



Cisco Fabric Manager IP サービス コンフィギュレーション ガイド

Cisco Fabric Manager IP Services Configuration Guide

Cisco MDS NX-OS リリース 4.2(1)
2009 年 8 月

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

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

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

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

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

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

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

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

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

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

Cisco Fabric Manager IP サービス コンフィギュレーション ガイド
© 2009 Cisco Systems, Inc.
All rights reserved.

Copyright © 2009–2010, シスコシステムズ合同会社.
All rights reserved.



CONTENTS

新しい情報および変更点	xi
はじめに	xiii
対象読者	xiii
マニュアルの構成	xiii
表記法	xiv
関連資料	xv
リリース ノート	xv
準拠規格および安全情報	xv
互換性情報	xv
ハードウェアのインストール	xv
ソフトウェアのインストールおよびアップグレード	xvi
Cisco NX-OS	xvi
Cisco Fabric Manager	xvi
コマンドライン インターフェイス	xvi
インテリジェント ストレージ ネットワーキング サービス コンフィギュレーション ガイド	xvii
トラブルシューティングおよび参照情報	xvii
マニュアルの入手方法およびテクニカル サポート	xvii
<hr/> CHAPTER 1	
IP サービスの概要	1-1
FCIP	1-1
SAN 拡張チューナ	1-2
iSCSI	1-2
IP サービス	1-2
IP ストレージ	1-2
IPv4 および IPv6	1-3
<hr/> CHAPTER 2	
FCIP の設定	2-1
FCIP について	2-1
FCIP の概念	2-2
FCIP および VE Ports	2-2
FCIP リンク	2-3
FCIP プロファイル	2-4

FCIP インターフェイス	2-4
FCIP ハイアベイラビリティ ソリューション	2-4
ファイバ チャンネル PortChannel	2-5
FSPF	2-5
VRRP	2-6
イーサネット PortChannel	2-6
イーサネット PortChannel およびファイバ チャンネル PortChannel	2-7
FCIP の設定	2-8
FCIP のイネーブル化	2-8
FCIP Wizard の使用	2-8
基本 FCIP 設定	2-15
FCIP プロファイルの作成	2-15
FCIP リンクの作成	2-16
インターフェイスおよび拡張リンク プロトコルの確認	2-17
トランク ステータスのチェック	2-17
Cisco Transport Controller の起動	2-17
FCIP プロファイルの高度な設定	2-18
TCP パラメータの設定	2-18
FCIP インターフェイスの詳細設定	2-21
ピアの設定	2-21
ピア IP アドレスの割り当て	2-21
アクティブ接続の設定	2-22
タイム スタンプ制御の有効化	2-22
FCIP B ポート 相互運用性モード	2-23
Quality of Service	2-26
E ポートの設定	2-26
FCIP の拡張機能	2-27
FCIP 書き込みアクセラレーション	2-27
FCIP 書き込みアクセラレーションの設定	2-29
FCIP テープ アクセラレーション	2-29
FCIP テープ アクセラレーションの設定	2-34
FCIP 圧縮	2-34
デフォルト設定	2-36

CHAPTER 3

SAN 拡張チューナの設定	3-1
SAN 拡張チューナについて	3-1
SAN 拡張チューナの設定	3-3
データ パターン	3-3
ライセンス要件	3-3

SAN 拡張チューナの設定	3-4
FCIP リンクのチューニング	3-4
SAN 拡張チューナ ウィザードの使用法	3-4
デフォルト設定	3-7

CHAPTER 4

iSCSI の設定	4-1
iSCSI の概要	4-2
iSCSI 設定制限の概要	4-4
iSCSI の設定	4-4
iSCSI のイネーブル化	4-5
iSCSI インターフェイスの作成	4-6
iSCSI ウィザードの使用	4-7
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	4-9
ダイナミック マッピング	4-10
スタティック マッピング	4-12
iSCSI 仮想ターゲットの設定例	4-14
iSCSI ホストの仮想ファイバ チャネル ホストとしての提示	4-16
イニシエータの識別	4-16
イニシエータ プレゼンテーション モード	4-17
iSCSI の VSAN メンバシップ	4-24
iSCSI デバイスの VSAN メンバシップの例	4-25
iSCSI ホストの詳細な VSAN メンバシップ	4-26
iSCSI アクセス コントロール	4-26
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	4-27
iSCSI ベースのアクセス コントロール	4-28
アクセス コントロールの実行	4-29
iSCSI セッション認証	4-30
認証メカニズムの設定	4-31
ローカル認証の設定	4-32
iSCSI イニシエータ認証の制約	4-32
相互 CHAP 認証の設定	4-33
iSCSI RADIUS サーバの設定	4-33
iSCSI の即時データ機能と非請求データ機能	4-34
iSCSI インターフェイスの詳細機能	4-34
iSCSI リスナー ポート	4-34
TCP 調整パラメータ	4-34
QoS 値の設定	4-35
iSCSI ルーティング モード	4-35
iSLB の設定	4-37

iSLB 設定制限の概要	4-38
iSLB 設定の前提条件	4-39
iSLB イニシエータの概要	4-39
Device Manager を使用した iSLB の設定	4-39
iSLB イニシエータの設定	4-42
WWN の iSLB イニシエータへの割り当て	4-42
ダイナミック iSLB イニシエータの WWN マッピングをスタティックにする	4-42
iSLB イニシエータの VSAN メンバシップの割り当て	4-43
ロード バランシングのメトリックの設定	4-43
iSLB イニシエータ ターゲットの設定	4-43
iSLB のイニシエータおよびイニシエータ ターゲットのゾーンの設定とアクティブ化	4-45
iSLB セッション認証の設定	4-45
VRRP を使用するロード バランシングの概要	4-46
iSCSI インターフェイス パラメータの変更とロード バランシングに対するその影響	4-48
ギガビット イーサネット インターフェイス選択のための VRRP ロード バランシング アルゴリズム	4-48
VRRP を使用するロード バランシングの設定	4-49
CFS を使用した iSLB 設定配信の概要	4-49
CFS を使用した iSLB 設定の配信	4-50
iSLB 設定配信のイネーブル化	4-51
ファブリックのロック	4-51
ファブリックに対する変更の確定	4-52
保留中の変更の廃棄	4-52
ファブリックのロックの解除	4-52
CFS マージ プロセス	4-53
iSLB CFS マージ ステータスの矛盾	4-53
iSCSI ハイ アベイラビリティ	4-53
透過的なターゲット フェールオーバー	4-54
マルチパス ソフトウェアを実行しているホストでの iSCSI ハイ アベイラビリティ	4-54
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	4-55
ストレージ ポート フェールオーバーの LUN trespass	4-56
同一 IP ネットワークに接続された複数の IPS ポート	4-57
VRRP ベースのハイ アベイラビリティ	4-59
イーサネット PortChannel ベースのハイ アベイラビリティ	4-60
iSCSI 認証セットアップに関する注意事項とシナリオ	4-60
認証なしの設定	4-61
ローカル パスワード データベースを使用した CHAP の設定	4-61

外部 RADIUS サーバを使用した CHAP の設定	4-62
iSCSI トランスペアレント モード イニシエータ	4-63
ターゲットストレージ デバイスに必要な LUN マッピング	4-67
iSNS	4-72
iSNS クライアント機能の概要	4-72
iSNS クライアント プロファイルの作成	4-73
iSNS サーバ機能の概要	4-75
シナリオの例	4-75
iSNS サーバの設定	4-76
iSNS サーバのイネーブル化	4-76
iSNS 設定配布	4-77
ESI 再試行カウントの設定	4-77
登録期間の設定	4-77
iSNS クライアント登録および登録解除	4-78
ターゲット検出	4-78
iSNS クラウド検出	4-79
クラウド検出の概要	4-79
iSNS クラウド検出の設定	4-80
iSNS クラウド検出のイネーブル化	4-80
オンデマンド iSNS クラウド検出の開始	4-80
自動 iSNS クラウド検出の設定	4-80
iSNS クラウド検出配布の設定	4-81
デフォルト設定	4-81
CHAPTER 5	IP サービスの設定
	5-1
トラフィック管理サービス	5-2
管理インターフェイスの設定	5-2
デフォルト ゲートウェイ	5-3
デフォルト ゲートウェイの概要	5-3
デフォルト ゲートウェイの設定	5-4
IPv4 デフォルト ネットワークの設定	5-6
IPFC	5-7
IPFC 設定時の注意事項	5-8
IPv4 スタティック ルート	5-8
オーバーレイ VSAN	5-8
オーバーレイ VSAN の概要	5-8
オーバーレイ VSAN の設定	5-9
複数の VSAN の設定	5-10

仮想ルータ冗長プロトコル	5-11
VRRP の概要	5-11
VRRP の設定	5-13
仮想ルータの追加および削除	5-13
仮想ルータの起動	5-13
仮想ルータ IP アドレスの追加	5-13
仮想ルータのプライオリティの設定	5-14
アダバタイズ パケットのタイム インターバルの設定	5-14
プライオリティのプリエンプトの設定またはイネーブル化	5-14
仮想ルータの認証の設定	5-14
インターフェイスのステート追跡に基づいたプライオリティ	5-15
DNS サーバの設定	5-15
デフォルト設定	5-15

CHAPTER 6

IP ストレージの設定	6-1
サービス モジュール	6-1
モジュール ステータスの確認	6-3
IPS モジュールのアップグレード	6-3
MPS-14/2 モジュールのアップグレード	6-3
サポートされているハードウェア	6-3
IPv4 のギガビット イーサネット インターフェイスの設定	6-4
ギガビット イーサネットの基本設定	6-5
インターフェイスの説明の設定	6-5
ビーコン モードの設定	6-6
自動ネゴシエーションの設定	6-6
MTU フレーム サイズの設定	6-6
無差別モードの設定	6-6
ギガビット イーサネットの VLAN について	6-6
インターフェイスのサブネットの要件	6-7
ギガビット イーサネット接続の確認	6-7
ギガビット イーサネットの IPv4-ACL に関する注意事項	6-8
ギガビット イーサネットのハイ アベイラビリティの設定	6-8
iSCSI および FCIP サービスの VRRP	6-8
ギガビット イーサネット インターフェイスに対する VRRP の設定	6-9
イーサネット PortChannel の集約の概要	6-10
イーサネット PortChannel の設定	6-11
Cisco Discovery Protocol (CDP) の設定	6-11
デフォルト設定	6-11

CHAPTER 7

ギガビットイーサネットインターフェイスの IP バージョン 4 (IPv4) の設定 7-1

IPv4 の概要	7-1
IPv4 の基本的なギガビットイーサネットの設定	7-2
インターフェイスの説明の設定	7-3
ビーコンモードの設定	7-3
自動ネゴシエーションの設定	7-3
MTU フレームサイズの設定	7-4
無差別モードの設定	7-4
VLAN	7-5
ギガビットイーサネットの VLAN について	7-5
VLAN サブインターフェイスの設定	7-5
インターフェイスのサブネットの要件	7-6
IPv4-ACL	7-6
ギガビットイーサネット IPv4-ACL の注意事項	7-7
デフォルト設定	7-7

CHAPTER 8

ギガビットイーサネットインターフェイスの IP バージョン 6 (IPv6) の設定 8-1

IPv6 の概要	8-1
一意なアドレスに対する拡張 IPv6 アドレス領域	8-2
IPv6 アドレスのフォーマット	8-2
IPv6 アドレスプレフィックスのフォーマット	8-3
IPv6 アドレスタイプ: ユニキャスト	8-3
グローバルアドレス	8-3
リンクローカルアドレス	8-4
IPv6 アドレスタイプ: マルチキャスト	8-5
IPv6 のインターネット制御メッセージプロトコル (ICMP)	8-6
IPv6 Path MTU Discovery	8-7
IPv6 近隣探索	8-7
IPv6 ネイバー送信要求メッセージおよびアドバタイズメントメッセージ	8-7
ルータの検出	8-9
IPv6 ステートレス自動設定	8-9
IPv4 と IPv6 の二重プロトコルスタック	8-10
IPv6 用の基本的な接続の設定	8-11
IPv6 アドレッシングの設定および IPv6 ルーティングのイネーブル化	8-11
IPv4 および IPv6 プロトコルアドレスの設定	8-13
IPv6 スタティックルートの設定	8-13
IPv6 スタティックルートの設定	8-13
ギガビットイーサネット IPv6-ACL の注意事項	8-14

IPv4 から IPv6 への移行	8-14
デフォルト設定	8-15

INDEX



新しい情報および変更点

Cisco MDS NX-OS リリース 4.2(1) では、次の情報に関する新しい機能固有のコンフィギュレーションガイドで、ソフトウェア コンフィギュレーション情報が利用できるようになりました。

- システム管理
- インターフェイス
- ファブリック
- Quality of Service
- セキュリティ
- IP サービス
- ハイ アベイラビリティおよび冗長性

これらの新しいガイドにある情報は、以前は、『*Cisco MDS 9000 Family CLI Configuration Guide*』および『*Cisco MDS 9000 Family Fabric Manager Configuration Guide*』に記載されていました。これらのコンフィギュレーションガイドは、現在でも Cisco.com で提供されており、MDS NX-OS リリース 4.2(1) 以前のすべてのソフトウェア リリースで使用することをお勧めします。各ガイドでは、特定のリリースで導入された機能や利用できる機能について説明しています。ご使用のスイッチにインストールされているソフトウェアに関するコンフィギュレーションガイドを選択して参照してください。

マニュアル タイトルの完全なリストについては、「はじめに」の関連資料のリストを参照してください。

Cisco MDS NX-OS リリース 4.2(x) に関する詳細については、シスコ システムズの Web サイトから入手可能な『*Cisco MDS 9000 Family Release Notes*』を参照してください。

http://www.cisco.com/en/US/products/ps5989/prod_release_notes_list.htm

このマニュアルについて

新しい『*Cisco Fabric Manager IP サービス コンフィギュレーションガイド*』に記載の情報は、従来、『*Cisco MDS 9000 Family Fabric Manager Configuration Guide*』の「Part 6: IP Services」に記載されていたものです。

表 1 に、このガイドで説明する、MDS NX-OS リリース 4.2(1) からの新機能および変更された機能を示します。

表 1 Cisco MDS NX-OS リリース 4.2(x) の新機能および変更された機能

機能	新規および変更トピック	対象リリース	参照項目
モジュール単位の iSCSI イネーブラ	Fabric Manager または Device Manager を使用して、モジュールで iSCSI をイネーブルまたはディセーブルにするモードを追加しました。	4.2(1)	第 4 章 「iSCSI の設定」
CCP および IP ルート	Fabric Manager を使用して、IP ルートを設定するための手順を追加しました。 Fabric Manager および Device Manager を使用して、デフォルトのゲートウェイ設定中の CCP インターフェイスのサポートを追加しました。	4.2(1)	第 5 章 「IP サービスの設定」



はじめに

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

対象読者

このマニュアルは、マルチレイヤ ディレクタおよびファブリック スイッチの Cisco MDS 9000 ファミリの設定および保守を担当する、経験豊富なネットワーク管理者を対象にしています。

マニュアルの構成

このマニュアルは、次の章で構成されています。

章	タイトル	説明
第 1 章	IP サービスの概要	Cisco MDS 9000 NX-OS ソフトウェアでサポートされるインテリジェント ストレージ サービスの概要を説明します。
第 2 章	FCIP の設定	IP ホストが 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るようにするためのスイッチの設定について説明します。
第 3 章	SAN 拡張チューナの設定	FCIP パフォーマンスを最適化する SAN Extension Tuner (SET) 機能について説明します。
第 4 章	iSCSI の設定	Cisco MDS 9200 スイッチまたは Cisco MDS 9500 ディレクタで使用可能な IPS モジュール固有の iSCSI 機能について説明します。
第 5 章	IP サービスの設定	IP over Fibre Channel (IPFC) サービスについて詳述するとともに、IPFC、仮想ルータ、および DNS サーバの設定情報も示します。

章	タイトル	説明
第 6 章	IP ストレージの設定	FCIP を使用して IP ネットワークを通じて別個の SAN アイランドを接続することによってファイバチャネル SAN の到達範囲を拡大する方法、および IP ホストが iSCSI プロトコルを使用して FC ストレージにアクセスできるようにする方法について詳述します。
第 7 章	ギガビット イーサネット インターフェイスの IP バージョン 4 (IPv4) の設定	Cisco MDS 9000 ファミリ スイッチで提供される IPv4 プロトコル サポートについて説明します。
第 8 章	ギガビット イーサネット インターフェイスの IP バージョン 6 (IPv6) の設定	Cisco MDS 9000 ファミリ スイッチで提供される IPv6 プロトコル サポートについて説明します。

表記法

コマンドの説明では、次の表記法を使用しています。

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

出力例では、次の表記法を使用しています。

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

このマニュアルでは、次の表記法を使用しています。



(注)

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



注意

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

関連資料

Cisco MDS 9000 ファミリー向けのマニュアルセットには、次のマニュアルが含まれています。マニュアルをオンラインで検索するには、次のサイトにある Cisco MDS NX-OS Documentation Locator を使用してください。

http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/roadmaps/doclocator.htm

リリース ノート

- 『Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Releases』
- 『Cisco MDS 9000 Family Release Notes for MDS SAN-OS Releases』
- 『Cisco MDS 9000 Family Release Notes for Storage Services Interface Images』
- 『Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images』
- 『Release Notes for Cisco MDS 9000 Family Fabric Manager』

準拠規格および安全情報

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

互換性情報

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

ハードウェアのインストール

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

ソフトウェアのインストールおよびアップグレード

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

Cisco NX-OS

- 『Cisco MDS 9000 Family NX-OS Licensing Guide』
- 『Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS System Management Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS Fabric Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS Quality of Service Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS Security Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS IP Services Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS Intelligent Storage Services Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide』

Cisco Fabric Manager

- 『Cisco Fabric Manager Fundamentals Configuration Guide』
- 『Cisco Fabric Manager System Management Configuration Guide』
- 『Cisco Fabric Manager Interfaces Configuration Guide』
- 『Cisco Fabric Manager Fabric Configuration Guide』
- 『Cisco Fabric Manager Quality of Service Configuration Guide』
- 『Cisco Fabric Manager Security Configuration Guide』
- 『Cisco Fabric Manager IP サービス コンフィギュレーション ガイド』 (本書)
- 『Cisco Fabric Manager Intelligent Storage Services Configuration Guide』
- 『Cisco Fabric Manager High Availability and Redundancy Configuration Guide』
- 『Cisco Fabric Manager Inter-VSAN Routing Configuration Guide』
- 『Cisco Fabric Manager Online Help』
- 『Cisco Fabric Manager Web Services Online Help』

コマンドライン インターフェイス

- 『Cisco MDS 9000 Family Command Reference』

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

- 『Cisco MDS 9000 I/O Acceleration Configuration Guide』
- 『Cisco MDS 9000 Family SANTap Deployment Guide』
- 『Cisco MDS 9000 Family Data Mobility Manager Configuration Guide』
- 『Cisco MDS 9000 Family Storage Media Encryption Configuration Guide』
- 『Cisco MDS 9000 Family Secure Erase Configuration Guide』
- 『Cisco MDS 9000 Family Cookbook for Cisco MDS SAN-OS』

トラブルシューティングおよび参照情報

- 『Cisco NX-OS System Messages Reference』
- 『Cisco MDS 9000 Family NX-OS Troubleshooting Guide』
- 『Cisco MDS 9000 Family NX-OS MIB Quick Reference』
- 『Cisco MDS 9000 Family NX-OS SMI-S Programming Reference』
- 『Cisco MDS 9000 Family Fabric Manager Server Database Schema』

マニュアルの入手方法およびテクニカル サポート

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

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

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



CHAPTER 1

IP サービスの概要

Cisco MDS 9000 NX-OS ソフトウェアは、FCIP、Storage Area Network (SAN; ストレージエリアネットワーク) 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。Virtual Routing Redundancy Protocol (VRRP; 仮想ルータ冗長プロトコル) 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。

この章の内容は、次のとおりです。

- 「FCIP」(P.1-1)
- 「SAN 拡張チューナ」(P.1-2)
- 「iSCSI」(P.1-2)
- 「IP サービス」(P.1-2)
- 「IP ストレージ」(P.1-2)
- 「IPv4 および IPv6」(P.1-3)

FCIP

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 の設定の詳細については、第 2 章「FCIP の設定」を参照してください。

SAN 拡張チューナ

SAN Extension Tuner (SET; SAN 拡張チューナ) 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、第 3 章「SAN 拡張チューナの設定」を参照してください。

iSCSI

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装置は、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 の設定の詳細については、第 4 章「iSCSI の設定」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。IP スタティックルーティング機能は、VSAN 間のトラフィックをルーティングするのに使用されます。この章では、Fabric Manager および Device Manager を使用した IP ルートの設定手順についても説明します。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、第 5 章「IP サービスの設定」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 モジュールおよび MPS-14/2 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、第 6 章「IP ストレージの設定」を参照してください。

IPv4 および 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)、グローバルユニーク アドレスなどのサービスを提供しながら、既存の IPv4 ユーザが簡単に IPv6 に移行することができるように設計されました。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。

ギガビット イーサネット インターフェイス用の IPv4 設定の詳細については、[第 7 章「ギガビット イーサネット インターフェイスの IP バージョン 4 \(IPv4\) の設定」](#)を参照してください。

ギガビット イーサネット インターフェイス用の IPv6 設定の詳細については、[第 8 章「ギガビット イーサネット インターフェイスの IP バージョン 6 \(IPv6\) の設定」](#)を参照してください。



CHAPTER 2

FCIP の設定

Cisco MDS 9000 ファミリの IP Storage (IPS; IP ストレージ) 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して、ファイバチャネル Storage Area Network (SAN; ストレージエリアネットワーク) 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、別の SAN アイランドに接続できます。



(注) FCIP は、MDS 9222i スイッチ、MSM-18/4 モジュール、MDS 9216i スイッチ、MPS-14/2 モジュール、16 ポートストレージサービス ノード (SSN-16)、および MDS 9200 シリーズディレクトリの IPS モジュールでサポートされています。

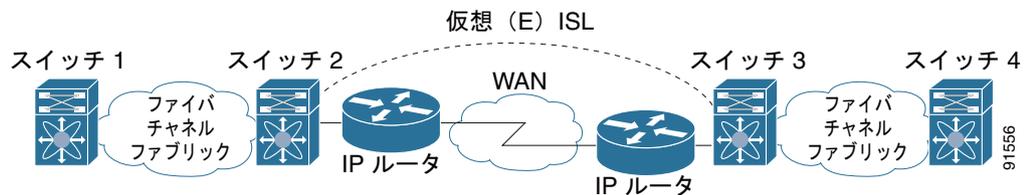
この章の内容は、次のとおりです。

- 「FCIP について」 (P.2-1)
- 「FCIP の設定」 (P.2-8)
- 「FCIP Wizard の使用」 (P.2-8)
- 「デフォルト設定」 (P.2-36)

FCIP について

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 Local Area Network (LAN; ローカルエリアネットワーク)、Metropolitan Area Network (MAN; メトロポリタンエリアネットワーク)、および Wide Area Network (WAN; ワイドエリアネットワーク) 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 (図 2-1 を参照)。

図 2-1 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 レイヤ トランスポートとして TCP を使用します。DF ビットは TCP ヘッダーとして設定されます。



(注)

FCIP プロトコルの詳細については、IP ストレージの IETF 標準を参照してください (<http://www.ietf.org>)。また、スイッチ バックボーン接続に関するファイバ チャンネル標準も参照してください (<http://www.t11.org> の FC-BB-2 を参照)。

ここで説明する内容は、次のとおりです。

- 「FCIP の概念」 (P.2-2)
- 「FCIP ハイアベイラビリティ ソリューション」 (P.2-4)
- 「イーサネット PortChannel およびファイバ チャンネル PortChannel」 (P.2-7)

FCIP の概念

IPS モジュールまたは MPS-14/2 モジュールを FCIP 用に設定するには、次に示す基本的な概念を理解しておく必要があります。

- 「FCIP および VE Ports」 (P.2-2)
- 「FCIP リンク」 (P.2-3)
- 「FCIP プロファイル」 (P.2-4)
- 「FCIP インターフェイス」 (P.2-4)

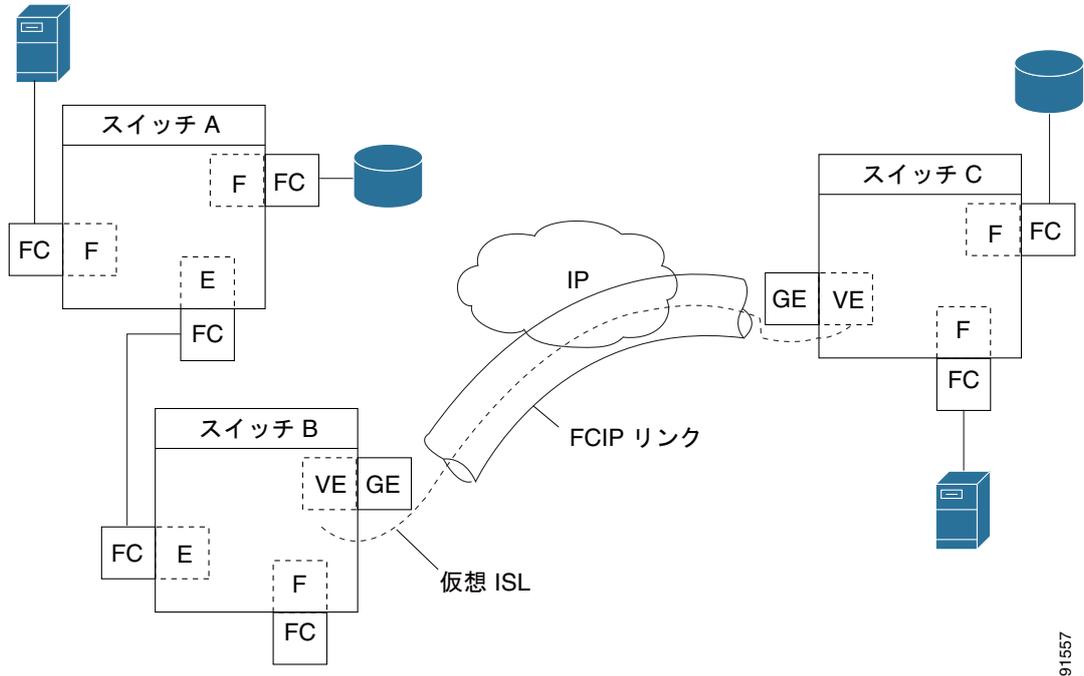
FCIP および VE Ports

図 2-2 に、ファイバ チャンネル Inter-Switch Link (ISL; スイッチ間リンク) およびシスコの拡張 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 チャンネルではなく FCIP を介して転送される点を除き、標準ファイバ チャンネル E ポートとまったく同様に機能します。唯一の要件は、VE ポートの反対側を別の VE ポートにすることです。

仮想 ISL は FCIP リンク上に確立され、ファイバ チャンネル トラフィックを転送します。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 チャンネル ISL と似ています (図 2-2 を参照)。

図 2-2 FCIP リンクおよび仮想 ISL



91557

詳細については、「E ポートの設定」(P.2-26) を参照してください。

FCIP リンク

FCIP リンクは、2つの FCIP リンク エンドポイントを結ぶ 1つ以上の 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 を始動します。

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

- 1つの接続はデータ フレーム用です。
- もう1つの接続はファイバ チャネル コントロール フレーム、つまりスイッチ/スイッチ プロトコル フレーム (すべてのクラス F) 専用です。これにより、すべてのコントロール フレームの遅延が軽減されます。

IPS モジュールまたは MPS-14/2 モジュールで FCIP をイネーブルにするには、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) を設定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、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) に基づきます。

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、および 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。

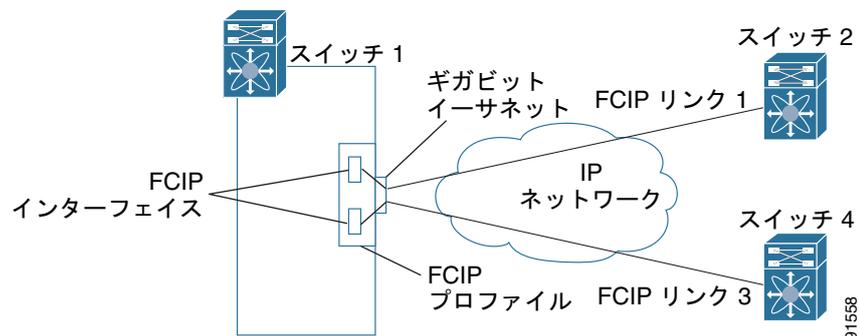
FCIP プロファイル

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ています。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 リンクが終端するギガビット イーサネット 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（図 2-3 を参照）。

図 2-3 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 プロファイルは、FCIP リンクを開始するギガビット イーサネット 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

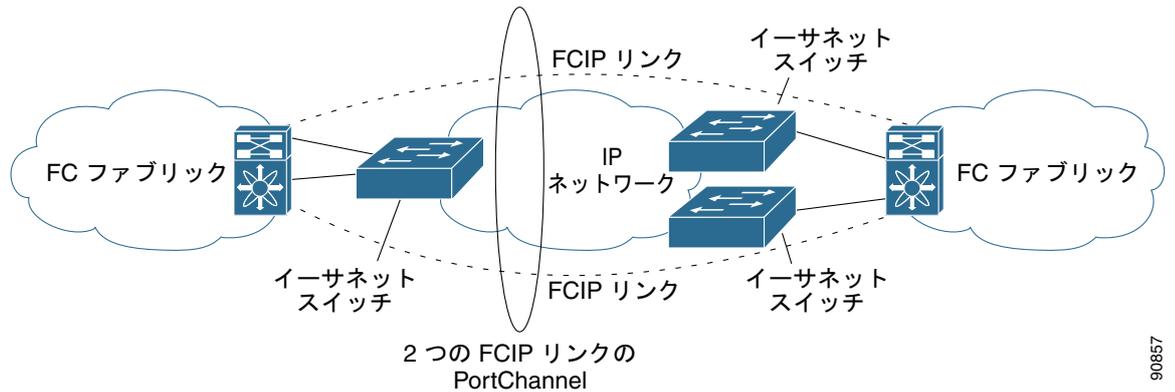
FCIP 設定で使用できるハイアベイラビリティ ソリューションは、次のとおりです。

- 「ファイバ チャネル PortChannel」(P.2-5)
- 「FSPF」(P.2-5)
- 「VRRP」(P.2-6)
- 「イーサネット PortChannel」(P.2-6)

ファイバチャネル PortChannel

図 2-4 に、PortChannel ベースのロード バランシング設定例を示します。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ってリンク障害に対応します。

図 2-4 PortChannel ベースのロード バランシング



90857

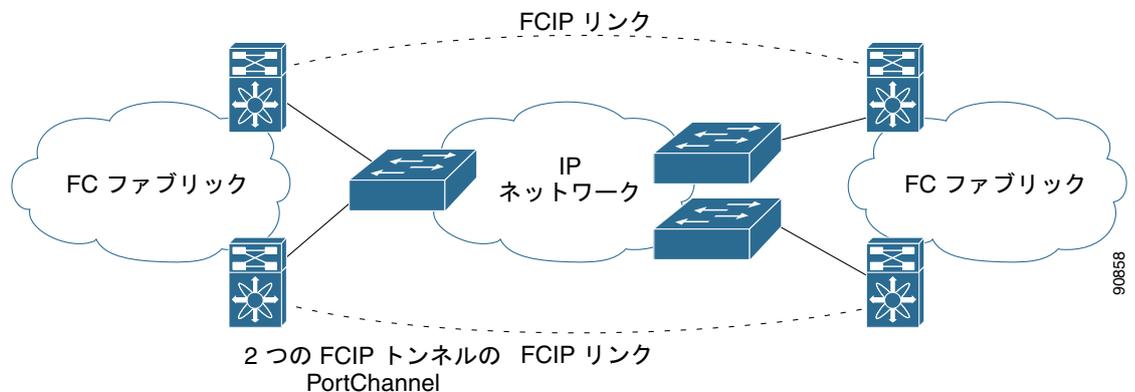
ファイバチャネル PortChannel ソリューションは、次の特性によって他のソリューションから区別されます。

- バンドル全体が 1 つの論理 (E) ISL リンクになります。
- PortChannel 内のすべての FCIP リンクが、同じ 2 つのスイッチ間に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 PortChannel 内の FCIP リンク間でロード バランシングされます。

FSPF

図 2-5 に、FSPF ベースのロード バランシングの設定例を示します。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 リンク障害に対応します。

図 2-5 Fabric Shortest Path First (FSPF) ベースのロード バランシング



90858

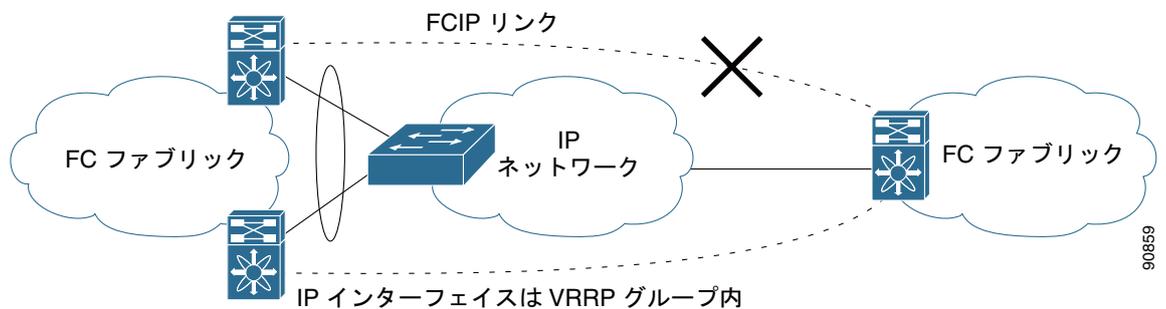
FSPF ソリューションは、次の特性によって他のソリューションから区別されます。

- 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 アイランドの複数のスイッチを接続できます。
- 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。

VRRP

図 2-6 に、Virtual Router Redundancy Protocol (VRRP; 仮想ルータ冗長プロトコル) ベースのハイアベイラビリティ FCIP 設定例を示します。この設定では、VRRP を使用してハイアベイラビリティを実装する必要のあるアイランドのイーサネットスイッチに対して、少なくとも 2 つの物理ギガビットイーサネットポートを接続する必要があります。

図 2-6 VRRP ベースのハイアベイラビリティ



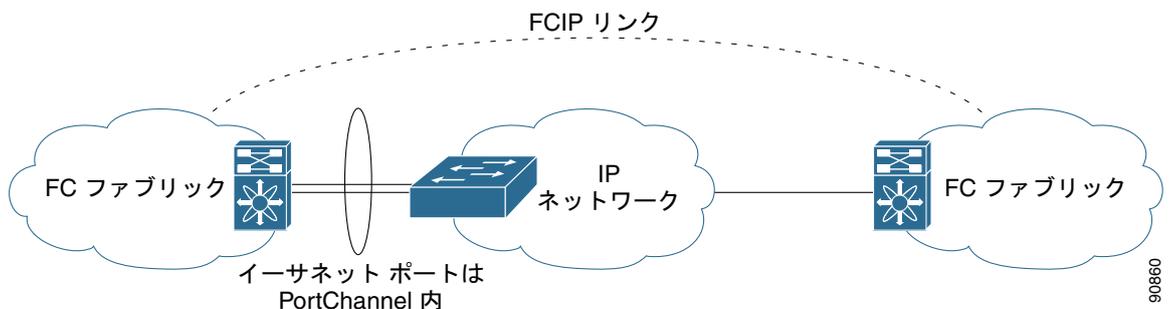
VRRP ソリューションは、次の特性によってその他のソリューションから区別されます。

- アクティブ VRRP ポートに障害が発生すると、スタンバイ VRRP ポートが VRRP IP アドレスを引き継ぎます。
- VRRP スイッチオーバーが発生すると、FCIP リンクは自動的に解除されて、再接続されます。
- この設定では、FCIP (E) ISL リンクを 1 つだけ使用します。

イーサネット PortChannel

図 2-7 に、イーサネット PortChannel ベースのハイアベイラビリティ FCIP の例を示します。このソリューションは、各ギガビットイーサネットリンク障害によって引き起こされる問題を解決します。

図 2-7 イーサネット PortChannel ベースのハイアベイラビリティ



イーサネット PortChannel 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。

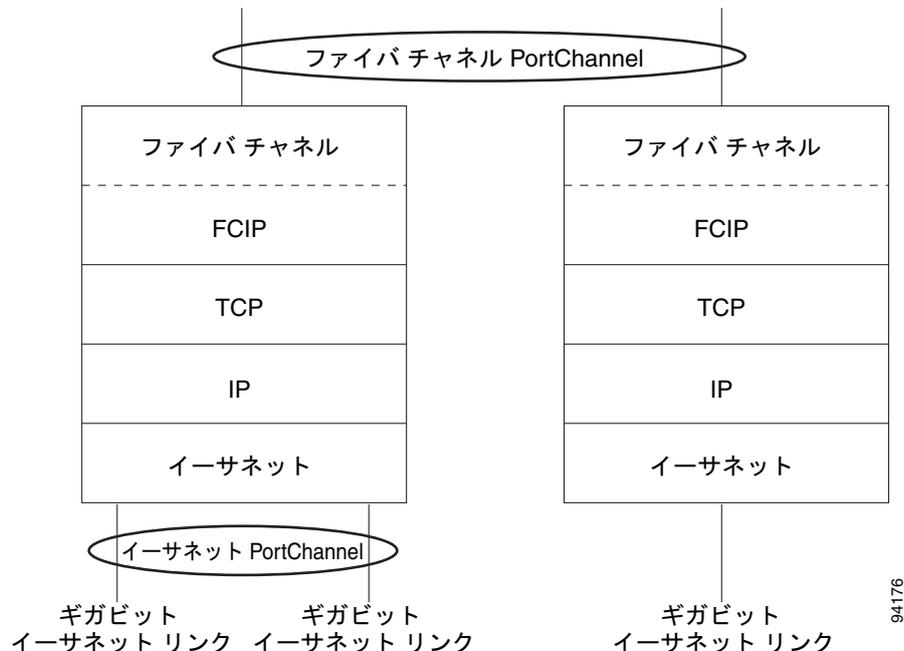
- ギガビットイーサネットリンクレベルの冗長性により、ギガビットイーサネットリンクの1つに障害が発生した場合も、透過的なフェールオーバーが実現します。
- イーサネット PortChannel 上の2つのギガビットイーサネットポートが、1つの論理ギガビットイーサネットリンクのように表示されます。
- フェールオーバー中に、FCIP リンクはアップ状態のままです。

イーサネット PortChannel およびファイバチャネル PortChannel

イーサネット PortChannel では、Cisco MDS 9000 ファミリースイッチのギガビットイーサネットポートと接続しているイーサネットスイッチ間でのリンク冗長性が確保されます。ファイバチャネル PortChannel でも、ファイバチャネルスイッチ間での (E) ISL リンクの冗長性が確保されます。FCIP は (E) ISL リンクで、ファイバチャネル PortChannel だけに適用されます。FCIP レベルの下で、FCIP リンクはイーサネット PortChannel 上または1つのギガビットイーサネットポート上で稼働できます。このリンクは、ファイバチャネルレイヤに対して完全に透過的です。

イーサネット PortChannel の制約により、1つのイーサネット PortChannel 内で組み合わせて使用できる IPS ポートは、連続する2つのポート（ポート1～2や3～4）です（詳細については第6章「ギガビットイーサネットのハイアベイラビリティの設定」を参照してください）。この制約が適用されるのは、イーサネット PortChannel だけです。ファイバチャネル PortChannel (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 PortChannel 内で組み合わせて使用できる (E) ISL リンクに制約はありません（詳細については『Cisco Fabric Manager Interfaces Configuration Guide』を参照してください）。ファイバチャネル PortChannel に加えることのできるファイバチャネルポートの数は最大で16です（図2-8を参照）。

図 2-8 ファイバチャネルおよびイーサネットレベルの PortChannel



ファイバチャネル PortChannel を設定するには、『Cisco Fabric Manager Interfaces Configuration Guide』を参照してください。

イーサネット PortChannel を設定するには、『Cisco Fabric Manager High Availability and Redundancy Configuration Guide』を参照してください。

FCIP の設定

ここでは、FCIP を設定する方法について説明します。内容は次のとおりです。

- 「FCIP のイネーブル化」 (P.2-8)
- 「基本 FCIP 設定」 (P.2-15)
- 「インターフェイスおよび拡張リンク プロトコルの確認」 (P.2-17)
- 「トランク ステータスのチェック」 (P.2-17)
- 「FCIP プロファイルの高度な設定」 (P.2-18)
- 「FCIP インターフェイスの詳細設定」 (P.2-21)
- 「E ポートの設定」 (P.2-26)
- 「E ポートの設定」 (P.2-26)
- 「FCIP の拡張機能」 (P.2-27)

