」を参照）。

（注） IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールはデフォルトで、iSCSI にファイバ チャネル ターゲットをインポートしません。IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールで iSCSI 発信側からファイバ チャネル ターゲットを使用できるようにするには、ダイナミック マッピングまたはスタティック マッピングを構成しておく必要があります。

ダイナミック マッピング

ダイナミック マッピングを構成すると、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールはすべてのファイバ チャネル ターゲットを iSCSI ドメインにインポートし、各物理ファイバ チャネル ターゲット ポートを 1 つの iSCSI ターゲットとしてマッピングします。つまり、物理ストレージ ターゲット ポートを介してアクセス可能なすべての LU は、物理ファイバ チャネル ターゲット ポートの場合と同じ論理ユニット番号（LUN）を持つ iSCSI LU として使用できます。

iSCSI ターゲット ノード名は、iSCSI 修飾名 （IQN）フォーマットを使用して、自動的に作成されます。iSCSI 修飾名の長さは、最大 223、最小 16 の英数字に制限されています。

名前は SAN 内で一意である必要があるため、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールでは次の規則に従って、IQN フォーマットの iSCSI ターゲット ノード名を作成します。

- Virtual Router Redundancy Protocol（VRRP）グループまたはポート チャネルに属していない IPS ギガビット イーサネット ポートでは、次のフォーマットを使用します。

  `iqn.1987-05.com.cisco:05.<mgmt-ip-address>.<slot#>-<port#>-<sub-intf#>.<Target-pWWN>`
- VRRP グループに属している IPS ポートでは、次のフォーマットを使用します。

  `iqn.1987-05.com.cisco:05.vrrp-<vrrp-ID#>-<vrrp-IP-addr>.<Target-pWWN>`
- ポート チャネルの一部であるポートではこのフォーマットを使用します。

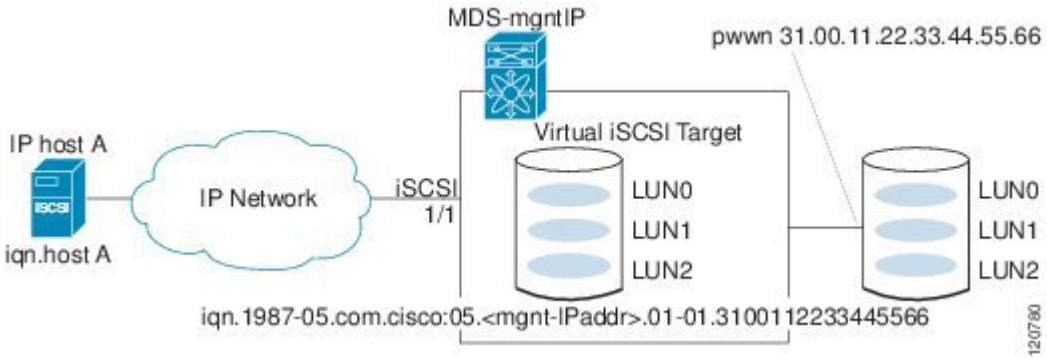
  `iqn.1987-02.com.cisco:02.<mgmt-ip-address>.pc-<port-ch-sub-intf#>.<Target-pWWN>`

（注） スイッチ名が設定されている場合、スイッチ名は管理 IP アドレスの代わりに使用されます。スイッチ名が設定されていない場合は、管理 IP アドレスが使用されます。

Cisco MDS 9000 ファミリ スイッチ内の各 IPS ポートはこの規則に従って、SAN 内の同じファイバ チャネル ターゲット ポートに対して一意の iSCSI ターゲット ノード名を作成します。

たとえば、pWWN が 31:00:11:22:33:44:55:66 のファイバ チャネル ターゲット ポートに対して iSCSI ターゲットが作成され、その pWWN に LUN 0、LUN 1、および LUN 2 が含まれる場合、これらの LUN は、iSCSI ターゲット ノード名 iqn.1987-05.com.cisco:05.*MDS_switch_management_IP_address* .

図 *19* : ダイナミック ターゲット マッピング



（注） 構成されているアクセス コントロール メカニズムによっては、個々の iSCSI イニシエータで一部のターゲットにアクセスできない場合があります（「iSCSI アクセス コントロール」を参照）。

ファイバ チャネル ターゲットから *iSCSI* へのダイナミック マッピングを有効にする

ファイバ チャネル ターゲットから iSCSI へのダイナミック マッピングを有効にするには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 IPS ポートを搭載したファイバ チャネル モジュールと MPS-14/2 モジュールは、ファイバ チャネル SAN のファイバチャネル ターゲットをすべて IP ネットワークにダイナミックにインポートします。

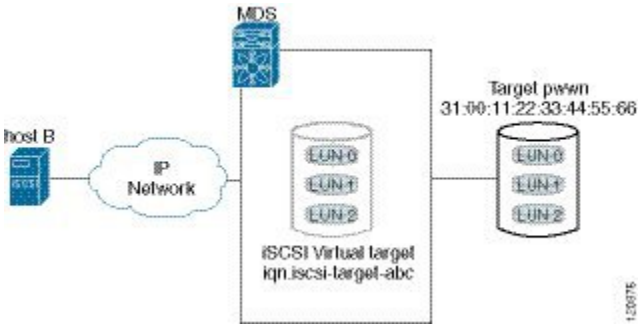
```
switch(config)# iscsi import target fc
```

スタティック マッピング

ユーザーが定義した一意の iSCSI ノード名を割り当てることによって、 iSCSI ターゲットを手動で（スタティックに）作成できます。iSCSI 修飾名の長さは、最小 16 文字、最大 223 文字に制限されています。スタティック マッピングの iSCSI ターゲットでは、ファイバチャネル ターゲット ポート全体をマッピング（ターゲット ポート内のすべての LUN を iSCSI ターゲットに

マッピング）することも、ファイバ チャネル ターゲット ポートの 1 つまたは複数の LU を含めることもできます。

図 *20 :* スタティック マッピングの *iSCSI* ターゲット



（注） iSCSI ターゲットに複数のファイバ チャネル ターゲット ポートを含めることはできません。ファイバ チャネル ターゲット ポート全体をすでにマッピングしている場合、LUN マッピング オプションは使用できません。

スタティックにマッピングされたターゲットへのアクセスを制御する手順については、「iSCSI ベース アクセス コントロール」セクションを参照してください。

スタティック iSCSI ターゲットのアドバタイズ

スタティック iSCSI ターゲットをアドバタイズする場合に経由するギガビット イーサネット インターフェイスを制限できます。デフォルトでは、iSCSI ターゲットはすべてのギガビット イーサネットインターフェイス、サブインターフェイス、ポートチャネルインターフェイス、およびポート チャネル サブインターフェイスでアドバタイズされます。

iSCSI 仮想ターゲットをアドバタイズするインターフェイスを構成する

iSCSI 仮想ターゲットをアドバタイズする特定のインターフェイスを構成するステップは、次のとおりです。

手順

ステップ 1 指定されたインターフェイスでのみ、仮想ターゲットをアドバタイズします。デフォルトでは、すべての IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールのすべてのインターフェイスでアドバタイズされます。

```
switch(config-iscsi-tgt)# advertise interface GigabitEthernet 2/5
```

（注）
仮想ターゲットを複数インターフェイスでアドバタイズするには、インターフェイスごとに次のコマンドを発行します。

ステップ 2 ターゲットのアドバタイズ元インターフェイスのリストから、このインターフェイスを削除します。

```
switch(config-iscsi-tgt)# no advertise interface GigabitEthernet 2/5
```

iSCSI 仮想ターゲットの設定例

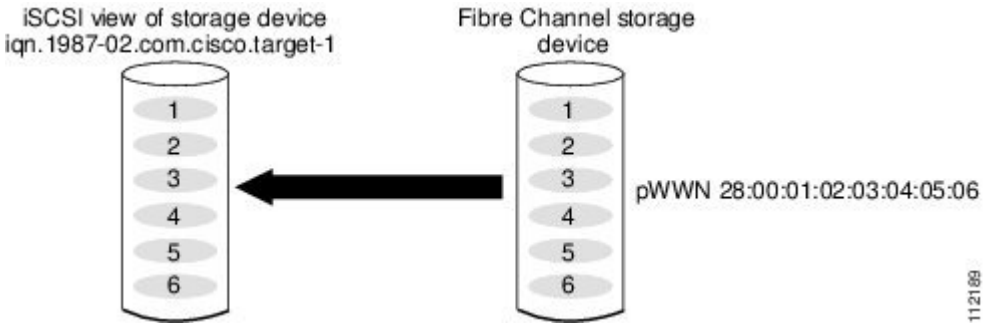
ここでは、3 種類の iSCSI 仮想ターゲット設定例を示します。

例 1

iSCSI 仮想ターゲットとしてファイバ チャネル ターゲット全体を割り当てる例を示します。ファイバ チャネル ターゲットに属しているすべての LUN を iSCSI ターゲットの一部として使用できます。

```
iscsi virtual-target name iqn.1987-02.com.cisco.target-1
pWWN 28:00:01:02:03:04:05:06
```

図 *21 : iSCSI* ノード名の割り当て

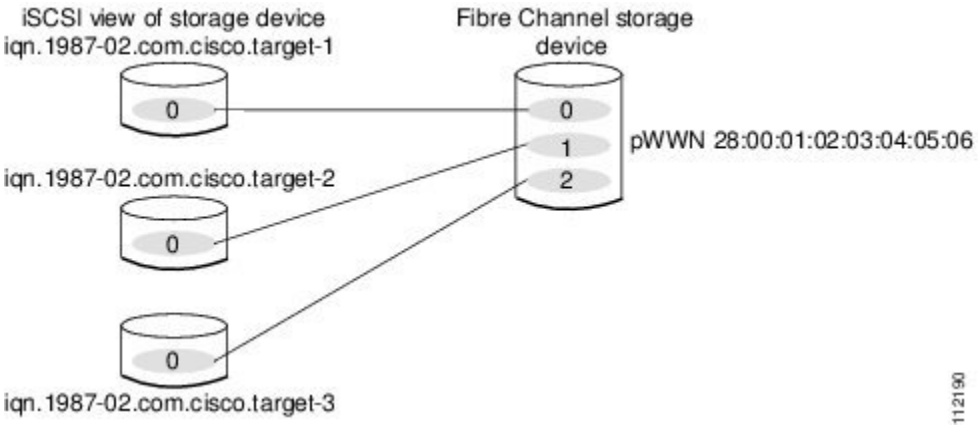


例 2

ファイバ チャネル ターゲットの LUN のサブセットを 3 つの iSCSI 仮想ターゲットにマッピングする例を示します。各 iSCSI ターゲットが所有する LUN は 1 つのみです。

```
iscsi virtual-target name iqn.1987-02.com.cisco.target-1
pWWN 28:00:01:02:03:04:05:06 fc-lun 0 iscsi-lun 0
iscsi virtual-target name iqn.1987-02.com.cisco.target-2
pWWN 28:00:01:02:03:04:05:06 fc-lun 1 iscsi-lun 0
iscsi virtual-target name iqn.1987-02.com.cisco.target-3
pWWN 28:00:01:02:03:04:05:06 fc-lun 2 iscsi-lun 0
```

図 *22 : iSCSI* ノード名への *LUN* のマッピング

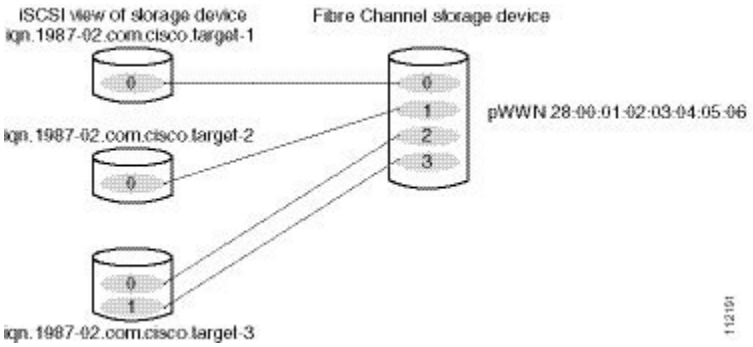


例 3

ファイバ チャネル LUN ターゲットの 3 つのサブセットを 3 つの iSCSI 仮想ターゲットにマッピングする例を示します。2 つの iSCSI ターゲットで LUN を 1 つ使用し、3 つ目の iSCSI ターゲットで LUN を 2 つ使用します。

```
iscsi virtual-target name iqn.1987-02.com.cisco.target-1
pWWN 28:00:01:02:03:04:05:06 fc-lun 0 iscsi-lun 0
iscsi virtual-target name iqn.1987-02.com.cisco.target-2
pWWN 28:00:01:02:03:04:05:06 fc-lun 1 iscsi-lun 0
iscsi virtual-target name iqn.1987-02.com.cisco.target-3
pWWN 28:00:01:02:03:04:05:06 fc-lun 2 iscsi-lun 0
pWWN 28:00:01:02:03:04:05:06 fc-lun 3 iscsi-lun 1
```

図 *23 :* 複数の *iSCSI* ノード名への *LUN* のマッピング



iSCSI ターゲットとしてのファイバ チャネル ターゲットの提示

IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールは、物理ファイバ チャネル ターゲットを iSCSI 仮想ターゲットとして提示し、 iSCSI ホストからこれらへのアクセスを許可します。このモジュールは、これらのターゲットを次の2つのうちいずれかの方法で示します。

- ダイナミック マッピング：すべてのファイバ チャネル ターゲット デバイスまたはポートを iSCSI デバイスとして、自動的に対応付けます。このマッピングを使用して、自動 iSCSI ターゲット名が作成されます。

。

- スタティック マッピング：手動で iSCSI ターゲット デバイスを作成し、ファイバ チャネル ターゲット ポート全体またはファイバ チャネル LUN のサブセットに対応付けます。このマッピングの場合は、ユーザー側で一意の iSCSI ターゲット名を指定する必要があります。

スタティック マッピングは、iSCSI ホストをファイバ チャネル ターゲット内の LU のサブセットに限定する必要がある場合、iSCSI アクセス コントロールが必要な場合、またはその両方が当てはまる場合に使用します（「iSCSI アクセス コントロール」を参照）。また、スタティック マッピングを使用すると、冗長ファイバ チャネル ポートがファイバ チャネル ターゲットの LU に到達可能な場合、透過的なフェールオーバを構成できます（「透過的なフェールオーバ」を参照）。

（注） IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールはデフォルトで、iSCSI にファイバ チャネル ターゲットをインポートしません。IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールで iSCSI 発信側からファイバ チャネル ターゲットを使用できるようにするには、ダイナミック マッピングまたはスタティック マッピングを構成しておく必要があります。

ダイナミック マッピング

ダイナミック マッピングを構成すると、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールはすべてのファイバ チャネル ターゲットを iSCSI ドメインにインポートし、各物理ファイバ チャネル ターゲット ポートを 1 つの iSCSI ターゲットとしてマッピングします。つまり、物理ストレージ ターゲット ポートを介してアクセス可能なすべての LU は、物理ファイバ チャネル ターゲット ポートの場合と同じ論理ユニット番号（LUN）を持つ iSCSI LU として使用できます。

iSCSI ターゲット ノード名は、iSCSI 修飾名 （IQN）フォーマットを使用して、自動的に作成されます。iSCSI 修飾名の長さは、最大 223、最小 16 の英数字に制限されています。

名前は SAN 内で一意である必要があるため、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールでは次の規則に従って、IQN フォーマットの iSCSI ターゲット ノード名を作成します。

- Virtual Router Redundancy Protocol（VRRP）グループまたはポートチャネルに属していない IPS ギガビット イーサネット ポートでは、次のフォーマットを使用します。

```
iqn.1987-05.com.cisco:05.<mgmt-ip-address>.<slot#>-<port#>-<sub-intf#>.<Target-pWWN>
```

- VRRP グループに属している IPS ポートでは、次のフォーマットを使用します。

```
iqn.1987-05.com.cisco:05.vrrp-<vrrp-ID#>-<vrrp-IP-addr>.<Target-pWWN>
```

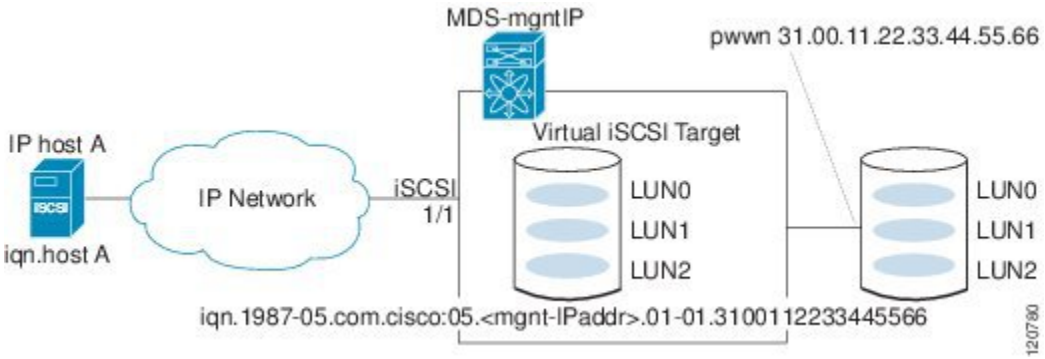
- ポート チャネルの一部であるポートではこのフォーマットを使用します。
  `iqn.1987-02.com.cisco:02.<mgmt-ip-address>.pc-<port-ch-sub-intf#>.<Target-pWWN>`

（注） スイッチ名が設定されている場合、スイッチ名は管理 IP アドレスの代わりに使用されます。スイッチ名が設定されていない場合は、管理 IP アドレスが使用されます。

Cisco MDS 9000 ファミリ スイッチ内の各 IPS ポートはこの規則に従って、SAN 内の同じファイバ チャネル ターゲット ポートに対して一意の iSCSI ターゲット ノード名を作成します。

たとえば、pWWN が 31:00:11:22:33:44:55:66 のファイバ チャネル ターゲット ポートに対して iSCSI ターゲットが作成され、その pWWN に LUN 0、LUN 1、および LUN 2 が含まれる場合、これらの LUN は、iSCSI ターゲット ノード名 iqn.1987-05.com.cisco:05.*MDS_switch_management_IP_address* .

図 *24 :* ダイナミック ターゲット マッピング

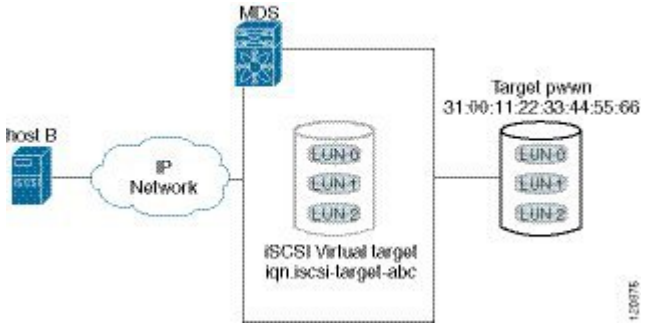


（注） 構成されているアクセス コントロール メカニズムによっては、個々の iSCSI イニシエータで一部のターゲットにアクセスできない場合があります（「iSCSI アクセス コントロール」を参照）。

スタティック マッピング

ユーザーが定義した一意の iSCSI ノード名を割り当てることによって、 iSCSI ターゲットを手動で（スタティックに）作成できます。iSCSI 修飾名の長さは、最小 16 文字、最大 223 文字に制限されています。スタティック マッピングの iSCSI ターゲットでは、ファイバ チャネル ターゲット ポート全体をマッピング（ターゲット ポート内のすべての LUN を iSCSI ターゲットにマッピング）することも、ファイバ チャネル ターゲット ポートの 1 つまたは複数の LU を含めることもできます。

図 *25* : スタティック マッピングの *iSCSI* ターゲット



（注） iSCSI ターゲットに複数のファイバ チャネル ターゲット ポートを含めることはできません。ファイバ チャネル ターゲット ポート全体をすでにマッピングしている場合、LUN マッピング オプションは使用できません。

スタティックにマッピングされたターゲットへのアクセスを制御する手順については、「iSCSI ベース アクセス コントロール」セクションを参照してください。

スタティック iSCSI ターゲットのアドバタイズ

スタティック iSCSI ターゲットをアドバタイズする場合に経由するギガビット イーサネット インターフェイスを制限できます。デフォルトでは、iSCSI ターゲットはすべてのギガビット イーサネットインターフェイス、サブインターフェイス、ポートチャネルインターフェイス、およびポート チャネル サブインターフェイスでアドバタイズされます。

iSCSI 仮想ターゲットをアドバタイズするインターフェイスを構成する

iSCSI 仮想ターゲットをアドバタイズする特定のインターフェイスを構成するステップは、次のとおりです。

手順

ステップ 1 指定されたインターフェイスでのみ、仮想ターゲットをアドバタイズします。デフォルトでは、すべての IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールのすべてのインターフェイスでアドバタイズされます。

```
switch(config-iscsi-tgt)# advertise interface GigabitEthernet 2/5
```

（注）
仮想ターゲットを複数インターフェイスでアドバタイズするには、インターフェイスごとに次のコマンドを発行します。

ステップ 2 ターゲットのアドバタイズ元インターフェイスのリストから、このインターフェイスを削除します。

```
switch(config-iscsi-tgt)# no advertise interface GigabitEthernet 2/5
```

仮想ファイバ チャネル ホストとしての iSCSI ホストの提示

IPS ポートまたは MPS-14/2 モジュールを搭載したファイバ チャネルは、iSCSI ホストの代わりにファイバ チャネル ストレージ デバイスに接続し、ストレージ デバイスにコマンドを送信し、ストレージデバイスと相互にデータを転送します。これらのモジュールでは、仮想ファイバ チャネル N ポートを使用して、iSCSI ホストに代わってファイバ チャネル ストレージ デバイスにアクセスします。iSCSI ホストは、iSCSI 修飾名（IQN）または IP アドレスにより識別されます。

イニシエータ識別モードの指定

イニシエータ識別モードを指定するには、次のステップを実行します。

手順

ステップ 1 すべてのイニシエータを識別するスイッチ上の iSCSI インターフェイスを選択します。

```
switch# config terminal
switch(config)# interface iscsi 4/1
switch(config-if)#
```

ステップ 2 IP アドレスに基づいて iSCSI イニシエータを識別します。

```
switch(config-if)# switchport initiator id ip-address
```

ステップ 3 イニシエータ ノード名に基づいて iSCSI イニシエータを識別します。これはデフォルトの動作です。

```
switch(config-if)# switchport initiator id name
```

iSCSI 仮想ターゲットの設定例

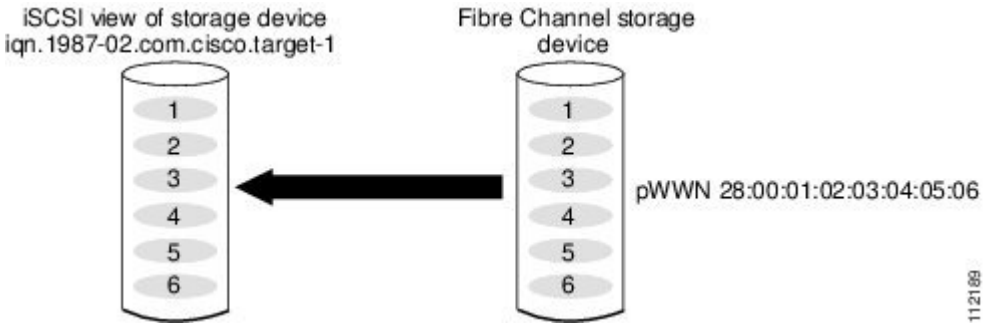
ここでは、3 種類の iSCSI 仮想ターゲット構成例を示します。

iSCSI 仮想ターゲットとしてファイバ チャネル ターゲット全体を割り当てます。

iSCSI 仮想ターゲットとしてファイバ チャネル ターゲット全体を割り当てる例を示します。ファイバ チャネル ターゲットに属しているすべての LUN を iSCSI ターゲットの一部として使用できます。

```
iscsi virtual-target name iqn.1987-02.com.cisco.target-1
pWWN 28:00:01:02:03:04:05:06
```

図 *26 : iSCSI* ノード名の割り当て

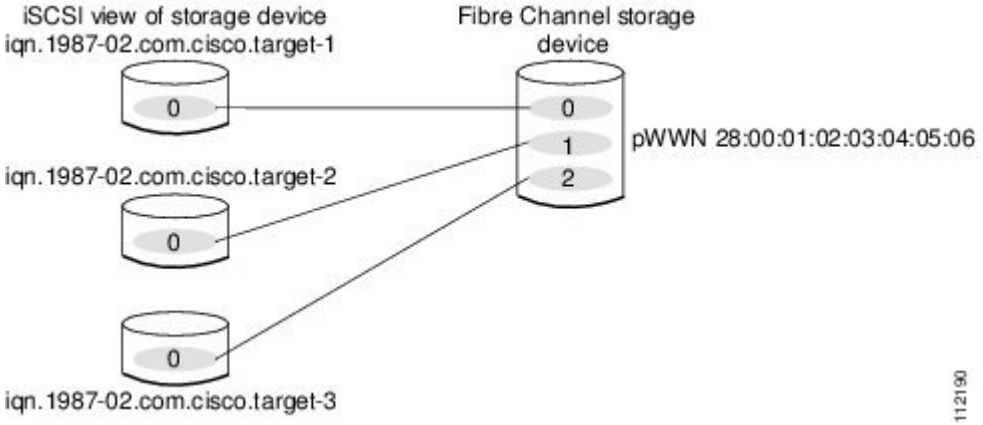


ファイバ チャネル ターゲットの LUN のサブセットを 3 つの iSCSI 仮想ターゲットにマッピング

ファイバ チャネル ターゲットの LUN のサブセットを 3 つの iSCSI 仮想ターゲットにマッピングする例を示します。各 iSCSI ターゲットが所有する LUN は 1 つのみです。

```
iscsi virtual-target name iqn.1987-02.com.cisco.target-1
pWWN 28:00:01:02:03:04:05:06 fc-lun 0 iscsi-lun 0
iscsi virtual-target name iqn.1987-02.com.cisco.target-2
pWWN 28:00:01:02:03:04:05:06 fc-lun 1 iscsi-lun 0
iscsi virtual-target name iqn.1987-02.com.cisco.target-3
pWWN 28:00:01:02:03:04:05:06 fc-lun 2 iscsi-lun 0
```

図 *27 : iSCSI* ノード名への *LUN* のマッピング



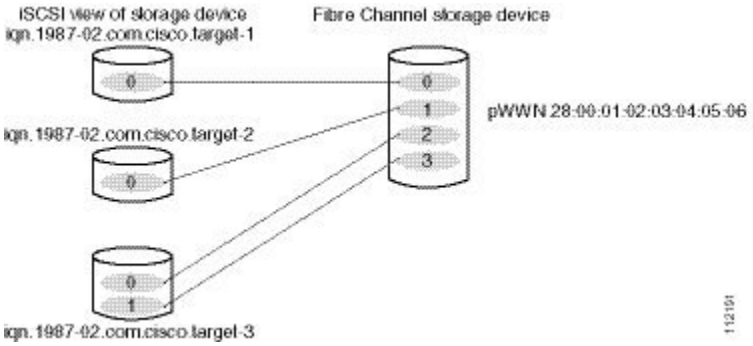
ファイバ チャネル LUN ターゲットの 3 つのサブセットを 3 つの iSCSI 仮想ターゲットにマッピング

ファイバ チャネル LUN ターゲットの 3 つのサブセットを 3 つの iSCSI 仮想ターゲットにマッピングする例を示します。2 つの iSCSI ターゲットで LUN を 1 つ使用し、3 つ目の iSCSI ターゲットで LUN を 2 つ使用します。

```
iscsi virtual-target name iqn.1987-02.com.cisco.target-1
pWWN 28:00:01:02:03:04:05:06 fc-lun 0 iscsi-lun 0
iscsi virtual-target name iqn.1987-02.com.cisco.target-2
pWWN 28:00:01:02:03:04:05:06 fc-lun 1 iscsi-lun 0
iscsi virtual-target name iqn.1987-02.com.cisco.target-3
```

```
pWWN 28:00:01:02:03:04:05:06 fc-lun 2 iscsi-lun 0
pWWN 28:00:01:02:03:04:05:06 fc-lun 3 iscsi-lun 1
```

図 *28* : 複数の *iSCSI* ノード名への *LUN* のマッピング



発信側提供モード

ファイバ チャネル ファブリックの iSCSI ホストは、透過型イニシエータ モードおよびプロキシ イニシエータ モードの 2 種類のモードで提供できます。

- 透過型イニシエータ モードでは、各 iSCSI ホストが 1 つの仮想ファイバ チャネル ホストとして提供されます。トランスペアレント モードの利点は、ファイバ チャネル アクセス コントロールを「実」ファイバ チャネル ホストを管理する場合と同様に、きめ細かく設定できることです。iSCSI からファイバ チャネルへの 1 対 1 のマッピングなので、ファイバ チャネル ストレージ デバイスに関して、ホストごとに異なるゾーン分割または LUN アクセス コントロールを設定できます。
- プロキシ イニシエータ モードでは、1 つの IPS ポートに与えられる仮想ファイバ チャネル ホストは 1 つだけであり、すべての iSCSI ホストがその仮想ファイバ チャネル ホストを使用して、ファイバ チャネル ターゲットにアクセスします。ファイバ チャネル ストレージ デバイスでホストごとに明示的な LUN アクセス コントロールを必要とするシナリオでは、iSCSI 発信側ごとのスタティックな設定は大きな負担となる可能性があります。このような状況では、プロキシ イニシエータ モードを使用すると、設定が簡素化されます。

（注） iSLB VRRP グループに属している iSCSI インターフェイスについて、プロキシ イニシエータ モードをイネーブルにすると、インターフェイスのロード バランシングが影響を受けます。「iSCSI インターフェイス パラメータの変更およびロード バランシングへの影響」セクションを参照してください

Cisco MDS スイッチは、次の iSCSI セッション制限をサポートします。

- スイッチ上の最大 iSCSI セッション数は 5000 です。
- 透過型イニシエータ モードの場合、各 IPS ポートの最大 iSCSI セッション数は 500 です。

- プロキシ イニシエータ モードの場合、各 IPS ポートの最大 iSCSI セッション数は 500 です。
- IPS ポートで作成できる同時セッションの最大数は 5 です（サポート可能なセッションの合計数は 500）。

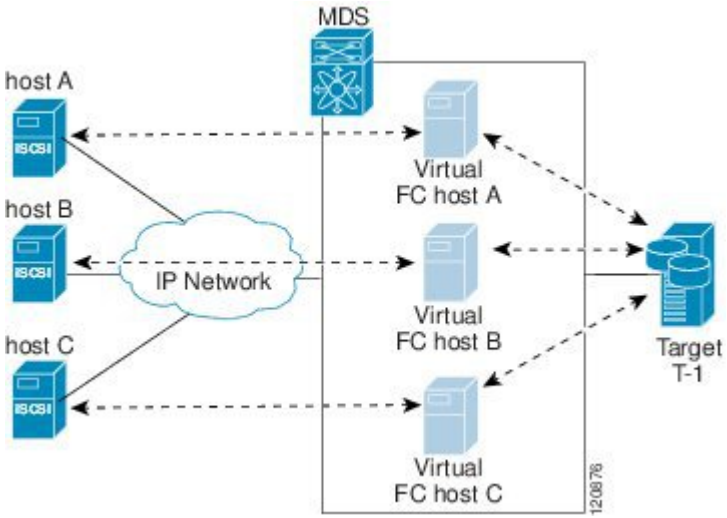
（注） ポート上で 6 つ以上の iSCSI セッションを同時にアクティブにしようとすると、発信側に一時的なエラーが伝えられ、あとでセッションの作成を再試行することになります。

透過型イニシエータ モード

個々の iSCSI ホストが、1 つの仮想ファイバ チャネル ホスト（つまり、1 つのファイバ チャネル N ポート）として提供されます。トランスペアレント モードの利点は、ファイバ チャネル アクセス コントロールをきめ細かく設定できることです。iSCSI からファイバ チャネルへの 1 対 1 のマッピングなので、ファイバ チャネル ストレージ デバイスに関して、ホストごとに異なるゾーン分割または LUN アクセス コントロールを設定できます。

iSCSI ホストから IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールに接続すると、そのホスト用の仮想ホスト N ポート（HBA ポート）が作成されます。ファイバ チャネル N ポートごとに、一意の Node WWN および Port WWN が 1 つずつ必要です。

図 *29 :* 仮想ホスト *HBA* ポート



WWN を指定して仮想 N ポートを作成したあとで、IPS ポートの仮想 iSCSI インターフェイスを介してファブリック ログイン（FLOGI）を行います。FLOGI の完了後、ファイバ チャネル SAN で仮想 N ポートがオンラインになり、ファイバ チャネル ネーム サーバーで仮想 N ポートが登録されます。IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールは、ファイバ チャネル ネーム サーバに次のエントリを登録します。

- ネーム サーバーの IP-address フィールドに iSCSI ホストの IP アドレス

- ネーム サーバーの symbolic-node-name フィールドに iSCSI ホストの IQN
- ネーム サーバーの FC-4 type フィールドに SCSI_FCP
- ネーム サーバーの FC-4 feature に発信側フラグ
- ネーム サーバーの N ポート デバイスを iSCSI ゲートウェイ デバイスとして指定する FC-4 type フィールドに、ベンダー固有の iSCSI GW フラグ

iSCSI ホストからのすべての iSCSI セッションが終了すると、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールが明示的なファブリック ログアウト（FLOGO）を実行し、ファイバ チャネル SAN から仮想 N ポート デバイスを除去します（間接的に、ファイバ チャネル ネーム サーバからデバイスを登録解消することになります）。

ホストから iSCSI 仮想ターゲットへの iSCSI セッションごとに、実ファイバ チャネル ターゲットへの対応するファイバ チャネル セッションが 1 つずつ存在します。3 つの iSCSI ホストがあり、そのすべてが同じファイバ チャネル ターゲットに接続しています。3 つの仮想ファイバ チャネル ホストのそれぞれからターゲットに、ファイバ チャネル セッションが 1 つずつあります。

iSCSI イニシエータのアイドル タイムアウト

iSCSI 発信側アイドル タイムアウトでは、発信側が最後の iSCSI セッションからログアウトするまでに、仮想ファイバ チャネル N ポートのアイドル状態が続く時間を指定します。このタイマーのデフォルト値は 300 秒です。これは、IP ネットワークで一時的な障害が発生したときに、N ポートがファイバ チャネル SAN に対してログインとログオフを繰り返さないようにするために有用です。ファイバ チャネル SAN で不必要に RSCN が生成される可能性が少なくなります。

アイドル タイムアウトを構成する

発信側のアイドル タイムアウトを設定するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを開始します。

```
switch# config terminal
switch(config)#
```

ステップ 2 iSCSI イニシエータのアイドル タイムアウト値を 10 秒に構成します。

```
switch(config)# iscsi initiator idle-timeout 10
```

iSCSI イニシエータへの WWN の割り当て

iSCSI ホストは次のいずれかのメカニズムで、N ポートの WWN に対応付けられます。

- ダイナミック マッピング（デフォルト）
- スタティック マッピング

ダイナミック マッピング

ダイナミック マッピングの場合、iSCSI ホストはダイナミックに生成されたポート WWN（pWWN）およびノード WWN（nWWN）に対応付けられます。iSCSI ホストは接続のたびに、異なる WWN に対応付けられる可能性があります。このオプションは、ファイバ チャネル ターゲット デバイス上でアクセス コントロールが不要な場合に使用します。ターゲット デバイスのアクセス コントロールは通常、ホスト WWN を使用して設定するからです。

WWN は、MDS スイッチの WWN プールから割り当てられます。iSCSI ホストへの WWN マッピングは、iSCSI ホストに IPS ポートとの iSCSI セッションが 1 つ以上あるかぎり維持されます。ホストからのすべての iSCSI セッションが終了し、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールがホストの仮想 N ポートに対して FLOGO を実行すると、WWN は解放されてスイッチのファイバ チャネル WWN プールに戻ります。戻されたアドレスは、ファイバ チャネル ファブリックにアクセスする必要がある他の iSCSI ホストに割り当てることができます。

次の 3 種類のダイナミック イニシエータ モードがサポートされます。

- iSCSI：ダイナミック発信側は iSCSI 発信側として扱われ、ダイナミック仮想ターゲットおよび設定された iSCSI 仮想ターゲットにアクセスできます。
- iSLB：ダイナミック イニシエータは iSLB イニシエータとして扱われます。
- 拒否：ダイナミック イニシエータは、MDS スイッチにログインできません。

iSCSI ダイナミック マッピングがデフォルトの動作モードです。この構成は、CFS を使用して配信されます。

スタティック マッピング

スタティック マッピングの場合、iSCSI ホストは特定の pWWN および nWWN に対応付けられます。このマッピングは、永続ストレージで維持され、iSCSI ホストが接続するたびに、同じ WWN マッピングが使用されます。ターゲット デバイス上でアクセス コントロールを使用する場合は、このモードが必要です。

スタティック マッピングは、次の 2 つの方法のいずれかで実装できます。

- ユーザー割り当て：構成プロセス中に、一意の WWN を独自に指定できます。
- システム割り当て：スイッチのファイバ チャネル WWN プールから WWN を提供し、スイッチ構成でマッピングを維持することをスイッチに要求できます。

system-assign オプションの使用を推奨します。手動でWWNを割り当てる場合は、固有の割り当てにする必要があります（詳細については、『Cisco Fabric Manager ファブリック構成ガイド』『Cisco MDS 9000 ファミリ NX-OS ファブリック構成ガイド』を参照してください）。すでに割り当てられている WWN は使用できません。

ダイナミック iSCSI 発信側 WWN マッピングをスタティックにする方法

ダイナミック iSCSI 発信側のログイン後に、その発信側で次回ログイン時にも同じマッピングが使用されるように、自動的に割り当てられたnWWN/pWWNマッピングを維持することがあります。

ダイナミック iSCSI イニシエータをスタティック iSCSI イニシエータに変換して、その WWN を永続的に使用することができます。

（注） ダイナミック iSCSI 発信側をスタティック iSLB 発信側に変換したり、ダイナミック iSLB 発信側をスタティック iSCSI 発信側に変換したりはできません。

（注） イニシエータの作成後にダイナミック pWWN をスタティックにできるのは、CLI を使用した場合だけです。Device Manager または Fabric Manager ではできません。Fabric Manager または Device Manager で pWWN をスタティックにするには、この発信側を削除してから作成し直す必要があります。

WWN の衝突チェック

アップグレードに失敗した場合、またはシステム ソフトウェアをダウングレードした場合に、システムによってスタティック iSCSI 発信側に割り当てられた WWN がシステムに偶発的に戻されることがあります（**install all** コマンドを使用せずに、旧来の Cisco MDS SAN-OS を手動でブート）。このような場合、システムはそれらの WWN をあとで他の iSCSI 発信側（ダイナミックまたはスタティック）に割り当て、衝突を引き起こす可能性があります。

このような状況になったときには常に、システムに属している設定済みのWWNを調べて削除することによって、この問題に対処できます。

iSCSI イニシエータの名 name プションを使用したダイナミック マッピングを構成する

iSCSI イニシエータに（**name** オプションを使用して） ダイナミック マッピングを構成するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 iSLB ダイナミック イニシエータ モードを指定します。

```
switch(config)# iscsi dynamic initiator islb
```

ステップ 3 ダイナミック イニシエータの MDS スイッチへのログインを禁止する

```
switch(config)# iscsi dynamic initiator deny
```

ステップ 4 iSCSI モード（デフォルト）に戻します。

```
switch(config)# no iscsi dynamic initiator islb
```

iSCSI イニシエータの名 name プションを使用したスタティック マッピングを構成する

iSCSI イニシエータ に（**[name]** オプションを使用して）スタティック マッピングを構成するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 イニシエータ ノードの iSCSI 名を使用して iSCSI イニシエータを構成します。名前の最大長は英数字 223 文字です。最小長は 16 です。

```
switch(config)# iscsi initiator name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-init)#
```

ステップ 3 構成済み iSCSI イニシエータを削除します。

```
switch(config)# no iscsi initiator name iqn.1987-02.com.cisco.initiator
```

iSCSI イニシエータの名 IP アドレス プションを使用したスタティック マッピングを構成する

iSCSI イニシエータに（**ip-address** オプションを使用して）スタティック マッピングを構成するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 イニシエータ ノードの IPv4 アドレスを使用して iSCSI イニシエータを構成します。

```
switch(config)# iscsi initiator ip-address 10.50.0.0
switch(config-iscsi-init)#
```

ステップ 3 イニシエータ ノードの IPv6 ユニキャスト アドレスを使用して iSCSI イニシエータを構成します。

```
switch(config)# iscsi initiator ip-address 2001:0DB8:800:200C::417A
switch(config-iscsi-init)#
```

ステップ 4 （オプション）設定済み iSCSI イニシエータを削除します。

```
switch(config)# no iscsi initiator ip-address 2001:0DB8:800:200C::417A
```

iSCSI イニシエータに対する WWN の割り当て

iSCSI イニシエータに WWN を割り当てるには、次のステップを実行します。

始める前に

system-assign オプションを使用して iSCSI イニシエータに WWN を設定した場合、設定を ASCII ファイルに保存すると、システムによって割り当てられた WWN も保存されます。以後、write erase コマンドを実行する場合は、ASCII ファイルから WWN 設定を手動で削除する必要があります。この作業を怠ると、ASCII 設定ファイルをスイッチ上で再適用した場合に、WWN を二重に割り当てることになる可能性があります。

手順

ステップ 1 スイッチの WWN プールを使用してこの iSCSI イニシエータに nWWN を割り当て、それを永続的に保持します。

```
switch(config-iscsi-init)# static nWWN system-assign
```

ステップ 2 ユーザーが指定した WWN を、iSCSI イニシエータの nWWN として割り当てます。iSCSI ノードごとに 1 つの nWWN だけを指定できます。

```
switch(config-iscsi-init)# static nWWN 20:00:00:05:30:00:59:11
```

ステップ 3 スイッチの WWN プールを使用して、この iSCSI イニシエータに 2 つの pWWN を割り当て、それらを永続的に保持します。範囲は 1 ～ 64 です。

```
switch(config-iscsi-init)# static pWWN system-assign 2
```

ステップ 4 ユーザーが指定した WWN を iSCSI イニシエータの pWWN として割り当てます。

```
switch(config-iscsi-init)# static pWWN 21:00:00:20:37:73:3b:20
```

自動的に割り当てられた nWWN/pWWN マッピングの保存

自動的に割り当てられた nWWN/pWWN マッピングを永続的に維持するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 名前で指定された iSCSI イニシエータに自動的に割り当てられた pWWN および nWWN を保存します。

```
switch(config)# iscsi save-initiator name iqn.1987-02.com.cisco.initiator
```

ステップ 3 IPv4 アドレスで指定された iSCSI イニシエータに自動的に割り当てられた pWWN および nWWN を保存します。

```
switch(config)# iscsi save-initiator ip-address 10.10.100.11
```

ステップ 4 IPv6 ユニキャスト アドレスで指定された iSCSI イニシエータに自動的に割り当てられた pWWN および nWWN を保存します。

```
switch(config)# iscsi save-initiator ip-address 2001:0DB8:800:200C::417A
```

ステップ 5 すべてのイニシエータに自動的に割り当てられた nWWN および pWWN を保存します。

```
switch(config)# iscsi save-initiator
```

ステップ 6 EXEC モードに戻ります。

```
switch(config)# exit

switch#
```

ステップ 7 システム リブート後も nWWN/pWWN マッピング構成を保存します。

```
switch# copy running-config startup-config
```

WWN の競合の確認と削除

WWN の競合を調べて削除するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 WWN 競合を確認します。

```
switch(config)# iscsi duplicate-wwn-check

List of Potential WWN Conflicts:
--------------------------------
Node : iqn.test-local-nwwn:1-local-pwwn:1
nWWN : 22:03:00:0d:ec:02:cb:02
pWWN : 22:04:00:0d:ec:02:cb:02
```

ステップ 3 iqn.test-local-nwwn:1-local-pwwn:1 というイニシエータの iSCSI イニシエータ コンフィギュレーション モードを開始します。

```
switch(config)# iscsi initiator name iqn.test-local-nwwn:1-local-pwwn:1
```

ステップ 4 競合する nWWN が削除されます。

```
switch(config-iscsi-init)# no static nWWN 22:03:00:0d:ec:02:cb:02
```

ステップ 5 競合する pWWN が削除されます。

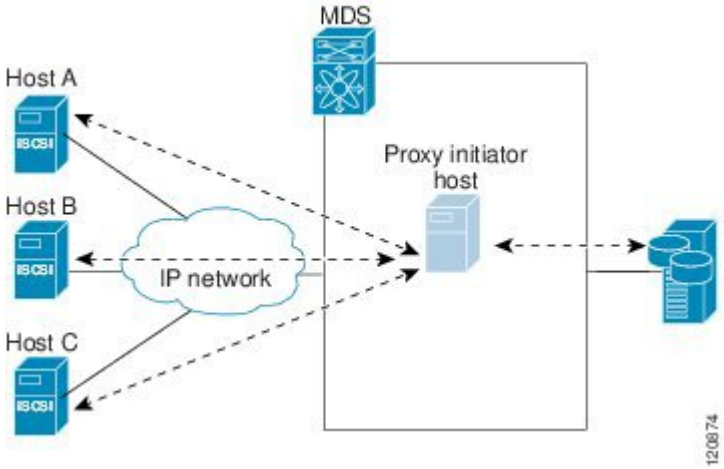
```
switch(config-iscsi-init)# no static pWWN 22:04:00:0d:ec:02:cb:02
```

プロキシ イニシエータ モード

ファイバ チャネル ストレージ デバイスで、あらゆるホストに関して明示的な LUN アクセス コントロールが必要な場合、透過型イニシエータ モードを使用します（1 つの iSCSI ホストを 1 つのファイバ チャネル ホストとして提供）。各 iSCSI ホストは静的に設定する必要があります。この場合、iSCSI ホストごとにいくつもの設定作業が必要です。明示的な LUN アクセス コントロールが必要ない場合、プロキシ イニシエータ モードを使用すると、構成が簡略化されます。

このモードでは、作成される仮想ホスト N ポート（HBA ポート）は IPS ポートごとに 1 つだけです。その IPS ポートに接続するすべての iSCSI ホストは同じ仮想ホスト N ポートを使用して多重化されます。このモードを使用すると、WWN をスタティックにバインドする作業が簡単になります。この IPS ポートを介して接続する各 iSCSI イニシエータで使用されるすべての LUN について、プロキシ仮想 N ポートの pWWN からアクセスできるように、ファイバ チャネル ストレージ アレイ上の LUN マッピングおよび割り当てを設定する必要があります。さらに、LUN マッピングおよび iSCSI アクセス コントロール（「スタティック マッピング」セクションを参照）を指定して iSCSI 仮想ターゲットを構成することによって、各 iSCSI イニシエータに LUN が割り当てられます。

図 *30 : IPS* ポートの多重化



プロキシ イニシエータ モードは IPS ポート単位で設定できますが、その場合にこのモードになるのは、その IPS ポートで終端する iSCSI イニシエータのみです。

プロキシ イニシエータ モードで IPS ポートを設定した場合、IPS ポートの仮想 iSCSI インターフェイスを介してファブリック ログイン（FLOGI）を行います。FLOGI の完了後、ファイバ チャネル ファブリックでプロキシ発信側仮想 N ポートがオンラインになり、ファイバ チャネル ネーム サーバーで仮想 N ポートが登録されます。IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールは、ファイバ チャネル ネーム サーバーに次のエントリを登録します。

- ネーム サーバーの symbolic-node-name フィールドに iSCSI インターフェイス名 iSCSI スロット/ポート
- ネーム サーバーの FC-4 type フィールドに SCSI_FCP
- ネーム サーバーの FC-4 feature に発信側フラグ
- ネーム サーバ]の N ポート デバイスを iSCSI ゲートウェイ デバイスとして指定する FC-4 type フィールドに、ベンダー固有のフラグ（iscsi-gw）

透過型イニシエータ モードと同様、ユーザーは pWWN および nWWN を指定することも、またはプロキシ発信側 N ポートへの WWN 割り当てをシステムに要求することもできます。

（注） iSLB VRRP グループに属している iSCSI インターフェイスについて、プロキシ イニシエータ モードをイネーブルにすると、インターフェイスのロード バランシングが影響を受けます。「iSCSIインターフェイスパラメータの変更およびロードバランシングへの影響」セクションを参照してください。

（注） インターフェイスがプロキシイニシエータ モードの場合、iSCSI インターフェイスのプロキシ N ポート属性（WWN ペアまたは FC ID）に基づいてファイバ チャネル アクセス コントロール（ゾーン分割）のみを設定できます。iSCSI 発信側の IP アドレス、IQN などの iSCSI 属性を使用してゾーン分割を設定することはできません。イニシエータ ベースのアクセス コントロールを実行するには、iSCSI ベース アクセス コントロールを使用します。

プロキシ イニシエータの構成

プロキシ イニシエータを構成するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 イニシエータの接続先となるスイッチの iSCSI インターフェイスを選択します。

```
switch(config)# interface iscsi 4/1
switch(config-if)#
```

ステップ 3 システム割り当て nWWN および pWWN を使用してプロキシ イニシエータ モードを構成します。

```
switch(config-if)# switchport proxy-initiator
```

ステップ 4 （オプション）プロキシ イニシエータ モードを無効にします。

```
switch(config-if)# no switchport proxy-initiator
```

ステップ 5 （オプション）指定された WWN を使用してプロキシ イニシエータ モードを構成します。

```
switch(config-if)# switchport proxy-initiator nWWN 11:11:11:11:11:11:11:11 pwwn 22:22:22:22:22:22:22:22
```

ステップ 6 （オプション）プロキシ イニシエータ モードを無効にします。

```
switch(config-if)# no switchport proxy-initiator nWWN 11:11:11:11:11:11:11:11 pwwn
22:22:22:22:22:22:22:22
```

iSCSI の VSAN メンバーシップ

iSCSI インターフェイスにはポート VSAN という VSAN メンバーシップを構成できます。このインターフェイスに接続するすべての iSCSI デバイスは、VSAN 内で明示的に設定されていない場合には、自動的にこの VSAN のメンバーになります。iSCSI インターフェイスのデフォルト ポート VSAN は、VLAN 1 です。iSCSI デバイスもファイバ チャネル デバイスと同様、2 種類の方式で VSAN メンバーシップを定義できます。

- iSCSI ホスト：iSCSI ホストに対する VSAN メンバーシップ。（この方法は、iSCSI インターフェイスより優先して実行されます）。
- iSCSI インターフェイス：iSCSI インターフェイスに対する VSAN メンバーシップ（ホストが iSCSI ホストによる方法でどの VSAN にも設定されていない場合、この iSCSI インターフェイスに接続するすべての iSCSI ホストがインターフェイス VSAN メンバーシップを継承します）。

個々の iSCSI ホストを特定の VSAN に属すように設定できます。指定した VSAN によって、iSCSI インターフェイスの VSAN メンバーシップが上書きされます。

iSCSI ホストの VSAN メンバーシップの割り当て

iSCSI ホストの VSAN メンバーシップを割り当てるには、次のステップを実行します。

始める前に

その他の VSAN（VSAN 1 以外）内に発信側を設定すると（VSAN 2 など）、発信側は自動的に VSAN 1 から削除されます。VSAN 1 にもこの発信側を存続させる場合は、この発信側を VSAN 1 内に明示的に設定する必要があります。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 iSCSI イニシエータを構成します。

```
switch(config)# iscsi initiator name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-init)#
```

ステップ 3 指定された VSAN に iSCSI イニシエータ ノードを割り当てます。

```
switch(config-iscsi-init)# vsan 3
```

（注）
1 つ以上の VLAN にこのホストを割り当てることができます。

ステップ 4 指定された VSAN から iSCSI ノードを削除します。

```
switch(config-iscsi-init)# no vsan 5
```

iSCSI インターフェイスのデフォルト ポート VSAN の設定

iSCSI インターフェイスにはポート *VSAN* という VSAN メンバーシップを構成できます。このインターフェイスに接続するすべての iSCSI デバイスは、VSAN 内で明示的に設定されていない場合には、自動的にこの VSAN のメンバーになります。言い換えると、iSCSI インターフェ

イスのポート VSAN は、すべてのダイナミック iSCSI 発信側のデフォルト VSAN になります。iSCSI インターフェイスのデフォルト ポート VSAN は、VLAN 1 です。

iSCSI インターフェイスのデフォルト ポート VSAN を変更するステップは、次のとおりです。

始める前に

iSLB VRRP グループに属している iSCSI インターフェイスの VSAN メンバーシップを変更すると、インターフェイスのロードバランシングが影響を受けます。「iSCSI インターフェイス パラメータの変更およびロード バランシングへの影響」セクションを参照してください。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 iSCSI インターフェイスの VSAN メンバーシップを構成します。

```
switch(config)# iscsi interface vsan-membership
```

ステップ 3 VSAN に対するデータベースを構成します。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。

```
switch(config)# vsan database
switch(config-vsan-db)#
```

ステップ 4 指定された VSAN（VSAN 2）に、iscsi 2/1 インターフェイスのメンバーシップを割り当てます。

```
switch(config - vsan-db)# vsan 2 interface iscsi 2/1
```

ステップ 5 iSCSI インターフェイスのポート VSAN としてデフォルトの VSAN を使用するように設定を戻します。

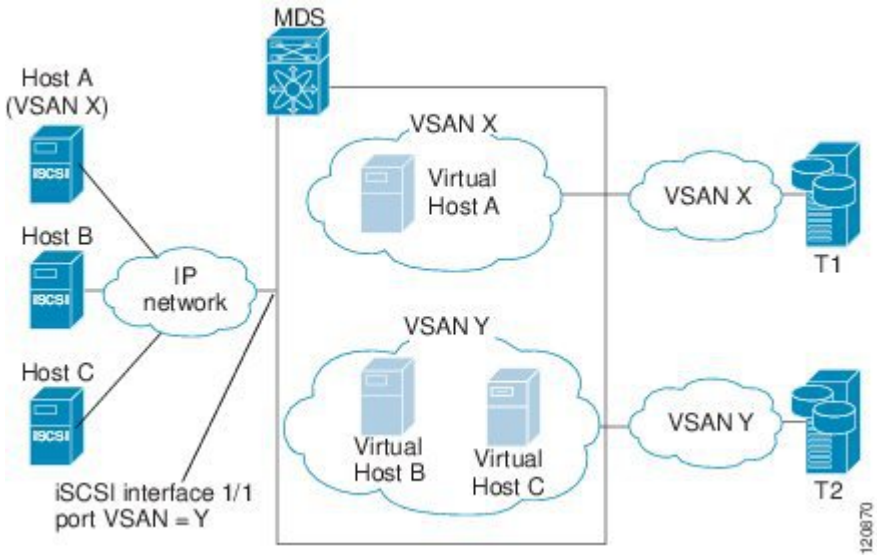
```
switch(config - vsan-db)# no vsan 2 interface iscsi 2/1
```

iSCSI デバイスの VSAN メンバーシップ

以下のような iSCSI デバイスの VSAN メンバーシップの例：

- SCSI インターフェイス 1/1 は VSAN Y のメンバーです。
- iSCSI 発信側ホスト A は、VSAN X に対する明示的 VSAN メンバーシップが与えられています。
- 3 つの iSCSI 発信側（ホスト A、ホスト B、およびホスト C）が iSCSI インターフェイス 1/1 に接続します。