FCIP のイネーブル化

FCIP 機能の設定を開始するには、ファブリック内で必要なスイッチ上で 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、Cisco MDS 9000 ファミリの全スイッチでこの機能がディセーブルに設定されています。

FCIP 機能を設定および確認する操作は、スイッチ上で FCIP がイネーブルに設定されていないと使用できません。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。

FCIP 機能を使用するには、IP 経由 SAN 拡張パッケージ ライセンス (SAN_EXTN_OVER_IP または SAN_EXTN_OVER_IP_IPS4) を入手する必要があります (『Cisco MDS 9000 Family NX-OS Licensing Guide』を参照)。デフォルトで、MDS 9222i および 9216i スイッチには IP 経由 SAN 拡張パッケージ ライセンスが同梱されています。

FCIP Wizard の使用



(注)

Cisco MDS SAN-OS リリース 2.0 以降および NX-OS リリース 4.x は、既存のファブリックの一部ではないスイッチにログインするための追加のログインプロンプトがあります。

Fabric Manager を使用して FCIP リンクの作成と管理を行うには、FCIP Wizard を使用します。IP サービス モジュールが必要な Cisco MDS 9000 ファミリ スイッチに挿入されていることと、そのスイッチ上のギガビット イーサネット インターフェイスが接続されていて、接続が確認されていることを確認します。FCIP Wizard を使用した FCIP リンクの作成手順は次のとおりです。

- エンドポイントを選択します。
- インターフェイスの IP アドレスを選択します。
- リンク属性を指定します。
- (任意) FCIP 書き込みアクセラレーションまたは FCIP 圧縮をイネーブルにします。

FCIP ウィザードを使用して FCIP リンクを作成するには、次の手順に従います。

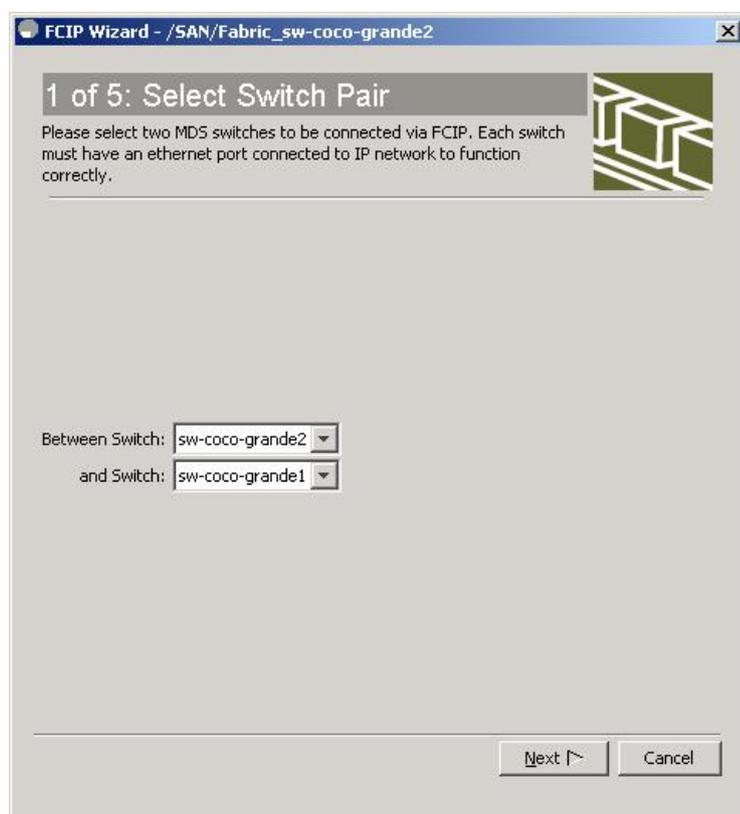
- ステップ 1** Fabric Manager ツールバーで [FCIP Wizard] アイコンをクリックします。図 2-9 を参照してください。

図 2-9 FCIP Wizard



- 図 2-10 に示すスイッチ選択が表示されます。

図 2-10 スイッチ選択



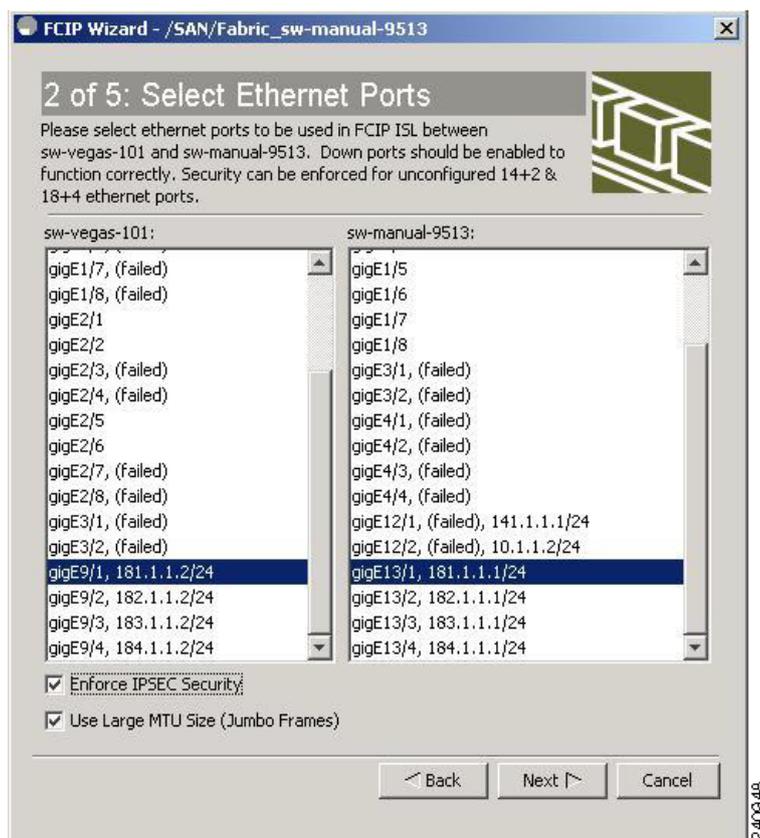
- ステップ 2** FCIP リンクのエンドポイントとして機能するスイッチを選択して、[Next] をクリックします。
- ステップ 3** FCIP リンクを形成する各スイッチのギガビットイーサネットポートを選択します。
- ステップ 4** 両方のギガビットイーサネットポートが MPS-14/2 モジュールの一部である場合、[Enforce IPSEC Security] チェックボックスをオンにして、図 2-11 で示しているように [IKE Auth Key] を設定します。IPsec および IKE の詳細については、『Cisco Fabric Manager Security Configuration Guide』を参照してください。

2300 というジャンボ サイズのフレームを使用するために、[Use Large MTU Size (Jumbo Frames)] オプションを選択します。ファイバ チャネル フレームは 2112 なので、このオプションを使用します。このチェックボックスをオフにすると、FCIP Wizard で MTU サイズが設定されず、デフォルトの 1500 が設定されています。



(注) Cisco MDS 9000 SAN-OS, リリース 3.0(3) では、デフォルトで [Use Large MTU Size (Jumbo Frames)] オプションが選択されていません。

図 2-11 FCIP リンクでの IPsec のイネーブル化



ステップ 5 [Next] をクリックします。[IP Address/Route] 入力画面が表示されます。

ステップ 6 IP ルートを追加する場合、[Add IP Route] を選択します。選択しない場合、デフォルトのままになります。図 2-12 を参照してください。

図 2-12 IP アドレス/ルートの指定

FCIP Wizard - /SAN/Fabric_sw-manual-9513

3 of 5: Specify IP Address/Route

Please supply Ethernet Port IP Address. Specify Route if the Port addresses are in different subnet.
Note: The changes to IP Address and IP Route Addition will be applied on pressing the Next button.

Switch sw-vegas-101 (gigE9/1)

IP Address/Mask: 181.1.1.2/24 e.g. 10.1.1.1/24
Dest/Mask: e.g. 10.1.0.0/16
 Add IP Route: Gateway: e.g. 11.1.1.1
Metric: 0 e.g. 0,32766

Switch sw-manual-9513 (gigE13/1)

IP Address/Mask: 181.1.1.1/24 e.g. 10.1.1.1/24
Dest/Mask: e.g. 10.1.0.0/16
 Add IP Route: Gateway: e.g. 11.1.1.1
Metric: 0 e.g. 0,32766

Back Next Cancel

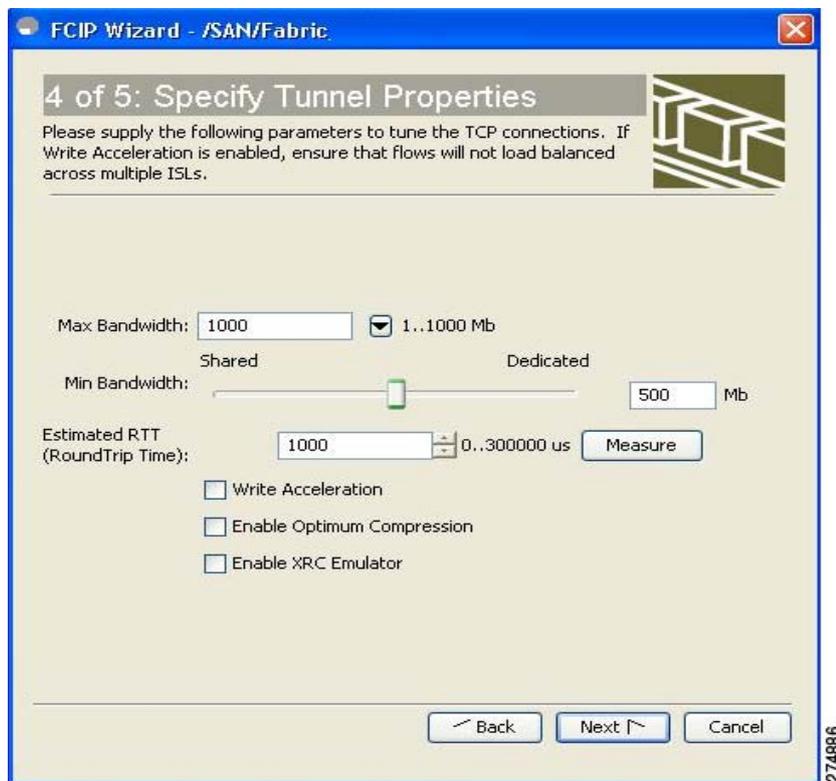
240976

ステップ 7 [Next] をクリックします。TCP 接続特性が表示されます。

ステップ 8 図 2-13 で示すように、この FCIP リンクの TCP 接続に関する最小および最大帯域幅設定とラウンドトリップ時間を設定します。

[Measure] ボタンをクリックすると、ギガビットイーサネットエンドポイント間のラウンドトリップ時間を測定できます。

図 2-13 トンネル プロパティの指定



ステップ 9 [Write Acceleration] チェックボックスをオンにして、この FCIP リンクの FCIP 書き込みアクセラレーションをイネーブルにします。

「FCIP 書き込みアクセラレーション」(P.2-27) を参照してください。

ステップ 10 [Enable Optimum Compression] チェックボックスをオンにして、この FCIP リンクの IP 圧縮をイネーブルにします。

「FCIP 圧縮」(P.2-34) を参照してください。

ステップ 11 [Enable XRC Emulator] チェックボックスをオンにして、この FCIP リンクの XRC エミュレータをイネーブルにします。

XRC エミュレータの詳細については、『Cisco Fabric Manager Fabric Configuration Guide』を参照してください。

ステップ 12 [Next] をクリックします。

ステップ 13 [Port VSAN] を設定して、この FCIP リンクの [Trunk Mode] ラジオ ボタンをクリックします (図 2-14 を参照してください)。



(注) FICON がイネーブルで FICON VSAN が両方のスイッチに存在する場合、図 2-16 が表示され、そうでない場合は 図 2-17 が表示されます。

図 2-14 FCIP ISL の作成

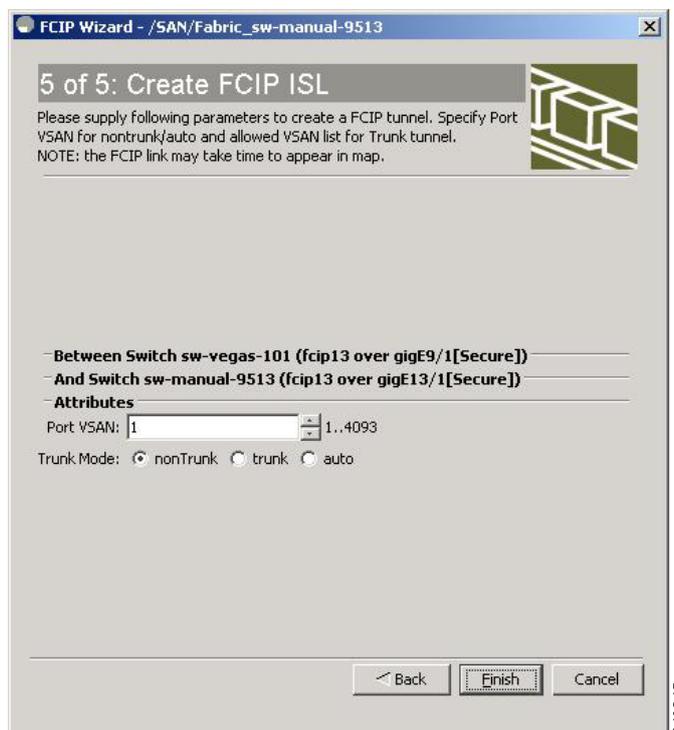


図 2-15 FICON ポートアドレスを入力します。

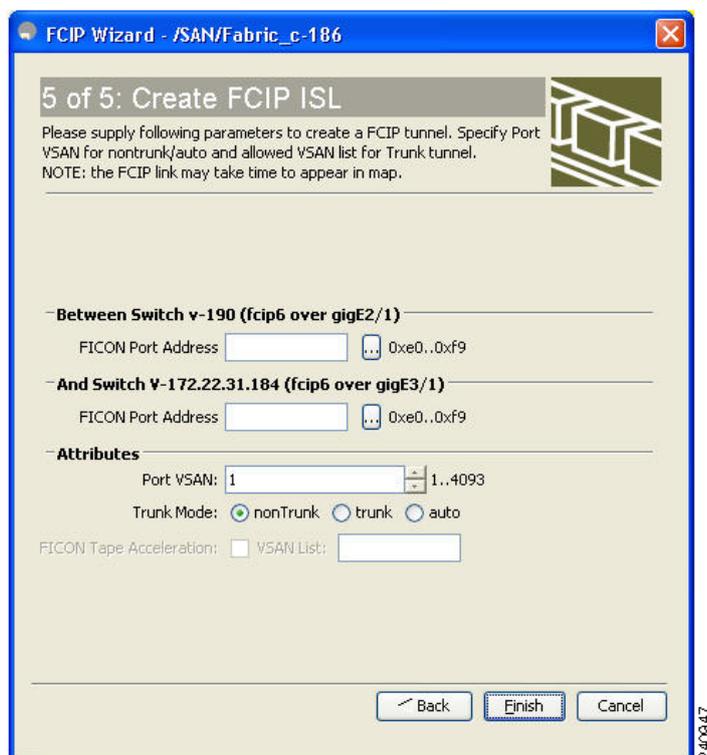


図 2-16 FCIP ISL の作成

FCIP Wizard - /SAN/Fabric_sw-manual-9513

5 of 5: Create FCIP ISL

Please supply following parameters to create a FCIP tunnel. Specify Port VSAN for nontrunk/auto and allowed VSAN list for Trunk tunnel.
NOTE: the FCIP link may take time to appear in map.

Between Switch sw-vegas-101 (fcip13 over gigE9/1[Secure])

And Switch sw-manual-9513 (fcip13 over gigE13/1[Secure])

Attributes

Port VSAN: 1 1..4093

Trunk Mode: nonTrunk trunk auto

Back Finish Cancel

240946

図 2-17 FICON ポートアドレスを入力します。

FCIP Wizard - /SAN/Fabric_c-186

5 of 5: Create FCIP ISL

Please supply following parameters to create a FCIP tunnel. Specify Port VSAN for nontrunk/auto and allowed VSAN list for Trunk tunnel.
NOTE: the FCIP link may take time to appear in map.

Between Switch v-190 (fcip6 over gigE2/1)

FICON Port Address 0xe0..0xf9

And Switch V-172.22.31.184 (fcip6 over gigE3/1)

FICON Port Address 0xe0..0xf9

Attributes

Port VSAN: 1 1..4093

Trunk Mode: nonTrunk trunk auto

FICON Tape Acceleration: VSAN List:

Back Finish Cancel

240947

ステップ 14 [Finish] をクリックして、この FCIP リンクを作成します。

基本 FCIP 設定

FCIP Wizard で FCIP リンクを作成したら、これらのリンクのパラメータを変更する必要がある場合があります。これには、FCIP プロファイルの変更や FCIP リンク パラメータの変更があります。各ギガビットイーサネットインターフェイスは、同時に 3 つのアクティブ FCIP リンクを持つことができます。

FCIP リンクを設定するには、両方のスイッチで次の手順を実行します。

-
- ステップ 1** ギガビットイーサネットインターフェイスを設定します。
 - ステップ 2** FCIP プロファイルを作成し、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、プロファイルをインターフェイスに割り当てます。
 - 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

ギガビットイーサネットインターフェイスのローカル IP アドレスまたは FCIP プロファイルのサブインターフェイスを FCIP プロファイルに割り当てて、FCIP プロファイルを作成する必要があります。インターフェイスには IPv4 または IPv6 アドレスに割り当てられます。図 2-18 に、設定の例を示します。

図 2-18 各ギガビットイーサネットインターフェイスへのプロファイルの割り当て



スイッチ 1 に FCIP プロファイルを作成するには、次の手順を実行します。

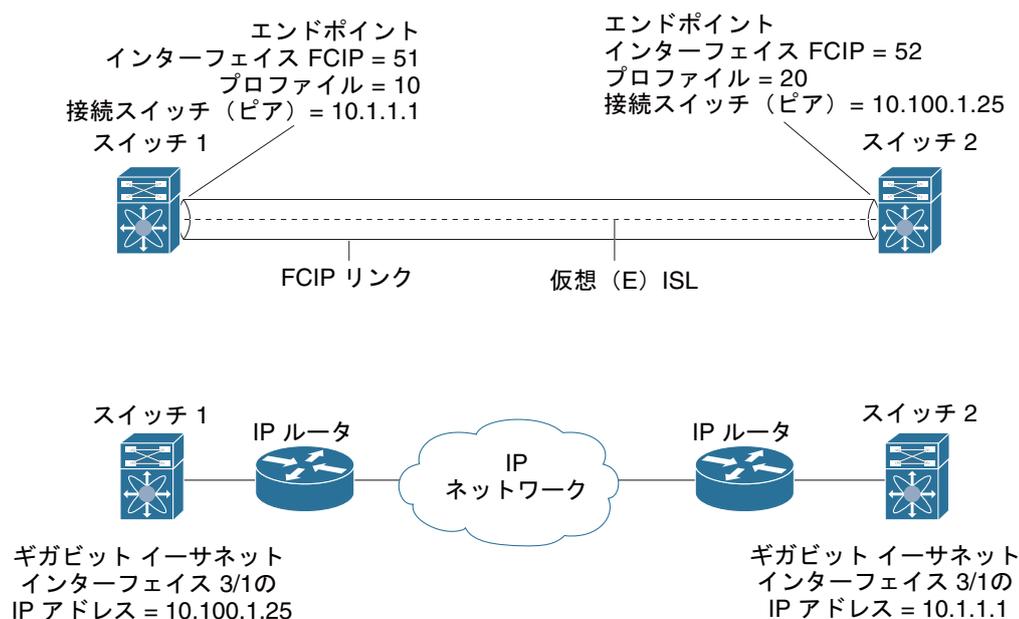
-
- ステップ 1** IPS モジュールが含まれるスイッチへの接続を確認します。
 - ステップ 2** Fabric Manager の [Physical Attributes] ペインで、[Switches] > [ISLs] > [FCIP] を選択します。Device Manager の [IP] メニューで [FCIP] を選択します。
 - ステップ 3** Fabric Manager の [Create Row] アイコンまたは Device Manager の [Create] ボタンをクリックして、新規プロファイルを追加します。
 - ステップ 4** [ProfileId] フィールドに新しいプロファイル ID を入力します。
 - ステップ 5** プロファイルをバインドするインターフェイスの IP アドレスを入力します。

- ステップ 6** 必要に応じて、オプションの TCP パラメータを変更します。これらのフィールドの説明については、Fabric Manager のオンラインヘルプを参照してください。
- ステップ 7** (任意) [Tunnels] タブをクリックして、リンクするエンドポイントの [Remote IPAddress] フィールド内のリモート IP アドレスを変更します。
- ステップ 8** 必要に応じて、オプションパラメータを入力します。FCIP プロファイル情報を表示する場合の詳細については、「FCIP プロファイル」(P.2-4) を参照してください。
- ステップ 9** [Apply Changes] アイコンをクリックして、これらの変更を保存します。

FCIP リンクの作成

FCIP リンク エンドポイントを 2 つ作成すると、2 つの IPS モジュールまたは MPS-14/2 モジュールとの間で FCIP リンクが確立されます。FCIP リンクを作成するには、FCIP インターフェイスにプロファイルを割り当てて、ピア情報を設定します。ピア IP スイッチ情報により、該当するピア スイッチへの FCIP リンクが開始 (作成) されます (図 2-19 を参照)。

図 2-19 各ギガビットイーサネット インターフェイスへのプロファイルの割り当て



91562

インターフェイスおよび拡張リンク プロトコルの確認

Device Manager で FCIP インターフェイスおよび拡張リンク プロトコル (ELP) を確認するには、次の手順を実行します。

-
- ステップ 1** IPS モジュールを含むスイッチに接続していることを確認します。
 - ステップ 2** [Interface] メニューから [FCIP] を選択します。
 - ステップ 3** まだ選択されていない場合、[Interfaces] タブをクリックします。[FCIP Interfaces] ダイアログボックスが表示されます。
 - ステップ 4** まだ選択されていない場合、[ELP] タブをクリックします。[FCIP ELP] ダイアログボックスが表示されます。
-

トランク ステータスのチェック

Device Manager の FCIP インターフェイスのトランク ステータスをチェックするには、次の手順を実行します。

-
- ステップ 1** IPS モジュールを含むスイッチに接続していることを確認します。
 - ステップ 2** [IP] メニュー から [FCIP] を選択します。
 - ステップ 3** まだ選択されていない場合、[Trunk Config] タブをクリックします。[FCIP Trunk Config] ダイアログボックスが表示されます。これには、インターフェイスのステータスが表示されます。
 - ステップ 4** まだ選択されていない場合、[Trunk Failures] タブをクリックします。[FCIP Trunk Failures] ダイアログボックスが表示されます。
-

Cisco Transport Controller の起動

Cisco Transport Controller (CTC) は、ネットワーク エレメントのインストール、プロビジョニング、およびメンテナンスに使用されるタスク志向型ツールです。これは、NE 障害のトラブルシューティングおよび修復にも使用されます。

Fabric Manager を使用して CTC を起動するには、次の手順を実行します。

-
- ステップ 1** ファブリック内の ISL 伝送オプティカル トラフィックを右クリックします。
 - ステップ 2** [Element Manager] をクリックします。
 - ステップ 3** Cisco Transport Controller の URL を入力します。
 - ステップ 4** [OK] をクリックします。
-

FCIP プロファイルの高度な設定

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 プロファイルを設定する場合は、ローカル IP アドレスやローカル ポートだけでなく、その他の TCP パラメータも指定できます。

TCP パラメータの設定

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 が WAN リンク上で送信されると、デフォルトの TCP 設定は適切でない場合があります。この場合、TCP パラメータ（特に、帯域幅、ラウンドトリップ時間、および CWM バースト サイズ）を変更して FCIP WAN リンクを調整することを推奨します。

ここで説明する内容は、次のとおりです。

- 「最小再送信タイムアウト」 (P.2-18)
- 「キープアライブ タイムアウト」 (P.2-18)
- 「最大再送信数」 (P.2-19)
- 「Path MTU」 (P.2-19)
- 「選択的 確認応答」 (P.2-19)
- 「ウィンドウ 管理」 (P.2-19)
- 「輻輳の監視」 (P.2-19)
- 「最大ジッタの予測」 (P.2-20)
- 「バッファ サイズ」 (P.2-20)

最小再送信タイムアウト

再送信するまでに TCP が待機する最小期間を制御できます。デフォルトでは、この値は 200 ミリ秒 (ms) です。

キープアライブ タイムアウト

TCP 接続で、FCIP リンクが機能しているかどうかを確認するインターバルを設定できます。これにより、トラフィックが発生していない場合でも、FCIP リンク障害がすばやく検出されます。

TCP 接続のアイドル期間が指定期間を超えると、キープアライブ タイムアウト パケットが送信されて、接続がアクティブかどうかを確認します。キープアライブ タイムアウト機能を使用すると、FCIP リンク障害を検出する期間を調整できます。

最初の接続アイドル インターバルを設定できます（デフォルトは 60 秒です）。設定したインターバルの間、接続がアイドルである場合、1 秒間隔で 8 個のキープアライブ プロブが送信されます。これらの 8 個のプロブに対する応答が受信されないで、接続がアイドルのままである場合、FCIP リンクは自動的に終了します。



(注) (接続がアイドル中の) 最初の接続アイドル インターバルだけ変更できます。

最大再送信数

TCP が接続を終了する前にパケットを再送信する最大回数を指定できます。

Path MTU

Path MTU (PMTU) は、FCIP リンクの 2 つのエンドポイント間の IP ネットワークに関する最小 MTU です。PMTU 検出は、TCP が PMTU を動的に学習し、それに応じて最大 TCP セグメントを調整する場合に使用するメカニズムです (RFC 1191)。

デフォルトで、PMTU 検出はすべてのスイッチでイネーブルです。タイムアウトは 3600 秒です。PMTU が変更されて TCP の最大セグメント サイズが小さくなった場合は、TCP が元の MTU を試行してから経過時間を `reset-timeout` で指定します。

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ことがあります。蓄積された確認応答の中で使用できる情報は限られるため、TCP 送信側は 1 回のラウンドトリップにつき、失われたパケットを 1 つしか学習できません。Selective Acknowledgment (SACK; 選択的確認応答) メカニズムを使用すると、TCP 送信中に複数のパケットが失われた場合の制限を解消できます。

受信 TCP が送信側に SACK アドバタイズメントを送信します。送信側は消失したデータ セグメントだけ再送信できます。Cisco MDS 9000 ファミリー スイッチでは、SACK がデフォルトでイネーブルです。

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 Round-trip Time (RTT; ラウンドトリップ時間) 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) TCP 接続のウィンドウ倍率は、設定された `round-trip-time` パラメータによって決まります。このパラメータは近似値にすぎません。ウィンドウを管理するための `round-trip-time` パラメータは、測定された RTT 値によって上書きされます。設定された `round-trip-time` が測定された RTT と比べて小さすぎると、ウィンドウ倍率が極端に小さくなるため、リンクを完全利用できないことがあります。

`min-available-bandwidth` パラメータおよび測定された RTT の組み合わせによって、下回った場合に、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 が積極的に維持することになるしきい値が決まります。

`max-bandwidth-mbps` パラメータと測定された 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 トンネル、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。

輻輳の監視

Congestion window monitoring (CWM; 輻輳ウィンドウ監視) パラメータをイネーブルにすると、アイドル期間の経過ごとに TCP で輻輳を監視できます。アイドル期間後に許可される最大バースト サイズも、CWM パラメータによって決まります。デフォルトで、このパラメータはイネーブルになっており、デフォルトバースト サイズは 50 KB です。

帯域幅パラメータと CWM の相互作用および最終的な TCP 動作の概要を、次に示します。

- 直前の 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 を乗じた値よりも小さい場合、TCP がドロップされていなければ、バースト全体が **min-available-bandwidth** レートで即座に送信されます。
- 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に、設定された CWM 値よりも小さなバーストサイズでファイバチャネルトラフィックが送信されると、FCIP はバースト全体を **max-bandwidth** レートで即座に送信します。
- 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 値よりも大きい場合、バーストの一部だけが即座に送信されます。残りは次の RTT で送信されます。

ソフトウェアは標準 TCP 規則を使用して、**min-available-bandwidth** を維持するために必要な値から **max-bandwidth** までウィンドウサイズを増加させます。



(注)

デフォルトのバーストサイズは 50 KB です。



ヒント

最適なパフォーマンスを実現するには、この機能をイネーブルのままにしてください。CWM バーストサイズを大きくすると、IP ネットワークでドロップされるパケット数が増え、TCP パフォーマンスが低下することがあります。IP ネットワークに十分なバッファがある場合だけ、CWM バーストサイズをデフォルトよりも大きくして、送信遅延を低下させてください。

最大ジッタの予測

ジッタは受信パケットの遅延における変動として定義されています。送信側で、パケットはパケット間隔が均一な連続ストリームとして送信されます。ネットワーク輻輳、不適切なキューイング、または設定ミスにより、この等間隔で連続的なパケットの送信に波が生じたり、遅延時間が一定ではなくパケットによって異なったりする場合があります。

パケット送信側で、最大推定ジッタ（マイクロ秒）を設定できます。推定変動には、ネットワークのキューイング遅延を含める必要はありません。Cisco MDS スイッチに IPS モジュールまたは MPS-14/2 モジュールが搭載されている場合、このパラメータはデフォルトでイネーブルです。

FCIP インターフェイスの場合、デフォルト値は 1000 マイクロ秒です。

バッファ サイズ

必要な追加バッファリングを定義し、FCIP インターフェイスに対するスイッチの出力パスをフロー制御するまでに、TCP で許容される標準送信ウィンドウサイズより大きくすることができます。デフォルトの FCIP バッファサイズは 0 KB です。



(注)

FCIP トラフィックが高速 WAN リンクで送信される場合は、デフォルト値を使用します。ファイバチャネルリンクと WAN リンクの速度にミスマッチがある場合、DMA ブリッジでタイムスタンプエラーが発生します。この場合、タイムスタンプエラーを回避するには、バッファサイズを大きくします。

FCIP インターフェイスの詳細設定

ここでは、ピアとの接続を確立するため、FCIP インターフェイスに設定できるオプションについて説明します。次のようなトピックが含まれています。

- 「ピアの設定」 (P.2-21)
- 「ピア IP アドレスの割り当て」 (P.2-21)
- 「アクティブ接続の設定」 (P.2-22)
- 「タイムスタンプ制御の有効化」 (P.2-22)
- 「FCIP B ポート 相互運用性モード」 (P.2-23)
- 「Quality of Service」 (P.2-26)

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する必要があります。

ピアの設定

ピアとの FCIP リンクを確立するには、ピア IP アドレス オプションを使用できます。このオプションは、FCIP リンクの両端を設定します。オプションで、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。

ピア IP アドレスの割り当て

FCIP の基本設定では、ピア IP アドレスを使用してピア情報を設定します。ピアのポート番号を指定して、ピア情報を設定することもできます。ポートを指定しない場合、デフォルトの 3225 ポート番号を使用して接続を確立します。IPv4 アドレスまたは IPv6 アドレスを指定できます。

Fabric Manager を使用して IPv4 アドレスとポート番号に基づいてピア情報を割り当てるには、次の手順を実行します。

-
- ステップ 1** [Physical Attributes] ペインで [ISLs] を展開して、[FCIP] を選択します。
FCIP プロファイルとリンクが [Information] ペインに表示されます。
Device Manager で、[IP] > [FCIP] を選択します。
[FCIP] ダイアログボックスが表示されます。
 - ステップ 2** [Tunnels] タブをクリックします。FCIP リンク情報が表示されます。
 - ステップ 3** Fabric Manager の [Create Row] アイコンまたは Device Manager の [Create] ボタンをクリックします。
[FCIP Tunnels] ダイアログボックスが表示されます。
 - ステップ 4** [ProfileID] および [TunnelID] フィールドを設定します。
 - ステップ 5** 設定しているピア IP アドレスの [RemoteIPAddress] および [RemoteTCPPort] フィールドを設定します。
 - ステップ 6** このリンクの終端で TCP 接続を開始しない場合、[PassiveMode] チェックボックスをオンにします。
 - ステップ 7** (任意) [NumTCPCon] フィールドを、この FCIP リンクからの TCP 接続数に設定します。
 - ステップ 8** (任意) [Time Stamp] セクションの [Enable] チェックボックスをオンにして、[Tolerance] フィールドを設定します。

- ステップ 9** (任意) このダイアログボックス内の他のフィールドを設定して、[Create] をクリックして、この FCIP リンクを作成します。

Fabric Manager を使用して IPv6 アドレスに基づくピア情報とポート番号を割り当てるには、次の手順を実行します。

- ステップ 1** Fabric Manager の [Physical Attributes] ペインで、[ISLs] > [FCIP] を選択します。
FCIP プロファイルとリンクが [Information] ペインに表示されます。
Device Manager で、[IP] > [FCIP] を選択します。[FCIP] ダイアログボックスが表示されます。
- ステップ 2** [Tunnels] タブをクリックします。FCIP リンク情報が表示されます。
- ステップ 3** Fabric Manager の [Create Row] アイコンまたは Device Manager の [Create] ボタンをクリックします。
[FCIP Tunnels] ダイアログボックスが表示されます。
- ステップ 4** [ProfileID] および [TunnelID] フィールドを設定します。
- ステップ 5** 設定しているピア IP アドレスの [RemoteIPAddress] および [RemoteTCPPort] フィールドを設定します。
- ステップ 6** このリンクの終端で TCP 接続を開始しない場合、[PassiveMode] チェックボックスをオンにします。
- ステップ 7** (任意) [NumTCPCon] フィールドを、この FCIP リンクからの TCP 接続数に設定します。
- ステップ 8** (任意) [Time Stamp] セクションの [Enable] チェックボックスをオンにして、[Tolerance] フィールドを設定します。
- ステップ 9** (任意) このダイアログボックス内の他のフィールドを設定して、[Create] をクリックして、この FCIP リンクを作成します。
-

アクティブ接続の設定

TCP 接続を開始するために必要なモードを設定できます。IP 接続を能動的に試行するアクティブモードは、デフォルトでイネーブルです。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ていないことを確認します。両端がパッシブに設定されている場合、接続は開始されません。
-

タイムスタンプ制御の有効化

指定時間外のパケットを廃棄するようにスイッチを設定できます。この機能をイネーブルにすると、パケットを受け入れる時間を指定できます。このオプションで指定された期間内に着信したパケットは受け入れられます。それ以外のパケットはドロップされます。

デフォルトで、タイムスタンプ制御は、すべての Cisco MDS 9000 ファミリースイッチでディセーブルになっています。パケットがネットワーク時間を基準として 2000 ミリ秒のインターバル (+ または -2000 ミリ秒) 内に着信した場合、パケットは受け入れられます。



(注) パケットを受け入れるデフォルト値は 2000 マイクロ秒です。time-stamp オプションがイネーブルの場合は、両方のスイッチに NTP が設定されていることを確認してください（詳細については、『Cisco NX-OS Fundamentals Configuration Guide』を参照してください）。

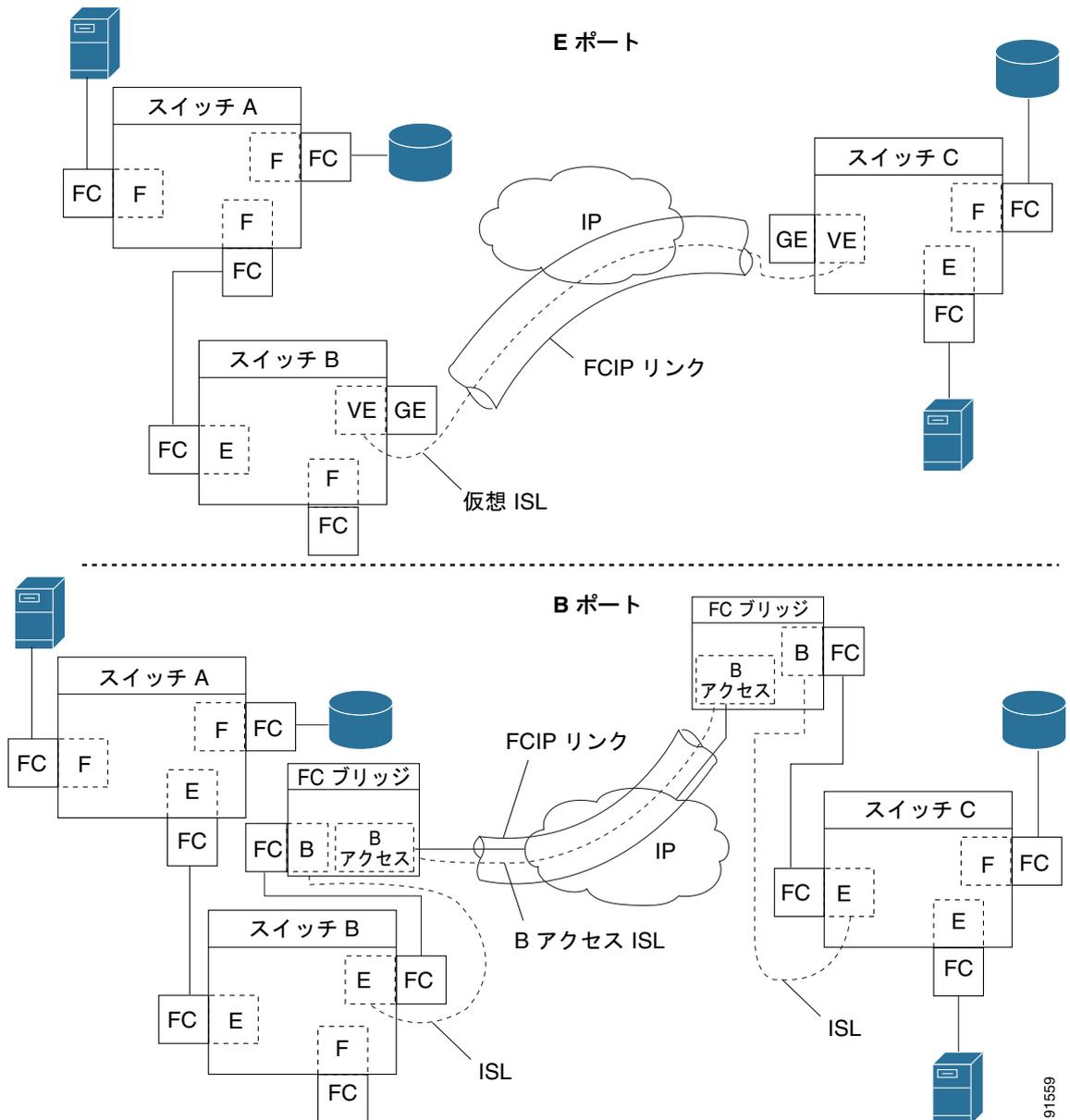


ヒント テープアクセラレーションまたは書き込みアクセラレーションが設定されている FCIP インターフェイスでは、タイムスタンプ制御をイネーブルにしないでください。

FCIP B ポート 相互運用性モード

通常、E ポートはファイバチャネルスイッチと相互接続します。一方、シスコ製 PA-FC-1G ファイバチャネルポートアダプタや SN 5428-2 ストレージルータなど、一部の SAN エクステンダデバイスは、地理的に分散されたファブリックを接続するためのブリッジポートモデルを実装しています。このモデルでは、T11 標準 FC-BB-2 で規定された B ポートを使用します。図 2-20 に、IP ネットワークを介して SAN を拡張する一般的な例を示します。