図 *31 : iSCSI* インターフェイスの *VSAN* メンバーシップ



ホスト A の仮想ファイバ チャネル N ポートは、イニシエータの明示的メンバーシップが設定されているので、VSAN X に追加されます。仮想ホスト B およびホスト C の N ポートは、明示的メンバーシップが設定されていないので、iSCSI インターフェイスの VSAN メンバーシップを引き継ぎ、VSAN Y に属します。

iSCSI ホストの拡張 VSAN メンバーシップ

iSCSI ホストは、複数の VSAN のメンバーになることができます。この場合、iSCSI ホストがメンバーになっている VSAN ごとに 1 つずつ仮想ファイバ チャネル ホストが複数作成されます。この設定は、ファイバ チャネル テープ デバイスなどのリソースをさまざまな VSAN 間で共有しなければならない場合に便利です。

iSCSI のアクセス コントロール

iSCSI デバイスでは 2 種類のアクセス コントロール方式を使用できます。ファイバ チャネル ファブリックに iSCSI ホストを提供するイニシエータ モードに応じて、一方または両方のアクセス コントロール方式を使用できます。

- ファイバ チャネル ゾーン分割ベースのアクセス コントロール：ファイバ チャネル ゾーン分割は、iSCSI デバイスをサポートできるように拡張されました。この拡張により、SAN 全体にわたって、統一された柔軟性の高いアクセス コントロール方式を使用する利点が得られます。iSCSI の場合、複数の iSCSI デバイスが iSCSI インターフェイスの背後に接続される可能性があります。インターフェイスベースのゾーン分割は、インターフェイスの背後にあるすべての iSCSI デバイスが自動的に同じゾーンに含まれるので、役に立たない場合があります。
- iSCSI ACL ベースのアクセス コントロール：iSCSI ベースのアクセス コントロールが適用されるのは、スタティック iSCSI 仮想ターゲットを作成した場合だけです。スタティック iSCSI ターゲットの場合は、ターゲットにアクセス可能な iSCSI 発信側のリストを設定で

きます。デフォルトでは、スタティック iSCSI 仮想ターゲットは iSCSI ホストにアクセスできません。

ファイバ チャネル ファブリックに iSCSI ホストを提供するイニシエータ モードに応じて、一方または両方のアクセス コントロール方式を使用できます。

この項では、次の項目について説明します。

- ファイバ チャネル ゾーン分割ベースのアクセス コントロール
- iSCSI ベースのアクセス コントロール
- アクセス コントロールの実行

ファイバ チャネル ゾーン分割ベースのアクセス コントロール

Cisco SAN-OS リリース 3.x と NX-OS リリース 4.1(1b) の VSAN およびゾーン分割の概念は、ファイバチャネルデバイスと iSCSI デバイスの両方を対象とするように拡張されました。ゾーン分割は、ファイバ チャネル デバイスの標準アクセス コントロール方式であり、VSAN のコンテキストの中で適用されます。ファイバチャネル ゾーン分割は、iSCSI デバイスをサポートできるように拡張されました。この拡張により、SAN 全体にわたって、統一された柔軟性の高いアクセス コントロール方式を使用する利点が得られます。

ファイバ チャネル ゾーンのメンバーを識別する共通メカニズムは、次のとおりです。

- ファイバ チャネル デバイスの pWWN。
- インターフェイスおよびスイッチの WWN。そのインターフェイス経由で接続するデバイスはゾーン内にあります。

ファイバ チャネル ゾーン分割の詳細については、『Cisco Fabric Manager ファブリック構成ガイド』『Cisco MDS 9000 ファミリ NX-OS ファブリック構成ガイド』を参照してください。

iSCSI の場合、複数の iSCSI デバイスが iSCSI インターフェイスの背後に接続される可能性があります。インターフェイスベースのゾーン分割は、インターフェイスの背後にあるすべての iSCSI デバイスが自動的に同じゾーンに含まれるので、役に立たない場合があります。

透過型イニシエータ モード（「透過型イニシエータ モード」で説明したとおり、iSCSI ホストごとに 1 つずつファイバチャネル仮想 N ポートが作成される）では、iSCSI ホストにスタティックな WWN マッピングが設定されている場合に、標準のファイバ チャネル デバイス pWWN ベースのゾーン分割メンバーシップ メカニズムを使用できます。

ゾーン分割メンバーシップ メカニズムは、次の情報に基づいて iSCSI デバイスをゾーンに追加するように拡張されています。

- IPv4 アドレス/サブネット マスク
- IPv6 アドレス/プレフィックス長
- iSCSI 修飾名（IQN）
- symbolic-node-name（IQN）

スタティック WWN マッピングが設定されていない iSCSI ホストの場合、この機能を使用すると、ゾーン メンバーとして IP アドレスまたは iSCSI ノード名を指定できます。スタティック WWN マッピングが設定されている iSCSI ホストでも、これらの機能を使用できます。サブネットマスクを指定することにより、1 つのコマンドで複数のデバイスを IP アドレス ベースのゾーン メンバーシップに指定できます。

（注） プロキシ イニシエータ モードでは、IPS ポートに接続するすべての iSCSI デバイスが、単一の仮想ファイバ チャネル N ポート経由でファイバ チャネル ファブリックにアクセスできます。iSCSI ノード名または IP アドレスに基づくゾーン分割を設定しても効果はありません。WWN ベースのゾーン分割を使用した場合、その IPS ポートに接続するすべての iSCSI デバイスが同じゾーンに組み込まれます。プロキシ イニシエータ モードで個別のイニシエータ アクセス コントロールを実施するには、仮想ターゲットに iSCSI ACL を構成します（「iSCSI ベース アクセス コントロール」を参照）。

*iSCSI:*ゾーン データベースへのイニシエータの追加

ゾーン データベースに iSCSI イニシエータを追加するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールの iSCSI デバイスを含めるゾーン名を作成します。

```
switch(config)# zone name iSCSIzone vsan 1
switch(config-zone)
```

ステップ 3 ゾーンに iSCSI ノード名ベースのメンバーシップを割り当てます。

```
switch(config-zone)# member symbolic-nodename iqn.1987-02.com.cisco.initiator1
```

ステップ 4 （オプション）ゾーンから指定したデバイスを削除します。

```
switch(config-zone)# no member symbolic-nodename iqn.1987-02.com.cisco.init1
```

ステップ 5 ゾーンに iSCSI IPv4 アドレス ベースのメンバーシップを割り当てます。

```
switch(config-zone)# member ip-address 10.50.1.1
```

ステップ 6 （オプション）ゾーンから指定したデバイスを削除します。

```
switch(config-zone)# no member ip-address 10.50.1.1
```

ステップ 7 ゾーンに iSCSI IPv6 アドレス ベースのメンバーシップを割り当てます。

```
switch(config-zone)# member ipv6-address 2001:0DB8:800:200C::417A
```

ステップ 8 ゾーンから指定したデバイスを削除します。

```
switch(config-zone)# no member ipv6-address 2001:0DB8:800:200C::417A
```

ステップ 9 ゾーンに iSCSI ポート WWN ベースのメンバーシップを割り当てます。

```
switch(config-zone)# member pwwn 20:00:00:05:30:00:59:11
```

ステップ 10 ポート WWN によって識別されたデバイスをゾーンから削除します。

```
switch(config-zone)# no member pwwn 20:00:00:05:30:00:59:11
```

iSCSI ベースのアクセス コントロール

iSCSI ベース のアクセス コントロールが適用されるのは、スタティック iSCSI 仮想ターゲットを作成した場合だけです（「スタティック マッピング」 を参照）。スタティック iSCSI ターゲットの場合は、ターゲットにアクセス可能な iSCSI 発信側のリストを設定できます。

デフォルトでは、スタティック iSCSI 仮想ターゲットは iSCSI ホストにアクセスできません。すべてのホストから iSCSI 仮想ターゲットにアクセスできるようにするには、アクセス可能性を明示的に設定する必要があります。発信側アクセス リストには、発信側を 1 つまたは複数指定できます。iSCSI 発信側は、次のいずれかの方式で指定できます。

- iSCSI ノード名
- IPv4 アドレスおよびサブネット
- IPv6 アドレス

iSCSI のアクセス コントロールを構成するには、次のステップを実行します。

始める前に

トランスペアレント モードの iSCSI イニシエータで、ファイバ チャネル ゾーン分割と iSCSI ACL の両方を使用する場合、iSCSI ホストにアクセス可能なスタティック iSCSI ターゲットごとに、イニシエータの仮想 N ポートをファイバ チャネル ターゲットと同じファイバ チャネル ゾーンに含める必要があります。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 iSCSI ターゲット（iqn.1987-02.com.cisco.initiator）を作成します。

```
switch(config)# iscsi virtual-target name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-tgt)#
```

ステップ 3 仮想ターゲット ノードをファイバ チャネル ターゲットにマップします。

```
switch(config-iscsi-tgt)# pWWN 26:00:01:02:03:04:05:06
switch(config-iscsi-tgt)#
```

ステップ 4 指定の iSCSI イニシエータ ノードがこの仮想ターゲットにアクセスできるようにします。複数のイニシエータにこの操作を許可するには、このコマンドを複数回発行します。

```
switch(config-iscsi-tgt)# initiator iqn.1987-02.com.cisco.initiator1 permit
```

ステップ 5 （オプション）指定されたイニシエータ ノードが仮想ターゲットにアクセスするのを防止します。

```
switch(config-iscsi-tgt)# no initiator iqn.1987-02.com.cisco.initiator1 permit
```

ステップ 6 指定された IPv4 アドレスが仮想ターゲットにアクセスするのを防止します。

```
switch(config-iscsi-tgt)# no initiator ip address 10.50.1.1 permit
```

ステップ 7 この IPv4 サブネットワーク（10.50.1/24）内のすべてのイニシエータに、この仮想ターゲットへのアクセスを許可します。

```
switch(config-iscsi-tgt)# initiator ip address 10.50.1.0 255.255.255.0 permit
```

ステップ 8 この IPv4 サブネットワーク内のすべてのイニシエータが仮想ターゲットにアクセスするのを防止します。

```
switch(config-iscsi-tgt)# no initiator ip address 10.50.1.0 255.255.255.0 permit
```

ステップ 9 この IPv6 サブネットワーク内のすべてのイニシエータ（2001:0DB8:800:200C::/64）にこの仮想ターゲットへのアクセスを許可します。

```
switch(config-iscsi-tgt)# initiator ip address 2001:0DB8:800:200C::/64 permit
```

ステップ 10 この IPv6 サブネットワーク内のすべてのイニシエータが仮想ターゲットにアクセスするのを防止します。

```
switch(config-iscsi-tgt)# no initiator ip address 2001:0DB8:800:200C::/64 permit
```

ステップ 11 すべてのイニシエータ ノードにこの仮想ターゲットへのアクセスを許可します。

```
switch(config-iscsi-tgt)# all-initiator-permit
```

ステップ 12 イニシエータが仮想ターゲットにアクセスするのを防止します（デフォルト）。

```
switch(config-iscsi-tgt)# no all-initiator-permit
```

アクセス コントロールの実行

IPS ポートを搭載したファイバ チャネル モジュールおよび MPS-14/2 モジュールでは、iSCSI および ファイバ チャネル ゾーン分割ベースの両方の アクセス コントロール リストを使用して、 アクセス コントロールを実行します。アクセス コントロールは、iSCSI 検出フェーズおよびiSCSIセッション作成フェーズの両方で実行されます。入出力フェーズでは、アクセス コントロールの実行は不要です。IPS ポートを搭載したファイバ チャネルまたは MPS-14/2 モジュールがiSCSIトラフィックのファイバチャネルへのルーティングを引き受けるためです。

- iSCSI 検出フェーズ：iSCSI ホストが iSCSI 検出セッションを作成し、すべての iSCSI ターゲットにクエリを送信すると、IPS ポートを搭載したファイバ チャネルまたは MPS-14/2

モジュールは直前の項に記載されたアクセス コントロール ポリシーに基づいて、この iSCSI ターゲットホストからアクセス可能な iSCSI ターゲット リストだけを戻します。IPS ポートを搭載したファイバ チャネルまたは MPS-14/2 モジュールは、ファイバ チャネル ネーム サーバにクエリを送信し、すべての VSAN で発信側と同じゾーンに含まれているすべてのデバイスを要求することによって、これを実行します。さらに、FCNS エントリの FC4-feature フィールドを調べることによって、発信側デバイスを除外します。（デバイスが FC4-feature フィールドにイニシエータとしてもターゲットとしても登録していない場合、IPS ポートを搭載したファイバ チャネルまたは MPS-14/2 モジュールはそれをアドバタイズします）。その後に iSCSI ホストにターゲットのリストを返します。各ターゲットには、ユーザーが構成したスタティックな iSCSI ターゲット名または IPS モジュールまたは MPS-14/2 モジュールによって作成されたダイナミックな iSCSI ターゲット名が与えられます（「ダイナミック マッピング」を参照）。

- iSCSI セッションの作成：IP ホストが iSCSI セッションを開始すると、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールが、「iSCSI ベース アクセス コントロール」で説明した両方のアクセス コントロール方式を使用して、（セッション ログイン要求で）指定された iSCSI ターゲットにアクセスが許可されているかどうかを検証します。

iSCSI ターゲットがスタティックに対応付けられたターゲットの場合、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールは、iSCSI ターゲットのアクセス リスト内で、iSCSI ホストが許可されているかどうかを検証します。IP ホストからアクセスできない場合は、ログインが拒否されます。iSCSI ホストからアクセスできる場合は、iSCSI ホストが使用する仮想ファイバ チャネル N ポートと、スタティック仮想ターゲットに対応付けられたファイバ チャネル ターゲットが同じファイバ チャネル ゾーンに属しているかどうかが検証されます。

iSCSI ターゲットが自動生成の iSCSI ターゲットの場合、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールが iSCSI ターゲット名からファイバ チャネル ターゲットの WWN を抽出して、発信側とファイバ チャネル ターゲットが同じファイバ チャネル ゾーンに属しているかどうかを検証します。属している場合は、アクセスが許可されます。

IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールでは、iSCSI ホストのファイバ チャネル N ポートを使用して、ゾーン適用ネーム サーバー クエリーによって、ファイバ チャネル ターゲット WWN を調べます。FC ID がネーム サーバーから戻された場合は、iSCSI セッションが許可されます。これ以外の場合、ログイン要求は拒否されます。

iSCSI セッション認証

IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールは、ストレージ デバイスへのアクセスを要求する iSCSI ホスト を認証するための iSCSI 認証メカニズムをサポートします。デフォルトでは、IPS ポートを搭載したファイバチャネルモジュールおよび MPS-14/2 モジュールは、iSCSI 発信側に関する CHAP または None 認証を許可します。認証を必ず使用する場合は、CHAP 認証だけが許可されるようにスイッチを設定する必要があります。

CHAP のユーザー名またはシークレット検証では、Cisco MDS AAA インフラストラクチャでサポートおよび許可されている任意の方式を使用できます。AAA 認証は、RADIUS、TACACS+、

またはローカル認証デバイスをサポートします。『Cisco Fabric Manager セキュリティ構成ガイド』を参照してください。

aaa authentication iscsi コマンドは、iSCSI ホストの AAA 認証を有効にして、使用する方式を指定します。『Cisco MDS 9000 Family NX-OS Security Configuration Guide』を参照してください。

iSCSI ユーザーの AAA 認証の構成

iSCSI ユーザーの AAA 認証を構成するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 iSCSI CHAP 認証に RadServerGrp と呼ばれるグループに追加された RADIUS サーバを使用します。

```
switch(config)# aaa authentication iscsi default group RadServerGrp
```

ステップ 3 iSCSI CHAP 認証には、TacServerGrp と呼ばれるグループに追加された TACACS+ サーバを使用します。

```
switch(config)# aaa authentication iscsi default group TacServerGrp
```

ステップ 4 ローカル パスワード データベースを使用して iSCSI CHAP の認証を行います。

```
switch(config)# aaa authentication iscsi default local
```

iSCSI の認証 メカニズムの構成

iSCSI の認証メカニズムを構成するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 CHAP をデフォルトの認証メカニズムとして Cisco MDS スイッチ用にグローバルに構成します。CHAP 認証はすべての iSCSI セッションで必要です。

```
switch(config)# iscsi authentication chap
```

インターフェイスで iSCSI セッションの認証メカニズムの構成

特定のインターフェイスに対する iSCSI セッションの認証メカニズムを構成するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 ギガビット イーサネット インターフェイスを選択します。

```
switch(config)# interface GigabitEthernet 2/1.100
switch(config-if)#
```

ステップ 3 選択されているインターフェイスへの iSCSI セッションに認証が不要であることを指定します。

```
switch(config-if)# iscsi authentication none
```

ローカル認証の構成

ローカル認証のための iSCSI ユーザーを構成するには、次のステップを実行します。

手順

ステップ 1 構成モード に入ります

```
switch# config terminal
switch(config)#
```

ステップ 2 iSCSI ログイン認証用に、ローカル データベースでユーザー名（iscsiuser）とパスワード（ffsffsfsffs345353554535）を構成します。

```
switch(config)# username iscsiuser password ffsffsfsffs345353554535 iscsi
```

iSCSI イニシエータ認証の制限

iSCSI イニシエータはデフォルトで、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールに対する自身の認証用に、RADIUS サーバーまたはローカル データベースの任意のユーザー名を使用できます（CHAP ユーザー名は iSCSI イニシエータ名と無関係です）。IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュール

は、スイッチから送信されたCHAPチャレンジに有効な応答があった場合にかぎり、発信側にログインを許可します。ただし、CHAPユーザー名およびパスワードが信用できないものであると、問題が生じる可能性があります。

イニシエータがCHAP認証に特定のユーザー名を使用するように制限するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 イニシエータ iqn.1987-02.com.cisco.init のコンフィギュレーション サブモードを開始します。

```
switch(config)# iscsi initiator name iqn.1987-02.com.cisco.init
switch(config-iscsi-init)#
```

ステップ 3 イニシエータ iqn.1987-02.com.cisco.init を、CHAP ユーザー名として user1 を使用する認証だけに制限します。

```
switch(config-iscsi-init)# username user1
```

（注）
ローカル AAA データベースまたは RADIUS サーバーで user1 を iSCSI ユーザーとして必ず定義してください。

相互 CHAP 認証の設定

IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールは、iSCSI イニシエータが iSCSI ログイン フェーズで Cisco MDS スイッチの iSCSI ターゲットを認証するメカニズムをサポートします。iSCSI 発信側の IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュール認証に加えて、この認証を使用できます。

iSCSIイニシエータに関するIPSポートを搭載したファイバチャネルモジュールまたはMPS-14/2モジュールの認証に加え、IPSポートを搭載したファイバチャネルモジュールまたはMPS-14/2モジュールは、iSCSI ログイン フェーズで Cisco MDS スイッチの iSCSI ターゲットを認証する、iSCSI イニシエータのメカニズムもサポートします。この認証には、ユーザー側で iSCSI 発信側に提示するスイッチ用のユーザー名およびパスワードを設定する必要があります。提供されたパスワードを使用して、発信側が IPS ポートに送信する CHAP チャレンジへの CHAP 応答が計算されます。

スイッチが発信側に対する自身の認証に使用するグローバルiSCSIターゲットユーザー名およびパスワードを設定する手順は、次のとおりです。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 すべてのイニシエータに対し、スイッチのユーザー アカウント（testuser）をクリア テキスト（デフォルト）で指定されたパスワード（abc123）とともに構成します。パスワードは 128 文字に制限されています。

```
switch(config)# iscsi authentication username testuser password abc123
```

ステップ 3 すべてのイニシエータに対し、スイッチのユーザ アカウント（user1）を 7 で指定された暗号化パスワード（!@*asdsfsdfjh!@df）とともに設定します。

```
switch(config)# iscsi authentication username user1 password 7!@*asdsfsdfjh!@df
```

ステップ 4 すべてのイニシエータに対し、スイッチのユーザー アカウント（user1）をクリア テキスト（デフォルトで 0 で示される）で指定されたパスワード（abcd12AAA）とともに構成します。パスワードは 128 文字に制限されています。

```
switch(config)# iscsi authentication username user1 password 0 abcd12AAA
```

ステップ 5 すべてのイニシエータのグローバル構成を削除します。

```
switch(config)# no iscsi authentication username testuser
```

認証用のイニシエータごとの iSCSI ターゲット ユーザ名とパスワードの構成

スイッチがイニシエータに対する自身の認証に使用するイニシエータ単位の iSCSI ターゲットのユーザー名およびパスワードを設定するには、次の手順を実行します。

始める前に

グローバル構成を表示するには、 **show running-config** および **show iscsi global** コマンドを使用します。**show running-config** および **show iscsi initiator configured** コマンドを使用して、イニシエータ固有の構成を表示します（コマンドの出力例については「iSCSI 情報の表示 」セクションを参照してください）。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 イニシエータ ノードの iSCSI 名を使用して iSCSI イニシエータを構成します。

```
switch(config)# iscsi initiator name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-init)#
```

ステップ 3 スイッチのユーザー アカウント（testuser）をクリア テキスト（デフォルト）で指定されたパスワード（abcd12AAA）とともに設定します。パスワードは 128 文字に制限されています。

```
switch(config-iscsi-init)# mutual-chap username testuser password abcd12AAA
```

ステップ 4 スイッチのユーザー アカウント（user1）および 7（!@*asdsfsdfjh!@df）で指定された暗号化パスワードを構成します。

```
switch(config-iscsi-init)# mutual-chap username user1 password 7!@*asdsfsdfjh!@df
```

ステップ 5 スイッチ認証構成を削除します。

```
switch(config-iscsi-init)# no mutual-chap username testuser
```

iSCSI 即時データ機能および割り込みデータ機能

Cisco MDS スイッチは、ログイン ネゴシエーション フェーズで発信側が要求した場合に、iSCSI 即時データ機能および割り込みデータ機能をサポートします。即時データは、iSCSI コマンド プロトコル データ ユニット（PDU）のデータ セグメントに格納された iSCSI 書き込みデータで、1 つの PDU に書き込みコマンドと書き込みデータが結合されたものなどです。割り込みデータは、発信側が MSD スイッチなどの iSCSI ターゲットに送信する iSCSI 書き込みデータで、ターゲットから明示的な Ready To Transfer（R2T）PDU を受信する必要のない、iSCSI 送信データ PDU として送信されます。

この 2 つの機能は、発信側とターゲット間で R2T PDU の往復が 1 つ少なくなるため、小規模な書き込みコマンドでは入出力時間の短縮に有効です。MSD スイッチは iSCSI ターゲットとして、1 つのコマンドで最大 64 KB の割り込みデータを使用できます。これは、iSCSI ログイン ネゴシエーション フェーズで、FirstBurstLength パラメータによって制御されます。

iSCSI 発信側が即時データ機能および割り込みデータ機能をサポートする場合、MDS スイッチ上でこれらの機能が自動的にイネーブルになるので、設定は不要です。

iSCSI インターフェイス拡張機能

iSCSI インターフェイスでは IPS ポート単位で拡張設定オプションを使用できます。これらの構成は詳細な FCIP 構成と同様であり、該当する項ですでに説明されています（「詳細な FCIP プロファイル構成」

iSCSI インターフェイスからこれらのコマンドにアクセスするには、次の例を活用します。

```
switch# config terminal
switch(config)# interface iscsi 4/1
switch(config-if)#
```

Cisco MDS スイッチ向け iSCSI インターフェイスの拡張機能

Cisco MDS スイッチが iSCSI インターフェイスに関してサポートする拡張機能は、次のとおりです。

- iSCSI リスナー ポート
- TCP 調整パラメータ
- iSCSI ルーティング モード
- QoS 値の設定

iSCSI リスナー ポート

新しい TCP 接続を待ち受ける iSCSI インターフェイスの TCP ポート番号を設定できます。デフォルト ポート番号は 3260 です。TCP ポート番号を変更すると、iSCSI ポートは以後、新しく設定されたポート上の TCP 接続だけを許可します。

TCP 調整パラメータ

次の TCP パラメータを構成できます。

- 最小再送信タイムアウト（詳細については、「最小再送信タイムアウト」セクションを参照）。
- キープアライブ タイムアウト（詳細については、「キープアライブ タイムアウト」セクションを 参照）。
- 最大再送信回数（詳細については、「最大再送信回数」セクションを参照 ）。
- パス MTU（詳細については、 「パス MTU」を参照）。
- SACK（SACK は、iSCSI TCP 設定でデフォルトでイネーブルです）。
- ウィンドウ管理（iSCSI のデフォルトは、最大帯域幅 1 Gbps、最小使用可能帯域幅 70 Mbps、往復時間 1 ミリ秒です）。（詳細については、「ウィンドウ管理」を参照）。
- バッファ サイズ（iSCSI のデフォルト送信バッファ サイズは 4096 KB です）（詳細については、「FCIP プロファイル情報の表示」 を参照）。
- ウィンドウ輻輳モニタリング（デフォルトで有効で、デフォルト バースト サイズは 50 KB）（詳細については、「輻輳モニタリング」 を参照してください）
- 最大遅延ジッタ（デフォルトでイネーブルで、デフォルト時間は 500 マイクロ秒です）。

iSCSI ルーティング モード

Cisco MDS 9000 ファミリ スイッチは、複数の iSCSI ルーティング モードをサポートします。モードごとにネゴシエーションを行う動作パラメータが異なり、長所も短所も異なります。また、適切な用途も異なります。

- パススルー モード：パススルー モードでは、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS 14/2 モジュールのポートがファイバ チャネル ターゲットから読み取ったデータ フレームを変換し、バッファリングしないで 1 フレームずつ iSCSI ホストに転送します。したがって、着信フレームを 1 つ受信すると、ただちに 1 つの iSCSI 着信データ PDU として送信されます。

  反対方向では、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS 14/2 モジュールのポートが、iSCSI ホストから送信できる iSCSI 書き込み送信データ PDU の最大サイズを、それを受信できるファイバ チャネル ターゲットで指定された最大データ サイズに制限します。その結果、iSCSI 送信データ PDU を 1 つ受信すると、1 つのファイバ チャネル データ フレームとしてファイバ チャネル ターゲットに送信されます。

  どちらの方向でもバッファリングが行われないので、転送遅延が短縮される利点があります。しかし、最大データ セグメント長が小さいので、ホスト システムの処理のオーバーヘッドが大きくなり、ホストからのデータ転送パフォーマンスが下がるのが一般的です。このモードのもう 1 つの利点は、iSCSI データ ダイジェストが可能になることです。これは TCP チェックサムで得られる以上に、PDU で伝送される iSCSI データの完全性保護に有効です。

- ストア アンド フォワード モード（デフォルト）：ストア アンド フォワード モードでは、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールのポートが交換されたすべてのファイバ チャネル データ フレームを組み立て、1 つの大きい iSCSI 受信データ PDU にしてから、iSCSI クライアントに転送します。

  反対方向では、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールのポートがホストに小さいデータ セグメント サイズを適用しないので、iSCSI ホストは任意のサイズ（最大 256 KB）の iSCSI 送信データ PDU を送信できます。ポートはさらに、iSCSI 送信データ PDU 全体を受信するまで待機し、PDU 全体を受信してから変換または分割して、ファイバ チャネル フレームをファイバ チャネル ターゲットに転送します。

  このモードの利点は、ホストからのデータ転送パフォーマンスが向上することです。欠点は、転送遅延が大きくなることと、iSCSI データ ダイジェスト（CRC）を使用できないことです。

（注） ストア アンド フォワード モードは、デフォルトの転送モードです。

- カットスルー モード：カットスルー モードを使用すると、ストア アンド フォワード モードより読み取り処理のパフォーマンスが向上します。IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールのポートは、各ファイバ チャネル受信データ フレームを受信すると、交換全体の完了を待たずに、ただちに iSCSI ホストに転送することによって、パフォーマンスの向上を実現します。書き込み送信データの処理に関しては、ストア アンド フォワード モードと差はありません。

図 *32 : iSCSI* ルーティング モード

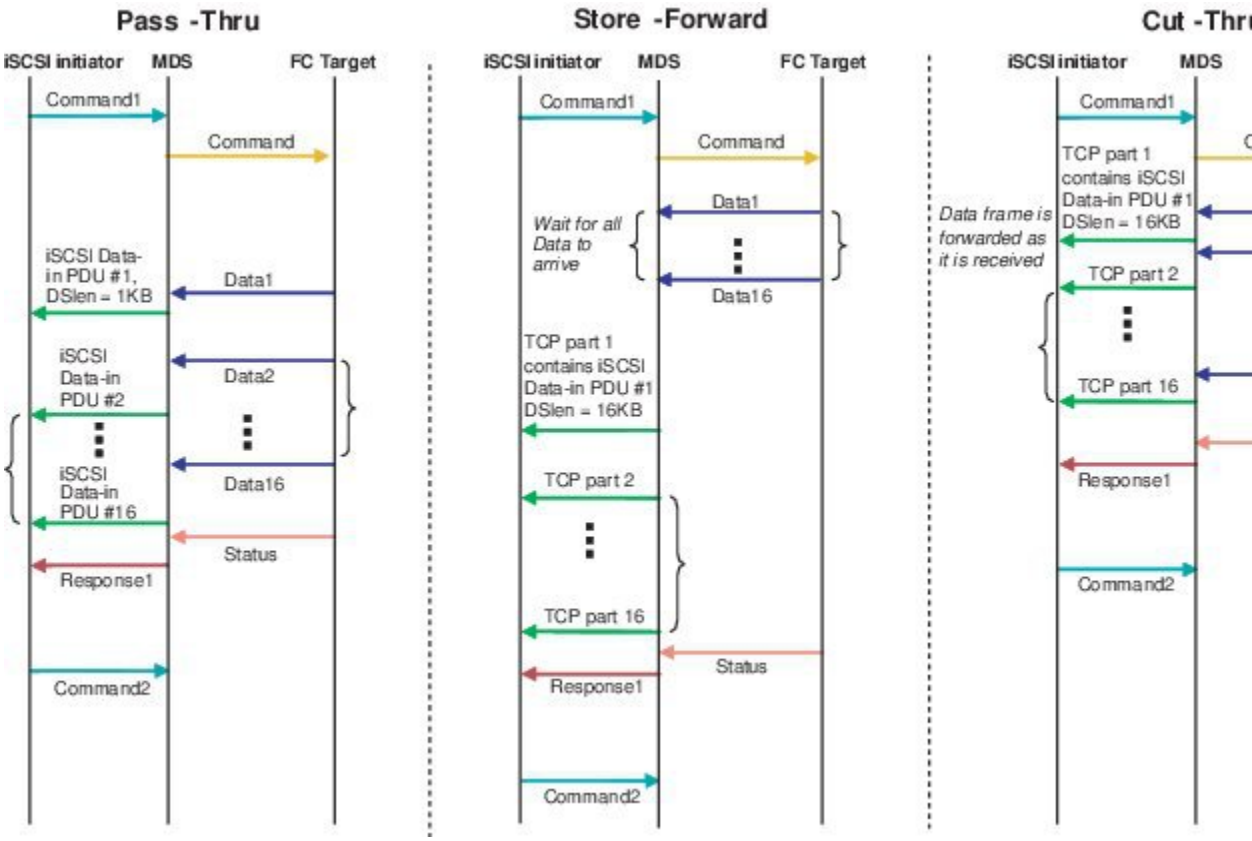


表 *7 : iSCSI* ルーティング モードの比較

モード	利点	欠点
パススルー	遅延が小さい。 データ ダイジェストが使用可能。	データ転送パフォーマンスが低い。
ストア アンド フォワード	データ転送パフォーマンスが高い。	データ ダイジェストが使用不可。

モード	利点	欠点
カットスルー	読み取りパフォーマンスがストア アンド フォワードより向上。	ファイバチャネル ターゲットが置換可能なさまざまなコマンド用の読み取りデータを送信した場合、最初のコマンドのデータはカットスルー モードで転送されるが、後続コマンドのデータはバッファリングされ、動作はストア アンド フォワード モードと同じになる。 データ ダイジェストが使用不可。

（注） iSLB VRRP グループに属している iSCSI インターフェイスの転送モードを変更すると、インターフェイスのロードバランシングが影響を受けます。「iSCSIインターフェイス パラメータの変更およびロード バランシングへの影響」セクションを参照してください。

QoS 値の設定

QoS 値を設定するには、次のステップを実行します。

手順

ステップ 1 この iSCSI インターフェイスのすべての発信 IP パケットに適用される Differentiated Services Code Point（DSCP）値を 3 に構成します。iSCSI DSCP 値の有効範囲は 0～63 です。

```
switch(config-if)# qos 3
```

ステップ 2 スイッチを工場出荷時設定に戻します（すべてのパケットが DSCP 値 0 でマークされます）。

```
switch(config-if)# no qos 5
```

iSCSI 情報の表示

iSCI の構成に関する詳細情報を取得するには、**show iscsi** コマンドを使用します。

この項では、次のトピックについて取り上げます。

- iSCSI インターフェイスの表示
- iSCSI 統計情報の表示

- プロキシ イニシエータ情報の表示
- グローバル iSCSI 情報の表示
- iSCSI セッションの表示
- iSCSI イニシエータの表示
- iSCSI 仮想ターゲットの表示
- iSCSI ユーザー情報の表示

iSCSI インターフェイスの表示

iSCSI インターフェイスの概要、カウンタ、説明、およびステータスを表示するには、**show iscsi interface** コマンドを使用します。この出力を使用して、管理モード、インターフェイスのステータス、現在使用中の TCP パラメータ、および短い統計情報を確認します。

iSCSI インターフェイス情報の表示例

```
switch# show interface iscsi 4/1
iscsi4/1 is up
Hardware is GigabitEthernet
Port WWN is 20:cf:00:0c:85:90:3e:80
Admin port mode is ISCSI
Port mode is ISCSI
Speed is 1 Gbps
iSCSI initiator is identified by name
Number of iSCSI session: 0 (discovery session: 0)
Number of TCP connection: 0
Configured TCP parameters
Local Port is 3260
PMTU discover is enabled, reset timeout is 3600 sec
Keepalive-timeout is 60 sec
Minimum-retransmit-time is 300 ms
Max-retransmissions 4
Sack is enabled
QOS code point is 0
Maximum allowed bandwidth is 1000000 kbps
Minimum available bandwidth is 70000 kbps
Estimated round trip time is 1000 usec
Send buffer size is 4096 KB
Congestion window monitoring is enabled, burst size is 50 KB
Configured maximum jitter is 500 us
Forwarding mode: store-and-forward
TMF Queueing Mode : disabled
Proxy Initiator Mode : disabled
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
iSCSI statistics
Input 0 packets, 0 bytes
Command 0 pdus, Data-out 0 pdus, 0 bytes
Output 0 packets, 0 bytes
Response 0 pdus (with sense 0), R2T 0 pdus
Data-in 0 pdus, 0 bytes
```

iSCSI 統計情報の表示

iSCSI インターフェイスごとの短い iSCSI 統計情報または詳細な iSCSI 統計情報を表示するには、 **show iscsi stats** コマンドを使用します。詳細については、次の例を参照してください。

次の例は、IPS ポートでのインバウンドおよびアウトバウンドの両方向の iSCSI スループットを示します。また、この IPS ポートが送受信する異なる種類の iSCSI PDU の数を示します

iSCSI インターフェイスの短い iSCSI 統計情報の表示例

```
switch# show iscsi stats iscsi 2/1
iscsi2/1
5 minutes input rate 704 bits/sec, 88 bytes/sec, 1 frames/sec
5 minutes output rate 704 bits/sec, 88 bytes/sec, 1 frames/sec
iSCSI statistics
974756 packets input, 142671620 bytes
Command 2352 pdus, Data-out 44198 pdus, 92364800 bytes, 0 fragments, unsolicited 0 bytes
output 1022920 packets, 143446248 bytes
Response 2352 pdus (with sense 266), R2T 1804 pdus
Data-in 90453 pdus, 92458248 bytes
```

次の例は、IPS ポートの詳細な iSCSI 統計情報を表示します。トラフィック レートおよび各タイプの iSCSI PDU の数とともに、受信および転送した FCP フレームの数、iSCSI ログインの試行回数、成功回数、および失敗回数が表示されます。また、送受信された各種 iSCSI PDU のうち、重大ではないかまたは頻繁には発生しない iSCSI PDU の数（受信 NOP および送信 NOP（NOP-In および NOP-Out）、テキスト リクエストおよび応答（Text-REQ および Text-RESP）、およびタスク管理リクエストおよび応答（TMF-REQ および TMF-RESP）など）も表示されます。

さまざまなエラー タイプと PDU またはフレーム ドロップ発生回数もカウントされ、表示されます。たとえば、Bad ヘッダーダイジェストは、CRC 検証に失敗したヘッダー ダイジェストがある受信 iSCSI PDU の数を示します。iSCSI Drop セクションには、ターゲットの停止、LUN マッピングの失敗、データ CRC エラー、予想外の即時または非請求データなどの原因でドロップされた PDU の数が示されます。これらの統計情報は、機能が予期したように動作しない場合のデバッグに役立ちます。

最後の [Buffer Stats] セクションは、内部 IPS パケット バッファ動作に関する統計情報を表示します。このセクションはデバッグだけを目的としています。

iSCSI インターフェイスの詳細な iSCSI 統計情報の表示例

```
switch# show iscsi stats iscsi 2/1 detail
iscsi2/1
5 minutes input rate 704 bits/sec, 88 bytes/sec, 1 frames/sec
5 minutes output rate 704 bits/sec, 88 bytes/sec, 1 frames/sec
iSCSI statistics
974454 packets input, 142656516 bytes
Command 2352 pdus, Data-out 44198 pdus, 92364800 bytes, 0 fragments, unsolicited 0 bytes
output 1022618 packets, 143431144 bytes
Response 2352 pdus (with sense 266), R2T 1804 pdus
Data-in 90453 pdus, 92458248 bytes
iSCSI Forward:
Command:2352 PDUs (Rcvd:2352)
Data-Out (Write):16236 PDUs (Rcvd 44198), 0 fragments, 92364800 bytes, unsolicited 0
bytes
FCP Forward:
Xfer_rdy:1804 (Rcvd:1804)
Data-In:90453 (Rcvd:90463), 92458248 bytes
```

```
Response:2352 (Rcvd:2362), with sense 266
TMF Resp:0

iSCSI Stats:
Login:attempt:13039, succeed:110, fail:12918, authen fail:0
Rcvd:NOP-Out:914582, Sent:NOP-In:914582
NOP-In:0, Sent:NOP-Out:0
TMF-REQ:0, Sent:TMF-RESP:0
Text-REQ:18, Sent:Text-RESP:27
SNACK:0
Unrecognized Opcode:0, Bad header digest:0
Command in window but not next:0, exceed wait queue limit:0
Received PDU in wrong phase:0
SCSI Busy responses:0
Immediate data failure::Separation:0
Unsolicited data failure::Separation:0, Segment:0
Add header:0
Sequence ID allocation failure:0
FCP Stats:
Total:Sent:47654
Received:96625 (Error:0, Unknown:0)
Sent:PLOGI:10, Rcvd:PLOGI_ACC:10, PLOGI_RJT:0
PRLI:10, Rcvd:PRLI_ACC:10, PRLI_RJT:0, Error:0, From initiator:0
LOGO:4, Rcvd:LOGO_ACC:0, LOGO_RJT:0
PRLO:4, Rcvd:PRLO_ACC:0, PRLO_RJT:0
ABTS:0, Rcvd:ABTS_ACC:0
TMF REQ:0
Self orig command:10, Rcvd:data:10, resp:10
Rcvd:PLOGI:156, Sent:PLOGI_ACC:0, PLOGI_RJT:156
LOGO:0, Sent:LOGO_ACC:0, LOGO_RJT:0
PRLI:8, Sent:PRLI_ACC:8, PRLI_RJT:0
PRLO:0, Sent:PRLO_ACC:0, PRLO_RJT:0
ADISC:0, Sent:ADISC_ACC:0, ADISC_RJT:0
ABTS:0

iSCSI Drop:
Command:Target down 0, Task in progress 0, LUN map fail 0
CmdSeqNo not in window 0, No Exchange ID 0, Reject 0
No task:0
Data-Out:0, Data CRC Error:0
TMF-Req:0, No task:0
Unsolicited data:0, Immediate command PDU:0
FCP Drop:
Xfer_rdy:0, Data-In:0, Response:0

Buffer Stats:
Buffer less than header size:0, Partial:45231, Split:322
Pullup give new buf:0, Out of contiguous buf:0, Unaligned m_data:0
```

プロキシ イニシエータ情報の表示

プロキシイニシエータ機能がiSCSIインターフェイスで有効になっている場合、設定されているプロキシ イニシエータの情報を表示するには、**show interface iscsi** コマンドを使用します。

システムにより割り当てられたWWNを持つiSCSIインターフェイスのプロキシイニシエータ情報の表示例：

```
switch# show interface iscsi 4/1
iscsi4/1 is up
Hardware is GigabitEthernet
Port WWN is 20:c1:00:05:30:00:a7:9e
Admin port mode is ISCSI
Port mode is ISCSI
```

```
Speed is 1 Gbps
iSCSI initiator is identified by name
Number of iSCSI session: 0, Number of TCP connection: 0
Configured TCP parameters
Local Port is 3260
PMTU discover is enabled, reset timeout is 3600 sec
Keepalive-timeout is 60 sec
Minimum-retransmit-time is 300 ms
Max-retransmissions 4
Sack is disabled
QOS code point is 0
Forwarding mode: pass-thru
TMF Queueing Mode : disabled
Proxy Initiator Mode : enabled<----------------------------Proxy initiator is enabled
nWWN is 28:00:00:05:30:00:a7:a1 (system-assigned)<----System-assigned nWWN
pWWN is 28:01:00:05:30:00:a7:a1 (system-assigned)<---- System-assigned pWWN
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
iSCSI statistics
Input 7 packets, 2912 bytes
Command 0 pdus, Data-out 0 pdus, 0 bytes
Output 7 packets, 336 bytes
Response 0 pdus (with sense 0), R2T 0 pdus
Data-in 0 pdus, 0 bytes
```

ユーザーによって割り当てられたWWNを持つiSCSIインターフェイスのプロキシイニシエータ情報の表示例：

```
switch# show interface iscsi 4/2
iscsi4/2 is up
Hardware is GigabitEthernet
Port WWN is 20:c1:00:05:30:00:a7:9e
Admin port mode is ISCSI
Port mode is ISCSI
Speed is 1 Gbps
iSCSI initiator is identified by name
Number of iSCSI session: 0, Number of TCP connection: 0
Configured TCP parameters
Local Port is 3260
PMTU discover is enabled, reset timeout is 3600 sec
Keepalive-timeout is 60 sec
Minimum-retransmit-time is 300 ms
Max-retransmissions 4
Sack is disabled
QOS code point is 0
Forwarding mode: pass-thru
TMF Queueing Mode : disabled
Proxy Initiator Mode : enabled
nWWN is 11:11:11:11:11:11:11:11 (manually-configured)<----User-assigned nWWN
pWWN is 22:22:22:22:22:22:22:22 (manually-configured)<----User-assigned pWWN
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
iSCSI statistics
Input 7 packets, 2912 bytes
Command 0 pdus, Data-out 0 pdus, 0 bytes
Output 7 packets, 336 bytes
Response 0 pdus (with sense 0), R2T 0 pdus
Data-in 0 pdus, 0 bytes
```

グローバル iSCSI 情報の表示

全体的な設定と iSCSI ステータスを表示するには、**show iscsi global** コマンドを使用します。

現在のグローバル iSCSI 構成とステータスの表示例：

```
switch# show iscsi global
iSCSI Global information
Authentication: CHAP, NONE
Import FC Target: Enabled
Initiator idle timeout: 300 seconds
Number of target node: 0
Number of portals: 11
Number of session: 0
Failed session: 0, Last failed initiator name:
```

iSCSI セッションの表示

スイッチの現在の iSCSI セッションに関する詳細を表示するには、**show iscsi session** コマンドを使用します。パラメータを指定しない場合、このコマンドはすべてのセッションを表示します。イニシエータ、ターゲット、またはこの両方を指定して出力をフィルタリングできます。次の例では、IQN（iqn.1987-05.com.cisco:02.3021b0f2fda0.avanti12-w2k）に基づいて構成されている iSCSI イニシエータと、IPv4 アドレス（10.10.100.199）に基づいて構成されている別の iSCSI イニシエータを示します。

すべての iSCSI セッションの短い情報の表示例

```
switch# show iscsi session
Initiator iqn.1987-05.com.cisco:02.3021b0f2fda0.avanti12-w2k
Initiator ip addr (s): 10.10.100.116
Session #1
Discovery session, ISID 00023d000043, Status active
Session #2
Target VT1
VSAN 1, ISID 00023d000046, Status active, no reservation
Session #3
Target VT2
VSAN 1, ISID 00023d000048, Status active, no reservation
Initiator 10.10.100.199
Initiator name iqn.1987-05.com.cisco.01.7e3183ae458a94b1cd6bc168cba09d2e
Session #1
Target VT2
VSAN 1, ISID 246700000000, Status active, no reservation
Session #2
Target VT1
VSAN 1, ISID 246b00000000, Status active, no reservation
Session #3
Target iqn.1987-05.com.cisco:05.switch.04-01.2100002037a6be32
VSAN 1, ISID 246e00000000, Status active, no reservation
```

次の例は、IPv4 アドレス（10.10.100.199）に基づいて設定された iSCSI イニシエータを示します。

指定した iSCSI セッション短い情報の表示例：

```
switch# show iscsi session initiator 10.10.100.199 target VT1
Initiator 10.10.100.199
Initiator name iqn.1987-05.com.cisco.01.7e3183ae458a94b1cd6bc168cba09d2e
Session #1
Target VT1
VSAN 1, ISID 246b00000000, Status active, no reservation
```

指定した iSCSI セッションの詳細情報の表示例：

```
switch# show iscsi session initiator 10.10.100.199 target VT1 detail
Initiator 10.10.100.199 (oasis-qa)
Initiator name iqn.1987-05.com.cisco.01.7e3183ae458a94b1cd6bc168cba09d2e
Session #1 (index 3)
Target VT1
VSAN 1, ISID 246b00000000, TSIH 384, Status active, no reservation
Type Normal, ExpCmdSN 39, MaxCmdSN 54, Barrier 0
MaxBurstSize 0, MaxConn 0, DataPDUInOrder No
DataSeqInOrder No, InitialR2T Yes, ImmediateData No
Registered LUN 0, Mapped LUN 0
Stats:
PDU: Command: 38, Response: 38
Bytes: TX: 8712, RX: 0
Number of connection: 1
Connection #1
Local IP address: 10.10.100.200, Peer IP address: 10.10.100.199
CID 0, State: LOGGED_IN
StatSN 62, ExpStatSN 0
MaxRecvDSLength 1024, our_MaxRecvDSLength 1392
CSG 3, NSG 3, min_pdu_size 48 (w/ data 48)
AuthMethod none, HeaderDigest None (len 0), DataDigest None (len 0)
Version Min: 2, Max: 2
FC target: Up, Reorder PDU: No, Marker send: No (int 0)
Received MaxRecvDSLen key: No
```

iSCSI イニシエータの表示

スイッチの iSCSI インターフェイスに接続されているすべてのイニシエータに関する情報を表示するには、**show iscsi initiator** コマンドを使用します。目的の iSCSI 発信側だけを表示するように情報をフィルタリングするには、発信側名を指定します。iSCSI イニシエータの詳細出力を取得するには、**detail** オプションを指定します。**iscsi-session**（およびオプションで **detail**）パラメータを指定すると、iSCSI セッション情報だけが表示されます。**fcp-session**（およびオプションで **detail**）パラメータを指定すると、FCP セッション情報だけが表示されます。出力には、スタティック イニシエータとダイナミック イニシエータが含まれます。

接続されている iSCSI イニシエータの情報の表示例

```
switch# show iscsi initiator
iSCSI Node name is iqn.1987-05.com.cisco:02.3021b0f2fda0.avanti12-w2k
Initiator ip addr (s): 10.10.100.116
iSCSI alias name: AVANTI12-W2K
Node WWN is 22:01:00:05:30:00:10:e1 (configured)
Member of vsans: 1, 2, 10
Number of Virtual n_ports: 1
Virtual Port WWN is 22:04:00:05:30:00:10:e1 (configured)
Interface iSCSI 4/1, Portal group tag: 0x180
VSAN ID 1, FCID 0x6c0202
VSAN ID 2, FCID 0x6e0000
VSAN ID 10, FCID 0x790000

iSCSI Node name is 10.10.100.199
iSCSI Initiator name: iqn.1987-05.com.cisco.01.7e3183ae458a94b1cd6bc168cba09d2e
iSCSI alias name: oasis-qa
Node WWN is 22:03:00:05:30:00:10:e1 (configured)
Member of vsans: 1, 5
Number of Virtual n_ports: 1
Virtual Port WWN is 22:00:00:05:30:00:10:e1 (configured)
Interface iSCSI 4/1, Portal group tag: 0x180
VSAN ID 5, FCID 0x640000
VSAN ID 1, FCID 0x6c0203
```

iSCSI イニシエータの詳細情報の表示例

```
switch# show iscsi initiator iqn.1987-05.com.cisco:02.3021b0f2fda0.avanti12-w2k detail
iSCSI Node name is iqn.1987-05.com.cisco:02.3021b0f2fda0.avanti12-w2k
Initiator ip addr (s): 10.10.100.116
iSCSI alias name: AVANTI12-W2K
Node WWN is 22:01:00:05:30:00:10:e1 (configured)
Member of vsans: 1, 2, 10
Number of Virtual n_ports: 1

Virtual Port WWN is 22:04:00:05:30:00:10:e1 (configured)
Interface iSCSI 4/1, Portal group tag is 0x180
VSAN ID 1, FCID 0x6c0202
1 FC sessions, 1 iSCSI sessions
iSCSI session details <-------------------iSCSI session details
Target: VT1
Statistics:
PDU: Command: 0, Response: 0
Bytes: TX: 0, RX: 0
Number of connection: 1
TCP parameters
Local 10.10.100.200:3260, Remote 10.10.100.116:4190
Path MTU: 1500 bytes
Retransmission timeout: 310 ms
Round trip time: Smoothed 160 ms, Variance: 38
Advertized window: Current: 61 KB, Maximum: 62 KB, Scale: 0
Peer receive window: Current: 63 KB, Maximum: 63 KB, Scale: 0
Congestion window: Current: 1 KB

FCP Session details <-------------------FCP session details
Target FCID: 0x6c01e8 (S_ID of this session: 0x6c0202)
pWWN: 21:00:00:20:37:62:c0:0c, nWWN: 20:00:00:20:37:62:c0:0c
Session state: CLEANUP
1 iSCSI sessions share this FC session
Target: VT1
Negotiated parameters
RcvDataFieldSize 1392 our_RcvDataFieldSize 1392
MaxBurstSize 0, EMPD: FALSE
Random Relative Offset: FALSE, Sequence-in-order: Yes
Statistics:
PDU: Command: 0, Response: 0
```

SAN の iSCSI イニシエータ用に作成されたファイバ チャネル N ポートのファイバ チャネル ネーム サーバ エントリを表示するには、**show fcns database**（およびオプションで **detail**）コマンドを使用します。

FCNS データベースの内容の表示例

```
switch# show fcns database
VSAN 1:
------------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
------------------------------------------------------------------------
0x020101 N 22:04:00:05:30:00:35:e1 (Cisco) scsi-fcp:init isc..w <--iSCSI
0x020102 N 22:02:00:05:30:00:35:e1 (Cisco) scsi-fcp:init isc..w initiator
0x0205d4 NL 21:00:00:04:cf:da:fe:c6 (Seagate) scsi-fcp:target
0x0205d5 NL 21:00:00:04:cf:e6:e4:4b (Seagate) scsi-fcp:target
...
Total number of entries = 10

VSAN 2:
------------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
------------------------------------------------------------------------
```

```
0xef0001 N 22:02:00:05:30:00:35:e1 (Cisco) scsi-fcp:init isc..w
Total number of entries = 1

VSAN 3:
--------------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0xed0001 N 22:02:00:05:30:00:35:e1 (Cisco) scsi-fcp:init isc..w
Total number of entries = 1
```

FCNS データベースの詳細表示例

```
switch# show fcns database detail
------------------------
VSAN:1 FCID:0x020101
------------------------
port-wwn (vendor) :22:04:00:05:30:00:35:e1 (Cisco)
node-wwn :22:03:00:05:30:00:35:e1
class :2,3
node-ip-addr :10.2.2.12 <--- iSCSI initiator's IPv4 address
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :iqn.1991-05.com.microsoft:oasis2-dell <--- iSCSI initiator's IQN
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :22:01:00:05:30:00:35:de
hard-addr :0x000000
------------------------
VSAN:1 FCID:0x020102
------------------------
port-wwn (vendor) :22:02:00:05:30:00:35:e1 (Cisco)
node-wwn :22:01:00:05:30:00:35:e1
class :2,3
node-ip-addr :10.2.2.11
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :iqn.1987-05.com.cisco.01.14ac33ba567f986f174723b5f9f2377
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :22:01:00:05:30:00:35:de
hard-addr :0x000000
...
Total number of entries = 10
==========================================================================
------------------------
VSAN:2 FCID:0xef0001
------------------------
port-wwn (vendor) :22:02:00:05:30:00:35:e1 (Cisco)
node-wwn :22:01:00:05:30:00:35:e1
class :2,3
node-ip-addr :10.2.2.11
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :iqn.1987-05.com.cisco.01.14ac33ba567f986f174723b5f9f2377
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :22:01:00:05:30:00:35:de
hard-addr :0x000000
Total number of entries = 1
...
```

構成されたすべての iSCSI イニシエータに関する情報を表示するには、**show iscsi initiator configured** を使用します。名前を指定すると、目的のイニシエータに関する情報が表示されます。

構成したイニシエータに関する情報の表示例

```
switch# show iscsi initiator configured
iSCSI Node name is iqn.1987-05.com.cisco:02.3021b0f2fda0.avanti12-w2k
Member of vsans: 1, 2, 10
Node WWN is 22:01:00:05:30:00:10:e1
No. of PWWN: 5
Port WWN is 22:04:00:05:30:00:10:e1
Port WWN is 22:05:00:05:30:00:10:e1
Port WWN is 22:06:00:05:30:00:10:e1
Port WWN is 22:07:00:05:30:00:10:e1
Port WWN is 22:08:00:05:30:00:10:e1

iSCSI Node name is 10.10.100.199
Member of vsans: 1, 5
Node WWN is 22:03:00:05:30:00:10:e1
No. of PWWN: 4
Port WWN is 22:00:00:05:30:00:10:e1
Port WWN is 22:09:00:05:30:00:10:e1
Port WWN is 22:0a:00:05:30:00:10:e1
Port WWN is 22:0b:00:05:30:00:10:e1

User Name for Mutual CHAP: testuser
```

iSCSI 仮想ターゲットの表示

iSCSI イニシエータに iSCSI 仮想ターゲットとしてエクスポートされたファイバ チャネル ターゲットに関する情報を表示するには、 **show iscsi virtual-target** を使用します。出力には、スタティック ターゲットとダイナミック ターゲットが含まれます。

エクスポートされたターゲットの表示例

```
switch# show iscsi virtual-target
target: VT1
* Port WWN 21:00:00:20:37:62:c0:0c
Configured node
all initiator permit is enabled
target: VT2
Port WWN 21:00:00:04:cf:4c:52:c1
Configured node
all initiator permit is disabled
target: iqn.1987-05.com.cisco:05.switch.04-01.2100002037a6be32
Port WWN 21:00:00:20:37:a6:be:32 , VSAN 1
Auto-created node
```

iSCSI ユーザー情報の表示

構成されたすべての iSCSI ユーザー名を表示するには、**show user-account iscsi** コマンドを使用します。

iSCSI ユーザー名の表示例

```
switch# show user-account iscsi
username:iscsiuser
secret: dsfffsffsffasffsdffg
username:user2
secret:cshadhdhsadadjajdjas
```

iSLB の構成

iSCSI サーバ ロードバランシング（iSLB）機能を使用すると、百単位、場合によっては千単位のイニシエータからなる大規模な iSCSI 環境を容易に構成できます。iSLB には次の機能があります。

- 発信側ターゲットおよび自動ゾーンがサポートされるので、iSLB 発信側の設定が簡素化されます。
- Cisco Fabric Services（CFS）によって、ファブリックのすべての MDS スイッチに iSLB 発信側設定が配信されるので、手動設定が不要になります。
- iSCSI ログイン リダイレクトおよび VRRP を使用することによって、iSLB 発信側のダイナミック ロード バランシングが使用できます。

iSLB を使用しない場合、iSCSI を設定するために次の作業が必要になります。

- 次の作業を含め、MDS スイッチ上で複数の設定手順を実行する必要があります。
  - スタティック pWWN および VSAN を使用した発信側の設定
  - 発信側およびターゲットのゾーン分割設定
  - （任意）仮想ターゲットの作成および発信側へのアクセス権付与
  - MDS スイッチ上で発信側に作成したスタティック pWWN に基づく、発信側に関するストレージ システム上でのターゲット LUN マッピングおよびマスクの設定
- 複数の MDS スイッチに、設定を手動でコピーする必要があります。
- IPS ポートにロード バランシングはありません。次に例を示します。
  - 仮想ルータ冗長プロトコル（VRRP）がサポートするのは、アクティブおよびバックアップだけであり、ロード バランシングはサポートしません。
  - 複数の VRRP グループを使用し、さまざまなグループでホストを設定する必要があります。

iSLB には次の機能があります。

- 発信側ターゲットおよび自動ゾーンがサポートされるので、iSLB 発信側の設定が簡素化されます。
- Cisco Fabric Services（CFS）によって、ファブリックのすべての MDS スイッチに iSLB 発信側設定が配信されるので、手動設定が不要になります。

（注） CFS を使用した場合、ファブリック全体に配信されるのは、スタティック マッピングの iSLB 発信側設定だけです。ダイナミックおよびスタティック マッピングの iSCSI 発信側設定は配信されません。

- iSCSI ログイン リダイレクトおよび VRRP を使用することによって、iSLB 発信側のダイナミック ロード バランシングが使用できます。

（注） iSLB を構成する前に、iSCSI を有効にする必要があります（「iSCSI の有効化」セクションを参照）。

iSLB を使用するには、ファブリック内のすべてのスイッチで、Cisco MDS SAN-OS Release 2.1(1a) 以降が稼働している必要があります。

この項では、次のトピックについて取り上げます。

iSLB の設定制限

iSLB の設定に関しては、次の限度があります。

- ファブリックでサポートされる iSLB および iSCSI 発信側の最大数は 2000 です。
- 透過型またはプロキシイニシエータ モードで IPS ポートがサポートする iSLB および iSCSI セッションの最大数は 500 です。
- ファブリックでサポートされる iSLB イニシエータの最大数は 2000 です。
- スイッチがサポートする iSLB イニシエータおよび iSCSI セッションの最大数は 5000 です。
- 透過型またはプロキシ イニシエータ モードにおいて、各 IPS ポートの最大 iSLB セッション数は 500 です。
- ファブリックでサポートされる iSLB および iSCSI ターゲットの最大数は 6000 です。
- CFS 配信が有効な iSLB を使用できるファブリック内のスイッチの最大数は 4 です。
- 保留中の設定に追加できる新規 iSLB 発信側の最大数は 200 です。発信側をそれ以上追加する場合は、設定をいったんコミットする必要があります。
- 実行コンフィギュレーションで 200 を超える iSLB 発信側を設定している場合、iSCSI をディセーブルにできません。iSLB 発信側を 200 未満に減らしてから、iSCSI をディセーブルにしてください。
- CFS の配信を使用しないで iSLB を使用することは可能ですが、iSLB 自動ゾーン機能を使用した場合、ゾーンセットがアクティブになった時点で、トラフィックが中断されます。

- IVR および iSLB 機能が同じファブリックでイネーブルの場合、ファブリック内に両方の機能がイネーブルのスイッチが少なくとも 1 つは必要です。ゾーン分割関連の設定およびアクティブ化（標準ゾーン、IVR ゾーン、または iSLB ゾーン）は、このスイッチ上で実行する必要があります。そうしないと、ファブリック内のトラフィックが中断することがあります。

iSLB 構成の前提条件

iSLB を設定する前に、次の前提作業を実行します。

- iSCSI を有効にします（詳細については、「iSCSI の有効化」セクションを参照してください）。
- ギガビット イーサネット インターフェイスを構成します（「IPv4 のギガビット イーサネットの基本構成」セクションを参照）。
- VRRP グループを構成します（「VRRP を使用したロードバランシングを構成」セクションを参照）。
- ゾーン セットを設定してアクティブにします（詳細については、『Cisco Fabric Manager ファブリック構成ガイド』『Cisco MDS 9000 Family NX-OS ファブリック構成ガイド』を参照してください）。
- iSLB の CFS 配信を有効にします（「iSLB 構成の配信の有効化」セクションを参照）。

iSLB イニシエータ

iSLB イニシエータは、iSCSI イニシエータが提供する機能のほかに、次の機能を提供します。

- iSLB 発信側は、iSLB 仮想ターゲットもサポートします。
- イニシエータ ターゲット：これらのターゲットは、特定のイニシエータに対して設定されます。
- iSCSI ログイン リダイレクトおよび VRRP を使用するロード バランシング：iSCSI ログイン リダイレクトが有効な場合、IPS Manager はインターフェイスごとに計算した負荷に基づいて、最良のインターフェイスに着信セッションをリダイレクトします。
- CFS を使用して行う他のスイッチへの設定配信

iSLB イニシエータは、iSCSI イニシエータが提供する機能のほかに、次の機能を提供します。

- iSLB 発信側は、iSLB 仮想ターゲットもサポートします。これらのターゲットは iSCSI 仮想ターゲットときわめて類似していますが、アドバタイズ インターフェイス オプションがないので、CFS を使用して配信可能であることが異なります。
- 発信側ターゲット：これらのターゲットは、特定の発信側に対して設定されます。

- iSCSI ログイン リダイレクトおよび VRRP を使用するロード バランシング：ロード バランシングがイネーブルの場合、IPS Manager はインターフェイスごとに計算した負荷に基づいて、最良のインターフェイスに着信セッションをリダイレクトします。
- CFS を使用して行う他のスイッチへの設定配信

iSLB イニシエータの構成

このセクションは、次のトピックで構成されています。

iSLB イニシエータの構成

iSLB イニシエータの **name** オプションを 使用して iSLB イニシエータ構成サブモードを開始するには、次のステップを実行します。

始める前に

iSLB 発信側を設定する前に、その名前または IP アドレスを指定する必要があります。

iSLB 発信側の名前または IP アドレスの指定方法は、iSCSI 発信側の場合と同じです。「スタティック マッピング」を参照してください。

手順

ステップ 1 イニシエータ ノードの iSCSI 名 (iqn.1987-02.com.cisco.initiator) を使用して iSLB イニシエータを設定し、iSLBイニシエータ設定サブモードに入ります。名前の最大長は、英数字223 文字です。最小長は16 です。

```
switch# config terminal
switch(config)#
switch(config)# islb initiator name iqn.1987-02.com.cisco.initiator
switch(config-islb-init)#
```

ステップ 2 構成済み iSLB イニシエータを削除します。

```
switch(config)# no lslb initiator name iqn.1987-02.com.cisco.initiator
```

iSLB イニシエータ IP アドレスの構成

iSLB イニシエータの **ip-address** オプションを使用して iSLB イニシエータ コンフィギュレーション サブモードを開始するには、次の手順を実行します。

始める前に

iSLB 発信側を設定する前に、その名前または IP アドレスを指定する必要があります。

iSLB 発信側の名前または IP アドレスの指定方法は、iSCSI 発信側の場合と同じです。「スタティック マッピング」を参照してください。

手順

ステップ 1 イニシエータ ノードの IPv4 アドレスを使用して iSLB イニシエータを構成し、iSLB イニシエータ構成サブモードを開始します。

```
switch# config terminal
switch(config)# islb initiator ip-address 10.1.1.3
```

ステップ 2 構成済み iSLB イニシエータを削除します。

```
switch(config)# no islb initiator ip-address 10.1.1.3
```

ステップ 3 イニシエータ ノードの IPv6 ユニキャスト アドレスを使用して iSLB イニシエータを構成し、iSLB イニシエータ構成サブモードを開始します。

```
switch(config)# islb initiator ip-address 2001:0DB8:800:200C::417A
switch(config-islb-init)#
```

ステップ 4 構成済み iSLB イニシエータを削除します。

```
switch(config)# no islb initiator ip-address 2001:0DB8:800:200C::417A
```

iSLB 発信側への WWN の割り当て

iSLB ホストは次のいずれかのメカニズムで、N ポートの WWN に対応付けられます。

- ダイナミック マッピング（デフォルト）
- スタティック マッピング

（注） iSLB 発信側の WWN 割り当ては、iSCSI 発信側の場合と同じです。ダイナミックおよびスタティック マッピングの詳細については、「iSCSI イニシエータの WWN 割り当て」を参照してください。

SystemAssign system-assign オプションの使用を推奨します。手動で WWN を割り当てる場合は、固有の割り当てにする必要があります（詳細については、『Cisco Fabric Manager ファブリック構成ガイド』『Cisco MDS 9000 ファミリ NX-OS ファブリック構成ガイド』を参照してください）。すでに割り当てられている WWN は使用できません。

ダイナミック iSLB 発信側 WWN マッピングをスタティックにする方法

ダイナミック iSLB イニシエータのログイン後に、そのイニシエータで次回ログイン時にも同じマッピングが使用されるように、自動的に割り当てられた nWWN/pWWN マッピングを維持することがあります（「ダイナミック マッピング」セクションを参照してください）。

ダイナミック iSLB イニシエータをスタティック iSLB イニシエータに変換し、対応する WWN を固定にすることができます

（注） ダイナミック iSCSI 発信側をスタティック iSLB 発信側に変換したり、ダイナミック iSLB 発信側をスタティック iSCSI 発信側に変換したりはできません。詳細については、「ダイナミック マッピング」を参照してください）。

（注） iSLB イニシエータのダイナミック マッピングをスタティックにする方法は、iSCSI の場合と同じです。

（注） CFS を使用した場合、ファブリック全体に配信されるのは、スタティック マッピングの iSLB 発信側設定だけです。ダイナミックおよびスタティックに設定された iSCSI 発信側設定は配信されません。

iSLB ターゲット アクセス マッピング

iSLB では、iSCSI 仮想ターゲット アクセスを含むすべてのファブリック配信設定は、iSCSI イニシエータ設定の一部です。アクセスは pWWN またはデバイス エイリアスを使用して付与されます。次のオプション パラメータを 1 つまたは複数指定することもできます。

- セカンダリ pWWN
- セカンダリ デバイス エイリアス
- LUN マッピング
- IQN

さらに、自動ゾーン分割を無効にできます。

イニシエータ ターゲットに IQN を設定する場合は、その名前を使用してターゲットを特定する必要があります。そうしないと、イニシエータ ターゲットに一意の IQN が生成されます。

永続的な nWWN/pWWN マッピングの構成

自動的に割り当てられた nWWN/pWWN マッピングを永続的に維持するには、次のステップを実行します。

手順

ステップ 1 名前で指定された iSLB イニシエータに自動的に割り当てられた pWWN および nWWN を保存します。

```
switch# config terminal
switch(config)# islb save-initiator name iqn.1987-02.com.cisco.initiator
```

ステップ 2 IPv4 アドレスで指定された iSLB イニシエータに自動的に割り当てられた pWWN および nWWN を保存します。

```
switch(config)# islb save-initiator 10.10.100.11
```

ステップ 3 IPv6 ユニキャスト アドレスで指定された iSCSI イニシエータに自動的に割り当てられた pWWN および nWWN を保存します。

```
switch(config)# iscsi save-initiator ip-address 2001:0DB8:800:200C::417A
```

ステップ 4 すべての iSLB イニシエータに自動的に割り当てられた nWWN と pWWN を保存します。

```
switch(config)# islb save-initiator
switch(config)# exit
```

ステップ 5 システム リブート後も nWWN/pWWN マッピング構成を保存します。

```
switch# copy running-config startup-config
```

iSCSI 仮想ターゲットへの iSLB イニシエータ アクセスの構成

iSCSI 仮想ターゲットへの iSLB イニシエータ アクセスを構成するには、次のステップを実行します。

手順

ステップ 1 名前を使用してイニシエータを構成し、iSLB イニシエータ コンフィギュレーション サブモードを開始します。

```
switch# config terminal
switch(config)# islb initiator ip-address 10.1.1.3
switch(config-iscsi-islb-init)#
```

ステップ 2 自動ゾーン分割が有効な状態（デフォルト）で pWWN を使用してターゲットへのアクセスを iSLB イニシエータに付与します。

```
switch(config-iscsi-islb-init)# target pwwn 26:00:01:02:03:04:05:06
```

ステップ 3 自動ゾーン分割が無効な状態で pWWN を使用してターゲットへのアクセスを iSLB イニシエータに付与します。

```
switch(config-iscsi-islb-init)# target pwwn 26:00:01:02:03:04:05:06 no-zone
```

ステップ 4 自動ゾーン分割が有効な状態（デフォルト）でデバイス エイリアスを使用してターゲットへのアクセスを iSLB イニシエータに付与します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias
```

ステップ 5 デバイス エイリアスとオプションの LUN マッピングを使用して、ターゲットへのアクセスを iSLB イニシエータに許可します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias fc-lun 0x1234 iscsi-lun 0x2345
```

ステップ 6 デバイス エイリアスとオプションの IQN を使用して、iSLB イニシエータがターゲットにアクセスすることを許可します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias iqn-name
iqn.1987-01.com.cisco.initiator
```

ステップ 7 デバイスエイリアスとオプションのセカンダリデバイスエイリアスを使用して、iSLBイニシエータにターゲットへのアクセスを許可します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias sec-device-alias SecondaryAlias
```

ステップ 8 デバイス エイリアスとオプションのセカンダリ pWWN を使用して、iSLB イニシエータ ターゲットへのアクセスを許可します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias sec-pwwn 26:01:02:03:04:05:06:07
```

ステップ 9 ターゲット アクセスを削除します。

```
switch(config-iscsi-init)# no target pwwn 26:00:01:02:03:04:05:06
```

iSLB ターゲットの構成の確認

iSLB ターゲット構成を確認するには、**show islb initiator configured** コマンドを使用します。

```
switch# show islb initiator configured
iSCSI Node name is 10.1.1.3
Number of Initiator Targets: 1
Initiator Target: iqn.1987-05.com.cisco:05.ips-hac4
Port WWN 50:06:04:82:ca:e1:26:8d
Zoning Enabled
No. of LU mapping: 3
iSCSI LUN: 0x0001, FC LUN: 0x0001
iSCSI LUN: 0x0002, FC LUN: 0x0002
iSCSI LUN: 0x0003, FC LUN: 0x0003
```

iSLB イニシエータへの VSAN メンバーシップの割り当て

特定の VSAN に属すように、個々の iSLB ホストを設定できます（ファイバチャネルの DPVM 機能と同様）。指定した VSAN によって、iSCSI インターフェイスの VSAN メンバーシップが上書きされます。

詳細については、『Cisco MDS 9000 ファミリ NX-OS Fabric Manager ファブリック構成ガイド』を参照してください。

iSLB 発信側の VSAN メンバーシップを割り当てるには、次の手順を実行します。

始める前に

iSLB 発信側 VSAN の指定方法は、iSCSI 発信側の場合と同じです。「iSCSI の VSAN メンバーシップ」を参照してください。

その他の VSAN（デフォルトの VSAN である VSAN 1 以外）内に iSLB 発信側を設定すると（VSAN 2 など）、発信側は自動的に VSAN 1 から削除されます。VSAN 1 にもこの発信側を存続させる場合は、この発信側を VSAN 1 内に明示的に設定する必要があります。

手順

ステップ 1 IPv4 アドレスを使用して iSLB イニシエータを構成し、iSLB イニシエータ構成サブモードを開始します

```
switch# config terminal
switch(config)# islb initiator ip-address 10.1.1.3
switch(config-islb-init)#
```

ステップ 2 指定された VSAN に iSLB 発信側ノードを割り当てます。1 つ以上の VLAN にこのホストを割り当てることができます。

```
switch(config-islb-init)# vsan 3
```

ステップ 3 指定された VSAN から iSLB イニシエータを削除します。

```
switch(config-islb-init)# no vsan 3
```

ロード バランシングのメトリック設定

重み付け ロード バランシングのために、各発信側にロード メトリックを 割り当てることができます。算出される負荷は、所定の iSCSI インターフェイス上の発信側の数に基づいて決まります。この機能を使用すると、発信側間で帯域幅要件が異なる状況に対応できます。たとえば、データベース サーバーには Web サーバーよりも大きいロード メトリックを割り当てることができます。重み付けロードバランシングは、発信側間でリンク速度の異なる状況にも対応できます。

また、デバイス エイリアスまたは pWWN を使用することによって、発信側ターゲットを設定することもできます。発信側ターゲットに IQN を設定する場合は、その名前を使用して発信側ターゲットを特定する必要があります。そうしないと、イニシエータ ターゲットに一意の IQN が生成されます。

ロード バランシングの詳細については、「VRRP を使用したロード バランシング」を参照してください。

ロード バランシングの重みを設定するには、次の手順を実行します。

手順

ステップ 1 イニシエータ ノードの名前を使用して iSLB イニシエータを構成し、iSLB イニシエータ構成サブモードを開始します。

```
switch# config terminal
switch(config)# islb initiator name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-init)#
```

ステップ 2 この iSLB イニシエータの重みメトリックとして 100 を割り当てます。

```
switch(config-iscsi-init)# metric 100
```

ステップ 3 デフォルト値（1000）に戻します。

```
switch(config-iscsi-init)# no metric 100
```

iSLB イニシエータ構成の確認

iSLB イニシエータ構成を確認するには、**show islb initiator configured** コマンドを使用します。

```
switch# show islb initiator configured
iSCSI Node name is 10.1.1.2
Member of vsans: 10
Node WWN is 23:02:00:0c:85:90:3e:82
Load Balance Metric: 100
Number of Initiator Targets: 1
Initiator Target: test-targt
Port WWN 01:01:01:01:02:02:02:02
Primary PWWN VSAN 1
Zoning support is enabled
Trespass support is disabled
Revert to primary support is disabled
```

iSLB イニシエータ ターゲットの構成

デバイス エイリアスまたは pWWN を使用することによって、発信側ターゲットを設定できます。次のオプション パラメータを 1 つまたは複数指定することもできます（任意）。

- セカンダリ pWWN
- セカンダリ デバイス エイリアス
- LUN マッピング
- IQN
- VSAN ID

さらに、auto-zoning を無効にできます。発信側ターゲットに IQN を設定する場合は、その名前を使用して発信側ターゲットを特定する必要があります。そうしないと、発信側ターゲットに一意の IQN が生成されます。

iSLB イニシエータ ターゲットを構成するには、次のステップを実行します。

始める前に

ターゲットがオンラインの場合、VSAN ID は省略可能です。ターゲットがオンラインではない場合、VSAN ID は必須です。

手順

ステップ 1 IPv4 アドレスを使用して iSLB イニシエータを構成し、iSLB イニシエータ構成サブモードを開始します

```
switch# config terminal
switch(config)# islb initiator ip-address 10.1.1.3
switch(config-islb-init)#
```

ステップ 2 自動ゾーニングが有効になった状態（デフォルト）で pWWN を使用して、iSLB イニシエータターゲットを構成します。

```
switch(config-iscsi-islb-init)# target pwwn 26:00:01:02:03:04:05:06
```

ステップ 3 自動ゾーニングが無効になっている pWWN を使用して、iSLB イニシエータターゲットを構成します。

```
switch(config-iscsi-islb-init)# target pwwn 26:00:01:02:03:04:05:06 no-zone
```

ステップ 4 自動ゾーニングが有効になった状態（デフォルト）でデバイスエイリアスを使用して、iSLBイニシエータ ターゲットを構成します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias
```

ステップ 5 デバイス エイリアスとオプションの LUN マッピングを使用して iSLB イニシエータ ターゲットを構成します。CLI は、**0x** プレフィックスが含まれているかどうかに関係なく、LUN ID の値を 16 進値として解釈します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias fc-lun 0x1234 iscsi-lun 0x2345
```

ステップ 6 デバイス エイリアスとオプションの IQN を使用して iSLB イニシエータ ターゲットを構成します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias iqn-name
iqn.1987-01.com.cisco.initiator
```

ステップ 7 デバイス エイリアスとオプションのセカンダリ デバイス エイリアスを使用して、iSLB イニシエータ ターゲットを構成します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias sec-device-alias SecondaryAlias
```

ステップ 8 デバイス エイリアスとオプションのセカンダリ pWWN を使用して、iSLB イニシエータ ターゲットを構成します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias sec-pwwn 26:01:02:03:04:05:06:07
```

ステップ 9 デバイス エイリアスと VSAN 識別子を使用して iSLB イニシエータ ターゲットを構成します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias vsan 10
```

ステップ 10 iSLB イニシエータ ターゲットを削除します。

```
switch(config-iscsi-init)# no target pwwn 26:00:01:02:03:04:05:06
```

iSLB発信側および発信側ターゲット用のゾーンの設定およびアクティブ化

iSLB 発信側および発信側ターゲットを追加するゾーンの名前を設定できます。ゾーン名を指定しなかった場合、IPS マネージャによってダイナミックに作成されます。iSLB ゾーン セットに関する次の考慮事項があります。

- 発信側ターゲットが設定された発信側の自動ゾーン分割は、デフォルトでイネーブルになります。
- VSAN で自動ゾーンを作成するには、その VSAN でゾーン セットをアクティブにする必要があります。
- 別のゾーン セットがアクティブ化の途中にある場合、またはゾーン分割データベースがロックされている場合、iSLB ゾーン セットのアクティブ化に失敗する可能性があります。失敗した場合は、iSLB ゾーン セットのアクティブ化を再試行してください。この問題を回避するために、ゾーン分割関連の処理（標準ゾーン、IVR ゾーン、または iSLB ゾーン）は、一度に 1 つだけ実行してください。
- 自動ゾーンが作成されるのは、ゾーン セットがアクティブで、そのゾーン セットに少なくとも 1 つ変更があった場合です。自動ゾーンだけが変化した場合、アクティブ化は無効です。

iSLB イニシエータのオプションの自動ゾーン名を構成し、ゾーン セットをアクティブ化するには、次のステップを実行します。

始める前に

同じファブリック内で IVR と iSLB がイネーブルになっている場合は、ファブリック内の少なくとも 1 つのスイッチで両方の機能をイネーブルにする必要があります。ゾーン分割関連の設定またはアクティブ化の操作（通常のゾーン、IVR ゾーン、または iSLB ゾーンに対して）は、このスイッチ上で実行する必要があります。そうしなければ、ファブリック内のトラフィックが中断される可能性があります。

手順

ステップ 1 IPv4 アドレスを使用して iSLB イニシエータを構成し、iSLB イニシエータ構成サブモードを開始します

```
switch# config terminal
switch(config)# islb initiator ip-address 10.1.1.3
switch(config-islb-init)#
```

ステップ 2 （オプション）イニシエータとイニシエータターゲットを追加するゾーン名を指定します。

```
switch(config-islb-init)# zonename IslbZone
```

ステップ 3 （デフォルト）イニシエータとイニシエータ ターゲットをゾーンから削除し、動的に作成されたゾーンに追加します。

```
switch(config-islb-init)# no zonename IslbZone
```

ステップ 4 コンフィギュレーション モードに戻ります。

```
switch(config-islb-init)# exit
```

ステップ 5 ゾーン分割が有効になっている iSLB イニシエータおよびイニシエータ ターゲットのゾーン分割をアクティブにし、ゾーン名が構成されていない場合は自動ゾーンを作成します。

CFS が有効な場合は、このステップは不要です。CFS は、設定変更が確定されると、自動的にゾーンをアクティブにします。

```
switch(config)# islb zoneset activate
```

iSLB ゾーン分割設定の確認

次に、動的に生成されたゾーン名を使用した場合の **show zoneset active** コマンドの出力例を示します。

```
switch# show zoneset active
zoneset name zoneset-1 vsan 1
zone name ips_zone_5d9603bcff68008a6fc5862a6670ca09 vsan 1
* fcid 0x010009 [ip-address 10.1.1.3]
pwwn 22:00:00:04:cf:75:28:4d
pwwn 22:00:00:04:cf:75:ed:53
pwwn 22:00:00:04:cf:75:21:d5
pwwn 22:00:00:04:cf:75:ee:59
.
.
.
```

次に、設定されたゾーン名 IslbZone を使用した場合の **show zoneset active** コマンドの出力例を示します。

```
switch# show zoneset active
zoneset name zoneset-1 vsan 1
zone name ips_zone_IslbZone vsan 1
ip-address 10.1.1.3
pwwn 22:00:00:04:cf:75:28:4d
pwwn 22:00:00:04:cf:75:ed:53
pwwn 22:00:00:04:cf:75:21:d5
pwwn 22:00:00:04:cf:75:ee:59
.
.
.
```

iSLB セッション認証の設定

IPS ポートを搭載したファイバ チャネル モジュールおよび MPS-14/2 モジュールは、ストレージへのアクセスを要求する iSLB ホストを認証する iSLB 認証メカニズムをサポートします。デフォルトでは、IPS ポートを搭載したファイバ チャネル モジュールおよび MPS-14/2 モジュールは、iSCSI 発信側に関する CHAP または None 認証を許可します。認証を必ず使用する場合は、CHAP 認証だけが許可されるようにスイッチを設定する必要があります。

CHAP ユーザー名またはシークレットの検証には、Cisco MDS AAA インフラストラクチャでサポートおよび許可されている方法を使用できます（詳細については、『Cisco Fabric Manager セキュリティ構成ガイド』『Cisco MDS 9000 Family NX-OS セキュリティ構成ガイド』を参照してください）。AAA 認証は、RADIUS、TACACS+、またはローカル認証デバイスをサポートします。

（注） iSLB セッション認証の指定方法は、iSCSI の場合と同じです。「iSCSI セッション 認証」を参照してください。

iSLB イニシエータ認証の制限

iSLB イニシエータはデフォルトで、IPS ポートを搭載したファイバ チャネルまたは MPS-14/2 モジュールに対する自身の認証用に、RADIUS またはローカル AAA データベースの任意のユーザー名を使用できます（CHAP ユーザー名は iSLB 発信側名と無関係です）。IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールは、スイッチから送信された CHAP チャレンジに有効な応答があった場合にかぎり、発信側にログインを許可します。ただし、CHAP ユーザー名およびパスワードが信用できないものであると、問題が生じる可能性があります。

イニシエータが CHAP 認証に特定のユーザー名を使用するように制限するには、次のステップを実行します。

手順

ステップ 1 イニシエータ ノードの IQN を使用して iSLB イニシエータを構成し、iSLB イニシエータ構成サブモードを開始します。

```
switch# config terminal
switch(config)# islb initiator name iqn.1987-02.com.cisco.init
switch(config-islb-init)#
```

ステップ 2 イニシエータ `iqn.1987-02.com.cisco.init` を、CHAP ユーザー名として `user1` を使用する認証だけに制限します。

（注）
ローカル AAA データベースまたは RADIUS サーバーで user1 を iSCSI ユーザーとして必ず定義してください。

```
switch(config-islb-init)#
switch(config-islb-init)# username user1
```

相互 CHAP 認証

iSLB イニシエータに関する IPS ポートを搭載したファイバ チャネル モジュールおよび MPS-14/2 モジュールの認証に加え、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールは、iSCSI ログイン フェーズで Cisco MDS スイッチのイニシエータ ターゲットを認証する、iSLB イニシエータのメカニズムもサポートします。この認証には、ユーザー側で iSLB 発信側に提示するスイッチ用のユーザー名およびパスワードを設定する必要があります。

提供されたパスワードを使用して、発信側がIPSポートに送信するCHAPチャレンジへのCHAP応答が計算されます。

スイッチが発信側に対する自身の認証に使用する発信側単位のユーザー名およびパスワードを設定するには、次の手順を実行します。

手順

ステップ 1 イニシエータ ノードの名前を使用して iSLB イニシエータを構成し、iSLB イニシエータ構成サブモードを開始します。

```
switch# config terminal
switch(config)# islb initiator name iqn.1987-02.com.cisco.initiator
switch(config-islb-init)#
```

ステップ 2 クリア テキスト（デフォルト）で指定されたパスワード（dcba12LKJ）とともに、スイッチのユーザ アカウント（testuser）を構成します。パスワードは 128 文字に制限されています。

```
switch(config-islb-init)# mutual-chap username testuser password dcba12LKJ
```

ステップ 3 7 (!@*asdsfsdfjh!@df) で指定された暗号化パスワードとともに、スイッチのユーザーアカウント（testuser）を構成します。

```
switch(config-islb-init)# mutual-chap username testuser password 7!@*asdsfsdfjh!@df
```

ステップ 4 スイッチ認証構成を削除します。

```
switch(config-iscsi-init)# no mutual-chap username testuser
```

iSLB ゾーン認証設定の確認

グローバル構成を表示するには、**show running-config** および **show iscsi global** コマンドを使用します。イニシエータ固有の設定を表示するには、 **show running-config** コマンドと **show islb initiator configured** コマンドを使用します。

iSLB ユーザー名と相互 CHAP 構成を確認するには、**show islb initiator configured** コマンドを使用します。

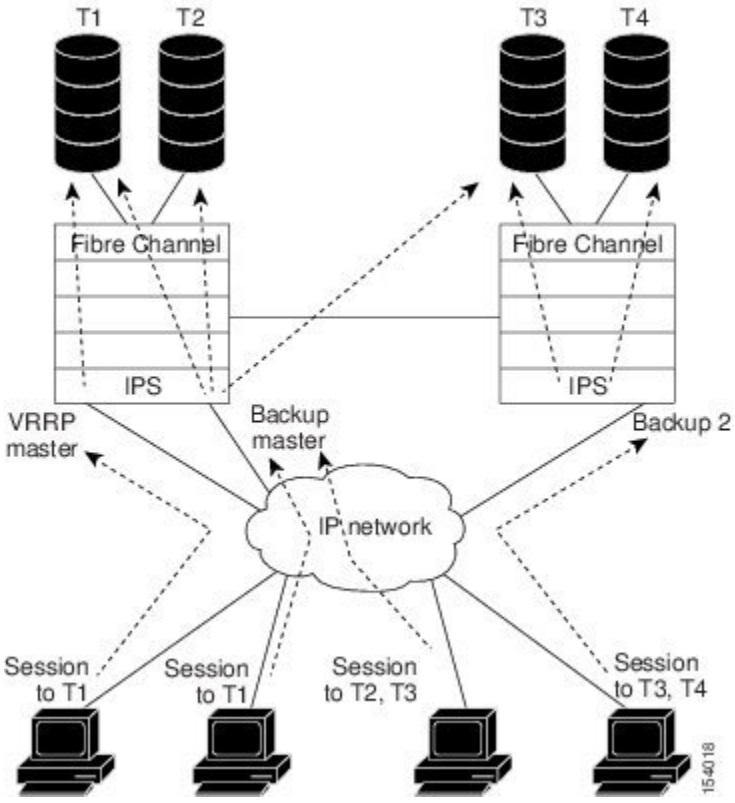
```
switch# show islb initiator configured
iSCSI Node name is 10.1.1.3
Member of vsans: 3
User Name for login authentication: user1
User Name for Mutual CHAP: testuser
Load Balance Metric: 1000 Number of Initiator Targets: 1
Number of Initiator Targets: 1
Initiator Target: iqn.1987-05.com.cisco:05.ips-hac4
Port WWN 50:06:04:82:ca:e1:26:8d
Zoning Enabled
No. of LU mapping: 3
iSCSI LUN: 0x0001, FC LUN: 0x0001
iSCSI LUN: 0x0002, FC LUN: 0x0002
iSCSI LUN: 0x0003, FC LUN: 0x0003
```

VRRP を使用するロード バランシング

iSLB に仮想ルータ冗長プロトコル（VRRP）ロードバランシングを設定できます。ホストは、ポータル アドレスとして VRRP アドレスを指定して設定されています。VRRP マスター ポートは発信側から最初の iSCSI セッションを受信すると、そのホスト用のバックアップ ポートを割り当てます。マスター ポートの障害時に回復が必要な場合は、CFS によってこの情報がすべてのスイッチで同期化されます。発信側には、一時リダイレクト iSCSI ログイン応答が与えられます。ホストはその後、対応する物理 IP アドレスでバックアップ ポートにログインします。VRRP グループ内で、ロード バランシングがイネーブルに設定されているすべての iSCSI インターフェイスに、同じインターフェイス VSAN、認証、プロキシ イニシエータ モード、および転送モードを設定する必要があります。

iSLB に仮想ルータ冗長プロトコル（VRRP）ロードバランシングを設定できます。次の図に、iSLB を使用したロード バランシングの例を示します。

図 *33 : iSLB* 発信側のロード バランシング例



ホストは、ポータルアドレスとしてVRRPアドレスを指定して設定されています。VRRPマスターポートは発信側から最初のiSCSIセッションを受信すると、そのホスト用のバックアップポートを割り当てます。マスター ポートの障害時に回復が必要な場合は、CFS によってこの情報がすべてのスイッチで同期化されます。発信側には、一時リダイレクト iSCSI ログイン応答が与えられます。ホストはその後、対応する物理 IP アドレスでバックアップ ポートにログインします。バックアップ ポートが停止した場合、ホストはマスター ポートに戻ります。マ

スター ポートは CFS によって、バックアップ ポートが停止したことを認識し、ホストを別のバックアップ ポートにリダイレクトします。

（注） IPS ポートを搭載したファイバ チャネル モジュールとイーサネット スイッチ間にイーサネット ポート チャネルが構成されている場合は、VRRP によるロード バランシングを正常に動作させるために、イーサネット スイッチ上のロード バランシング ポリシーをポート番号ではなく、送信元/宛先 IP アドレスだけに基づいたものにする必要があります。

（注） 発信側をマスター インターフェイスの物理 IP アドレスにリダイレクトすることもできます。

iSLB VRRP ロード バランシングは、セッション数ではなく iSLB 発信側の数に基づいて実行されます。ターゲットの多い iSLB 発信側は（セッション数が結果的に多くなるので）、他の iSLB 発信側より大きいロード メトリックを指定して設定する必要があります。たとえば、ターゲットの多い iSLB 発信側のロード メトリックをデフォルト値の 1000 から 3000 に引き上げることができます。

iSLB 対応として設定されたギガビット イーサネット インターフェイスが所属できる VRRP グループは 1 つだけです。これは、リダイレクトされたセッションが VRRP IP アドレスまたはグループに関する情報を伝達しないからです。この制限によって、スレーブ バックアップ ポートは所属先の VRRP グループを一意のものとして識別できます。

iSCSI インターフェイス パラメータの変更およびロード バランシングへの影響

VRRP グループ内で、ロード バランシングがイネーブルに設定されているすべての iSCSI インターフェイスに、同じインターフェイス VSAN、認証、プロキシ イニシエータ モード、および転送モードを設定する必要があります。VRRP グループ内の iSCSI インターフェイスで、これらのパラメータのいずれかを変更しなければならない場合は、一度に 1 つずつ、インターフェイスを処理する必要があります。VRRP グループの一部のインターフェイスでパラメータが変更され、他のインターフェイスでは変更されていない移行期の間、マスター ポートは新しい発信側をリダイレクトする代わりにローカルで処理します。

VRRP グループに含まれる iSCSI インターフェイスの VSAN、プロキシ発信側、認証、および転送モードを変更すると、セッションが繰り返し停止することがあります。

ギガビット イーサネット インターフェイスを選択する VRRP ロード バランシング アルゴリズム

発信側から iSCSI セッション要求を受信した VRRP マスターは、VRRP グループに含まれるインターフェイスの 1 つに対して既存のマッピングがあるかどうかを最初に調べます。該当するマッピングがある場合、VRRP マスターは発信側をそのインターフェイスにリダイレクトします。該当するマッピングがない場合、VRRP マスターは負荷が最小のインターフェイスを選択

し、イニシエータの iSLB メトリック（重み）を使用して、選択したインターフェイスの負荷を更新します。

（注） VRRPマスターインターフェイスは特別に扱い、他のインターフェイスに比べて小さい負荷で済むようにする必要があります。これは、セッションごとにマスターインターフェイスがリダイレクト作業を実行するためです。新しいイニシエータは、他のすべてのインターフェイスで次の条件が満たされている場合のみ、マスターインターフェイスに割り当てられます。 VRRP backup interface load > [2 * VRRP master interface load + 1]

この次の例は、次の構成に基づいています。

- GigabitEthernet2/1.441 は Switch1 の VRRP マスター インターフェイスです。
- GigabitEthernet2/2.441 は Switch1 の VRRP バックアップ インターフェイスです。
- GigabitEthernet1/1.441 は Switch2 の VRRP バックアップ インターフェイスです。
- GigabitEthernet1/2.441 は Switch2 の VRRP バックアップ インターフェイスです。

デフォルト メトリックを使用した負荷分散

次の出力例は、デフォルトのロードメトリック値を使用した3台のイニシエータへの初期負荷分散を示しています。

```
switch# show islb vrrp summary
.
.
.
--------------------------------------------------------------------------------
VR Id VRRP IP Switch WWN Ifindex Load
--------------------------------------------------------------------------------
M 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441 0
1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441 1000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441 1000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441 1000
-- Initiator To Interface Assignment --
--------------------------------------------------------------------------------
Initiator VR Id VRRP IP Switch WWN Ifindex
--------------------------------------------------------------------------------
iqn.cisco.test-linux.init0 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441
iqn.cisco.test-linux.init1 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441
iqn.cisco.test-linux.init 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441
```

次の出力例は、4 台の発信側の負荷分散を示しています。マスター インターフェイスのインターフェイス ロード メトリック値が 0 から 1000 に変更されています。

```
switch# show islb vrrp summary
.
.
.
--------------------------------------------------------------------------------
VVR Id VRRP IP Switch WWN Ifindex Load
--------------------------------------------------------------------------------
M 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441 1000
1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441 1000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441 1000
```

```
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441 1000
-- Initiator To Interface Assignment --
--------------------------------------------------------------------------------
Initiator VR Id VRRP IP Switch WWN Ifindex
--------------------------------------------------------------------------------
iqn.cisco.test-linux.init0 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441
iqn.cisco.test-linux.init1 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441
iqn.cisco.test-linux.init2 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441
iqn.cisco.test-linux.init3 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441
```

次の出力例は、9台のイニシエータの負荷分散を示しています。バックアップ インターフェイスのインターフェイス ロード メトリック値が変更されています。

```
switch# show islb vrrp summary
.
.
.
--------------------------------------------------------------------------------
VVR Id VRRP IP Switch WWN Ifindex Load
--------------------------------------------------------------------------------
M 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441 1000
1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441 3000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441 3000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441 2000
-- Initiator To Interface Assignment --
--------------------------------------------------------------------------------
Initiator VR Id VRRP IP Switch WWN Ifindex
--------------------------------------------------------------------------------
iqn.cisco.test-linux.init0 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441
iqn.cisco.test-linux.init1 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441
iqn.cisco.test-linux.init2 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441
iqn.cisco.test-linux.init3 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441
iqn.cisco.test-linux.init4 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441
iqn.cisco.test-linux.init5 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441
iqn.cisco.test-linux.init6 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441
iqn.cisco.test-linux.init7 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441
iqn.cisco.test-linux.init8 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441
```

1 台のイニシエータでメトリックが 3000 に設定された負荷分散

次の出力例は、1台のイニシエータでロードメトリックが3000に設定され、残りのイニシエータでデフォルトのメトリック値が設定されている3台のイニシエータの初期負荷分散を示します。

```
switch# show islb vrrp summary
.
.
.
--------------------------------------------------------------------------------
VVR Id VRRP IP Switch WWN Ifindex Load
--------------------------------------------------------------------------------
M 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441 0
1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441 1000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441 3000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441 1000
-- Initiator To Interface Assignment --
--------------------------------------------------------------------------------
Initiator VR Id VRRP IP Switch WWN Ifindex
--------------------------------------------------------------------------------
iqn.cisco.test-linux.init0 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441
iqn.cisco.test-linux.init1 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441
iqn.cisco.test-linux.init2 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441
```

次の出力例は、4 台の発信側の負荷分散を示しています。マスター インターフェイスのインターフェイス ロード メトリック値が 0 から 1000 に変更されています。

```
switch# show islb vrrp summary
.
.
.
--------------------------------------------------------------------------------
VVR Id VRRP IP Switch WWN Ifindex Load
--------------------------------------------------------------------------------
M 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441 1000
1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441 3000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441 1000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441 1000
-- Initiator To Interface Assignment --
--------------------------------------------------------------------------------
Initiator VR Id VRRP IP Switch WWN Ifindex
--------------------------------------------------------------------------------
iqn.cisco.test-linux.init0 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441
iqn.cisco.test-linux.init1 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441
iqn.cisco.test-linux.init2 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441
iqn.cisco.test-linux.init3 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441
```

次の出力例は、9台のイニシエータの負荷分散を示しています。バックアップインターフェイスのインターフェイス ロード メトリック値が変更されています。

```
switch# show islb vrrp summary
.
.
.
--------------------------------------------------------------------------------
VVR Id VRRP IP Switch WWN Ifindex Load
--------------------------------------------------------------------------------
M 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441 2000
1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441 3000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441 3000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441 3000
-- Initiator To Interface Assignment --
--------------------------------------------------------------------------------
Initiator VR Id VRRP IP Switch WWN Ifindex
--------------------------------------------------------------------------------
iqn.cisco.test-linux.init0 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441
iqn.cisco.test-linux.init1 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441
iqn.cisco.test-linux.init2 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441
iqn.cisco.test-linux.init3 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441
iqn.cisco.test-linux.init4 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441
iqn.cisco.test-linux.init5 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441
iqn.cisco.test-linux.init6 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441
iqn.cisco.test-linux.init7 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441
iqn.cisco.test-linux.init8 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441
```

VRRP を使用したロード バランシングの構成

iSLB 用の VRRP を設定する前に、IP ネットワークに接続するスイッチのギガビット イーサネットインターフェイス上で、VRRPを設定しておく必要があります。ギガビットイーサネットインターフェイス上で VRRP を構成する方法については、「仮想 ルータの冗長性プロトコル」を参照してください。

ロード バランシング用の VRRP の有効化

iSLB の VRRP を有効または無効にするには、次のステップを実行します。

手順

ステップ 1 IPv4 VR グループ 10 用に iSLB VRRP をイネーブルにします。

```
switch# config terminal
switch(config)# islb vrrp 10 load-balance
```

ステップ 2 IPv4 VR グループ 10 用に iSLB VRRP をディセーブルにします。

```
switch(config)# no islb vrrp 10 load-balance
```

ステップ 3 IPv6 VR グループ 20 用に iSLB VRRP をイネーブルにします。

```
switch(config)# islb vrrp ipv6 20 load-balance
```

ステップ 4 IPv6 VR グループ 20 用に iSLB VRRP をディセーブルにします。

```
switch(config)# no islb vrrp ipv6 20 load-balance
```

iSLB VRRP ロード バランシング構成の確認

IPv4 用の iSLB VRRP ロード バランシング構成を確認するには、**show vrrp vr** コマンドを使用します。

```
switch# show vrrp vr 1
Interface VR IpVersion Pri Time Pre State VR IP addr
---------------------------------------------------------------------------
GigE1/5 1 IPv4 100 1 s master 10.10.10.1
GigE1/6 1 IPv4 100 1 s master 10.10.10.1
```

IPv6 用の iSLB VRRP ロード バランシング構成を確認するには、**show vrrp ipv6 vr** コマンドを使用します。

```
switch# show vrrp ipv6 vr 1
Interface VR IpVersion Pri Time Pre State VR IP addr
---------------------------------------------------------------------
GigE6/2 1 IPv6 100 100cs master 5000:1::100
PortCh 4 1 IPv6 100 100cs master 5000:1::100
```

iSLB VRRP 情報の表示

VRRP ロード バランシング情報を表示するには、**show islb vrrp summary vr** コマンドを使用します。

```
switch# show islb vrrp summary vr 30

-- Groups For Load Balance --
-------------------------------------------------------------------------------------------
VR Id VRRP Address Type Configured Status
-------------------------------------------------------------------------------------------
30 IPv4 Enabled
```

```
-- Interfaces For Load Balance --
------------------------------------------------------------------------------------------
VR Id VRRP IP Switch WWN Ifindex Load
------------------------------------------------------------------------------------------
30 192.168.30.40 20:00:00:0d:ec:02:cb:00 GigabitEthernet3/1 2000
30 192.168.30.40 20:00:00:0d:ec:02:cb:00 GigabitEthernet3/2 2000
30 192.168.30.40 20:00:00:0d:ec:0c:6b:c0 GigabitEthernet4/1 2000
M 30 192.168.30.40 20:00:00:0d:ec:0c:6b:c0 GigabitEthernet4/2 1000
```

CFS を使用した iSLB 構成の配信

iSLB 発信側および MDS スイッチ上の発信側ターゲットに設定を配信できます。この機能を使用すると、1 台の MDS スイッチのコンソールから、ファブリック全体で iSLB の設定を同期化できます。iSCSI 発信側アイドル タイムアウト、グローバル認証、および iSCSI ダイナミック イニシエータ モード パラメータも配信されます。CFS 配信は、デフォルトではディセーブルになっています。

MDS スイッチにおける iSLB 発信側および発信側ターゲットの設定は、Cisco Fabric Services（CFS）を使用して配信できます。この機能を使用すると、1 台の MDS スイッチのコンソールから、ファブリック全体で iSLB の設定を同期化できます。iSCSI 発信側アイドル タイムアウト、iSCSI ダイナミック イニシエータ モード、およびグローバル認証パラメータも配信されます。CFS 配信はデフォルトで無効になっています（詳細については『Cisco Fabric Manager システム管理構成ガイド』『Cisco MDS 9000 ファミリ NX-OS システム管理構成ガイド』を参照してください）。

配信をイネーブルにすると、最初の設定によって暗黙セッションが開始されます。それ以降に入力されたすべてのサーバー設定変更は、一時データベースに保存され、データベースを明示的にコミットしたときに、ファブリック内のすべてのスイッチ（送信元スイッチを含む）に適用されます。

iSLB に対して CFS がイネーブルの場合は、最初の iSLB 設定処理によって CFS セッションが開始され、ファブリック内の iSLB コンフィギュレーションがロックされます。設定変更は、保留中の設定データベースに適用されます。ファブリックに対して変更を行うと、保留中の設定がファブリック内のすべてのスイッチに配信されます。その後、スイッチごとにコンフィギュレーションが検証されます。このチェックによって、次の保証が得られます。

- iSLB 発信側に割り当てられた VSAN は、すべてのスイッチ上で設定されている。
- iSLB 発信側に設定されたスタティック WWN は一意であり、すべてのスイッチで使用できる。
- iSLB 発信側ノード名は、すべてのスイッチ上の iSCSI 発信側と衝突しない。

チェックが正常に完了すると、すべてのスイッチが保留中の設定を実行コンフィギュレーションにコミットします。チェックが失敗した場合は、コミット全体が失敗します。

（注） iSLB が全面的にサポートされるのは、CFS がイネーブルの場合だけです。CFS モードを有効にしないで iSLB 自動ゾーン分割を使用すると、ゾーン セットをアクティブにしたときに、トラフィックが中断することがあります。

CFS は非 iSLB 発信側設定を配信しません。また、ファイバ チャネル ターゲット設定をインポートしません。

非 iSLB 仮想ターゲットは引き続き、アドバタイズされたインターフェイス オプションをサポートします。

（注） 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。

CFS を使用した iSLB 構成の配信

この項の内容は、次のとおりです。

iSLB 構成配信の有効化

CFS による iSLB 設定の配信を有効にするには、次のステップを実行します。

手順

ステップ 1 構成モードに入ります。

```
switch# config terminal
```

ステップ 2 iSLB 設定の配信をイネーブルにします。

```
switch(config)# islb distribute
```

ステップ 3 iSLB 設定の配信をディセーブル（デフォルト）にします。

```
switch(config)# no islb distribute
```

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。ファブリックをロックすると、次の条件が適用されます。

- 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。これ以後の変更は保留設定に対して行われ、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）に変更をコミットするか、または変更を廃棄するまで、保留設定にとどまります。

（注） iSLB CFS セッションがアクティブな場合は、iSCSI の設定変更は認められません。

ファブリックへの変更のコミット

保留中の iSLB 設定変更をアクティブ コンフィギュレーションおよびファブリック内のその他の MDS スイッチに適用するには、その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、コミットが正常に完了した時点で、ファブリック全体の MDS スイッチでアクティブ コンフィギュレーションに設定変更が適用されます。さらに、自動ゾーンがアクティブになり、ファブリックのロックが解除されます。

ファブリック内の他の MDS スイッチに iSLB の設定変更をコミットし、iSLB 自動ゾーンをアクティブにして、ファブリックのロックを解除するには、次の手順を実行します。

手順

ステップ 1 構成モードに入ります。

```
switch# config terminal
```

ステップ 2 iSLB 構成の配布をコミットし、iSLB 自動ゾーンをアクティブにして、ファブリック ロックをリリースします。

```
switch(config)# islb commit
```

保留中の変更の廃棄

いつでも iSLB コンフィギュレーションに対する保留中の変更を廃棄し、ファブリックのロックを解除できます。このアクションによって、ファブリック内のスイッチのアクティブ コンフィギュレーションが影響を受けることはありません。

保留中の iSLB の構成変更を廃棄し、ファブリックのロックを解除するには、次のステップを実行します。

手順

ステップ 1 構成モードに入ります。

```
switch# config terminal
```

ステップ 2 iSLB 設定の配信をコミットします。

```
switch(config)# islb abort
```

ファブリックのロックのクリア

ユーザーが iSLB の設定作業を実行し、変更をコミットまたは廃棄することによってロックを解除しなかった場合は、管理者がファブリック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。

始める前に

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。

手順

ファブリック ロックを解除するには、管理者権限を持つログイン ID を使用して EXEC モードで **clear islb session**コマンドを発行します。

```
switch# clear islb session
```

CFS マージ プロセス

2 つのファブリックでマージする場合、CFS は両方のファブリックから iSLB のコンフィギュレーションをマージしようとします。一方のファブリックの指定スイッチ（上位スイッチ）が自身の iSLB 構成を他方のファブリックの指定スイッチ（下位スイッチ）に送信します。下位スイッチは自身の実行コンフィギュレーションと受信したコンフィギュレーションを比較し、矛盾の有無を調べます。矛盾が見つからなかった場合は、2つのコンフィギュレーションをマージして、両方のファブリックのすべてのスイッチに送信します。その後、スイッチごとにコンフィギュレーションが検証されます。このチェックによって、次の保証が得られます。

- iSLB 発信側に割り当てられた VSAN は、すべてのスイッチ上で設定されている。
- iSLB 発信側に設定されたスタティック WWN は一意であり、すべてのスイッチで使用できる。
- iSLB 発信側ノード名は、すべてのスイッチ上の iSCSI 発信側と衝突しない。

このチェックが正常に完了すると、下位スイッチはすべてのスイッチに、マージされた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コミットするように指示します。チェックに失敗した場合は、マージが失敗します。

show islb merge status コマンドは、失敗の正確な理由を表示します。マージの失敗後に最初に正常終了するコミット要求により、ファブリックはマージ失敗状態から解放されます。

保留中の iSLB 設定変更の表示

保留中の構成変更は **show islb pending** コマンドを使用して表示できます。

```
switch# show islb pending
iscsi initiator idle-timeout 10
islb initiator ip-address 10.1.1.1
static pWWN 23:01:00:0c:85:90:3e:82
static pWWN 23:06:00:0c:85:90:3e:82
username test1
islb initiator ip-address 10.1.1.2
static nWWN 23:02:00:0c:85:90:3e:82
```

保留中の構成と現在の構成の違いは、 **show islb pending-diff** コマンドを使用して表示できます。

```
switch# show islb pending-diff
+iscsi initiator idle-timeout 10
islb initiator ip-address 10.1.1.1
+ static pWWN 23:06:00:0c:85:90:3e:82
+islb initiator ip-address 10.1.1.2
+ static nWWN 23:02:00:0c:85:90:3e:82
```

iSLB CFS ステータスの表示

iSLB CFS ステータスは、 show islb session statuss コマンドを使用して表示する：

iSLB CFS ステータスは、**show islb session status** コマンドを使用して表示できます。

```
switch# show islb status
iSLB Distribute is enabled
iSLB CFS Session exists
```

iSLB CFS 配信セッション ステータスの表示

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

```
switch# show islb cfs-session status
last action : fabric distribute enable
last action result : success
last action failure cause : success
```

iSLB CFS マージ ステータスの表示

iSLB CFS マージ ステータスは、**show islb merge status** コマンドを使用して表示できます。