図 2-20 FCIP B ポートおよびファイバチャネル E ポート

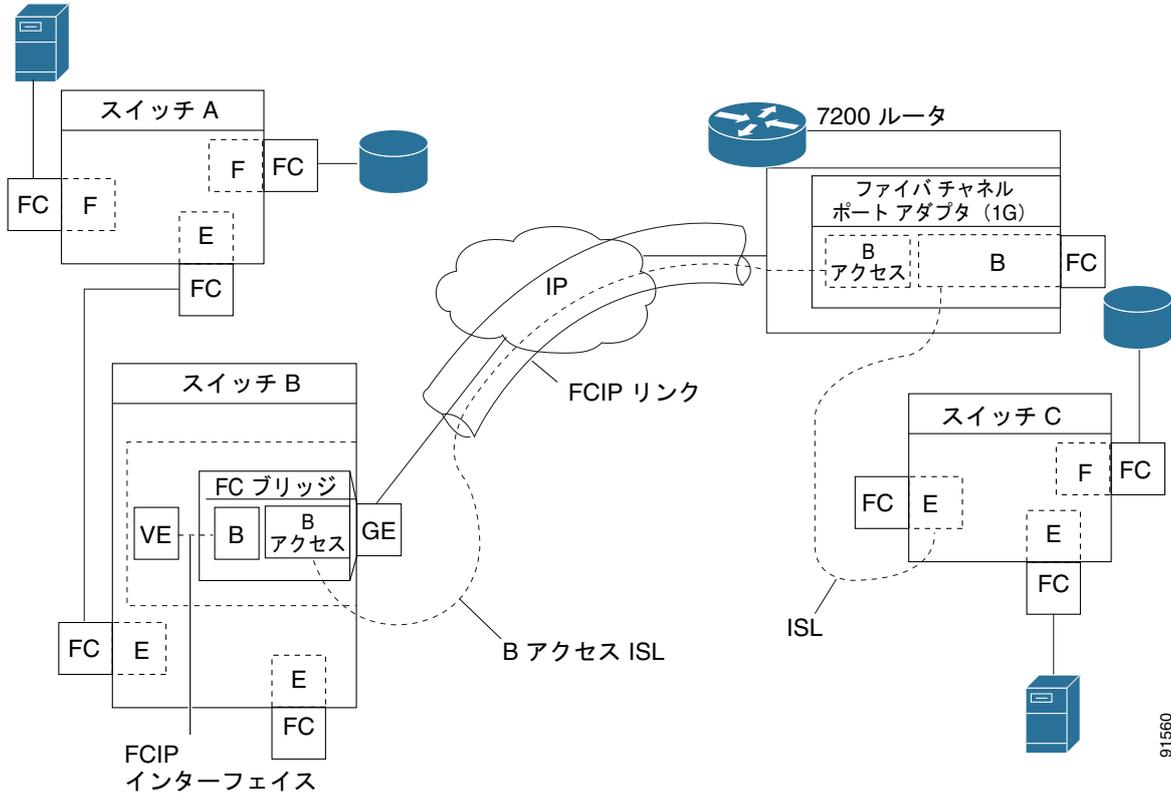


B ポートは、ローカル E ポートからリモート E ポートにファイバチャネルトラフィックをブリッジします。主要スイッチの選定、ドメイン ID の割り当て、ファイバチャネル Fabric Shortest Path First (FSPF) ルーティングなど、ファブリック関連アクティビティには関与しません。たとえば、SAN エクステンダデバイスに入るクラス F トラフィックは、B ポートと相互作用しません。このトラフィックは WAN インターフェイスを介して透過的に伝播（ブリッジ）され、その後、リモート B ポートから送信されます。このブリッジにより、両方の E ポートでクラス F 情報が交換され、最終的に、ファブリック統合やルーティングなどの通常の ISL 動作が実行されます。

B ポート SAN 拡張機能間の FCIP リンクでは、E ポート間の FCIP リンクと同じ情報が交換されないため、互換性がありません。このことは、FC-BB-2 で次のように表現されています。「VE ポートでは FCIP リンクを使用して仮想 ISL を確立しますが、B ポートでは B アクセス ISL を使用します。」

IPS モジュールおよび MPS-14/2 モジュールは、ギガビット イーサネット インターフェイスに B アクセス ISL プロトコルを実装して、B ポート SAN エクステンダ デバイスから接続されている FCIP リンクをサポートします。対応する仮想 B ポートと仮想 E ポートは内部的に接続されているため、エンドツーエンドの E ポート接続要件が満たされています (図 2-21 を参照)。

図 2-21 B ポートモードでの FCIP リンク終端



IPS モジュールや MPS-14/2 モジュールの B ポート機能を使用すると、リモート B ポート SAN エクステンダ デバイスが Cisco MDS 9000 ファミリー スイッチと直接通信できるため、ローカルブリッジ デバイスが不要になります。

B ポートの設定

FCIP ピアがファイバチャネル B ポートだけをサポートする SAN エクステンダ デバイスの場合、FCIP リンクに対して B ポートモードをイネーブルにする必要があります。B ポートがイネーブルにされている場合、E ポート機能もイネーブルにされ、共存します。B ポートをディセーブルにしても、E ポート機能はイネーブルのままです。

B ポートモードをイネーブルにするには、Fabric Manager を使用して、次の手順を実行します。

- ステップ 1** [Physical Attributes] ペインから [ISLs] > [FCIP] を選択します。
FCIP プロファイルとリンクが [Information] ペインに表示されます。
Device Manager で、[IP] > [FCIP] を選択します。[FCIP] ダイアログボックスが表示されます。
- ステップ 2** [Tunnels] タブをクリックします。
FCIP リンク情報が表示されます。

- ステップ 3** Fabric Manager の [Create Row] アイコンまたは Device Manager の [Create] ボタンをクリックします。
[FCIP Tunnels] ダイアログボックスが表示されます。
- ステップ 4** [ProfileID] および [TunnelID] フィールドを設定します。
- ステップ 5** 設定しているピア IP アドレスの [RemoteIPAddress] および [RemoteTCPPort] フィールドを設定します。
- ステップ 6** このリンクの終端で TCP 接続を開始しない場合、[PassiveMode] チェックボックスをオンにします。
- ステップ 7** (任意) [NumTCPCon] フィールドを、この FCIP リンクからの TCP 接続数に設定します。
- ステップ 8** ダイアログボックスの [B Port] セクションの [Enable] チェックボックスをオンにして、オプションで、FCIP ピアから受信した ELS エコー フレームに送信される応答が必要な場合は [KeepAlive] チェックボックスをオンにします。
- ステップ 9** (任意) このダイアログボックス内の他のフィールドを設定して、[Create] をクリックして、この FCIP リンクを作成します。

Quality of Service

Quality of Service (QoS) パラメータは、すべての IP パケット (IP ヘッダー内の Type Of Service [Tos; タイプ オブ サービス] フィールド) にマークする Differentiated Services Code Point [DSCP; 差別化サービス コード ポイント] 値を指定します。

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

FCIP リンクに 1 つの TCP 接続だけが存在する場合、データ DSCP 値はこの接続内のすべてのパケットに適用されます。

E ポートの設定

FCIP インターフェイスと同じ方法で E ポートを設定できます。FCIP インターフェイスでは、次の機能も使用できます。

- 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。
『*Cisco Fabric Manager Fabric Configuration Guide*』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
『*Cisco Fabric Manager Interfaces Configuration Guide*』を参照してください。
- PortChannel
『*Cisco Fabric Manager Security Configuration Guide*』を参照してください。
 - 複数の FCIP リンクを 1 つのファイバチャネル PortChannel にバンドルできます。
 - FCIP リンクおよびファイバチャネル リンクを 1 つの PortChannel に結合できません。
- FSPF
『*Cisco Fabric Manager Fabric Configuration Guide*』を参照してください。
- ファイバチャネル ドメイン (fcdomains)
『*Cisco Fabric Manager System Management Configuration Guide*』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
『Cisco Fabric Manager System Management Configuration Guide』を参照してください。

FCIP の拡張機能

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」(P.2-27)
- 「FCIP 書き込みアクセラレーションの設定」(P.2-29)
- 「FCIP テープ アクセラレーション」(P.2-29)
- 「FCIP テープ アクセラレーションの設定」(P.2-34)
- 「FCIP 圧縮」(P.2-34)

FCIP 書き込みアクセラレーション

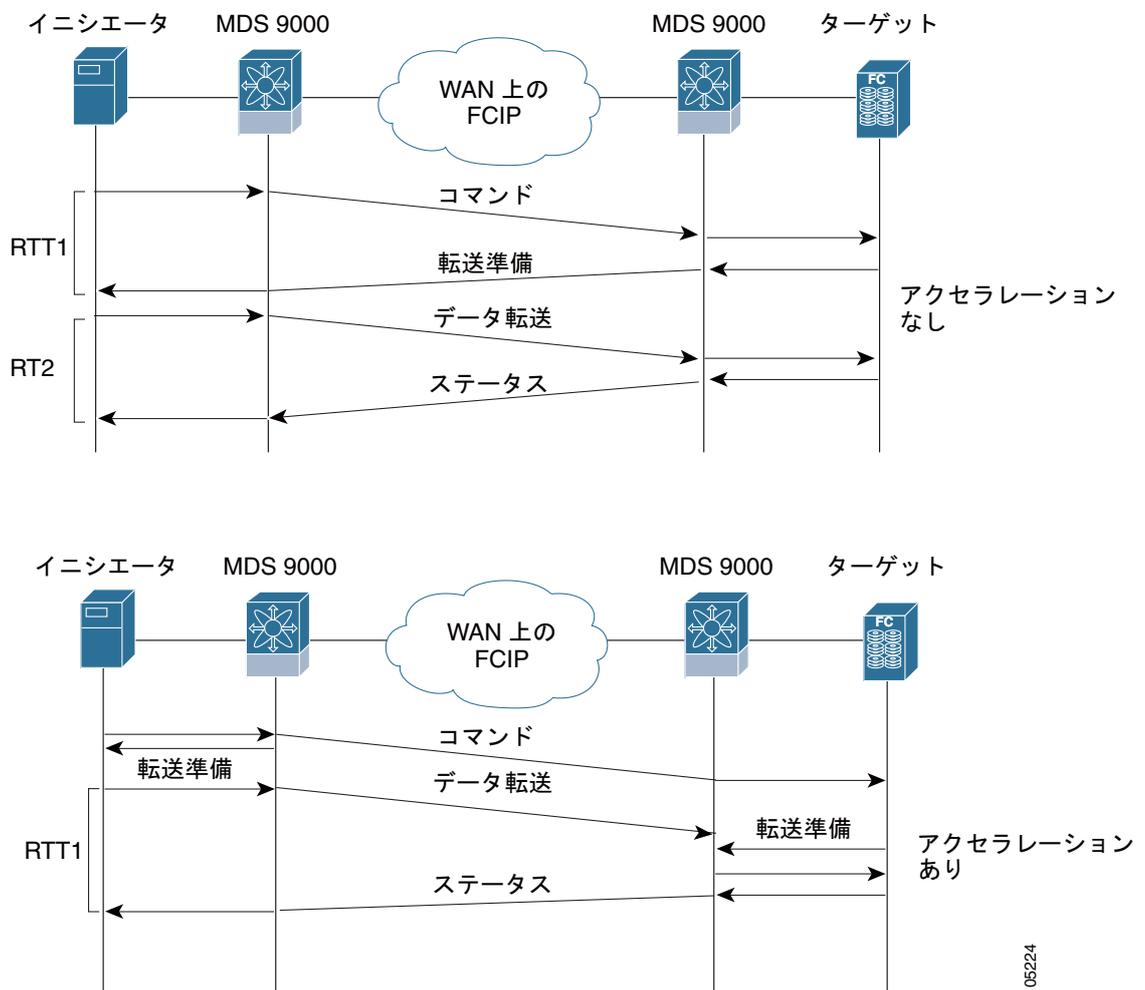
FCIP 書き込みアクセラレーション機能を使用すると、FCIP を使用してストレージ トラフィックを WAN 経由でルーティングするときに、アプリケーションの書き込み性能を大幅に改善できます。FCIP 書き込みアクセラレーションがイネーブルの場合、書き込み動作の WAN 遅延の影響が最小化されて、WAN スループットが最大化されます。



(注) デフォルトでは、書き込みアクセラレーション機能はディセーブルで、FCIP リンクの両端でイネーブルにする必要があります。書き込みアクセラレーション機能が FCIP トンネルの片側だけでイネーブルになっている場合、動作上は無効になります。

図 2-22 では、書き込みアクセラレーションを使用しないで WRITE コマンドを実行する場合は、Round-Trip Transfer (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 WRITE コマンドを実行する場合に必要な RTT は 1 つだけです。最大サイズの転送準備が FCIP リンクのホスト側からホストに戻された後に、WRITE 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 コマンドおよび転送準備を長時間待機しなくても、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転送準備が必要ですが、これによる遅延もなくなります。

図 2-22 FCIP リンク書き込みアクセラレーション



ヒント

チャンネルモードがアクティブに設定されているダイナミック PortChannel に属するトンネルの場合、複数の FCIP トンネル用に FCIP 書き込みアクセラレーションをイネーブルにできます。イニシエータとターゲットポート間にウェイトが等しい複数の非 PortChannel ISL が存在する場合、FCIP 書き込み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、読み書き操作が失敗したりすることがあります。

ヒント

書き込みアクセラレーションが設定されている FCIP インターフェイスでは、タイムスタンプ制御をイネーブルにしないでください。

(注)

FCIP 展開における複数の 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できません。ネイティブのファイバチャネル書き込みアクセラレーションは、PortChannel で使用できます。また、FCIP 書き込みアクセラレーションは、チャンネルモードがアクティブに設定されている、または Port Channel Protocol (PCP) で構成された PortChannel で使用できます。



注意

Cisco MDS SAN-OS リリース 2.0(1b) 以降および NX-OS リリース 4.x では、PortChannel に属する FCIP ポートに対応した FCIP 書き込みアクセラレーションとそれ以前の FCIP 書き込みアクセラレーションは、互換性がありません。

FCIP 書き込みアクセラレーションの設定

FCIP Wizard を使用して、FCIP リンクの作成時に FCIP 書き込みアクセラレーションをイネーブルにすることができます。

既存 FCIP リンクで書き込みアクセラレーションをイネーブルにするには、次の手順を実行します。

- ステップ 1** Fabric Manager の [Physical Attributes] ペインで [ISLs] > [FCIP] を選択します。
FCIP プロファイルとリンクが [Information] ペインに表示されます。
Device Manager で、[IP] > [FCIP] を選択します。
[FCIP] ダイアログボックスが表示されます。
- ステップ 2** [Tunnels (Advanced)] タブをクリックします。
FCIP リンク情報が表示されます (図 2-23 を参照)。

図 2-23 [FCIP Tunnels (Advanced)] タブ

Switch	ProfileID	Interface	Timestamp Enable	Timestamp Tolerance	NumConn	Passive	QoS Control	QoS Data	IP Compression	Write Accelerator	Write Accelerator Oper
sw172-22-46-174 3		fcip3	<input type="checkbox"/>	2000	2	<input type="checkbox"/>	0	0	none	<input checked="" type="checkbox"/>	False
sw172-22-46-174 4		fcip4	<input type="checkbox"/>	2000	2	<input type="checkbox"/>	0	0	none	<input type="checkbox"/>	False
sw172-22-46-174 7		fcip7	<input type="checkbox"/>	2000	2	<input type="checkbox"/>	0	0	high-comp-ratio(1.3)	<input type="checkbox"/>	False
sw172-22-46-174 8		fcip8	<input type="checkbox"/>	2000	2	<input type="checkbox"/>	0	0	high-throughput(1.3)	<input type="checkbox"/>	False

- ステップ 3** [Write Accelerator] チェックボックスをオンまたはオフにします。
- ステップ 4** [IP Compression] ドロップダウン リストから適切な圧縮比を選択します。
- ステップ 5** [Apply Changes] アイコンをクリックして、これらの変更を保存します。

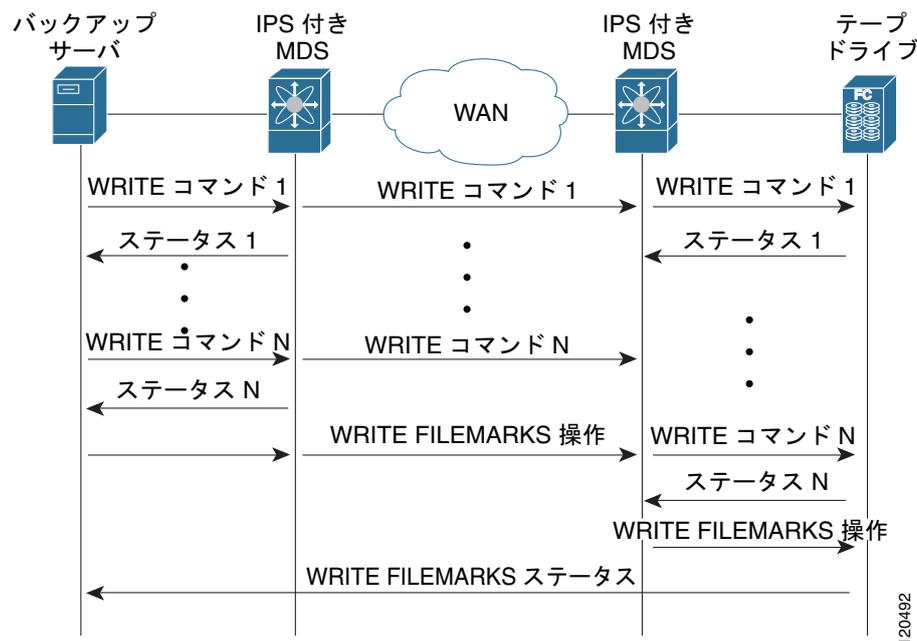
FCIP テープ アクセラレーション

テープは、ユーザ 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、テープ読み書きアクセラレーションを提供します。

通常、テープ ドライブにアクセスするアプリケーションは、SCSI WRITE または READ 操作を 1 回だけ実行します。FCIP トンネルを長距離 WAN リンクで使用する場合、コマンド処理が 1 回しかないため、テープ アクセラレーション機能の利点が制約されます。SCSI WRITE または READ 操作はホストがテープ ドライブから正常応答を受信するまで完了しないため、バックアップ、アーカイブ、および復元性能に影響を与えます。FCIP テープ アクセラレーション機能は、この問題を解決するのに役立ちます。FCIP テープ アクセラレーションを使用すると、ホストからテープへの WAN リンク経由でのデータ伝送を高速化できるため、テープバックアップ、アーカイブ、および復元操作が改善されます。

図 2-24 のテープ書き込み操作アクセラレーションの例で、バックアップサーバはテープライブラリ内のドライブに書き込み操作を発行します。ローカルの 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 (転送可) を代行し、ホストにデータ送信の開始を伝えます。ローカル Cisco MDS スイッチは、すべてのデータが受信されると、SCSI WRITE 操作の正常終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 操作を開始できます。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 トンネル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 2-24 FCIP リンクでのテープ書き込みアクセラレーション



FCIP トンネルのテープ側では、別の Cisco MDS スイッチが受信したコマンドとデータをバッファリングします。この Cisco MDS スイッチは、テープドライブに対するバックアップサーバとして機能し、データを転送する前にテープドライブからの transfer ready を待ち受けます。



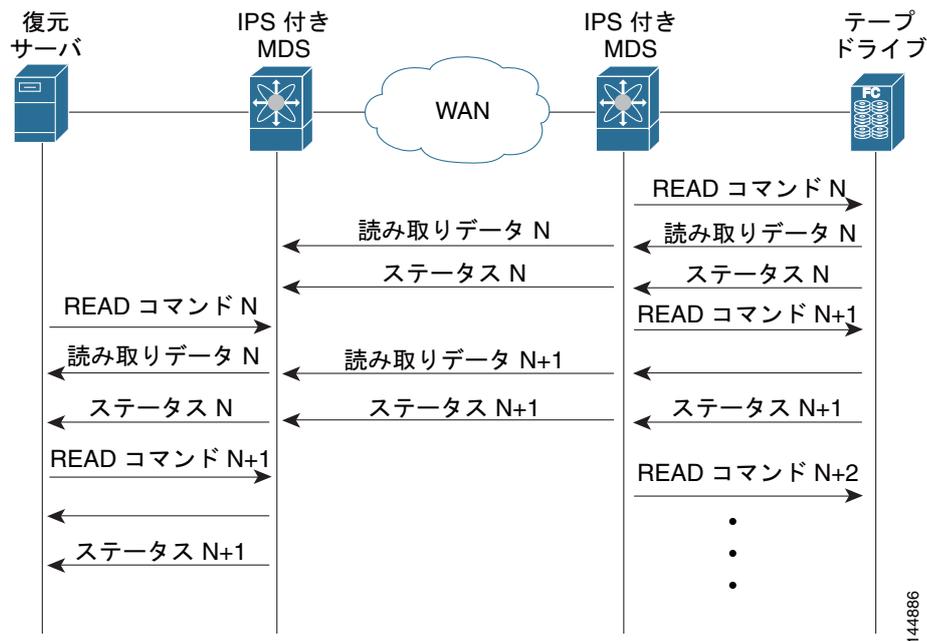
(注)

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、短時間でのリンクアップ/ダウンイベント (FCIP リンク、サーバ/テープポートリンク) などが発生した場合、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 経由で TCP/IP を使用してリモートテープドライブに対する信頼性の高いデータ配送を実現します。Cisco NX-OS は、プロキシ機能を使用せずに WRITE FILEMARKS 操作をエンドツーエンドで実行することにより、書き込みデータの完全性を維持しています。WRITE FILEMARKS 操作は、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を処理するバックアップサーバに返されると、テープビジーエラーが Cisco NX-OS ソフトウェアによって自動的に再試行されます。

読み取り操作のテープ読み取り操作アクセラレーションの例で、図 2-25 の復元サーバは、テープ ライブラリ内のドライブに読み取り操作を発行します。復元プロセス中、テープ側にあるリモート Cisco MDS スイッチは、ホストからさらに SCSI READ 操作が実行されることを予期して、独自にテープ ドライブに SCSI READ 操作を発行します。事前に取得された読み取りデータは、ローカル Cisco MDS スイッチにキャッシュされます。ローカル Cisco MDS スイッチは、ホストから SCSI READ 操作を受信すると、キャッシュされたデータを送出します。この方式により、テープ読み取りアクセラレーションがない場合に比べて、同じ時間に FCIP トンネルでより多くのデータが送信されます。そのため、WAN リンクでのテープ読み取り性能が改善されます。

図 2-25 FCIP リンクでのテープ読み取りアクセラレーション



Cisco NX-OS は、WAN 経由で TCP/IP を使用して復元アプリケーションに対する信頼性の高いデータ配送を実現します。読み取り操作中のテープ メディア エラーがエラー処理のために復元サーバへ返されると、Cisco NX-OS ソフトウェアは他のエラーから復旧します。



(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。テープ アクセラレーション機能が FCIP トンネルの片側だけでイネーブルになっている場合、動作上は無効になります。



ヒント

FCIP ポートが PortChannel に属する場合、またはイニシエータとターゲット ポート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、読み書き操作が中断されたりすることがあります。



注意

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は、このインターフェイスで 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 トンネルでテープ アクセラレーション機能をイネーブルにすると、トンネルが再度初期化され、読み書きアクセラレーション機能も自動的にイネーブルになります。

書き込みのテープ アクセラレーションで、リモートの 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、Transfer Ready の代行によってではなく、ローカルの Cisco MDS スイッチによって、ホストからの書き込み操作がフロー制御されます。書き込み操作が完了し、一部のデータバッファが解放されると、ローカルの Cisco MDS スイッチは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。読み取り操作の完了時に、一部のデータバッファが解放されると、リモートの Cisco MDS スイッチは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** オプションが使用されます。このオプションは WAN の遅延とテープ速度を考慮して、最適なパフォーマンスを実現します。また、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）。



ヒント フロー制御バッファリングでは、デフォルト オプションを使用することを推奨します。



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



(注) FCIP トンネルの片側が Cisco MDS SAN OS リリース 3.0(1) 以降および NX-OS リリース 4.x を実行し、もう一方の側が Cisco MDS SAN OS リリース 2.x を実行している場合、テープ アクセラレーションをイネーブルにすると、FCIP トンネルはテープ書き込みアクセラレーションだけを実行しますが、テープ読み取りアクセラレーションは実行しません。



(注) Cisco MDS NX-OS リリース 4.2(1) では、FCIP テープ アクセラレーション機能は、MDS スイッチ間の FCIP バックツーバック接続でサポートされていません。

FCIP テープ アクセラレーション用のテープ ライブラリ LUN マッピング

テープ ライブラリが LU（論理ユニット）マッピングを提供し、FCIP テープ アクセラレーションをイネーブルにする場合は、対象ポートからアクセスできる各物理テープ ドライブに一意の LU 番号（LUN）を割り当てる必要があります。

図 2-26 に、1 つの対象ポートを通じてスイッチ 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 マッピングを提供している場合は、4 台のテープ ドライブのすべてに一意の LUN を割り当てる必要があります。

図 2-26 FCIP LUN マッピングの例

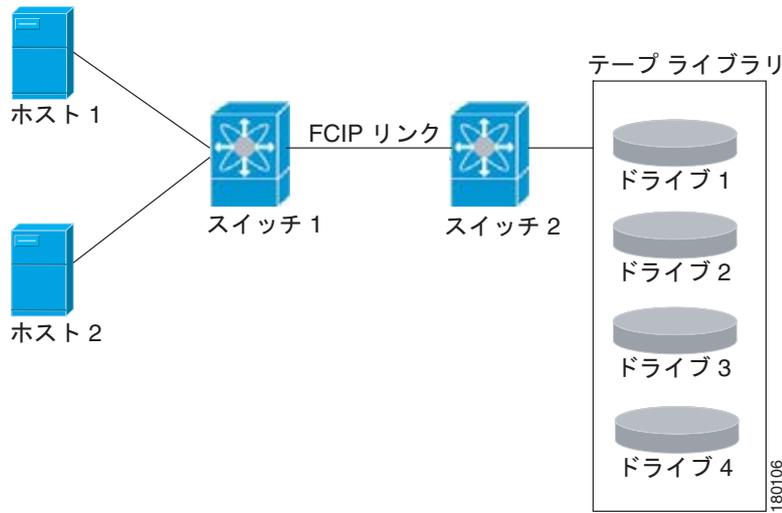


表 2-1 と表 2-2 に説明するマッピングでは、ホスト 1 はドライブ 1 とドライブ 2 にアクセスでき、ホスト 2 はドライブ 3 とドライブ 4 にアクセスできます。

表 2-1 で、正しいテープ ライブラリ LUN マッピングを説明します。

表 2-1 ホスト アクセスが 1 つの場合の正しい 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

表 2-2 に、誤ったテープ ライブラリ LUN マッピングを説明します。

表 2-2 ホスト アクセスが 1 つの場合の誤った 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

別の設定例では、テープ ドライブが 1 つのテープ ポートを通じて複数のホストに共有されます。たとえば、ホスト 1 はドライブ 1 とドライブ 2 にアクセスでき、ホスト 2 はドライブ 2、ドライブ 3、およびドライブ 4 にアクセスできます。表 2-3 に、このような設定での正しい LUN マッピングを示します。

表 2-3 複数のホスト アクセスがある場合の正しい 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設定

Fabric Manager を使用して FCIP テープ アクセラレーションをイネーブルにするには、次の手順を実行します。

- ステップ 1** Fabric Manager の [Physical Attributes] ペインで、[ISLs] > [FCIP] を選択します。
FCIP プロファイルとリンクが [Information] ペインに表示されます。
Device Manager で、[IP] > [FCIP] を選択します。
[FCIP] ダイアログボックスが表示されます。
- ステップ 2** [Tunnels] タブをクリックします。FCIP リンク情報が表示されます。
- ステップ 3** Fabric Manager の [Create Row] アイコンまたは Device Manager の [Create] ボタンをクリックします。
[FCIP Tunnels] ダイアログボックスが表示されます。
- ステップ 4** [Profile ID] フィールドでプロファイル ID を設定し、[Tunnel ID] フィールドでトンネル ID を設定します。
- ステップ 5** 設定しているピア IP アドレスの [RemoteIPAddress] および [RemoteTCPPort] フィールドを設定します。
- ステップ 6** [TapeAccelerator] チェックボックスをオンにします。
- ステップ 7** (任意) このダイアログボックス内の他のフィールドを設定して、[Create] をクリックして、この FCIP リンクを作成します。

FCIP 圧縮

FCIP 圧縮機能を使用すると、この機能がイネーブル化された FCIP リンク上で、IP パケットを圧縮できます。デフォルトで、FCIP 圧縮はディセーブルです。イネーブルに設定すると、ソフトウェアはデフォルトで **auto** モードを使用します (モードが指定されていない場合)。



(注)

auto モード (デフォルト) では、カードタイプおよびリンクの帯域幅 (FCIP プロファイルの TCP パラメータに設定されているリンクの帯域幅) に基づいて適切な圧縮方式が選択されます。

表 2-4 に、さまざまなカードで使用されるモードを示します。

表 2-4 アルゴリズム分類

モード	IPS カード	MPS 14/2 カード	MSM-18/4/MDS 9222i/SSN-16
mode1	SW	HW	HW
mode2	SW	SW	HW
mode3	SW	SW	HW



(注) SAN-OS リリース 3.3(1) 以降および NX-OS リリース 4.x では、MDS 9222i スイッチおよび MSM-18/4 モジュールのすべての圧縮オプションはハードウェア圧縮を意味します。リリース 4.2(1) より、自動圧縮およびモード 2 圧縮だけが MDS 9222i スイッチ、MSM-18/4 モジュール、および SSN-16 モジュールでサポートされています。

表 2-5 に、各カードのパフォーマンス設定を示します。

表 2-5 パフォーマンス設定

帯域幅	IPS カード	MPS 14/2 カード	MSM-18/4/MDS 9222i/SSN-16
任意	-	-	auto
25 Mbps 以上	モード 1	モード 1	auto
10 ~ 25 Mbps	モード 2	モード 2	auto
10 Mbps	モード 3	モード 3	auto



(注) Cisco MDS 9216i および 9222i スイッチは、IP 圧縮機能もサポートします。統合型スーパーバイザ モジュールには、MPS-14/2 モジュールと同じハードウェア コンポーネントが搭載されています。



注意 Cisco SAN-OS リリース 2.0(1b) 以降および NX-OS リリース 4.x の圧縮モードは、Cisco SAN-OS リリース 1.3(1) 以前の圧縮モードと互換性がありません。



ヒント Cisco SAN OS リリース 1.x から Cisco SAN OS リリース 2.0(1b) 以降または NX-OS リリース 4.x にアップグレードする場合、アップグレードする前に圧縮をディセーブルにして、アップグレードが完了してから必要な圧縮モードをイネーブルにすることを推奨します。

FCIP リンクの両側で Cisco SAN OS リリース 2.0(1b) 以降および NX-OS リリース 4.x が使用されていて、FCIP トンネルの一方の側で圧縮をイネーブルにする場合には、必ずリンクのもう一方の側でも圧縮をイネーブルにします。

デフォルト設定

表 2-6 に、FCIP パラメータのデフォルト設定値を示します。

表 2-6 デフォルトの FCIP パラメータ

パラメータ	デフォルト
FCIP の TCP デフォルト ポート	3225
minimum-retransmit-time	200 ミリ秒
キープアライブ タイムアウト	60 秒
最大再送信	4 回の再送信
PMTU 検出	イネーブル
pmtu-enable reset-timeout	3600 秒
SACK	イネーブル
max-bandwidth	1 Gbps
min-available-bandwidth	500 Mbps
round-trip-time	1 ミリ秒
バッファ サイズ	0 KB
制御 TCP およびデータ接続	パケット送信なし
TCP 輻輳ウィンドウの監視	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 モードがイネーブル
special-frame	ディセーブル
FCIP タイムスタンプ	ディセーブル
パケットを受け入れる acceptable-diff 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	ディセーブル
テープ アクセラレーション	ディセーブル



CHAPTER 3

SAN 拡張チューナの設定

SAN Extension Tuner (SET; SAN 拡張チューナ) 機能は、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 I/O 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転送することにより、FCIP パフォーマンスを最適化するのに役立ちます。テスト I/O 転送のサイズとテスト時に生成する同時またはシリアル I/O の数を指定できます。SET は 1 秒あたりの入出力数（IOPS）と入出力待ち時間を通知します。この情報は、FCIP スループットを最大化するために必要な並行入出力の数を決定するのに役立ちます。

この章の内容は、次のとおりです。

- 「SAN 拡張チューナについて」 (P.3-1)
- 「ライセンス要件」 (P.3-3)
- 「SAN 拡張チューナの設定」 (P.3-4)
- 「SAN 拡張チューナ ウィザードの使用法」 (P.3-4)
- 「デフォルト設定」 (P.3-7)

SAN 拡張チューナについて



(注)

SAN 拡張チューナは、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)

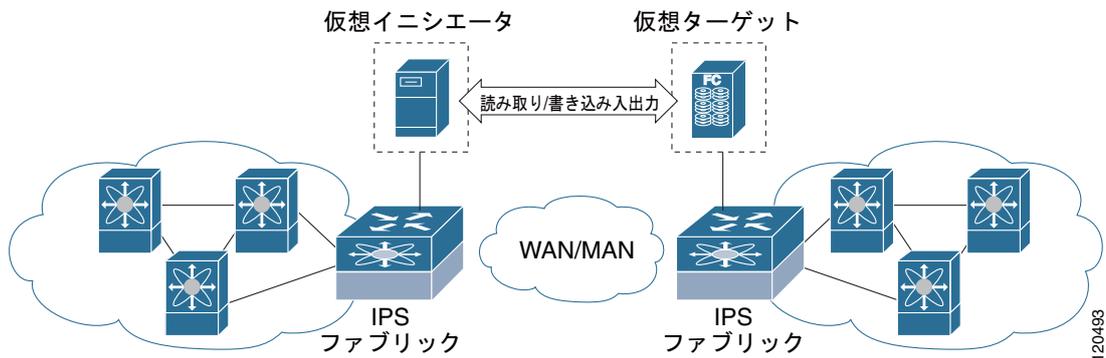
Cisco MDS SAN-OS リリース 3.3(1a) 以降 SAN 拡張チューナはマルチサービス モジュール (MSM) およびマルチサービス モジュラ スイッチでサポートされています。

リモート コピーやデータ バックアップなどのアプリケーションは、IP ネットワーク上で FCIP を使用して、地理的に分散している SAN を接続します。ファブリック全体のスループットを最大化するために、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](#)」 (P.2-19) を参照）
- アプリケーションによって生成される同時 SCSI 入出力数
- アプリケーションが FCIP リンク上で使用する伝送サイズ

SET は、IPS ポートに実装されます。この機能がイネーブルの場合、設定されたオプションに基づいて仮想ターゲットに対して SCSI 入出力コマンド（読み取りおよび書き込み）が生成されます（[図 3-1](#) を参照）。

図 3-1 仮想ターゲットに対する SCSI コマンドの生成



SET 機能を使用すると、さまざまな SCSI トラフィック負荷を生成して調整できます。また、FCIP リンクを経由した入出力ごとのスループットと応答時間も測定されます。

SAN ファブリックを調整する前に、次の注意事項に注意してください。

- 次の実装詳細に従ってください。
 - 調整される設定が永続的でないこと。
 - 作成された仮想 N ポートが、ネーム サーバでサポートされる FC4 機能を登録しないこと。これは、SAN 内のホストがこれらの N ポートを通常のイニシエータやターゲットとして検出するのを避けるためです。
 - SAN 内の他のイニシエータからのログイン要求が拒否されること。
 - 仮想 N ポートが SCSI スイート全体を実装せず、SCSI 読み取り/書き込みコマンドだけを実装すること。
 - チューナのイニシエータはチューナのターゲットとだけ通信できること。
- ギガビット イーサネット インターフェイスが物理レイヤ（GBIC および接続ケーブル、IP アドレスは不要）で動作していることを確認します。
- スイッチで iSCSI をイネーブルにします（その他の iSCSI 設定は不要）。
- インターフェイスをイネーブルにします（その他の iSCSI インターフェイス設定は不要）。
詳細については、「[iSCSI インターフェイスの作成](#)」(P.4-6) を参照してください。
- ネットワークでの必要性に応じて、個別の VSAN またはゾーンで仮想 N ポートを設定します。
- 仮想 N ポートだけを持つ個別の VSAN は必須ではありませんが、ターゲットへのログインが拒否された場合に従来の一部の HBA がログインできない可能性がある場合に推奨されます。
- 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（別のギガビット 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、仮想 N ポートによって生成されるトラフィックが FCIP リンクのパフォーマンスを妨げる可能性がある場合に推奨されます。

SAN 拡張チューナの設定

図 3-2 は、スループットと遅延が測定される FCIP リンクに属さないポート上で作成された仮想 N ポートの物理構成例です。

図 3-2 N ポート チューニングの物理構成例

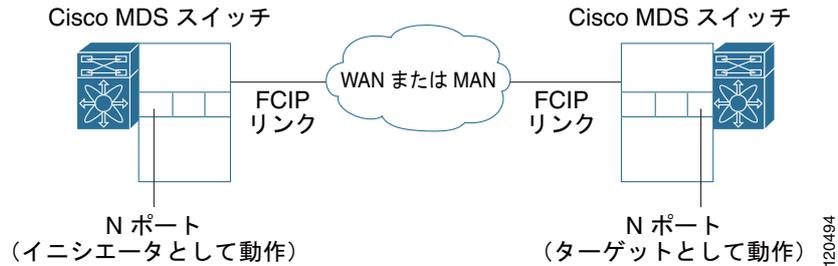
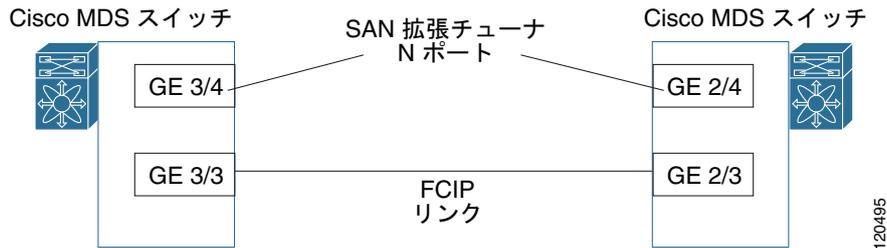


図 3-3 は、スループットと遅延が測定される FCIP リンクに属さないポート上で作成された仮想 N ポートの論理構成例です。

図 3-3 FCIP リンクの N ポート チューニングの論理構成例



データ パターン

デフォルトでは、仮想 N ポートによって生成されたデータのパターンとして、すべてゼロ パターンが使用されます。オプションで、3 つの位置の 1 つからデータ パターン ファイルを選択して、データ パターンを生成するファイルを指定できます (bootflash: ディレクトリ、volatile: ディレクトリ、または slot0: ディレクトリ)。このオプションは、特に Fibre Channel over IP (FCIP) リンクで圧縮をテストするときに役立ちます。また、ベンチマークを目的として、Canterbury コーパス ファイルまたは人工的コーパス ファイルも使用できます。

ライセンス要件

SET を使用するには、SAN_EXTN_OVER_IP ライセンスが必要です (『Cisco MDS 9000 Family NX-OS Licensing Guide』を参照)。

SAN 拡張チューナの設定

ここで説明する内容は、次のとおりです。

- 「FCIP リンクのチューニング」(P.3-4)

FCIP リンクのチューニング

所定の FCIP リンクをチューニングする手順は、次の手順を実行します。

-
- ステップ 1** スイッチ上で仮想 N ポートの 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で、iSCSI をイネーブルにします。
 - ステップ 3** FCIP リンクの各端で仮想 N ポートを設定します。
 - ステップ 4** 仮想 N ポートが SAN 内の実際のイニシエータから参照できないようにします。実際のイニシエータを分離するには、ゾーン分割 (『Cisco Fabric Manager Fabric Configuration Guide』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、ゾーン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** スイッチ内の他のギガビットイーサネットポートに N ポートを (必要に応じて) 追加し、スループットを最大化します。たとえば、FCIP PortChannel を使用する場合に追加 N ポートが必要になる可能性があります。
-

SAN 拡張チューナ ウィザードの使用法

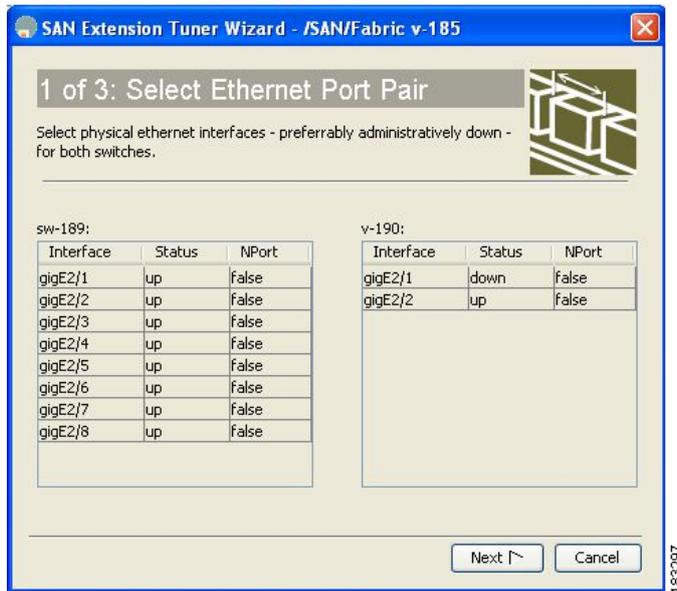
SAN 拡張チューナ ウィザードを使用して、次の作業を行います。

- nWWN ポートの設定
- iSCSI のイネーブル化
- 仮想 N ポートの設定
- SCSI read および write CLI コマンドの割り当て
- SCSI tape read および write CLI コマンドの割り当て
- SCSI コマンドの対応するデータ パターンの設定

Fabric Manager の SAN 拡張チューナ ウィザードを使用して所定の FCIP リンクを調整するには、次の手順を実行します。

-
- ステップ 1** [Fabric] ペインで有効な FCIP リンクを右クリックし、ドロップダウンリストから [SAN Extension Tuner] を選択します。リンクを強調表示して、[Tools] > [Other] > [SAN Extension Tuner] を選択することもできます。
[Select Ethernet Port Pair] ダイアログボックスが表示されます (図 3-4 を参照)。

図 3-4 [Select Ethernet Port Pair] ダイアログボックス



ステップ 2 調整予定の FCIP リンクに対応するイーサネットポートペアを選択し、[Next] をクリックします。

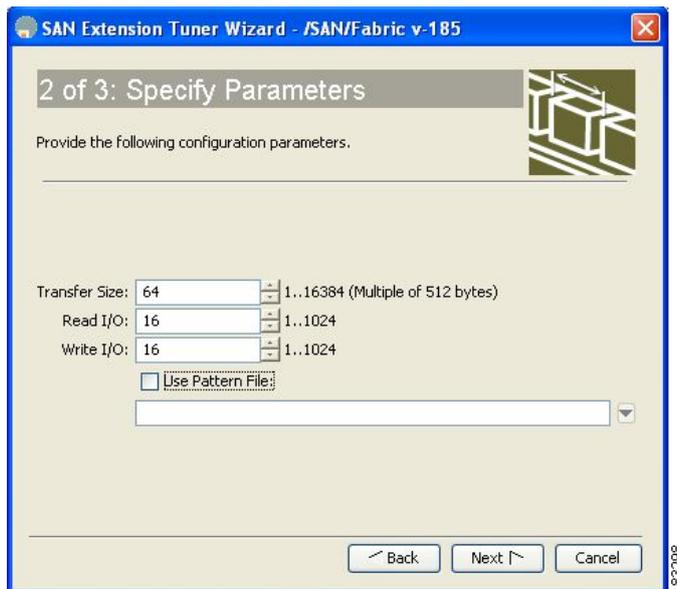


(注) 選択したイーサネットポートが表示されます。

[Specify Parameters] ダイアログボックスが表示されます (図 3-5 を参照)。

ステップ 3 新しいゾーンを作成してアクティブにし、ゾーン作成ダイアログボックスで [Yes] をクリックすることによって、SAN 内の実発信側に仮想 N ポートが認識されないようにします。

図 3-5 [Specify Parameters] ダイアログボックス



- ステップ 4** (任意) 転送データ サイズおよび並行 SCSI read/write コマンドの数について、デフォルトの設定を変更します。
- [Transfer Size] を FCIP リンク上でアプリケーションが使用すると予想されるバイト数に設定します。
 - [Read I/O] を FCIP リンク上でアプリケーションが生成すると予想される並行 SCSI read コマンドの数にします。
 - [Write I/O] を FCIP リンク上でアプリケーションが生成すると予想される並行未処理 SCSI write コマンドの数に設定します。

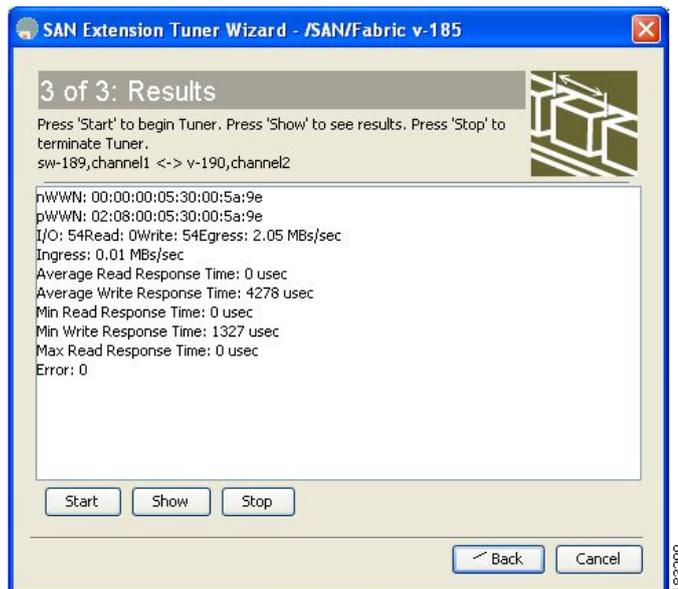


(注) テープ動作をエミュレーションする仮想 N ポートに対しては、未処理の入出力は一時点で 1 つだけです。

- [Use Pattern File] チェックボックスをオンにして、SET に生成させるデータ パターンを設定する目的で使用するファイルを選択します。「データ パターン」(P.3-3) を参照してください。

- ステップ 5** [Next] をクリックします。
[Results] ダイアログボックスが表示されます (図 3-6 を参照)。

図 3-6 [Results] ダイアログボックス



- ステップ 6** [Start] をクリックしてチューナーを起動します。[Stop] をクリックするまで、チューナーはトラフィックの連続ストリームを送信します。
- ステップ 7** [Show] をクリックして、最新の調整統計情報を表示します。これは、チューナーの動作中でも、停止後でも選択できます。
- ステップ 8** [Stop] をクリックして、SET を停止します。

デフォルト設定

表 3-1 に、調整パラメータのデフォルト設定を示します。

表 3-1 デフォルトの調整パラメータ

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



CHAPTER 4

iSCSI の設定

Cisco MDS 9000 ファミリの IP Storage (IPS; IP ストレージ) 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して、ファイバチャネル Storage Area Network (SAN; ストレージエリアネットワーク) の到達距離を延長します。このスイッチを使用すると、iSCSI プロトコルを使用して 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ます。



(注) iSCSI 機能は、IPS モジュールに特有の機能であり、Cisco MDS 9200 スイッチまたは Cisco MDS 9500 ディレクタで使用できます。

Cisco MDS 9216i スイッチと 14/2 Multiprotocol Services (MPS-14/2) モジュールを使用すると、ファイバチャネル、FCIP、および iSCSI の機能も利用できます。MPS-14/2 モジュールは、Cisco MDS 9200 シリーズまたは Cisco MDS 9500 シリーズのどのスイッチでも使用できます。



(注) ギガビットイーサネットインターフェイスの設定については、「IPv4 の基本的なギガビットイーサネットの設定」(P.7-2) を参照してください。

この章の内容は、次のとおりです。

- 「iSCSI の概要」(P.4-2)
- 「iSCSI の設定」(P.4-4)
- 「iSLB の設定」(P.4-37)
- 「iSCSI ハイアベイラビリティ」(P.4-53)
- 「iSCSI 認証セットアップに関する注意事項とシナリオ」(P.4-60)
- 「iSNS」(P.4-72)
- 「iSNS クラウド検出」(P.4-79)
- 「デフォルト設定」(P.4-81)

iSCSI の概要

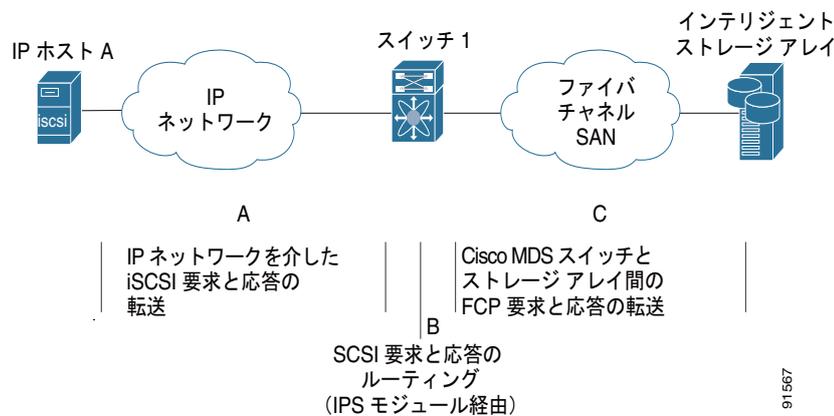


(注)

iSCSI 機能は、Cisco Fabric Switch for HP c-Class Bladesystem 上および Cisco Fabric Switch for IBM BladeCenter 上ではサポートされていません。

iSCSI 機能は、IP ネットワークでの iSCSI ホスト間の iSCSI 要求と応答のルーティングと、Cisco MDS 9000 ファミリのスイッチのファイバ チャンネル インターフェイスからアクセス可能なファイバ チャンネル SAN 内のファイバ チャンネル ストレージ デバイスで構成されます (図 4-1 を参照)。

図 4-1 透過的な iSCSI ルーティングのための iSCSI 要求と応答の転送

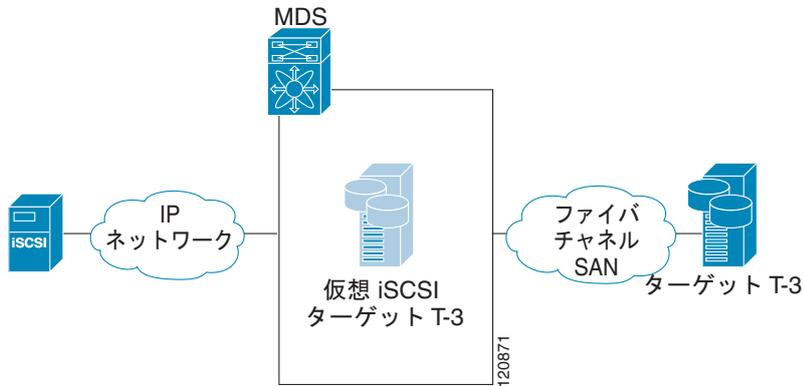


IPS モジュールまたは MPS-14/2 モジュールを介してストレージにアクセスする必要がある iSCSI ホストそれぞれに、互換性のある iSCSI ドライバがインストールされている必要があります (Cisco.com Web サイトの <http://www.cisco.com/cgi-bin/tablebuild.pl/sn5420-scsi> では、互換ドライバの一覧を確認できます)。iSCSI プロトコルを使用して、iSCSI ドライバは、iSCSI ホストからの SCSI の要求と応答を IP ネットワークを介して転送できます。ホストのオペレーティング システムの観点から、iSCSI ドライバは、ホスト内にファイバ チャンネル 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 モジュールまたは MPS-14/2 モジュールにより、透過的な SCSI ルーティングが提供されます。iSCSI プロトコルを使用する IP ホストは、ファイバ チャンネル 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。図 4-1 に、IP ネットワークを介して IPS モジュールまたは MPS-14/2 モジュールに接続した iSCSI ホストがファイバ チャンネル SAN 上のファイバ チャンネル ストレージにアクセスする場合の一般的な設定例を示します。

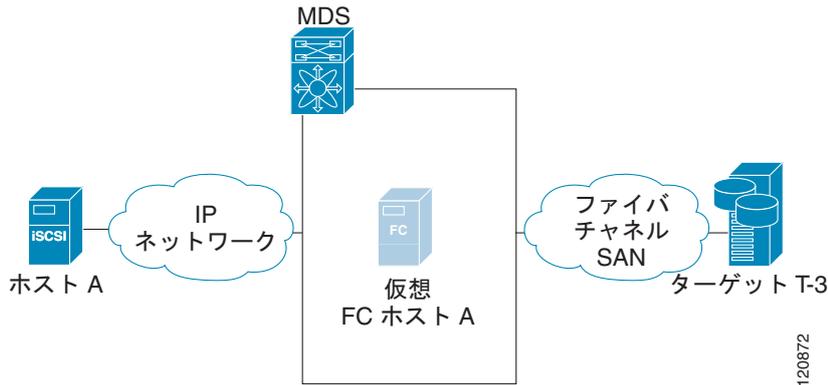
IPS モジュールまたは MPS-14/2 モジュールは、iSCSI SAN ビューとファイバ チャンネル SAN ビューを別々に作成します。iSCSI SAN ビューの場合、IPS モジュールまたは MPS-14/2 モジュールは、iSCSI 仮想ターゲットを作成してから、それをファイバ チャンネル SAN で使用可能な物理ファイバ チャンネル ターゲットにマッピングします。物理 iSCSI ターゲットが IP ネットワークに接続されているかのように、IP ホストに対してファイバ チャンネル ターゲットを示します (図 4-2 を参照)。

図 4-2 iSCSI SAN ビュー : iSCSI 仮想ターゲット



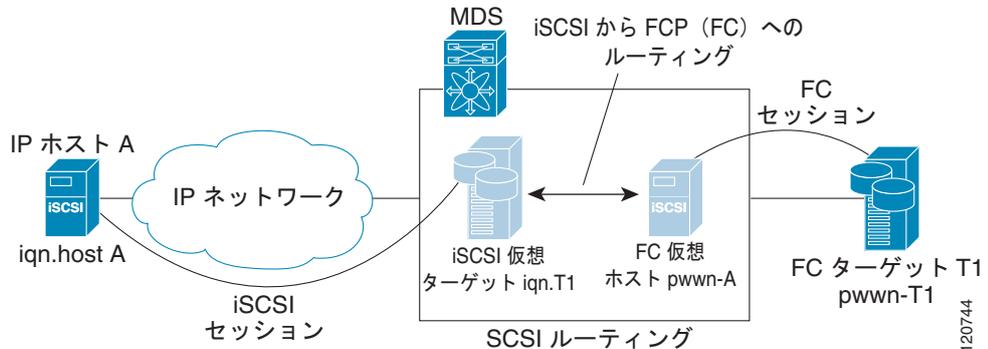
ファイバチャネル SAN ビューの場合、IPS モジュールまたは MPS-14/2 モジュールは、iSCSI ホストを仮想ファイバチャネルホストとして示します。ストレージデバイスは、実際のファイバチャネルホストと行う通信と同じように、仮想ファイバチャネルホストと通信します (図 4-3 を参照)。

図 4-3 ファイバチャネル SAN ビュー : HBA としての iSCSI ホスト



IPS 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のコマンドを透過的に対応付けます (図 4-4 を参照)。

図 4-4 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 SCSI のルーティングは、次の主要な処理で構成されます。

- iSCSI の要求と応答は、ホストと IPS モジュールまたは MPS-14/2 モジュールの間を IP ネットワークを介して転送されます。
- SCSI の要求と応答が、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の間でルーティングされます (iSCSI から FCP に変換されます。この逆も同様です)。IPS モジュールまたは MPS-14/2 モジュールは、このような変換とルーティングを実行します。
- FCP の要求または応答は、IPS 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の間で転送されます。



(注)

FCP (ファイバチャネルから見た場合 iSCSI に相当する) は、ファイバチャネル SAN を介して SCSI コマンドを渡します。

iSCSI プロトコルの詳細については、<http://www.ietf.org> で IP ストレージの IETF 標準を参照してください。

iSCSI 設定制限の概要

iSCSI 設定には次の制限があります。

- 1 つのファブリック内でサポートされる iSCSI イニシエータおよび iSLB イニシエータの最大数は 2000 です。
- サポートされる iSCSI イニシエータおよび iSLB イニシエータの最大数は、ポートあたり 200 です。
- トランスペアレント イニシエータ モードまたはプロキシ イニシエータ モードの IPS ポートでサポートされる iSCSI セッションおよび iSLB セッションの最大数は 500 です。
- スイッチでサポートされる iSCSI セッションおよび iSLB セッションの最大数は 5000 です。
- 1 つのファブリック内でサポートされる iSCSI ターゲットおよび iSLB ターゲットの最大数は 6000 です。

iSCSI の設定

ここでは、Cisco MDS 9000 ファミリのスイッチで iSCSI を設定する方法について説明します。

ここで説明する内容は、次のとおりです。

- 「iSCSI のイネーブル化」 (P.4-5)
- 「iSCSI インターフェイスの作成」 (P.4-6)
- 「iSCSI ウィザードの使用」 (P.4-7)
- 「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」 (P.4-9)
- 「iSCSI ホストの仮想ファイバチャネルホストとしての提示」 (P.4-16)
- 「iSCSI アクセスコントロール」 (P.4-26)
- 「iSCSI セッション認証」 (P.4-30)
- 「iSCSI の即時データ機能と非請求データ機能」 (P.4-34)
- 「iSCSI インターフェイスの詳細機能」 (P.4-34)

iSCSI のイネーブル化

iSCSI の機能を使用するには、ファブリック内の必要なスイッチで iSCSI を明示的にイネーブル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、Cisco MDS 9000 ファミリの全スイッチでこの機能がディセーブルに設定されています。



注意

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。

Fabric Manager を使用して任意のスイッチで iSCSI をイネーブルにする手順は、次のとおりです。

- ステップ 1** [Physical Attributes] ペインで [End Devices] > [iSCSI] を選択します。
[Information] ペインに iSCSI テーブルが表示されます (図 4-5 を参照)。

図 4-5 Fabric Manager の iSCSI テーブル

Switch	Feature	Status	Command	LastCommand	Result
sw172-22-46-102	iscsi	disabled	noSelection	noSelection	none
sw172-22-46-222	iscsi	enabled	noSelection	noSelection	none
sw172-22-46-224	iscsi	disabled	noSelection	noSelection	none
sw172-22-46-233	iscsi	enabled	noSelection	noSelection	none
sw172-22-46-220	iscsi	enabled	noSelection	noSelection	none
sw172-22-46-102	iscsi-interface-vsan-membership	disabled	noSelection	noSelection	none
sw172-22-46-221	iscsi	disabled	noSelection	noSelection	none
sw172-22-46-224	iscsi-interface-vsan-membership	disabled	noSelection	noSelection	none
sw172-22-46-223	iscsi	enabled	noSelection	noSelection	none
sw172-22-46-225	iscsi	disabled	noSelection	noSelection	none
sw172-22-46-174	iscsi	enabled	noSelection	noSelection	none
sw172-22-46-153	iscsi	enabled	noSelection	noSelection	none
sw172-22-46-153	iscsi-interface-vsan-membership	enabled	noSelection	noSelection	none

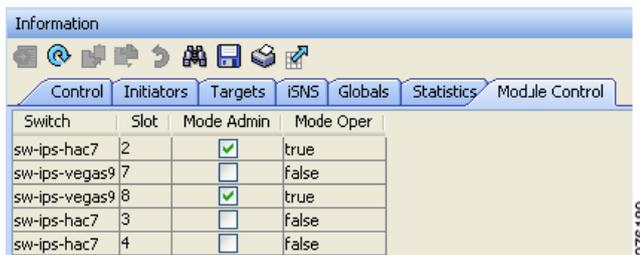
[Control] タブがデフォルトのタブです。ファブリック内の IPS ポートを持つすべてのスイッチについて、iSCSI のイネーブルの状態が表示されます。

- ステップ 2** iSCSI をイネーブルにする各スイッチの [Command] 列で [enable] を選択します。
ステップ 3 [Apply Changes] アイコンをクリックして、これらの変更を保存します。

Fabric Manager を使用してモジュールで iSCSI をイネーブルにする手順は、次のとおりです。

- ステップ 1** [Physical Attributes] ペインで [End Devices] > [iSCSI] を選択します。
[Information] ペインに iSCSI テーブルが表示されます。
ステップ 2 [Module Control] タブをクリックします。
[Information] ペインに [Module Control] ダイアログボックスが表示されます (図 4-6 を参照)。

図 4-6 [Module Control] ダイアログボックス



- ステップ 3** [Mode Admin] チェックボックスをオンにすると、選択したモジュールの特定のポートに対して iSCSI がイネーブルになります。
- ステップ 4** [Apply Changes] アイコンをクリックして、これらの変更を保存します。

Device Manager を使用してモジュールで iSCSI をイネーブルにする手順は、次のとおりです。

- ステップ 1** [IP] > [iSCSI] を選択します。
iSCSI テーブルが表示されます (図 4-7 を参照)。

図 4-7 iSCSI テーブル



- ステップ 2** [Admin Status] チェックボックスをオンにすると、選択したモジュールの指定ポートに対して iSCSI がイネーブルになります。
- ステップ 3** [Apply] をクリックして、これらの変更を保存します。

iSCSI インターフェイスの作成

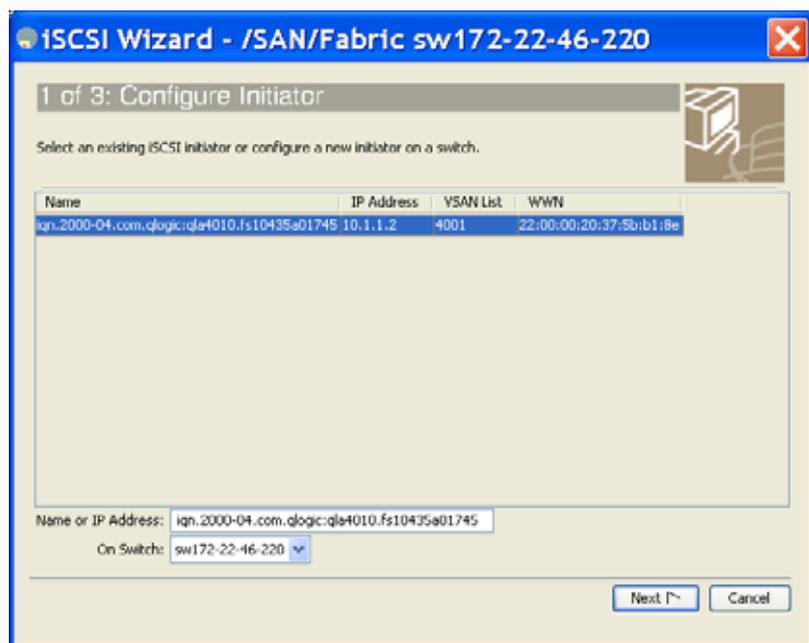
IPS モジュールまたは MPS-14/2 モジュールの各物理ギガビットイーサネットインターフェイスを使用して、iSCSI 要求を変換してファイバチャネルターゲットにルーティングし、これと反対の方向に応答を返します。この機能をイネーブルにするには、対応する iSCSI インターフェイスがイネーブルの状態になっている必要があります。

iSCSI ウィザードの使用

Fabric Manager の iSCSI ウィザードを使用する手順は、次のとおりです。

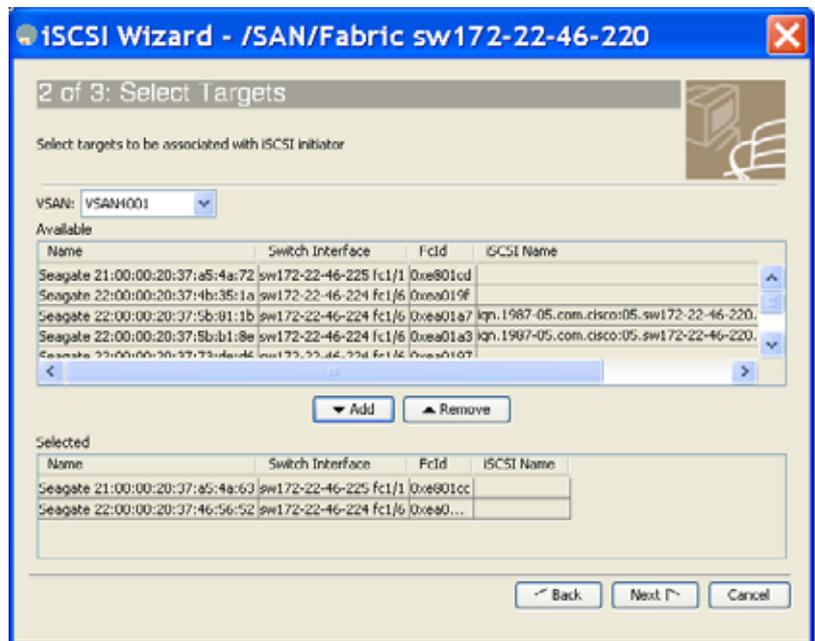
- ステップ 1** [iSCSI Setup Wizard] アイコンをクリックします。
iSCSI ウィザードの [Configure Initiator] ダイアログボックスが表示されます (図 4-8 を参照)。

図 4-8 iSCSI ウィザードの [Configure Initiator] ダイアログボックス



- ステップ 2** 既存の iSCSI イニシエータを選択するか、新規 iSCSI イニシエータの iSCSI ノード名または IP アドレスを追加します。
- ステップ 3** 新規 iSCSI イニシエータを追加する場合は、この iSCSI イニシエータに使用するスイッチを選択して、[Next] をクリックします。
iSCSI ウィザードの [Select Targets] ダイアログボックスが表示されます (図 4-9 を参照)。

図 4-9 iSCSI ウィザードの [Select Targets] ダイアログボックス



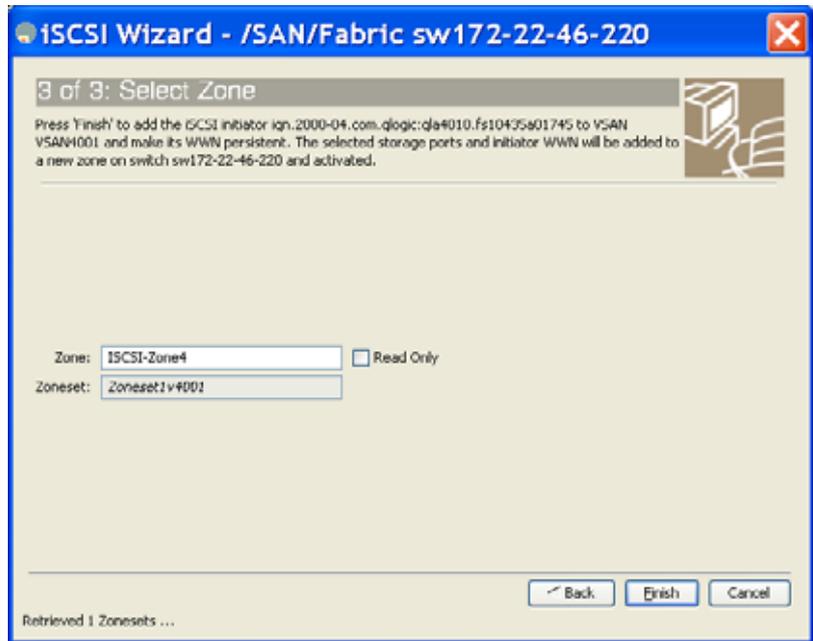
- ステップ 4** この iSCSI イニシエータに関連付ける VSAN およびターゲットを選択して、[Next] をクリックします。



(注) iSCSI ウィザードにより、FC ターゲットを動的にインポートする機能が有効になります。

iSCSI ウィザードの [Select Zone] ダイアログボックスが表示されます (図 4-10 を参照)。

図 4-10 iSCSI ウィザードの [Select Zone] ダイアログボックス



ステップ 5 この新しい iSCSI ゾーンにゾーン名を設定し、必要に応じて [Read Only] チェックボックスをオンにします。

ステップ 6 [Finish] をクリックして、この iSCSI イニシエータを作成します。
作成されると、ターゲット VSAN が iSCSI ホストの VSAN リストに追加されます。



(注) iSCSI ウィザードにより、FC ターゲットを動的にインポートする機能が自動的に有効になります。

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 モジュールまたは MPS-14/2 モジュールが物理ファイバ チャネル ターゲットを iSCSI 仮想ターゲットとして示すことで、iSCSI ホストはそれにアクセスできるようになります。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/ポートを iSCSI デバイスとして自動的にマッピングします。このマッピングを使用すると、自動的に iSCSI ターゲット名を作成します。
- **スタティック マッピング** : iSCSI ターゲット デバイスを手動で作成し、それをファイバ チャネル ターゲット ポート全体、またはファイバ チャネルの Logical Unit Number (LUN) のサブセットにマッピングします。このマッピングを使用する場合は、固有の iSCSI ターゲット名を指定する必要があります。

iSCSI ホストをファイバ チャネル ターゲットの LU のサブセットに制限すべき場合、iSCSI アクセス コントロールを必要とする場合（「[iSCSI アクセス コントロール](#)」(P.4-26) を参照）、またはどちらの条件もあてはまる場合は、スタティック マッピングを使用する必要があります。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ーを設定できます（「[透過的なターゲット フェールオーバー](#)」(P.4-54) を参照）。



(注)

IPS モジュールまたは MPS-14/2 モジュールは、デフォルトではファイバ チャネル ターゲットを iSCSI にインポートしません。IPS モジュールまたは MPS-14/2 モジュールで iSCSI イニシエータが使用可能なファイバ チャネル ターゲットを作成する前に、ダイナミック マッピングまたはスタティック マッピングのいずれかを設定する必要があります。

ダイナミック マッピング

ダイナミック マッピングを設定する場合、IPS 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て、物理ファイバ チャネル ターゲット ポートをそれぞれ 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 ポートを使用してアクセス可能なすべての LU を、物理ファイバ チャネル ターゲット ポート内と同じ LU Number (LUN) を用いて iSCSI LU として使用できます。

iSCSI ターゲット ノード名は、iSCSI Qualified Name (IQN; iSCSI 修飾名) フォーマットを使用して自動的に作成されます。iSCSI 修飾名には、名前の長さを最大 223 文字、最小 16 文字の英数字とする制約があります。

SAN 内では固有の名前になる必要があるため、IPS モジュールまたは MPS-14/2 モジュールは、次の表記法を使用して IQN フォーマットに基づいた iSCSI ターゲット ノード名を作成します。

- Virtual Router Redundancy Protocol (VRRP; 仮想ルータ冗長プロトコル) グループまたは PortChannel に属していない IPS ギガビット イーサネット ポートは、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>
```

- PortChannel に属しているポートは、次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)

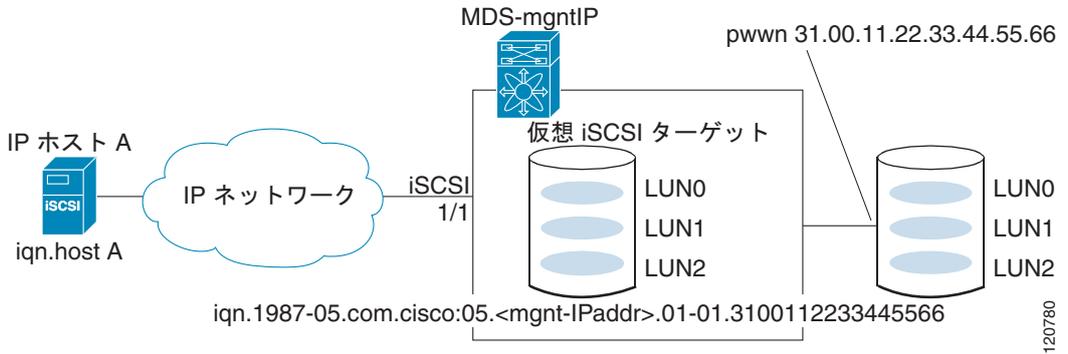
スイッチ名を設定している場合は、管理 IP アドレスの代わりにスイッチ名を使用します。スイッチ名を設定していない場合は、管理 IP アドレスを使用します。

この表記法を使用して、Cisco MDS 9000 ファミリのスイッチの IPS ポートはそれぞれ、SAN 内で同一のファイバ チャネル ターゲット ポートに対する固有の iSCSI ターゲット ノード名を作成します。

たとえば、pWWN 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 ターゲットを作成した場合で、その pWWN に LUN 0、LUN 1、および LUN 2 が含まれるとき、IP ホストは iSCSI ターゲット ノード名

iqn.1987-05.com.cisco:05.MDS_switch_management_IP_address.01-01.3100112233445566 を使用して、これらの LUN を使用できるようになります（[図 4-11](#) を参照）。

図 4-11 ダイナミック ターゲット マッピング



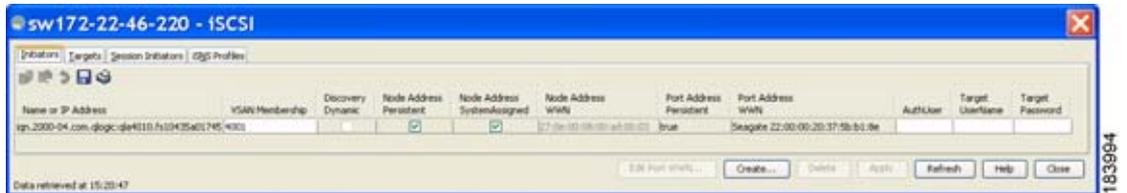
(注)

設定されているアクセスコントロールのメカニズムによっては、各 iSCSI イニシエータがアクセスできるターゲットがすべてのターゲットではない場合があります（「iSCSI アクセス コントロール」(P.4-26) を参照）。

Device Manager を使用してファイバチャネルターゲットの iSCSI へのダイナミック マッピングをイネーブルにする手順は、次のとおりです。

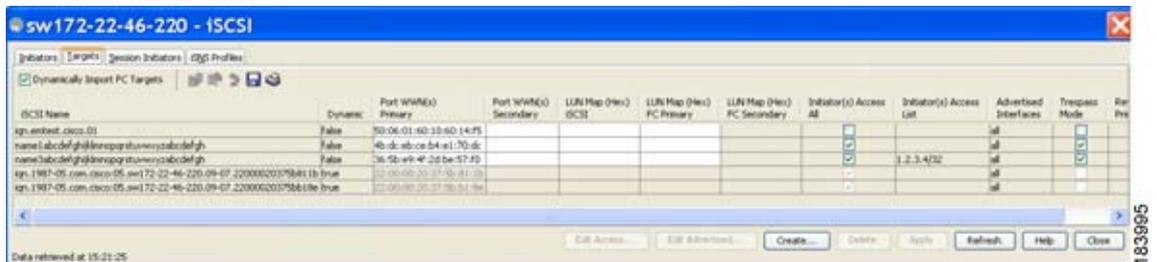
- ステップ 1** [IP] > [iSCSI] を選択します。
iSCSI 設定が表示されます (図 4-12 を参照)。

図 4-12 Device Manager での iSCSI 設定



- ステップ 2** [Targets] タブをクリックして、既存の iSCSI ターゲットのリストを表示します (図 4-13 を参照)。

図 4-13 iSCSI の [Targets] タブ

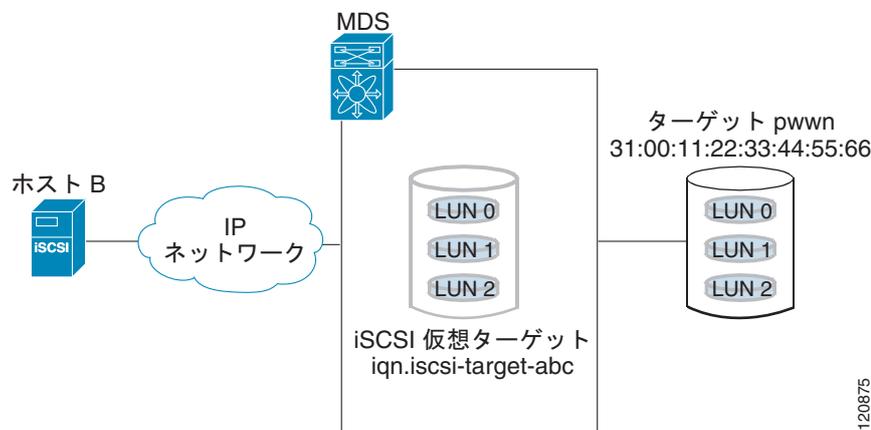


- ステップ 3** [Dynamically Import FC Targets] チェックボックスをオンにします。
- ステップ 4** [Apply] をクリックして、この変更を保存します。

スタティック マッピング

ユーザ定義の固有の iSCSI ノード名を割り当てることで iSCSI ターゲットを手動で（静的に）作成できます。iSCSI 修飾名の長さには、最小 16 文字、最大 223 文字の制約があります。スタティック マッピングされた iSCSI ターゲットは、ファイバチャネルターゲットポート全体（iSCSI ターゲットにマッピングされたターゲットポートのすべての LUN）を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から 1 つ以上の LU を含めることもできます（図 4-14 を参照）。

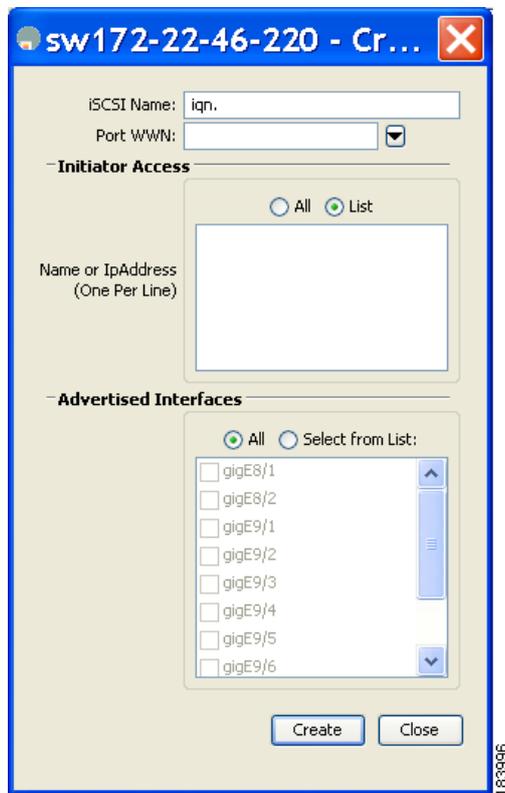
図 4-14 スタティック マッピングされた iSCSI ターゲット



Device Manager を使用してファイバチャネルターゲットポート全体に対してスタティック iSCSI 仮想ターゲットを作成する手順は、次のとおりです。

- ステップ 1** [IP] > [iSCSI] をクリックします。
iSCSI 設定が表示されます（図 4-12 を参照）。
- ステップ 2** [Targets] タブをクリックして、既存の iSCSI ターゲットのリストを表示します（図 4-13 を参照）。
- ステップ 3** [Create] をクリックして iSCSI ターゲットを作成します。
[Create iSCSI Targets] ダイアログボックスが表示されます（図 4-15 を参照）。

図 4-15 [Create iSCSI Targets] ダイアログボックス



- ステップ 4** [iSCSI Name] フィールドに iSCSI ターゲット ノード名を IQN フォーマットで設定します。
- ステップ 5** [Port WWN] フィールドにマッピングするファイバチャネルターゲットポートを設定します。
- ステップ 6** [Select from List] オプション ボタンをクリックして、この仮想 iSCSI ターゲットをアクセスさせる iSCSI イニシエータ ノード名または IP アドレスを設定するか、または、[All] オプション ボタンをクリックして、この仮想 iSCSI ターゲットをすべての iSCSI イニシエータにアクセスさせるようにします。「[iSCSI アクセス コントロール](#)」(P.4-26) も参照してください。
- ステップ 7** [Select from List] オプション ボタンをクリックして、iSCSI ターゲットをアドバタイズするインターフェイスをそれぞれ選択するか、[All] オプション ボタンをクリックして、すべてのインターフェイスをアドバタイズします。
- ステップ 8** [Apply] をクリックして、この変更を保存します。


ヒント

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。すでにファイバチャネルターゲットポート全体をマッピングしている場合は、LUN マッピング オプションを使用できません。


(注)

スタティック マッピングされたターゲットへのアクセスの制御については、「[iSCSI ベースのアクセス コントロール](#)」(P.4-28) 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ジング

スタティック iSCSI ターゲットをアドバタイズ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。iSCSI ターゲットは、デフォルトで、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、PortChannel インターフェイス、および PortChannel サブインターフェイスでアドバタイズされます。

Device Manager を使用して iSCSI 仮想ターゲットをアドバタイズする必要がある特定のインターフェイスを設定する手順は、次のとおりです。

-
- ステップ 1** [IP] > [iSCSI] を選択します。
iSCSI 設定が表示されます (図 4-12 を参照)。
- ステップ 2** [Targets] タブをクリックして、既存の iSCSI ターゲットのリストを表示します (図 4-13 を参照)。
- ステップ 3** 修正する iSCSI ターゲットを右クリックして [Edit Advertised] をクリックします。
[Advertised Interfaces] ダイアログボックスが表示されます。
- ステップ 4** (任意) 削除するインターフェイスを右クリックして [Delete] をクリックします。
- ステップ 5** (任意) アドバタイズするインターフェイスをさらに作成する場合は、[Create] をクリックします。
[Create Advertised Interfaces] ダイアログボックスが表示されます。
-

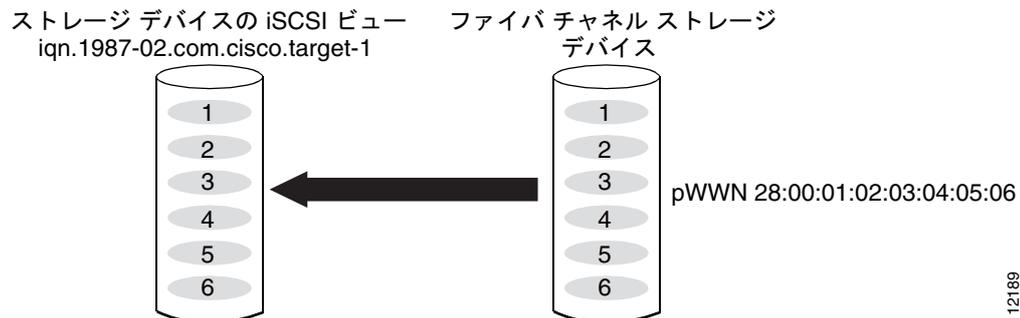
iSCSI 仮想ターゲットの設定例

ここでは、iSCSI 仮想ターゲットの設定例を 3 つ説明します。

例 1

この例では、ファイバチャネルターゲット全体を iSCSI 仮想ターゲットとして割り当てます。ファイバチャネルターゲットに属しているすべての LUN は、iSCSI ターゲットに属しているものとして使用できます (図 4-16 を参照)。

図 4-16 iSCSI ノード名の割り当て



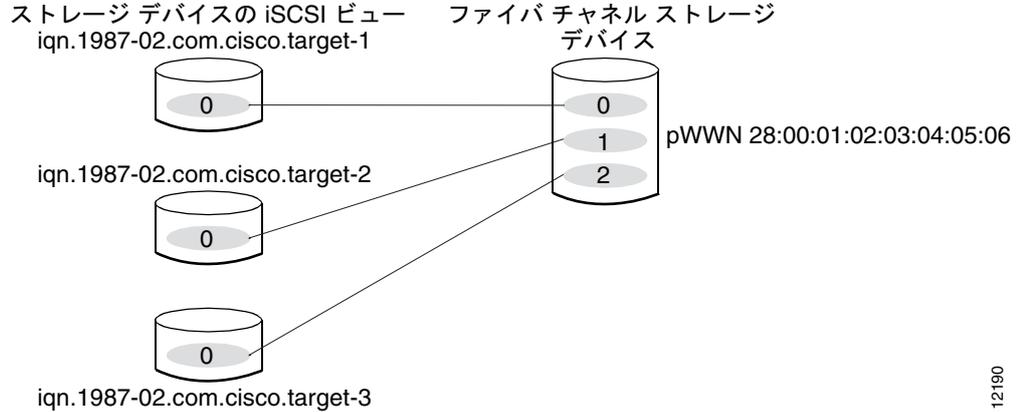
```
iscsi virtual-target name iqn.1987-02.com.cisco.target-1
pwwn 28:00:01:02:03:04:05:06
```

112189

例 2

この例では、ファイバチャネルターゲットの LUN のサブネットを 3 つの iSCSI 仮想ターゲットにマッピングします。各 iSCSI ターゲットは LUN を 1 つずつ持ちます (図 4-17 を参照)。

図 4-17 LUN の iSCSI ノード名へのマッピング



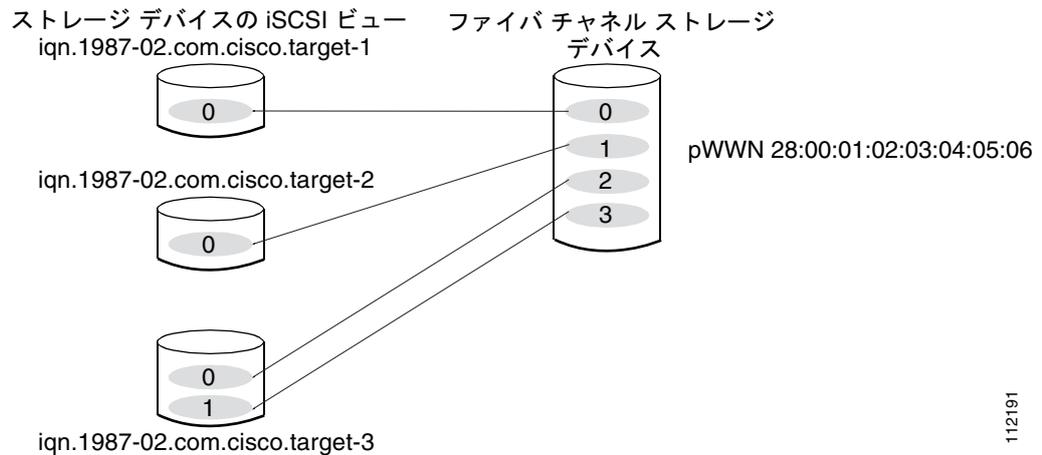
112190