```
switch# show islb merge status
Merge Status: Success
```

iSLB CFS マージ ステータスの矛盾

マージで矛盾が生じる場合があります。マージで次の矛盾が生じた場合は、ユーザーの介入が必要です。

- iSCSI グローバル認証または iSCSI 発信側アイドル タイムアウトのパラメータが、2 つのファブリックで同じ設定になっていない。
- 同じ iSLB 発信側の設定が 2 つのファブリックでそれぞれ異なる。
- 一方のファブリックの iSLB 発信側に、他方のファブリックの iSCSI 発信側と同じ名前が与えられている。
- 2 つのファブリックで重複する pWWN/nWWN の設定が見つかった。たとえば、一方のファブリックの iSLB 発信側に設定された pWWN/nWWN が、他方のファブリックの iSCSI 発信側または別の iSLB 発信側に設定されているなどです。
- 一方のファブリックの iSLB 発信側に設定された VSAN が他方のファブリックに存在しない。

マージの矛盾の詳細については、Syslog を調べてください。同じ iSLB 発信側に、衝突しない別の発信側ターゲット セットがある場合は、ユーザーの介入は不要です。マージされたコンフィギュレーションは、すべての発信側ターゲットの和集合です。

iSCSI ハイ アベイラビリティ

iSCSI 設定で使用できるハイ アベイラビリティ機能は、次のとおりです。

透過型ターゲット フェールオーバー

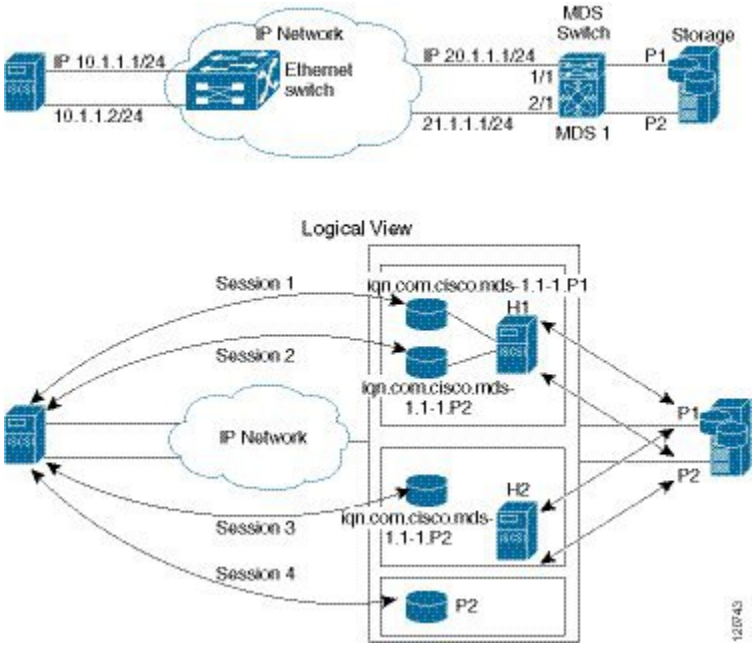
iSCSI 設定で使用できるハイ アベイラビリティ機能は、次のとおりです。

- マルチパス ソフトウェアが稼働しているホストでの iSCSI ハイ アベイラビリティ：このトポロジでは、あらゆるコンポーネントの障害から回復できます。ホストのマルチパス ソフトウェアがストレージにアクセスする別のパスで、ロードバランシングまたはフェールオーバーを処理します。
- マルチパス ソフトウェアのないホストでの iSCSI ハイ アベイラビリティ：マルチパス ソフトウェアのないホストは、同じストレージへの複数のパスについて、情報が得られません。

マルチパス ソフトウェアが稼働しているホストでの iSCSI ハイ アベイラビリティ

以下の図に、マルチパス ソフトウェアが稼働しているホストの iSCSI HA ソリューションに対応する物理および論理トポロジを示します。このシナリオでは、ホストに 4 つの iSCSI セッションがあります。各ホスト NIC から 2 つの IPS ポートへの iSCSI セッションが 2 つあります。

図 *34 :* マルチパス ソフトウェアが稼働しているホスト



各 IPS ポートはストレージの 2 つの同じファイバ チャネル ターゲット ポートをエクスポートしますが、ダイナミック iSCSI ターゲットを使用している場合、iSCSI ターゲット名は異なります。したがって、2 つの IPS ポートで合計 4 つの iSCSI ターゲット デバイスをエクスポートします。この 4 つの iSCSI ターゲットは、ファイバ チャネル ターゲットの同じ 2 つのポートをマッピングします。

iSCSI ホストは NIC-1 を使用して、IPS ポート 1 に接続し、NIC-2 を使用して IPS ポート 2 に接続します。各 IPS ポートは 2 つの iSCSI ターゲットをエクスポートするので、iSCSI ホストは 4 つの iSCSI セッションを作成します。

iSCSI ホストの NIC-1 で障害が発生した場合、セッション 1 および 2 は失敗しますが、セッション 3 および 4 がまだ残っています。

IPS ポート 1 で障害が発生した場合、iSCSI ホストは IPS ポートに接続できないので、セッション 1 および 2 が失敗します。しかし、セッション 3 および 4 はそのまま使用できます。

ストレージのポート 1 に障害が発生すると、IPS ポートはセッション 1 とセッション 3 を終了します（iSCSI 仮想ターゲットの iqn.com.cisco.mds-5.1-2.p1 および iqn-com.cisco.mds-5.1-1.p1 をオフラインの状態にします）。しかし、セッション 2 および 4 はそのまま使用できます。

このトポロジでは、あらゆるコンポーネントの障害から回復できます。ホストのマルチパス ソフトウェアがストレージにアクセスする別のパスで、ロードバランシングまたはフェールオーバーを処理します。

マルチパス ソフトウェアを使用していないホストでの iSCSI HA

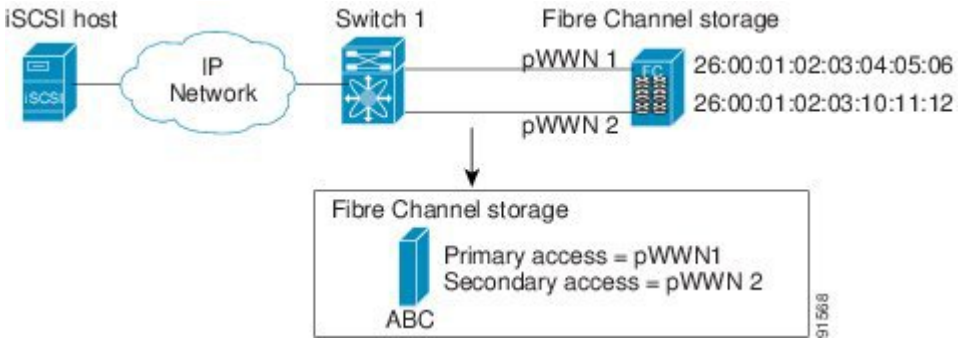
ホストにマルチパス ソフトウェアがない場合、ホストは同じストレージに複数のセッションを実行するので、上記のトポロジは当てはまりません。マルチパス ソフトウェアを使用していないホストは、同じストレージへの複数のパスについて、情報が得られません。

IP ストレージには、このシナリオで HA ソリューションを提供する機能が、他に 2 つあります。

- IPS ポートは VRRP 機能をサポートし（「IPStorage インターフェイスの VRRP の構成」セクションを参照）、IPS ポートのフェールオーバーを提供します。
- IPS には、iSCSI スタティック仮想ターゲットに関して、透過型のファイバ チャネル ターゲット フェールオーバー機能があります。

スタティックにインポートされた iSCSI ターゲットは、別の方法でファイバ チャネル ターゲットにセカンダリ pWWN を提供することもできます。この方法は、複数の冗長ポートで LU を認識できるように物理ファイバ チャネル ターゲットが設定されている場合に使用できます。アクティブ ポートに障害が発生した場合は、セカンダリ ポートがアクティブになり、新しいアクティブ ポートを使用するように iSCSI セッションが切り替わります。

図 *35 : 2* つのファイバ チャネル ポートを介したスタティック ターゲット インポート



上の図では、pWWN1 および pWWN2 の両方にマッピングされた iSCSI 仮想ターゲットを作成して、ファイバ チャネル ターゲットに冗長アクセスを行うことができます。

セカンダリ ポートへのフェールオーバーは、ホストからの iSCSI セッションに影響を与えることなく、IPS ポートから透過的に実行されます。プライマリ ポートに障害が発生した場合は、すべての未処理入出力が終了し、状態確認ステータスになります。フェールオーバーが未完了の間に受信された新規入出力は、ビジー ステータスを受け取ります。

LUN マッピングを使用すると、別のセカンダリ ファイバ チャネル LUN を定義できます（LU 番号が異なる場合）。

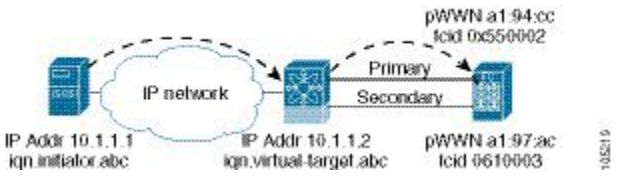
プライマリ ポートが再起動した場合に、IPS ポートがプライマリ ポートに再び切り替わるようにするには、**revert-primary port** オプションをイネーブルにします。このオプションがディセーブル（デフォルト）の場合は、スイッチオーバーのあとにプライマリ ポートを再起動しても、元のセッションは引き続きセカンダリ ポートにとどまり、プライマリ ポートに切り替わりません。ただし、新規セッションはプライマリ ポートを使用します。これは、プライマリおよびセカンダリ ポートが同時に使用される唯一の状況です。

ストレージ ポート フェールオーバー用の LUN トレスパス

スタティックにインポートされた iSCSI ターゲットにハイ アベイラビリティをもたらす以外に、アクティブ ポートで障害が発生した場合に、トレスパス機能を使用して、スタティックにインポートされた iSCSI ターゲットのアクティブ ポートからパッシブ ポートに LU を移動できます。

2 つのファイバ チャネル N ポートで LU を認識できるように設定された物理ファイバ チャネル ターゲットでは、アクティブ ポートに障害が発生した場合、パッシブ ポートが処理を引き継ぎます。一部の物理ファイバ チャネル ターゲットでは、アクティブ ポートからパッシブ ポートに LU を移動する場合に、トレスパス機能を使用する必要があります。スタティックにインポートされた iSCSI ターゲットのセカンダリ pWWN オプション、およびトレスパス機能をイネーブルにする追加オプションは、冗長ポートを持つ物理ファイバ チャネル ターゲットに使用できます。アクティブ ポートに障害が発生すると、パッシブ ポートがアクティブになります。トレスパス機能がイネーブルの場合、Cisco MDS スイッチは、LU を新規アクティブ ポート上に移動するようターゲットに要求を送信します。新しいアクティブ ポートを使用するように iSCSI セッションが切り替わり、移動した LU は新しいアクティブ ポートを介してアクセスされます。

図 *36 :* アクティブ プライマリ ポートを含む仮想ターゲット



スタティック iSCSI 仮想ターゲットの作成

スタティック iSCSI 仮想ターゲットを作成するには、次のステップを実行します。

手順

ステップ 1 iSCSI ターゲット（iqn.1987-02.com.cisco.initiator）を作成します。

```
switch# config terminal
switch(config)# iscsi virtual-target name iqn.1987-02.com.cisco.initiator
```

ステップ 2 この仮想ターゲットのプライマリ ポートを構成します。

```
switch(config-iscsi-tgt)# pwwn 26:00:01:02:03:04:05:06
```

ステップ 3 この仮想ターゲットのプライマリ ポートとセカンダリ ポートを構成します。

```
switch(config-iscsi-tgt)# pwwn 26:00:01:02:03:04:05:06 secondary-pwwn 26:00:01:02:03:10:11:12
```

ステップ 4 LUN マッピングと、セカンダリ ファイバ チャネル ポート上の異なる LUN を使用して、この仮想ターゲットのプライマリ ポートを構成します。

```
switch(config-iscsi-tgt)# pwwn 26:00:01:02:03:04:05:06 fc-lun 0x1 iscsi-lun 0x0 sec-lun 0x3
```

ステップ 5 この仮想ターゲットのプライマリ ポート、セカンダリ ポート、およびLUNマッピング構成を削除します。

```
switch(config-iscsi-tgt)# no pwwn 26:00:01:02:03:04:05:06
```

ステップ 6 プライマリ ポートがアクティブになったときにセッションをすべてプライマリ ポートに戻すように、この仮想ターゲットのセッション フェールオーバー冗長性を構成します。

```
switch(config-iscsi-tgt)# revert-primary-port
```

ステップ 7 既存のセッションに対してセカンダリ ポートを引き続き使用し、新しいセッションに対してプライマリ ポートを使用するようにスイッチを設定します（デフォルト）。

```
switch(config-iscsi-tgt)# no revert-primary-port
```

スタティック iSCSI 仮想ターゲットのトレスパス機能を有効にする

スタティック iSCSI 仮想ターゲットのトレスパス機能を有効にするには、次のステップを実行します。

手順

ステップ 1 iSCSI ターゲット（iqn.1987-02.com.cisco.initiator）を作成します。

```
switch# config terminal
switch(config)# iscsi virtual-target name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-tgt)#
```

ステップ 2 ファイバ チャネル ターゲットに仮想ターゲット ノードをマッピングし、セカンダリ pWWN を構成します。

```
switch(config-iscsi-tgt)# pwwn 50:00:00:a1:94:cc secondary-pwwn 50:00:00:a1:97:ac
```

ステップ 3 トレスパス機能を有効にします。

```
switch(config-iscsi-tgt)# trespass
```

ステップ 4 トレスパス機能を無効にします（デフォルト）。

```
switch(config-iscsi-tgt)# no trespass
```

スタティック iSCSI 仮想ターゲットのトレスパス機能の確認

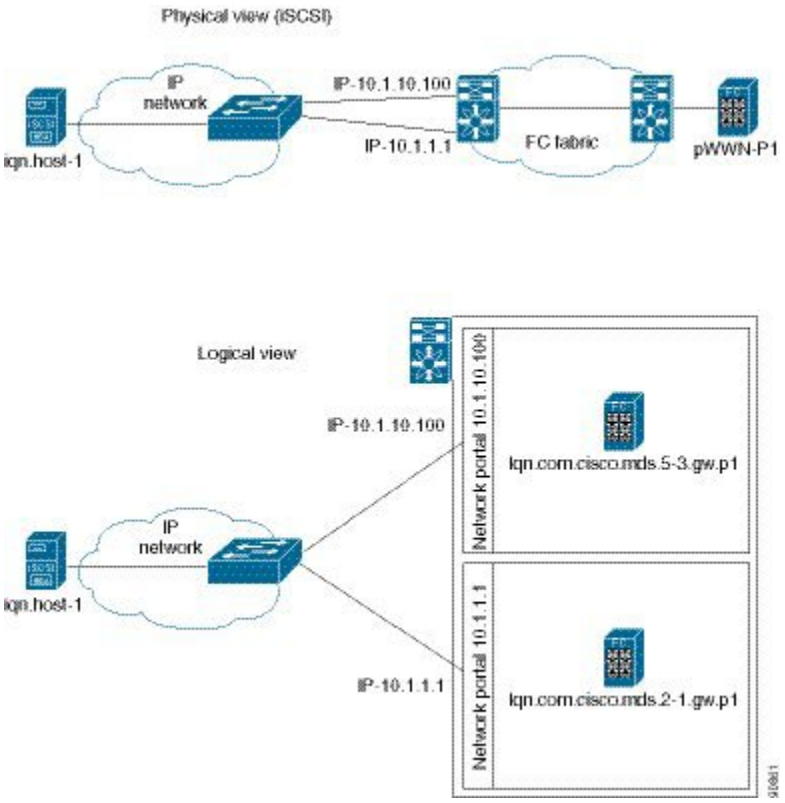
show iscsi virtual-target コマンドを使用して、スタティック iSCSI 仮想ターゲットのトレスパス機能を確認します。

```
switch# show iscsi virtual-target iqn.1987-02.com.cisco.initiator
target: 1987-02.com.cisco.initiator
Port WWN 10:20:10:00:56:00:70:50
Configured node
all initiator permit is disabled
trespass support is enabled
```

同じ IP ネットワークに接続された複数の IPS ポート

次の図では、各 iSCSI ホストは物理ファイバ チャネル ターゲット（異なる名前のターゲット）ごとに 2 つの iSCSI ターゲットを検出します。ホスト上のマルチパス ソフトウェアは、両方のパスでロード バランシングを行います。いずれかのギガビット イーサネット インターフェイスに障害が発生しても、ホストのマルチパス対応ソフトウェアは別のパスを使用できるので、影響を受けません。

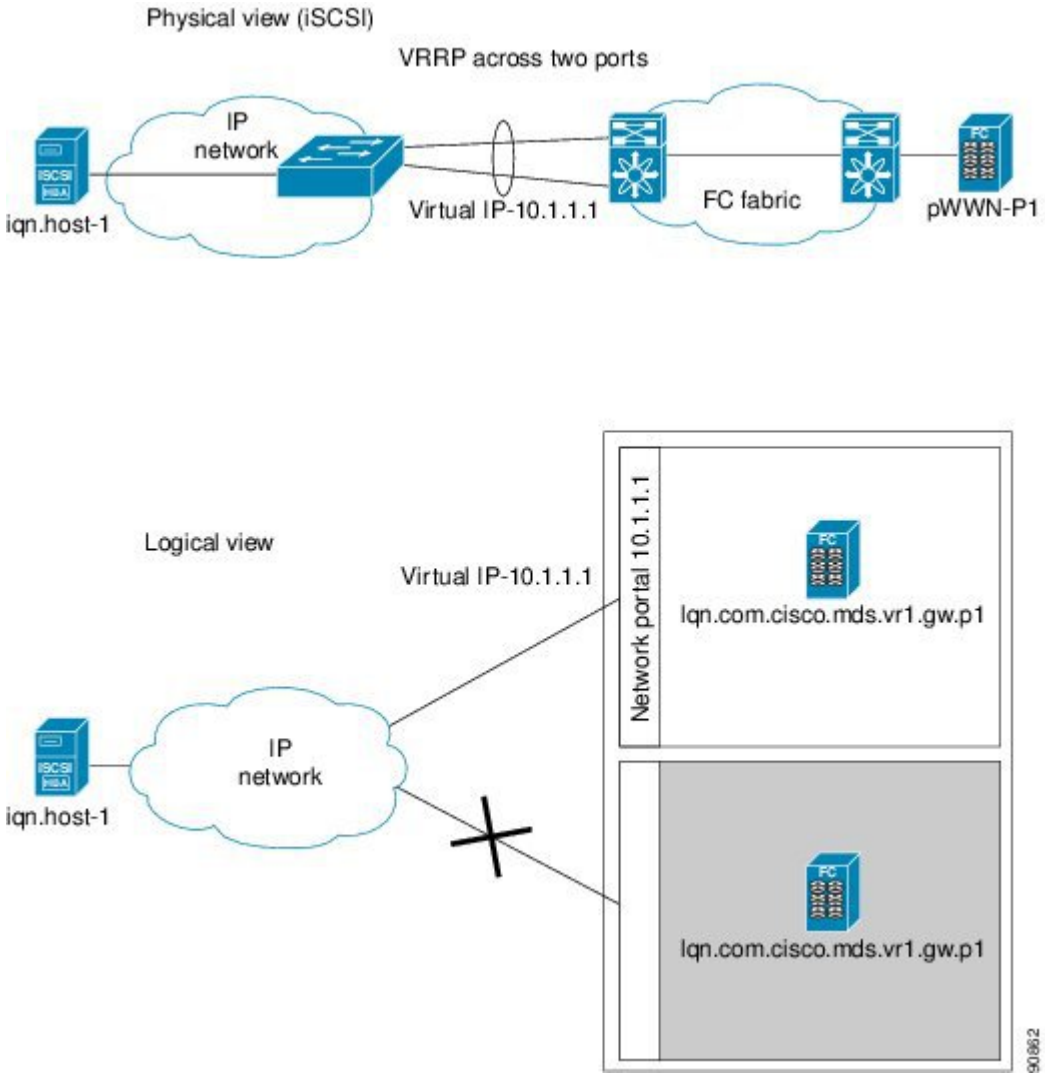
図 *37*：同じ *IP* ネットワーク内の複数のギガビット イーサネット インターフェイス



VRRP ベースのハイ アベイラビリティ

次の図では、各 iSCSI ホストは物理ファイバ チャネル ターゲットごとに 1 つの iSCSI ターゲットを検出します。 VRRP マスターのギガビット イーサネット インターフェイスに障害が発生すると、iSCSI セッションが終了します。別のギガビットイーサネットインターフェイスが新しいマスターとして仮想 IP アドレスを引き継ぐため、ホストはターゲットに再接続し、セッションが起動します。

図 *38 : VRRP* ベースの *iSCSI* ハイ アベイラビリティ



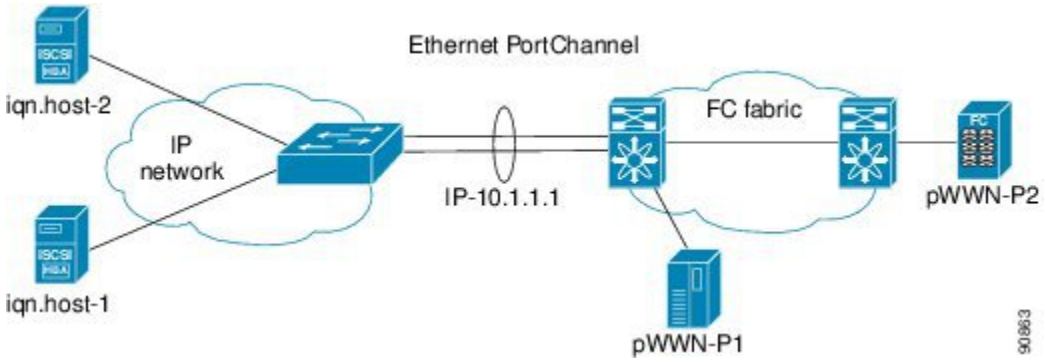
イーサネット ポート チャネル ベースのハイ アベイラビリティ

次の図では、各 iSCSI ホストは物理ファイバ チャネル ターゲットごとに 1 つの iSCSI ターゲットを検出します。 iSCSI ホストから iSCSI 仮想ターゲット（IPS ポート上）への iSCSI セッションでは、2 つの物理インターフェイスのうちの 1 つを使用します（1 つの iSCSI セッションが 1 つの TCP 接続を使用するため）。ギガビット イーサネット インターフェイスに障害が発生すると、IPS ポートを搭載したファイバ チャネル モジュールおよびイーサネット スイッチはすべてのフレームを別のギガビット イーサネット インターフェイスに透過的に転送します。

（注） 1 つの iSCSI リンクのすべての iSCSI データ トラフィックは、1 つの TCP 接続上で伝送されます。したがって、この iSCSI リンクの集約帯域幅は 1 Gbps になります。

（注） IPS ポートを搭載したファイバ チャネル モジュールとイーサネット スイッチ間にイーサネット ポート チャネルが構成されている場合は、VRRP によるロード バランシングを正常に動作させるために、イーサネット スイッチ上のロード バランシング ポリシーをポート番号ではなく、送信元/宛先 IP アドレスだけに基づいたものにする必要があります。

図 *39* : イーサネット ポート チャネル ベースの *iSCSI* ハイ アベイラビリティ



iSCSI 認証設定時の注意事項およびシナリオ

ここでは、iSCSI 認証に関する注意事項および設定要件について説明し、シナリオの例を示します。

（注） この項の内容は、EXEC モード、コンフィギュレーション モード、およびすべてのサブモードを開始、終了する手順を指定するものではありません。いずれかのコマンドを入力する前に、プロンプトを確認する必要があります。

（注） iSLB VRRP グループに属している iSCSI インターフェイスの認証を変更すると、インターフェイスのロードバランシングが影響を受けます。「iSCSI インターフェイス パラメータの変更およびロード バランシングへの影響」セクションを参照してください。

取り上げる認証設定時の注意事項は、次のとおりです。

認証なしの構成

iSCSI 認証を **[none]** に設定して、ネットワークを認証なしに構成します。認証なしを構成するには、次のコマンドを使用します。

```
switch(config)# iscsi authentication none
```

ローカル パスワード データベースを使用した CHAP の構成

ローカル パスワード データベースで CHAP オプションを 使用して認証 を構成するには、次のステップを実行します。

手順

ステップ 1 iSCSI プロトコルにローカル パスワード データベースを使用するように、AAA 認証を設定します。

```
switch(config)# aaa authentication iscsi default local
```

ステップ 2 すべての iSCSI クライアントに CHAP を要求するように、iSCSI 認証方式を設定します。

```
switch(config)# iscsi authentication chap
```

ステップ 3 iSCSI ユーザーのユーザー名およびパスワードを設定します。

```
switch(config)# username iscsi-user password abcd iscsi
```

（注）
iscsi オプションを指定しない場合、iSCSI ユーザーの代わりにユーザー名が Cisco MDS スイッチ ユーザーと見なされます。

ステップ 4 グローバル iSCSI 認証の設定を確認します。

```
switch# show iscsi global
iSCSI Global information Authentication: CHAP <----Verify
Import FC Target: Disabled
.
.
.
```

外部 RADIUS サーバを使用した CHAP の構成

外部 RADIUS サーバで CHAP オプションを使用して認証を構成するステップは、次のとおりです。

始める前に

手順

ステップ 1 RADIUS サーバに対する RADIUS クライアントとしての Cisco MDS スイッチのパスワードを構成します。

```
switch(config)# radius-server key mds-1
```

ステップ 2 次のいずれかを実行して RADIUS サーバーの IP アドレスを設定します。

a) IPv4 アドレスを設定します。

```
switch(config)# radius-server host 10.1.1.10
```

b) IPv6 アドレスを設定します。

```
switch(config)# radius-server host 2001:0DB8:800:200C::417A
```

ステップ 3 次のいずれかを実行して、RADIUS サーバー グループ IP アドレスを設定します。

a) IPv4 アドレスを設定します。

```
switch(config)# aaa group server radius iscsi-radius-group
switch(config-radius)# server 10.1.1.1
```

b) IPv6 アドレスを設定します。

```
switch(config)# aaa group server radius iscsi-radius-group
switch(config-radius)# server 001:0DB8:800:200C::4180
switch(config)# aaa authentication iscsi default group iscsi-radius-group
```

ステップ 4 すべての iSCSI クライアントに CHAP を要求するように、iSCSI 認証方式を設定します。

```
switch(config)# iscsi authentication chap
```

ステップ 5 グローバル iSCSI 認証設定が CHAP 用であることを確認します。

```
switch# show iscsi global
iSCSI Global information
Authentication: CHAP <---------------- Verify CHAP
.
.
.
```

ステップ 6 AAA 許可情報が iSCSI 用であることを確認します。

```
switch# show aaa authentication
default: local
console: local
iscsi: group iscsi-radius-group <--------- Group name
dhchap: local

switch# show radius-server groups
total number of groups:2

following RADIUS server groups are configured:
group radius:
server: all configured radius servers
group iscsi-radius-group:
server: 10.1.1.1 on auth-port 1812, acct-port 1813

switch# show radius-server
Global RADIUS shared secret:mds-1 <-------- Verify secret
.
.
.
.

following RADIUS servers are configured:
10.1.1.1: <----------- Verify the server IPv4 address
available for authentication on port:1812
available for accounting on port:1813
```

iSCSI トランスペアレント モード イニシエータ

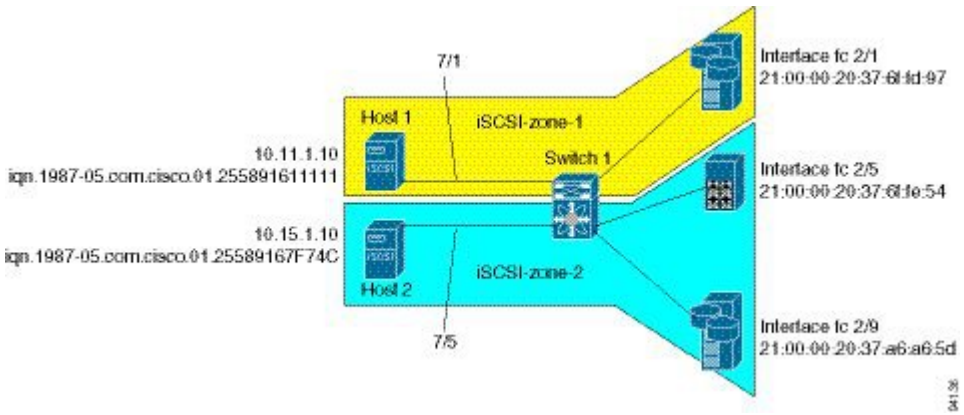
この構成は、次の構成を前提としています。

- ターゲット デバイス上に LUN マッピング、LUN マスキング、またはその他のホスト アクセス コントロールを設定しない。
- iSCSI ログイン認証を行わない（ログイン認証は none に設定）。
- トポロジは次のとおり。
  - iSCSI インターフェイス 7/1 は、IP アドレスで発信側を識別するように設定する。
  - iSCSI インターフェイス 7/5 は、ノード名で発信側を識別するように設定する。
  - IPS ポート 7/1 に接続する、IPv4 アドレスが 10.11.1.10 で名前が iqn.1987-05.com.cisco:01.255891611111 の iSCSI 発信側ホスト 1 を IPv4 アドレス（ホスト 1 = 10.11.1.10）で指定する。
  - IPv4 アドレスが 10.15.1.10 でノード名が iqn.1987-05.com.cisco:01.25589167f74c の iSCSI 発信側ホスト 2 を、IPS ポート 7/5 に接続する。

iSCSI の構成シナリオ 1

次の図は、シナリオ 1 を表しています。シナリオ 1 を構成するステップは、次のとおりです。

図 *40 : iSCSI* のシナリオ *1*



手順

ステップ 1 Cisco MDS スイッチのすべての iSCSI ホストにヌル認証を構成します。

```
switch(config)# iscsi authentication none
```

ステップ 2 自動生成された iSCSI ターゲット名を使用して、すべてのファイバ チャネル ターゲットを iSCSI SAN にダイナミックにインポートするように、iSCSI を設定します。

```
switch(config)# iscsi import target fc
```

ステップ 3 IPv4 アドレスを指定してスロット 7 ポート 1 のギガビット イーサネット インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface gigabitethernet 7/1
switch(config-if)# ip address 10.11.1.1 255.255.255.0
switch(config-if)# no shutdown
```

（注）
ホスト 2 はこのポートに接続します。

ステップ 4 すべてのダイナミック iSCSI イニシエータを IP アドレスで識別するように、スロット 7 ポート 1 の iSCSI インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface iscsi 7/1
switch(config-if)# switchport initiator id ip-address
switch(config-if)# no shut
```

ステップ 5 IPv4 アドレスを指定してスロット 7 ポート 5 のギガビット イーサネット インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface gigabitethernet 7/5
switch(config-if)# ip address 10.15.1.1 255.255.255.0
switch(config-if)# no shutdown
```

ステップ 6 すべてのダイナミック iSCSI イニシエータをノード名で識別するように、スロット 7 ポート 5 の iSCSI インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface iscsi 7/5
switch(config-if)# switchport initiator id name
switch(config-if)# no shutdown
```

（注）
ホスト 1 はこのポートに接続します。

ステップ 7 使用可能なファイバ チャネル ターゲットを確認します。

```
switch# show fcns database
VSAN 1:
--------------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x6d0001 NL 21:00:00:20:37:6f:fd:97 (Seagate) scsi-fcp:target
0x6d0101 NL 21:00:00:20:37:6f:fe:54 (Seagate) scsi-fcp:target
0x6d0201 NL 21:00:00:20:37:a6:a6:5d (Seagate) scsi-fcp:target
Total number of entries = 3
```

ステップ 8 ホスト 1 および 1 つのファイバ チャネル ターゲットが所属している *iscsi-zone-1* という名前のゾーンを作成します。

```
switch(config)# zone name iscsi-zone-1 vsan 1
switch(config-zone)# member pwwn 21:00:00:20:37:6f:fd:97
switch(config-zone)# member ip-address 10.11.1.10
```

（注）
iSCSI インターフェイスはすべてのホストを IP アドレスで識別するように設定されているので、ゾーン メンバーシップの設定には IP アドレスを使用します。

ステップ 9 ホスト 2 および 2 つのファイバ チャネル ターゲットが所属している *iscsi-zone-2* という名前のゾーンを作成します。

```
switch(config)# zone name iscsi-zone-2 vsan 1
switch(config-zone)# member pwwn 21:00:00:20:37:6f:fe:54
switch(config-zone)# member pwwn 21:00:00:20:37:a6:a6:5d
switch(config-zone)# member symbolic-nodename iqn.1987-05.com.cisco:01.25589167f74c
```

（注）
すべてのホストをノード名で識別するように iSCSI インターフェイスが設定されているので、ゾーン メンバーシップの設定には、iSCSI ホストのシンボリック ノード名を使用します。

ステップ 10 ゾーン セットを作成し、2 つのゾーンをメンバーとして追加します。

```
switch(config)# zoneset name zoneset-iscsi vsan 1
switch(config-zoneset)# member iscsi-zone-1
switch(config-zoneset)# member iscsi-zone-2
```

ステップ 11 ゾーン セットをアクティブにします。

```
switch(config)# zoneset activate name zoneset-iscsi vsan 1
```

ステップ 12 アクティブ ゾーン セットを表示します。

```
switch# show zoneset active
zoneset name zoneset-iscsi vsan 1
zone name iscsi-zone-1 vsan 1
* fcid 0x6d0001 [pwwn 21:00:00:20:37:6f:fd:97] <-----------Target
symbolic-nodename 10.11.1.10 <---------------------------------- iSCSI host (host 1, not online)

zone name iscsi-zone-2 vsan 1
* fcid 0x6d0101 [pwwn 21:00:00:20:37:6f:fe:54] <------------Target
* fcid 0x6d0201 [pwwn 21:00:00:20:37:a6:a6:5d] <------------Target
symbolic-nodename iqn.1987-05.com.cisco:01.25589167f74c <-iSCSI host (host 2, not online)
```

ステップ 13 iSCSI ホスト（ホスト 1 およびホスト 2）を起動します。

ステップ 14 すべての iSCSI セッションを表示します（詳細情報を表示する場合は **detail** オプションを使用します）。

```
switch# show iscsi session
Initiator iqn.1987-05.com.cisco:01.25589167f74c <-----Host 2
Initiator ip addr (s): 10.15.1.11
Session #1
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-05.21000020376ffe54
VSAN 1, ISID 00023d000001, Status active, no reservation

Session #2
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-05.2100002037a6a65d
VSAN 1, ISID 00023d000001, Status active, no reservation

Initiator 10.11.1.10 <----------------------------------Host 1
Initiator name iqn.1987-05.com.cisco:01.e41695d16b1a
Session #1
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-01.21000020376ffd97
VSAN 1, ISID 00023d000001, Status active, no reservation
```

（注）
自動作成されたターゲット名の最後の部分は、ファイバ チャネル ターゲットの pWWN です。

ステップ 15 2 つの iSCSI イニシエータの詳細を確認します。

ホスト 2：ノード名に基づくイニシエータ ID（イニシエータは iSCSI インターフェイス 7/5 に入るため）：

```
switch# show iscsi initiator

iSCSI Node name is iqn.1987-05.com.cisco:01.25589167f74c
Initiator ip addr (s): 10.15.1.11
iSCSI alias name: oasis11.cisco.com
Node WWN is 20:02:00:0b:fd:44:68:c2 (dynamic)
Member of vsans: 1
Number of Virtual n_ports: 1
Virtual Port WWN is 20:03:00:0b:fd:44:68:c2 (dynamic)
Interface iSCSI 7/5 , Portal group tag: 0x304
VSAN ID 1, FCID 0x6d0300
```

ホスト 1：IPv4 アドレスに基づくイニシエータ ID（イニシエータは iSCSI インターフェイス 7/1 に入るため）：

```
iSCSI Node name is 10.11.1.10
iSCSI Initiator name: iqn.1987 - 05.com.cisco:01.e41695d16b1a
iSCSI alias name: oasis10.cisco.com
Node WWN is 20:04:00:0b:fd:44:68:c2 (dynamic)
Member of vsans: 1
Number of Virtual n_ports: 1
Virtual Port WWN is 20:05:00:0b:fd:44:68:c2 (dynamic)
Interface iSCSI 7/1 , Portal group tag: 0x300
VSAN ID 1, FCID 0x6d0301
```

ステップ 16 アクティブ ゾーン セットを表示します。iSCSI イニシエータの FC ID が解決されます。

ホスト 1 の解決された FC ID：

```
switch# show zoneset active
zoneset name zoneset-iscsi vsan 1
zone name iscsi-zone-1 vsan 1
* fcid 0x6d0001 [pwwn 21:00:00:20:37:6f:fd:97]
* fcid 0x6d0301 [symbolic-nodename 10.11.1.10]
```

ホスト 2 の FC ID：

```
zone name iscsi-zone-2 vsan 1
* fcid 0x6d0101 [pwwn 21:00:00:20:37:6f:fe:54]
* fcid 0x6d0201 [pwwn 21:00:00:20:37:a6:a6:5d]
* fcid 0x6d0300 [symbolic-nodename iqn.1987-05.com.cisco:01.25589167f74c] <--------------------------
```

ステップ 17 ファイバ チャネル ネーム サーバーによって、iSCSI ホスト用に作成された仮想 N ポートが表示されます。

```
switch# show fcns database
VSAN 1:
--------------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x6d0001 NL 21:00:00:20:37:6f:fd:97 (Seagate) scsi-fcp:target
0x6d0101 NL 21:00:00:20:37:6f:fe:54 (Seagate) scsi-fcp:target
0x6d0201 NL 21:00:00:20:37:a6:a6:5d (Seagate) scsi-fcp:target
0x6d0300 N 20:03:00:0b:fd:44:68:c2 (Cisco) scsi-fcp:init isc..w
0x6d0301 N 20:05:00:0b:fd:44:68:c2 (Cisco) scsi-fcp:init isc..w
```

ステップ 18 ファイバ チャネル ネーム サーバーの iSCSI イニシエータ ノードに関する詳細出力を確認します。

```
switch# show fcns database fcid 0x6d0300 detail vsan 1
-----------------------
VSAN:1 FCID:0x6d0300
```

```
-----------------------
port-wwn (vendor) :20:03:00:0b:fd:44:68:c2 (Cisco)
node-wwn :20:02:00:0b:fd:44:68:c2
class :2,3
node-ip-addr :10.15.1.11
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :iqn.1987-05.com.cisco:01.25589167f74c <--------------------
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :21:91:00:0b:fd:44:68:c0
hard-addr :0x000000
Total number of entries = 1
```

```
switch# show fcns database fcid 0x6d0301 detail vsan 1
-----------------------
VSAN:1 FCID:0x6d0301
-----------------------
port-wwn (vendor) :20:05:00:0b:fd:44:68:c2 (Cisco)
node-wwn :20:04:00:0b:fd:44:68:c2
class :2,3
node-ip-addr :10.11.1.10
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :10.11.1.10
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :21:81:00:0b:fd:44:68:c0
hard-addr :0x000000
```

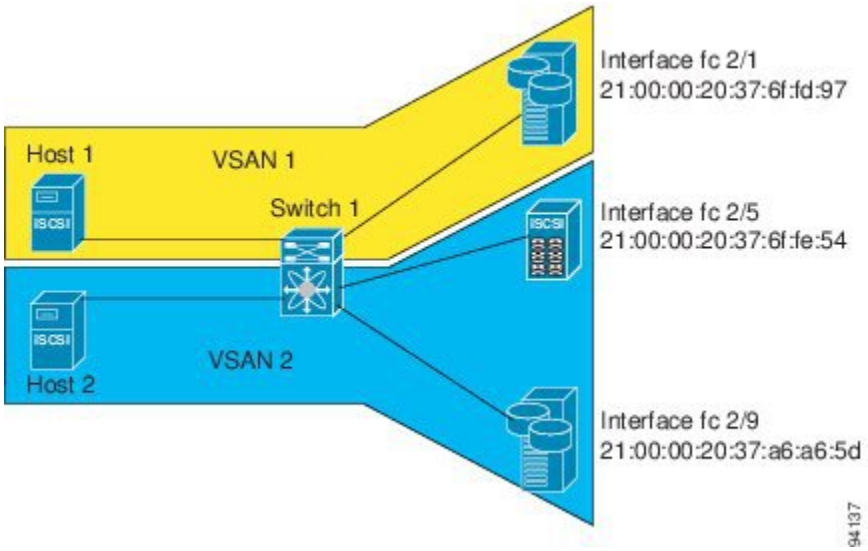
iSCSI の構成シナリオ 2

シナリオ 2 の例で想定されている構成は、次のとおりです。

- アクセス コントロールはファイバ チャネル ゾーン分割に基づく。
- ターゲットベースの LUN マッピングまたは LUN マスキングを使用する。
- iSCSI 認証は行わない（none）。
- iSCSI 発信側を個別の VSAN に割り当てる。

次の図は、シナリオ 2 を表します。シナリオ 2 を構成するステップは、次のとおりです。

図 *41 : iSCSI* のシナリオ *2*



手順

ステップ 1 すべての iSCSI ホストにヌル認証を設定します。

```
switch(config)# iscsi authentication none
```

ステップ 2 自動生成された iSCSI ターゲット名を使用して、すべてのファイバ チャネル ターゲットを iSCSI SAN にダイナミックにインポートするように、iSCSI を設定します。

```
switch(config)# iscsi import target fc
```

ステップ 3 IPv4 アドレスを指定してスロット 7 ポート 1 のギガビット イーサネット インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface gigabitethernet 7/1
switch(config-if)# ip address 10.11.1.1 255.255.255.0
switch(config-if)# no shutdown
```

ステップ 4 すべてのダイナミック iSCSI イニシエータを IP アドレスで識別するように、スロット 7 ポート 1 の iSCSI インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface iscsi 7/1
switch(config-if)# switchport initiator id ip-address
switch(config-if)# no shutdown
```

ステップ 5 IPv4 アドレスを指定してスロット 7 ポート 5 のギガビット イーサネット インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface gigabitethernet 7/5
switch(config-if)# ip address 10.15.1.1 255.255.255.0
switch(config-if)# no shutdown
```

ステップ 6 すべてのダイナミック iSCSI イニシエータを IP アドレスで識別するように、スロット 7 ポート 5 の iSCSI インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface iscsi 7/5
switch(config-if)# switchport initiator id ip-address
switch(config-if)# no shutdown
```

ステップ 7 iSCSI イニシエータごとにスタティック設定を追加します。

```
switch(config)# iscsi initiator name iqn.1987-05.com.cisco:01.e41695d16b1a <-----Host 2
switch(config-iscsi-init)# static pWWN system-assign 1
switch(config-iscsi-init)# static nWWN system-assign
switch(config)# iscsi initiator ip address 10.15.1.11 <----------------------------------Host 1
switch(config-iscsi-init)# static pwwn system-assigned 1
switch(config-iscsi-init)# vsan 2
```

（注）
ホスト 1 は VSAN 2 で設定されます。

ステップ 8 設定済みの WWN を表示します。

```
switch# show iscsi initiator configured
iSCSI Node name is iqn.1987-05.com.cisco:01.e41695d16b1a
Member of vsans: 1
Node WWN is 20:03:00:0b:fd:44:68:c2
No. of PWWN: 1
Port WWN is 20:02:00:0b:fd:44:68:c2

iSCSI Node name is 10.15.1.11
Member of vsans: 2
No. of PWWN: 1
Port WWN is 20:06:00:0b:fd:44:68:c2
```

（注）
WWN はシステムによって割り当てられています。発信側はさまざまな VSAN に所属しています。

ステップ 9 ホスト 1 を含むゾーンを作成します。

```
switch(config)# zone name iscsi-zone-1 vsan 1
```

ステップ 10 *iscsi-zone-1* という名前のゾーンに 3 つのメンバーを追加します。

a) 次のコマンドは、シンボリック ノード名に基づいています。

```
switch(config-zone)# member symbolic-nodename iqn.1987-05.com.cisco:01.e41695d16b1a
```

b) 次のコマンドは、発信側に割り当てられた固定 pWWN に基づいています。pWWN は **show iscsi initiator** 出力から取得できます。

```
switch(config-zone)# member pwwn 20:02:00:0b:fd:44:68:c2
```

ステップ 11 ホスト 2 および 2 つのファイバ チャネル ターゲットがあるゾーンを作成します。

```
switch(config)# zone name iscsi-zone-2 vsan 2
```

（注）
ホストが VSAN 2 にある場合、ファイバ チャネル ターゲットおよびゾーンも VSAN 2 になければなりません。

ステップ 12 VSAN 2 のゾーン セットをアクティブにします。

```
switch(config)# zoneset activate name iscsi-zoneset-v2 vsan 2
Zoneset activation initiated. check zone status
switch# show zoneset active vsan 2
zoneset name iscsi-zoneset-v2 vsan 2
zone name iscsi-zone-2 vsan 2
* fcid 0x750001 [pwwn 21:00:00:20:37:6f:fe:54]
* fcid 0x750101 [pwwn 21:00:00:20:37:a6:a6:5d]
pwwn 20:06:00:0b:fd:44:68:c2
```

ステップ 13 両方のホストで iSCSI クライアントを起動し、該当するセッションが開始されたことを確認します。

ステップ 14 iSCSI セッションを表示し、ファイバ チャネル ターゲットおよび構成された WWN を確認します。

```
switch# show iscsi session
Initiator iqn.1987-05.com.cisco:01.e41695d16b1a
Initiator ip addr (s): 10.11.1.10
Session #1
Discovery session, ISID 00023d000001, Status active
Session #2
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-01.21000020376ffd97 <----
VSAN 1, ISID 00023d000001, Status active, no reservation
```

ステップ 15 iSCSI イニシエータを表示し、設定された pWWN および nWWN を確認します。

```
switch# show iscsi initiator
iSCSI Node name is iqn.1987-05.com.cisco:01.e41695d16b1a
Initiator ip addr (s): 10.11.1.10
iSCSI alias name: oasis10.cisco.com
Node WWN is 20:03:00:0b:fd:44:68:c2 (configured) <----------
Member of vsans: 1
Number of Virtual n_ports: 1
Virtual Port WWN is 20:02:00:0b:fd:44:68:c2 (configured) <----
Interface iSCSI 7/1, Portal group tag: 0x300
VSAN ID 1, FCID 0x680102
```

ステップ 16 ファイバ チャネルのネーム サーバーを確認します。

```
switch# show fcns database vsan 1
VSAN 1:
--------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------
0x680001 NL 21:00:00:20:37:6f:fd:97 (Seagate) scsi-fcp:target
0x680102 N 20:02:00:0b:fd:44:68:c2 (Cisco) scsi-fcp:init iscw
```

ステップ 17 ネーム サーバーの iSCSI イニシエータ ノードの FC ID に関する詳細を確認します。

```
switch(config)# show fcns database fcid 0x680102 detail vsan 1
------------------------
VSAN:1 FCID:0x680102
------------------------
port-wwn (vendor) :20:02:00:0b:fd:44:68:c2 (Cisco)
node-wwn :20:03:00:0b:fd:44:68:c2
class :2,3
node-ip-addr :10.11.1.10
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :iqn.1987-05.com.cisco:01.e41695d16b1a
port-type :N
port-ip-addr :0.0.0.0
```

```
fabric-port-wwn :21:81:00:0b:fd:44:68:c0
iSCSI alias name: oasis10.cisco.com
```

ステップ 18 ファイバ チャネルのネーム サーバーを確認します。

```
switch# show fcns database vsan 1

VSAN 1:
------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
------------------------------------------------------------------
0x680001 NL 21:00:00:20:37:6f:fd:97 (Seagate) scsi-fcp:target
0x680102 N 20:02:00:0b:fd:44:68:c2 (Cisco) scsi-fcp:init isc..w
```

ステップ 19 ネーム サーバーの iSCSI イニシエータ ノードの FC ID に関する詳細を確認します。

```
switch(config)# show fcns database fcid 0x680102 detail vsan 1
------------------------
VSAN:1 FCID:0x680102
------------------------
port-wwn (vendor) :20:02:00:0b:fd:44:68:c2 (Cisco)
node-wwn :20:03:00:0b:fd:44:68:c2
class :2,3
node-ip-addr :10.11.1.10
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :iqn.1987-05.com.cisco:01.e41695d16b1a
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :21:81:00:0b:fd:44:68:c0
hard-addr :0x000000
```

ステップ 20 iSCSI クライアントの FC ID がゾーン分割によって解決されたことを確認します。

```
switch# show zoneset active vsan 1
zoneset name iscsi-zoneset-v1 vsan 1
zone name iscsi-zone-1 vsan 1
* fcid 0x680001 [pwwn 21:00:00:20:37:6f:fd:97]
* fcid 0x680102 [pwwn 20:02:00:0b:fd:44:68:c2]
```

ステップ 21 2 番目のイニシエータが VSAN 2 の 2 つのファイバ チャネル ターゲットに接続されていることを確認します。

次のコマンドは、最初のターゲットへのセッションと2番目のターゲットへのセッションを表示します。

```
switch# show iscsi session initiator 10.15.1.11
Initiator 10.15.1.11
Initiator name iqn.1987-05.com.cisco:01.25589167f74c
Session #1
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-05.21000020376ffe54 <--
VSAN 2, ISID 00023d000001, Status active, no reservation
Session #2
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-05.2100002037a6a65d <--
VSAN 2, ISID 00023d000001, Status active, no reservation
```

次のコマンドを実行すると、ダイナミック WWN が割り当てられていないスタティック WWN およびスタティック pWWN としてイニシエータに表示されます。

```
switch# show iscsi initiator
iSCSI Node name is 10.15.1.11
iSCSI Initiator name: iqn.1987-05.com.cisco:01.25589167f74c
iSCSI alias name: oasis11.cisco.com
```

```
Node WWN is 20:04:00:0b:fd:44:68:c2 (dynamic)
Member of vsans: 2
Number of Virtual n_ports: 1
Virtual Port WWN is 20:06:00:0b:fd:44:68:c2 (configured)
Interface iSCSI 7/5, Portal group tag: 0x304
VSAN ID 2, FCID 0x750200
```

次の出力には、ネームサーバの iSCSI イニシエータ エントリが表示されています。

```
switch# show fcns database vsan 2
VSAN 2:
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
0x750001 NL 21:00:00:20:37:6f:fe:54 (Seagate) scsi-fcp:target
0x750101 NL 21:00:00:20:37:a6:a6:5d (Seagate) scsi-fcp:target
0x750200 N 20:06:00:0b:fd:44:68:c2 (Cisco) scsi-fcp:init isc..w
Total number of entries = 3
```

```
switch# show fcns database fcid 0x750200 detail vsan 2
-----------------------
VSAN:2 FCID:0x750200
-----------------------
port-wwn (vendor) :20:06:00:0b:fd:44:68:c2 (Cisco)
node-wwn :20:04:00:0b:fd:44:68:c2
class :2,3
node-ip-addr :10.15.1.11
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :10.15.1.11
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :21:91:00:0b:fd:44:68:c0
hard-addr :0x000000
Total number of entries = 1
```

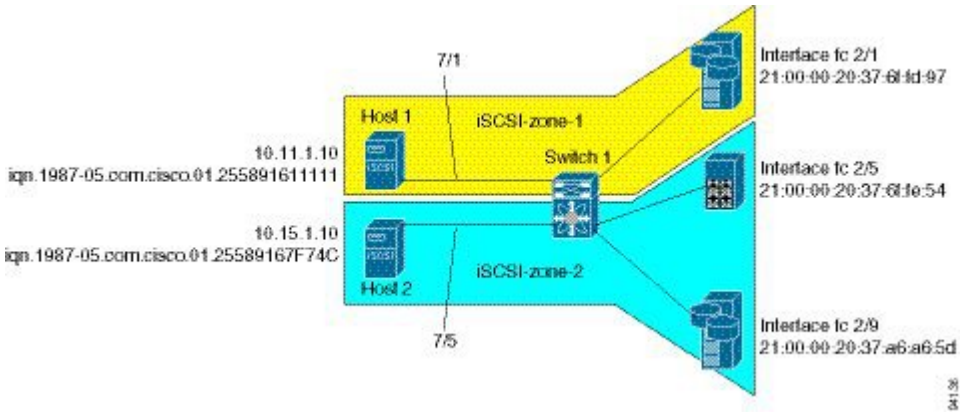
次のコマンドは、iSCSI イニシエータに解決された FC ID を表示します。

```
switch# show zoneset active vsan 2
zoneset name iscsi-zoneset-v2 vsan 2
zone name iscsi-zone-2 vsan 2
* fcid 0x750001 [pwwn 21:00:00:20:37:6f:fe:54]
* fcid 0x750101 [pwwn 21:00:00:20:37:a6:a6:5d]
```

iSCSI の構成シナリオ 1

次の図は、シナリオ 1 を表しています。シナリオ 1 を構成するステップは、次のとおりです。

図 *42 : iSCSI* のシナリオ *1*



手順

ステップ 1 Cisco MDS スイッチのすべての iSCSI ホストにヌル認証を構成します。

```
switch(config)# iscsi authentication none
```

ステップ 2 自動生成された iSCSI ターゲット名を使用して、すべてのファイバ チャネル ターゲットを iSCSI SAN にダイナミックにインポートするように、iSCSI を設定します。

```
switch(config)# iscsi import target fc
```

ステップ 3 IPv4 アドレスを指定してスロット 7 ポート 1 のギガビット イーサネット インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface gigabitethernet 7/1
switch(config-if)# ip address 10.11.1.1 255.255.255.0
switch(config-if)# no shutdown
```

（注）
ホスト 2 はこのポートに接続します。

ステップ 4 すべてのダイナミック iSCSI イニシエータを IP アドレスで識別するように、スロット 7 ポート 1 の iSCSI インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface iscsi 7/1
switch(config-if)# switchport initiator id ip-address
switch(config-if)# no shut
```

ステップ 5 IPv4 アドレスを指定してスロット 7 ポート 5 のギガビット イーサネット インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface gigabitethernet 7/5
switch(config-if)# ip address 10.15.1.1 255.255.255.0
switch(config-if)# no shutdown
```

ステップ 6 すべてのダイナミック iSCSI イニシエータをノード名で識別するように、スロット 7 ポート 5 の iSCSI インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface iscsi 7/5
switch(config-if)# switchport initiator id name
switch(config-if)# no shutdown
```

（注）
ホスト 1 はこのポートに接続します。

ステップ 7 使用可能なファイバ チャネル ターゲットを確認します。

```
switch# show fcns database
VSAN 1:
--------------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x6d0001 NL 21:00:00:20:37:6f:fd:97 (Seagate) scsi-fcp:target
0x6d0101 NL 21:00:00:20:37:6f:fe:54 (Seagate) scsi-fcp:target
0x6d0201 NL 21:00:00:20:37:a6:a6:5d (Seagate) scsi-fcp:target
Total number of entries = 3
```

ステップ 8 ホスト 1 および 1 つのファイバ チャネル ターゲットが所属している *iscsi-zone-1* という名前のゾーンを作成します。

```
switch(config)# zone name iscsi-zone-1 vsan 1
switch(config-zone)# member pwwn 21:00:00:20:37:6f:fd:97
switch(config-zone)# member ip-address 10.11.1.10
```

（注）
iSCSI インターフェイスはすべてのホストを IP アドレスで識別するように設定されているので、ゾーン メンバーシップの設定には IP アドレスを使用します。

ステップ 9 ホスト 2 および 2 つのファイバ チャネル ターゲットが所属している *iscsi-zone-2* という名前のゾーンを作成します。

```
switch(config)# zone name iscsi-zone-2 vsan 1
switch(config-zone)# member pwwn 21:00:00:20:37:6f:fe:54
switch(config-zone)# member pwwn 21:00:00:20:37:a6:a6:5d
switch(config-zone)# member symbolic-nodename iqn.1987-05.com.cisco:01.25589167f74c
```

（注）
すべてのホストをノード名で識別するように iSCSI インターフェイスが設定されているので、ゾーン メンバーシップの設定には、iSCSI ホストのシンボリック ノード名を使用します。

ステップ 10 ゾーン セットを作成し、2 つのゾーンをメンバーとして追加します。

```
switch(config)# zoneset name zoneset-iscsi vsan 1
switch(config-zoneset)# member iscsi-zone-1
switch(config-zoneset)# member iscsi-zone-2
```

ステップ 11 ゾーン セットをアクティブにします。

```
switch(config)# zoneset activate name zoneset-iscsi vsan 1
```

ステップ 12 アクティブ ゾーン セットを表示します。

```
switch# show zoneset active
zoneset name zoneset-iscsi vsan 1
zone name iscsi-zone-1 vsan 1
* fcid 0x6d0001 [pwwn 21:00:00:20:37:6f:fd:97] <-----------Target
symbolic-nodename 10.11.1.10 <--------------------------------- iSCSI host (host 1, not online)
```

```
zone name iscsi-zone-2 vsan 1
* fcid 0x6d0101 [pwwn 21:00:00:20:37:6f:fe:54] <------------Target
* fcid 0x6d0201 [pwwn 21:00:00:20:37:a6:a6:5d] <------------Target
symbolic-nodename iqn.1987-05.com.cisco:01.25589167f74c <-iSCSI host (host 2, not online)
```

ステップ 13 iSCSI ホスト（ホスト 1 およびホスト 2）を起動します。

ステップ 14 すべての iSCSI セッションを表示します（詳細情報を表示する場合は **detail** オプションを使用します）。

```
switch# show iscsi session
Initiator iqn.1987-05.com.cisco:01.25589167f74c <-----Host 2
Initiator ip addr (s): 10.15.1.11
Session #1
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-05.21000020376ffe54
VSAN 1, ISID 00023d000001, Status active, no reservation

Session #2
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-05.2100002037a6a65d
VSAN 1, ISID 00023d000001, Status active, no reservation

Initiator 10.11.1.10 <----------------------------------Host 1
Initiator name iqn.1987-05.com.cisco:01.e41695d16b1a
Session #1
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-01.21000020376ffd97
VSAN 1, ISID 00023d000001, Status active, no reservation
```

（注）
自動作成されたターゲット名の最後の部分は、ファイバ チャネル ターゲットの pWWN です。

ステップ 15 2 つの iSCSI イニシエータの詳細を確認します。

ホスト 2：ノード名に基づくイニシエータ ID（イニシエータは iSCSI インターフェイス 7/5 に入るため）：

```
switch# show iscsi initiator

iSCSI Node name is iqn.1987-05.com.cisco:01.25589167f74c
Initiator ip addr (s): 10.15.1.11
iSCSI alias name: oasis11.cisco.com
Node WWN is 20:02:00:0b:fd:44:68:c2 (dynamic)
Member of vsans: 1
Number of Virtual n_ports: 1
Virtual Port WWN is 20:03:00:0b:fd:44:68:c2 (dynamic)
Interface iSCSI 7/5 , Portal group tag: 0x304
VSAN ID 1, FCID 0x6d0300
```

ホスト 1：IPv4 アドレスに基づくイニシエータ ID（イニシエータは iSCSI インターフェイス 7/1 に入るため）：

```
iSCSI Node name is 10.11.1.10
iSCSI Initiator name: iqn.1987 - 05.com.cisco:01.e41695d16b1a
iSCSI alias name: oasis10.cisco.com
Node WWN is 20:04:00:0b:fd:44:68:c2 (dynamic)
Member of vsans: 1
Number of Virtual n_ports: 1
Virtual Port WWN is 20:05:00:0b:fd:44:68:c2 (dynamic)
Interface iSCSI 7/1 , Portal group tag: 0x300
VSAN ID 1, FCID 0x6d0301
```

ステップ 16 アクティブ ゾーン セットを表示します。iSCSI イニシエータの FC ID が解決されます。

ホスト 1 の解決された FC ID：

```
switch# show zoneset active
zoneset name zoneset-iscsi vsan 1
zone name iscsi-zone-1 vsan 1
* fcid 0x6d0001 [pwwn 21:00:00:20:37:6f:fd:97]
* fcid 0x6d0301 [symbolic-nodename 10.11.1.10]
```

ホスト 2 の FC ID：

```
zone name iscsi-zone-2 vsan 1
* fcid 0x6d0101 [pwwn 21:00:00:20:37:6f:fe:54]
* fcid 0x6d0201 [pwwn 21:00:00:20:37:a6:a6:5d]
* fcid 0x6d0300 [symbolic-nodename iqn.1987-05.com.cisco:01.25589167f74c] <-------------------------
```

ステップ 17 ファイバ チャネル ネーム サーバーによって、iSCSI ホスト用に作成された仮想 N ポートが表示されます。

```
switch# show fcns database
VSAN 1:
--------------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x6d0001 NL 21:00:00:20:37:6f:fd:97 (Seagate) scsi-fcp:target
0x6d0101 NL 21:00:00:20:37:6f:fe:54 (Seagate) scsi-fcp:target
0x6d0201 NL 21:00:00:20:37:a6:a6:5d (Seagate) scsi-fcp:target
0x6d0300 N 20:03:00:0b:fd:44:68:c2 (Cisco) scsi-fcp:init isc..w
0x6d0301 N 20:05:00:0b:fd:44:68:c2 (Cisco) scsi-fcp:init isc..w
```

ステップ 18 ファイバ チャネル ネーム サーバーの iSCSI イニシエータ ノードに関する詳細出力を確認します。

```
switch# show fcns database fcid 0x6d0300 detail vsan 1
------------------------
VSAN:1 FCID:0x6d0300
------------------------
port-wwn (vendor) :20:03:00:0b:fd:44:68:c2 (Cisco)
node-wwn :20:02:00:0b:fd:44:68:c2
class :2,3
node-ip-addr :10.15.1.11
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :iqn.1987-05.com.cisco:01.25589167f74c <--------------------
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :21:91:00:0b:fd:44:68:c0
hard-addr :0x000000
Total number of entries = 1

switch# show fcns database fcid 0x6d0301 detail vsan 1
------------------------
VSAN:1 FCID:0x6d0301
------------------------
port-wwn (vendor) :20:05:00:0b:fd:44:68:c2 (Cisco)
node-wwn :20:04:00:0b:fd:44:68:c2
class :2,3
node-ip-addr :10.11.1.10
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :10.11.1.10
port-type :N
port-ip-addr :0.0.0.0
```

```
fabric-port-wwn :21:81:00:0b:fd:44:68:c0
hard-addr :0x000000
```

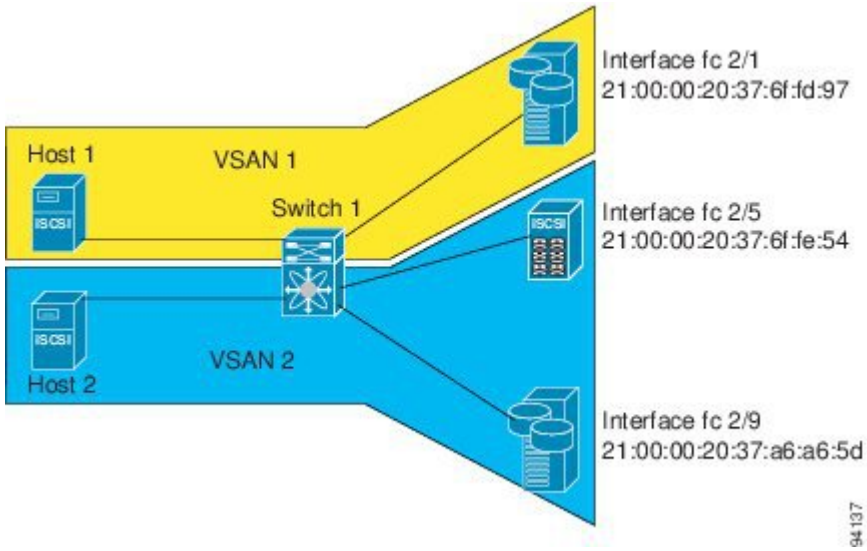
iSCSI の構成シナリオ 2

シナリオ 2 の例で想定されている構成は、次のとおりです。

- アクセス コントロールはファイバ チャネル ゾーン分割に基づく。
- ターゲットベースの LUN マッピングまたは LUN マスキングを使用する。
- iSCSI 認証は行わない（none）。
- iSCSI 発信側を個別の VSAN に割り当てる。

次の図は、シナリオ 2 を表します。シナリオ 2 を構成するステップは、次のとおりです。

図 *43 : iSCSI* のシナリオ *2*



手順

ステップ 1 すべての iSCSI ホストにヌル認証を設定します。

```
switch(config)# iscsi authentication none
```

ステップ 2 自動生成された iSCSI ターゲット名を使用して、すべてのファイバ チャネル ターゲットを iSCSI SAN にダイナミックにインポートするように、iSCSI を設定します。

```
switch(config)# iscsi import target fc
```

ステップ 3 IPv4 アドレスを指定してスロット 7 ポート 1 のギガビット イーサネット インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface gigabitethernet 7/1
switch(config-if)# ip address 10.11.1.1 255.255.255.0
switch(config-if)# no shutdown
```

ステップ 4 すべてのダイナミック iSCSI イニシエータを IP アドレスで識別するように、スロット 7 ポート 1 の iSCSI インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface iscsi 7/1
switch(config-if)# switchport initiator id ip-address
switch(config-if)# no shutdown
```

ステップ 5 IPv4 アドレスを指定してスロット 7 ポート 5 のギガビット イーサネット インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface gigabitethernet 7/5
switch(config-if)# ip address 10.15.1.1 255.255.255.0
switch(config-if)# no shutdown
```

ステップ 6 すべてのダイナミック iSCSI イニシエータを IP アドレスで識別するように、スロット 7 ポート 5 の iSCSI インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface iscsi 7/5
switch(config-if)# switchport initiator id ip-address
switch(config-if)# no shutdown
```

ステップ 7 iSCSI イニシエータごとにスタティック設定を追加します。

```
switch(config)# iscsi initiator name iqn.1987-05.com.cisco:01.e41695d16b1a <-----Host 2
switch(config-iscsi-init)# static pWWN system-assign 1
switch(config-iscsi-init)# static nWWN system-assign
switch(config)# iscsi initiator ip address 10.15.1.11 <----------------------------------Host 1
switch(config-iscsi-init)# static pwwn system-assigned 1
switch(config-iscsi-init)# vsan 2
```

（注）
ホスト 1 は VSAN 2 で設定されます。

ステップ 8 設定済みの WWN を表示します。

```
switch# show iscsi initiator configured
iSCSI Node name is iqn.1987-05.com.cisco:01.e41695d16b1a
Member of vsans: 1
Node WWN is 20:03:00:0b:fd:44:68:c2
No. of PWWN: 1
Port WWN is 20:02:00:0b:fd:44:68:c2

iSCSI Node name is 10.15.1.11
Member of vsans: 2
No. of PWWN: 1
Port WWN is 20:06:00:0b:fd:44:68:c2
```

（注）
WWN はシステムによって割り当てられています。発信側はさまざまな VSAN に所属しています。

ステップ 9 ホスト 1 を含むゾーンを作成します。

```
switch(config)# zone name iscsi-zone-1 vsan 1
```

ステップ 10 *iscsi-zone-1* という名前のゾーンに 3 つのメンバーを追加します。

a) 次のコマンドは、シンボリック ノード名に基づいています。

```
switch(config-zone)# member symbolic-nodename iqn.1987-05.com.cisco:01.e41695d16b1a
```

b) 次のコマンドは、発信側に割り当てられた固定 pWWN に基づいています。pWWN は **show iscsi initiator** 出力から取得できます。

```
switch(config-zone)# member pwwn 20:02:00:0b:fd:44:68:c2
```

ステップ 11 ホスト 2 および 2 つのファイバ チャネル ターゲットがあるゾーンを作成します。

```
switch(config)# zone name iscsi-zone-2 vsan 2
```

（注）
ホストが VSAN 2 にある場合、ファイバ チャネル ターゲットおよびゾーンも VSAN 2 になければなりません。

ステップ 12 VSAN 2 のゾーン セットをアクティブにします。

```
switch(config)# zoneset activate name iscsi-zoneset-v2 vsan 2
Zoneset activation initiated. check zone status
switch# show zoneset active vsan 2
zoneset name iscsi-zoneset-v2 vsan 2
zone name iscsi-zone-2 vsan 2
* fcid 0x750001 [pwwn 21:00:00:20:37:6f:fe:54]
* fcid 0x750101 [pwwn 21:00:00:20:37:a6:a6:5d]
pwwn 20:06:00:0b:fd:44:68:c2
```

ステップ 13 両方のホストで iSCSI クライアントを起動し、該当するセッションが開始されたことを確認します。

ステップ 14 iSCSI セッションを表示し、ファイバ チャネル ターゲットおよび構成された WWN を確認します。

```
switch# show iscsi session
Initiator iqn.1987-05.com.cisco:01.e41695d16b1a
Initiator ip addr (s): 10.11.1.10
Session #1
Discovery session, ISID 00023d000001, Status active
Session #2
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-01.21000020376ffd97 <----
VSAN 1, ISID 00023d000001, Status active, no reservation
```

ステップ 15 iSCSI イニシエータを表示し、設定された pWWN および nWWN を確認します。

```
switch# show iscsi initiator
iSCSI Node name is iqn.1987-05.com.cisco:01.e41695d16b1a
Initiator ip addr (s): 10.11.1.10
iSCSI alias name: oasis10.cisco.com
Node WWN is 20:03:00:0b:fd:44:68:c2 (configured) <----------
Member of vsans: 1
Number of Virtual n_ports: 1
Virtual Port WWN is 20:02:00:0b:fd:44:68:c2 (configured) <----
Interface iSCSI 7/1, Portal group tag: 0x300
VSAN ID 1, FCID 0x680102
```

ステップ 16 ファイバ チャネルのネーム サーバーを確認します。

```
switch# show fcns database vsan 1
VSAN 1:
--------------------------------------------------------------------
```

```
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------
0x680001 NL 21:00:00:20:37:6f:fd:97 (Seagate) scsi-fcp:target
0x680102 N 20:02:00:0b:fd:44:68:c2 (Cisco) scsi-fcp:init iscw
```

ステップ 17 ネーム サーバーの iSCSI イニシエータ ノードの FC ID に関する詳細を確認します。

```
switch(config)# show fcns database fcid 0x680102 detail vsan 1
-----------------------
VSAN:1 FCID:0x680102
-----------------------
port-wwn (vendor) :20:02:00:0b:fd:44:68:c2 (Cisco)
node-wwn :20:03:00:0b:fd:44:68:c2
class :2,3
node-ip-addr :10.11.1.10
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :iqn.1987-05.com.cisco:01.e41695d16b1a
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :21:81:00:0b:fd:44:68:c0
iSCSI alias name: oasis10.cisco.com
```

ステップ 18 ファイバ チャネルのネーム サーバーを確認します。

```
switch# show fcns database vsan 1

VSAN 1:
--------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------
0x680001 NL 21:00:00:20:37:6f:fd:97 (Seagate) scsi-fcp:target
0x680102 N 20:02:00:0b:fd:44:68:c2 (Cisco) scsi-fcp:init isc..w
```

ステップ 19 ネーム サーバーの iSCSI イニシエータ ノードの FC ID に関する詳細を確認します。

```
switch(config)# show fcns database fcid 0x680102 detail vsan 1
-----------------------
VSAN:1 FCID:0x680102
-----------------------
port-wwn (vendor) :20:02:00:0b:fd:44:68:c2 (Cisco)
node-wwn :20:03:00:0b:fd:44:68:c2
class :2,3
node-ip-addr :10.11.1.10
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :iqn.1987-05.com.cisco:01.e41695d16b1a
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :21:81:00:0b:fd:44:68:c0
hard-addr :0x000000
```

ステップ 20 iSCSI クライアントの FC ID がゾーン分割によって解決されたことを確認します。

```
switch# show zoneset active vsan 1
zoneset name iscsi-zoneset-v1 vsan 1
zone name iscsi-zone-1 vsan 1
* fcid 0x680001 [pwwn 21:00:00:20:37:6f:fd:97]
* fcid 0x680102 [pwwn 20:02:00:0b:fd:44:68:c2]
```

ステップ 21 2 番目のイニシエータが VSAN 2 の 2 つのファイバ チャネル ターゲットに接続されていることを確認します。

次のコマンドは、最初のターゲットへのセッションと2番目のターゲットへのセッションを表示します。

```
switch# show iscsi session initiator 10.15.1.11
Initiator 10.15.1.11
Initiator name iqn.1987-05.com.cisco:01.25589167f74c
Session #1
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-05.21000020376ffe54 <--
VSAN 2, ISID 00023d000001, Status active, no reservation
Session #2
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-05.2100002037a6a65d <--
VSAN 2, ISID 00023d000001, Status active, no reservation
```

次のコマンドを実行すると、ダイナミック WWN が割り当てられていないスタティック WWN およびスタティック pWWN としてイニシエータに表示されます。

```
switch# show iscsi initiator
iSCSI Node name is 10.15.1.11
iSCSI Initiator name: iqn.1987-05.com.cisco:01.25589167f74c
iSCSI alias name: oasis11.cisco.com
Node WWN is 20:04:00:0b:fd:44:68:c2 (dynamic)
Member of vsans: 2
Number of Virtual n_ports: 1
Virtual Port WWN is 20:06:00:0b:fd:44:68:c2 (configured)
Interface iSCSI 7/5, Portal group tag: 0x304
VSAN ID 2, FCID 0x750200
```

次の出力には、ネームサーバの iSCSI イニシエータ エントリが表示されています。

```
switch# show fcns database vsan 2
VSAN 2:
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
0x750001 NL 21:00:00:20:37:6f:fe:54 (Seagate) scsi-fcp:target
0x750101 NL 21:00:00:20:37:a6:a6:5d (Seagate) scsi-fcp:target
0x750200 N 20:06:00:0b:fd:44:68:c2 (Cisco) scsi-fcp:init isc..w
Total number of entries = 3
```

```
switch# show fcns database fcid 0x750200 detail vsan 2
------------------------
VSAN:2 FCID:0x750200
------------------------
port-wwn (vendor) :20:06:00:0b:fd:44:68:c2 (Cisco)
node-wwn :20:04:00:0b:fd:44:68:c2
class :2,3
node-ip-addr :10.15.1.11
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :10.15.1.11
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :21:91:00:0b:fd:44:68:c0
hard-addr :0x000000
Total number of entries = 1
```

次のコマンドは、iSCSI イニシエータに解決された FC ID を表示します。

```
switch# show zoneset active vsan 2
zoneset name iscsi-zoneset-v2 vsan 2
zone name iscsi-zone-2 vsan 2
```

```
* fcid 0x750001 [pwwn 21:00:00:20:37:6f:fe:54]
* fcid 0x750101 [pwwn 21:00:00:20:37:a6:a6:5d]
```

Internet Storage Name Service の概要

Internet Storage Name Service（iSNS）を使用すると、iSCSI デバイスの検出、管理、および設定の自動化により、既存の TCP/IP ネットワークが SAN としてより効率的に機能できるようになります。その実現のために、iSNS サーバーおよびクライアントは、次のように動作します。

- iSNS クライアントは、使用するとアクセスできる iSCSI ポータルおよびすべての iSCSI デバイスを iSNS サーバーに登録します。
- iSNS サーバは、iSNS クライアントに次のサービスを提供します。
  - デバイス登録
  - ステート変更通知
  - リモート ドメイン検出サービス

iSNS クライアントとして動作するすべての iSCSI デバイス（イニシエータおよびターゲットの両方）を、iSNS サーバーに登録できます。iSCSI イニシエータはその後 iSNS サーバーに対しターゲットのリストをクエリーできます。iSNS サーバーは応答として、クエリーの送信元クライアントが設定されているアクセス コントロール パラメータに基づいてアクセスできるターゲットのリストを提供します。

Cisco MDS 9000 ファミリ スイッチは、iSNS クライアントとして動作可能であり、使用可能なすべての iSCSI ターゲットを外部 iSNS サーバーに登録できます。IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールが搭載されている Cisco MDS 9000 ファミリのスイッチはすべて、iSNS サーバ機能をサポートします。したがって、iSCSI 発信元などの外部 iSNS クライアントをスイッチに登録し、SAN で使用可能なすべての iSCSI ターゲットを検出できます。

このセクションは、次のトピックで構成されています。

iSNS クライアント機能の概要

Internet Storage Name Service（iSNS）を使用すると、iSCSI デバイスの検出、管理、および設定の自動化により、既存の TCP/IP ネットワークが SAN としてより効率的に機能できるようになります。iSNS クライアントは、使用するとアクセスできる iSCSI ポータルおよびすべての iSCSI デバイスを iSNS サーバーに登録します。iSNS クライアントとして動作するすべての iSCSI デバイス（発信側およびターゲットの両方）を、iSNS サーバーに登録できます。iSNS クライアントが iSNS サーバーにオブジェクトを登録/登録解除できない場合（クライアントが iSNS サーバーに TCP 接続できない場合など）、この iSNS クライアントは継続的に、関連するインターフェイスのすべての iSNS オブジェクトを iSNS サーバーに再登録しようとします。

各 IPS インターフェイス（ギガビット イーサネット インターフェイス、サブインターフェイス、またはポート チャネル）の iSNS クライアント機能によって、iSNS サーバーに情報が登録されます。

インターフェイスにプロファイルをタグ付けすると、スイッチはプロファイル内の iSNS サーバー IP アドレスへの TCP 接続を開始し（既知の iSNS ポート番号 3205 を使用）、ネットワーク エンティティおよびポータル オブジェクトを登録します。IPS インターフェイスごとに一意のエンティティが対応付けられます。スイッチはさらに、ファイバ チャネル ネーム サーバー（FCNS）データベースおよびスイッチの設定を検索し、iSNS サーバーに登録するストレージ ノードを検出します。

FCNS データベースにファイバ チャネル pWWN が対応付けられていて、アクセス コントロールが設定されていない場合は、スタティックにマッピングされた仮想ターゲットが登録されます。ダイナミック ターゲット インポートがイネーブルの場合は、ダイナミックにマッピングされたターゲットが登録されます。iSCSI がファイバチャネル ターゲットをインポートする方法の詳細については、「iSCSI ターゲットとしてのファイバ チャネル ターゲットの表示」を参照してください。

設定変更（アクセス コントロールの変更、ダイナミック インポートのディセーブル化など）が発生したために、またはファイバチャネル ストレージ ポートがオフラインになったために、ストレージ ノードを使用できなくなった場合は、ストレージ ノードが iSNS サーバーから登録解除されます。ストレージ ノードがオンラインに戻ると、ストレージ ノードが再登録されます。

iSNS クライアントが iSNS サーバーにオブジェクトを登録/登録解除できない場合（クライアントが iSNS サーバーに TCP 接続できない場合など）、この iSNS クライアントは継続的に、関連するインターフェイスのすべての iSNS オブジェクトを iSNS サーバーに再登録しようとします。iSNS クライアントで使用される登録インターバル値は 15 分です。クライアントがこのインターバルの間に登録を更新できなかった場合、サーバーはエントリの登録を解除します。

プロファイルのタグ付けを解除すると、ネットワーク エンティティおよびポータルも該当するインターフェイスから登録解除されます。

（注） iSNS クライアントは VRRP インターフェイスではサポートされません。

iSNS クライアント プロファイルの作成

iSNS プロファイルを作成するには、次のステップを実行します。

手順

ステップ 1 MyIsns と呼ばれるプロファイルを作成します。

```
switch# config terminal
switch(config)# isns profile name MyIsns
switch(config-isns-profile)#
```

ステップ 2 このプロファイルに iSNS サーバの IPv4 アドレスを指定します。

```
switch(config-isns-profile)# server 10.10.100.211
```

ステップ 3 このプロファイルから構成されている iSNS サーバを削除します。

```
switch(config-isns-profile)# no server 10.10.100.211
```

ステップ 4 このプロファイルに iSNS サーバの IPv6 アドレスを指定します。

```
switch(config-isns-profile)# server 2003::11
```

ステップ 5 このプロファイルから構成されている iSNS サーバを削除します。

```
switch(config-isns-profile)# no server 10.20.100.211
```

インターフェイスにプロファイルをタグ付け

インターフェイスにプロファイルをタグ付けするには、次の手順を実行します。

手順

ステップ 1 次の構成モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 指定されたギガビット イーサネット インターフェイスを構成します。

```
switch(config)# interface gigabitethernet 4/1
switch(config-if)#
```

ステップ 3 インターフェイスにプロファイルをタグ付けします。

```
switch(config-if)# isns MyIsns
```

ステップ 4 インターフェイスからプロファイルのタグ付けを解除します。

```
switch(config-if)# no isns OldIsns
```

iSNS クライアント構成の確認

構成された iSNS プロファイルの表示：

構成された iSNS プロファイルを表示するには、**show isns profile** コマンドを使用します。プロファイル ABC には、iSNS サーバーに登録された 2 つのポータルがあります。各ポータルは、特定のインターフェイスに対応しています。プロファイル XYZ には指定された iSNS サーバがありますが、タグ付けされたインターフェイスは構成されていません。

構成された iSNS プロファイル情報の表示

```
switch# show isns profile
iSNS profile name ABC
tagged interface GigabitEthernet2/3
tagged interface GigabitEthernet2/2
iSNS Server 10.10.100.204

iSNS profile name XYZ
iSNS Server 10.10.100.211
```

指定した iSNS プロファイルの表示

```
switch# show isns profile ABC
iSNS profile name ABC
tagged interface GigabitEthernet2/3
tagged interface GigabitEthernet2/2
iSNS Server 10.10.100.204
```

タグ付きインターフェイスごとの iSNS PDU 統計情報を含む、すべての構成済みプロファイルの表示：

タグ付けされたインターフェイスごとに、設定されたすべてのプロファイルおよび iSNS PDU 統計情報を表示するには、**show isns profile counters** コマンドを使用します。

構成されたプロファイルおよび iSNS 統計情報の表示

```
switch# show isns profile counters
iSNS profile name ABC
tagged interface port-channel 1
iSNS statistics
Input 54 pdus (registration/deregistration pdus only)
Reg pdus 37, Dereg pdus 17
Output 54 pdus (registration/deregistration pdus only)
Reg pdus 37, Dereg pdus 17
iSNS Server 10.10.100.204

iSNS profile name XYZ
tagged interface port-channel 2
iSNS statistics
Input 30 pdus (registration/deregistration pdus only)
Reg pdus 29, Dereg pdus 1
Output 30 pdus (registration/deregistration pdus only)
Reg pdus 29, Dereg pdus 1
iSNS Server 10.1.4.218
```

指定したプロファイルの iSNS 統計情報の表示

```
switch# show isns profile ABC counters
iSNS profile name ABC
tagged interface port-channel 1
iSNS statistics
Input 54 pdus (registration/deregistration pdus only)
Reg pdus 37, Dereg pdus 17
Output 54 pdus (registration/deregistration pdus only)
Reg pdus 37, Dereg pdus 17
iSNS Server 10.10.100.204
```

iSNS サーバに登録されたオブジェクト、および所定のプロファイルで指定されたオブジェクトをすべて表示します。

iSNS サーバに登録されたオブジェクト、および所定のプロファイルで指定されたオブジェクトをすべて表示するには、**show isns** コマンドを使用します。

iSNS クエリの表示：

```
switch# show isns query ABC gigabitethernet 2/3
iSNS server: 10.10.100.204
Init: iqn.1991-05.com.w2k
Alias: <MS SW iSCSI Initiator>
Tgt : iqn.1987-05.com.cisco:05.172.22.94.22.02-03
Tgt : iqn.1987-05.com.cisco:05.172.22.94.22.02-03.210000203762fa34
nWWN: 200000203762fa34
```

インターフェイスがタグ付けされている iSNS プロファイルの表示

インターフェイスがタグ付けされた iSNS プロファイルを表示するには、**show interface** コマンドを使用します。

タグ付けされた iSNS インターフェイスの表示：

```
switch# show interface gigabitethernet 2/3
GigabitEthernet2/3 is up
Hardware is GigabitEthernet, address is 0005.3000.ae94
Internet address is 10.10.100.201/24
MTU 1500 bytes
Port mode is IPS
Speed is 1 Gbps
Beacon is turned off
Auto-Negotiation is turned on
iSNS profile ABC
^^^^^^^^^^^^^^^^
5 minutes input rate 112 bits/sec, 14 bytes/sec, 0 frames/sec
5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
1935 packets input, 132567 bytes
4 multicast frames, 0 compressed
0 input errors, 0 frame, 0 overrun 0 fifo
1 packets output, 42 bytes, 0 underruns
0 output errors, 0 collisions, 0 fifo
0 carrier errors
```

iSNS サーバ機能

イネーブルの場合、Cisco 9000 ファミリ MDS スイッチ上の iSNS サーバーは登録されているすべての iSCSI デバイスを追跡します。その結果、iSNS クライアントは iSNS サーバーにクエリーを送信することによって、他の iSNS クライアントを突き止めることができます。iSNS サーバーは次の機能も提供します。

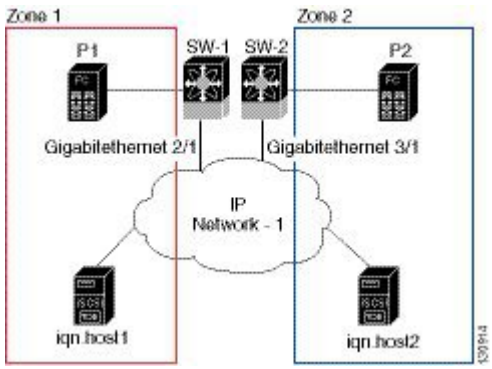
- iSNS クライアントを登録および登録解除できるようにします。また、iSNS クライアントから iSNS サーバーに登録されている他の iSNS クライアントを照会できるようにします。
- 特定の発信側からターゲットへのアクセスを許可または拒否する、アクセス コントロールの実施を集中管理します。

- 登録されている iSNS クライアントが、他の iSNS クライアントのステータス変更に関する変更通知を受け取るための通知方式を提供します。
- ファイバ チャネル デバイスと iSCSI デバイスの両方について、1 つのアクセス コントロール設定で対応できます。
- iSCSI 発信側に直接 IP 接続していない iSCSI ターゲットを検出します。

シナリオ例

iSNS サーバーは、ファイバ チャネルのゾーン分割情報と、iSCSI アクセス コントロール情報および設定の両方を利用することによって、ファイバ チャネル デバイスと iSCSI デバイスにまたがって、統一されたアクセス コントロールを提供します。iSNS クライアントとして動作する iSCSI 発信側だけが、両方のアクセス コントロール情報に基づいてアクセスが許可されるデバイスを検出します。次の図は、このシナリオの例を示しています。

図 *44 : Cisco MDS* 環境における *iSNS* サーバーの使用例



上の図で、iqn.host1 および iqn.host2 は iSCSI イニシエータです。P1 および P2 はファイバ チャネル ターゲットです。2 つのイニシエータはそれぞれ異なるゾーンにあります。ゾーン 1 は iqn.host1 およびターゲット P1 からなり、ゾーン 2 は iqn.host2 およびターゲット P2 からなります。iSNS サーバー機能は両方のスイッチ（SW-1 および SW-2）で有効です。登録処理の流れは、次のとおりです。

1. 発信側 iqn.host1 が SW-1 のポート Gigabitethernet2/1 に登録されます。
2. 発信側 iqn.host2 が SW-2 のポート Gigabitethernet3/1 に登録されます。
3. 発信側 iqn.host1 が SW-1 に iSNS クエリーを送信し、アクセス可能なすべてのターゲットを調べます。
4. 次に iSNS サーバーがファイバ チャネル ネーム サーバー（FCNS）にクエリーを送信し、クエリー元からアクセス可能な（つまり、同じゾーン内の）デバイスのリストを取得します。このクエリーの結果は P1 だけです。
5. iSNS サーバーは次に自身のデータベースに問い合せ、ファイバ チャネル デバイスを対応する iSCSI ターゲットに変換します。これは仮想ターゲット、そのアクセス コントロールの設定、ダイナミック ファイバ チャネル ターゲット インポート機能がイネーブルなのかディセーブルなのかといった iSCSI の設定に基づいて行われます。

6. iSNS サーバーはクエリーの発信側に応答を戻します。この応答には、iSNS サーバーが認識しているすべての iSCSI ポータルを記したリストが含まれます。したがって、iqn.host1 は SW-1（Gigabitethernet 2/1）または SW-2（Gigabitethernet 3/1）のどちらからターゲット P1 にログインするかを選択できます。
7. 発信側が SW-1 へのログインを選択し、あとでポートがアクセス不能になった場合（Gigabitethernet 2/1 の停止など）、発信側は代わりに SW-2 のポート Gigabitethernet 3/1 からターゲット P1 への接続に移行することを選択できます。
8. ターゲットが停止するか、またはゾーンから除去された場合、iSNS サーバーは発信側に iSNS State Change Notification（SCN）メッセージを送信し、発信側がセッションを削除できるようにします。

iSNS サーバの構成

ここでは、Cisco MDS 9000 ファミリ スイッチ上で iSNS サーバーを設定する方法について説明します。

このセクションは、次のトピックで構成されています。

iSNS サーバの有効化

iSNS サーバーをイネーブルにするには、次の手順を実行します。

始める前に

iSNS サーバ機能を有効にする前に、iSCSI を有効にする必要があります（「iSCSI の有効化」を参照）。iSCSI をディセーブルにすると、自動的に iSNS がディセーブルになります。スイッチ上で iSNS サーバーがイネーブルになると、対応する iSCSI インターフェイスがアップ状態であるすべての IPS ポートで、外部 iSNS クライアントからの iSNS 登録およびクエリー要求に応じられるようになります。

手順

ステップ 1 iSNS サーバを有効にします。

```
switch# config terminal
switch(config)# isns-server enable
```

ステップ 2 iSNS サーバを無効にします（デフォルト）。

```
switch(config)# no isns-server enable
```

iSNS の構成配信

iSNS 構成の配信を有効にするには、次のステップを実行します。

始める前に

CFS インフラストラクチャを使用すると、ファブリック全域の iSNS サーバーに iSCSI 発信側の設定を配信できます。したがって、どのスイッチ上で動作している iSNS サーバーであっても、クエリーの送信元である iSNS クライアントに、ファブリックの任意の場所で使用できる iSCSI デバイスのリストを提供できます。CFS の詳細については、『Cisco Fabric Manager システム管理構成ガイド』『Cisco MDS 9000 ファミリ NX-OS システム管理構成ガイド』を参照してください。

手順

ステップ 1 CFS インフラストラクチャを使用して、iSCSI 仮想ターゲット構成をファブリック内のすべてのスイッチに配信します。

```
switch# config terminal
switch(config)# isns distribute
```

ステップ 2 iSCSI 仮想ターゲット構成のファブリック内のすべてのスイッチへの配信を停止します（デフォルト）。

```
switch(config)# no isns distribute
```

ESI 再試行カウントの設定

iSNS クライアントは iSNS プロファイルを使用して、設定されている iSNS サーバーに情報を登録します。クライアントは登録時に、60 秒以上のエンティティ ステータス照会（ESI）インターバルを指定できます。クライアントが ESI インターバルをゼロ（0）に設定して登録した場合、サーバーは ESI を使用したクライアントのモニタリングを行いません。このような場合、クライアントの登録は明示的に登録解除されるまで、または iSNS サーバー機能がディセーブルになるまで有効です。

ESI 再試行カウントは、iSNS サーバーが iSNS クライアントにそれぞれのエンティティ ステータスを問い合せる回数です。デフォルトの ESI 再試行カウントは 3 です。クライアントはサーバーに、引き続きアライブ状態であることを伝える応答を送信します。設定された回数だけ再試行しても、クライアントが応答できなかった場合、そのクライアントはサーバーから登録解除されます。

iSNS サーバの ESI 再試行回数を構成するには、次のステップを実行します。

手順

ステップ 1 クライアントへの接続を最大 6 回再試行するように ESI を構成します。指定できる範囲は 1 ～ 10 です。

```
switch# config terminal
switch(config)# isns esi retries 6
```

ステップ 2 デフォルト値の 3 回の再試行に戻します。

```
switch(config)# no isns esi retries 6
```

登録期間の設定

iSNS クライアントは、iSNS サーバーへの登録期間を指定します。iSNS サーバーはこの期間が終了するまで、登録をアクティブなものとして維持します。この期間内に iSNS クライアントからコマンドが送信されなかった場合、iSNS サーバーはデータベースからクライアントの登録を削除します。

iSNS クライアントが登録期間を指定しなかった場合、iSNS サーバーはデフォルトの 0 が指定されたものとして、登録を無限にアクティブにしておきます。MDS iSNS サーバー上で登録期間を手動設定することもできます。

iSNS サーバ上で登録期間を構成するには、次のステップを実行します。

手順

ステップ 1 登録を 300 秒間アクティブに構成します。有効な登録期間の範囲は 0 ～ 65536 秒です。

```
switch# config terminal
switch(config)# isns registration period 300
```

ステップ 2 クライアントが登録したタイムアウト値、またはデフォルト値の 0 に戻します。

```
switch(config)# no isns registration period
```

iSNS クライアントの登録および登録解除

show isns database コマンドを使用すると、登録されているすべての iSNS クライアントとそれらに関連付けられた構成を表示できます。

iSNSクライアントは、登録するまでiSNSサーバに問い合わせることができません。iSNS クライアントの登録解除は、明示的に行うことも、iSNS サーバーが（ESI モニタリングによって）クライアントに到達できないことを検出した時点で行われることもあります。

iSNS クライアントの登録および登録解除によって、ステータス変更通知（SCN）が生成され、関係するすべての iSNS クライアントに送信されます。

ターゲットの検出

iSCSI 発信側は、iSNS サーバーにクエリーを送信することによってターゲットを検出します。サーバはターゲット リストを検索する DevGetNext 要求をサポートします。また、接続先 IP アドレスまたはポート番号など、ターゲットおよびポータルの詳細を調べる DevAttrQuery をサポートします。

iSNS クライアントからクエリー要求を受信した iSNS サーバーは、FCNS に問い合せて、クエリー元である発信側がアクセスできるファイバ チャネル ターゲットのリストを取得します。このクエリーの結果は、発信側のその時点でアクティブなゾーン分割の設定および現在の設定（複数可）によって決まります。iSNS サーバーはその後、iSCSI ターゲットの設定（仮想ターゲットおよびダイナミック インポート設定）を使用して、ファイバ チャネル ターゲットを同等の iSCSI ターゲットに変換します。この段階で、仮想ターゲットにアクセス コントロールが設定されている場合は、それも適用されます。さらに、ターゲットの詳細を記した応答メッセージがクエリー発信側に戻されます。

iSNS サーバーは、可能性のあるターゲットおよびポータルをすべて指定し、統合した応答をクエリー元である発信側に送信します。たとえば、ファイバ チャネル ターゲットがさまざまな IPS インターフェイス上で異なる iSCSI ターゲットとしてエクスポートされる場合、iSNS サーバーは可能性のあるすべての iSCSI ターゲットおよびポータルを示したリストで応答します。

最新のターゲット リストを維持するために、iSNS サーバーは iSCSI ターゲットが到達可能または到達不能になるたびに、クライアントにステート変更通知（SCN）を送信します。クライアントはその場合、iSNS クエリーをもう一度開始することによって、アクセス可能なターゲットのリストを再検出することが想定されています。iSCSI ターゲットの到達可能性が変化するのは、次のいずれかが発生した場合です。

- ターゲットがアップまたはダウンする。
- FC ターゲットのダイナミック インポート設定が変更される。
- ゾーン セットが変更される。
- デフォルトのゾーン アクセス コントロールが変更される。
- IPS インターフェイスのステートが変化する。
- イニシエータの構成変更によって、ターゲットがアクセス可能またはアクセス不能になる。

iSNS サーバ構成の確認

iSNS データベースに関する ESI インターバルおよび要約情報の表示

ESI インターバルおよび iSNS データベースの内容に関するサマリ情報を確認するには、**show isns config** コマンドを使用します（ を参照）。

ESI インターバルおよびデータベースの内容の iSNS サーバ構成の表示：

```
switch# show isns config
Server Name: switch1(Cisco Systems) Up since: Fri Jul 30 04:08:16 2004
Index: 1 Version: 1 TCP Port: 3205
fabric distribute (remote sync): ON
ESI
Non Response Threshold: 5 Interval(seconds): 60
Database contents
Number of Entities: 2
Number of Portals: 3
```

```
Number of ISCSI devices: 4
Number of Portal Groups: 0
```

iSNS データベースの内容に関する詳細情報の表示：

iSNS データベースの内容に関する詳細情報を表示するには、**show isns database**コマンドを使用しま。このコマンドは、iSNS データベースの情報（データベースに登録されているすべてのエンティティ、ノード、およびポータル）を表示します。このコマンドでオプションを指定しない場合、明示的に登録されたオブジェクトだけが表示されます。VSAN ID の横のアスタリスクは、iSCSI ノードが VSAN のデフォルト ゾーンにあることを示します。

明示的に登録されているオブジェクトの表示

```
switch# show isns database
Entity Id: dp-204
Index: 2 Last accessed: Fri Jul 30 04:08:46 2004
iSCSI Node Name: iqn.1991-05.comdp-2041
Entity Index: 2
Node Type: Initiator(2) Node Index: 0x1
SCN Bitmap: OBJ_UPDATED|OBJ ADDED|OBJ REMOVED|TARGET&SELF
Node Alias: <MS SW iSCSI Initiator>
VSANS: 1(*), 5(*)
Portal IP Address: 192.168.100.2 TCP Port: 4179
Entity Index: 2 Portal Index: 1
ESI Interval: 0 ESI Port: 4180 SCN Port: 4180
```

登録されたノードとポータル、および構成されたノードとポータルの完全なデータベースの表示

```
switch# show isns database full
Entity Id: isns.entity.mds9000
Index: 1 Last accessed: Fri Jul 30 04:08:16 2004

iSCSI Node Name: iqn.com.cisco.disk1
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000001
WWN(s):
22:00:00:20:37:39:dc:45
VSANS:
iSCSI Node Name: iqn.isns-first-virtual-target
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000002

VSANS:
iSCSI Node Name: iqn.com.cisco.disk2
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000003
WWN(s):
22:00:00:20:37:39:dc:45

VSANS:
Portal IP Address: 192.168.100.5 TCP Port: 3205
Entity Index: 1 Portal Index: 3

Portal IP Address: 192.168.100.6 TCP Port: 3205
Entity Index: 1 Portal Index: 5

Entity Id: dp-204
Index: 2 Last accessed: Fri Jul 30 04:08:46 2004

iSCSI Node Name: iqn.1991-05.com.microsoft:dp-2041
Entity Index: 2
```

```
Node Type: Initiator(2) Node Index: 0x1
SCN Bitmap: OBJ_UPDATED|OBJ ADDED|OBJ REMOVED|TARGET&SELF
Node Alias: <MS SW iSCSI Initiator>

VSANS: 1(*), 5(*)
Portal IP Address: 192.168.100.2 TCP Port: 4179
Entity Index: 2 Portal Index: 1
ESI Interval: 0 ESI Port: 4180 SCN Port: 4180
```

（注） *local option* は、仮想ターゲットにのみ使用可能です。

ローカル スイッチの仮想ターゲット情報の表示：

```
switch# show isns database virtual-targets local
Entity Id: isns.entity.mds9000
Index: 1 Last accessed: Fri Jul 30 04:08:16 2004

iSCSI Node Name: iqn.com.cisco.disk1
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000001
WWN(s):
22:00:00:20:37:39:dc:45

VSANS:
iSCSI Node Name: iqn.isns-first-virtual-target
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000002

VSANS:
iSCSI Node Name: iqn.com.cisco.disk2
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000003
WWN(s):
22:00:00:20:37:39:dc:45

VSANS:
Portal IP Address: 192.168.100.5 TCP Port: 3205
Entity Index: 1 Portal Index: 3

Portal IP Address: 192.168.100.6 TCP Port: 3205
Entity Index: 1 Portal Index: 5
```

指定したスイッチの仮想ターゲットの表示：

```
switch# show isns database virtual-targets switch 20:00:00:0d:ec:01:04:40
Entity Id: isns.entity.mds9000
Index: 1 Last accessed: Fri Jul 30 04:08:16 2004

iSCSI Node Name: iqn.com.cisco.disk1
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000001
WWN(s):
22:00:00:20:37:39:dc:45

VSANS:
iSCSI Node Name: iqn.isns-first-virtual-target
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000002

VSANS:
iSCSI Node Name: iqn.com.cisco.disk2
```

```
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000003
WWN(s):
22:00:00:20:37:39:dc:45

VSANS:
Portal IP Address: 192.168.100.5 TCP Port: 3205
Entity Index: 1 Portal Index: 3

Portal IP Address: 192.168.100.6 TCP Port: 3205
Entity Index: 1 Portal Index: 5
```

iSNS サーバに登録されたノードの属性の表示：

iSNS サーバに登録されているノードの属性を表示するには、**show isns node** コマンドを使用します。オプションを指定しない場合、名前とノードタイプ属性が 1 行に 1 つずつ簡潔に表示されます。

明示的に登録されているオブジェクトの表示：

```
switch# show isns node all
--------------------------------------------------------------------------------
iSCSI Node Name Type
--------------------------------------------------------------------------------
iqn.1987-05.com.cisco:05.switch1.02-03.22000020375a6c8 Target
...
iqn.com.cisco.disk1 Target
iqn.com.cisco.ipdisk Target
iqn.isns-first-virtual-target Target
iqn.1991-05.cw22 Target
iqn.1991-05.cw53 Target
```

指定したノードの表示

```
switch# show isns node name iqn.com.cisco.disk1
iSCSI Node Name: iqn.com.cisco.disk1
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000001
WWN(s):
22:00:00:20:37:39:dc:45
VSANS: 1
```

すべてのノードの属性詳細の表示

```
switch# show isns node all detail
iSCSI Node Name: iqn.1987-05.com.cisco:05.switch1.02-03.22000020375a6c8f
Entity Index: 1
Node Type: Target(1) Node Index: 0x3000003
Configured Switch WWN: 20:00:00:0d:ec:01:04:40
WWN(s):
22:00:00:20:37:5a:6c:8f
VSANS: 1
...
iSCSI Node Name: iqn.com.cisco.disk1
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000001
Configured Switch WWN: 20:00:00:0d:ec:01:04:40
WWN(s):
22:00:00:20:37:39:dc:45
VSANS: 1

iSCSI Node Name: iqn.com.cisco.ipdisk
Entity Index: 1
```

```
Node Type: Target(1) Node Index: 0x80000002
Configured Switch WWN: 20:00:00:0d:ec:01:04:40
WWN(s):
22:00:00:20:37:5a:70:1a
VSANS: 1

iSCSI Node Name: iqn.isns-first-virtual-target
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000003
Configured Switch WWN: 20:00:00:0d:ec:01:04:40

iSCSI Node Name: iqn.parna.121212
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000004
Configured Switch WWN: 20:00:00:0d:ec:01:04:40

iSCSI Node Name: iqn.parna.121213
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000005
Configured Switch WWN: 20:00:00:0d:ec:01:04:40
```

ポータルの属性とそのアクセス可能なノードの表示：

ポータルの属性をアクセス可能なノードとともに表示するには、**show isns portal** コマンドを使用します。スイッチの WWN とインターフェイスの組み合わせ、または IP アドレスとポート番号の組み合わせを使用して、ポータルを指定できます。

すべてのポータルの属性情報の表示：

```
switch# show isns portal all
--------------------------------------------------------------------------------
IPAddress TCP Port Index SCN Port ESI port
--------------------------------------------------------------------------------
192.168.100.5 3205 3 - -
192.168.100.6 3205 5 - -
```

すべてのポータルの詳細な属性情報の表示：

```
switch# show isns portal all detail
Portal IP Address: 192.168.100.5 TCP Port: 3205
Entity Index: 1 Portal Index: 3

Portal IP Address: 192.168.100.6 TCP Port: 3205
Entity Index: 1 Portal Index: 5
```

仮想ポータルの表示：

```
switch# show isns portal virtual
--------------------------------------------------------------------------------
IPAddress TCP Port Index SCN Port ESI port
--------------------------------------------------------------------------------
192.168.100.5 3205 3 - -
192.168.100.6 3205 5 - -
```

指定したスイッチの仮想ポータルの表示：

```
switch# show isns portal virtual switch 20:00:00:0d:ec:01:04:40
--------------------------------------------------------------------------------
IPAddress TCP Port Index SCN Port ESI port
--------------------------------------------------------------------------------
192.168.100.5 3205 3 - -
192.168.100.6 3205 5 - -
```

指定したスイッチの仮想ポータルの詳細情報の表示：

```
switch# show isns portal virtual switch 20:00:00:0d:ec:01:04:40 detail
Portal IP Address: 192.168.100.5 TCP Port: 3205
Entity Index: 1 Portal Index: 3
Switch WWN: 20:00:00:0d:ec:01:04:40
Interface: GigabitEthernet2/3

Portal IP Address: 192.168.100.6 TCP Port: 3205
Entity Index: 1 Portal Index: 5
Switch WWN: 20:00:00:0d:ec:01:04:40
Interface: GigabitEthernet2/5
```

エンティティの属性をエンティティ内のポータルとノードのリストとともに表示します。

エンティティの属性をエンティティ内のポータルとノードのリストとともに表示するには、**show isns entity** コマンドを使用します。オプションを指定しない場合、エンティティに関連付けられたノードまたはポータルのエンティティ ID および番号が、1 行に 1 つずつ簡潔に表示されます

登録されているすべてのエントリの表示：

```
switch1# show isns entity
--------------------------------------------------------------------------------
Entity ID Last Accessed
--------------------------------------------------------------------------------
dp-204 Tue Sep 7 23:15:42 2004
```

データベース内のすべてのエンティティの表示：

```
switch# show isns entity all

--------------------------------------------------------------------------------
Entity ID Last Accessed
--------------------------------------------------------------------------------
isns.entity.mds9000 Tue Sep 7 21:33:23 2004

dp-204 Tue Sep 7 23:15:42 2004
```

指定した ID のエンティティの表示：

```
switch1# show isns entity id dp-204
Entity Id: dp-204
Index: 2 Last accessed: Tue Sep 7 23:15:42 2004
```

データベース内のすべてのエンティティの詳細情報の表示：

```
switch1# show isns entity all detail
Entity Id: isns.entity.mds9000
Index: 1 Last accessed: Tue Sep 7 21:33:23 2004

Entity Id: dp-204
Index: 2 Last accessed: Tue Sep 7 23:16:34 2004
```

仮想エンティティの表示：

```
switch# show isns entity virtual
Entity Id: isns.entity.mds9000
Index: 1 Last accessed: Thu Aug 5 00:58:50 2004

Entity Id: dp-204
Index: 2 Last accessed: Thu Aug 5 01:00:23 2004
```

インポート ターゲットに関する情報の表示

show iscsi global config コマンドを使用して、インポート ターゲットに関する情報を表示します。

指定したスイッチのインポート ターゲット設定の表示：

```
switch# show isns iscsi global config switch 20:00:00:05:ec:01:04:00
iSCSI Global configuration:
Switch: 20:00:00:05:ec:01:04:00 iSCSI Auto Import: Enabled
```

すべてのスイッチのインポート ターゲット設定の表示：

```
switch# show isns iscsi global config all
iSCSI Global configuration:
Switch: 20:00:44:0d:ec:01:02:40 iSCSI Auto Import: Enabled
```

iSNS アプリケーションの CFS ピア スイッチ情報の表示

iSNS アプリケーションに関する CFS ピア スイッチ情報を表示するには、**show cfs peers** コマンドを使用します。

iSNS アプリケーションの CFS ピア スイッチ情報の表示：

```
switch# show cfs peers name isns

Scope : Physical
--------------------------------------------------
Switch WWN IP Address
--------------------------------------------------
20:00:00:00:ec:01:00:40 10.10.100.11 [Local]

Total number of entries = 1
```

iSNS Cloud Discovery

iSNS クラウド検出を設定することによって、IP ネットワーク内の iSNS サーバーを検出する処理を自動化できます。

この項では、次のトピックについて取り上げます。

- クラウド検出
- iSNS クラウド検出の設定
- クラウド検出ステータスの確認
- クラウド検出メンバーシップの確認
- クラウド検出統計情報の表示

クラウド検出

クエリー要求を受信した iSNS サーバーは、発信側がターゲットに到達するために通過できる、使用可能なターゲットおよびポータルのリストで応答します。MDS スイッチ外部の IP ネットワーク設定によって、発信側から到達できるのがギガビット イーサネット インターフェイス

のサブセットだけになる場合があります。発信側に戻されたポータルセットに到達できるようにするには、所定の発信側から到達できるギガビット イーサネット インターフェイス セットを iSNS サーバーで認識する必要があります。

（注） iSNS クラウド検出は、Cisco Fabric Switch for IBM BladeCenter および Cisco Fabric Switch for HP c-Class BladeSystem ではサポートされません。

iSNS クラウド検出機能は、スイッチ上のインターフェイスをばらばらの IP クラウドに分割することによって、発信側から到達できる各種インターフェイスの情報を iSNS サーバーに提供します。この検出では、その時点でアップしている他のあらゆる既知の IPS ポートにメッセージを送信し、応答（または応答がないこと）によって、リモート IPS ポートが同一 IP ネットワークにあるのか、それとも別の IP ネットワークにあるのかを判別します。

クラウド検出は、次のイベントが発生したときに開始されます。

- CLI からの手動要求によって、CLI からクラウド検出が開始される。この動作によって、既存のメンバーシップが破棄され、新しいメンバーシップが作成されます。
- インターフェイスの自動検出により、インターフェイスが適切なクラウドに割り当てられる。他のすべてのクラウドメンバーは影響を受けません。各クラウドのメンバーシップは増分方式で作成され、次のイベントによって開始されます。
  - ギガビット イーサネット インターフェイスがアップする（ローカルまたはリモート ギガビット イーサネット インターフェイス）。
  - ギガビット イーサネット インターフェイスの IP アドレスが変更される。
  - ポートの VRRP 設定が変更される。

iSNS サーバーは CFS を使用して、あらゆるスイッチにクラウドおよびメンバーシップ情報を配信します。したがって、ファブリック内のすべてのスイッチでクラウド メンバーシップ ビューが一致します。

（注） iSNS クラウド検出で CFS 配信が正しく行われるようにするには、ファブリック内のすべてのスイッチで Cisco SAN-OS Release 3.0(1) または NX-OS 4.1(1b) 以降が稼働している必要があります。

iSNS クラウド検出の設定

ここでは、iSNS クラウド検出の設定方法について説明します。

- iSNS クラウド検出のイネーブル化
- オンデマンド型 iSNS クラウド検出の開始
- iSNS クラウド自動検出の設定

- iSNS クラウド自動検出構成の確認
- iSNS クラウド検出の設定
- iSNS クラウド検出メッセージ タイプの設定

iSNS クラウド検出のイネーブル化

iSNS クラウド検出を有効にするには、次のステップを実行します。

手順

ステップ 1 iSNS クラウド検出を有効にします。

```
switch# config terminal
switch(config)# cloud-discovery enable
```

ステップ 2 iSNS クラウド検出を無効にします（デフォルト）。

```
switch(config)# no cloud-discovery enable
```

オンデマンド型 iSNS クラウド検出の開始

オンデマンドの iSNS クラウド検出を開始するには、EXEC モードで **cloud discover** コマンドを使用します。

次に、ファブリック全体のオンデマンド クラウド検出を開始する例を示します。

```
switch# cloud discover
```

iSNS クラウド自動検出の設定

iSNS クラウド自動検出を構成するステップは、次のとおりです。

手順

ステップ 1 iSNS クラウド自動検出を有効にします（デフォルト）。

```
switch# config terminal
switch(config)# cloud discovery auto
```

ステップ 2 iSNS クラウド自動検出を無効にします。

```
switch(config)# no cloud discovery auto
```

ステップ 3 iSNS クラウド自動検出構成の確認：

```
switch# show cloud discovery config
Auto discovery: Enabled
```

iSNS クラウド検出の配信の構成

CFS を使用した iSNS クラウド検出配信を設定するには、次の手順を実行します。

手順

ステップ 1 iSNS クラウド検出ファブリック配信を有効にします（デフォルト）。

```
switch# config terminal
switch(config)# cloud discovery fabric distribute
```

ステップ 2 iSNS クラウド検出ファブリック配信を無効にします。