```
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
```

例 3

この例では、ファイバチャネル LUN ターゲットの 3 つのサブネットを 3 つの iSCSI 仮想ターゲットにマッピングします。2 つの iSCSI ターゲットはそれぞれ LUN を 1 つずつ持ち、3 つめの iSCSI ターゲットは 2 つの LUN を持ちます (図 4-18 を参照)。

図 4-18 LUN の複数の iSCSI ノード名へのマッピング



112191

```
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
```

iSCSI ホストの仮想ファイバ チャンネル ホストとしての提示

IPS モジュールまたは MPS-14/2 モジュールは、iSCSI ホストの代わりにファイバ チャンネル ストレージ デバイスに接続し、コマンドを送信してストレージ デバイスを出入りするデータを転送します。これらのモジュールは、仮想ファイバ チャンネル N ポートを使用して、iSCSI ホストの代わりにファイバ チャンネル 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 アドレスのいずれかで識別されます。

イニシエータの識別

IPS モジュールまたは MPS-14/2 モジュールでは、次の情報を使用して iSCSI ホストを識別できます。

- iSCSI 修飾名 (IQN)

iSCSI イニシエータは、iSCSI ログインの際に提供する iSCSI ノード名に基づいて識別されます。iSCSI ホストに複数の IP アドレスがある場合で、そのホストで使用する IP アドレスに依存せずに、同一サービスを提供する場合にはこのモードが便利です。複数の IP アドレス (複数の Network Interface Card [NIC; ネットワーク インターフェイス カード]) を持つイニシエータは、ログインする IPS ポートそれぞれに 1 つずつ仮想 N ポートを持ちます。

- IP アドレス

iSCSI イニシエータは、iSCSI ホストの IP アドレスに基づいて識別されます。iSCSI ホストに複数の IP アドレスがある場合で、そのホストで使用する IP アドレスに基づいて異なるサービスを提供する場合にはこのモードが便利です。また、iSCSI ノード名の取得に比べ、ホストの IP アドレスを取得する方が簡単です。仮想 N ポートは、iSCSI ターゲットへのログインに使用する IP アドレスごとに作成されます。ホストが 1 つの IP アドレスを使用して複数の IPS ポートにログインする場合、各 IPS ポートがその IP アドレスに対して仮想 N ポートを 1 つずつ作成します。

各 IPS ポートで iSCSI イニシエータの識別モードを設定し、その設定に従って、IPS ポートで終端するすべての iSCSI ホストを識別できます。デフォルトモードは、名前によるイニシエータの識別です。

Fabric Manager を使用してイニシエータの識別モードを指定する手順は、次のとおりです。

-
- ステップ 1** [Physical Attributes] ペインで [Interfaces] > [FC Logical] を選択します。
[Information] ペインにインターフェイス設定が表示されます。
- ステップ 2** [iSCSI] タブをクリックします。
iSCSI インターフェイス設定が表示されます。
- ステップ 3** 修正する iSCSI インターフェイスの [Initiator ID Mode] フィールドを右クリックして、ドロップダウンメニューから [name] または [ipaddress] を選択します。
- ステップ 4** [Apply Changes] をクリックして、この変更を保存します。
-

イニシエータ プレゼンテーション モード

ファイバチャネル ファブリック内で iSCSI ホストを示すために、トランスペアレント 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 つのモードを使用できます。

- トランスペアレント イニシエータ モードでは、iSCSI ホストがそれぞれ 1 つの仮想ファイバチャネル ホストとして示されます。トランスペアレント モードの利点は、「実際の」ファイバチャネル ホストを管理するのと同じように) より詳細にファイバチャネル アクセス コントロールを設定できることです。iSCSI からファイバチャネルへのマッピングは 1 対 1 であるため、ホストごとに異なるゾーン分割が設定されるか、ファイバチャネル ストレージ デバイスでの LUN アクセス コントロールが設定されます。
- プロキシ イニシエータ モードでは、1 つの IPS ポート単位に仮想ファイバチャネル ホストが 1 つだけあり、すべての iSCSI ホストがそれ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 デバイスですべてのホストに対して明示的な LUN アクセス コントロールを必要とする状況では、iSCSI イニシエータごとに固定した設定を避けられない場合があります。この場合は、プロキシ イニシエータ モードを使用すると、設定を簡易化できます。



注意

iSLB VRRP グループに属している iSCSI インターフェイスのプロキシ イニシエータ モードをイネーブルにすると、そのインターフェイスのロード バランシングに影響します。「[iSCSI インターフェイス パラメータの変更とロード バランシングに対するその影響](#)」(P.4-48) を参照してください。

Cisco MDS スイッチには、次の iSCSI セッション制限があります。

- スイッチでの iSCSI セッションの最大数は 5000 です。
- トランスペアレント イニシエータ モードの IPS ポートあたりの iSCSI セッションの最大数は 500 です。
- プロキシ イニシエータ モードの IPS ポートあたりの iSCSI セッションの最大数は 500 です。
- IPS ポートが同時に作成できるセッションの最大数は 5 です (ただし、サポートできるセッションの合計は 500 です)。



(注)

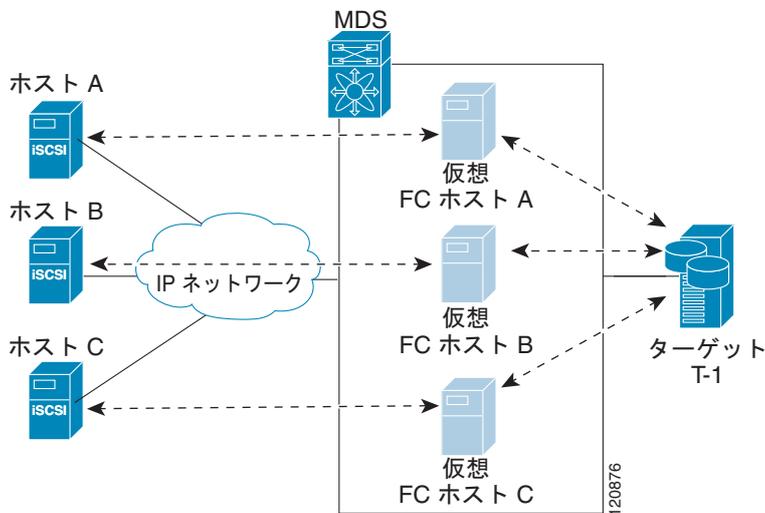
5 個を超えて iSCSI セッションが 1 つのポート上に同時に発生しそうになると、イニシエータが一時的なエラーを受信して、セッションの作成を後で再試行します。

トランスペアレント イニシエータ モード

iSCSI ホストはそれぞれ、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) として示されます。トランスペアレント モードの利点は、より詳細にファイバチャネル アクセス コントロールを設定できることです。iSCSI からファイバチャネルへのマッピングは 1 対 1 であるため、ホストごとに異なるゾーン分割が設定されるか、ファイバチャネル ストレージ デバイスでの LUN アクセス コントロールが設定されます。

iSCSI ホストが IPS モジュールまたは MPS-14/2 モジュールに接続するときに、そのホストに対する仮想ホスト N ポート (Host Bus Adapter [HBA] ポート) が作成されます (図 4-19 を参照)。どのファイバチャネル N ポートにも固有のノード WWN とポート WWN が必要です。

図 4-19 仮想ホストの HBA ポート



仮想 N ポートを WWN で作成した後、IPS ポートの仮想 iSCSI インターフェイスを介して Fabric Login (FLOGI; ファブリック ログイン) が実行されます。FLOGI が完了すると、仮想 N ポートがファイバ チャンネル SAN でオンラインになり、ファイバ チャンネル ネーム サーバに仮想 N ポートが登録されます。IPS モジュールまたは MPS-14/2 モジュールは、ファイバ チャンネル 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 サーバの symbolic-node-name フィールドに iSCSI ホストの IQN
- ネーム サーバの FC-4 type フィールドに SCSI_FCP
- ネーム サーバの FC-4 機能のイニシエータ フラグ
- FC-4 type フィールドにベンダー固有の iSCSI GW フラグ (ネーム サーバで N ポート デバイスを iSCSI ゲートウェイ デバイスとして識別するため)

iSCSI ホストからの iSCSI セッションがすべて終了すると、IPS モジュールまたは MPS-14/2 モジュールは、明示的な Fabric Logout (FLOGO; ファブリック ログアウト) を実行して、仮想 N ポート デバイスをファイバ チャンネル SAN から削除します (これにより、間接的にファイバ チャンネル ネーム サーバからデバイスが登録解除されます)。

ホストから iSCSI 仮想ターゲットへのどの iSCSI セッションにも、実際のファイバ チャンネル ターゲットへの対応するファイバ チャンネル セッションが 1 つずつ存在します。図 4-19 では、3 つの iSCSI ホストが存在し、その 3 つすべてが同じファイバ チャンネル ターゲットに接続しています。3 つの仮想ファイバ チャンネル ホストごとにターゲットへのファイバ チャンネル 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 イニシエータのアイドル タイムアウトは、イニシエータが自身の最後の iSCSI セッションをログアウトしてから、仮想ファイバ チャンネル N ポートがアイドル状態を続ける時間を指定します。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 チャンネル SAN に対してログインおよびログアウトを行わないようにするのに役立ちます。これにより、ファイバ チャンネル SAN で不必要に生成される Registered State Change Notification (RSCN) が削減されます。

Fabric Manager を使用してイニシエータのアイドル タイムアウトを設定する手順は、次のとおりです。

-
- ステップ 1** [Physical Attributes] ペインで [End Devices] > [iSCSI] を選択します。
[Information] ペインに iSCSI テーブルが表示されます (図 4-5 を参照)。
- ステップ 2** [Globals] タブをクリックします。
iSCSI グローバル設定が表示されます。
- ステップ 3** 修正する [InitiatorIdle Timeout] フィールドを右クリックして、新しいタイムアウト値を入力します。
- ステップ 4** [Apply Changes] アイコンをクリックして、これらの変更を保存します。
-

iSCSI イニシエータの WWN の割り当て

iSCSI ホストは、次のメカニズムのいずれかを使用して N ポートの WWN にマッピングされます。

- 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、動的に生成された port WWN (pWWN; ポート WWN) および node WWN (nWWN; ノード WWN) にマッピングされます。iSCSI ホストが接続するたびに、異なる WWN にマッピングされる可能性があります。ファイバ チャンネル ターゲット デバイスでアクセス コントロールを必要としない場合は、このオプションを使用します (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 を使用して設定されるためです)。

WWN は、MDS スイッチの WWN プールから割り当てられます。iSCSI に対する WWN マッピングは、iSCSI ホストから IPS ポートへの iSCSI セッションが 1 つ以上存在する限り維持されます。ホストからの iSCSI セッションがすべて終了し、IPS 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 チャンネル WWN プールに戻されます。これで、ファイバ チャンネル ファブリックへのアクセスを要求している他の iSCSI ホストの割り当てに、これらのアドレスを使用できるようになります。

サポートされるダイナミック イニシエータ モードは次の 3 つです。

- iSCSI : ダイナミック イニシエータは、iSCSI イニシエータとして扱われ、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。
- Deny : 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で動作するモードです。この設定は、CFS を使用して配信されます。



(注)

ダイナミック イニシエータ モードは、Device Manager または Fabric Manager ではなく、CLI による設定だけがサポートされます。

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 にマッピングされます。このマッピングは永続的なストレージに保持され、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 デバイスでアクセス コントロールを使用する場合は、このモードを使用する必要があります。

スタティック マッピングは次の 2 つのうちいずれかの方法で実装できます。

- ユーザ割り当て : 設定処理中に WWN を指定することで、独自に固有の WWN を指定できます。

- システム割り当て：スイッチが自身のファイバチャネル WWN プールから WWN を提供し、スイッチの設定にマッピングを保持するように要求できます。



ヒント システム割り当てのオプションを使用することをお勧めします。手動で WWN を割り当てる場合は、それが固有の割り当てになるようにする必要があります（詳細については、『Cisco Fabric Manager Fabric Configuration Guide』を参照してください）。すでに割り当てられている WWN は使用しないでください。

Device Manager を使用して iSCSI イニシエータのスタティック マッピングを設定する手順は、次のとおりです。

- ステップ 1** [IP] > [iSCSI] を選択します。
iSCSI 設定が表示されます（図 4-12 を参照）。[Initiators] タブがデフォルトです。
- ステップ 2** [Create] をクリックして iSCSI イニシエータを作成します。
[Create iSCSI Initiators] ダイアログボックスが表示されます（図 4-20 を参照）。

図 4-20 [Create iSCSI Initiators] ダイアログボックス

- ステップ 3** iSCSI ノード名または IP アドレス、および VSAN メンバシップを設定します。
- ステップ 4** [Node WWN Mapping] セクションの [Persistent] チェックボックスをオンにします。
- ステップ 5** スイッチで nWWN を割り当てるようにする場合は [System Assigned] チェックボックスをオンにし、それ以外の場合は、このチェックボックスをオフのままにして [Static WWN] フィールドを設定します。

- ステップ 6** pWWN を iSCSI イニシエータにスタティック マッピングする場合は、[Port WWN Mapping] セクションの [Persistent] チェックボックスをオンにします。
- ステップ 7** [Persistent] をオンにした場合、スイッチで pWWN を割り当てるようにするときは、[System Assigned] チェックボックスをオンにして、この iSCSI イニシエータ用に予約する pWWN の数を設定します。または、このチェックボックスをオフのままにして、この iSCSI イニシエータ用に 1 つ以上の pWWN を設定することもできます。
- ステップ 8** (任意) 認証をイネーブルにする場合は [AuthUser] フィールドを設定します。「[iSCSI セッション認証 \(P.4-30\)](#)」も参照してください。
- ステップ 9** [Create] をクリックして、この iSCSI イニシエータを作成します。



(注)

システム割り当てのオプションを使用して iSCSI イニシエータに WWN を設定する場合、その設定を ASCII ファイルに保存すると、システム割り当てされた WWN も保存されます。以降、write erase を実行した場合は、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。これを行わないと、ASCII 設定ファイルがスイッチ上で再適用されたときに、WWN 割り当てが重複する可能性があります。

ダイナミック iSCSI イニシエータの WWN マッピングをスタティックにする

ダイナミック iSCSI イニシエータがログインした後、このイニシエータで次のログイン時と同じマッピングを使用できるように、自動的に割り当てられた nWWN/pWWN マッピングを永続的に保持するかどうかを判断できます。

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（「[ダイナミック マッピング \(P.4-19\)](#)」を参照）。



(注)

ダイナミック iSCSI イニシエータをスタティック iSLB イニシエータに変換したり、ダイナミック iSLB イニシエータをスタティック iSCSI イニシエータに変換したりすることはできません。



(注)

イニシエータ作成後にダイナミック pWWN をスタティックにする方法は、Device Manager または Fabric Manager ではなく、CLI による設定だけがサポートされます。Fabric Manager または Device Manager では、このイニシエータを削除してから再作成し、pWWN をスタティックに設定する必要があります。

WWN の競合の確認

システムによってスタティック iSCSI イニシエータに割り当てられた WWN は、アップグレードに失敗したり、システム ソフトウェアをダウングレードしたりすると、予期せずシステムに戻される場合があります。このような場合、その後システムがその WWN を他の（ダイナミックまたはスタティックの）iSCSI イニシエータに割り当てる可能性があるため、競合が発生する場合があります。

このような状況が発生した場合はすぐに、システムに属している WWN を確認し、設定済みの WWN があれば削除することで、この問題に対処できます。

Fabric Manager を使用して自動的に割り当てられた nWWN マッピングを永続的に保持する手順は、次のとおりです。

- ステップ 1** [Physical Attributes] ペインで [End Devices] > [iSCSI] を選択します。
[Information] ペインに iSCSI テーブルが表示されます（[図 4-5](#) を参照）。

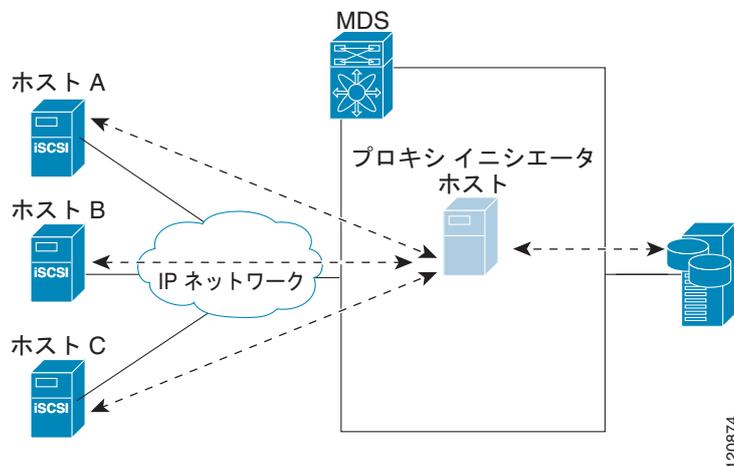
- ステップ 2** [Initiators] タブをクリックします。
設定されている iSCSI イニシエータが表示されます。
- ステップ 3** スタティックにする iSCSI イニシエータの [Persistent Node WWN] チェックボックスをオンにします。
- ステップ 4** [Apply Changes] アイコンをクリックして、これらの変更を保存します。

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すべてのホストに対して明示的な LUN アクセスコントロールを必要とする場合に、トランスペアレントイニシエータモード（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示すモード）を使用することは、すべての iSCSI ホストをスタティックに設定しなければならないことを意味します。つまり、iSCSI ホストごとにいくつかの設定作業が発生することになります。この場合は、プロキシイニシエータモードを使用すると、設定を簡易化できます。

このモードでは、IPS ポート単位に仮想ホスト N ポート（HBA ポート）が1つだけ作成されます。この IPS ポートに接続しているすべての iSCSI ホストは、同一の仮想ホスト N ポートを使用して多重化されます（図 4-21 を参照）。このモードは、WWN を静的にバインディングする作業を簡易化します。この IPS ポートを介して接続する各 iSCSI イニシエータが使用するすべての LUN に対して、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での 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。その後、LUN マッピングおよび iSCSI アクセスコントロール（「iSCSI アクセスコントロール」(P.4-26) を参照）を設定した iSCSI 仮想ターゲット（「スタティックマッピング」(P.4-12) を参照）を設定することで、LUN が各 iSCSI イニシエータに割り当てられます。

図 4-21 IPS ポートの多重化



プロキシイニシエータモードは IPS ポート単位に設定できます。この場合、これを設定した IPS ポートで終端する iSCSI イニシエータだけがこのモードになります。

プロキシイニシエータモードで IPS ポートを作成すると、その 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）が実行されます。FLOGI の完了後、プロキシイニシエータの仮想 N ポートがファイバチャネルファブリックでオンラインになり、ファイバチャネルネームサーバに仮想 N ポートが登録されます。IPS 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。

- 「iSCSI インターフェイス名 iSCSI スロット/ポート」がネームサーバの symbolic-node-name フィールドに登録されます。

- ネーム サーバの FC-4 type フィールドに SCSI_FCP
- ネーム サーバの FC-4 機能のイニシエータ フラグ
- FC-4 type フィールドにベンダー固有のフラグ (iscsi-gw)、(ネーム サーバで N ポート デバイスを iSCSI ゲートウェイ デバイスとして識別するため)

トランスペアレント イニシエータ モードと同様に、ユーザが pWWN および nWWN を指定したり、プロキシ イニシエータ N ポートに対してシステム割り当てされた WWN を要求したりすることもできます。



注意

iSLB VRRP グループに属している iSCSI インターフェイスのプロキシ イニシエータ モードをイネーブルにすると、そのインターフェイスのロード バランシングに影響します。「[iSCSI インターフェイス パラメータの変更とロード バランシングに対するその影響](#)」(P.4-48) を参照してください。

Fabric Manager を使用してプロキシ イニシエータを設定する手順は、次のとおりです。

ステップ 1 [Switches] を展開し、[Interfaces] を展開して [Physical Attributes] ペインの [FC Logical] を選択します。

[Information] ペインにインターフェイス テーブルが表示されます (図 4-22 を参照)。

図 4-22 FC 論理インターフェイス テーブル

Switch	Interface	Mode Admin	Mode Oper	Port VSAN	Dynamic VSAN	Description	Speed Admin	Speed Oper	Rate Mode	Status Service	Status Admin	Status Oper	FailureCause	Was Enabled	LastC
sw172-22-46-220	fc2	auto	E	1	n/a		auto	1 Gb	shared	in	up	up	none	true	2007/11/16 18:59
sw172-22-46-221	channel1	E	TE	1	n/a	To sw172-22-46-220	auto	2 Gb	shared	in	up	up	none	false	2007/11/16 18:59
sw172-22-47-50	channel1	E	TE	1	n/a	To sw172-22-46-174	auto	10 Gb	shared	in	up	up	none	false	2007/11/16 18:59
sw172-22-47-133	channel1	E	TE	1	n/a	To sw172-22-47-132	auto	8 Gb	shared	in	up	up	none	false	2007/11/16 18:59
sw172-22-46-223	channel2	E	TE	1	n/a	To sw172-22-46-220	auto	1 Gb	shared	in	up	up	trunkNotFullyActive	false	2007/11/16 18:59
sw172-22-46-223	fc6	auto	E	1	n/a		auto	1 Gb	shared	in	up	up	none	true	2007/11/16 18:59
sw172-22-46-223	channel1	E	TE	1	n/a	To sw172-22-46-220	auto	2 Gb	shared	in	up	up	trunkNotFullyActive	false	2007/11/16 18:59
sw172-22-47-132	channel1	E	TE	1	n/a	To sw172-22-47-133	auto	8 Gb	shared	in	up	up	trunkNotFullyActive	false	2007/11/16 18:59
sw172-22-46-220	channel4	E	TE	1	n/a	To sw172-22-46-221	auto	2 Gb	shared	in	up	up	trunkNotFullyActive	false	2007/11/16 18:59

ステップ 2 Device Manager で [Interface] > [Ethernet and iSCSI] を選択します。

[Ethernet Interfaces and iSCSI] ダイアログボックスが表示されます (図 4-23 を参照)。

図 4-23 [Ethernet Interfaces and iSCSI] ダイアログボックス

Interface	Description	Mtu	Oper	PhysAddress	Admin	Oper	LastChange	Connector Present	CDP	IscsiAuthMethod	iSNS ProfileName	Promiscuous Mode	Auto Negotiate	Beacon Mode
gigE/1		2300	n/a	00:05:30:01:80:3e	up	down	2007/05/25-12:48:25	False	<input checked="" type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
gigE/2		2300	1 Gb	00:05:30:01:80:3f	up	up	2007/05/24-01:17:48	true	<input checked="" type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
gigE/1		1500	1 Gb	00:05:30:00:a1:9a	up	up	2007/06/07-08:18:59	true	<input checked="" type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
gigE/2		1500	1 Gb	00:05:30:00:a1:9b	up	up	2007/06/07-08:18:59	true	<input checked="" type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
gigE/3		2300	1 Gb	00:05:30:00:a1:9c	up	up	2007/06/07-08:18:59	true	<input checked="" type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
gigE/4		1500	1 Gb	00:05:30:00:a1:9d	up	up	2007/06/07-08:18:59	true	<input checked="" type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
gigE/5		2300	1 Gb	00:05:30:00:a1:9e	up	up	2007/05/16-15:03:58	true	<input checked="" type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
gigE/6		2300	1 Gb	00:05:30:00:a1:9f	up	up	2007/05/16-15:03:58	true	<input checked="" type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
gigE/7		1500	1 Gb	00:05:30:00:a1:a0	up	up	2007/05/16-15:03:58	true	<input checked="" type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
gigE/8		1500	1 Gb	00:05:30:00:a1:a1	up	up	2007/05/16-15:03:58	true	<input checked="" type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

- ステップ 3** FM または DM で [iSCSI] タブをクリックします。
iSCSI インターフェイス設定テーブルが表示されます (図 4-24 を参照)。

図 4-24 Device Manager の [iSCSI] タブ

Interface	Description	Oper	PhysAddress	Admin	Oper	LastChange	PortVSAN	ForwardingMode	Initiator ID-Mode	Proxy Mode Enable	Assignment	Port WWN	Node WWN
iscsi1		Up	21:cd:00:05:30:00:34:9e	down	down	Up	1	storeAndForward	name	<input type="checkbox"/>	Manual	21:00:00:00:00:00:00:00	21:00:00:00:00:00:00:00
iscsi2	1 Gb	Up	21:cd:00:05:30:00:34:9e	up	up	2007/05/24 01:17:48	1	storeAndForward	name	<input type="checkbox"/>	Manual	21:00:00:00:00:00:00:00	21:00:00:00:00:00:00:00
iscsi3		Up	22:01:00:05:30:00:34:9e	down	down	Up	1	storeAndForward	name	<input type="checkbox"/>	Manual	22:00:00:00:00:00:00:00	22:00:00:00:00:00:00:00
iscsi4		Up	22:05:00:05:30:00:34:9e	down	down	Up	1	storeAndForward	name	<input type="checkbox"/>	Manual	22:00:00:00:00:00:00:00	22:00:00:00:00:00:00:00
iscsi5		Up	22:09:00:05:30:00:34:9e	down	down	Up	1	storeAndForward	name	<input type="checkbox"/>	Manual	22:00:00:00:00:00:00:00	22:00:00:00:00:00:00:00
iscsi6		Up	22:0a:00:05:30:00:34:9e	down	down	Up	1	storeAndForward	name	<input type="checkbox"/>	Manual	22:00:00:00:00:00:00:00	22:00:00:00:00:00:00:00
iscsi7		Up	22:11:00:05:30:00:34:9e	down	down	Up	1	storeAndForward	name	<input type="checkbox"/>	Manual	22:00:00:00:00:00:00:00	22:00:00:00:00:00:00:00
iscsi8	1 Gb	Up	22:19:00:05:30:00:34:9e	up	up	2007/05/16-15:03:59	1	storeAndForward	name	<input type="checkbox"/>	Manual	22:00:00:00:00:00:00:00	22:00:00:00:00:00:00:00
iscsi9		Up	22:1a:00:05:30:00:34:9e	down	down	Up	1	storeAndForward	name	<input type="checkbox"/>	Manual	22:00:00:00:00:00:00:00	22:00:00:00:00:00:00:00

- ステップ 4** [Proxy Mode Enable] チェックボックスをオンにします。
ステップ 5 Fabric Manager の [Apply Changes] アイコンをクリックするか、Device Manager の [Apply] をクリックして、これらの変更を保存します。



(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 ポート属性である、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) だけを設定できます。IP アドレスや iSCSI イニシエータの 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 ベースのアクセス コントロールを使用します (「iSCSI アクセス コントロール」(P.4-26) を参照)。

iSCSI の VSAN メンバシップ

ファイバチャネル デバイスと同様に、iSCSI デバイスには、VSAN メンバシップを定義できる 2 つのメカニズムがあります。

- iSCSI ホスト : iSCSI ホストに対する VSAN メンバシップ (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 メンバシップを継承します)。

iSCSI ホストの VSAN メンバシップ

個々の iSCSI ホストを特定の VSAN に属するように設定できます。指定された VSAN は、iSCSI インターフェイスの VSAN メンバシップを上書きします。

Fabric Manager を使用して iSCSI ホストの VSAN メンバシップを割り当てる手順は、次のとおりです。

- ステップ 1** [Physical Attributes] ペインで [End Devices] > [iSCSI] を選択します。
[Information] ペインに iSCSI テーブルが表示されます (図 4-5 を参照)。

- ステップ 2** [Initiators] タブをクリックします。
設定されている iSCSI イニシエータが表示されます。
- ステップ 3** [VSAN Membership] フィールドを入力して、VSAN を iSCSI ホストに割り当てます。
- ステップ 4** [Apply Changes] アイコンをクリックして、これらの変更を保存します。



(注) 他の VSAN (VSAN 1 以外)、たとえば VSAN 2 にイニシエータを設定すると、そのイニシエータは VSAN 1 から自動的に削除されます。このイニシエータを VSAN 1 にも存在させる場合は、VSAN 1 でイニシエータを明示的に設定する必要があります。

iSCSI インターフェイスの VSAN メンバシップ

ポート VSAN と呼ばれる iSCSI インターフェイスに VSAN メンバシップを設定できます。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 で明示的に設定されていない場合、自動的にこの VSAN のメンバーになります。つまり、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 イニシエータのデフォルト VSAN となります。iSCSI インターフェイスのデフォルト ポート VSAN は VSAN 1 です。



注意 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 バランシングに影響します。「[iSCSI インターフェイス パラメータの変更とロード バランシングに対するその影響](#)」(P.4-48) を参照してください。

Device Manager を使用して iSCSI インターフェイスのデフォルト ポート VSAN を変更する手順は、次のとおりです。

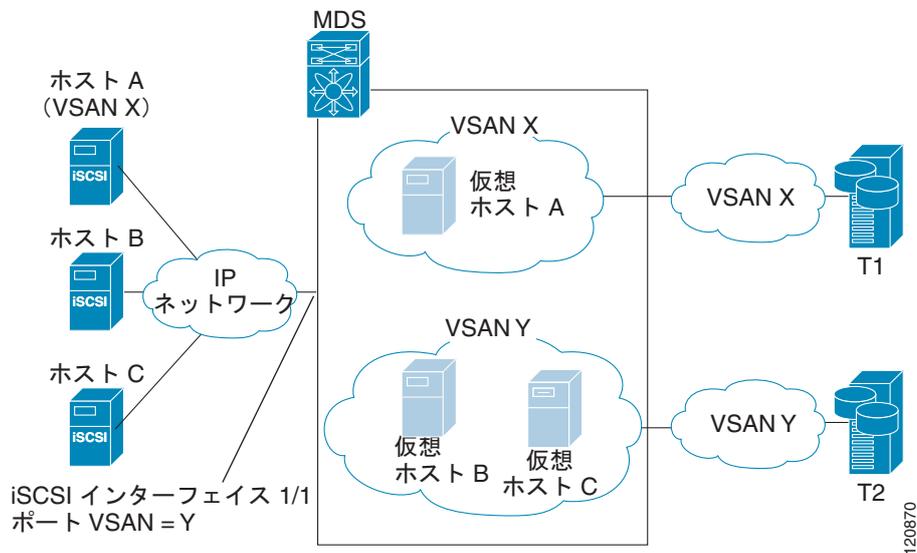
- ステップ 1** [Interface] > [Ethernet and iSCSI] を選択します。
[Ethernet Interfaces and iSCSI] ダイアログボックスが表示されます (図 4-23 を参照)。
- ステップ 2** [iSCSI] タブをクリックします。
iSCSI インターフェイス設定テーブルが表示されます (図 4-24 を参照)。
- ステップ 3** [PortVSAN] 列をダブルクリックして、デフォルトのポート VSAN を修正します。
- ステップ 4** [Apply] をクリックして、これらの変更を保存します。

iSCSI デバイスの VSAN メンバシップの例

図 4-25 に、次の iSCSI デバイスの VSAN メンバシップの例を示します。

- iSCSI インターフェイス 1/1 は、VSAN Y のメンバーです。
- iSCSI イニシエータのホスト A は、VSAN X に対する明示的な VSAN メンバシップを持ちます。
- 3 つの iSCSI イニシエータ (ホスト A、ホスト B、およびホスト C) は、iSCSI インターフェイス 1/1 に接続します。

図 4-25 iSCSI インターフェイスの VSAN メンバシップ



ホスト A の仮想ファイバ チャンネル N ポートは、イニシエータの明示的なメンバシップを持つため、VSAN X に追加されます。仮想ホスト B と C の N ポートは、明示的なメンバシップ設定を持たないため、iSCSI インターフェイスの VSAN メンバシップを継承して、VSAN Y に所属します。

iSCSI ホストの詳細な VSAN メンバシップ

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 チャンネル ホストが複数作成されます。この設定は、ファイバ チャンネル テープ デバイスなど、特定のリソースを異なる VSAN 間で共有する必要がある場合に便利です。

iSCSI アクセス コントロール

iSCSI デバイスに使用できるアクセス コントロールには、次の 2 つのメカニズムがあります。

- ファイバ チャンネル ゾーン分割ベースのアクセス コントロール
- iSCSI ACL ベースのアクセス コントロール

ファイバ チャンネル ファブリック内で iSCSI ホストを示すために使用されるイニシエータ モードに応じて、いずれかのアクセス コントロール メカニズムを使用することも、両方のメカニズムを使用することも使用できます。

ここで説明する内容は、次のとおりです。

- 「[ファイバ チャンネル ゾーン分割ベースのアクセス コントロール](#)」 (P.4-27)
- 「[iSCSI ベースのアクセス コントロール](#)」 (P.4-28)
- 「[アクセス コントロールの実行](#)」 (P.4-29)

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 デバイスの標準的なアクセスコントロールメカニズムであり、VSAN のコンテキスト内で適用されます。ファイバチャネルのゾーン分割は、iSCSI デバイスをサポートするように拡張され、この拡張には、SAN 全体で一貫した柔軟なアクセスコントロールメカニズムを得られるというメリットがあります。

ファイバチャネルゾーンのメンバーを識別する共通のメカニズムは、次のとおりです（ファイバチャネルのゾーン分割については、『Cisco Fabric Manager Fabric Configuration Guide』を参照してください）。

- 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。このインターフェイスを介して接続するデバイスはゾーン内に存在します。

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接続されるすべての iSCSI デバイスが自動的に同じゾーン内に存在することになるため、実用的ではない場合があります。

トランスペアレントイニシエータモードでは（「トランスペアレントイニシエータモード」(P.4-17)で説明したように、ファイバチャネル仮想 N ポートが iSCSI ごとに 1 つずつ作成される場合）、iSCSI ホストにスタティック WWN マッピングが設定されていれば、標準のファイバチャネル デバイスの pWWN ベースのゾーン分割メンバシップメカニズムを使用できます。

ゾーン分割メンバ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ました。

- IPv4 アドレス/サブネットマスク
- IPv6 アドレス/プレフィクス長
- 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、この機能により、IP アドレスまたは iSCSI ノード名をゾーンメンバーとして指定できます。スタティック WWN マッピングが設定された iSCSI ホストがこれらの機能も使用できることに留意してください。IP アドレスベースのゾーンメンバシップは、サブネットマスクを指定して 1 つのコマンドで複数のデバイスを指定できません。



(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 デバイスは、単一の仮想ファイバチャネル N ポートを介して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。pWWN に基づくゾーン分割を使用する場合、この IPS ポートに接続するすべての iSCSI デバイスは、同じゾーンに配置されます。プロキシイニシエータモードで個別のイニシエータのアクセスコントロールを実装するには、仮想ターゲット上で iSCSI ACL を設定します（「iSCSI ベースのアクセスコントロール」(P.4-28)を参照）。

Fabric Manager を使用して iSCSI イニシエータをゾーンデータベースに追加する手順は、次のとおりです。

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

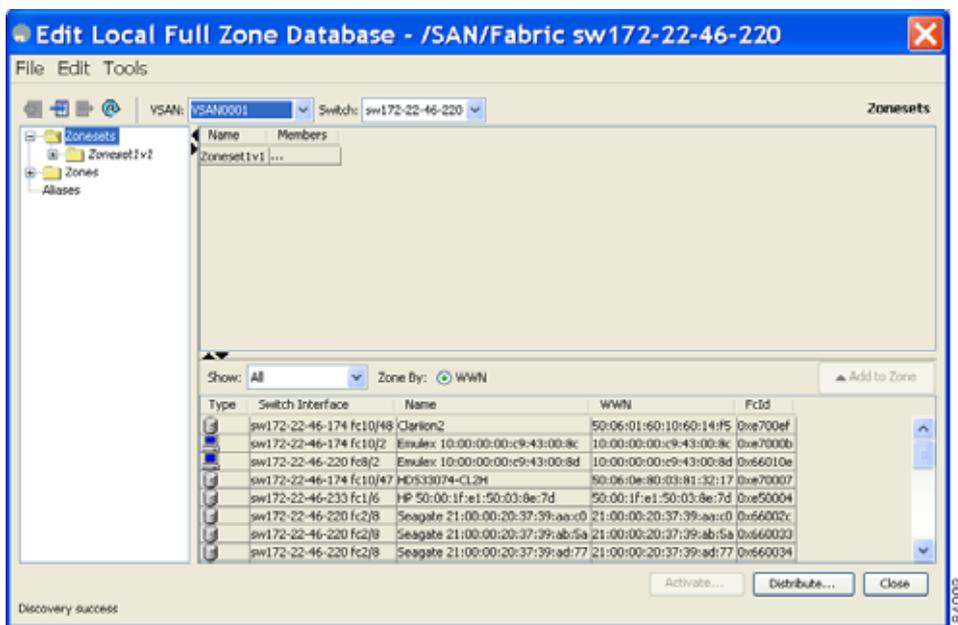
[Edit Local Zone Database] ダイアログボックスが表示されます（図 4-26 を参照）。

図 4-26 Fabric Manager の [Edit Local Zone Database] ダイアログボックス



- ステップ 2** iSCSI ホスト イニシエータを追加する VSAN を選択して [OK] をクリックします。
この VSAN に使用可能なゾーンおよびゾーン セットが表示されます (図 4-27 を参照)。

図 4-27 使用可能なゾーンおよびゾーン セット



- ステップ 3** iSCSI ホスト イニシエータで使用可能なデバイスのリストから、ゾーンに追加するイニシエータをドラッグします。
- ステップ 4** [Distribute] をクリックして変更を配信します。

iSCSI ベースのアクセス コントロール

iSCSI ベースのアクセス コントロールは、スタティック iSCSI 仮想ターゲットを作成する場合にだけ適用できます (「スタティック マッピング」(P4-12) を参照)。スタティック iSCSI ターゲットの場合、そのターゲットにアクセスできる iSCSI イニシエータ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 仮想ターゲットはどの iSCSI ホストにもアクセスできるわけではありません。すべてのホストが iSCSI 仮想ターゲットにアクセスできるようにアクセシビリティを明示的に設定する必要があります。イニシエータ アクセス リストには、1 つ以上のイニシエータを含めることができます。次のいずれかのメカニズムを使用して、iSCSI イニシエータを識別できます。

- iSCSI ノード名

- IPv4 アドレスおよびサブネット
- IPv6 アドレス



(注)

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は、その iSCSI ホストにアクセス可能なすべてのスタティック iSCSI ターゲットに対するイニシエータの仮想 N ポートが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存在する必要があります。

- ステップ 1** [IP] > [iSCSI] を選択します。
iSCSI 設定が表示されます (図 4-12 を参照)。
- ステップ 2** [Targets] タブをクリックします。
iSCSI 仮想ターゲットが表示されます。
- ステップ 3** [Initiators Access All] チェックボックスがオンになっている場合はオフにします。
- ステップ 4** [Edit Access] をクリックします。
[Initiators Access] ダイアログボックスが表示されます。
- ステップ 5** [Create] をクリックして、イニシエータアクセスリストにさらにイニシエータを追加します。
[Create Initiators Access] ダイアログボックスが表示されます。
- ステップ 6** この仮想ターゲットに許可するイニシエータの名前または IP アドレスを追加します。
- ステップ 7** [Create] をクリックして、イニシエータアクセスリストにこのイニシエータを追加します。

アクセスコントロールの実行

IPS モジュールおよび MPS-14/2 モジュールは、iSCSI ベースと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 検出フェーズと iSCSI セッション作成フェーズの両方で実行されます。IPS モジュールも MPS-14/2 モジュールも iSCSI トラフィックのファイバチャネルへのルーティングに関与していないため、I/O フェーズではアクセスコントロールを実行する必要はありません。

- 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 ターゲットを問い合わせると、IPS モジュールまたは MPS-14/2 モジュールは、前述したアクセスコントロールポリシーに基づいてこの iSCSI ホストがアクセスできる iSCSI ターゲットのリストだけを返します。IPS モジュールまたは MPS-14/2 モジュールは、すべての VSAN でイニシエータと同じゾーンにあるすべてのデバイスについて、ファイバチャネルネームサーバに問い合わせることで、これを実行します。次に、FCNS エントリの FC4-feature フィールドを検索して、イニシエータになっているデバイスをフィルタします (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 モジュールまたは MPS-14/2 モジュールはそれをアドバタイズします)。その後、iSCSI ホストにターゲットのリストを返します。それぞれのターゲットには、ユーザが設定するスタティック iSCSI ターゲット名、あるいは IPS モジュールまたは MPS-14/2 モジュールがそのターゲット用に作成するダイナミック iSCSI ターゲット名のいずれかが付けられています (「ダイナミックマッピング」(P.4-10) を参照)。

- iSCSI セッション作成 : IP ホストが iSCSI セッションを開始すると、IPS モジュールまたは MPS-14/2 モジュールは、(セッション ログイン要求で) 指定された iSCSI ターゲットが、「iSCSI ベースのアクセス コントロール」(P.4-28) で説明したアクセス コントロールの両方のメカニズムで許可されているかどうかを確認します。

iSCSI ターゲットがスタティック マッピングされたターゲットである場合、IPS モジュールまたは MPS-14/2 モジュールは、iSCSI ホストが iSCSI ターゲットのアクセス リスト内で許可されているかどうかを確認します。IP ホストがアクセスできない場合、そのログインは拒否されます。iSCSI ホストが許可されている場合、iSCSI ホストで使用する仮想ファイバ チャンネル N ポート、およびスタティック iSCSI 仮想ターゲットにマッピングされているファイバ チャンネル ターゲットが同じファイバ チャンネル ゾーンに存在するかどうかを確認します。

iSCSI ターゲットが自動生成された iSCSI ターゲットである場合、IPS モジュールまたは MPS-14/2 モジュールは、ファイバ チャンネル ターゲットの WWN を iSCSI ターゲット名から抽出し、イニシエータとファイバ チャンネル ターゲットが同じファイバ チャンネル ゾーンに存在するかどうかを確認します。同じゾーンに存在している場合、アクセスが許可されます。

IPS モジュールまたは MPS-14/2 モジュールは、iSCSI ホストのファイバ チャンネル仮想 N ポートを使用して、ネーム サーバにゾーンを制限したファイバ チャンネル ターゲットの WWN を問い合わせます。ネーム サーバから FC ID が返されると、iSCSI セッションが受け入れられます。そうでない場合は、ログイン要求が拒否されます。

iSCSI セッション認証

IPS 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 モジュールまたは MPS-14/2 モジュールは、iSCSI イニシエータの CHAP 認証または None 認証を許可します。認証を常に使用する場合は、CHAP 認証だけを許可するようにスイッチを設定する必要があります。

CHAP ユーザ名または CHAP 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され許可されている方法であれば任意に使用できます (詳細については、『Cisco Fabric Manager Security Configuration Guide』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。

Fabric Manager を使用して iSCSI ユーザの AAA 認証を設定する手順は、次のとおりです。

- ステップ 1** [Physical Attributes] ペインで [Switches] > [Security] > [AAA] を選択します。
[Information] ペインに AAA 設定が表示されます。
- ステップ 2** [Applications] タブをクリックします。
アプリケーションごとに AAA 設定が表示されます (図 4-28 を参照)。

図 4-28 アプリケーション設定ごとの AAA

Switch	Type, SubType, Function	Server Group IdList	Local	Trivial
sw172-22-46-233	default, all, accounting		<input checked="" type="checkbox"/>	<input type="checkbox"/>
sw172-22-46-220	default, all, accounting		<input checked="" type="checkbox"/>	<input type="checkbox"/>
sw172-22-46-224	default, all, accounting		<input checked="" type="checkbox"/>	<input type="checkbox"/>
sw172-22-46-223	default, all, accounting		<input checked="" type="checkbox"/>	<input type="checkbox"/>
sw172-22-46-182	default, all, accounting		<input checked="" type="checkbox"/>	<input type="checkbox"/>
sw172-22-46-222	default, all, accounting		<input checked="" type="checkbox"/>	<input type="checkbox"/>
sw172-22-46-225	default, all, accounting		<input checked="" type="checkbox"/>	<input type="checkbox"/>
sw172-22-47-20	default, all, accounting		<input checked="" type="checkbox"/>	<input type="checkbox"/>
sw172-22-46-221	default, all, accounting		<input checked="" type="checkbox"/>	<input type="checkbox"/>
sw172-22-47-167	default, all, accounting		<input checked="" type="checkbox"/>	<input type="checkbox"/>
sw172-22-46-224	login, all, authentication		<input checked="" type="checkbox"/>	<input type="checkbox"/>

ステップ 3 iSCSI アプリケーションの [Server Group IdList] フィールドを右クリックして、iSCSI に使用するサーバグループを入力します。



(注) 既存のサーバグループを使用するか、新規サーバグループを作成してから、そのグループを iSCSI セッション認証用に設定する必要があります。

ステップ 4 [Apply Changes] アイコンをクリックして、これらの変更を保存します。

ここで説明する内容は、次のとおりです。

- 「認証メカニズムの設定」(P.4-31)
- 「ローカル認証の設定」(P.4-32)
- 「iSCSI イニシエータ認証の制約」(P.4-32)
- 「相互 CHAP 認証の設定」(P.4-33)
- 「iSCSI RADIUS サーバの設定」(P.4-33)

認証メカニズムの設定

iSCSI の CHAP 認証または None 認証を、グローバル レベルでも各インターフェイス レベルでも設定することができます。

ギガビットイーサネットのインターフェイスまたはサブインターフェイスの認証は、グローバルレベルで設定された認証方法を上書きします。

Fabric Manager を使用して iSCSI ユーザの AAA 認証を設定する手順は、次のとおりです。

ステップ 1 [Physical Attributes] ペインで [End Devices] > [iSCSI] を選択します。
[Information] ペインに iSCSI テーブルが表示されます (図 4-5 を参照)。

ステップ 2 [Globals] タブをクリックします。
iSCSI 認証設定テーブルが表示されます。

ステップ 3 [authMethod] 列から [chap] または [none] を選択します。

ステップ 4 Fabric Manager の [Apply Changes] アイコンをクリックして、これらの変更を保存します。

Fabric Manager を使用して、特定のインターフェイスへの iSCSI セッションに認証メカニズムを設定する手順は、次のとおりです。

ステップ 1 [Physical Attributes] ペインで [Switches] > [Interfaces] > [Gigabit Ethernet] を選択します。
[Information] ペインにギガビットイーサネットの設定が表示されます。

ステップ 2 [iSNS] タブをクリックします。
iSCSI および iSNS の設定が表示されます (図 4-29 を参照)。

図 4-29 インターフェイス上での iSCSI 認証の設定

Switch	Interface	IscsiAuthMethod	iSCSI ProfileName	IscsiSessions
sw172-22-46-220	gigE8/1			0
sw172-22-46-223	gigE2/1			0
sw172-22-46-233	gigE1/1			0
sw172-22-46-220	gigE8/2			0
sw172-22-46-223	gigE2/2			0
sw172-22-46-233	gigE1/2			0
sw172-22-46-220	gigE9/1			0
sw172-22-46-174	gigE12/1			0
sw172-22-46-220	gigE9/2			0

ステップ 3 [IscsiAuthMethod] フィールドを右クリックして、[none] または [chap] を選択します。

ステップ 4 [Apply Changes] アイコンをクリックして、これらの変更を保存します。

ローカル認証の設定

『Cisco Fabric Manager Security Configuration Guide』を参照して、ローカルパスワードデータベースを作成します。iSCSI イニシエータのローカルパスワードデータベースにユーザを作成するには、iSCSI キーワードが必須です。

Device Manager を使用してローカル認証の iSCSI ユーザを設定する手順は、次のとおりです。

ステップ 1 [Security] > [iSCSI] を選択します。

[iSCSI Security] ダイアログボックスが表示されます (図 4-30 を参照)。

図 4-30 [iSCSI Security] ダイアログボックス

ステップ 2 [iSCSI User]、[Password]、および [Password Confirmation] の各フィールドを入力します。

ステップ 3 [Create] をクリックして、この新しいユーザを保存します。

iSCSI イニシエータ認証の制約

デフォルトでは、iSCSI イニシエータは、IPS モジュールまたは MPS-14/2 モジュールに対して自身を認証する際に、RADIUS サーバまたはローカルデータベースの任意のユーザ名を使用できません (CHAP ユーザ名は、iSCSI イニシエータ名とは関係ありません)。IPS 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る CHAP 認証確認に正しい応答を返している間は、イニシエータのログインを許可します。これは、CHAP ユーザ名およびパスワードが 1 つでも侵害されると問題に発展する可能性があります。

Fabric Manager を使用してイニシエータが CHAP 認証に特定のユーザ名を使用するように制限する手順は、次のとおりです。

-
- ステップ 1** [Physical Attributes] ペインで [End Devices] > [iSCSI] を選択します。
[Information] ペインに iSCSI テーブルが表示されます (図 4-5 を参照)。
- ステップ 2** [AuthUser] フィールドを右クリックして、iSCSI イニシエータに限定するユーザ名を入力します。
- ステップ 3** [Apply Changes] アイコンをクリックして、これらの変更を保存します。
-

相互 CHAP 認証の設定

iSCSI イニシエータの IPS モジュールまたは MPS-14/2 モジュールの認証の他にも、IPS モジュールまたは MPS-14/2 モジュールは、iSCSI のログインフェーズで Cisco MDS スイッチの iSCSI ターゲットを iSCSI イニシエータが認証するメカニズムをサポートします。この認証では、iSCSI イニシエータに対して示すスイッチのユーザ名とパスワードをユーザが設定する必要があります。指定されたパスワードを使用して、イニシエータが IPS ポートに送信する CHAP 認証確認に対する CHAP 応答を計算します。

Fabric Manager を使用して、イニシエータに対するスイッチの認証のために、そのスイッチで使用するグローバル iSCSI ターゲットのユーザ名とパスワードを設定する手順は、次のとおりです。

-
- ステップ 1** [Physical Attributes] ペインで [End Devices] > [iSCSI] を選択します。
[Information] ペインに iSCSI テーブルが表示されます (図 4-5 を参照)。
- ステップ 2** [Globals] タブを選択します。
グローバル iSCSI 設定が表示されます。
- ステップ 3** [Target UserName] フィールドと [Target Password] フィールドに入力します。
- ステップ 4** [Apply Changes] アイコンをクリックして、これらの変更を保存します。
-

Device Manager を使用して、イニシエータに対するスイッチの認証のために、そのスイッチで使用するイニシエータごとの iSCSI ターゲットのユーザ名とパスワードを設定する手順は、次のとおりです。

-
- ステップ 1** [IP] > [iSCSI] を選択します。
iSCSI 設定が表示されます (図 4-12 を参照)。
- ステップ 2** 設定するイニシエータの [Target UserName] フィールドと [Target Password] フィールドを入力します。
- ステップ 3** [Create] をクリックして、イニシエータ アクセス リストにこのイニシエータを追加します。
-

iSCSI RADIUS サーバの設定

iSCSI RADIUS サーバを設定する手順は、次のとおりです。

-
- ステップ 1** Cisco MDS スイッチの管理イーサネット IP アドレスからのアクセスを許可するように RADIUS サーバを設定します。
- ステップ 2** Cisco MDS スイッチを認証する RADIUS サーバの共有秘密を設定します。
- ステップ 3** RADIUS サーバで iSCSI ユーザとパスワードを設定します。
-

iSCSI の即時データ機能と非請求データ機能

Cisco MDS スイッチは、ログイン ネゴシエーション フェーズにイニシエータによって要求された場合、iSCSI の即時データ機能と非請求データ機能をサポートします。即時データは、書き込みコマンドと書き込みデータを 1 つの Protocol Data Unit (PDU; プロトコル データ ユニット) にまとめるなど、iSCSI コマンドの PDU のデータ部分に含まれる iSCSI 書き込みデータのことで、非請求データは、イニシエータがターゲットからの明示的な Ready to Transfer (R2T) PDU の受信を必要とせず、MDS スイッチなどの iSCSI ターゲットに iSCSI データ出力 PDU で送信する iSCSI 書き込みデータのことで

す。これら 2 つの機能により、R2T PDU のイニシエータとターゲット間の 1 往復がなくなるため、小さい書き込みコマンドの I/O 時間を短縮できるようになります。iSCSI ターゲットの場合、MDS スイッチは、コマンドあたり最大 64 KB の非請求データを許可します。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 イニシエータが即時データ機能と非請求データ機能をサポートする場合、これらの機能は、MDS スイッチ上で設定の必要なく自動的にイネーブルになります。

iSCSI インターフェイスの詳細機能

IPS ポートごとに iSCSI インターフェイスの詳細設定オプションを使用できます。これらの設定については、詳細な FCIP 設定と同様で、この該当セクションですでに説明されています。

Cisco MDS スイッチは、iSCSI インターフェイスの次の詳細機能をサポートします。

- 「iSCSI リスナー ポート」(P.4-34)
- 「TCP 調整パラメータ」(P.4-34)
- 「QoS 値の設定」(P.4-35)
- 「iSCSI ルーティング モード」(P.4-35)

iSCSI リスナー ポート

新規 TCP 接続をリッスンする 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すぐに、iSCSI ポートは、新しく設定されたポート上の TCP 接続だけを受け入れます。

TCP 調整パラメータ

設定できる TCP パラメータは次のとおりです。

- 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](#)」(P.2-18) を参照してください)。
- 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](#)」(P.2-18) を参照してください)。
- 最大再送信回数 (詳細については、「[最大再送信数](#)」(P.2-19) を参照してください)。
- Path MTU (詳細については、「[Path MTU](#)」(P.2-19) を参照してください)。
- 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](#)」(P.2-19) を参照してください)。

- 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、「[バッファ サイズ](#)」(P.2-20) を参照してください)。
- ウィンドウ輻輳監視 (デフォルトでイネーブルで、デフォルトバースト サイズは 50 KB)、(詳細については、「[輻輳の監視](#)」(P.2-19) 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)。

QoS 値の設定

Fabric Manager を使用して QoS 値を設定する手順は、次のとおりです。

-
- ステップ 1** [Switches] を展開し、[Interfaces] を展開して [Physical Attributes] ペインの [FC Logical] を選択します。
[Information] ペインにインターフェイス テーブルが表示されます (図 4-22 を参照)。
 - ステップ 2** Device Manager で [Interface] > [Ethernet and iSCSI] を選択します。
[Ethernet Interfaces and iSCSI] ダイアログボックスが表示されます (図 4-23 を参照)。
 - ステップ 3** Fabric Manager または Device Manager のいずれかで、[iSCSI TCP] タブをクリックします。
iSCSI TCP 設定テーブルが表示されます。
 - ステップ 4** [QoS] フィールドを 1 ~ 6 の範囲で設定します。
 - ステップ 5** Fabric Manager の [Apply Changes] アイコンをクリックするか、Device Manager の [Apply] をクリックして、これらの変更を保存します。
-

iSCSI ルーティング モード

Cisco MDS 9000 ファミリのスイッチは、複数の iSCSI ルーティング モードをサポートします。各モードは、さまざまな運用パラメータが調整され、異なるメリットとデメリットを持ちながら、さまざまな使用状況に合わせるすることができます。

- パススルー モード

パススルー モードでは、IPS モジュールまたは MPS 14/2 モジュール上のポートがファイバ チャネル ターゲットからの読み取りデータ フレームを変換して、iSCSI ホストにバッファリングせずにフレーム単位で転送します。これは、データ入力フレームを 1 回受信するとすぐに、iSCSI データ入力 PDU として 1 回送信することを指します。

これと反対の方向では、IPS モジュールまたは MPS 14/2 モジュール上のポートは、iSCSI ホストが送信できる iSCSI 書き込みデータ出力 PDU の最大サイズを、ファイバ チャネル ターゲットで受信可能なサイズとして規定された最大データ サイズに制限します。この結果、iSCSI データ出力 PDU を 1 回受信すると、ファイバ チャネル ターゲットにファイバ チャネル データ フレームが 1 回送信されることとなります。

両方向でのバッファリングを行わないため、転送遅延を小さくするメリットにつながります。ただし、最大データ セグメント長が小さいと、通常は、ホストシステムで処理オーバーヘッドが増加するため、ホストからのデータ転送パフォーマンスが低下します。このモードの別の利点は、iSCSI データ ダイジェストをイネーブルにできることです。これにより、PDU で運ばれる iSCSI データの完全性の保護は、TCP チェックサムで提供される以上に優れたものになります。

- 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 モジュールまたは MPS 14/2 モジュール上のポートが交換のためのすべてのファイバ チャンネル データ フレームをアセンブルして、1 つの大きい iSCSI データ入力 PDU に組み立ててから iSCSI クライアントに転送します。

これと反対の方向では、IPS モジュールまたは MPS 14/2 モジュール上のポートが小さいデータ セグメント サイズをホストに強制しないため、iSCSI ホストは任意のサイズ (最大 256 KB) の iSCSI データ出力 PDU を送信できます。次に、ポートは、PDU を変換または分割してファイバ チャンネル フレームをファイバ チャンネル ターゲットに転送する前に、iSCSI データ出力 PDU を受信するまで待機します。

このモードのメリットは、ホストからのデータ転送パフォーマンスが高くなることです。デメリットは、転送遅延が大きくなり、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、デフォルトのフォワーディング モードです。

- カットスルー モード

カットスルー モードは、ストア アンド フォワード モードよりも読み取り動作のパフォーマンスが向上します。IPS モジュールまたは MPS 14/2 モジュール上のポートは、交換が全部完了するのを待たずに受信している間も各ファイバ チャンネル データ入力フレームを iSCSI ホストに転送することで、これを実現します。書き込みデータ出力動作に、ストア アンド フォワード モードとの違いはありません。

図 4-31 では、iSCSI ルーティング モードで交換されるメッセージを比較しています。

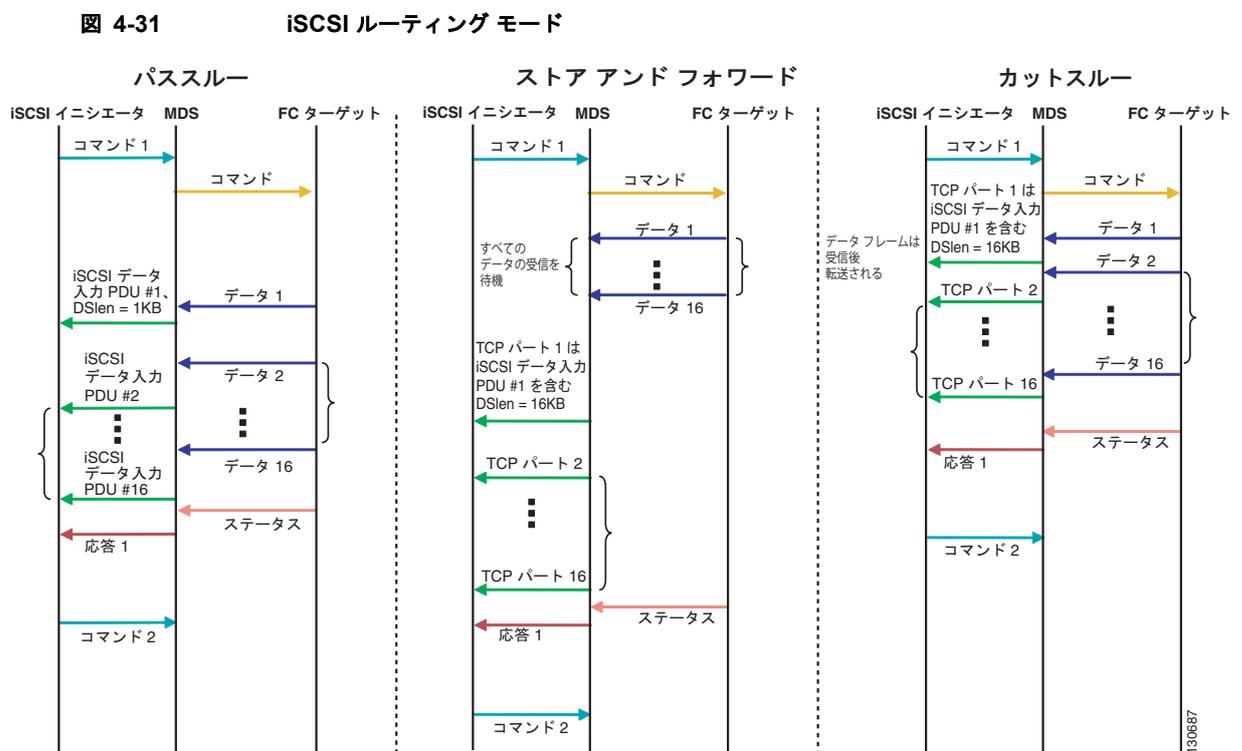


表 4-1 では、iSCSI ルーティング モードの違いによるメリットとデメリットを比較しています。

表 4-1 iSCSI ルーティング モードの比較

モード	メリット	デメリット
パススルー	遅延が小さい データ ダイジェストを使用できる	データ転送パフォーマンスが下がる
ストア アンド フォワード	データ転送パフォーマンスが上がる	データ ダイジェストを使用できない
カットスルー	ストア アンド フォワードよりも読み取りパフォーマンスが向上する	ファイバチャネルターゲットが異なるコマンドで相互に置き換えて使用できるように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 モードで転送されますが、それ以降のコマンドのデータはバッファリングされ、ストア アンド フォワード モードと同じ動作になります。 データ ダイジェストを使用できない



注意

iSLB VRRP グループに属している iSCSI インターフェイスのフォワーディング モードを変更すると、インターフェイスのロード バランシングに影響します。「[iSCSI インターフェイス パラメータの変更とロード バランシングに対するその影響](#)」(P.4-48)を参照してください。

iSLB の設定

iSCSI サーバのロード バランシング (iSLB) 機能は、数百あるいは数千にも上る数のイニシエータを含む大規模な iSCSI の導入を簡単に設定する手段を提供します。iSLB を使用しない場合、iSCSI の設定には次の作業が必要になります。

- 次の手順を含め、MDS スイッチ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 を使用するイニシエータの設定
 - イニシエータおよびターゲットのゾーン分割設定
 - 任意で、仮想ターゲットの作成およびイニシエータへのアクセス権付与
 - MDS スイッチ上のイニシエータ用に作成されたスタティック pWWN に基づいた、イニシエータに対する、ストレージ システム上でのターゲット LUN のマッピングおよびマスキングの設定
- 複数の MDS スイッチ上で手動で設定を複製する必要があります。
- IPS ポートに対するロード バランシングはありません。例：
 - 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されません。
 - 複数の VRRP グループを使用して、区別された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。

- iSLB イニシエータ設定は、イニシエータ ターゲットおよび自動ゾーンのサポートによって簡易化されます。

- Cisco Fabric Service (CFS) により、ファブリック内のすべての MDS スイッチ間で iSLB イニシエータ設定を配信する手動による設定の必要性がなくなります。



(注) スタティック マッピングされた iSLB イニシエータ設定だけが、CFS を使用するファブリック全体で配信されます。ダイナミック マッピングおよびスタティック マッピングされた iSCSI イニシエータ設定は配信されません。

- iSLB イニシエータのダイナミック ロード バランシングは、iSCSI ログイン リダイレクトおよび VRRP を使用して利用できます。

ここでは、次の内容について説明します。

- 「iSLB 設定制限の概要」 (P.4-38)
- 「iSLB 設定の前提条件」 (P.4-39)
- 「iSLB イニシエータの概要」 (P.4-39)
- 「Device Manager を使用した iSLB の設定」 (P.4-39)
- 「iSLB イニシエータの設定」 (P.4-42)
- 「VRRP を使用するロード バランシングの概要」 (P.4-46)
- 「VRRP を使用するロード バランシングの設定」 (P.4-49)
- 「CFS を使用した iSLB 設定配信の概要」 (P.4-49)
- 「CFS を使用した iSLB 設定の配信」 (P.4-50)



(注) iSLB を設定する前に、iSCSI をイネーブルにする必要があります (「iSCSI のイネーブル化」 (P.4-5) を参照)。



(注) iSLB の場合、ファブリック内のすべてのスイッチで Cisco MDS SAN-OS リリース 2.1(1a) 以降を実行する必要があります。

iSLB 設定制限の概要

iSLB 設定には次の制限があります。

- 1 つのファブリック内でサポートされる iSLB イニシエータおよび iSCSI イニシエータの最大数は 2000 です。
- トランスペアレント イニシエータ モードまたはプロキシ イニシエータ モードの IPS ポートでサポートされる iSLB セッションおよび iSCSI セッションの最大数は 500 です。
- 1 つのファブリック内でサポートされる iSLB イニシエータの最大数は、2000 です。
- トランスペアレント イニシエータ モードまたはプロキシ イニシエータ モードの IPS ポートあたりの iSLB セッションの最大数は、500 です。
- CFS 配信がイネーブルに設定された iSLB を備えることができるファブリック内のスイッチの最大数は 4 です。
- 200 を超える新規 iSLB イニシエータを保留設定に追加できません。それ以上のイニシエータを追加する前に、設定を確定する必要があります。

- 実行コンフィギュレーションに 200 を超える iSLB イニシエータを含む場合は、iSCSI をディセーブルにできません。iSLB イニシエータの数を 200 よりも少なくしてから iSCSI をディセーブルにします。
- CFS 配信を設定しなくても iSLB を使用できますが、iSLB 自動ゾーン機能を使用する場合は、いずれかのゾーンセットがアクティブになるとトラフィックが中断されます。
- Inter-VSAN Routing (IVR) および iSLB の機能が同じファブリック内でイネーブルになっている場合、ファブリック内にこれらの機能がどちらもイネーブルになっているスイッチが少なくとも 1 つ必要です。ゾーン分割関連の設定とアクティベーション（通常ゾーン用、IVR ゾーン用、または iSLB ゾーン用）をこのスイッチ上で実行する必要があります。このようにしないと、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。

iSLB 設定の前提条件

iSLB を設定する前に次の前提条件の処理を実行します。

- iSCSI のイネーブル化（詳細については、「[iSCSI のイネーブル化](#)」(P.4-5) を参照してください)。
- ギガビット イーサネット インターフェイスの設定（「[IPv4 の基本的なギガビット イーサネットの設定](#)」(P.7-2) を参照）。
- VRRP グループの設定（「[VRRP を使用するロード バランシングの設定](#)」(P.4-49) を参照）。
- ゾーン セットの設定とアクティブ化（詳細については、『*Cisco Fabric Manager Fabric Configuration Guide*』を参照してください）。
- iSLB の CFS 配信のイネーブル化（「[iSLB 設定配信のイネーブル化](#)」(P.4-51) を参照）。

iSLB イニシエータの概要

iSLB イニシエータには、iSCSI イニシエータでサポートされる機能の他に次の機能があります。

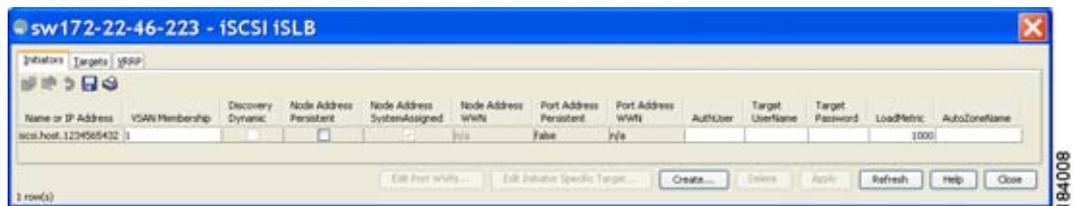
- iSLB イニシエータは、iSLB 仮想ターゲットもサポートします。これらのターゲットは、iSCSI 仮想ターゲットと非常に類似しています。アダプタイズ インターフェイス オプションがない例外はありますが、結果的には CFS を使用して配信できます。
- イニシエータ ターゲット：これらのターゲットを特定のイニシエータに設定します。
- iSCSI ログイン リダイレクトおよび VRRP を使用するロード バランシング：ロード バランシングがイネーブルの場合、IPS Manager は、インターフェイスごとに計算した負荷に基づく最適なインターフェイスへ着信セッションをリダイレクトします。
- CFS を使用した他のスイッチへの配信の設定

Device Manager を使用した iSLB の設定

Device Manager を使用して iSLB を設定する手順は、次のとおりです。

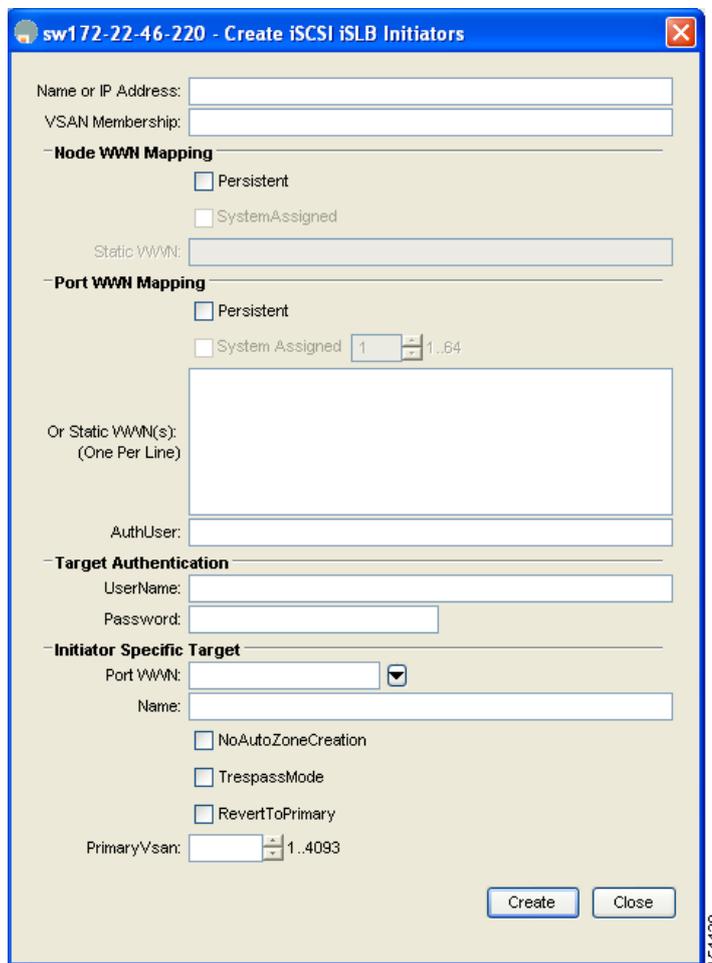
-
- ステップ 1** [IP] > [iSCSI iSLB] を選択します。
[iSCSI iSLB] ダイアログボックスが表示されます（[図 4-32](#) を参照）。

図 4-32 [iSCSI iSLB] ダイアログボックス



- ステップ 2** [Create] をクリックして新しい iSCSI iSLB イニシエータを作成します。
[Create iSCSI iSLB Initiators] ダイアログボックスが表示されます (図 4-33 を参照)。

図 4-33 [Create iSCSI iSLB Initiators] ダイアログボックス



- ステップ 3** [Name or IP Address] フィールドに iSLB 名または IP アドレスを設定します。
ステップ 4 [VSAN Membership] フィールドに iSLB イニシエータを参加させる VSAN を設定します。
「iSLB イニシエータの VSAN メンバシップの割り当て」(P.4-43) も参照してください。

- ステップ 5** iSLB イニシエータのダイナミック nWWN をスタティックに変換する場合は、[Persistent] チェックボックスをオンにします。
「ダイナミック iSLB イニシエータの WWN マッピングをスタティックにする」(P.4-42) も参照してください。
- ステップ 6** (任意) スイッチで nWWN を割り当てるようにする場合は、[SystemAssigned] チェックボックスをオンにします。
- ステップ 7** (任意) 手動でスタティック nWWN を割り当てる場合は [Static WWN] フィールドを設定します。この nWWN に対して固有の割り当てになるようにする必要があります。
- ステップ 8** (任意) iSLB イニシエータのダイナミック pWWN をスタティックに変換する場合は、[Port WWN Mapping] の [Persistent] チェックボックスをオンにします。
「ダイナミック iSLB イニシエータの WWN マッピングをスタティックにする」(P.4-42) を参照してください。
- ステップ 9** (任意) [SystemAssigned] チェックボックスをオンにして、スイッチで割り当てるようにする pWWN の数を設定します。
- ステップ 10** (任意) 手動でスタティック pWWN を割り当てる場合は、[Static WWN(s)] フィールドを設定します。これらの pWWN に対して固有の割り当てになるようにする必要があります。
- ステップ 11** (任意) iSLB 認証用に iSLB イニシエータに限定するユーザ名を設定する場合は、[AuthUser] フィールドを設定します。
「iSLB イニシエータ認証の制約」(P.4-46) も参照してください。
- ステップ 12** iSLB イニシエータ ターゲットの CHAP 認証を設定する場合は、[Username] フィールドと [Password] フィールドを入力します。
「iSLB セッション認証の設定」(P.4-45) も参照してください。
- ステップ 13** [Initiator Specific Target] セクションでは、iSLB イニシエータ ターゲットを設定する pWWN を設定します。
- ステップ 14** (任意) [Name] フィールドにグローバルな固有識別情報 (IQN) を設定します。
- ステップ 15** (任意) 自動ゾーン分割をディセーブルにする場合は、[NoAutoZoneCreation] チェックボックスをオンにします。
「iSLB のイニシエータおよびイニシエータ ターゲットのゾーンの設定とアクティブ化」(P.4-45) も参照してください。
- ステップ 16** (任意) [TresspassMode] チェックボックスをオンにします。
「ストレージ ポート フェールオーバーの LUN trespass」(P.4-56) も参照してください。
- ステップ 17** (任意) HA フェールオーバーの後、プライマリ ポートが再びアップになったときにプライマリ ポートに戻す場合は、[RevertToPrimary] チェックボックスをオンにします。
- ステップ 18** [PrimaryVsan] を iSLB イニシエータ ターゲットの VSAN に設定します。
- ステップ 19** [Create] をクリックして、この iSLB イニシエータを作成します。
- ステップ 20** CFS がイネーブルの場合、[CFS] ドロップダウン メニューから [commit] を選択します。

iSLB イニシエータの設定

ここで説明する内容は、次のとおりです。

- 「[WWN の iSLB イニシエータへの割り当て](#)」 (P.4-42)
- 「[ダイナミック iSLB イニシエータの WWN マッピングをスタティックにする](#)」 (P.4-42)
- 「[iSLB イニシエータの VSAN メンバシップの割り当て](#)」 (P.4-43)
- 「[ロード バランシングのメトリックの設定](#)」 (P.4-43)
- 「[VRRP を使用するロード バランシングの概要](#)」 (P.4-46)
- 「[iSLB のイニシエータおよびイニシエータ ターゲットのゾーンの設定とアクティブ化](#)」 (P.4-45)
- 「[iSLB セッション認証の設定](#)」 (P.4-45)

WWN の iSLB イニシエータへの割り当て

iSLB ホストは、次のメカニズムのいずれかを使用して N ポートの WWN にマッピングされます。

- 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 イニシエータの WWN を割り当てる方法は、iSCSI イニシエータの場合と同様です。ダイナミック マッピング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 の割り当て](#)」 (P.4-19) を参照してください。



ヒント

[SystemAssign] オプションを使用することを推奨します。手動で WWN を割り当てる場合は、それが固有の割り当てになるようにする必要があります (詳細については、『*Cisco Fabric Manager Fabric Configuration Guide*』を参照してください)。すでに割り当てられている WWN は使用しないでください。

「[Device Manager を使用した iSLB の設定](#)」の手順 (P.4-39) を参照してください。

ダイナミック iSLB イニシエータの WWN マッピングをスタティックにする

ダイナミック iSLB イニシエータがログインした後、このイニシエータで次のログイン時に同じマッピングを使用できるように、自動的に割り当てられた nWWN/pWWN マッピングを永続的に保持するかどうかを判断できます («[ダイナミック マッピング](#)」 (P.4-10) を参照)。

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て、その WWN を永続的に使用することができます。



(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 の場合と同様です。「[ダイナミック iSLB イニシエータの WWN マッピングをスタティックにする](#)」 (P.4-42) を参照してください。



(注) スタティック マッピングされた iSLB イニシエータ設定だけが、CFS を使用するファブリック全体で配信されます。動的および静的に設定された iSCSI イニシエータ設定は配信されません。

「[Device Manager を使用した iSLB の設定](#)」の手順 (P.4-39) を参照してください。

iSLB イニシエータの VSAN メンバシップの割り当て

特定の VSAN に参加するように個々の iSLB ホストを設定できます (ファイバチャネルの Dynamic Port VSAN Membership [DPVM] 機能と同様です。詳細については、『Cisco Fabric Manager Fabric Configuration Guide』を参照してください)。指定された VSAN は、iSCSI インターフェイスの VSAN メンバシップを上書きします。