```
switch(config)# no cloud discovery fabric distribute
```

iSNS クラウド検出メッセージ タイプの設定

使用する iSNS クラウド検出メッセージのタイプを設定できます。デフォルトで、iSNS クラウド検出では ICMP が使用されます。

iSNS クラウド検出メッセージのタイプを設定するには、次の手順を実行します。

手順

ステップ 1 次の構成モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 ICMP メッセージを使用する iSNS クラウド検出を有効にします（デフォルト）。

```
switch(config)# cloud discovery message icmp
```

（注）
ICMP メッセージだけがサポートされています。

クラウド検出ステータスの確認

クラウド検出動作のステータスを確認するには、**show cloud discovery status** コマンドを使用します。

```
switch# show cloud discovery status
Discovery status: Succeeded
```

クラウド検出メンバーシップの確認

スイッチのクラウド メンバーシップを確認するには **show cloud membership all** コマンドを使用します。

```
switch# show cloud membership all
Cloud 2
GigabitEthernet1/5[20:00:00:0d:ec:02:c6:c0] IP Addr 10.10.10.5
GigabitEthernet1/6[20:00:00:0d:ec:02:c6:c0] IP Addr 10.10.10.6
#members=2
```

スイッチの未解決メンバーシップを確認するには **show cloud membership unresolved** コマンドを使用します。

```
switch# show cloud membership unresolved
Undiscovered Cloud
No members
```

クラウド検出動作の統計情報を確認するには、**show cloud discovery statistics** コマンドを使用します。

```
switch# show cloud discovery statistics
Global statistics
Number of Auto Discovery = 1
Number of Manual Discovery = 0
Number of cloud discovery (ping) messages sent = 1
Number of cloud discovery (ping) success = 1
```

デフォルト設定

次の表に、iSCSI パラメータのデフォルト設定を示します。

表 *8 :* デフォルトの *iSCSI* パラメータ

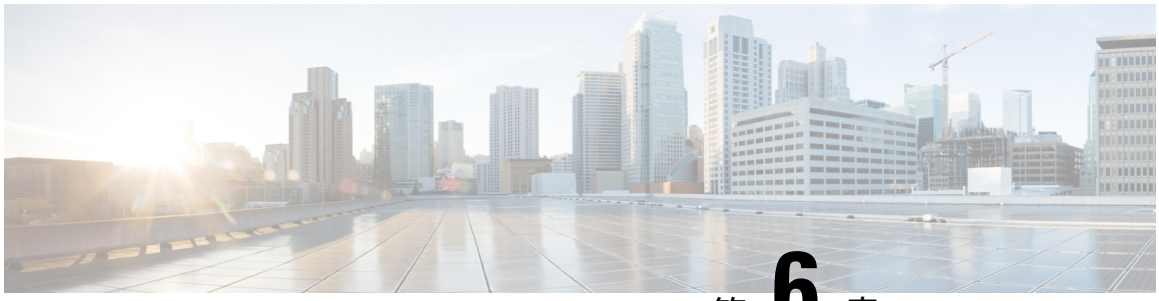
パラメータ	デフォルト
TCP 接続の数	iSCSI セッションごとに 1 つ
minimum-retransmit-time	300 ミリ秒
keepalive-timeout	60 秒
max-retransmissions	4 回
PMTU ディスカバリ	イネーブル
pmtu-enable reset-timeout	3600 秒
SACK	イネーブル
max-bandwidth	1 Gbps
min-available-bandwidth	70 Mbps
round-trip-time	1 ミリ秒
バッファ サイズ	4096 KB
制御 TCP およびデータ接続	パケットの送信なし
TCP 輻輳ウィンドウ モニタリング	イネーブル

パラメータ	デフォルト
バースト サイズ	50 KB
ジッタ	500 マイクロ秒
TCP 接続モード	アクティブ モードがイネーブル
iSCSI へのファイバ チャネル ターゲット	未インポート
iSCSI ターゲットのアドバタイズ	すべてのギガビット イーサネット インターフェイス、サブインターフェイス、ポートチャネル インターフェイス、およびポート チャネル サブインターフェイスでアドバタイズ
仮想ファイバ チャネル ホストへの iSCSI ホストのマッピング	ダイナミック マッピング
ダイナミック iSCSI 発信側	VSAN 1 のメンバー
発信側の識別	iSCSI ノード名
スタティック仮想ターゲットのアドバタイズ	仮想ターゲットへのアクセスを許可されているイニシエータはありません（明示的に設定されている場合を除く）
iSCSI ログイン認証	CHAP または非認証メカニズム
revert-primary-port	ディセーブル
ヘッダーおよびデータ ダイジェスト	iSCSI発信側が要求を送信した時点で自動的にイネーブル。ストアアンドフォワードモードの場合、この機能は設定不可および使用不可
iSNS 登録インターバル	60 秒（設定不可）
iSNS 登録インターバルの再試行回数	3
ファブリック配信	ディセーブル

次の表に、iSLB パラメータのデフォルト設定を示します。

表 *9:* デフォルト *iSLB*

ファブリック配信	ディセーブル
ロード バランシング メトリック	1000



第 6 章

IP サービスの設定

Cisco MDS 9000 ファミリ スイッチは、イーサネットとファイバ チャネル インターフェイス間で IP トラフィックをルーティングできます。VSAN 間でトラフィックをルーティングするには、IP スタティック ルーティング機能を使用します。この機能を使用するには、VSAN をそれぞれ異なる IP サブネットワークに配置する必要があります。各 Cisco MDS 9000 ファミリ スイッチは、ネットワーク管理システム（NMS）に対して次のサービスを提供します。

- スーパーバイザ モジュールの前面パネルにある帯域外イーサネット インターフェイス（mgmt0）での IP 転送
- IP over Fibre Channel（IPFC）機能を使用した帯域内ファイバ チャネル インターフェイスでの IP 転送：IPFC はカプセル化技術を使用してファイバ チャネル上で IP フレームを伝送する手順を規定します。IP フレームはファイバ チャネル フレームにカプセル化されるため、オーバーレイ イーサネット ネットワークを使用しなくても、ファイバ チャネル ネットワーク上で NMS 情報を伝達できます。
- IP ルーティング（デフォルト ルーティングおよびスタティック ルーティング）：外部ルータを必要としない設定の場合は、スタティック ルーティングを使用してデフォルト ルートを設定できます。

スイッチは仮想ルータ冗長プロトコル（VRRP）機能の RFC 2338 標準に準拠します。VRRP は、冗長な代替パスをゲートウェイ スイッチに提供する、再起動可能なアプリケーションです。

（注） Cisco MDS NX-OS リリース 8.3(1) 以降、VRRP 機能は Cisco MDS 9000 シリーズ スイッチでサポートされません。

IPv6 の設定については、ギガビット イーサネット インターフェイスでの IPv4 の構成 （257 ページ）を参照してください。

この章は、次の項で構成されています。

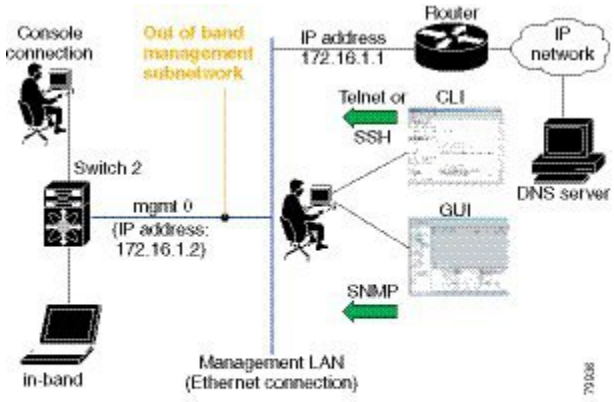
- トラフィック管理サービス （212 ページ）
- Management Interface Configuration （212 ページ）
- デフォルト ゲートウェイ （214 ページ）

• IPv4 デフォルト ネットワークの構成 （215 ページ）
• IP over Fibre Channel （217 ページ）
• IPv4 スタティックルート （222 ページ）
• オーバーレイ VSAN （224 ページ）
• DNS の設定 （229 ページ）
• DNS ホスト情報の表示 （230 ページ）
• DNS 機能のデフォルト設定 （231 ページ）

トラフィック管理サービス

帯域内オプションは RFC 2625 標準に準拠し、これに従います。ファイバ チャネル インターフェイス上で IP プロトコルが稼働する NMS ホストは、IPFC 機能を使用してスイッチにアクセスできます。NMS にファイバ チャネル HBA がない場合でも、いずれかのスイッチをファブリックへのアクセスポイントとして使用して、インバンド管理を実行できます（次の図を参照）。

図 *45 :* スイッチへの管理者アクセス



Management Interface Configuration

スイッチ上の管理インターフェイスは、同時に複数の Telnet または SNMP セッションを許可します。管理インターフェイスを介してスイッチを遠隔から設定できますが、スイッチにアクセスできるようにまずIPバージョン4（IPv4）パラメータ（IPアドレス、サブネットマスク）またはIPバージョン6（IPv6）アドレスおよびプレフィックス長を設定する必要があります。IPv6アドレスの構成については、ギガビット イーサネット インターフェイスでの IPv4 の構成（257 ページ） を参照してください。

ディレクタ クラスのスイッチでは、1 つの IP アドレスを使用してスイッチを管理します。アクティブなスーパーバイザ モジュールの管理（mgmt0）インターフェイスはこの IP アドレスを使用します。スタンバイ スーパーバイザ モジュール上の mgmt0 インターフェイスは非アクティブなままで、スイッチオーバーが発生するまでアクセスできません。スイッチオーバーが行われると、スタンバイ スーパーバイザ モジュール上の mgmt0 インターフェイスがアクティブになり、アクティブであったスーパーバイザ モジュールと同じ IP アドレスを引き継ぎます。

（注） MDS 管理インターフェイスが接続されているイーサネット スイッチ上のポートは、スイッチ ポートの代わりにホスト ポート（アクセス ポートともいう）として設定する必要があります。（イーサネット スイッチ上の）そのポートのスパニングツリー設定をディセーブルにする必要があります。これにより、（スパニングツリー設定がイネーブルであればイーサネット スイッチが実行する）イーサネット スパニングツリー処理の待ち時間による MDS 管理ポートの起動待ち時間を回避できます。Cisco イーサネット スイッチの場合は、Cisco IOS の **switchport host** コマンドまたは Catalyst OS の **set port host** コマンドのいずれかを使用します。イーサネット スイッチの設定ガイドを参照してください。

（注） 手動による管理インターフェイスの設定を始める前に、スイッチの IP アドレスと IP サブネット マスクを取得します。また、コンソール ケーブルがコンソール ポートに接続されていることを確認します。

ここでは、次の内容について説明します。

IPv4 の mgmt0 イーサネット インターフェイスの構成

IPv4 の mgmt0 イーサネット インターフェイスを構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface mgmt0**	管理イーサネット インターフェイス（mgmt0）でインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **ip address 10.1.1.1 255.255.255.0**	管理インターフェイスの IPv4 アドレス（10.1.1.1）および IPv4 サブネット マスク（255.255.255.0）を入力します。
ステップ 4	switch(config-if)# **no shutdown**	インターフェイスをイネーブルにします。

IPv6 の mgmt0 イーサネット インターフェイスの構成

IPv6 の mgmt0 イーサネット インターフェイスを構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface mgmt0**	管理イーサネットインターフェイス（mgmt0）でインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **ipv6 address 2001:0db8:800:200c::417a/64**	管理インターフェイスの IPv6 アドレス（2001:0DB8:800:200C::417A）および IPv6 プレフィックス長（/64）を入力し、インターフェイスの IPv6 処理を有効にします。
ステップ 4	switch(config-if)# **ipv6 enable**	インターフェイスのリンク ローカル IPv6 アドレスを自動的に設定し、インターフェイスの IPv6 処理を有効にします。
ステップ 5	switch(config-if)# **no shutdown**	インターフェイスをイネーブルにします。

デフォルト ゲートウェイ

Cisco MDS 9000 ファミリ スイッチで、デフォルト ゲートウェイ IPv4 アドレスを設定できます。

デフォルト ゲートウェイ IPv4 アドレスを設定する場合は、IPv4 スタティック ルーティング属性（IP デフォルト ネットワーク、送信先プレフィックス、送信先マスク、およびネクスト ホップ アドレス）も使用する必要があります。スタティック ルートの IP 転送およびデフォルト ネットワークの詳細を設定する場合は、デフォルト ゲートウェイがイネーブルであるか、またはディセーブルであるかに関係なく、これらの IPv4 アドレスが使用されます。

デフォルト ゲートウェイ IPv4 アドレスは、IPv4 スタティック ルーティング属性コマンド（IP デフォルト ネットワーク、送信先プレフィックス、送信先マスク、およびネクスト ホップ アドレス）とともに設定する必要があります。

ヒント　スタティック ルートの IP 転送およびデフォルト ネットワークの詳細を設定する場合は、デフォルト ゲートウェイがイネーブルであるか、またはディセーブルであるかに関係なく、これらの IPv4 アドレスが使用されます。これらの IP アドレスが設定されているにもかかわらず、使用できない場合、スイッチは代わりにデフォルト ゲートウェイ IP アドレスを使用します（デフォルト ゲートウェイ IP アドレスが設定されている場合）。スイッチのすべてのエントリに IP アドレスが設定されていることを確認してください。

スイッチのデフォルト ゲートウェイの IP アドレスを構成するには **ip default-gateway** コマンドを使用し、デフォルト ゲートウェイの IPv4 アドレスが構成されていることを確認するには **show ip route**コマンドを使用します。

このセクションは、次のトピックで構成されています。

デフォルト ゲートウェイの設定

デフォルト ゲートウェイを構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	構成モードに入ります。
ステップ 2	switch(config)# **ip default- gateway 1.12.11.1**	デフォルト ゲートウェイの IPv4 アドレスを設定します。

デフォルト ゲートウェイの構成の確認

デフォルト ゲートウェイの構成を確認するには、**show ip route** コマンドを使用します。

```
switch# show ip route
Codes: C - connected, S - static

Gateway of last resort is 1.12.11.1

S 5.5.5.0/24 via 1.1.1.1, GigabitEthernet1/1
C 1.12.11.0/24 is directly connected, mgmt0
C 1.1.1.0/24 is directly connected, GigabitEthernet1/1
C 3.3.3.0/24 is directly connected, GigabitEthernet1/6
C 3.3.3.0/24 is directly connected, GigabitEthernet1/5
S 3.3.3.0/24 via 1.1.1.1, GigabitEthernet1/1
```

IPv4 デフォルト ネットワークの構成

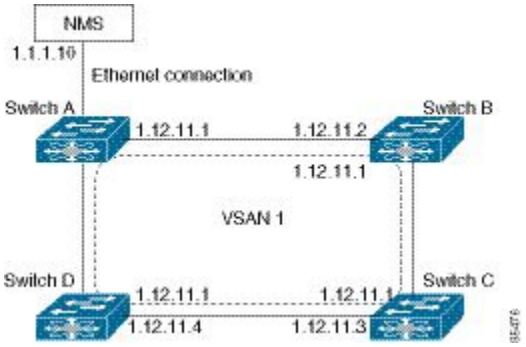
IPv4デフォルト ネットワーク アドレスが割り当てられている場合、スイッチはこのネットワークへのルートを最終的なルートと見なします。IPv4 デフォルト ネットワーク アドレスを使用

できない場合は、IPv4 デフォルト ゲートウェイ アドレスが使用されます。IPv4 デフォルト ネットワーク アドレスが設定された各ネットワークのルートは、デフォルト ルート候補としてフラグが設定されます（ルートが使用可能な場合）。

スタティック ルートの IP 転送およびデフォルト ネットワークの詳細を構成する場合は、デフォルト ゲートウェイが有効であるか、または無効であるかに関係なく、これらの IPv4 アドレスが使用されます。これらの IPv4 アドレスが設定されているにもかかわらず、使用できない場合、スイッチは代わりにデフォルト ゲートウェイ IPv4 アドレスを使用します（デフォルト ゲートウェイ IPv4 アドレスが設定されている場合）。IPv4 を使用している場合は、スイッチのすべてのエントリに IPv4 アドレスを設定するようにしてください。

イーサネット インターフェイスが設定されている場合、スイッチは IP ネットワークのゲートウェイ ルータを指していなければなりません。ホストはゲートウェイ スイッチを使用して、ゲートウェイにアクセスします。このゲートウェイ スイッチは、デフォルト ゲートウェイとして設定されます。ゲートウェイ スイッチと同じ VSAN に接続されたファブリック内の別のスイッチも、ゲートウェイ スイッチを通して接続できます。この VSAN に接続されたすべてのインターフェイスに、ゲートウェイ スイッチの VSAN IPv4 アドレスを構成する必要があります（次の図を参照）。

図 *46 :* オーバーレイ *VSAN* 機能



上の図で、スイッチ A の IPv4 アドレスは 1.12.11.1、スイッチ B の IPv4 アドレスは 1.12.11.2、スイッチ C の IPv4 アドレスは 1.12.11.3、スイッチ D の IPv4 アドレスは 1.12.11.4 です。スイッチ A はイーサネット接続されたゲートウェイ スイッチです。NMS は IPv4 アドレス 1.1.1.10 を使用して、ゲートウェイ スイッチに接続しています。オーバーレイされた VSAN 1 内の任意のスイッチに転送されるフレームは、ゲートウェイ スイッチを通してルーティングされます。他のスイッチにゲートウェイ スイッチの IPv4 アドレス（1.12.11.1）を設定すると、ゲートウェイ スイッチはフレームを目的の送信先に転送できるようになります。同様に、VSAN 内の非ゲートウェイ スイッチからイーサネット環境にフレームを転送する場合も、ゲートウェイ スイッチを通してフレームがルーティングされます。

転送がディセーブル（デフォルト）である場合、IP フレームはインターフェイス間で送信されません。このような場合、ソフトウェアは帯域内オプション（ファイバ チャネル トラフィックの場合）および mgmt0 オプション（イーサネット トラフィックの場合）を使用して、2 つのスイッチ間でローカルに IP ルーティングを実行します。

VSAN 作成時に、VSAN インターフェイスは自動作成されません。インターフェイスは手動で作成する必要があります。

IPv4 アドレスを使用して デフォルト ネットワークを構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	構成モードに入ります。
ステップ 2	switch(config)# **ip default- network 190.10.1.0**	デフォルト ネットワークの IPv4 アドレス（190.10.1.0）を設定します。
ステップ 3	switch(config)# **ip route 10.0.0.0 255.0.0.0 131.108.3.4**	ネットワークへの ip ルートを定義します。
ステップ 4	switch(config)# **ip default-network 10.0.0.0**	ネットワーク 10.0.0.0 へのスタティック ルートをスタティック デフォルト ルートとして定義します。

IP over Fibre Channel

IP over Fibre Channel（IPFC）は、（ギガビット イーサネット mgmt 0 インターフェイスを使用した帯域外ではなく）ファイバ チャネル インターフェイス経由の 帯域内スイッチ管理での IP 転送を提供します。IPFC を使用すると、カプセル化を使用してファイバ チャネル経由で IP フレームを伝送するように指定できます。IP フレームはファイバ チャネル フレームにカプセル化されるため、オーバーレイ イーサネット ネットワークを使用しなくても、ファイバ チャネル ネットワーク上で NMS 情報を伝達できます。

VSAN インターフェイスを作成すると、その VSAN の IP アドレスを指定できます。IPv4 アドレスまたは IPv6 アドレスを指定できます。

Cisco MDS 9000 ファミリ スイッチで IPv6 を設定する方法については、ギガビット イーサネット インターフェイスでの IPv4 の構成 （257 ページ） を参照してください。

このトピックには次のセクションを含みます。

IPFC 設定

IPFC を設定するには、次の手順に従います。

1. 必要な場合、帯域内管理に使用する VSAN を作成します。
2. VSAN インターフェイスの IPv4 アドレスとサブネット マスクを設定します。
3. IPv4 ルーティングをイネーブルにします。
4. 接続を確認します。

VSAN での IPv4 アドレスの構成

VSAN インターフェイスを作成し、そのインターフェイスの IPv4 アドレスを構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface vsan 10**	指定された VSAN（10）のインターフェイスを設定します。
ステップ 3	switch(config-if)# **ip address 10.0.0.12 255.255.255.0**	選択したインターフェイスの IPv4 アドレスおよびネットマスクを設定します。
ステップ 4	switch(config-if)# **no shutdown**	インターフェイスをイネーブルにします。

VSAN インターフェイスの構成の確認

VSAN インターフェイスの構成を確認するには、**show interface vsan** コマンドを使用します。

（注） 前に VSAN インターフェイスを設定した場合のみ、このコマンドの出力を表示できます。

```
switch# show interface vsan 1
vsan1 is down (Administratively down)
WWPN is 10:00:00:0c:85:90:3e:85, FCID not assigned
Internet address is 10.0.0.12/24
MTU 1500 bytes, BW 1000000 Kbit
0 packets input, 0 bytes, 0 errors, 0 multicast
0 packets output, 0 bytes, 0 errors, 0 dropped
```

IPv4 ルーティングの有効化

デフォルトでは、IPv4 ルーティング機能はすべてのスイッチで無効になっています。

IPv4 ルーティング機能を有効にするには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **ip routing**	IPv4 ルーティングを有効にします（デフォルトでは無効）。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **no ip routing**	IPv4 ルーティングを無効にし、工場出荷時の設定に戻します。

次のタスク

IPv4 ルーティング構成の確認

IPv4 ルーティング構成を確認するには、**show ip routing**コマンドを使用します。

```
switch(config)# show ip routing
ip routing is enabled
```

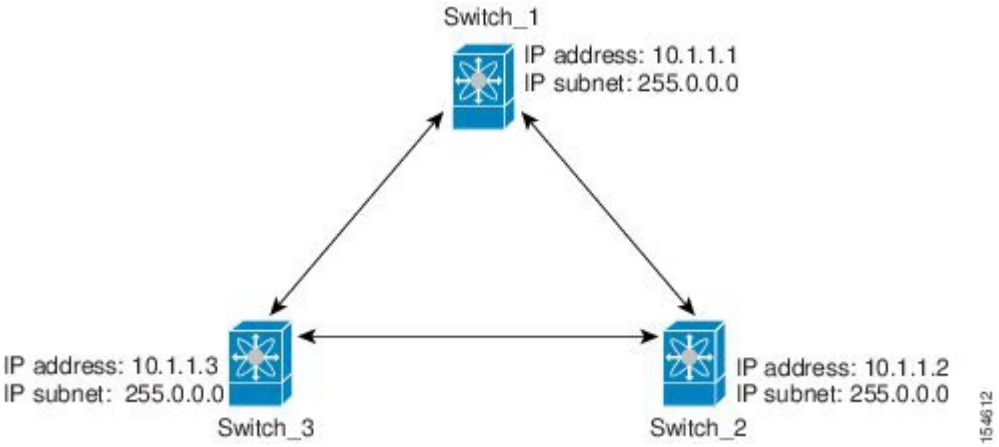
IPFC の構成例

ここでは、IPFC の設定例について説明します。下の図に、ネットワークの例を示します。

ネットワーク例に次のリンクがあります。

- Switch_1 は、mgmt 0 インターフェイスによってメイン ネットワークに接続され、ISL によってファブリックに接続されています。
- Switch_2 および Switch_3 は、ISL によってファブリックに接続されていますが、メイン ネットワークに接続されていません。

図 *47 : IPFC* のネットワーク例



手順

ステップ 1 ネットワーク例の Switch_1 を構成するには、以下のステップを実行します。

a) VSAN インターフェイスを作成し、インターフェイス コンフィギュレーション サブモードを開始します。

```
switch_1# config t
switch_1(config)# interface vsan 1
switch_1(config-if)#
```

b) IP アドレスおよびサブネット マスクを設定します。

```
switch_1(config-if)# ip address 10.1.1.1 255.0.0.0
```

c) VSAN インターフェイスを有効にし、インターフェイス コンフィギュレーション サブモードを終了します。

```
switch_1(config-if)# no shutdown
switch_1(config-if)# exit
switch_1(config)#
```

d) IPv4 ルーティングを有効にします。

```
switch_1(config)# ip routing
switch_1(config)# exit
switch_1#
```

e) ルートを表示します。

```
switch_1# show ip route

Codes: C - connected, S - static

C 172.16.1.0/23 is directly connect, mgmt0
C 10.0.0.0./8 is directly connected, vsan1
```

ステップ 2 ネットワーク例の Switch_2 を構成するには、以下のステップを実行します。

a) mgmt 0 インターフェイスを有効にします。

（注）
コンソール接続を使用してこのスイッチを設定します。

```
switch_2# config terminal
switch_2(config)# interface mgmt 0
switch_2(config-if)# no shutdown
switch_2(config-if)# exit
switch_2(config)#
```

b) VSAN インターフェイスを作成し、インターフェイス コンフィギュレーションを開始します。

```
switch_2# config terminal
switch_2(config)# interface vsan 1
switch_2(config-if)#
```

c) IP アドレスおよびサブネット マスクを設定します。

```
switch_2(config-if)# ip address 10.1.1.2 255.0.0.0
```

d) VSAN インターフェイスを有効にし、インターフェイス コンフィギュレーション サブモードを終了します。

```
switch_2(config-if)# no shutdown
switch_2(config-if)# exit
switch_2(config)#
```

e) IPv4 ルーティングを有効にします。

```
switch_2(config)# ip routing
switch_2(config)# exit
switch_2#
```

f) ルートを表示します。

```
switch_2# show ip route

Codes: C - connected, S - static

C 10.0.0.0./8 is directly connected, vsan1
```

g) Switch_1 への接続を確認します。

```
switch_2# ping 10.1.1.1
PING 10.1.1.1 (10.1.1.1) 56(84) bytes of data.
64 bytes from 10.1.1.1: icmp_seq=1 ttl=64 time=0.618 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=64 time=0.528 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=64 time=0.567 ms

--- 10.1.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 4998 ms
rtt min/avg/max/mdev = 0.528/0.570/0.618/0.057 ms
```

ステップ 3 ネットワーク例の Switch_3 を構成するには、以下のステップを実行します。

a) mgmt 0 インターフェイスを有効にします。

（注）
コンソール接続を使用してこのスイッチを設定します。

```
switch_3# config terminal
switch_3(config)# interface mgmt 0
switch_3(config-if)# no shutdown
switch_3(config-if)# exit
switch_3(config)#

switch_3# config terminal
switch_3(config)# interface vsan 1
switch_3(config-if)#
```

b) IP アドレスおよびサブネット マスクを設定します。

```
switch_3(config-if)# ip address 10.1.1.3 255.0.0.0
```

c) VSAN インターフェイスを有効にし、インターフェイス コンフィギュレーション サブモードを終了します。

```
switch_3(config-if)# no shutdown
switch_3(config-if)# exit
switch_3(config)#
```

d) IPv4 ルーティングを有効にします。

```
switch_3(config)# ip routing
switch_3(config)# exit
switch_3#
```

e) ルートを表示します。

```
switch_3# show ip route

Codes: C - connected, S - static
```

```
C 10.0.0.0./8 is directly connected, vsan1
```

f) Switch_1 への接続を確認します。

```
switch_3# ping 10.1.1.1
PING 10.1.1.1 (10.1.1.1) 56(84) bytes of data.
64 bytes from 10.1.1.1: icmp_seq=1 ttl=64 time=1.19 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=64 time=0.510 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=64 time=0.653 ms

--- 10.1.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008 ms
rtt min/avg/max/mdev = 0.510/0.787/1.199/0.297 ms
```

IPv4 スタティックルート

スタティック ルーティングは、スイッチに IPv4 ルートを設定するメカニズムです。複数のスタティック ルートを設定できます。

VSAN に複数の出力点が存在する場合は、適切なゲートウェイ スイッチにトラフィックが転送されるように、スタティック ルートを設定します。帯域外管理インターフェイスとデフォルト VSAN 間、または直接接続された VSAN 間のゲートウェイ スイッチでは、IPv4 ルーティングはデフォルトでディセーブルです。

ネットワーク構成で外部ルータが必要でない場合は、MDS スイッチに IPv4 スタティック ルーティングを設定できます。

IPv6 スタティック ルーティングを設定する手順については、ギガビット イーサネット インターフェイスでの IPv4 の構成 （257 ページ）を参照してください。

このセクションは、次のトピックで構成されています。

IPv4 スタティック ルートの設定

IPv4 スタティック ルートを構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **ip route network IP address netmask next hop IPv4 address distance number interface vsan number** 例：	指定した IPv4 アドレス、サブネット マスク、ネクストホップ、ディスタンス、およびインターフェイスについてスタティック ルートを設定します。

	コマンドまたはアクション	目的
	switch(config)# **ip route 10.0.0.0 255.0.0.0 20.20.20.10 distance 10 interface vsan 1** switch(config)#	

IPv4 スタティック ルート情報の確認

IPv4 スタティック ルートの構成を確認するには、**show ip route** コマンドを使用します。

```
switch# show ip route configured
Destination Gateway Mask Metric Interface

default 172.22.95.1 0.0.0.0 0 mgmt0
10.1.1.0 0.0.0.0 255.255.255.0 0 vsan1
172.22.95.0 0.0.0.0 255.255.255.0 0 mgmt0
```

アクティブで接続されている IPv4 スタティック ルートを確認するには、**show ip route** コマンドを使用します。

```
switch# show ip route

Codes: C - connected, S - static

Default gateway is 172.22.95.1

C 172.22.95.0/24 is directly connected, mgmt0
C 10.1.1.0/24 is directly connected, vsan1
```

IP ルーティング ステータスの表示

```
switch# show ip routing
ip routing is disabled
```

ARP の表示とクリア

Cisco MDS 9000 ファミリ スイッチの Address Resolution Protocol（ARP）エントリを表示、削除、またはクリアできます。ARP 機能はすべてのスイッチで有効になっています。

ARP テーブルを表示するには、**show arp** コマンドを使用します。

```
switch# show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 171.1.1.1 0 0006.5bec.699c ARPA mgmt0
Internet 172.2.0.1 4 0000.0c07.ac01 ARPA mgmt0
```

ARP テーブルから 1 つの ARP エントリを削除するには、構成モードで **no arp** コマンドを使用します。

```
switch(config)# no arp 172.2.0.1
```

ARP テーブルからすべてのエントリを削除するには、**clear arp** コマンドを使用します。ARP テーブルは、デフォルトでは空です。

```
switch# clear arp-cache
```

オーバーレイ VSAN

VSAN では、個別のファブリック サービス インスタンスを実行する複数の論理 SAN を 1 つの大規模な物理ネットワーク上でオーバーレイすることにより、より大規模な SAN を構成できます。このようなファブリック サービスの分離によって、ファブリックの再設定やエラー状態が個々の VSAN 内に限定されるので、ネットワークの安定性が向上します。また、物理的に分離された SAN と同じように、各 VSAN を隔離できます。トラフィックは VSAN 境界を通過できず、デバイスは複数の VSAN に属することはできません。VSAN ごとにファブリック サービスのインスタンスが個別に実行されるため、各 VSAN には独自のゾーン サーバーが設定され、VSAN 機能を持たない SAN とまったく同じ方法でゾーンを設定できます。

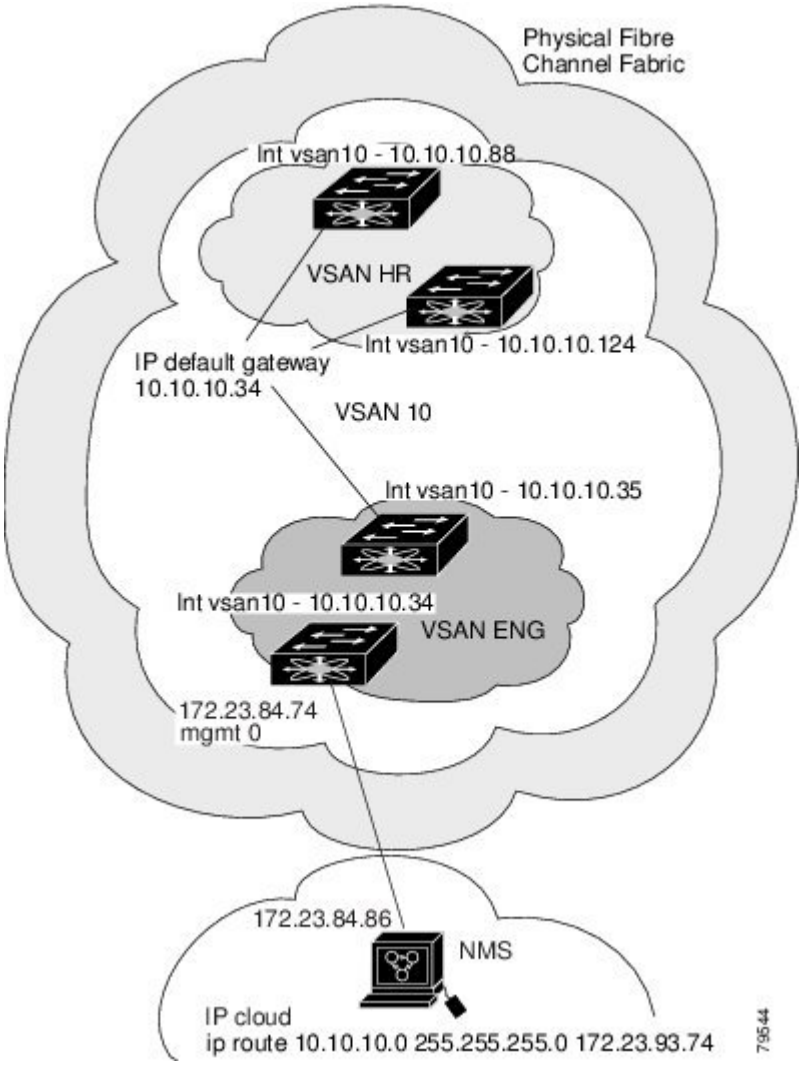
このセクションは、次のトピックで構成されています。

オーバーレイ VSAN の設定

オーバーレイ VSAN を設定する手順は、次のとおりです。

1. ファブリック内のすべてのスイッチの VSAN データベースに、VSAN を追加します。
2. ファブリック内のすべてのスイッチに VSAN 用の VSAN インターフェイスを作成します。VSAN に属するすべての VSAN インターフェイスに、同じサブネットに属する IP アドレスが設定されます。IP 側に IPFC クラウドへのルートを作成します。
3. ファイバ チャネル ファブリック内のスイッチごとに、NMS アクセスを提供するスイッチを指すデフォルト ルートを設定します。
4. 次の図に示されるように、NMS を指すスイッチにデフォルト ゲートウェイ（ルート）と IPv4 アドレスを構成します。

図 *48* : オーバーレイ *VSAN* の構成例



（注） 上の図に示す管理インターフェイスを設定するには、イーサネット ネットワークの IPv4 アドレスへのデフォルト ゲートウェイを構成します。

次の手順では、1 台のスイッチにオーバーレイ VSAN を設定します。この手順をファブリックのスイッチごとに繰り返す必要があります。

1 台のスイッチにオーバーレイ VSAN を構成するには（上の図を使用）、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **vsan database**	VSAN データベースを設定します。
ステップ 3	switch--config-vsan-db# **vsan 10 name MGMT_VSAN**	ファイバ チャネル ファブリックのすべてのスイッチの VSAN データベースに VSAN を定義します。
ステップ 4	switch--config-vsan-db# **exit**	VSAN データベース モードを終了します。
ステップ 5	switch(config)# **interface vsan 10**	VSANインターフェイス（VSAN 10）を作成します。
ステップ 6	switch(config-if)# **ip address 10.10.10.0 netmask 255.255.255.0**	このスイッチに IPv4 アドレスとサブネット マスクを割り当てます。
ステップ 7	switch(config-if)# **no shutdown**	設定されたインターフェイスを有効にします。
ステップ 8	switch(config-if)# **end**	EXEC モードに戻ります。
ステップ 9	switch# **exit**	スイッチを終了してNMSに戻ります。この例では、NMS が、ファイバ チャネル ファブリックにアクセスできるエッジのイーサネット管理インターフェイスの同じサブネット上に存在していることを前提としています。

次のタスク

上の図に表示されている NMS ステーションを構成するには、次のコマンドを使用します。

コマンドまたはアクション	目的
`nms# route ADD 10.10.10.0 MASK 255.255.255.0 172.22.93.74`	ファイバチャネルファブリックにアクセスできるエッジ スイッチの管理インターフェイスを指す NMS のスタティック ルートを定義します。

複数の VSAN の構成

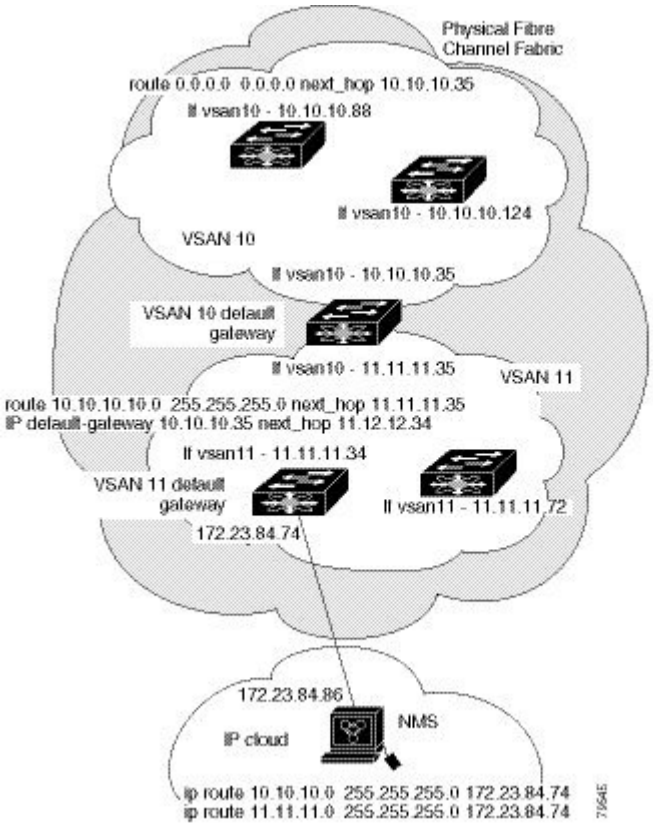
複数のVSANを使用して、管理ネットワークを複数のサブネットに分割できます。アクティブインターフェイスは、イネーブルにするVSANインターフェイスのスイッチ上に存在している必要があります。

複数の VSAN を構成するステップは、次のとおりです。

1. ファブリック内の任意のスイッチの VSAN データベースに、VSAN を追加します。

2. ファブリック内の任意のスイッチに、該当するVSAN用のVSANインターフェイスを作成します。
3. 対応する VSAN と同じサブネットの各 VSAN インターフェイスに、IP アドレスを割り当てます。
4. ファイバチャネル スイッチおよびIP クラウド上で複数のスタティック ルートを定義します（次の図を参照）。

図 *49 :* 複数の *VSAN* の構成例



オーバーレイ VSAN を構成するには（前の図の例を使用）、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **vsan database**	VSAN データベースを設定します。
ステップ 3	switch-config-vsan-db# **vsan 10 name MGMT_VSAN_10**	VSAN 10 のすべてのスイッチの VSAN データベースに VSAN を定義します。

	コマンドまたはアクション	目的
ステップ 4	witch-config-vsan-db# **exit**	VSAN データベース コンフィギュレーション サブモードを終了します。
ステップ 5	switch-config-vsan-db# **vsan 11 name MGMT_VSAN_11**	VSAN 11 のすべてのスイッチの VSAN データベースに VSAN を定義します。
ステップ 6	switch-config-vsan-db# **exit**	VSAN データベース コンフィギュレーション サブモードを終了します。
ステップ 7	switch(config)# **interface vsan 10**	VSAN 10 のインターフェイス コンフィギュレーション サブモードを開始します。
ステップ 8	switch(config-if)# **ip address 10.10.10.0 netmask 255.255.255.0**	このインターフェイスに IPv4 アドレスとサブネット マスクを割り当てます。
ステップ 9	switch(config-if)# **no shutdown**	VSAN 10 に設定したインターフェイスを有効にします。
ステップ 10	switch(config-if)# **exit**	VSAN 10 インターフェイス モードを終了します。
ステップ 11	switch(config)# **interface vsan 11**	VSAN 11 のインターフェイス コンフィギュレーション サブモードを開始します。
ステップ 12	switch(config-if)# **ip address 11.11.11.0 netmask 255.255.255.0**	このインターフェイスに IPv4 アドレスとサブネット マスクを割り当てます。
ステップ 13	switch(config-if)# **no shutdown**	VSAN 11 に設定したインターフェイスを有効にします。
ステップ 14	switch(config-if)# **end**	EXEC モードに戻ります。
ステップ 15	switch# **exit**	スイッチを終了して NMS に戻ります。この例では、NMS が、ファイバチャネル ファブリックにアクセスできるエッジのイーサネット管理インターフェイスの同じサブネット上に存在していることを前提としています。
ステップ 16	NMS# **route ADD 10.10.10.0 MASK 255.255.255.0 172.22.93.74**	IPv4 クラウドにアクセスできるエッジ スイッチの管理インターフェイスを指す NMS のスタティック ルートを定義します。
ステップ 17	NMS# **route ADD 11.11.11.0 MASK 255.255.255.0 172.22.93.74**	ファイバ チャネル ファブリックにアクセスできるエッジ スイッチの管理インターフェイスを指す NMS の VSAN 11 のスタティック ルートを定義します。
ステップ 18	switch# **route 10.10.10.0 255.255.255.0 next_hop 11.11.11.35**	サブネット 11 からサブネット 10 に到達するルートを定義します。

DNS の設定

スイッチ上の DNS クライアントは DNS サーバと通信して、IP アドレスとネーム サーバを対応付けます。

DNS サーバーは、次のいずれかの理由で、2 回試行されたあとに削除されることがあります。

- IP アドレスまたはスイッチ名が正しく設定されていない場合
- 外的要因により（制御不可能な理由により）DNS サーバーに到達できない場合

（注） Telnet ホストにアクセスするときに、（何らかの理由により）DNS サーバーに到達できない場合、スイッチ ログイン プロンプトが表示されるまでの期間が長くなることがあります。この場合は、DNS サーバーが正しく設定されていて、到達可能であることを確認してください。

DNS サーバを構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **ip domain-lookup**	IP ドメイン ネーム システム（DNS）ベースのホスト名からアドレスへの変換を有効にします。
ステップ 3	switch(config)# **no ip domain-lookup**	（デフォルト）IP DNS ベースのホスト名からアドレスへの変換を無効にし、出荷時のデフォルトに戻します。
ステップ 4	switch(config)# **ip domain-name cisco.com**	非修飾ホスト名を完成するためのデフォルトのドメイン名機能を有効にします。ドメイン名を含まない IP ホスト名（つまりドットのない名前）にはドットと cisco.com が追加され、その後でホスト テーブルに追加されます。
ステップ 5	switch(config)# **no ip domain-name cisco.com**	（デフォルト）ドメイン名を無効にします。
ステップ 6	switch(config)# **ip domain-list harvard.edu** or switch(config)# **ip domain-list stanford.edu** or switch(config)# **ip domain-list yale.edu**	ip domain-list グローバル構成コマンドを使用して、非修飾ホスト名を完成するためにデフォルト ドメイン名のフィルタを定義します。このフィルタで最大 10 個のドメイン名を定義できます。フィルタから名前を削除するには、このコマンドの no 形式を使用します。 （注）

	コマンドまたはアクション	目的
		ドメイン リストを設定していない場合は、ip domain-name グローバル コンフィギュレーション コマンドで指定したドメイン名が使用されます。ドメイン リストを設定した場合、デフォルトのドメイン名は使用されません。ip domain-list コマンドは ip domain-name コマンドと似ていますが、ip domain-list コマンドを使用すると、ドメインのリストを定義して、リストの順番でドメインが検索されるところが異なっています。
ステップ 7	switch(config)# **no ip domain-list**	定義したフィルタを削除し、出荷時のデフォルトに戻します。デフォルトではドメインは設定されていません。
ステップ 8	switch(config)# **ip name-server 15.1.0.1 2001:0db8:800:200c::417a**	プライマリ サーバーとして最初のアドレス（15.1.0.1）およびセカンダリ サーバーとして 2 番目のアドレス（2001:0db8:800:200c::417a）を指定します。最大 6 台のサーバーを設定できます。 （注） または、（IP アドレスの代わりに）スイッチ名を使用して DNS エントリを設定できます。設定したスイッチ名が自動的に対応する IP アドレスを検索します。
ステップ 9	switch(config)# **no ip name-server**	設定したサーバーを削除し、出荷時のデフォルトに戻します。デフォルトではサーバーは設定されていません。

DNS ホスト情報の表示

DNS 設定を表示するには、**show hosts** コマンドを使用します（ を参照）。

設定されたホストの詳細の表示

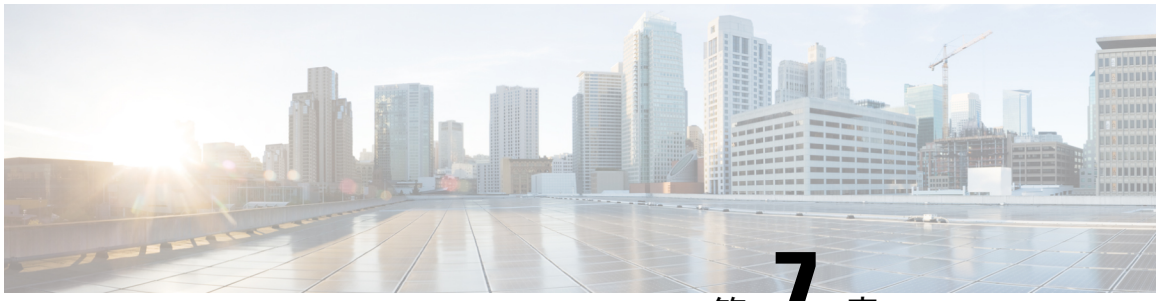
```
switch# show hosts
Default domain is cisco.com
Domain list: ucsc.edu harvard.edu yale.edu stanford.edu
Name/address lookup uses domain service
```

DNS 機能のデフォルト設定

以下のテーブルに、 DNS 機能のデフォルト設定を示します。

表 *10 : DNS* のデフォルト設定値

パラメータ	デフォルト
ドメイン参照	ディセーブル
ドメイン名	ディセーブル
ドメイン	なし
ドメイン サーバー	なし
最大ドメイン サーバー	6



第 7 章

IP ストレージ サービスの設定

Cisco MDS 9000 シリーズ IP ストレージ（IPS）サービスは、オープン規格の IP ベース テクノロジーを使用することによって、ファイバチャネルSANの到達距離を延長します。このスイッチは Fibre Channel over IP（FCIP）を使用して異なる SAN アイランド間を接続し、IP ホストからファイバ チャネル ストレージにアクセスできるようにします。

（注） FCIP 機能は、IPS ポートを備えたモジュールで使用でき、Cisco MDS 9250i、MDS 9220i、および Cisco MDS 9700 ディレクタ スイッチで使用できます。

MDS 9700 シリーズ スイッチ用 Cisco MDS 24/10 ポート SAN 拡張モジュールでは、ファイバチャネルおよび FCIP 機能を使用できます。Cisco MDS 24/10 ポート SAN 拡張モジュールは、どの Cisco MDS 9700 シリーズ スイッチでも使用できます。

この章は、次の項で構成されています。

- 機能情報 （234 ページ）
- サポート対象ハードウェア （234 ページ）
- FCIP および iSCSI インターフェイスのアップグレード （234 ページ）
- Cisco MDS 9220i スイッチでの IPS ポートの構成 （234 ページ）
- Cisco MDS 24/10 ポート SAN 拡張モジュールでの 40 Gbps 速度の構成 （235 ページ）
- IPv4 の IP ストレージ インターフェイスの構成 （236 ページ）
- 基本 IPStorage 構成 （237 ページ）
- IPS ポート コア ダンプを備えたファイバ チャネル モジュール （237 ページ）
- IPStorage の VLAN について （239 ページ）
- インターフェイス サブネットの要件 （240 ページ）
- IPStorage 接続の確認 （240 ページ）
- IPStorage IPv4-ACL のガイドライン （241 ページ）
- IPStorage ハイ アベイラビリティの構成 （242 ページ）
- CDP の設定 （244 ページ）
- IPStorage インターフェイスでのリンク速度の変更 （245 ページ）
- 統計の表示 （252 ページ）
- イーサネット MAC 統計情報の表示 （253 ページ）

- TCP 統計情報の表示 （254 ページ）
- IPStorage サービス パラメータのデフォルト設定 （256 ページ）

機能情報

この項では、Cisco MDS NX-OS リリース 9.x 以降の新機能と変更された機能について説明します。

表 *11* : 機能情報の表

機能	リリース	説明
Cisco MDS 24/10 ポート SAN 拡張モジュールでの 40 Gbps 速度の構成 （235 ページ）	9.3(1)	この機能を使用すると 、Cisco MDS 24/10 ポート SAN 拡張モジュールの IPS ポートで 40 Gbps の速度を構成できます。

サポート対象ハードウェア

次のタイプのハードウェアに FCIP および iSCSI 機能を構成できます。

- Cisco MDS 9700 シリーズ ディレクタ スイッチおよび Cisco MDS 9220i ファブリック スイッチの Cisco MDS 24/10 ポート SAN 拡張モジュールは、FCIP をサポートしています。
- Cisco MDS 9250i マルチサービス ファブリック スイッチは iSCSI をサポートします。

FCIP および iSCSI インターフェイスのアップグレード

ISSU/D は、これらの上位層インターフェイスをサポートする基盤となる IPS および GigabitEthernet インターフェイスの更新とともに、FCIP および iSCSI インターフェイスに影響を与えます。ファイバ チャネル インターフェイス（IPS および GigabitEthernet インターフェイスと同じモジュールまたはスイッチ上の FC インターフェイスを含む）、FCoE イーサネット インターフェイス、およびスーパーバイザ モジュールはすべて、中断することなく更新されます。

Cisco MDS 9700 ディレクタ内では、IPS ポートを備えたモジュールは、IPS ポートを備えた次のモジュールがアップグレードされる前に 5 分の遅延を実装します。

Cisco MDS 9220i スイッチでの IPS ポートの構成

Cisco MDS NX-OS リリース 8.5(1) 以降、Cisco MDS 9220i ファブリック スイッチがサポートされます。Cisco MDS 9220i スイッチは、6 つの IPS ポートをサポートします。ポート 1 ～ 4 は 1 Gbps および 10 Gbps の速度をサポートし 、ポート 6 は 40 Gbps の速度をサポートします。デフォルトでは、最初の 2 つのポートは 1 Gbps の速度モードで動作し、ライセンス付与されま

す。他のポートと異なる速度モードを有効にするには、ライセンスを取得する必要があります。最初の 2 つのポートから他のポートのいずれかにデフォルト ライセンスを移動できません。ライセンスの詳細については、『*Cisco MDS 9000* シリーズ *NX-OS* ライセンス ガイド』を参照してください。

Cisco MDS 9220i スイッチは、3 個の 1 Gbps または 10 Gbps IPS ポート、1 個の 1、10、25 Gbps IPS ポート、1 個の 25 Gbps IPS ポート、および 1 個の 40 Gbps IPS ポートをサポートします。これらのポートはすべて、単一のサービスエンジンによって処理されます。下のテーブルに、Cisco MDS 9220i スイッチの IPS ポートで構成できるさまざまな速度の組み合わせを示します。

25G 速度モードで動作する IPStorage インターフェイスには、FEC RS-IEEE が必要です。接続されたスイッチのイーサネット インターフェイスも、FEC RS-IEEE を使用するように構成する必要があります。IPStorage インターフェイスが init 状態のままである場合は、接続されたスイッチのイーサネット インターフェイスが FEC RS-IEEE を使用するように構成します。

表 *12 : Cisco MDS 9220i* スイッチの *IPS* ポート速度構成マトリックス

速度モード	ポート1	ポート2	ポート 3（Port 3）	ポート 4	ポート 5	ポート 6
1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	Out-of-service	Out-of-service
10 Gbps	10 Gbps	10 Gbps	10 Gbps	10 Gbps	Out-of-service	Out-of-service
25 Gbps	Out-of-service	Out-of-service	Out-of-service	25 Gbps	25 Gbps	Out-of-service
40 Gbps	Out-of-service	Out-of-service	Out-of-service	Out-of-service	Out-of-service	40 Gbps

（注） 25 Gbps の速度は、Cisco MDS NX-OS リリース 9.3(1) でサポートされます。

Cisco MDS 24/10 ポート SAN 拡張モジュールでの 40 Gbps 速度の構成

Cisco MDS NX-OS リリース 8.5(1) 以降では、Cisco MDS 24/10 ポート SAN 拡張モジュールの IPS ポート 9 および 10 で 40 Gbps を設定できます。Cisco MDS 24/10 ポート SAN 拡張モジュールは、8 個の 1 Gbps または 10 Gbps IPS ポートと 2 個の 40 Gbps IPS ポートをサポートします。ポート 1 ～ 4 およびポート 9 はサービス エンジン 1 によって処理され、ポート 5 ～ 8 およびポート 10 はサービスエンジン 2 によって処理されます。各 Service Engine の容量は 40 Gbps です。ポート 9 および 10 では 40 Gbps の速度のみを設定できます。ポート 9 で 40 Gbps の速度を設定すると、サービスエンジンの機能が 40 Gbps であるため、ポート 1 ～ 4 はアウトオブサービスになります。ただし、ポート 10 が 40 Gbps の速度に設定されていない場合は、ポート 5 ～ 8 を 1 Gbps または 10 Gbps の速度に設定できます。同様に、ポート 10 で 40 Gbps の速度を設定すると、ポート 5 ～ 8 はアウトオブサービスになります。ただし、ポート 9 が 40 Gbps の速度に設定されていない場合は、ポート 1 ～ 4 を 1 Gbps または 10 Gbps の速度に設定できま

す。次のテーブルに、Cisco MDS 24/10 ポート SAN 拡張モジュールの IPS ポートで構成できるさまざまな速度の組み合わせを示します。

40 Gbps IPS ポートで最大スループットを実現するための推奨設定は次のとおりです。

- FCIP トンネルの最大帯域幅は 10 Gbps です。したがって、40 Gbps IPS ポートに 4 つの FCIP トンネルを設定します。FCIP トンネルを作成するには、40 Gbps IPS ポートに 4 つの VLAN サブインターフェイスを作成します。各 VLAN で FCIP トンネルを作成します。
- TCP 接続の数を 5 に構成します。

表 *13 : Cisco MDS 24/10* ポート *SAN* 拡張モジュールの *IPS* ポート速度構成マトリクス

サービス エンジン 1		サービス エンジン 2	
ポート 1 ～ 4	ポート9	ポート 5 ～ 8	ポート10
1 Gbps	Out-of-service	1 Gbps	Out-of-service
10 Gbps	Out-of-service	10 Gbps	Out-of-service
1 Gbps	Out-of-service	10 Gbps	Out-of-service
10 Gbps	Out-of-service	1 Gbps	Out-of-service
Out-of-service	40 Gbps	1 Gbps	Out-of-service
Out-of-service	40 Gbps	10 Gbps	Out-of-service
1 Gbps	Out-of-service	Out-of-service	40 Gbps
10 Gbps	Out-of-service	Out-of-service	40 Gbps
Out-of-service	40 Gbps	Out-of-service	40 Gbps

IPv4 の IP ストレージ インターフェイスの構成

FCIP と iSCSI は両方とも TCP/IP を使用してネットワーク接続を行います。各 IPS ポートを搭載したファイバ チャネル モジュールでは、接続は適切に構成されている 24/10 ポート SAN 拡張モジュールを持つ Cisco MDS 9250i スイッチおよび Cisco MDS 9700 シリーズ スイッチで IP ストレージ ポートの形式で提供されます。ここでは、FCIP および iSCSI で IP を使用するように設定するための手順について説明します。

IPS ポートを備えた各ファイバ チャネル モジュールの IP ストレージ ポートには、IPS と呼ばれる新しいポート モードが定義されます。IPS ポートは、暗黙的に IPS モードに設定されているため、iSCSI および FCIP ストレージ機能を実行する場合だけ使用できます。IPS ポートでは、イーサネット フレームのブリッジングや、他の IP パケットのルーティングは行われません。

各 IPS ポートはファイバ チャネル SAN 内の 1 つの仮想ファイバ チャネル ホストを表します。この IPS ポートに接続されているすべての iSCSI ホストは、この 1 つのファイバ チャネル ホストを介して統合および多重化されます。

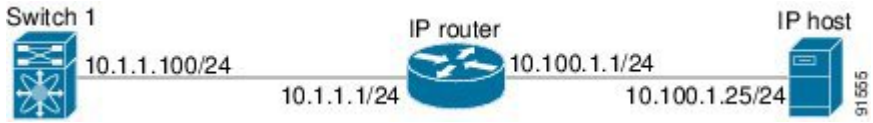
ファイバチャネル ストレージ サブシステムですべてのホスト デバイスに対する明示的な LUN アクセス コントロールが必要な大規模な iSCSI 構成では、プロキシ イニシエータ モードを使用して設定を簡素化します。

ヒント　IPS ポートを搭載したファイバ チャネル モジュールの IPStorage ポートは、同じ IPS ブロードキャスト ドメインで管理 IPS ポートとして構成しないでください。これらは、個別のスタンドアロン ハブまたは個別の VLAN を使用して、異なるブロードキャスト ドメインで構成する必要があります。

基本 IPStorage 構成

次の図に、IP バージョン 4（IPv4）での基本の IPStorage 構成例を示します。

図 *50 : IPStorage IPv4* 構成例



（注）　IPStorage インターフェイスが接続されているイーサネット スイッチ上のポートは、スイッチ ポートの代わりにホスト ポート（アクセス ポートともいう）として構成する必要があります。（イーサネット スイッチ上の）そのポートのスパニングツリー設定をディセーブルにする必要があります。これにより、（スパニングツリー設定がイネーブルであればイーサネット スイッチが実行する）イーサネット スパニングツリー処理の待ち時間による管理ポートの起動待ち時間を回避できます。Cisco イーサネット スイッチの場合は、Cisco IOS の **switchport host** コマンドまたは Catalyst OS の **set port host コマンド**のいずれかを使用します。

IPS ポート コア ダンプを備えたファイバ チャネル モジュール

IPS のコア ダンプは、他のモジュールに対するシステムのカーネル コア ダンプとは異なります。IPS ポートを搭載したファイバ チャネル モジュールのオペレーティング システム（OS）が予期せずにリセットされた場合、メモリ イメージのコピー（IPS コア ダンプ）を取得すると、リセットの原因の確認に役立ちます。その状況では、IPS ポートを搭載したファイバ モジュールからスーパーバーザ モジュールにコア ダンプが送られ、格納されます。シスコ製 MDS スイッチには、次の 2 つのレベルの IPS コア ダンプがあります。

- 部分コア ダンプ（デフォルト）：部分コア ダンプはそれぞれ 4 つの部分（4 つのファイル）で構成されます。4 つのファイルはすべて、アクティブなスーパーバイザ モジュールに保存されます。

  10/24 ポート SAN 拡張モジュールを搭載した Cisco MDS 9700 シリーズ スイッチで各部分のコア ダンプは、5 つの部分 (5 つのファイル) で構成されています。5 個のファイルはすべて、アクティブなスーパーバイザ モジュールに保存されます。

  これらのファイルを表示するには **show cores** コマンドを使用します。

- 完全コア ダンプ：Cisco MDS 9250i スイッチおよび SSN-16 モジュールの完全コア ダンプは、それぞれ 64 の部分（64 個のファイル）で構成され、24/10 ポート SAN 拡張モジュールを搭載した Cisco MDS 9700 シリーズ スイッチの完全コア ダンプは 67 の部分（67 個のファイル）で構成されます。MSM ~ 18/4 モジュールの IPS コア ダンプは、32 の部分で構成されています。このコア ダンプの保存には大きな容量が必要となるため、このコア ダンプはスーパーバイザ モジュールに保存されません。外部 TFTP サーバーに直接コピーされます。

  IPS コア ダンプ（およびその他のコア ダンプ）のコピー先となる外部 TFTP サーバの構成には、**system cores tftp:** コマンドを使用します。

IPS ポートを搭載したファイバ チャネル モジュールの IPS コア ダンプを構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **ips core dump full**	スイッチのすべての IPS ポートを搭載したファイバ チャネル モジュールの完全コア ダンプの生成を構成します。 `ips core dump full' successfully set for module 9`
ステップ 3	switch(config)# **no ips core dump full**	スロット 9 の IPS を搭載したファイバ チャネル モジュールの部分コア ダンプ（デフォルト）の生成を構成します。 `ips core dump partial' successfully set for module 9`

次のタスク

自動ネゴシエーションの設定

デフォルトで、自動ネゴシエーションはすべての IPStorage インターフェイスで有効になっています。指定した IPStorage インターフェイスに対して、自動ネゴシエーションを有効または無効に設定できます。自動ネゴシエーションをイネーブルに設定すると、ポートはリンクの相

手方に基づいて速度やポーズの方式、および着信信号のデュプレックスを自動的に検出します。また、自動ネゴシエーション機能を使用して、リンク アップの状態も検出できます。

MTU フレーム サイズを構成する

ポートで大きな（ジャンボ）フレームを伝送するようにスイッチのインターフェイスを設定できます。デフォルトの IP 最大伝送単位（MTU）フレーム サイズは、すべてのイーサネット ポートで 1500 バイトです。ポートにジャンボ フレームを設定すると、MTU サイズを最大 9000 バイトに拡張できます。

（注） MTU の最小サイズは 576 バイトです。

ヒント MTU の変更は中断を伴うため、ソフトウェアが MTU サイズの変更を検出すると、すべての FCIP リンクと iSCSI セッションにフラップが発生します。

無差別モードを構成する

無差別モードは、特定の IPStorage インターフェイスで有効または無効に設定できます。無差別モードを有効に設定すると、IPStorageインターフェイスはすべてのパケットを受信します。その後、ソフトウェアによって IPStorage インターフェイス宛てではないパケットがフィルタリングされて廃棄されます。

IPStorage の VLAN について

仮想 LAN（VLAN）は、1 つの物理 LAN ネットワーク上で複数の仮想レイヤ 2 ネットワークを構成します。VLAN を使用すると、トラフィックの隔離、セキュリティの確保、およびブロードキャストの制御が可能になります。

IPStorage ポートは、IEEE 802.1Q VLAN によってカプセル化されたイーサネット フレームを自動的に認識します。複数の VLAN から送信されたトラフィックを単一の IPStorage ポート上で終端させる必要がある場合は、VLAN ごとに 1 つずつサブインターフェイス構成します。

IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールがシスコ製イーサネット スイッチに接続されていて、複数の VLAN からのトラフィックを単一の IPS ポートに送信する必要がある場合は、イーサネット スイッチで次の要件を確認します。

- カプセル化がデフォルトの ISL でなく、802.1Q に設定されている
- VLAN ID を IPStorage インターフェイス名のサブスクリプションとして使用して、サブインターフェイス名を作成します。

```
 <slot-number> / <port-number>
<VLAN-ID>
```

インターフェイス サブネットの要件

IPStorage インターフェイス（メジャー）、サブインターフェイス（VLAN ID）、および管理インターフェイス（mgmt0）は、構成に応じて、同じサブネットまたは異なるサブネット上に設定できます（次のテーブルを参照）。

表 *14* : 同じスイッチ内のイーサネット インターフェイスのサブネット要件

インターフェイス1	インターフェイス2	同じサブネットを許可	注記
IPStorage 1/1	IPStorage 1/2	はい。	2 つのメジャー インターフェイスは同じサブネットまたは異なるサブネット内に設定できます。
IPStorage 1/1.100	IPStorage 1/2.100	○[1]	VLAN ID が同じ 2 つのサブインターフェイスは、同じサブネットまたは異なるサブネット内に設定できます。
IPStorage 1/1.100	IPStorage 1/2.200	No	VLAN ID が異なる 2 つのサブインターフェイスは、同じサブネットに設定できません。
IPStorage 1/1	IPStorage 1/1.100	No	サブインターフェイスは、メジャーインターフェイスと同じサブネットに設定できません。
mgmt0	IPStorage 1/1.100	いいえ	mgmt0 インターフェイスは、IPStorage インターフェイスまたはサブインターフェイスと同じサブネットに構成できません。
mgmt0	IPStorage 1/1	いいえ	

[1] IPSec 対応インターフェイスを除き、同じ IP サブネットに構成しないでください。

（注） 上のテーブルの構成要件は、イーサネット ポートチャネルにも適用されます。

IPStorage 接続の確認

有効な IP アドレスを使用して IPStorage インターフェイスを接続したら、各スイッチのインターフェイス接続を確認します。IP ホストの IP アドレスを使用してこのホストに対して ping を実行し、スタティック IP ルートが正しく設定されていることを確認します。

（注） 接続に失敗した場合は、次のことを確認してから、IP ホストに再び ping を実行してください。

- 宛先（IP ホスト）の IP アドレスが正しく構成されている。
- ホストがアクティブ状態である（電源が投入されている）。
- IP ルートが正しく構成されている。
- IP ホストから IPStorage インターフェイス サブネットに至るルートが存在する。
- IPStorage インターフェイスは up 状態です。

IPStorage IPv4-ACL のガイドライン

ヒント IPStorage インターフェイスに IPv4-ACL がすでに構成されている場合、このインターフェイスをイーサネット ポートチャネル グループに追加できません。

IPStorage インターフェイスで IPv4-ACL を構成する際には、次の注意事項に従ってください。

- Transmission Control Protocol（TCP）または Internet Control Message Protocol（ICMP）だけを使用します。

（注） ユーザー データグラム プロトコル（UDP）や HTTP などの他のプロトコルは、IPStorage インターフェイスではサポートされていません。これらのプロトコルに関するルールを含む ACL を IPStorage インターフェイスに適用することは可能ですが、これらのルールは無効になります。

- インターフェイスをイネーブルにする前に、インターフェイスに IPv4-ACL を適用します。このようにすれば、トラフィックが流れ始める前にフィルタを適用できます。
- 次の条件を確認します。
  - **[log-deny]** オプションを使用する場合、1 秒ごとに記録されるメッセージ数は最大 50 です。
  - IPStorage インターフェイスに **established**、**precedence**、および **fragments** オプションを含む IPv4-ACL を適用すると、これらのオプションは無視されます。
  - 前から存在している TCP 接続に IPv4-ACL のルールを適用しても、このルールは無視されます。たとえば、A と B の間に既存の TCP 接続がある場合に、送信元が A で送信先が B のパケットをすべて廃棄する IPv4-ACL を適用しても、このルールは無効になります。

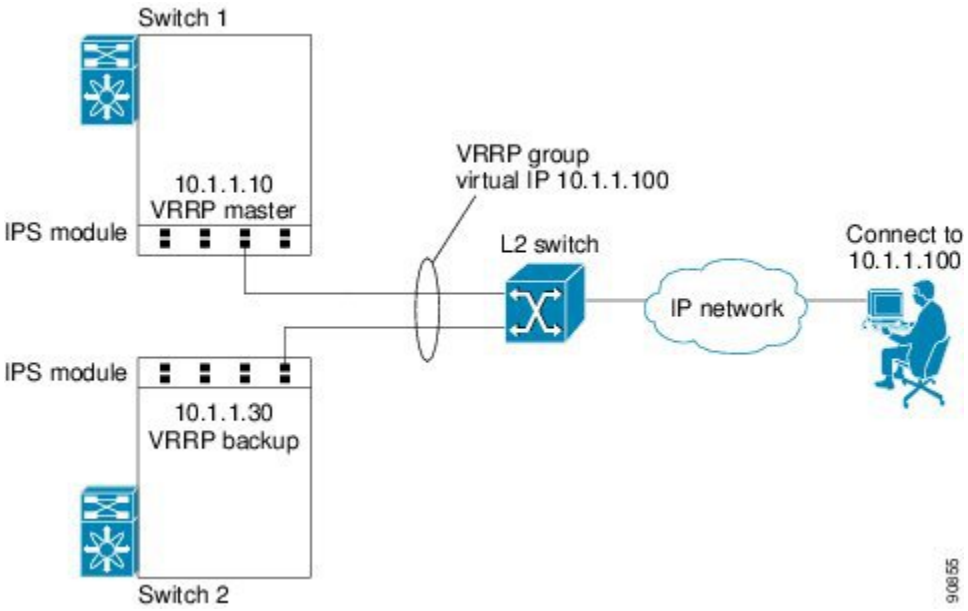
IPStorage ハイ アベイラビリティの構成

Virtual Router Redundancy Protocol（VRRP）およびイーサネット ポートチャネルは、iSCSI および FCIP サービスにハイ アベイラビリティを提供する 2 つの IPStorage 機能です。

iSCSI および FCIP サービスの VRRP

VRRP は iSCSI および FCIP サービスに対して、IPStorage ポートへの冗長代替パスを提供します。VRRP を利用すると、IP アドレスを代替 IPStorage インターフェイスにフェールオーバーして保護できます。これにより、IP アドレスが常に使用可能な状態になります（下の図を参照）。

図 *51 : VRRP* の例



上の図では、VRRP グループのメンバーは、すべて IPStorage ポートでなければなりません。VRRP グループ メンバーには、次のインターフェイスを 1 つまたは複数設定できます。

- 同じ IPS ポートを搭載したファイバ チャネル モジュールまたは MSM-18/4 モジュールの 1 つまたは複数のインターフェイス
- 1 台のスイッチの IPS を搭載したファイバ チャネル モジュールまたは MSM-18/4 モジュールのインターフェイス
- 異なるスイッチの IPS を搭載したファイバ チャネル モジュールまたは MSM-18/4 モジュールのインターフェイス
- IPStorage サブインターフェイス
- イーサネット ポートチャネルおよびポートチャネル サブインターフェイス

メイン インターフェイスとすべてのサブインターフェイスを含めて、1 つの IPStorage インターフェイスには、IPv4 と IPv6 の両方で最大 7 つの VRRP グループを構成できます。

IP ストレージ インターフェイスの VRRP の構成

IPv4 または IPv6 を使用して IPStorage インターフェイスの VRRP を構成するには、次のステップを実行します。

手順

ステップ 1 switch1# **config terminal**

構成モードに入ります。

ステップ 2 switch(config)# **interface IPStorage 2/2**

IPStorage インターフェイスでインターフェイス構成モードを開始します（スロット 2、ポート 2）。

ステップ 3 IPv4 を使用して IPStorage インターフェイスの VRRP を構成するには、次のステップを実行します。

a) switch(config-if)# **ip address 10.1.1.10 255.255.255.0**

IPStorage インターフェイスに IPv4 アドレス（10.1.1.10）およびサブネット マスク（255.255.255.0）を割り当てます。

b) switch(config-if)# **no shutdown**

選択されたインターフェイスを有効にします。

c) switch(config-if)# **vrrp 100**

VR ID 100 を作成します。

d) switch(config-if-vrrp) # **address 10.1.1.100**

選択した VRRP グループ（VR ID で識別される）の仮想 IPv4 アドレス（10.1.1.100）を設定します。

（注）
仮想 IPv4 アドレスは、IPStorage インターフェイスの IPv4 アドレスと同じサブネットにある必要があります。VRRP グループのメンバーはすべて同じ仮想 IPv4 アドレスを設定する必要があります。

e) switch(config-if-vrrp) # **priority 10**

この VRRP グループ内における、選択したインターフェイスのプライオリティを設定します。

（注）
プライオリティが最も高いルータがマスターとして選択されます。

f) switch(config-if-vrrp) # **no shutdown**

選択したインターフェイスで、VRRP プロトコルを有効にします。

ステップ 4 IPv6 を使用して IPStorage インターフェイスの VRRP を構成するには、次のステップを実行します。

a) switch(config-if)# **ipv6 address 2001:0db8:800:200c::417a/64**

IPStorage インターフェイスに IPv6 アドレスを割り当てます。

b) switch(config-if)# **no shutdown**

選択されたインターフェイスを有効にします。

c) switch(config-if)# **vrrp ipv6 100**

VR ID 100 を作成します。

d) switch(config-if-vrrp-ipv6) # **address 2001:0db8:800:200c::417a**

1 つのプライマリ リンクローカル IPv6 アドレス、または複数のセカンダリ IPv6 アドレスの 1 つを割り当てます。

（注）
この IPv6 アドレスが物理 IPv6 アドレスと同じ場合、このスイッチは自動的にこの IPv6 アドレスの所有者になります。

e) switch(config-if-vrrp-ipv6) # **priority 10**

この VRRP グループ内における、選択したインターフェイスのプライオリティを設定します。

（注）
プライオリティが最も高いルータがマスターとして選択されます。

f) switch(config-if-vrrp-ipv6) # **no shutdown**

選択したインターフェイスで、VRRP プロトコルを有効にします。

（注）
VRRP の **preempt** オプションは、IPS のインターフェイスではサポートされません。ただし、仮想 IPv4 IP アドレスがインターフェイスの IPv4IP アドレスでもある場合、プリエンプションは暗黙的に適用されます。

CDP の設定

Cisco Discovery Protocol（CDP）はスーパーバイザ モジュールの管理イーサネット インターフェイス、および IPS ポートを搭載したファイバ チャネル モジュールまたは MSM-18/4 モジュールの IPStorage インターフェイスでサポートされています。

CDP の構成の詳細は、『*Cisco MDS 9000* シリーズ *NX-OS* 基本構成ガイド』を参照してください。

IPStorage インターフェイスでのリンク速度の変更

ここでは、次の内容について説明します。

Cisco MDS 9250i マルチ サービス ファブリック スイッチのリンク速度の変更

Cisco MDS 9250i マルチサービス ファブリック スイッチには、1 Gbps および 10 Gps のリンク速度をサポートする 2 個の IPStorage インターフェイスがあります。デフォルトでは、IPStorage インターフェイスのリンク速度は 10 Gbps に構成されています。

リンク速度の変更は、Cisco MDS NX-OS リリース 6.2(13) 以降の Cisco 10 Gbps IPStorage プラットフォームでサポートされています。IPStorage ポートのいずれかが 1 Gbps に構成されている場合は、Cisco MDS NX-OS リリース 6.2(13) よりも前のリリースへの ISSD は許可されていません。このようなダウングレードを行う前に、ポートのリンク速度をデフォルトの 10 Gbps に再設定します。

IPStorage インターフェイスで 1 Gbps リンク速度を構成する

IP ストレージ インターフェイスで 1 Gbps のリンク速度を構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch1# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface IPStorage slot-number/port-number-range**	IPStorage インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **shutdown**	管理者がインターフェイスを無効にし、そのインターフェイスを通過するトラフィックを停止します。
ステップ 4	switch(config-if)# **switchport speed 1000**[2] 例： `This speed change will disrupt FCIP/iSCSI traffic for 5 mins on all IPStorage ports. If FCIP tunnels are configured please make sure max-bw <= 1000 Mbps and tcp-connections set to 2. Do you want to continue(y/n) ? [n]`	インターフェイスとすべてのサブインターフェイスのリンク速度を 1000 Mbps（1 Gbps）に設定します。 （注） このコマンドにより、選択された FCIP エンジンのすべての IPStorage ポートがリセットされます。これにより、トラフィックが最大 5 分間中断されることがあります。デフォルトでは、*n* が選択されます。コマンドを中止するには Enter キーを押しま

	コマンドまたはアクション	目的
		す。続行するには *y* と入力して Enter キーを押します。 [3]
ステップ 5	switch(config-if) # **no shutdown**	管理者がインターフェイスを有効にします。
ステップ 6	switch(config-if)# **end**	IPStorage 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、特権 EXEC モードに戻ります。
ステップ 7	switch# **show ips status**	IPStorage ポートの動作速度を表示します。

IPStorage インターフェイスで 10 Gbps リンク速度を構成する

IP ストレージインターフェイスで 10 Gbps のリンク速度を構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch1# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface IPStorage** *slot-number/port-number-range*	IPStorage インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **shutdown**	管理者がインターフェイスを無効にし、そのインターフェイスを通過するトラフィックを停止します。
ステップ 4	switch(config-if)# **switchport speed 10000**[4]	インターフェイスとすべてのサブインターフェイスのリンク速度を 10000 Mbps（10 Gbps）に設定します。 （注） このコマンドにより、選択された FCIP エンジンのすべての IPStorage ポートがリセットされます。これにより、トラフィックが最大 5 分間中断されることがあります。デフォルトでは、*n* が選択されます。コマンドを中止するには Enter キーを押します。続行するには *y* と入力して Enter キーを押します。 [5]
ステップ 5	switch(config-if) # **no shutdown**	管理者がインターフェイスを有効にします。

	コマンドまたはアクション	目的
ステップ 6	switch(config-if)# **end**	IPStorage 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、特権 EXEC モードに戻ります。
ステップ 7	switch# **show ips status**	IPStorage ポートの動作速度を表示します。

次のタスク

設定されているリンク速度と Small Form-Factor Pluggable（SFP）速度機能が一致しない場合、ポートは Error Disabled 状態になり、対応する syslog メッセージがログに記録されます。このような状況では、設定されているリンク速度または SFP のいずれかを変更する必要があります。リンク速度を変更すると、ポートがすでに有効になっている場合でも、変更を適用するために **shutdown** および **no shutdown** コマンドを明示的に発行する必要があります。

Cisco MDS 9250i マルチサービス ファブリック スイッチでサポートされている 1 Gbps SFP について詳しくは、「Cisco MDS 9000 ファミリ プラガブル トランシーバ データ シート」 を参照してください。

速度が 1 Gbps の IPStorage インターフェイスで FCIP トンネルを設定する方法の詳細については、「FCIP の設定 （7 ページ）」を参照してください。

Cisco MDS 9220i スイッチのリンク速度の変更

（注） Cisco MDS 9220i スイッチの場合は、1 Gbps または 10 Gbps の速度から 40 Gbps の速度に、またはその逆に切り替える前に、プロファイル、トンネルなどのすべての FCIP 関連の構成を削除します。

IPStorage インターフェイスでの 1 Gbps リンク速度の構成

IP ストレージ インターフェイスで 1 Gbps のリンク速度を構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface IPStorage 1/1-6**	IPStorage 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。

	コマンドまたはアクション	目的

ステップ 3	switch(config-if)# **1G-speed-mode**
	例：
	`This speed change will disrupt FCIP/iSCSI traffic for 60 seconds on selected IPStorage ports.`
	`If FCIP tunnels are configured please make sure max-bw <= 1000 Mbps and tcp-connections set to 2.`
	`Do you wish to continue(y/n)? [n]`
		インターフェイス IPS1/1-4 とすべてのサブインターフェイスのリンク速度を 1000 Mbps（1 Gbps）に設定し、インターフェイスを管理上有効にします。
		IPS1/5-6 を アウトオブサービスに設定します。

ステップ 4	switch(config-if)# **end**	IPStorage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、特権 EXEC モードに戻ります。

IPStorage インターフェイスで 10 Gbps リンク速度を構成する

IP ストレージインターフェイスで 10 Gbps のリンク速度を構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface IPStorage 1/1-6**	IPStorageインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	switch(config-if)# **10G-speed-mode**
	例：
	`This speed change will disrupt FCIP/iSCSI traffic for 60 seconds on select IPStorage ports.`
	`Do you wish to continue(y/n)? [n]`
		インターフェイス IPS1/1-4 とすべてのサブインターフェイスのリンク速度を 10000 Mbps（10 Gbps）に設定し、インターフェイスを管理上有効にします。
		IPS1/5-6 を アウトオブサービスに設定します。

ステップ 4	switch(config-if)# **end**	IPStorage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、特権 EXEC モードに戻ります。

IPStorage インターフェイスでの 25 Gbps リンク速度の構成

IP ストレージインターフェイスで 25 Gbps のリンク速度を構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface IPStorage 1/1-6**	IPStorageインターフェイス コンフィギュレーション モードを開始します。 （注） 最大スループットを実現するには、TCP接続の数を 5 に構成します。
ステップ 3	switch(config-if)# **25G-speed-mode**	インターフェイス IPS1/4-5 のリンク速度を 25000 Mbps（40 Gbps）を設定し、インターフェイスを管理上有効にします。 IPS1/1 ～ 3 および IPS1/6 をアウトオブサービスに設定します。 （注） 25g モードで IPStorage ポートを使用する場合、接続されたイーサネット インターフェイスを FEC RS-IEEE を使用するように構成します。
ステップ 4	switch(config-if)# **end**	IPStorage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、特権 EXEC モードに戻ります。

IPStorage インターフェイスでの 40 Gbps リンク速度の構成

IP ストレージインターフェイスで 40 Gbps のリンク速度を構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface IPStorage 1/1-6**	IPStorageインターフェイス コンフィギュレーション モードを開始します。 （注） 最大スループットを実現するには、TCP接続の数を 5 に構成します。

	コマンドまたはアクション	目的
ステップ 3	switch(config-if)# **40G-speed-mode**	インターフェイス IPS1/6 のリンク速度を 40000 Mbps（40 Gbps）に設定し、インターフェイスを管理上有効にします。 IPS1/1-5 を アウトオブサービスに設定します。
ステップ 4	switch(config-if)# **end**	IPStorage 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、特権 EXEC モードに戻ります。

Cisco MDS 24/10 ポート SAN 拡張モジュールでリンク速度の変更

（注） Cisco MDS 24/10 ポート SAN 拡張モジュールの場合は、1 Gbps または 10 Gbps の速度から 40 Gbps の速度に、またはその逆に切り替える前に、プロファイル、トンネルなどのすべての FCIP 関連の構成を削除します。

IPStorage インターフェイスでの 1 Gbps リンク速度の構成

IP ストレージ インターフェイスで 1 Gbps のリンク速度を構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface IPStorage** *slot-number/port-number-range*, **IPStorage** *slot-number/port-number*	IPStorage インターフェイス コンフィギュレーション モードを開始します。 （注） *port-number-range* の値は 1 ~ 4 および 5 ~ 8 のみです。*port-number-range* が 1 ～ 4 の場合、ポート番号の値は 9 になり、 *port-number-range* が 5 ～ 8 の場合、ポート番号の値は 10 になります。

ステップ 3	switch(config-if)# **1G-speed-mode**
	例：
	`This speed change will disrupt FCIP/iSCSI traffic for 60 seconds on selected IPStorage ports.`
	`If FCIP tunnels are configured please make sure`
	`max-bw <= 1000 Mbps and tcp-connections set to 2.`
		インターフェイスとすべてのサブインターフェイスのリンク速度を 1000 Mbps（1 Gbps）に設定し、インターフェイスを管理上イネーブルにします。

	コマンドまたはアクション	目的
	Do you wish to continue(y/n)? [**n**]	
ステップ 4	switch(config-if)# **end**	IPStorage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、特権 EXEC モードに戻ります。

IPStorage インターフェイスで 10 Gbps リンク速度を構成する

IP ストレージインターフェイスで10 Gbpsのリンク速度を構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface IPStorage***slot-number/port-number-range*, **IPStorage** *slot-number/port-number*	IPStorageインターフェイス コンフィギュレーション モードを開始します。 （注） *port-number-range* の値は 1 ~ 4 および 5 ~ 8 のみです。*port-number-range* が 1 ～ 4 の場合、ポート番号の値は 9 になり、 *port-number-range* が 5 ～ 8 の場合、ポート番号の値は 10 になります。
ステップ 3	switch(config-if)# **10G-speed-mode** 例： This speed change will disrupt FCIP/iSCSI traffic for 60 seconds on selected IPStorage ports. Do you wish to continue(y/n)? [**n**]	インターフェイスとすべてのサブインターフェイスのリンク速度を 10000 Mbps（10 Gbps）に設定し、インターフェイスを管理上イネーブルにします。
ステップ 4	switch(config-if)# **end**	IPStorage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、特権 EXEC モードに戻ります。

IPStorage インターフェイスでの 40 Gbps リンク速度の構成

IP ストレージインターフェイスで40 Gbpsのリンク速度を構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **interface IPStorage***slot-number/port-number-range*, **IPStorage** *slot-number/port-number*	IPStorageインターフェイス コンフィギュレーション モードを開始します。 （注） *port-number-range* の値は 1 ~ 4 および 5 ~ 8 のみです。*port-number-range* が 1 ～ 4 の場合、ポート番号の値は 9 になり、 *port-number-range* が 5 ～ 8 の場合、ポート番号の値は 10 になります。
ステップ 3	switch(config-if)# **40G-speed-mode**	インターフェイスのリンク速度を40 Gbpsに設定し、範囲内のインターフェイスをアウトオブサービスに設定します。
ステップ 4	switch(config-if)# **end**	IPStorage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、特権 EXEC モードに戻ります。

統計の表示

ここでは、IPStorage ポートのギガビット イーサネットおよび TCP/IP の統計情報を確認する例を示します。

インターフェイスが起動して期待どおりに機能していることを確認するには、各スイッチで **show interface IPStorage** コマンドを使用します。

IPStorage インターフェイスの表示

```
switch# show interface IPStorage 4/1
IPStorage4/1 is up
Hardware is IPStorage, address is 008e.7339.39e7
Internet address is 10.197.141.81/24
MTU 2500 bytes
Port mode is IPS
Speed is 10 Gbps
Beacon is turned off
Auto-Negotiation is turned on
5 minutes input rate 77012744 bits/sec, 9626593 bytes/sec, 112755 frames/sec
5 minutes output rate 2762915176 bits/sec, 345364397 bytes/sec, 175258 frames/sec
71187036 packets input, 6078261484 bytes
0 multicast frames, 0 compressed
0 input errors, 0 frame, 0 overrun 0 fifo
110617842 packets output, 217860230652 bytes, 0 underruns
0 output errors, 0 collisions, 0 fifo
0 carrier errors


switch# show interface IPStorage 5/1-10 brief

--------------------------------------------------------------------------------
Interface Status IP Address Speed MTU
--------------------------------------------------------------------------------
```

```
IPStorage5/1 up 1.1.1.1/24 10 Gbps 2500
IPStorage5/2 up 2.2.2.2/24 10 Gbps 2500
IPStorage5/3 up 3.3.3.3/24 10 Gbps 2500
IPStorage5/4 up 4.4.4.4/24 10 Gbps 2500
IPStorage5/5 up 6811::3456/64 1 Gbps 2300
IPStorage5/6 up 9.9.9.1/24 1 Gbps 2500
IPStorage5/7 up 7.7.7.1/24 1 Gbps 2500
IPStorage5/8 up 8.8.8.1/24 1 Gbps 2500
IPStorage5/9 outOfServc -- auto 1500
IPStorage5/10 outOfServc -- auto 1500
```

イーサネット MAC 統計情報の表示

show ips stats mac interface ips コマンドは、パラメータとして IPStorage インターフェイスをとり、そのインターフェイスの統計情報を返します。

（注） イーサネット MAC の統計情報を表示するには、サブインターフェイスではなく物理インターフェイスを使用します。

IPStorage インターフェイスの MAC 統計情報の表示

```
switch# show ips stats mac interface ips 4/1

DPP HW IPStorage port 4 (octeon port 19) statistics

Rx stats :
  dropped         : 0          octs,   0          pkts
  l2 red pkts     : 0          mcast,  0          bcasts
  l3 red pkts     : 0          mcast,  0          bcasts
  oversize        : 0          pkts,   0          crcpkts
  runt            : 0          pkts,   0          crcpkts
  inband          : 0          octs,   0          pkts,      0      err
  pci raw         : 0          pkts
  fcs_align_err   : 0          pkts

  total           : 0          octs,   0          pkts

  length of [pkts]:-
   [64B]          : 0            [65B-127B]       : 0
   [128B-255B]    : 0            [256B-511B]      : 0
   [512B-1023B]   : 0            [1024B-1518B]    : 0
   [1519B-MAX]    : 0

Tx stats :
  total           : 0          octs,   0          pkts
  dropped         : 0          octs,   0          pkts

Hw-intf stats :
  total           : 0            Rx_octs,   0           Rx_pkts
  dropped         : 0            Rx_pkts
  total           : 0            Tx_octs,   0           Tx_pkts
  dropped         : 0            Tx_pkts
```

TCP 統計情報の表示

TCP 統計情報を表示および確認するには、**show ips stats tcp interface ips** を使用します。このコマンドは、メイン イーサネット インターフェイスをパラメータとしてとり、接続リストおよび TCP 状態とともに TCP 統計情報を表示します。**detail** オプションは、インターフェイスで維持されているすべての情報を表示します。次の例を参照してください。

TCP 統計情報の表示

```
switch# show ips stats tcp interface ips 4/1

TCP statistics for port IPStorage4/1
Connection Stats
0 active openings, 3 accepts
0 failed attempts, 12 reset received, 3 established
Segment stats
163 received, 355 sent, 0 retransmitted
0 bad segments received, 0 reset sent
TCP Active Connections
Local Address Remote Address State Send-Q Recv-Q
0.0.0.0:3260 0.0.0.0:0 LISTEN 0 0
```

詳細な TCP 統計情報の表示

```
switch# show ips stats tcp interface ips 4/1 detail

TCP Statistics for port IPStorage4/1
TCP send stats
355 segments, 37760 bytes
222 data, 130 ack only packets
3 control (SYN/FIN/RST), 0 probes, 0 window updates
0 segments retransmitted, 0 bytes
0 retransmitted while on ethernet send queue, 0 packets split
0 delayed acks sent
TCP receive stats
163 segments, 114 data packets in sequence, 6512 bytes in sequence
0 predicted ack, 10 predicted data
0 bad checksum, 0 multi/broadcast, 0 bad offset
0 no memory drops, 0 short segments
0 duplicate bytes, 0 duplicate packets
0 partial duplicate bytes, 0 partial duplicate packets
0 out-of-order bytes, 1 out-of-order packets
0 packet after window, 0 bytes after window
0 packets after close
121 acks, 37764 ack bytes, 0 ack toomuch, 4 duplicate acks
0 ack packets left of snd_una, 0 non-4 byte aligned packets
8 window updates, 0 window probe
30 pcb hash miss, 0 no port, 0 bad SYN, 0 paws drops
TCP Connection Stats
0 attempts, 3 accepts, 3 established
3 closed, 2 drops, 0 conn drops
0 drop in retransmit timeout, 1 drop in keepalive timeout
0 drop in persist drops, 0 connections drained
TCP Miscellaneous Stats
115 segments timed, 121 rtt updated
0 retransmit timeout, 0 persist timeout
```

```
12 keepalive timeout, 11 keepalive probes
TCP SACK Stats
0 recovery episodes, 0 data packets, 0 data bytes
0 data packets retransmitted, 0 data bytes retransmitted
0 connections closed, 0 retransmit timeouts
TCP SYN Cache Stats
15 entries, 3 connections completed, 0 entries timed out
0 dropped due to overflow, 12 dropped due to RST
0 dropped due to ICMP unreach, 0 dropped due to bucket overflow
0 abort due to no memory, 0 duplicate SYN, 0 no-route SYN drop
0 hash collisions, 0 retransmitted
TCP Active Connections
Local Address Remote Address State Send-Q Recv-Q
0.0.0.0:3260 0.0.0.0:0 LISTEN 0 0
```

TCP 統計情報を表示および確認するには、**show ips stats icmp interface ips** を使用します。このコマンドは、メイン イーサネット インターフェイスをパラメータとしてとり、そのインターフェイスの ICMP 統計情報を返します。

ICMP 統計情報の表示

```
switch# show ips stats icmp interface ips 4/1

ICMP Statistics for port IPStorage4/1
0 ICMP messages received
0 ICMP messages dropped due to errors
ICMP input histogram
0 destination unreachable
0 time exceeded
0 parameter problem
0 source quench
0 redirect
0 echo request
0 echo reply
0 timestamp request
0 timestamp reply
0 address mask request
0 address mask reply
ICMP output histogram
0 destination unreachable
0 time exceeded
0 parameter problem
0 source quench
0 redirect
0 echo request
0 echo reply
0 timestamp request
0 timestamp reply
0 address mask request
0 address mask reply
```

IPStorage ポート速度の表示

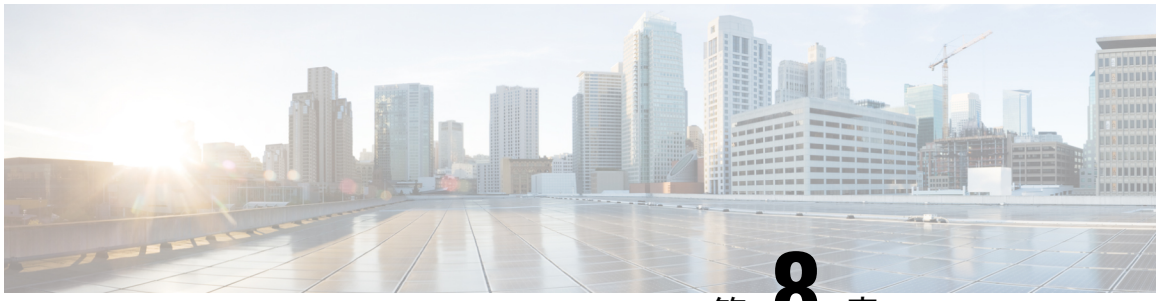
```
switch# show ips status
Port 1/1 READY 10G
Port 1/2 READY 1G
```

IPStorage サービス パラメータのデフォルト設定

以下のテーブルでは、IPStorage サービス パラメータのデフォルト設定をリスト化します。

表 *15 :* デフォルトの *IPStorage* パラメータ

パラメータ	デフォルト
IPS コア サイズ	一部



第 8 章

ギガビット イーサネット インターフェイスでの IPv4 の構成

Cisco MDS 9000 ファミリはギガビット イーサネット インターフェイス上で IP バージョン 4（IPv4）をサポートしています。この章では、IPv4 アドレスおよびその他の IPv4 機能の設定方法について説明します。

この章では、次の事項について説明します。

- IPv4 の概要 （257 ページ）
- IPv4 の基本的なギガビット イーサネット構成 （258 ページ）
- 自動ネゴシエーションの設定 （259 ページ）
- MTU フレーム サイズの設定 （260 ページ）
- 無差別モードの構成 （261 ページ）
- ギガビット イーサネット接続の確認 （262 ページ）
- Cisco MDS NX-OS での VLAN サポート （262 ページ）
- スタティック IPv4 ルーティングの構成 （264 ページ）
- IPv4 ルート テーブルの表示 （265 ページ）
- IPv4：アクセス コントロール リスト （265 ページ）
- Address Resolution Protocol キャッシュ （266 ページ）
- IPv4 統計情報の表示 （267 ページ）
- IPv4 パラメータのデフォルト設定 （268 ページ）

IPv4 の概要

Cisco MDS 9000 ファミリはギガビット イーサネット インターフェイス上で IP バージョン 4（IPv4）をサポートしています。FCIP と iSCSI は両方とも TCP/IP を使用してネットワーク接続を行います。各 IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールでは、ギガビット イーサネット インターフェイスを適切に構成することにより、接続を行います。

各 IPS ポートを搭載したファイバ チャネルまたは MPS-14/2 モジュールのギガビット イーサネット ポート用に、IPS という新しいポート モードが定義されています。IPS ポートは、暗黙

的に IPS モードに設定されているため、iSCSI および FCIP ストレージ機能を実行する場合だけ使用できます。IPS ポートでは、イーサネット フレームのブリッジングや、他の IP パケットのルーティングは行われません。

各 IPS ポートはファイバ チャネル SAN 内の 1 つの仮想ファイバ チャネル ホストを表します。この IPS ポートに接続されているすべての iSCSI ホストは、この 1 つのファイバ チャネル ホストを介して統合および多重化されます。

（注） MPS-14/2 モジュールのギガビット イーサネット インターフェイスは EtherChannel をサポートしていません。

FCIP と iSCSI は両方とも TCP/IP を使用してネットワーク接続を行います。各 IPS ポートを搭載したファイバチャネルモジュールまたは MSM-18/4 モジュールでは、ギガビットイーサネット インターフェイスを適切に構成することにより、接続を行います。ここでは、FCIP および iSCSI で IP を使用するように設定するための手順について説明します。

各 IPS ポートを搭載した ファイバ チャネルまたは MSM-18/4 モジュールのギガビット イーサネット ポート用に、IPS という新しい ポート モードが定義されています。IPS ポートは、暗黙的に IPS モードに設定されているため、iSCSI および FCIP ストレージ機能を実行する場合だけ使用できます。IPS ポートでは、イーサネット フレームのブリッジングや、他の IP パケットのルーティングは行われません。

各 IPS ポートはファイバ チャネル SAN 内の 1 つの仮想ファイバ チャネル ホストを表します。この IPS ポートに接続されているすべての iSCSI ホストは、この 1 つのファイバ チャネル ホストを介して統合および多重化されます。

ファイバ チャネル ストレージ サブシステムですべてのホスト デバイスの明示的な LUN アクセス コントロールが必要ない大規模な iSCSI 導入では、プロキシ イニシエータ モードを使用すると設定が簡単になります。

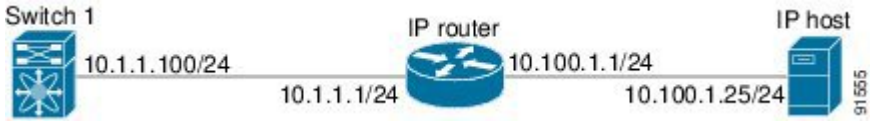
（注） MSM-18/4 モジュールのギガビット イーサネット インターフェイスは EtherChannel をサポートしていません。

ヒント IPS ポートを搭載したファイバ チャネル モジュールまたは MSM-18/4 モジュールのギガビット イーサネット ポートは、管理イーサネット ポートと同じイーサネット ブロードキャスト ドメイン内に設定しないでください。異なるスタンドアロン ハブまたはスイッチを使用するか、または異なる VLAN を使用して、異なるブロードキャスト ドメインに設定する必要があります。

IPv4 の基本的なギガビット イーサネット構成

次の図に、IP バージョン 4（IPv4）でのギガビット イーサネットの構成例を示します。

図 *52 : IPv4* でのギガビット イーサネットの設定例



（注） MDS ギガビット イーサネット インターフェイスが接続されているイーサネット スイッチ上のポートは、スイッチ ポートの代わりにホスト ポート（アクセス ポートともいう）として設定する必要があります。（イーサネット スイッチ上の）そのポートのスパニングツリー設定をディセーブルにする必要があります。これにより、（スパニングツリー設定がイネーブルであればイーサネット スイッチが実行する）イーサネット スパニングツリー処理の待ち時間による管理ポートの起動待ち時間を回避できます。シスコ イーサネット スイッチで、Cisco IOS の **switchport host** コマンドまたは Catalyst OS の **set port host** コマンドのいずれかを使用します。

上のイメージ例のギガビット イーサネット インターフェイスを構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface gigabitethernet 2/2**	ギガビット イーサネット インターフェイスでインターフェイス コンフィギュレーション モードを開始します（スロット 2、ポート 2）。
ステップ 3	switch(config-if)# **ip address 10.1.1.100 255.255.255.0**	ギガビット イーサネット インターフェイスの IPv4 アドレス（10.1.1.100）およびサブネット マスク（255.255.255.0）を入力します。
ステップ 4	switch(config-if)# **no shutdown**	インターフェイスをイネーブルにします。

自動ネゴシエーションの設定

デフォルトで、自動ネゴシエーションはすべてのギガビット イーサネット インターフェイスでイネーブルになっています。指定したギガビットイーサネットインターフェイスに対して、自動ネゴシエーションをイネーブルまたはディセーブルに設定できます。自動ネゴシエーションをイネーブルに設定すると、ポートはリンクの相手方に基づいて速度やポーズの方式、および着信信号のデュプレックスを自動的に検出します。また、自動ネゴシエーション機能を使用して、リンク アップの状態も検出できます。

（注） DS-X9316-SSNK9 モジュールのギガビット イーサネット インターフェイスで DS-SFP-GE-T（銅線 SFP）を使用する場合は、自動ネゴシエーションを無効にする必要があります。

自動ネゴシエーションを構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface gigabitethernet 2/2**	ギガビット イーサネット インターフェイスでインターフェイス コンフィギュレーション モードを開始します（スロット 2、ポート 2）。
ステップ 3	switch(config-if)# **switchport auto-negotiate**	このギガビット イーサネット インターフェイスの自動ネゴシエーションを有効にします（デフォルト）。
ステップ 4	switch(config-if)# **no switchport auto-negotiate**	このギガビット イーサネット インターフェイスの自動ネゴシエーションを無効にします。

MTU フレーム サイズの設定

ポートで大きな（ジャンボ）フレームを伝送するようにスイッチのインターフェイスを設定できます。デフォルトの IP 最大伝送単位（MTU）フレーム サイズは、すべてのイーサネット ポートで 1500 バイトです。ポートにジャンボ フレームを設定すると、MTU サイズを最大 9000 バイトに拡張できます。

（注） MTU の最小サイズは 576 バイトです。

ヒント MTU の変更は中断を伴うため、ソフトウェアが MTU サイズの変更を検出すると、すべての FCIP リンクと iSCSI セッションにフラップが発生します。

shutdown および **no shutdown** コマンドを明示的に発行する必要はありません。

MTU フレーム サイズを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface gigabitethernet 2/2**	ギガビット イーサネット インターフェイスでインターフェイス コンフィギュレーション モードを開始します（スロット 2、ポート 2）。
ステップ 3	switch(config-if)# **switchport mtu 3000**	MTU サイズを 3000 バイトに変更します。デフォルトは 1500 バイトです。

無差別モードの構成

無差別モードは、特定のギガビット イーサネット インターフェイスでイネーブルまたはディセーブルに設定できます。無差別モードをイネーブルに設定すると、ギガビットイーサネットインターフェイスはすべてのパケットを受信します。その後、ソフトウェアによってギガビット イーサネット インターフェイス宛てではないパケットがフィルタリングされて廃棄されます。

無差別モードを構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface gigabitethernet 2/2**	ギガビット イーサネット インターフェイスでインターフェイス コンフィギュレーション モードを開始します（スロット 2、ポート 2）。
ステップ 3	switch(config-if)# **switchport promiscuous-mode on**	このギガビット イーサネット インターフェイスの無差別モードをイネーブルにします。デフォルトは **off** です。
ステップ 4	switch(config-if)# **switchport promiscuous-mode off**	このギガビット イーサネット インターフェイスの無差別モードをディセーブルにします（デフォルト）。
ステップ 5	switch(config-if)# **no switchport promiscuous-mode**	このギガビット イーサネット インターフェイスの無差別モードを無効にします（デフォルト）。

ギガビット イーサネット接続の確認

有効な IP アドレスを使用してギガビット イーサネット インターフェイスを接続したら、各スイッチのインターフェイス接続を確認します。IP ホストの IP アドレスを使用してこのホストに対して ping を実行し、スタティック IP ルートが正しく設定されていることを確認します。

接続に失敗した場合は、次のことを確認してから、IP ホストに再び ping を実行してください。

- 宛先（IP ホスト）の IP アドレスが正しく構成されている。
- ホストがアクティブ状態である（電源が投入されている）。
- IP ルートが正しく構成されている。
- IP ホストからギガビット イーサネット インターフェイス サブネットに至るルートが存在する。
- ギガビット イーサネット インターフェイスが up 状態である。

ギガビット イーサネット接続を確認するには、**ping** コマンドを使用します（例 7-1 を参照）。ping コマンドは、指定した IP アドレスのリモート デバイスに対してエコー要求パケットを送信します。

ギガビット イーサネット インターフェイスが up 状態であるかどうかを確認するには、**show interface gigabitethernet** コマンドを使用します。

ギガビット イーサネット接続の確認

```
switch# ping 10.100.1.25
PING 10.100.1.25 (10.100.1.25): 56 data bytes
64 bytes from 10.100.1.25: icmp_seq=0 ttl=255 time=0.1 ms
64 bytes from 10.100.1.25: icmp_seq=1 ttl=255 time=0.1 ms
64 bytes from 10.100.1.25: icmp_seq=2 ttl=255 time=0.1 ms
--- 10.100.1.25 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.1 ms
```

Cisco MDS NX-OS での VLAN サポート

ここでは、Cisco MDS NX-OS での仮想 LAN（VLAN）のサポートについて説明します。内容は次のとおりです。

ギガビット イーサネットの VLAN

仮想 LAN（VLAN）は、1 つの物理 LAN ネットワーク上で複数の仮想レイヤ 2 ネットワークを構成します。VLAN を使用すると、トラフィックの隔離、セキュリティの確保、およびブロードキャストの制御が可能になります。

ギガビット イーサネット ポートは、IEEE 802.1Q VLAN によってカプセル化されたイーサネット フレームを自動的に認識します。複数の VLAN から送信されたトラフィックを単一のギガビット イーサネット ポート上で終端させる必要がある場合は、VLAN ごとに 1 つずつサブインターフェイスを設定します。

IPS ポートを搭載したファイバ チャネル モジュールまたは MSM-18/4 モジュールがシスコ製イーサネット スイッチに接続されていて、複数の VLAN からのトラフィックを単一の IPS ポートに送信する必要がある場合は、イーサネット スイッチで次の要件を確認します。

（注）
- IPS ポートを搭載したファイバ チャネル モジュールまたは MSM-18/4 モジュールに接続されたイーサネット スイッチ ポートがトランキング ポートとして構成されています。
- カプセル化がデフォルトの ISL でなく、802.1Q に設定されている

VLAN ID をギガビット イーサネット インターフェイス名のサブスクリプションとして使用して、サブインターフェイス名を作成します。

```
slot-number / port-number.VLAN-ID
```

VLAN サブインターフェイスの構成

VLAN サブインターフェイス（VLAN ID）を構成するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface gigabitethernet 2/2**	ギガビット イーサネット インターフェイスでインターフェイス コンフィギュレーション モードを開始します（スロット 2、ポート 2）。
ステップ 3	switch(config-if)# **ip address 10.1.1.101 255.255.255.0**	ギガビット イーサネット インターフェイスの IPv4 アドレス（10.1.1.100）およびサブネット マスク（255.255.255.0）を入力します。
ステップ 4	switch(config-if)# **shutdown**	インターフェイスをイネーブルにします。

インターフェイス サブネットの要件

ギガビット イーサネット インターフェイス（メジャー）、サブインターフェイス（VLAN ID）、および管理インターフェイス（mgmt0）は、構成に応じて、同じサブネットまたは異なるサブネット上に構成できます。

表 *16:* インターフェイスのサブネット要件

インターフェイス1	インターフェイス2	同じサブネットを許可	注
ギガビット イーサネット 1/1	ギガビット イーサネット 1/2	はい	2つのメジャーインターフェイスは同じサブネットまたは異なるサブネット内に設定できます。
ギガビット イーサネット 1/1.100	ギガビット イーサネット 1/2.100	はい	VLAN ID が同じ 2 つのサブインターフェイスは、同じサブネットまたは異なるサブネット内に設定できます。
ギガビット イーサネット 1/1.100	ギガビット イーサネット 1/2.200	No	VLAN ID が異なる 2 つのサブインターフェイスは、同じサブネットに設定できません。
ギガビット イーサネット 1/1	ギガビット イーサネット 1/1.100	No	サブインターフェイスは、メジャーインターフェイスと同じサブネットに設定できません。
mgmt0	ギガビット イーサネット 1/1.100	No	mgmt0 インターフェイスは、ギガビット イーサネット インターフェイスまたはサブインターフェイスと同じサブネットに設定できません。
mgmt0	ギガビット イーサネット 1/1	No	

（注） 上のテーブルの構成要件は、イーサネット ポートチャネルにも適用されます。

スタティック IPv4 ルーティングの構成

ギガビット イーサネット インターフェイスでスタティック IPv4 ルーティング（上の図を参照）を構成するに は、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **ip route 10.100.1.0 255.255.255.0 10.1.1.1**	IP ホストの IP サブネット（10.100.1.0 255.255.255.0）を入力し、ネクスト ホップ 10.1.1.1（ギガビット イーサネットインターフェイスに接続するルータの IPv4 アドレス）を設定します。

IPv4 ルート テーブルの表示

ip route interface コマンドは、パラメータとしてギガビット イーサネット インターフェイスを受け取り、 そのインターフェイスの ルート テーブルを返します。

IP ルート テーブルの表示

```
switch# show ips ip route interface gig 8/1
Codes: C - connected, S - static
No default gateway
C 10.1.3.0/24 is directly connected, GigabitEthernet8/1
```

Connected（C）は、インターフェイスが設定されているサブネットを示します（インターフェイスに直接接続）。Static（S）はルータ経由のスタティック ルートを示します。

IPv4：アクセス コントロール リスト

ここでは、IPv4 アクセス コントロール リストに関する注意事項と、ギガビット イーサネット インターフェイスに IPv4 アクセス コントロール リストを適用する方法について説明します。

このセクションは、次のトピックで構成されています。

ギガビット イーサネットの注意事項

ギガビット イーサネット インターフェイスの設定を行う際には、次の注意事項に従ってください。

- Transmission Control Protocol（TCP）または Internet Control Message Protocol（ICMP）だけを使用します。

（注） ユーザー データグラム プロトコル（UDP）や HTTP などの他のプロトコルは、ギガビット イーサネット インターフェイスではサポートされていません。これらのプロトコルに関するルールを含む ACL をギガビット イーサネット インターフェイスに適用することは可能ですが、これらのルールは無効になります。

- インターフェイスを有効にする前に、インターフェイスに適用します。このようにすれば、トラフィックが流れ始める前にフィルタを適用できます。
- 次の条件を確認します。
  - **[log-deny]** オプションを使用する場合、1 秒ごとに記録されるメッセージ数は最大 50 です。

- **[確立（established）]** オプションは、ギガビットイーサネットインターフェイスに適用しても無視されます。
- 前から存在している TCP 接続にルールを適用しても、ルールは無視されます。たとえば、A と B の間に既存の TCP 接続がある場合に、送信元が A で送信先が B のパケットをすべて廃棄する IPv4-ACL を適用しても、このルールは無効になります。

（注） ギガビットイーサネットインターフェイスにIPv4-ACLがすでに設定されている場合、このインターフェイスをイーサネット ポートチャネル グループに追加できません。IPv4-ACL の構成については、『Cisco Fabric Manager セキュリティ構成ガイド』『Cisco MDS 9000 ファミリ NX-OS セキュリティ構成ガイド』を参照してください。

ギガビット イーサネット インターフェイスへの適用

ギガビット イーサネット インターフェイスに適用するには、次のステップを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	構成モードに入ります。
ステップ 2	switch(config)# **interface gigabitethernet 3/1**	ギガビット イーサネット インターフェイス（3/1）を設定します。
ステップ 3	switch(config-if)# **ip access-group SampleName**	入力および出力トラフィックの両方について、ギガビット イーサネット 3/1 の IPv4-ACL SampleName を適用します（アソシエーションがまだ存在しない場合）。
ステップ 4	switch(config-if)# **ip access-group SampleName1 in**	入力トラフィックについて、ギガビットイーサネット 3/1 の IPv4-ACL SampleName を適用します。
ステップ 5	switch(config-if)# **ip access-group SampleName2 out**	出力トラフィックについて、ギガビットイーサネット 3/1 の IPv4-ACL SampleName を適用します（アソシエーションがまだ存在しない場合）。

Address Resolution Protocol キャッシュ

Cisco MDS NX-OS は IPv4 に設定されたギガビット イーサネット インターフェイスの Address Resolution Protocol（ARP）キャッシュをサポートします。このセクションは、次のトピックで構成されています。

ARP キャッシュの表示

ギガビット イーサネット インターフェイスの ARP キャッシュを表示できます。

すべての ARP キャッシュ コマンドには、サブインターフェイスではなく物理インターフェイスを使用します。

ギガビット イーサネット インターフェイスで ARP キャッシュを表示するには、**show ips arp interface gigabitethernet** コマンドを使用します。このコマンドは、イーサネット インターフェイスをパラメータとしてとり、そのインターフェイスの ARP キャッシュを返します。

ARP キャッシュの表示