(注) iSLB イニシエータの VSAN を指定する方法は、iSCSI イニシエータの場合と同様です。「[iSCSI の VSAN メンバシップ](#)」(P.4-24) を参照してください。



(注) 他の VSAN (デフォルト VSAN である VSAN 1 以外)、たとえば VSAN 2 に iSLB イニシエータを設定すると、そのイニシエータは VSAN 1 から自動的に削除されます。このイニシエータを VSAN 1 にも存在させる場合は、VSAN 1 でイニシエータを明示的に設定する必要があります。

「[Device Manager を使用した iSLB の設定](#)」の手順 (P.4-39) を参照してください。

ロード バランシングのメトリックの設定

ロード バランシングの重み付けのために、イニシエータごとに負荷メトリックを割り当てることができます。計算された負荷は、特定の iSCSI インターフェイス上にあるイニシエータの数に基づいています。この機能には、さまざまな帯域幅の要求を持つイニシエータに対応します。たとえば、Web サーバよりもデータベース サーバに大きい負荷メトリックを割り当てることができます。重み付けされたロード バランシングもまた、さまざまなリンク速度のイニシエータに対応します。

ロード バランシングの詳細については、「[VRRP を使用するロード バランシングの概要](#)」(P.4-46) を参照してください。

Device Manager で [IP] > [iSCSI iSLB] を選択し、[LoadMetric] フィールドを設定して iSLB イニシエータのロード バランシング メトリックを変更します。

「[Device Manager を使用した iSLB の設定](#)」の手順 (P.4-39) を参照してください。

iSLB イニシエータ ターゲットの設定

デバイス エイリアスまたは pWWN を使用して、イニシエータ ターゲットを設定できます。必要に応じて、次のオプション パラメータを 1 つ以上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
- VSAN ID



(注) 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。

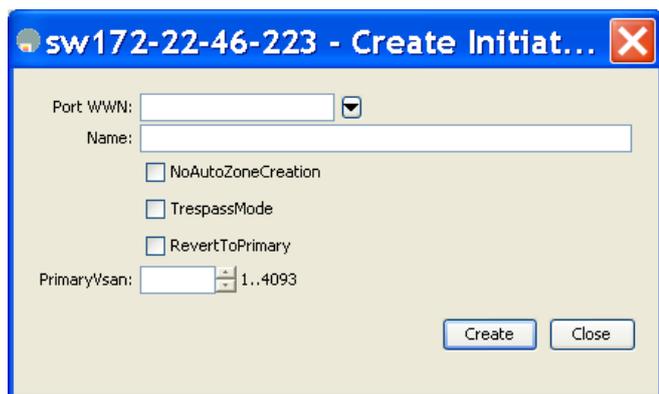
さらに、自動ゾーン分割をディセーブルにすることができます。

イニシエータ ターゲットの IQN を設定した場合、その名前を使用してイニシエータ ターゲットを識別します。設定していない場合は、イニシエータ ターゲットに固有の IQN が生成されます。

Device Manager を使用して追加の iSLB イニシエータ ターゲットを設定する手順は、次のとおりです。

- ステップ 1** [IP] > [iSCSI iSLB] を選択します。
- [iSCSI iSLB] ダイアログボックスが表示されます (図 4-32 を参照)。
- ステップ 2** ターゲットを追加するイニシエータをクリックして、[Edit Initiator Specific Targets] をクリックします。
- [Initiator Specific Target] ダイアログボックスが表示されます。
- ステップ 3** [Create] をクリックして新規イニシエータ ターゲットを作成します。
- [Create Initiator Specific Target] ダイアログボックスが表示されます (図 4-34 を参照)。

図 4-34 [Create Initiator Specific Target] ダイアログボックス



- ステップ 4** [Port WWN] フィールドにイニシエータ ターゲットの pWWN を入力します。
- ステップ 5** (任意) [Name] フィールドにグローバルな固有識別情報 (IQN) を設定します。
- ステップ 6** (任意) 自動ゾーン分割をディセーブルにする場合は、[NoAutoZoneCreation] チェックボックスをオンにします (図 4-33 を参照)。「iSLB のイニシエータおよびイニシエータ ターゲットのゾーンの設定とアクティブ化」(P.4-45) を参照してください。
- ステップ 7** (任意) [TrespassMode] チェックボックスをオンにします。「ストレージ ポート フェールオーバーの LUN trespass」(P.4-56) を参照してください。
- ステップ 8** (任意) HA フェールオーバーの後、プライマリ ポートが再びアップになったときにプライマリ ポートに戻す場合は、[RevertToPrimary] チェックボックスをオンにします。
- ステップ 9** [PrimaryVsan] を iSLB イニシエータ ターゲットの VSAN に設定します。
- ステップ 10** [Create] をクリックして、この iSLB イニシエータ ターゲットを作成します。
- ステップ 11** CFS がイネーブルの場合、[CFS] ドロップダウン メニューから [commit] を選択します。

iSLB のイニシエータおよびイニシエータ ターゲットのゾーンの設定とアクティブ化

iSLB のイニシエータおよびイニシエータ ターゲットの追加時にゾーン名を設定できます。ゾーン名を指定しない場合、IPS Manager によって動的にゾーン名が作成されます。iSLB ゾーン セットには次の考慮事項があります。

- イニシエータ ターゲットが設定されているイニシエータの自動ゾーン分割は、デフォルトでイネーブルです。
- VSAN 内に自動ゾーンを作成する場合は、ゾーン セットがその VSAN 内でアクティブである必要があります。
- 別のゾーン セットのアクティブ化の処理中の場合、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は、iSLB ゾーン セットのアクティブ化に失敗する場合があります。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には、一度に実行するゾーン分割に関する操作（通常ゾーン、IVR ゾーンまたは iSLB ゾーン）はいずれか 1 つだけにします。
- ゾーン セットがアクティブ化されたときに、そのゾーン セット内に 1 つ以上の変更がある場合、自動ゾーンが作成されます。自動ゾーンだけが変更された場合、アクティブ化は無効です。



注意

IVR および iSLB が同じファブリック内でイネーブルになっている場合、ファブリック内で少なくとも 1 つのスイッチで両方の機能がイネーブルになっている必要があります。ゾーン分割関連の設定とアクティベーション操作（通常ゾーン用、IVR ゾーン用、または iSLB ゾーン用）をこのスイッチ上で実行する必要があります。このようにしないと、ファブリック内でトラフィックが中断される可能性があります。

Device Manager で [IP] > [iSCSI iSLB] を選択し、[autoZoneName] フィールドを設定して iSLB イニシエータの自動ゾーン名を変更します。

「[Device Manager を使用した iSLB の設定](#)」の手順 (P.4-39) を参照してください。

iSLB セッション認証の設定

IPS モジュールまたは 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 ホストを認証するための iSLB 認証メカニズムをサポートします。デフォルトでは、IPS モジュールおよび MPS-14/2 モジュールは、iSCSI イニシエータの CHAP 認証または None 認証を許可します。認証を常に使用する場合は、CHAP 認証だけを許可するようにスイッチを設定する必要があります。

CHAP ユーザ名または CHAP 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され許可されている方法であれば任意に使用できます（詳細については、『*Cisco Fabric Manager Security Configuration Guide*』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 セッション認証を指定する方法は、iSCSI の場合と同様です。「[iSCSI セッション認証](#)」(P.4-30) を参照してください。

iSLB イニシエータ認証の制約

デフォルトでは、iSLB イニシエータは、IPS モジュールまたは MPS-14/2 モジュールに対して自身を認証する際に、RADIUS またはローカル AAA データベースの任意のユーザ名を使用できます (CHAP ユーザ名は、iSLB イニシエータ名とは関係ありません)。IPS 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る CHAP 認証確認に正しい応答を返している間は、イニシエータのログインを許可します。これは、CHAP ユーザ名およびパスワードが 1 つでも侵害されると問題に発展する可能性があります。

Device Manager で [IP] > [iSCSI iSLB] を選択し、[AuthName] フィールドを設定してイニシエータが CHAP 認証に特定のユーザ名を使用するように制限します。

「Device Manager を使用した iSLB の設定」の手順 (P.4-39) を参照してください。

相互 CHAP 認証

iSLB イニシエータの IPS モジュールまたは MPS-14/2 モジュールの認証以外にも、IPS モジュールまたは MPS-14/2 モジュールは、iSCSI のログイン フェーズで Cisco MDS スイッチのイニシエータターゲットを iSLB イニシエータが認証するメカニズムをサポートします。この認証では、iSLB イニシエータに対して示すスイッチのユーザ名とパスワードをユーザが設定する必要があります。指定されたパスワードを使用して、イニシエータが IPS ポートに送信する CHAP 認証確認に対する CHAP 応答を計算します。

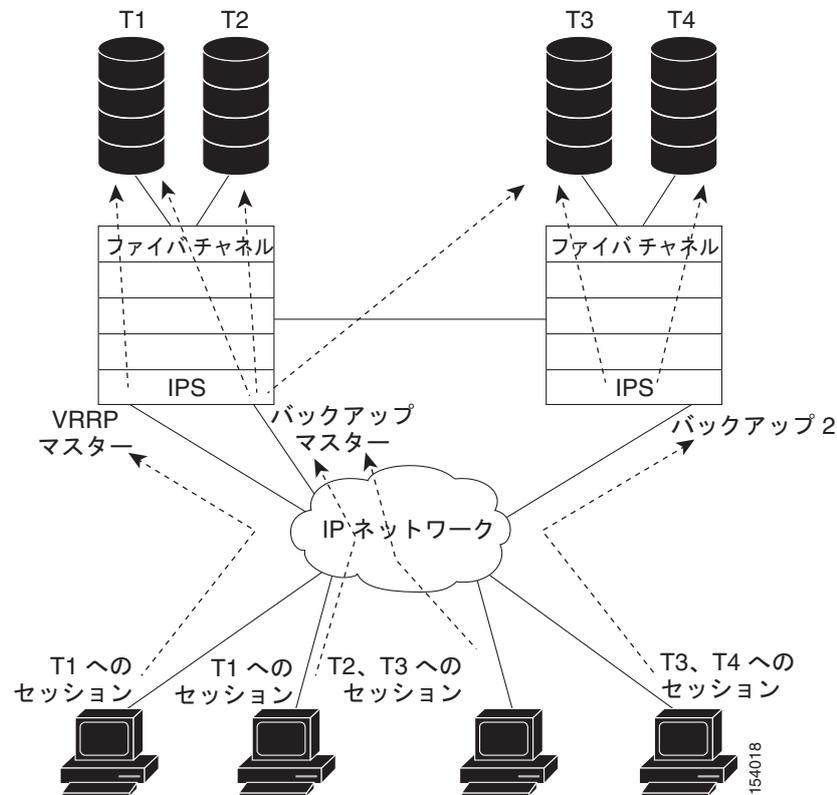
Device Manager で [IP] > [iSCSI iSLB] を選択し、[Target Username] フィールドと [Target Password] フィールドを設定して、イニシエータに対するスイッチの認証のために、そのスイッチで使用するイニシエータごとのユーザ名とパスワードを設定します。

「Device Manager を使用した iSLB の設定」の手順 (P.4-39) を参照してください。

VRRP を使用するロード バランシングの概要

仮想ルータ冗長プロトコル (VRRP) ロード バランシングを iSLB に設定できます。図 4-35 に、iSLB を使用するロード バランシングの例を示します。

図 4-35 iSLB イニシエータのロード バランシングの例



ポータルアドレスとして VRRP アドレスを指定してホストが設定されています。VRRP マスター ポートがイニシエータから最初の iSCSI セッションを受信すると、その特定ホストを提供するバックアップポートを割り当てます。マスターポートに障害が発生した際に復旧が必要な場合、CFS を使用してこの情報がすべてのスイッチに同期されます。イニシエータは、一時的にリダイレクトされた iSCSI ログイン応答を受け取ります。次に、ホストがその物理 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ダウンすると、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 により、バックアップポートがダウンしていることを認識し、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) イーサネット PortChannel が IPS モジュールとイーサネットスイッチ間に設定されている場合、VRRP を設定したロードバランシングを正常に動作させるためには、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は、ポート番号ではなく、送信元および宛先 IP アドレスだけに基いている必要があります。



(注) イニシエータをマスターインターフェースの物理 IP アドレスにリダイレクトすることもできます。

**ヒント**

iSLB VRRP ロード バランシングは、セッション数ではなく、iSLB イニシエータの数に基づいています。他の iSLB イニシエータよりも設定されているターゲットの数が多い（結果としてセッション数の多い）iSLB イニシエータは、より大きい負荷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 イニシエータの負荷メトリックを、デフォルト値の 1000 から 3000 に増やすことができます。

**注意**

リダイレクトされたセッションが VRRP IP アドレスや VRRP グループに関する情報を運ばないため、iSLB に設定されたギガビット イーサネット インターフェイスが所属できる VRRP グループは 1 つだけです。この制約により、スレーブ ポートが属する VRRP グループを一意に識別できます。

iSCSI インターフェイス パラメータの変更とロード バランシングに対するその影響

ロード バランシングがイネーブルにされている VRRP グループのすべての iSCSI インターフェイスは、インターフェイスの VSAN、認証、プロキシ イニシエータ モード、およびフォワーディング モードがすべて同じである必要があります。VRRP グループの iSCSI インターフェイスのこれらのパラメータのうちいずれでも変更が必要な場合は、一度に変更するインターフェイスは 1 つにする必要があります。VRRP グループ内でパラメータを変更したインターフェイスと変更していないインターフェイスが混在する移行期間、マスター ポートは新しいイニシエータをリダイレクトしない代わりにローカルで処理します。

**注意**

VRRP グループ内の iSCSI インターフェイスの VSAN、プロキシ イニシエータ、認証、およびフォワーディング モードを変更すると、セッションが何度もダウン状態になる可能性があります。

ギガビット イーサネット インターフェイス 選択のための VRRP ロード バランシング アルゴリズム

VRRP マスターが iSCSI セッション要求をイニシエータから受信すると、最初にその VRRP グループ内の 1 つのインターフェイスに対して既存のマッピングをチェックします。そのマッピングが存在する場合、VRRP マスターはイニシエータをそのインターフェイスにリダイレクトします。そのマッピングが存在しない場合、VRRP マスターは、最も負荷の小さいインターフェイスを選択し、選択したインターフェイスの負荷をイニシエータの iSLB メトリック（重み）で更新します。

**(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、すべてのセッションに対してマスター インターフェイスが実行するリダイレクト処理のためです。新規イニシエータは、次の式が他のすべてのインターフェイスで真となる場合にだけ、マスター インターフェイスに割り当てられます。

$$\text{VRRP バックアップ インターフェイスの負荷} > [2 * \text{VRRP マスター インターフェイスの負荷} + 1]$$

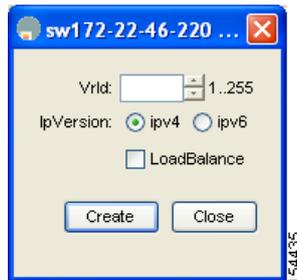
VRRP を使用するロード バランシングの設定

最初に IP ネットワークに接続するスイッチ上のギガビット イーサネット インターフェイスで VRRP を設定してから、iSLB の VRRP を設定する必要があります。ギガビット イーサネット インターフェイス上での VRRP の設定方法については、「[仮想ルータ冗長プロトコル](#)」(P.5-11) を参照してください。

Device Manager を使用して VRRP ロード バランシングを設定する手順は、次のとおりです。

- ステップ 1** [IP] > [iSCSI iSLB] を選択します。
[iSCSI iSLB] ダイアログボックスが表示されます (図 4-32 を参照)。
- ステップ 2** [VRRP] タブをクリックします。
- ステップ 3** [Create] をクリックして iSLB イニシエータの VRRP ロード バランシングを設定します。
[Create iSCSI iSLB VRRP] ダイアログボックスが表示されます (図 4-36 を参照)。

図 4-36 [Create iSCSI iSLB VRRP] ダイアログボックス



- ステップ 4** [Vrid] に VRRP グループ番号を設定します。
- ステップ 5** [ipv4] または [ipv6] を選択して [LoadBalance] チェックボックスをオンにします。
- ステップ 6** [Create] をクリックしてロード バランシングをイネーブルにします。
- ステップ 7** CFS がイネーブルの場合、[CFS] ドロップダウン メニューから [commit] を選択します。

CFS を使用した iSLB 設定配信の概要

MDS スイッチ上の iSLB のイニシエータおよびイニシエータ ターゲットの設定は、Cisco Fabric Service (CFS) を使用して配信できます。この機能により、1 つの MDS スイッチのコンソールからファブリック内で iSLB 設定を同期できます。iSCSI イニシエータの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のパラメータも配信されます。CFS 配信はデフォルトでディセーブルです (詳細については、『*Cisco Fabric Manager System Management Configuration Guide*』を参照してください)。

配信をイネーブルにした後、最初の設定を行ったときに暗黙的なセッションが開始されます。それ以降入力されたすべてのサーバ設定変更は、一時データベースに保管され、そのデータベースが明示的に確定されると、ファブリック内の (発信元スイッチを含む) すべてのスイッチに適用されます。

iSLB で CFS をイネーブルにすると、最初の iSLB 設定操作を行ったときに、CFS セッションが開始され、ファブリック内の iSLB 設定がロックされます。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。そして、各スイッチが設定を確認します。この確認では次の内容が保証されます。

- iSLB イニシエータに割り当てられた VSAN がすべてのスイッチ上で設定されていること。
- iSLB イニシエータに設定されたスタティック WWN が固有であり、すべてのスイッチで使用できること。
- iSLB イニシエータ ノード名がすべてのスイッチ上の iSCSI イニシエータと競合しないこと。

確認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確定します。確認ができないものがある場合は、すべての確定に失敗します。



(注)

iSLB は、CFS がイネーブルの場合にだけサポートされます。CFS モードをイネーブルにせずに iSLB 自動ゾーン分割を使用すると、いずれかのゾーンセットがアクティブになったときにトラフィックが中断する可能性があります。



(注)

CFS は、非 iSLB イニシエータの設定を配信することも、ファイバチャネル ターゲットの設定をインポートすることはありません。

非 iSLB 仮想ターゲットは、アドバタイズ対象インターフェイス オプションを引き続きサポートします。



ヒント

保留中の変更は一時的なディレクトリだけで使用可能であり、スイッチが再起動されると廃棄されま

CFS を使用した iSLB 設定の配信

ここで説明する内容は、次のとおりです。

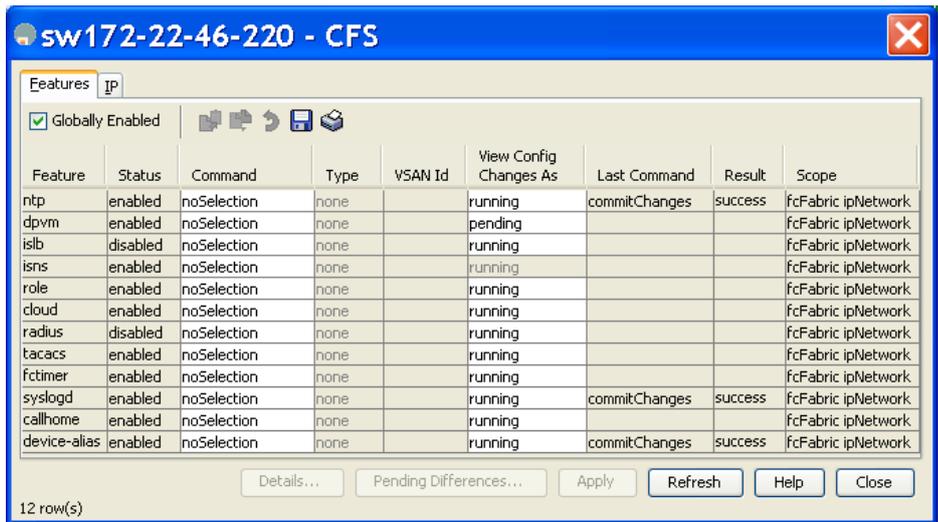
- 「iSLB 設定配信のイネーブル化」(P.4-51)
- 「ファブリックのロック」(P.4-51)
- 「ファブリックに対する変更の確定」(P.4-52)
- 「保留中の変更の廃棄」(P.4-52)
- 「ファブリックのロックの解除」(P.4-52)
- 「CFS マージ プロセス」(P.4-53)
- 「iSLB CFS マージ ステータスの矛盾」(P.4-53)

iSLB 設定配信のイネーブル化

Device Manager を使用して iSLB 設定の CFS 配信をイネーブルにする手順は、次のとおりです。

- ステップ 1** [Admin] > [CFS] を選択します。
[CFS] ダイアログボックスが表示されます (図 4-37 を参照)。

図 4-37 Device Manager の CFS のイネーブル化



- ステップ 2** iSLB 機能の [Command] フィールドを [enable] に設定します。
ステップ 3 [Apply] をクリックして、この変更を保存します。

ファブリックのロック

既存の設定を変更する最初の処理により、保留設定が作成されてファブリックの機能がロックされます。ファブリックがロックされると、次のような状況になります。

- 他のユーザは、この機能の設定を変更できなくなります。
- アクティブな設定をコピーすると、保留設定が作成されます。これ以後の変更は保留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の場合、iSCSI 設定を変更することはできません。

ファブリックに対する変更の確定

保留中の iSLB 設定の変更をアクティブな設定およびファブリック内の他の MDS スイッチに適用するには、変更を確定する必要があります。保留中の設定変更が配信され、正常に確定された時点で、設定変更がファブリック全体の MDS スイッチのアクティブな設定に適用され、自動ゾーンのアクティブ化とファブリックのロック解除が実行されます。

ファブリック内の他の MDS スイッチに iSLB の設定変更を確定するために、Device Manager を使用して、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手順は、次のとおりです。

-
- ステップ 1 [Admin] > [CFS] を選択します。
[CFS Configuration] ダイアログボックスが表示されます (図 4-37 を参照)。
 - ステップ 2 iSLB 機能の [Command] フィールドを [commit] に設定します。
 - ステップ 3 [Apply] をクリックして、この変更を保存します。
-

保留中の変更の廃棄

iSLB 設定に対する保留中の変更をいつでも廃棄し、ファブリックのロックを解除できます。この処理は、ファブリック内のスイッチのアクティブな設定に対しては何の作用もありません。

Device Manager を使用して保留中の iSLB 設定変更を廃棄し、ファブリックのロックを解除する手順は次のとおりです。

-
- ステップ 1 [Admin] > [CFS] を選択します。
[CFS Configuration] ダイアログボックスが表示されます (図 4-37 を参照)。
 - ステップ 2 iSLB 機能の [Command] フィールドを [abort] に設定します。
 - ステップ 3 [Apply] をクリックして、この変更を保存します。
-

ファブリックのロックの解除

iSLB 設定タスクを実行し、変更の確定か廃棄を行ってロックを解除していない場合、管理者はファブリック内のスイッチからロックを解除できます。管理者がこのタスクを実行すると、保留中の変更は廃棄され、ファブリックのロックは解除されます。



ヒント

保留中の変更は一時的なディレクトリだけで使用可能であり、スイッチが再起動されると廃棄されます。

Device Manager を使用してファブリックのロックを解除する手順は、次のとおりです。

-
- ステップ 1 [Admin] > [CFS] を選択します。
[CFS Configuration] ダイアログボックスが表示されます (図 4-37 を参照)。
 - ステップ 2 iSLB 機能の [Command] フィールドを [clear] に設定します。
 - ステップ 3 [Apply] をクリックして、この変更を保存します。
-

CFS マージ プロセス

2つのファブリックがマージされると、CFSは両方のファブリックのiSLB設定のマージを試行します。一方のファブリック内の指定スイッチ（上位スイッチと呼ぶ）がそのiSLB設定を、もう一方のファブリック内の指定スイッチ（下位スイッチと呼ぶ）に送信します。下位スイッチは、受信した設定と自身の実行コンフィギュレーションを比較して、矛盾がないか確認します。矛盾が検出されなかった場合は、2つの設定をマージして、それを両方のファブリック内のすべてのスイッチに送信します。そして、各スイッチが設定を確認します。この確認では次の内容が保証されます。

- iSLB イニシエータに割り当てられた VSAN がすべてのスイッチ上で設定されていること。
- iSLB イニシエータに設定されたスタティック WWN が固有であり、すべてのスイッチで使用できること。
- iSLB イニシエータ ノード名にすべてのスイッチ上の iSCSI イニシエータとの競合がないこと。

この確認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、マージされた設定を実行コンフィギュレーションに確定するように指示します。確認ができないものがある場合は、マージに失敗します。

iSLB CFS マージ ステータスの矛盾

マージで矛盾が発生する場合があります。マージで次の矛盾が発生した場合はユーザの介入が必要です。

- iSCSI グローバル認証または iSCSI イニシエータのアイドル タイムアウトのパラメータは、2つのファブリックで同じ値には設定されていません。
- 同一の iSLB イニシエータは、2つのファブリックで別々に設定されています。
- 一方のファブリックの iSLB イニシエータは、もう一方のファブリックの iSCSI イニシエータと同じ名前を持ちます。
- 2つのファブリックには重複する pWWN/nWWN 設定が見つかります。たとえば、一方のファブリックの iSLB イニシエータに設定された pWWN/nWWN は、もう一方のファブリックの iSCSI イニシエータまたは別の iSLB イニシエータに設定されています。
- 一方のファブリックの iSLB イニシエータに設定された VSAN は、もう一方のファブリックには存在しません。



ヒント

マージの矛盾に関する詳細は syslog を確認してください。

同一 iSLB イニシエータが矛盾していない別のセットのイニシエータ ターゲットを持つ場合は、ユーザの介入は必要ありません。マージされた設定は、すべてのイニシエータ ターゲットの和集合になります。

iSCSI ハイ アベイラビリティ

iSCSI 設定には、次のハイ アベイラビリティ機能を使用できます。

- 「[透過的なターゲット フェールオーバー](#)」 (P.4-54)
- 「[同一 IP ネットワークに接続された複数の IPS ポート](#)」 (P.4-57)
- 「[VRRP ベースのハイ アベイラビリティ](#)」 (P.4-59)
- 「[イーサネット PortChannel ベースのハイ アベイラビリティ](#)」 (P.4-60)

透過的なターゲット フェールオーバー

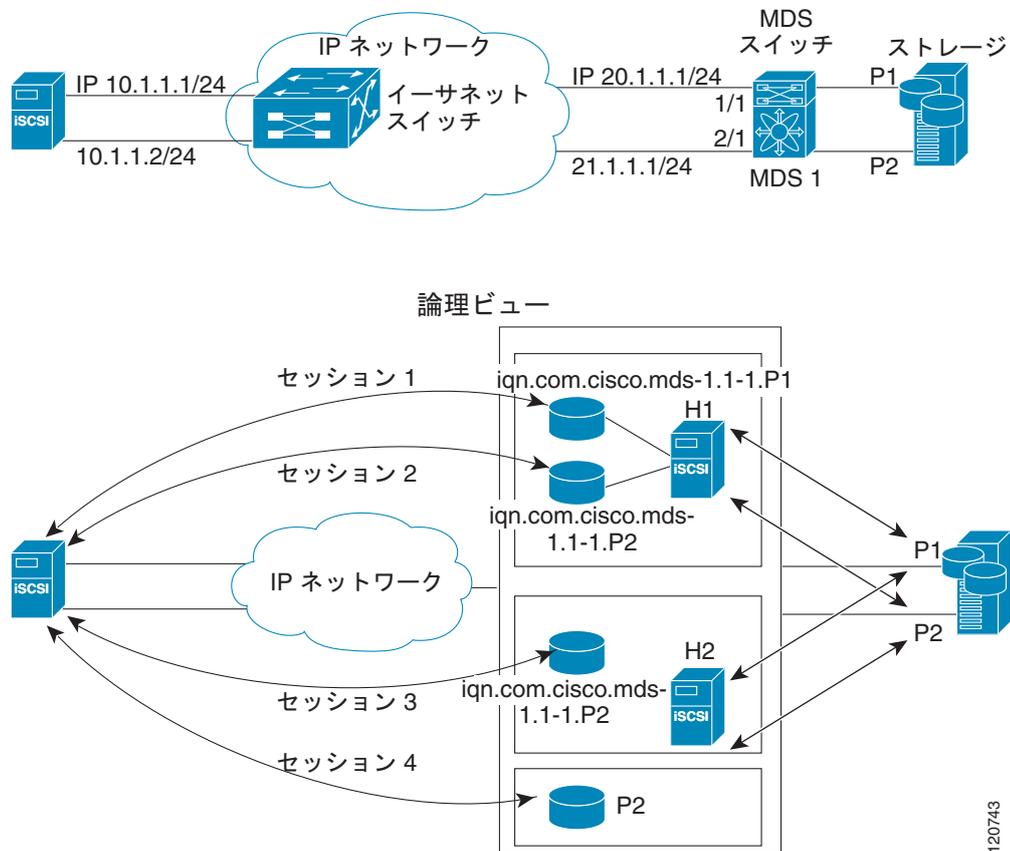
次のハイ アベイラビリティ設定を使用できます。

- マルチパス ソフトウェアを実行しているホストでの iSCSI ハイ アベイラビリティ
- マルチパス ソフトウェアを実行していないホストでの iSCSI ハイ アベイラビリティ

マルチパス ソフトウェアを実行しているホストでの iSCSI ハイ アベイラビリティ

図 4-38 に、複数のマルチパス ソフトウェアを実行しているホストに対する iSCSI HA ソリューションの物理トポロジと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。各ホストの NIC から 2 つの IPS ポートへ向かう iSCSI セッションが 2 つあります。

図 4-38 マルチパス ソフトウェアを実行しているホスト



各 IPS ポートは、ストレージの同じファイバチャネル ターゲット ポートを 2 つ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は異なる iSCSI ターゲット名としてエクスポートします。このため、2 つの IPS ポートは、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。これら 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。IPS ポートがそれぞれ 2 つの iSCSI ターゲットをエクスポートするため、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 に障害が発生すると（物理構成図については、[図 4-38](#) を参照してください）、セッション 1 とセッション 2 は失敗しても、セッション 3 とセッション 4 はそのまま維持されます。

IPS ポート 1 に障害が発生すると、iSCSI ホストは IPS ポートに接続できず、セッション 1、およびセッション 2 は失敗します。それでも、セッション 3 とセッション 4 はそのまま維持されます。

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）。それでも、セッション 2 とセッション 4 はそのまま維持されます。

このトポロジでは、どの構成要素の障害からでも復旧できることとなります。ホストのマルチパスソフトウェアは、ストレージにアクセスするためのさまざまなパス全体のロード バランシングまたはフェールオーバーに対処します。

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

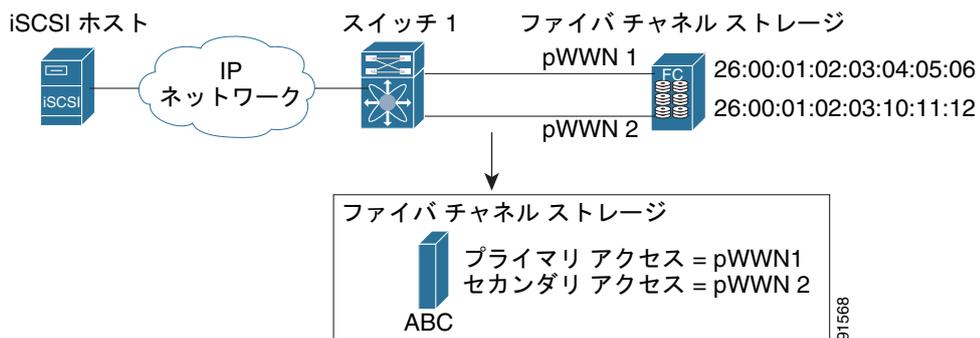
ホストがマルチパス ソフトウェアを使用していない場合、ホストに同一ストレージへの複数のセッションが発生するため、上記トポロジは機能しません。マルチパス ソフトウェアを使用しない場合、ホストは同一ストレージへの複数のパスを把握できません。

IP ストレージには、この状況での HA ソリューションを提供する、2 つの追加機能があります。

- IPS ポートは、VRRP 機能をサポートし（「[ギガビット イーサネット インターフェイスに対する VRRP の設定](#)」(P.6-9) を参照）、IPS ポートのフェールオーバーを提供します。
- IPS は、iSCSI スタティック仮想ターゲットに対する透過的なファイバチャネル ターゲット フェールオーバーを備えています。

スタティックにインポートされた iSCSI ターゲットには、ファイバチャネル ターゲットのセカンダリ pWWN を提供する別のオプションもあります。冗長ポート間で LU を可視化するように物理ファイバチャネル ターゲットを設定するにはこれを使用できます。アクティブ ポートに障害が発生した場合、セカンダリ ポートがアクティブになり、iSCSI セッションは新しいアクティブ ポートを使用するように切り替わります（[図 4-39](#) を参照）。

図 4-39 2 つのファイバチャネル ポートを介してインポートするスタティック ターゲット



[図 4-39](#) では、pWWN1 と 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 ターゲットへの冗長アクセスを提供します。

IPS ポートによって、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 セッションに影響することなく透過的に実行されます。プライマリ ポートに障害が発生すると状況確認のステータスになるため、未処理のすべての I/O は終了します。フェールオーバー中に受信した新規 I/O は完了せず、ビジー ステータスを受信します。



ヒント

LU 番号が異なる場合は、LUN マッピングを使用することで、別のセカンダリ ファイバ チャネル LUN を定義できます。

プライマリ ポートが再びアップの状態になったときに IPS ポートをプライマリ ポートにスイッチバックさせるには、任意の **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で (デフォルト)、スイッチオーバーの後にプライマリ ポートが再びアップ状態になった場合は、古いセッションはセカンダリ ポートに残り、プライマリ ポートにスイッチバックすることはありません。ただし、新しいセッションはいずれもプライマリ ポートを使用します。プライマリ ポートとセカンダリ ポートが同時に使用されるのは、この状況のときだけです。

Device Manager を使用してファイバ チャネル ターゲット ポート全体に対してスタティック iSCSI 仮想ターゲットを作成する手順は、次のとおりです。

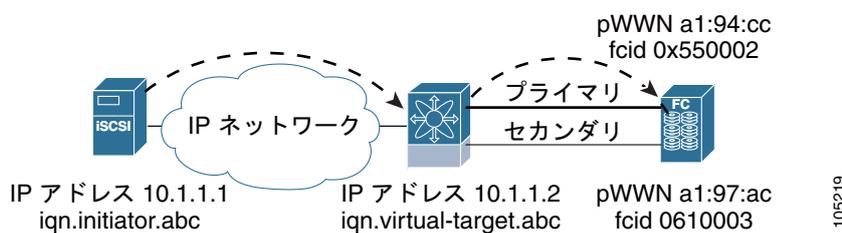
-
- ステップ 1** [IP] > [iSCSI] をクリックします。
iSCSI 設定が表示されます (図 4-12 を参照)。
- ステップ 2** [Targets] タブをクリックして、既存の iSCSI ターゲットのリストを表示します (図 4-13 を参照)。
- ステップ 3** [Create] をクリックして iSCSI ターゲットを作成します。
[Create iSCSI Targets] ダイアログボックスが表示されます (図 4-15 を参照)。
- ステップ 4** [iSCSI Name] フィールドに iSCSI ターゲット ノード名を IQN フォーマットで設定します。
- ステップ 5** [Port WWN] フィールドにマッピングするファイバ チャネル ターゲット ポートを設定します。
- ステップ 6** [Select from List] オプション ボタンをクリックして、この仮想 iSCSI ターゲットにアクセスさせる iSCSI イニシエータ ノード名または IP アドレスを設定するか、または、[All] オプション ボタンをクリックして、この仮想 iSCSI ターゲットをすべての iSCSI イニシエータにアクセスさせるようにします。「iSCSI アクセス コントロール」(P.4-26) を参照してください。
- ステップ 7** [Select from List] オプション ボタンをクリックして、iSCSI ターゲットをアドバタイズするインターフェイスをそれぞれ選択するか、[All] オプション ボタンを選択して、すべてのインターフェイスをアドバタイズします。
- ステップ 8** [Apply] をクリックして、この変更を保存します。
-

ストレージ ポート フェールオーバーの LUN trespass

スタティックにインポートされた iSCSI ターゲットのハイ アベイラビリティの他に、アクティブ ポートの障害時に、スタティックにインポートした 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 を移動できる trespass 機能を使用できます。

2つのファイバチャネル N ポート間で LU を可視化するように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するとパッシブ ポートに引き継がれます。物理ファイバチャネルターゲットの中には、trespass 機能を使用してアクティブ ポートからパッシブ ポートへの LU の移動を必要とするものもあります。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 trespass 機能をイネーブルにする追加のオプションは、冗長ポートを持つ物理ファイバチャネルターゲットで使用できます。アクティブ ポートに障害が発生した場合、パッシブ ポートがアクティブになり、trespass 機能がイネーブルの場合は、Cisco MDS スイッチは LU を新しいアクティブ ポートに移動するようにターゲットに要求を送信します。iSCSI セッションは、新しいアクティブ ポートを使用するように切り替わり、移動した LU には新しいアクティブ ポートを介したアクセスが行われます (図 4-40 を参照)。

図 4-40 アクティブ プライマリ ポートを持つ仮想ターゲット



スタティック iSCSI 仮想ターゲットの trespass 機能をイネーブルにするには、Device Manager で [IP] > [iSCSI] を選択し、[Targets] タブを選択して [Trespass Mode] チェックボックスをオンにします。

同一 IP ネットワークに接続された複数の IPS ポート

図 4-41 に、同一 IP ネットワーク内で複数のギガビットイーサネットインターフェイスを使用する設定例を示します。

VRRP ベースのハイ アベイラビリティ

図 4-42 に、VRRP ベースのハイ アベイラビリティ iSCSI の設定例を示します。

図 4-42 VRRP ベースの iSCSI ハイ アベイラビリティ

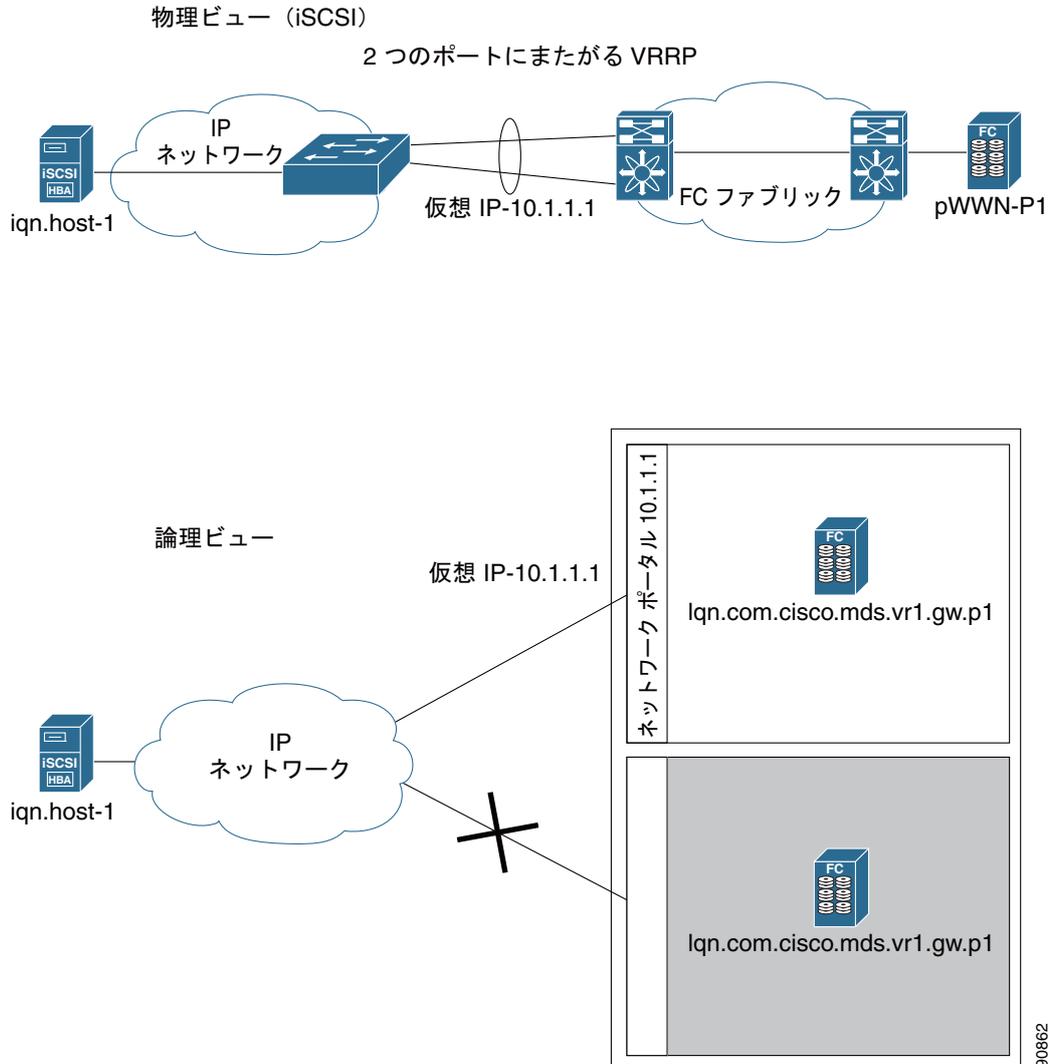


図 4-42 では、各 iSCSI ホストは、各物理ファイバチャネルターゲットごとに 1 つの iSCSI ターゲットを検出します。VRRP マスターのギガビットイーサネットインターフェイスに障害が発生すると、iSCSI セッションは終了します。次にホストがターゲットに再接続すると、別のギガビットイーサネットインターフェイスが新しいマスターとして仮想 IP アドレスを引き継いでいるため、セッションが発生します。

イーサネット PortChannel ベースのハイ アベイラビリティ



(注)

1 つの iSCSI リンクに対するすべての iSCSI データ トラフィックは、1 つの TCP 接続で実行されます。結果として、その iSCSI リンクに対する集約帯域幅は 1 Gbps となります。

図 4-43 に、サンプルのイーサネット PortChannel ベースのハイ アベイラビリティ iSCSI 構成を示します。

図 4-43 イーサネット PortChannel ベース iSCSI ハイ アベイラビリティ

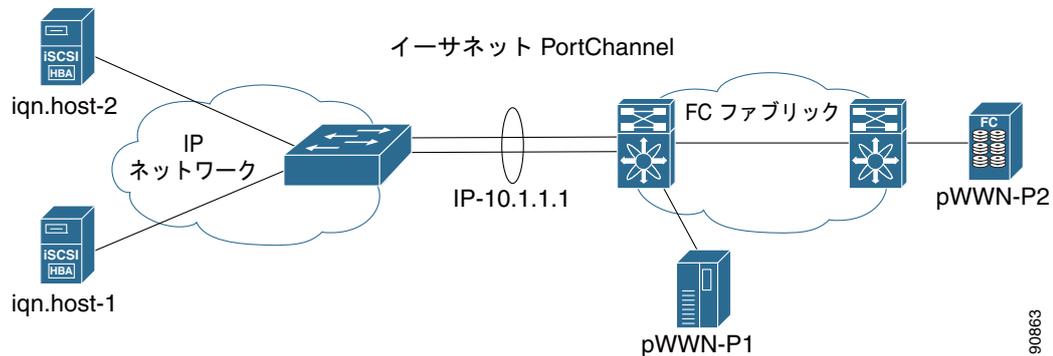


図 4-43 では、各 iSCSI ホストは、各物理ファイバ チャンネル ターゲットごとに 1 つの iSCSI ターゲットを検出します。iSCSI ホストから IPS ポート上の iSCSI 仮想ターゲットへの iSCSI セッションは、2 つの物理インターフェイスのいずれかを使用します (iSCSI セッションが使用する TCP 接続は 1 つであるため)。ギガビットイーサネットインターフェイスで障害が発生すると、IPS モジュールとイーサネットスイッチは透過的にすべてのフレームを 2 番目のギガビットイーサネットインターフェイスに転送します。



(注)

イーサネット PortChannel が IPS モジュールとイーサネットスイッチ間に設定されている場合、VRRP を設定したロード バランシングを正常に動作させるためには、イーサネットスイッチ上のロード バランシング ポリシーは、ポート番号ではなく、送信元および宛先 IP アドレスだけに基づいている必要があります。

iSCSI 認証セットアップに関する注意事項とシナリオ

ここでは、設定可能な各種 iSCSI 認証、セットアップ要件、およびサンプルシナリオに関する注意事項について説明します。次の認証セットアップに関する注意事項を説明します。

- 「認証なしの設定」(P.4-61)
- 「ローカルパスワードデータベースを使用した CHAP の設定」(P.4-61)
- 「外部 RADIUS サーバを使用した CHAP の設定」(P.4-62)
- 「iSCSI トランスペアレントモードイニシエータ」(P.4-63)
- 「ターゲットストレージデバイスに必要な LUN マッピング」(P.4-67)

**注意**

iSLB VRRP グループの一部である iSCSI インターフェイスの認証を変更すると、インターフェイス上のロード バランシングに影響をおよぼします。「[iSCSI インターフェイス パラメータの変更とロード バランシングに対するその影響](#)」(P.4-48) を参照してください。

認証なしの設定

iSCSI 認証方法を **none** に設定すると、認証なしのネットワークが構成されます。

Fabric Manager で、[Physical Attributes] ペインの [End Devices] > [iSCSI] を選択します。[Globals] タブを選択して、[AuthMethod] ドロップダウン メニューを [none] に設定してから、[Apply Changes] をクリックします。

ローカル パスワード データベースを使用した CHAP の設定

ローカル パスワード データベースの CHAP オプションを使用して認証を設定する場合は、次の手順に従います。

-
- ステップ 1** iSCSI プロトコルでローカル 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。
- Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Security] > [AAA] を選択します。
 - [Information] ペインで、[Applications] タブをクリックします。
 - iSCSI 行の [Local] チェックボックスをオンにして、[Apply Changes] をクリックします。
- ステップ 2** すべての iSCSI クライアントで CHAP を要求するように iSCSI 認証方法を設定します。
- Fabric Manager で、[Physical Attributes] ペインの [End Devices] > [iSCSI] を選択します。
 - [Information] ペインで、[Globals] タブをクリックします。
 - [AuthMethod] ドロップダウン メニューを [chap] に設定して、[Apply Changes] をクリックします。
- ステップ 3** iSCSI ユーザのユーザ名とパスワードを設定します。
- Device Manager で、[Security] > [iSCSI] を選択します。
 - [Username]、[Password]、および [Confirm Password] フィールドを設定します。
 - [Create] をクリックして変更を保存します。
- ステップ 4** グローバル iSCSI 認証セットアップを確認します。
- Fabric Manager で、[Physical Attributes] ペインの [End Devices] > [iSCSI] を選択します。
 - [Information] ペインで、[Globals] タブをクリックします。
-

外部 RADIUS サーバを使用した CHAP の設定

外部 RADIUS サーバで CHAP オプションを使用して認証を設定する場合は、次の手順に従います。

- ステップ 1** Cisco MDS スイッチのパスワードを RADIUS サーバへの RADIUS クライアントとして設定します。
 - a. Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Security] > [AAA] > [RADIUS] を選択します。
 - b. [Information] ペインで、[Default] タブをクリックします。
 - c. [AuthKey] フィールドをデフォルトのパスワードに設定して、[Apply Changes] アイコンをクリックします。
- ステップ 2** RADIUS サーバ IP アドレスの設定
 - a. Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Security] > [AAA] > [RADIUS] を選択します。
 - b. [Information] ペインで、[Server] タブをクリックして、[Create Row] をクリックします。
 - c. [Index] フィールドを一意の数に設定します。
 - d. [IP Type] オプション ボタンを [ipv4] または [ipv6] に設定します。
 - e. [Name] または [IP Address] フィールドを RADIUS サーバの IP アドレスに設定し、[Create] をクリックします。