```
switch# show ips arp interface gigabitethernet 7/1
Protocol Address Age (min) Hardware Addr Type Interface
Internet 20.1.1.5 3 0005.3000.9db6 ARPA GigabitEthernet7/1
Internet 20.1.1.10 7 0004.76eb.2ff5 ARPA GigabitEthernet7/1
Internet 20.1.1.11 16 0003.47ad.21c4 ARPA GigabitEthernet7/1
Internet 20.1.1.12 6 0003.4723.c4a6 ARPA GigabitEthernet7/1
Internet 20.1.1.13 13 0004.76f0.ef81 ARPA GigabitEthernet7/1
Internet 20.1.1.14 0 0004.76e0.2f68 ARPA GigabitEthernet7/1
Internet 20.1.1.15 6 0003.47b2.494b ARPA GigabitEthernet7/1
Internet 20.1.1.17 2 0003.479a.b7a3 ARPA GigabitEthernet7/1
.
.
.
```

ARP キャッシュのクリア

ARP キャッシュをクリアするには、2 通りの方法（ARP キャッシュの 1 つのエントリだけのクリアとすべてのエントリのクリア）があります。

ARP キャッシュをクリアするには、**clear ips arp** コマンドを使用します。

1 つの ARP キャッシュ エントリのクリア

```
switch# clear ips arp address 10.2.2.2 interface gigabitethernet 8/7
arp clear successful
```

すべての ARP キャッシュ エントリのクリア

```
switch# clear ips arp interface gigabitethernet 8/7
arp clear successful
```

IPv4 統計情報の表示

IP v4 統計情報を表示して確認するには、**show ips stats ip interface gigabitethernet** コマンドを使用します。このコマンドは、メイン イーサネット インターフェイスをパラメータとして受け取り、そのインターフェイスの IPv4 統計情報を返します。

IPv4 統計情報を表示するには、サブインターフェイスではなく物理インターフェイスを使用します。

IPv4 統計情報の表示

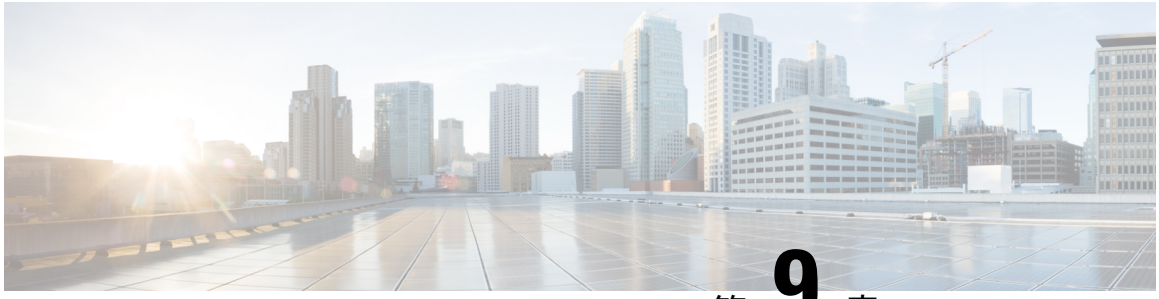
```
switch# show ips stats ip interface gigabitethernet 4/1
Internet Protocol Statistics for port GigabitEthernet4/1
168 total received, 168 good, 0 error
0 reassembly required, 0 reassembled ok, 0 dropped after timeout
371 packets sent, 0 outgoing dropped, 0 dropped no route
0 fragments created, 0 cannot fragment
```

IPv4 パラメータのデフォルト設定

次のテーブル、IPv4 パラメータのデフォルト設定値を示します。

表 *17 : IPv4* のデフォルト パラメータ

パラメータ	デフォルト
IPv4 MTU フレーム サイズ	すべてのイーサネット ポートで 1500 バイト
自動ネゴシエーション	イネーブル
無差別モード	無効化



第 9 章

IPv6 の設定

Cisco MDS 9000 ファミリは IP バージョン 6 をサポートします。この章では、IPv6 アドレスとその他の IPv6 機能を構成する方法について説明します。

この章では、次の事項について説明します。

- IPv6 の概要, on page 269
- IPv6 用の基本的な接続の設定 （279 ページ）
- ネイバー探索パラメータの構成の確認 （284 ページ）
- 重複アドレス検出試行回数 （284 ページ）
- 到達可能性時間 （284 ページ）
- 再送信時間 （285 ページ）
- ネイバー探索パラメータの構成の確認 （286 ページ）
- IPv6 スタティック ルート （286 ページ）
- ギガビット イーサネットの IPv6-ACL に関する注意事項 （288 ページ）
- IPv4 から IPv6 への移行 （289 ページ）
- IPv6 の表示 （289 ページ）
- デフォルト設定 （290 ページ）

IPv6 の概要

IP バージョン 6（IPv6）では、ネットワーク アドレス ビットが 32 ビット（IPv4）から 128 ビットへと 4 倍になることで、IP バージョン 4（IPv4）よりも拡張されたアドレッシング機能が Cisco MDS NX-OS で得られるようになります。IPv6 のアーキテクチャは、エンドツーエンドのセキュリティ、Quality Of Service（QoS）、およびグローバルに一意なアドレスなどのサービスを提供すると同時に、既存の IPv4 ユーザーが簡単に IPv6 へ移行できるように設計されています。

IPv6 の IPv4 に対する改良点は、次のとおりです。

- ネットワークの拡張性およびグローバルな到達可能性の実現
- プライベート アドレスおよびネットワーク アドレス変換（NAT）が不要
- アドレスの自動設定の簡素化

IPv6 の IPv4 に対する改良点は、次のとおりです。

- ネットワークの拡張性およびグローバルな到達可能性の実現
- プライベート アドレスおよびネットワーク アドレス変換（NAT）が不要
- アドレスの自動設定の簡素化

Note IP アドレッシングを使用する Cisco NX-OS 機能の IPv6 アドレッシングのサポートについては、このガイドの該当する章を参照してください。

Note ギガビット イーサネット インターフェイスで IP バージョン 4（IPv4）を構成するには、 第 7 章「 ギガビット イーサネット インターフェイスの IPv4 の構成」を参照してください。

ここでは、Cisco MDS NX-OS がサポートしている IPv6 機能について説明します。内容は次のとおりです。

IPv6 アドレス空間の拡張による一意アドレスの確保

IPv6 では、ネットワーク アドレスのビット数を（IPv4 の）32 ビットから 4 倍の 128 ビットに増やしてアドレス空間を拡張しています。これにより、利用できるグローバルに一意な IP アドレスの数が大幅に増加しています。グローバルに一意な IPv6 アドレスを利用すると、ネットワーク接続デバイスのグローバルな到達可能性とエンドツーエンドのセキュリティを実現できます。これは、より多くのアドレスを必要とするアプリケーションやサービスに不可欠な機能です。

IPv6 アドレス形式

IPv6 アドレスは、16 ビットの 16 進フィールドをコロン（:）で続けた x:x:x:x:x:x:x:x という形式で表現されます。次に、IPv6 アドレスの例を示します。

- 2001:0DB8:7654:3210:FEDC:BA98:7654:3210
- 2001:0DB8:0:0:8:800:200C:417A

IPv6 アドレスには、通常、連続するゼロの 16 進フィールドが含まれます。IPv6 アドレスの先頭、中間、または末尾にある連続した 0 の 16 進フィールドを 2 つのコロン（::）を使用して圧縮すると、IPv6 アドレスが使いやすくなります（2 つのコロンは連続した 0 の 16 進フィールドを表します）。テーブル 8-1 に、圧縮された IPv6 アドレスの形式をリストします。

Note IPv6 アドレスでは、最も長く連続するゼロの 16 進フィールドを表すために 2 つのコロン（::）を 1 回だけ使用できます。

Note IPv6 アドレスの 16 進文字は大文字と小文字が区別されません。

Table 18: 圧縮された ***IPv6*** アドレス形式

IPv6 アドレス タイプ	非圧縮形式	圧縮形式
ユニキャスト	2001:0DB8:800:200C:0:0:0:417A	2001:0DB8:800:200C::417A
マルチキャスト	FF01:0:0:0:0:0:0:101	FF01::101

IPv6 アドレス プレフィックスの形式

IPv6 アドレス プレフィックスは、ipv6-prefix/prefix-length の形式で、アドレス空間全体のビット連続ブロックを表すために使用できます。ipv6-prefix は、16 進の 16 ビット値をコロンで区切って指定します。 prefix-length は、

構成するアドレスの上位連続ビット数を示す 10 進値です。たとえば、2001:0DB8:8086:6502::/32 は有効な IPv6 プレフィックスです。

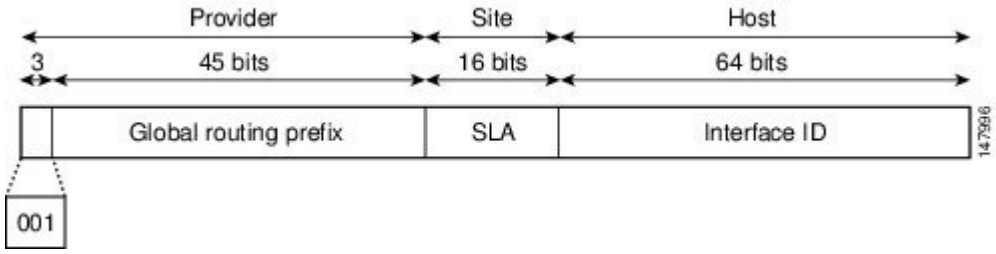
IPv6 アドレスタイプ：ユニキャスト

IPv6ユニキャストアドレスは、1つのノード上の1つのインターフェイスのIDです。ユニキャスト アドレスに送信されたパケットは、そのアドレスが示すインターフェイスに配信されます。Cisco MDS NX-OS は、次の種類の IPv6 ユニキャスト アドレスをサポートしています。

グローバル アドレス

グローバルIPv6アドレスは、グローバル ルーティング プレフィックス、サブネット ID、およびインターフェイス ID で定義されます。図 8-1 に、グローバル アドレスの構造を示します。

Figure 53: グローバル アドレスの形式



2000::/3（001）～ E000::/3（111）のプレフィックスを持つアドレスには、Extended Universal Identifier（EUI）64 形式の 64 ビット インターフェイス識別子が必要です。インターネット割り当て番号局（IANA）は、2000::/16 の範囲の IPv6 アドレス空間を地域レジストリに割り当てます。

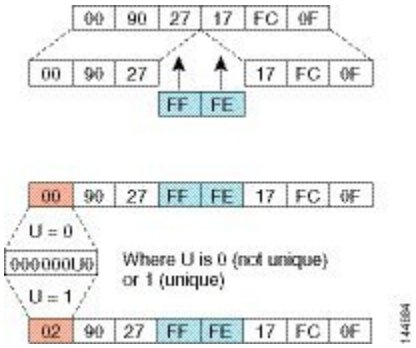
集約可能グローバル アドレスは、通常、48 ビットのグローバル ルーティング プレフィックスと、16 ビットのサブネット ID またはサイトレベル集約（SLA）で構成されます。RFC 2374（IPv6 集約可能グローバル ユニキャスト アドレス形式）では、グローバル ルーティング プレフィックスに Top-Level Aggregator（TLA）と Next-Level Aggregator（NLA）という他の 2 つの階層構造フィールドが含まれていました。IETF は、TLS フィールドと NLA フィールドがポリシーベースのフィールドであるため、これらのフィールドを RFC から削除することに決定しました。この変更の前に展開された既存の IPv6 ネットワークの中には、依然として古いアーキテクチャに基づくネットワークを使用しているものもあります。

個々の組織では、サブネット ID と呼ばれる 16 ビットのサブネット フィールドを使用して、独自のローカル アドレッシング階層を作成したり、サブネットを識別したりできます。サブネット ID は IPv4 でのサブネットに似ていますが、IPv6 サブネット ID を持つ組織では最大 65,535 個のサブネットをサポートできるという点が異なります。

インターフェイス ID は、リンク上のインターフェイスの識別に使用されます。インターフェイス ID は、リンク上で一意である必要があります。また、より広い範囲で一意にすることもできます。多くの場合、インターフェイス ID は、インターフェイスのリンク層アドレスと同じか、それに基づいているため、グローバルに一意になります。集約可能グローバル ユニキャストおよびその他の IPv6 アドレス タイプで使用されるインターフェイス ID は、長さが 64 ビットの変更された EUI-64 形式で構築されている必要があります。

Cisco MDS NX-OS は、IEEE 802 インターフェイス（たとえば、ギガビット イーサネット インターフェイス）をサポートしています。最初の 3 オクテット（24 ビット）は、インターフェイスの 48 ビットのリンク層アドレス（MAC アドレス）の Organizationally Unique Identifier（OUI）から取得され、4 番めと 5 番めのオクテット（16 ビット）は、FFFE の固定 16 進値であり、最後の 3 オクテット（24 ビット）は、MAC アドレスの最後の 3 オクテットから取得されます。インターフェイス ID の構成は、最初のオクテットの 7 番めのビットである Universal/Local（U/L）ビットを 0 または 1 の値に設定することで完成します。0 の値はローカルに管理される ID を表し、1 の値はグローバルに一意の IPv6 インターフェイス ID を表します（ 図 8-2 を参照）。

Figure 54: インターフェイス *ID* の形式

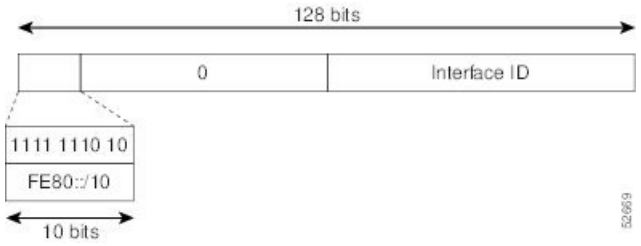


リンクローカル アドレス

リンクローカル アドレスは、リンクローカル プレフィックス FE80::/10 と Modified EUI-64 形式のインターフェイス ID を使用して自動的にインターフェイスに設定される IPv6 ユニキャス

トアドレスです。リンクローカル アドレスは、ネイバー探索プロトコルとステートレス自動設定プロセスで使用されます。ローカル リンク上のノードは、リンクローカル アドレスを使用して通信できます。次のイメージは、以下のリンク ローカル アドレスの構造を示しています。

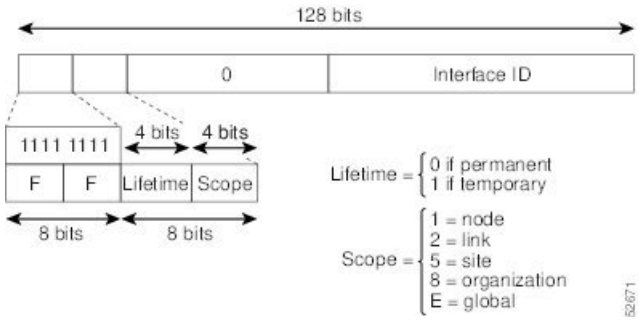
図 *55 :* リンクローカル アドレス形式



IPv6 アドレスタイプ：マルチキャスト

IPv6 マルチキャスト アドレスは、FF00::/8（1111 1111）というプレフィックスを持つ IPv6 アドレスです。IPv6 マルチキャスト アドレスは、通常は異なるノードに属するインターフェイス セットの識別子です。マルチキャスト アドレスに送信されたパケットは、マルチキャスト アドレスが示すすべてのインターフェイスに配信されます。プレフィックスに続く 2 番めのオクテットで、マルチキャストアドレスのライフタイムとスコープが定義されます。永久マルチキャスト アドレスはライフタイム パラメータが 0 に等しく、一時マルチキャスト アドレスのライフタイム パラメータは 1 に等しくなっています。ノード、リンク、サイト、組織、またはグローバル スコープを持つマルチキャスト アドレスのスコープ パラメータは、それぞれ 1、2、5、8、および E です。たとえば、プレフィックスが FF02::/16 のマルチキャスト アドレスは、リンク スコープを持つ永続マルチキャスト アドレスです。次の図に、IPv6 マルチキャスト アドレスの形式を示します。

図 *56 :* 図 *8-4 IPv6* マルチキャスト アドレス形式

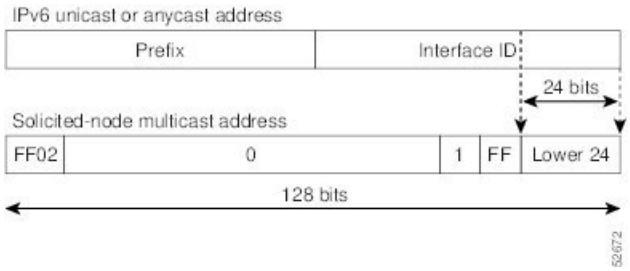


IPv6 ホストは、次のマルチキャスト グループに参加して、各マルチキャスト グループ宛のパケットを受信する必要があります。

- 全ノード マルチキャスト グループ FF02::1
- ユニキャストアドレスの下位 24 ビットと連結した送信要求ノードマルチキャスト グループ FFF02:0:0:0:0:1:FF00:0000/104

送信要求ノード マルチキャスト アドレスは、IPv6 ユニキャスト アドレスに対応するマルチキャスト グループです。IPv6 ノードは、割り当てられているすべてのユニキャスト アドレスについて、関連する送信要求ノードマルチキャスト グループに参加する必要があります。IPv6 送信要求ノード マルチキャスト アドレスは、対応する IPv6 ユニキャスト アドレスの下位 24 ビットと連結されるプレフィックス FF02:0:0:0:0:1:FF00:0000/104 を持ちます。（以下の図を参照してください。）たとえば、IPv6 アドレス 2037::01:800:200E:8C6C に対応する請求ノードマルチキャスト アドレスは FF02::1:FF0E:8C6C です。送信要求ノード アドレスは、ネイバー送信要求メッセージで使用されます。

図 *57 : IPv6* 送信要求ノード マルチキャスト アドレス形式



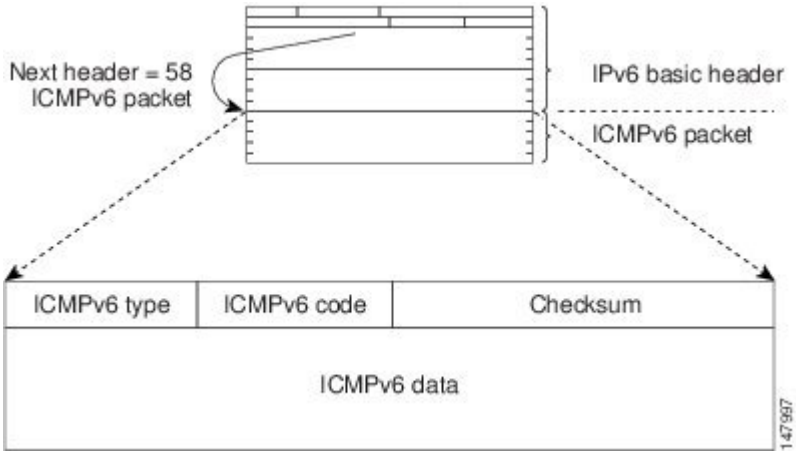
（注） IPv6 にはブロードキャスト アドレスはありません。ブロードキャスト アドレスの代わりに IPv6 マルチキャスト アドレスが使用されます。

IPv6 の ICMP

IPv6 の Internet Control Message Protocol（ICMP）の機能は、IPv4 の ICMP と同じです。ICMP は、ICMP 宛先到達不能メッセージのようなエラー メッセージ、および ICMP エコー要求や応答メッセージのような情報メッセージを生成します。また、IPv6 の ICMP パケットは、IPv6 ネイバー探索プロセス、パス MTU ディスカバリ、および Multicast Listener Discovery（MLD）プロトコル for IPv6 で使用されます。MLD は、バージョン 2 の Internet Group Management Protocol（IGMP）for IPv4 をベースとしています。

基本 IPv6 パケット ヘッダーの次ヘッダー フィールドの値 58 は、IPv6 ICMP パケットを示します。IPv6 の ICMP パケットは、すべての拡張ヘッダーに続いて IPv6 パケットの末尾に配置される点でトランスポートレイヤ パケットに似ています。IPv6 ICMP パケット内の ICMPv6 タイプ フィールドと ICMPv6 コード フィールドは、ICMP メッセージ タイプなどの IPv6 ICMP パケットの詳細を示します。チェックサム フィールドの値は、（送信側で計算し、受信側がチェックすることにより）IPv6 ICMP パケットと IPv6 疑似ヘッダーのフィールドから抽出されます。ICMPv6 データ フィールドには、IP パケット処理に関連するエラー情報または診断情報が含まれます。次の図は、IPv6 ICMP パケット ヘッダーの形式を示しています。

図 *58 : IPv6 ICMP* パケット ヘッダーの形式



IPv6 のパス MTU ディスカバリ

IPv4 の場合と同様に、IPv6 のパス MTU ディスカバリを使用すると、特定のデータ パス上のすべてのリンクの MTU サイズの差をホストが動的に検出し、調整できます。ただし、IPv6 では、特定のデータ パス上の 1 つのリンクのパス MTU がパケットのサイズに十分に対応できる大きさでない場合に、フラグメンテーションはパケットの送信元によって処理されます。IPv6 ホストでパケット フラグメンテーションを処理すると、IPv6 ルータの処理リソースが節約され、IPv6 ネットワークの効率が向上します。

（注） IPv4 では、最小リンク MTU が 68 オクテットであるため、特定のデータ パスに沿うすべてのリンクの MTU サイズが少なくとも 68 オクテットの MTU サイズをサポートする必要があります。

IPv6 では、最小リンク MTU は 1280 オクテットです。IPv6 リンクには、1500 オクテットの MTU 値の使用をお勧めします。

IPv6 ネイバー探索

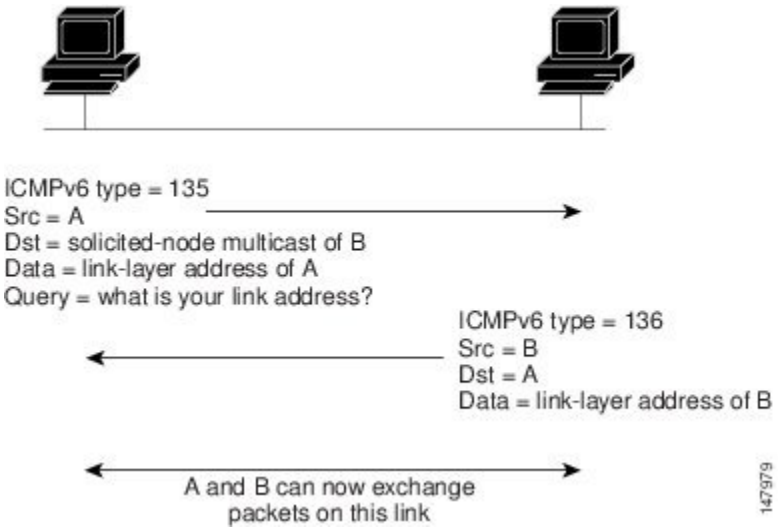
IPv6 のネイバー探索プロセスは、ICMP メッセージと送信要求ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンク層アドレスを判別し、ネイバーの到達可能性を確認して、近隣ルータの状況を把握します。

IPv6 ネイバー送信要求メッセージおよびアドバタイズ メッセージ

ICMP パケット ヘッダーのタイプ フィールドの値 135 は、ネイバー送信要求メッセージを示します。ネイバー送信要求メッセージは、ノードが同じローカル リンク上の別のノードのリンク層アドレスを決定するときに、ローカル リンク上で送信されます（次の図を参照してください）。ノードが別のノードのリンク層アドレスを判断する必要がある場合、ネイバー請求メッ

セージ内の送信元アドレスは、ネイバー請求メッセージを送信するノードの IPv6 アドレスです。ネイバー送信要求メッセージ内の宛先アドレスは、宛先ノードの IPv6 アドレスに対応する送信要求ノード マルチキャスト アドレスです。ネイバー送信要求メッセージには、送信元ノードのリンク層アドレスも含まれます。

図 *59 : IPv6* ネイバー探索 - ネイバー送信要求メッセージ



ネイバー送信要求メッセージを受信した後に、宛先ノードは、ICMP パケット ヘッダーのタイプ フィールドに値 136 を含むネイバー アドバタイズメント メッセージをローカル リンクに送信することで応答します。ネイバー アドバタイズメント メッセージの送信元アドレスは、ネイバー アドバタイズメント メッセージを送信するノードの IPv6 アドレス（具体的には、ノードインターフェイスの IPv6 アドレス）です。ネイバー アドバタイズメント メッセージ内の宛先アドレスは、ネイバー送信要求メッセージを送信したノードの IPv6 アドレスです。ネイバー アドバタイズメント メッセージのデータ部分には、ネイバー アドバタイズメント メッセージを送信するノードのリンク層アドレスが含まれます。

送信元ノードがネイバーアドバタイズメントを受信すると、送信元ノードと宛先ノードが通信できるようになります。

ネイバー送信要求メッセージは、ネイバーのリンク層アドレスが識別された後に、ネイバーの到達可能性の確認にも使用されます。ノードがあるネイバーの到達可能性を検証する場合、ネイバー送信要求メッセージ内の宛先アドレスとして、そのネイバーのユニキャストアドレスを使用します。

ネイバー アドバタイズメント メッセージは、ローカル リンク上のノードのリンク層アドレスが変更されたときにも送信されます。このような変更がある場合、ネイバーアドバタイズの宛先アドレスは、全ノード マルチキャスト アドレスになります。

ネイバー送信要求メッセージは、ネイバーのリンク層アドレスが識別された後に、ネイバーの到達可能性の確認にも使用されます。ネイバー到達不能検出では、ネイバーの障害またはネイバーへの転送パスの障害が識別されます。この検出は、ホストとネイバー ノード（ホストまたはルータ）間のすべてのパスで使用されます。ネイバー到達不能検出は、ユニキャストパケッ

トだけが送信されるネイバーに対して実行され、マルチキャスト パケットが送信されるネイバーに対しては実行されません。

直近にネイバーに送信したパケットがネイバーで受信され、処理されたことが確認できた場合、ネイバーは到達可能と見なされます。到達可能であるという確認は、接続が動作中（宛先に到達中）であることを示す TCP などの上位層プロトコルからの情報や、ネイバー送信要求メッセージに対するネイバー アドバタイズメント メッセージを受信することで行われます。パケットがピアに到達している場合、それらのパケットは送信元のネクストホップ ネイバーにも到達しています。したがって、転送の進行により、ネクストホップ ネイバーが到達可能であることも確認されます。

ローカル リンク上にない宛先の場合、転送の進行は、ファーストホップ ルータが到達可能であることを暗に意味します。上位層プロトコルからの確認応答がない場合、ノードは、ユニキャスト ネイバー送信要求メッセージを使用してネイバーを探し、転送パスがまだ機能していることを確認します。ネイバーから返信された請求ネイバー アドバタイズメント メッセージは、転送パスがまだ機能しているという肯定確認応答です（請求フラグが値 1 に設定されたネイバー アドバタイズメント メッセージは、ネイバー請求メッセージへの返信としてだけ送信されます）。非送信要求メッセージでは、送信元ノードから宛先ノードへの一方向パスだけが確認されます。送信要求ネイバー アドバタイズメント メッセージは、両方向のパスが機能していることを示します。

（注） 送信要求フラグが値 0 に設定されたネイバー アドバタイズメント メッセージは、転送パスがまだ機能していることを示す肯定確認応答とは見なされません。

ネイバー送信要求メッセージは、ユニキャスト IPv6 アドレスがインターフェイスに割り当てられる前にそのアドレスが一意であることを確認するために、ステートレス自動設定プロセスでも使用されます。新規のリンクローカル IPv6 アドレスに対しては、アドレスがインターフェイスに割り当てられる前に、最初に重複アドレス検出が実行されます（重複アドレス検出の実行中、新規アドレスは一時的な状態のままです）。具体的には、ノードは未指定の送信元アドレスと一時的なリンクローカルアドレスをメッセージの本文に含むネイバー送信要求メッセージを送信します。そのアドレスが別のノードですでに使用されている場合、ノードは一時的なリンクローカルアドレスを含むネイバーアドバタイズメントメッセージを返します。別のノードが同じアドレスの一意性を同時に検証している場合は、そのノードもネイバー送信要求メッセージを返します。ネイバー送信要求メッセージの返信としてネイバー アドバタイズメント メッセージが受信されず、同じ一時アドレスの検証を試行している他のノードからのネイバー送信要求メッセージも受信されない場合、最初のネイバー送信要求メッセージを送信したノードは、一時的なリンクローカルアドレスを一意であると見なし、そのアドレスをインターフェイスに割り当てます。

IPv6 ユニキャスト アドレス（グローバルまたはリンクローカル）はすべてリンクでの一意性を確認する必要があります。ただし、リンクローカルアドレスの一意性が確認されるまで、リンクローカル アドレスに関連付けられた他の IPv6 アドレスに対して重複アドレス検出は実行されません。

ルーター発見

ルータの検出では、ルータ送信要求およびルータ アドバタイズの両方を実行します。ホストは、全ルータのマルチキャストアドレスにルータ送信要求を送信します。ルータは、送信要求または割り込みに対して、デフォルトのルータ情報および MTU やホップ制限などの追加パラメータを含むルータ アドバタイズを送信します。

IPv6 ステートレス自動設定

IPv6 ノードのすべてのインターフェイスは、インターフェイスの ID およびリンクローカル プレフィックス FE80::/10 から自動的に構成されるリンクローカル アドレスを持つ必要があります。リンクローカルアドレスを使用すると、ノードがリンク上の他のノードと通信できます。また、リンクローカル アドレスを使用して、ノードをさらに設定することもできます。

ノードは、ネットワークに接続して自動的にサイトローカルおよびグローバル IPv6 アドレスを生成できます。手動設定や DHCP サーバーなどのサーバーによる支援は必要はありません。IPv6 の場合、リンク上のルータは、ルータ アドバタイズ（RA）メッセージで、任意のサイトローカルプレフィックスやグローバルプレフィックスをアドバタイズしたり、リンクのデフォルト ルータとして機能する意図をアドバタイズしたりします。RA メッセージは、定期的に送信される場合と、システム始動時にホストから送信されるルータ送信要求メッセージに対する応答として送信される場合があります。（次の図を参照してください）。

図 *60 : IPv6* ステートレス自動設定

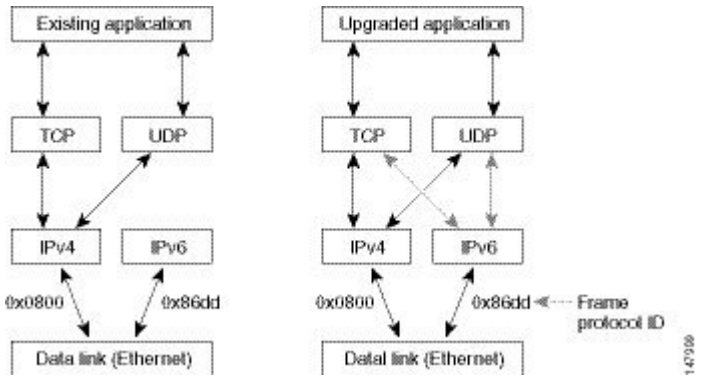
リンク上のノードは、RA メッセージに含まれるプレフィックス（64 ビット）にそのインターフェイス ID（64 ビット）を付加して、自動的にサイトローカル アドレスとグローバル IPv6 アドレスを設定できます。ノードによって設定された 128 ビットの IPv6 アドレスは、重複アドレス検出の対象となり、リンク上での一意性が確保されます。RA メッセージでアドバタイズされたプレフィックスがグローバルに一意である場合、ノードによって設定された IPv6 アドレスもグローバルに一意になります。ICMP パケット ヘッダーのタイプ フィールドの値が 133 であるルータ送信要求メッセージは、システム始動時にホストによって送信されるため、ホストは次のスケジュールされた RA メッセージを待機することなくすぐに自動設定できます。

IPv4 と IPv6 の二重プロトコル スタック

IPv4 と IPv6 の 二重プロトコル スタックは、IPv6 へ移行するための 1 つの方法です。これにより、ノードで稼働しているアプリケーションに対する段階的な 1 つずつのアップグレードが可能になります。ノードで稼働しているアプリケーションは、IPv6 プロトコル スタックを使用するようにアップグレードされます。アップグレードされていない（IPv4 プロトコル スタックしかサポートしない）アプリケーションは、同じノード上でアップグレードされたアプリ

ケーションと共存できます。新しいアプリケーションおよびアップグレードされたアプリケーションは、IPv4 および IPv6 の両方のプロトコル スタックを利用します以下の図を参照してください。）

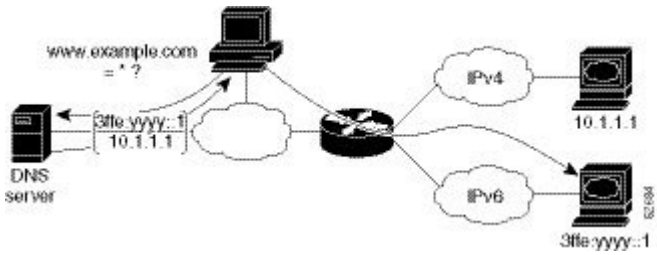
図 *61* : デュアル *IPv4* および *IPv6* プロトコル スタック手法



IPv4 と IPv6 の両方のアドレスおよび DNS 要求をサポートするために、新しい API が定義されています。アプリケーションを新しい API にアップグレードしても、依然として IPv4 プロトコル スタックだけを使用できます。Cisco MDS NX-OS は、IPv4 と IPv6 の二重プロトコル スタックをサポートしています。インターフェイスに IPv4 アドレスと IPv6 アドレスの両方を設定すると、そのインターフェイスは、IPv4 トラフィックと IPv6 トラフィックの両方を受け入れ、処理します。

上の図で、IPv4 と IPv6 の二重プロトコル スタックをサポートするアプリケーションは、DNS サーバから宛先ホスト www.a.com 用に使用できるすべてのアドレスを要求します。DNS サーバーは、www.a.com に使用できるすべてのアドレス（IPv4 アドレスと IPv6 アドレスの両方）を返信します。アプリケーションはアドレスを選択し（ほとんどの場合、IPv6 アドレスがデフォルトの選択肢です）、IPv6 プロトコル スタックを使用して送信元ノードを宛先に接続します。

図 *62* : デュアル *IPv4* および *IPv6* プロトコル スタック アプリケーション



IPv6 用の基本的な接続の設定

ここでは、IPv6の基本的な接続を実装する方法について説明します。一覧内の各作業は、必須と任意に分けています。このセクションは、次のトピックで構成されています。

IPv6 アドレッシングの設定と IPv6 ルーティングの有効化

IPv6 アドレッシングの設定と IPv6 ルーティングの有効化

IPv6 アドレスは、16 ビットの 16 進フィールドをコロン（:）で続けた x:x:x:x:x:x:x:x という形式で表現されます。IPv6アドレスには、通常、連続するゼロの16進フィールドが含まれます。IPv6 アドレスの先頭、中間、または末尾にある連続した 0 の 16 進フィールドを 2 つのコロン（::）を使用して圧縮すると、IPv6 アドレスが使いやすくなります（2 つのコロンは連続した0の16進フィールドを表します）。デフォルトでは、IPv6アドレスは設定されておらず、IPv6処理はディセーブルです。次の種類のインターフェイスに IPv6 アドレスを設定できます。

- ギガビット イーサネット
- 管理
- VLAN（ギガビット イーサネット サブインターフェイス）
- VSAN

インターフェイスにグローバル IPv6 アドレスを設定すると、リンクローカル アドレスが自動的に設定され、そのインターフェイスに対して IPv6 がアクティブになります。また、設定されたインターフェイスは、そのリンクに必要な次のマルチキャスト グループに自動的に加入します。

- 送信要求ノード マルチキャスト グループ FF02:0:0:0:0:1:FF00::/104（インターフェイスに割り当てられた各ユニキャスト アドレス用）
- 全ノード リンクローカル マルチキャスト グループ FF02::1

ここでは、個々のルータ インターフェイスに IPv6 アドレスを割り当て、IPv6 トラフィックの処理をイネーブルにする方法を説明します。デフォルトでは、IPv6アドレスは設定されておらず、IPv6 処理はディセーブルです。

次の種類のインターフェイスに IPv6 アドレスを設定できます。

- ギガビット イーサネット
- 管理
- VLAN（ギガビット イーサネット サブインターフェイス）
- VSAN

（注） **ipv6 address** コマンドの IPv6 アドレス *ipv6-address* 引数は、RFC2373 で文書化されている形式である必要があり、アドレスは 16 進数で指定され、コロンとコロンの間に 16 ビットの値を使用する必要があります。

ipv6 address コマンドの IPv6 プレフィックス *ipv6-prefix* 引数には、RFC 2373 に記載されている形式を使用する必要があります。その場合、16 ビット値を使用した 16 進数でアドレスを指定し、コロンで区切ります。

ipv6 address コマンドの IPv6 プレフィックス長 *prefix-length* 引数は、アドレスのうち連続する上位何ビットがプレフィックス（アドレスのネットワーク部）を構成するかを示す 10 進数値です。10 進数値の前にスラッシュ記号が必要です。

インターフェイスにグローバル IPv6 アドレスを設定すると、リンクローカル アドレスが自動的に設定され、そのインターフェイスに対して IPv6 がアクティブになります。また、設定されたインターフェイスは、そのリンクに必要な次のマルチキャスト グループに自動的に加入します。

- 送信要求ノード マルチキャスト グループ FF02:0:0:0:0:1:FF00::/104（インターフェイスに割り当てられた各ユニキャスト アドレス用）
- 全ノード リンクローカル マルチキャスト グループ FF02::1

（注） 送信要求ノード マルチキャスト アドレスは、ネイバー探索プロセスで使用されます。

各インターフェイスには IPv6 アドレス（スタティックおよび自動設定）を最大 8 つまで設定できます。ただし、管理（mgmt 0）インターフェイスには、スタティック IPv6 アドレスを 1 つだけ設定できます。

IPv4 および IPv6 プロトコル アドレスの構成

シスコ製ネットワーキング デバイスのインターフェイスに IPv4 アドレスと IPv6 アドレスの両方を設定すると、インターフェイスは IPv4 ネットワークと IPv6 ネットワークの両方でデータを送受信できます。

IPv4 と IPv6 の両方のプロトコル スタックをサポートするように Cisco 製ネットワーキング デバイスのインターフェイスを構成するには、次の手順を実行します。

手順

ステップ 1 構成モードに入ります。

```
switch# config t
switch(config)#
```

ステップ 2 インターフェイスを指定し、インターフェイス構成サブモードを開始します。

```
switch(config)# interface gigabitethernet 1/1
switch(config-if)#
```

ステップ 3 インターフェイスに対するプライマリ IPv4 アドレスまたはセカンダリ IPv4 アドレスを指定します。

switch(config-if)# **ip address 192.168.99.1 255.255.255.0**

ステップ 4 インターフェイスに割り当てられている IPv6 ネットワークを指定し、インターフェイスで IPv6 処理を有効にします。

```
switch(config-if)# ipv6 address 2001:0DB8:c18:1::3/64
```

ステップ 5 インターフェイスをイネーブルにします。

```
switch(config-if)# no shutdown
```

ステップ 6 インターフェイス構成サブモードを終了して、構成モードに戻ります。

```
switch(config-if)# exit
switch(config)
```

ステップ 7 IPv6 ユニキャスト データグラムの処理を有効にします。

```
switch(config)# ipv6 routing
```

IPv6 基本接続の設定と動作の確認

情報を表示して、基本的な IPv6 接続の構成 および動作を確認できます。ここでは、次の **show ipv6** コマンドの出力例を示します。

- show ipv6 interface コマンドの出力例
- show ipv6 neighbours コマンドの出力例
- show ipv6 traffic コマンドの出力例

show ipv6 interface コマンドの出力例

次の例では、**show ipv6 interface** コマンドを使用して、IPv6 アドレスがギガビット イーサネット 6/1 インターフェイスに対して正しく構成されていることを確認します。

```
switch# show ipv6 interface mgmt 0
mgmt0 is up
IPv6 is enabled
Global address(es):
2172:22::180/64
Link-local address(es):
fe80::b8db:adff:feba:d074
ND DAD is disabled
ND reachable time is 30000 milliseconds
ND retransmission time is 1000 milliseconds
Stateless autoconfig for addresses disabled
MTU is 1500 bytes
```

show ipv6 neighbours コマンドの出力例

次の例では、**show ipv6 neighbours** コマンドは、すべてのインターフェイスの IPv6 ネイバー探索キャッシュ情報を表示します。

```
switch# show ipv6 neighbours
R - Reachable, I - Incomplete, S - Stale, F - Failed, P - Probe, D - Delay
IPv6 Address Age State Link-layer Addr Interface
fe80::211:5dff:fe53:500a 0 S 0011.5d53.500a GigE6/1
fe80::211:5dff:fe53:500a 0 S 0011.5d53.500a GigE6/2
5000:1::250 0 S 0011.5d53.500a po 4
fe80::211:5dff:fe53:500a 0 S 0011.5d53.500a po 4
fe80::211:5dff:fe53:500a 0 S 0011.5d53.500a po 4
fe80::2d0:3ff:fe61:4800 184 S 00d0.0361.4800 mgmt0
```

次の例では、**show ipv6 neighbours interface** コマンドは、ギガビット イーサネット 6/1 インターフェイスの IPv6 ネイバー探索キャッシュ情報を表示します。

```
switch# show ipv6 neighbours interface gigabitethernet 6/1
R - Reachable, I - Incomplete, S - Stale, F - Failed, P - Probe, D - Delay
IPv6 Address Age State Link-layer Addr Interface
fe80::211:5dff:fe53:500a 0 S 0011.5d53.500a GigE6/1
```

show ipv6 traffic コマンドの出力例

show ipv6 traffic コマンドは、IPv6 および ICMP の統計情報を表示します。

```
switch# show ipv6 traffic
IPv6 Statistics:
Rcvd: 100 total, 0 local destination
0 errors, 0 truncated, 0 too big
0 unknown protocol, 0 dropped
0 fragments, 0 reassembled
0 couldn't reassemble, 0 reassembly timeouts
Sent: 0 generated, 0 forwarded 0 dropped
0 fragmented, 0 fragments created, 0 couldn't fragment

ICMPv6 Statistics:
Rcvd: 100 total, 0 errors, 0 unreachables, 0 time exceeded
0 too big, 0 param probs, 0 admin prohibs
0 echos, 0 echo reply, 0 redirects
0 group query, 0 group report, 0 group reduce
0 router solicit, 69 router advert
0 neighbor solicit, 31 neighbor advert
Sent: 55 total, 0 errors, 0 unreachables, 0 time exceeded
0 too big, 0 param probs, 0 admin prohibs
0 echos, 0 echo reply, 0 redirects
0 group query, 20 group report, 2 group reduce
0 router solicit, 0 router advert
0 neighbor solicit, 33 neighbor advert
```

IPv6 ネイバー探索キャッシュのクリア

IPv6 ネイバー探索キャッシュをクリアするには、EXEC モードで **clear ipv6 neighbor** コマンドを使用します。

```
switch# clear ipv6 neighbor
```

ネイバー探索パラメータの構成の確認

show ipv6 interface コマンドは、ネイバー探索パラメータの構成を表示します。

```
switch# show ipv6 interface mgmt 0
mgmt0 is up
IPv6 is enabled
Global address(es):
2003::1/64
Link-local address(es):
fe80::205:30ff:fe00:533e
ND DAD is enabled, number of DAD attempts: 5
ND reachable time is 50000 milliseconds
ND retransmission time is 3000 milliseconds
Stateless autoconfig for addresses disabled
```

重複アドレス検出試行回数

重複アドレス検出試行回数を構成するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config t
switch(config)#
```

ステップ 2 インターフェイスを指定し、インターフェイス コンフィギュレーション サブモードを開始します。

```
switch(config)# interface gigabitethernet 3/1
switch(config-if)#
```

ステップ 3 重複アドレス検出試行回数を 3 に設定します。指定できる範囲は 0 ～ 15 です。

```
switch(config-if)# ipv6 nd dad attempts 3
```

ステップ 4 デフォルト値（0）に戻します。

```
switch(config-if)# no ipv6 nd dad attempts
```

到達可能性時間

到達可能性時間を構成するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config t
switch(config)#
```

ステップ 2 インターフェイスを指定し、インターフェイス コンフィギュレーション サブモードを開始します。

```
switch(config)# interface gigabitethernet 3/1
switch(config-if)#
```

ステップ 3 再送信時間を 10000 ミリ秒に設定します。有効値は 1000 ～ 3600000 ミリ秒です。

```
switch(config-if)# ipv6 nd reachability-time 10000
```

ステップ 4 デフォルト値（30000 ミリ秒）に戻します。

```
switch(config-if)# no ipv6 nd reachability-time
```

再送信時間

再送信時間を構成するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config t
switch(config)#
```

ステップ 2 インターフェイスを指定し、インターフェイス コンフィギュレーション サブモードを開始します。

```
switch(config)# interface gigabitethernet 3/1
switch(config-if)#
```

ステップ 3 再送信時間を 20000 ミリ秒に設定します。有効値は 1000 ～ 3600000 ミリ秒です。

```
switch(config-if)# ipv6 nd retransmission-timer 20000
```

ステップ 4 デフォルト値（1000 ミリ秒）に戻します。

```
switch(config-if)# no ipv6 nd retransmission-timer
```

ネイバー探索パラメータの構成の確認

show ipv6 interface コマンドは、ネイバー探索パラメータの構成を表示します。

```
switch# show ipv6 interface mgmt 0
mgmt0 is up
IPv6 is enabled
Global address(es):
2003::1/64
Link-local address(es):
fe80::205:30ff:fe00:533e
ND DAD is enabled, number of DAD attempts: 5
ND reachable time is 50000 milliseconds
ND retransmission time is 3000 milliseconds
Stateless autoconfig for addresses disabled
```

IPv6 スタティック ルート

Cisco MDS NX-OS は、IPv6 のスタティック ルートをサポートしています。この項では、次のトピックについて取り上げます。

- IPv6 スタティック ルートの設定
- IPv6 スタティック ルートの設定と動作の確認

IPv6 スタティック ルートの設定

IPv6 スタティック ルートを設定するには、次の手順を実行します。

始める前に

IPv6 スタティック ルートを手動で設定し、2 台のネットワーキング デバイス間の明示的なパスを定義する必要があります。IPv6 スタティック ルートは自動的に更新されないので、ネットワーク トポロジが変化した場合は、手動で再設定する必要があります。

IPv6 スタティック ルートを手動で設定し、2 台のネットワーキング デバイス間の明示的なパスを定義する必要があります。IPv6 スタティック ルートは自動的に更新されないので、ネットワーク トポロジが変化した場合は、手動で再設定する必要があります。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config t
switch(config)#
```

ステップ 2 ギガビット イーサネット インターフェイスのデフォルト IPv6 スタティック ルートを構成します。

```
switch(config)# ipv6 route ::/0 gigabitethernet 3/1
```

ステップ 3 ギガビット イーサネット インターフェイスの完全指定 IPv6 スタティック ルートを構成します。

switch(config)# **ipv6 route 2001:0DB8::/32 gigabitethernet 3/2**

IPv6 スタティック ルートの設定と動作の確認

show ipv6 route コマンドは、スイッチの IPv6 ルート テーブルを表示します。

```
switch# show ipv6 route
IPv6 Routing Table
Codes: C - Connected, L - Local, S - Static G - Gateway
G ::/0
via fe80::211:5dff:fe53:500a, GigabitEthernet6/1, distance 2
G ::/0
via fe80::2d0:3ff:fe61:4800, mgmt0, distance 2
C 2000::/64
via ::, mgmt0
C 2172:22::/64
via ::, mgmt0, distance 2
C 3000:3::/64
via fe80::205:30ff:fe01:7ed6, GigabitEthernet4/1
C 3000:4::/64
via fe80::205:30ff:fe01:7ed6, GigabitEthernet4/1.250
C 3000:5::/64
via fe80::213:1aff:fee5:e69b, GigabitEthernet5/4
C 3000:6::/64
via fe80::213:1aff:fee5:e69b, GigabitEthernet5/4.250
C 3000:7::/64
via fe80::205:30ff:fe01:7ed7, GigabitEthernet4/2
C 3000:8::/64
via fe80::205:30ff:fe01:7ed7, GigabitEthernet4/2.250
C 3000:9::/64
via fe80::213:1aff:fee5:e69e, port-channel 3
C 3000:10::/64
via fe80::213:1aff:fee5:e69e, port-channel 3.250
C 5000:1::/64
via fe80::205:30ff:fe01:3917, GigabitEthernet6/2
C 5000:1::/64
via fe80::205:30ff:fe01:3918, port-channel 4
C 6000:1:1:1::/64
via fe80::205:30ff:fe01:3916, GigabitEthernet6/1
C 7000:1::/64
via fe80::205:30ff:fe01:3917, GigabitEthernet6/2.250
C 7000:1::/64
via fe80::205:30ff:fe01:3918, port-channel 4.250
C 7000:1:1:1::/64
via fe80::205:30ff:fe01:3917, GigabitEthernet6/2, distance 2
L fe80::/10
via ::
L ff00::/8
via ::
```

ギガビット イーサネットの IPv6-ACL に関する注意事項

ギガビット イーサネット インターフェイスで IPv6-ACL を設定する際には、次の注意事項に従ってください。

- Transmission Control Protocol（TCP）または Internet Control Message Protocol（ICMP）だけを使用します。

（注） ユーザー データグラム プロトコル（UDP）やHTTP などの他のプロトコルは、ギガビット イーサネット インターフェイスではサポートされていません。これらのプロトコルに関するルールを含む ACL をギガビット イーサネット インターフェイスに適用することは可能ですが、これらのルールは無効になります。

- インターフェイスをイネーブルにする前に、インターフェイスに IPv6-ACL を適用します。このようにすれば、トラフィックが流れ始める前にフィルタを適用できます。
- 次の条件を確認します。
  - **log-deny** オプションを使用する場合、1 秒ごとに記録されるメッセージ数は最大 50 です。
  - ギガビット イーサネット インターフェイスに **established** オプションを含む IPv6-ACL を適用すると、このオプションは無視されます。
  - 前から存在している TCP 接続に IPv6-ACL のルールを適用しても、このルールは無視されます。たとえば、A と B の間に既存の TCP 接続がある場合に、送信元が A で送信先が B のパケットをすべて廃棄する IPv6-ACL を適用しても、このルールは無効になります。

（注） ギガビット イーサネット インターフェイスに IPv6-ACL がすでに設定されている場合、このインターフェイスをイーサネット ポート チャネル グループに追加できません。IPv6-ACL の設定の詳細については、『Cisco Fabric Manager Security Configuration Guide』『Cisco MDS 9000 Family NX-OS Security Configuration Guide』を参照してください。

インターフェイスへの IPv6-ACL の適用の詳細については、『Cisco Fabric Manager セキュリティ構成ガイド』『Cisco MDS 9000 ファミリ NX-OS セキュリティ構成ガイド』を参照してください。

IPv4 から IPv6 への移行

Cisco MDS NX-OS は、IPv4 から IPv6 への移行メカニズムをサポートしていません。IPv4 から IPv6 への移行には、シスコ ルータ製品の移行スキームを利用できます。ネットワークを移行するように Cisco 製ルータを構成する方法の詳細については、「トンネリングまたは IPv6 の実装」の章を参照してください。

IPv6 の表示

インターフェイスの IPv6 ネイバーの情報を表示するには、**show ips ipv6 neighbours interface** コマンドを使用します。

```
switch# show ips ipv6 neighbours interface gigabitethernet 6/1
IPv6 Address Age (min) Link-layer Addr State Interface
fe80::211:5dff:fe53:500a 0 0011.5d53.500a S Gigabi tEthernet6/1
```

インターフェイスの IPv6 プレフィックスの情報を表示するには、**show ips ipv6 prefix-list interface** コマンドを使用します。

```
switch# show ips ipv6 prefix-list interface gigabitethernet 6/1
Prefix Prefix-len Addr
Valid Preferred
6000:1:1:1:: 64 ::
2592000 604800
```

インターフェイスの IPv6 ルートの情報を表示するには、**show ips ipv6 interface** コマンドを使用します。

```
switch# show ips ipv6 route interface gigabitethernet 6/1
IPv6 Routing Table - 4 entries
Codes: C - Connected, L - Local, S - Static, G - Gateway, M - Multicast
C 6000:1:1:1::/64 is directly connected, GigabitEthernet6/1
C 6000:1:1:1::/64 is directly connected, GigabitEthernet6/1
C fe80::/64 is directly connected, GigabitEthernet6/1
M ff02::/32 is multicast, GigabitEthernet6/1
G ::/0 via fe80::211:5dff:fe53:500a, GigabitEthernet6/1
```

インターフェイスの IPv6 ルータの情報を表示するには、**show ips ipv6 routers interface** コマンドを使用します。

```
switch# show ips ipv6 routers interface gigabitethernet 6/1
Addr Lifetime Expire
fe80::211:5dff:fe53:500a 1800 1781
```

インターフェイスの IPv6 トラフィック統計情報を表示するには、**show ips ipv6 traffic interface** コマンドを使用します。

```
switch# show ips ipv6 traffic interface gigabitethernet 6/1
IPv6 statistics:
Rcvd: 5094 total
0 bad header, 0 unknown option, 0 unknown protocol
0 fragments, 0 total reassembled
0 reassembly timeouts, 0 reassembly failures
Sent: 13625 generated
0 fragmented into 0 fragments, 0 failed
2 no route
```

```
ICMP statistics:
Rcvd: 1264 input, 0 checksum errors, 0 too short
0 unknown info type, 0 unknown error type
unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
parameter: 0 error, 0 header, 0 option
0 hopcount expired, 0 reassembly timeout,0 too big
0 echo request, 0 echo reply
734 group query, 0 group report, 0 group reduce
0 router solicit, 528 router advert, 0 redirects
0 neighbor solicit, 2 neighbor advert
Sent: 6045 output, 0 rate-limited
unreach: 0 routing, 0 admin, 0 neighbor, 1160 address, 0 port
parameter: 0 error, 0 header, 0 option
0 hopcount expired, 0 reassembly timeout,0 too big
0 echo request, 0 echo reply
0 group query, 1466 group report, 0 group reduce
1 router solicit, 0 router advert, 0 redirects
3412 neighbor solicit, 6 neighbor advert
```

デフォルト設定

次の表に、IPv6 パラメータのデフォルト設定を示します。

表 *19 :* デフォルト *IPv6* パラメータ

パラメータ	デフォルト
IPv6 処理	ディセーブル
重複アドレス検出試行回数	0（ネイバー探索ディセーブル）
到達可能性時間	1000 ミリ秒
再送信時間	30000 ミリ秒
IPv6-ACL	なし

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。