- ステップ 3** RADIUS サーバ グループを作成し、そのグループに RADIUS サーバを追加します。
 - a. Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Security] > [AAA] を選択します。
 - b. [Information] ペインで、[Server Groups] タブをクリックして、[Create Row] を選択します。
 - c. [Index] フィールドを一意の数に設定します。
 - d. [Protocol] オプション ボタンを [radius] に設定します。
 - e. [Name] フィールドをサーバ グループ名に設定します。
 - f. [ServerIDList] を RADIUS サーバのインデックス値に設定し（作成方法については、[ステップ 2 c.](#) を参照してください）、[Create] をクリックします。
- ステップ 4** RADIUS サーバに向かうように iSCSI プロトコルの認証確認をセットアップします。
 - a. Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Security] > [AAA] を選択します。
 - b. [Information] ペインで、[Applications] タブをクリックします。
 - c. [Type]、[SubType]、および [Function] カラムの iSCSI 行を右クリックします。
 - d. [ServerGroup IDList] を [Server Group] のインデックス値に設定し（作成方法については、[ステップ 3](#) を参照してください）、[Create] をクリックします。
- ステップ 5** すべての iSCSI クライアントで CHAP を要求するように iSCSI 認証方法を設定します。
 - a. Fabric Manager で、[Physical Attributes] ペインの [End Devices] > [iSCSI] を選択します。
 - b. [AuthMethod] ドロップダウン メニューから、[chap] を選択します。
 - c. [Apply Changes] アイコンをクリックします。
- ステップ 6** Fabric Manager で、[Physical Attributes] ペインの [End Devices] > [iSCSI] を選択します。
- ステップ 7** [Information] ペインで [Globals] タブをクリックして、グローバル iSCSI 認証セットアップが CHAP になっていることを確認します。
- ステップ 8** Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Security] > [AAA] を選択します。

ステップ 9 [Information] ペインで、[Applications] タブをクリックして、iSCSI の AAA 認証情報を確認します。

iSCSI RADIUS サーバを設定する手順は、次のとおりです。

ステップ 1 Cisco MDS スイッチの管理イーサネット IP アドレスからのアクセスを許可するように RADIUS サーバを設定します。

ステップ 2 Cisco MDS スイッチを認証する RADIUS サーバの共有秘密を設定します。

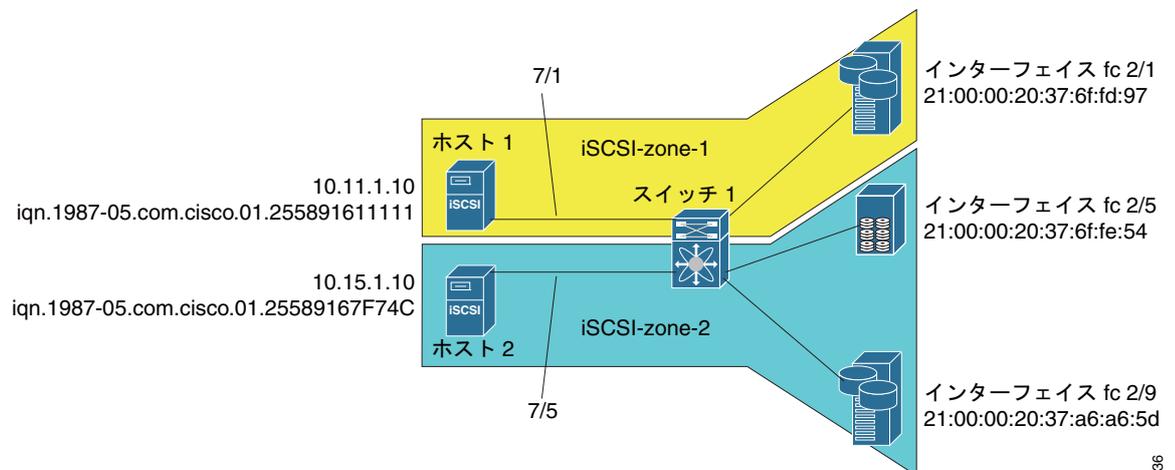
ステップ 3 RADIUS サーバで iSCSI ユーザとパスワードを設定します。

iSCSI トランスペアレント モード イニシエータ

このシナリオでは、次の構成を想定しています (図 4-44 を参照)。

- LUN マッピングまたは LUN マスキング、あるいはターゲット デバイスのその他のホストのアクセスコントロールがない
- iSCSI ログイン認証がない (つまりログイン認証が [none] に設定されている)
- トポロジは次のとおりです。
 - iSCSI インターフェイス 7/1 は、IP アドレスによりイニシエータを特定するように設定されています。
 - iSCSI インターフェイス 7/5 は、ノード名によりイニシエータを特定するように設定されています。
 - IPv4 アドレス 10.11.1.10、名前 iqn.1987-05.com.cisco:01.255891611111 の iSCSI イニシエータ ホスト 1 は、IPS ポート 7/1 に接続し、IPv4 アドレス (ホスト 1 = 10.11.1.10) によって識別されます。
 - IPv4 アドレス 10.15.1.10、ノード名 iqn.1987-05.com.cisco:01.25589167f74c の iSCSI イニシエータ ホスト 2 は、IPS ポート 7/5 に接続します。

図 4-44 iSCSI シナリオ 1



94136

シナリオ 1 を設定する場合は、次の手順に従います (図 4-44 を参照)。

- ステップ 1** Cisco MDS スイッチのすべての iSCSI ホストの null 認証を設定します。
- Fabric Manager で、[Physical Attributes] ペインの [End Devices] > [iSCSI] を選択します。
 - [Information] ペインで、[AuthMethod] ドロップダウン メニューから [none] を選択します。
 - [Apply Changes] アイコンをクリックします。
- 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 に動的にインポートするように iSCSI を設定します。
- Device Manager で、[IP] > [iSCSI] をクリックします。
 - [Targets] タブをクリックします。
 - [Dynamically Import FC Targets] チェックボックスをオンにします。
 - [Apply] をクリックします。
- ステップ 3** IPv4 アドレスを持つスロット 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て、インターフェイスをイネーブルにします。
- Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Interfaces] > [Gigabit Ethernet] を選択します。
 - [Information] ペインで、[IP Address] タブをクリックして、[Create Row] を選択します。
 - スロット 7 ポート 1 のギガビット イーサネット インターフェイスの IP アドレスとサブネット マスクを設定します。
 - [Create] をクリックします。
 - [General] タブを選択して、スロット 7 ポート 1 のギガビット イーサネット インターフェイスの [Admin] ドロップダウン メニューから [up] を選択します。
 - [Apply Changes] アイコンをクリックします。
-  (注) ホスト 2 はこのポートに接続しています。
- ステップ 4** IP アドレスによってすべての動的 iSCSI イニシエータを特定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イネーブルにします。
- Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Interfaces] > [FC Logical] を選択します。
 - [Information] ペインで、[iSCSI] タブをクリックします。
 - [Initiator ID Mode] ドロップダウン メニューから [ipaddress] を選択して、[Apply Changes] アイコンをクリックします。
 - Device Manager で、[Interfaces] > [Ethernet and iSCSI] を選択します。
 - [iSCSI] タブをクリックします。
 - スロット 7 ポート 1 の iSCSI インターフェイスの [Admin] ドロップダウン メニューから [up] を選択します。
 - [Apply] をクリックします。

- ステップ 5** IPv4 アドレスを持つスロット 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て、インターフェイスをイネーブルにします。
- Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Interfaces] > [Gigabit Ethernet] を選択します。
 - [Information] ペインで、[IP Address] タブをクリックして、[Create Row] をクリックします。
 - スロット 7 ポート 5 のギガビット イーサネット インターフェイスの IP アドレスとサブネット マスクを設定します。
 - [Create] をクリックします。
 - [General] タブを選択して、スロット 7 ポート 5 のギガビット イーサネット インターフェイスの [Admin] ドロップダウンメニューから [up] を選択します。
 - [Apply Changes] アイコンをクリックします。

- ステップ 6** ノード名によってすべての動的 iSCSI イニシエータを特定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イネーブルにします。
- Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Interfaces] > [FC Logical] を選択します。
 - [Information] ペインで、[iSCSI] タブをクリックします。
 - [Initiator ID Mode] ドロップダウンメニューから [name] を選択して、[Apply Changes] アイコンをクリックします。
 - Device Manager で、[Interfaces] > [Ethernet and iSCSI] を選択します。
 - [iSCSI] タブをクリックします。
 - スロット 7 ポート 5 の iSCSI インターフェイスの [Admin] ドロップダウンメニューから [up] を選択します。
 - [Apply] をクリックします。



(注) ホスト 1 はこのポートに接続しています。

- ステップ 7** 利用可能なファイバチャネル ターゲットを確認します。
- Device Manager で、[FC] > [Name Server] を選択します。
 - [General] タブをクリックします。

- ステップ 8** ホスト 1 とその中に 1 つのファイバチャネル ターゲットを入れた *iscsi-zone-1* という名前のゾーンを作成します。



(注) iSCSI インターフェイスは IP に基づいてすべてのホストを特定するように設定されているため、ゾーンメンバシップ設定のホストの IP アドレスを使用します。

- Fabric Manager で、[Zones] > [Edit Local Full Zone Database] を選択します。
- [Edit Local Full Zone Database] ダイアログボックスの [VSAN] ドロップダウンメニューから [VSAN 1] を選択します。
- 左側のナビゲーション ペインで [Zones] フォルダを選択して、[Insert] をクリックします。
- [Zone Name] フィールドを [iscsi-zone-1] に設定して、[OK] をクリックします。
- 左側のナビゲーション ペインで [iscsi-zone-1] フォルダを選択して、[Insert] をクリックします。
- [ZoneBy] オプション ボタンを [WWN] に設定します。

- g. Port WWN をファイバ チャネル ターゲットの pWWN (つまり、21:00:00:20:37:6f:fd:97) に設定して、[Add] をクリックします。
- h. [ZoneBy] オプション ボタンを [iSCSI IP Address/Subnet] に設定します。
- i. [IP Address/Mask] フィールドをホスト 1 iSCSI イニシエータ (10.11.1.10) の IP アドレスに設定して、[Add] をクリックします。

ステップ 9 ホスト 2 とその中に 2 つのファイバ チャネル ターゲットを入れた *iscsi-zone-2* という名前のゾーンを作成します。



(注) iSCSI インターフェイスはノード名に基づいてすべてのホストを特定するように設定されているため、ゾーン メンバシップ設定の iSCSI ホストのシンボリック ノード名を使用します。

- a. Fabric Manager で、メイン メニューから、[Zones] > [Edit Local Full Zone Database] を選択します。
- b. [Edit Local Full Zone Database] ダイアログボックスの [VSAN] ドロップダウン メニューから [VSAN 2] を選択します。
- c. 左側のナビゲーション ペインで [Zones] フォルダを選択して、[Insert] をクリックします。
- d. [Zone Name] フィールドを [iscsi-zone-2] に設定して、[OK] をクリックします。
- e. 左側のナビゲーション ペインで [iscsi-zone-2] フォルダを選択して、[Insert] をクリックします。
- f. [ZoneBy] オプション ボタンを [WWN] に設定します。
- g. Port WWN をファイバ チャネル ターゲットのいずれかの pWWN (例 : 21:00:00:20:37:6f:fe:5) に設定します。次に、[Add] をクリックします。
- h. Port WWN をファイバ チャネル ターゲットの別の pWWN (例 : 21:00:00:20:37:a6:a6:5d) に設定します。次に、[Add] をクリックします。
- i. [ZoneBy] オプション ボタンを [iSCSI name] に設定します。
- j. [Port Name] フィールドをホスト 2 のシンボリック名 (iqn.1987-05.com.cisco:01.25589167f74c) に設定して、[Add] をクリックします。

ステップ 10 ゾーンセットを作成して、メンバーとして 2 つのゾーンを追加し、ゾーンセットを有効にします。



(注) iSCSI インターフェイスは、ノード名に基づいてすべてのホストを特定するように設定されています。

- a. Fabric Manager で、[Zones] > [Edit Local Full Zone Database] を選択します。
- b. [Edit Local Full Zone Database] ダイアログボックスの [VSAN] ドロップダウン メニューから [VSAN 1] を選択します。
- c. 左側のナビゲーション ペインで [Zoneset] フォルダを選択して、[Insert] をクリックします。
- d. [Zoneset Name] を [zonset-iscsi] に設定して、[OK] をクリックします。
- e. [zonset-iscsi] フォルダをクリックして、[Insert] をクリックします。
- f. [Zone Name] フィールドを [iscsi-zone-1] に設定して、[OK] をクリックします。
- g. [Zone Name] フィールドを [iscsi-zone-2] に設定して、[OK] をクリックします。
- h. [Activate] をクリックして、新しいゾーンセットをアクティブにします。
- i. [Continue Activation] をクリックして、アクティブ化を完了します。

ステップ 11 iSCSI ホスト (ホスト 1 とホスト 2) を構築します。

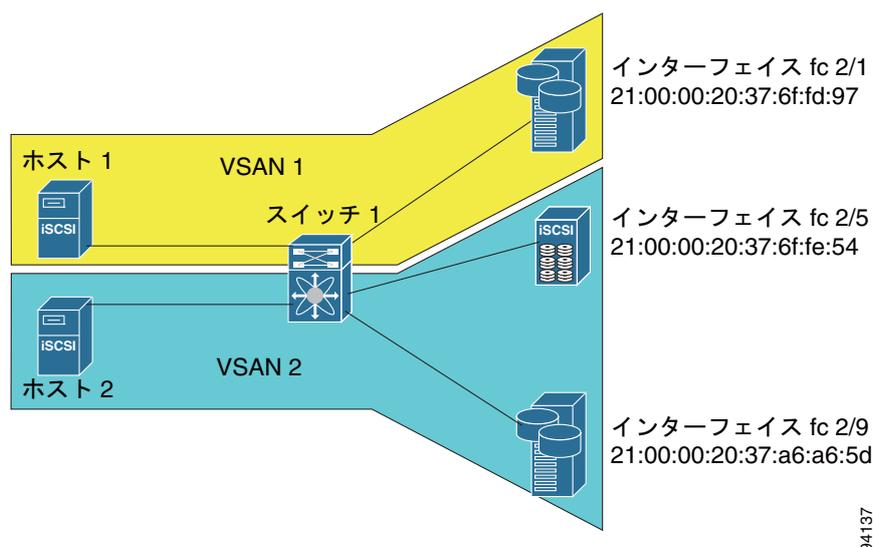
- ステップ 12** すべての iSCSI セッションを表示します。
- Device Manager で、[Interfaces] > [Monitor] > [Ethernet] を選択します。
 - [iSCSI connections] タブをクリックして、すべての iSCSI セッションを表示します。
 - Device Manager で、[IP] > [iSCSI] を選択して、[Session Initiators] タブを選択します。
 - [Details] をクリックします。
- ステップ 13** Fabric Manager で、[Physical Attributes] ペインで、[End Devices] > [iSCSI] を選択して、2 つの iSCSI イニシエータの詳細を確認します。
- ステップ 14** Fabric Manager で、[Zones] > [Edit Local Full Zone Database] を選択して、アクティブな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。
- ステップ 15** Device Manager で、[FC] > [Name Server] を選択します。ファイバチャネル ネーム サーバには、iSCSI ホストに対して作成された仮想 N ポートが表示されます。
- ステップ 16** Device Manager で、[FC] > [Name Server] を選択します。
- ステップ 17** [Advanced] タブをクリックします。ファイバチャネル ネーム サーバの iSCSI イニシエータ ノードの詳細出力を確認します。

ターゲットストレージデバイスに必要な LUN マッピング

サンプルシナリオ 2 は、次の構成を想定しています (図 4-45 を参照)。

- アクセスコントロールがファイバチャネル ゾーニングに基づいている。
- ターゲットベースの LUN マッピングまたは LUN マスキングがある。
- iSCSI 認証がない (none)。
- iSCSI イニシエータは異なる VSAN に割り当てられている。

図 4-45 iSCSI シナリオ 2



94137

シナリオ 2 を設定する場合は、次の手順に従います (図 4-45 を参照)。

- ステップ 1** すべての iSCSI ホストに対して null 認証を設定します。
- Fabric Manager で、[Physical Attributes] ペインの [End Devices] > [iSCSI] を選択します。
 - [Information] ペインで、[AuthMethod] ドロップダウン メニューから [none] を選択します。
 - [Apply Changes] アイコンをクリックします。
- 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 に動的にインポートするように iSCSI を設定します。
- Device Manager で、[IP] > [iSCSI] をクリックします。
 - [Targets] タブをクリックします。
 - [Dynamically Import FC Targets] チェックボックスをオンにします。
 - [Apply] をクリックします。
- ステップ 3** IPv4 アドレスを持つスロット 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て、インターフェイスをイネーブルにします。
- Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Interfaces] > [Gigabit Ethernet] を選択します。
 - [Information] ペインで、[IP Address] タブをクリックして、[Create Row] を選択します。
 - スロット 7 ポート 1 のギガビット イーサネット インターフェイスの IP アドレスとサブネット マスクを設定します。
 - [Create] をクリックします。
 - [General] タブをクリックして、スロット 7 ポート 1 のギガビット イーサネット インターフェイスの [Admin] ドロップダウン メニューから [up] を選択します。
 - [Apply Changes] アイコンをクリックします。
- ステップ 4** IP アドレスによってすべての動的 iSCSI イニシエータを特定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イネーブルにします。
- Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Interfaces] > [FC Logical] を選択します。
 - [Information] ペインで、[iSCSI] タブを選択します。
 - [Initiator ID Mode] ドロップダウン メニューから [ipaddress] を選択して、[Apply Changes] アイコンをクリックします。
 - Device Manager で、[Interfaces] > [Ethernet and iSCSI] を選択します。
 - [iSCSI] タブをクリックします。
 - スロット 7 ポート 1 の iSCSI インターフェイスの [Admin] ドロップダウン メニューから [up] を選択します。
 - [Apply] をクリックします。
- ステップ 5** IPv4 アドレスを持つスロット 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て、インターフェイスをイネーブルにします。
- Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Interfaces] > [Gigabit Ethernet] を選択します。
 - [Information] ペインで、[IP Address] タブをクリックして、[Create Row] をクリックします。

- c. スロット 7 ポート 5 のギガビットイーサネット インターフェイスの IP アドレスとサブネットマスクを設定します。
- d. [Create] をクリックします。
- e. [General] タブを選択して、スロット 7 ポート 5 のギガビットイーサネット インターフェイスの [Admin] ドロップダウンメニューから [up] を選択します。
- f. [Apply Changes] アイコンをクリックします。

ステップ 6 IP アドレスによってすべての動的 iSCSI イニシエータを特定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イネーブルにします。

- a. Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Interfaces] > [FC Logical] を選択します。
- b. [Information] ペインで、[iSCSI] タブをクリックします。
- c. [Initiator ID Mode] ドロップダウンメニューから [ipaddress] を選択して、[Apply Changes] アイコンをクリックします。
- d. Device Manager で、[Interfaces] > [Ethernet and iSCSI] を選択します。
- e. [iSCSI] タブをクリックします。
- f. スロット 7 ポート 5 の iSCSI インターフェイスの [Admin] ドロップダウンメニューから [up] を選択します。
- g. [Apply] をクリックします。

ステップ 7 ホスト 1 の静的 pWWN と nWWN の設定を行います。

- a. Device Manager で、[IP] > [iSCSI] を選択します。
- b. [Initiators] タブをクリックします。
- c. ホスト 1 iSCSI イニシエータの [Node Address Persistent] および [Node Address System-assigned] チェックボックスをオンにします。
- d. [Apply] をクリックします。

ステップ 8 ホスト 2 の静的 pWWN の設定を行います。

- a. Device Manager で、[IP] > [iSCSI] を選択します。
- b. [Initiators] タブをクリックします。
- c. ホスト 2 iSCSI イニシエータを右クリックして、[Edit pWWN] をクリックします。
- d. [System-assigned Num] フィールドで [1] を選択して、[Apply] をクリックします。

ステップ 9 設定した WWN を表示します。



(注) WWN はシステムで割り当てられます。イニシエータは異なる VSAN のメンバーです。

- a. Fabric Manager で、[Physical Attributes] ペインの [End Devices] > [iSCSI] を選択します。
- b. [Initiators] タブをクリックします。

ステップ 10 VSAN 1 のホスト 1 と iSCSI ターゲットを作成します。



(注) iSCSI インターフェイスは IP に基づいてすべてのホストを特定するように設定されているため、ゾーンメンバシップ設定のホストの IP アドレスを使用します。

- a. Fabric Manager で、[Zones] > [Edit Local Full Zone Database] を選択します。

- b. [Edit Local Full Zone Database] ダイアログボックスの [VSAN] ドロップダウン メニューから [VSAN 1] を選択します。
- c. 左側のナビゲーション ペインで [Zones] フォルダを選択して、[Insert] をクリックします。
- d. [Zone Name] フィールドを [iscsi-zone-1] に設定して、[OK] をクリックします。
- e. 左側のナビゲーション ペインで [iscsi-zone-1] フォルダを選択して、[Insert] をクリックします。
- f. [ZoneBy] オプション ボタンを [WWN] に設定します。
- g. Port WWN をファイバ チャネル ターゲットの pWWN (つまり、21:00:00:20:37:6f:fd:97) に設定します。次に、[Add] をクリックします。
- h. [ZoneBy] オプション ボタンを [iSCSI IP Address/Subnet] に設定します。
- i. [IP Address/Mask] フィールドをホスト 1 iSCSI イニシエータ (10.11.1.10) の IP アドレスに設定して、[Add] をクリックします。



(注) iSCSI シンボリック ノード名または pWWN のいずれかで、iSCSI イニシエータのゾーン メンバシップのファイバ チャネル ストレージを使用できます。この場合は、pWWN は固定的です。

ステップ 11 VSAN 1 で設定されたゾーンを作成し、アクティブ化します。

- a. Fabric Manager で、[Zones] > [Edit Local Full Zone Database] を選択します。
- b. [Edit Local Full Zone Database] ダイアログボックスの [VSAN] ドロップダウン メニューから [VSAN 1] を選択します。
- c. 左側のナビゲーション ペインで [Zoneset] フォルダを選択して、[Insert] をクリックします。
- d. [Zoneset Name] を [zonset-iscsi-1] に設定して、[OK] をクリックします。
- e. [zonset-iscsi-1] フォルダをクリックして、[Insert] をクリックします。
- f. [Zone Name] フィールドを [iscsi-zone-1] に設定して、[OK] をクリックします。
- g. [Activate] をクリックして、新しいゾーン セットをアクティブにします。
- h. [Continue Activation] をクリックして、アクティブ化を完了します。

ステップ 12 ホスト 2 と 2 つのファイバ チャネル ターゲットを含むゾーンを作成します。



(注) ホストが VSAN 2 にある場合、ファイバ チャネル ターゲットとゾーンも、VSAN 2 になければなりません。



(注) iSCSI インターフェイスは、ノード名に基づいてすべてのホストを特定するように設定されています。

- a. Fabric Manager で、[Zones] > [Edit Local Full Zone Database] を選択します。
- b. [Edit Local Full Zone Database] ダイアログボックスの [VSAN] ドロップダウン メニューから [VSAN 2] を選択します。
- c. 左側のナビゲーション ペインで [Zones] フォルダを選択して、[Insert] をクリックします。
- d. [Zone Name] フィールドを [iscsi-zone-2] に設定して、[OK] をクリックします。
- e. 左側のナビゲーション ペインで [iscsi-zone-2] フォルダを選択して、[Insert] をクリックします。
- f. [ZoneBy] オプション ボタンを [WWN] に設定します。

- g. Port WWN をファイバチャネルターゲットのいずれかの pWWN (例 : 21:00:00:20:37:6f:fe:5) に設定して、[Add] をクリックします。
- h. Port WWN をファイバチャネルターゲットの別の pWWN (例 : 21:00:00:20:37:a6:a6:5d) に設定して、[Add] をクリックします。
- i. [ZoneBy] オプション ボタンを [iSCSI IP Address/Subnet] に設定します。
- j. [IP Address/Mask] フィールドをホスト 2 iSCSI イニシエータ (10.15.1.11) の IP アドレスに設定して、[Add] をクリックします。

ステップ 13 VSAN 2 で設定されたゾーンを作成し、アクティブ化します。

- a. Fabric Manager で、[Zones] > [Edit Local Full Zone Database] を選択します。
- b. [Edit Local Full Zone Database] ダイアログボックスの [VSAN] ドロップダウン メニューから [VSAN 2] を選択します。
- c. 左側のナビゲーション ペインで [Zoneset] フォルダを選択して、[Insert] をクリックします。
- d. [Zoneset Name] を [zonset-iscsi-2] に設定して、[OK] をクリックします。
- e. [zonset-iscsi-2] フォルダをクリックして、[Insert] をクリックします。
- f. [Zone Name] フィールドを [iscsi-zone-2] に設定して、[OK] をクリックします。
- g. [Activate] をクリックして、新しいゾーンセットをアクティブにします。
- h. [Continue Activation] をクリックして、アクティブ化を完了します。

ステップ 14 両方のホストで、iSCSI クライアントを起動します。

ステップ 15 すべての iSCSI セッションを表示します。

- a. Device Manager で、[Interface] > [Monitor] > [Ethernet] を選択し、[iSCSI connections] タブをクリックして、すべての iSCSI セッションを表示します。
- b. Device Manager で、[IP] > [iSCSI] を選択して、[Session Initiators] タブを選択します。
- c. [Details] をクリックします。

ステップ 16 Fabric Manager で、[Physical Attributes] ペインで、[End Devices] > [iSCSI] を選択して、2 つの iSCSI イニシエータの詳細を確認します。

ステップ 17 Fabric Manager で、[Zones] > [Edit Local Full Zone Database] を選択して、アクティブな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。

ステップ 18 Device Manager で、[FC] > [Name Server] を選択します。ファイバチャネル ネーム サーバには、iSCSI ホストに対して作成された仮想 N ポートが表示されます。

ステップ 19 Device Manager で、[FC] > [Name Server] を選択します。

ステップ 20 [Advanced] タブをクリックします。ファイバチャネル ネーム サーバの iSCSI イニシエータ ノードの詳細出力を確認します。

iSNS

インターネットストレージネームサービス (iSNS) では、iSCSI デバイスの検出、管理、および設定を自動化することで、既存の TCP/IP ネットワークを SAN としてより効果的に機能させることができます。このような機能を容易に動作させるために、iSNS サーバとクライアントは次のように機能します。

- iSNS クライアントは、iSNS サーバでアクセスできる iSCSI ポータルとすべての iSCSI デバイスを登録します。
- 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
 - 状態変更通知
 - 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 (イニシエータとターゲット) は、iSNS サーバで登録できます。iSCSI イニシエータは、次に、ターゲットのリストの iSNS サーバに問い合わせます。iSNS サーバは、設定されたアクセス制御パラメータに基づいて問い合わせクライアントがアクセスできるターゲットのリストで応答します。

Cisco MDS 9000 ファミリースイッチは、iSNS クライアントとして動作し、外部 iSNS サーバですべての利用可能な iSCSI ターゲットを登録します。IPS モジュールまたは MPS-14/2 モジュールがインストールされている Cisco MDS 9000 ファミリーのすべてのスイッチは、iSNS サーバ機能をサポートします。これによって、iSCSI などの外部 iSNS クライアントは、スイッチを登録し、SAN のすべての利用可能な iSCSI ターゲットを検出できます。

ここで説明する内容は、次のとおりです。

- 「[iSNS クライアント機能の概要](#)」 (P.4-72)
- 「[iSNS クライアントプロファイルの作成](#)」 (P.4-73)
- 「[iSNS サーバ機能の概要](#)」 (P.4-75)
- 「[iSNS サーバの設定](#)」 (P.4-76)

iSNS クライアント機能の概要

各 IPS インターフェイスの iSNS クライアント機能 (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、あるいは PortChannel) は、iSNS サーバで情報を登録します。iSNS プロファイルを作成し、サーバの IP アドレスをプロファイルに追加し、プロファイルをインターフェイスに割り当て (タギング) することで、iSNS サーバの IP アドレスを指定する必要があります。iSNS プロファイルは、1 つ以上のインターフェイスにタギングできます。

プロファイルがインターフェイスにタギングされると、スイッチはプロファイルの iSNS サーバの IP アドレス (一般的な iSNS ポート番号 3205 を使用) への TCP 接続を開き、ネットワークエンティティとポータルオブジェクトを登録します。一意のエンティティは各 IPS インターフェイスに関連付けられます。次に、スイッチは Fibre Channel Name Server (FCNS; ファイバチャネルネームサーバ) データベースとスイッチ設定を検索して、iSNS サーバで登録するストレージノードを検索します。

関連付けられたファイバチャネル pWWN が FCNS データベースにあり、アクセスコントロール設定がそれを防止しない場合、静的にマッピングされた仮想ターゲットが登録されます。動的なターゲットインポートがイネーブルになっている場合は、動的にマッピングされたターゲットが登録されます。iSCSI によるファイバチャネルターゲットのインポート方法に関する詳細については、「[iSCSI ターゲットとしてのファイバチャネルターゲットの提示](#)」 (P.4-9) を参照してください。

設定が変更（アクセス コントロール変更または動的インポートのディセーブル化など）された場合や、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ときに、ストレージノードが利用できなくなると、ストレージノードは iSNS サーバから登録解除されます。ノードがオンラインになると、再登録されます。

iSNS クライアントが iSNS サーバでオブジェクトを登録または登録解除できないとき（たとえば、クライアントが iSNS サーバに対する TCP 接続を作成できない場合）には、毎分再試行して、iSNS サーバに影響するインターフェイスのすべての iSNS オブジェクトを再登録しようとします。iSNS クライアントが使用する登録間隔は 15 分です。クライアントがこの時間の間に登録を更新できない場合、サーバはエントリを登録解除します。

プロファイルのタグgingを解除しても、ネットワーク エンティティとポータルは、その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ていません。

iSNS クライアント プロファイルの作成

Fabric Manager を使用して iSNS プロファイルを作成する場合は、次の手順に従います。

- ステップ 1** [Physical Attributes] ペインで [End Devices] > [iSCSI] を選択します。
[Information] ペインに iSCSI 設定が表示されます（[図 4-12](#) を参照）。
- ステップ 2** [iSNS] タブを選択します。
- ステップ 3** 設定された iSNS プロファイルが表示されます（[図 4-46](#) を参照）。

図 4-46 Fabric Manager の iSNS プロファイル

Switch	Feature	Status	Command	LastCommand	Result
sw172-22-46-220	iscsi	enabled	noSelection	noSelection	none
sw172-22-46-223	iscsi	enabled	noSelection	noSelection	none
sw172-22-46-233	iscsi	enabled	noSelection	noSelection	none
sw172-22-46-224	iscsi	disabled	noSelection	noSelection	none
sw172-22-46-1R2	iscsi	disabled	noSelection	noSelection	none
sw172-22-46-223	isns-server	enabled	noSelection	noSelection	none
sw172-22-46-221	iscsi	disabled	noSelection	noSelection	none
sw172-22-46-222	iscsi	enabled	noSelection	noSelection	none
sw172-22-46-233	isns-server	enabled	noSelection	noSelection	none

- ステップ 4** [Create Row] アイコンをクリックします。
[Create iSNS Profiles] ダイアログボックスが表示されます。
- ステップ 5** [ProfileName] フィールドを作成する iSNS プロファイル名に設定します。
- ステップ 6** [ProfileAddr] フィールドを iSNS サーバの IP アドレスに設定します。
- ステップ 7** [Create] をクリックして変更を保存します。

Fabric Manager を使用して iSNS プロファイルを削除する場合は、次の手順に従います。

- ステップ 1** [Physical Attributes] ペインの [End Devices] > [iSCSI] を選択します。
[Information] ペインに iSCSI 設定が表示されます（[図 4-12](#) を参照）。

- ステップ 2** [iSNS] タブを選択します。
設定された iSNS プロファイルが表示されます (図 4-46 を参照)。
- ステップ 3** 削除するプロファイルを右クリックして、[Delete Row] アイコンをクリックします。

Fabric Manager を使用してインターフェイスにプロファイルをタグgingする場合は、次の手順に従います。

- ステップ 1** [Physical Attributes] ペインで [Switches] > [Interfaces] > [Gigabit Ethernet] を選択します。
[Information] ペインにギガビット イーサネットの設定が表示されます。
- ステップ 2** [iSNS] タブをクリックします。
これらのインターフェイスに設定された iSNS プロファイルが表示されます (図 4-47 を参照)。

図 4-47 Fabric Manager の iSNS プロファイル

Switch	Interface	IscsiAuthMethod	iSNS ProfileName	IscsiSessions
sw172-22-46-220	gigE8/1			0
sw172-22-46-223	gigE2/1			0
sw172-22-46-233	gigE1/1			0
sw172-22-46-220	gigE0/2			0
sw172-22-46-223	gigE2/2			0
sw172-22-46-233	gigE1/2			0
sw172-22-46-220	gigE0/1			0
sw172-22-46-174	gigE12/1			0
sw172-22-46-220	gigE0/2			0

- ステップ 3** [iSNS ProfileName] フィールドをこのインターフェイスに追加する iSNS プロファイル名に設定します。
- ステップ 4** [Apply Changes] アイコンをクリックして、これらの変更を保存します。

Fabric Manager を使用してインターフェイスからプロファイルのタグgingを解除する場合は、次の手順に従います。

- ステップ 1** [Physical Attributes] ペインで [Switches] > [Interfaces] > [Gigabit Ethernet] を選択します。
[Information] ペインにギガビット イーサネットの設定が表示されます。
- ステップ 2** [iSNS] タブをクリックします。
これらのインターフェイスに設定された iSNS プロファイルが表示されます (図 4-47 を参照)。
- ステップ 3** タグを解除する [iSNS ProfileName] フィールドを右クリックして、そのフィールドのテキストを削除します。
- ステップ 4** [Apply Changes] アイコンをクリックして、これらの変更を保存します。

iSNS サーバ機能の概要

イネーブルにすると、Cisco 9000 ファミリ MDS スイッチの iSNS サーバは、すべての登録された iSCSI デバイスを追跡します。結果として、iSNS クライアントは、iSNS サーバに問い合せて、その他の iSNS クライアントを検索できます。iSNS サーバは次の機能も提供します。

- iSNS クライアントは、iSNS サーバで登録されたその他の iSNS クライアントの登録、登録解除、および問い合わせができます。
- アクセス コントロールの実行を一元的に管理し、特定のイニシエータからターゲットへのアクセスを許可または拒否します。
- 登録された iSNS クライアントに通知メカニズムを提供し、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信します。
- ファイバチャネルと iSCSI デバイスの両方に単一のアクセス コントロール設定を提供します。
- iSCSI イニシエータへの直接 IP 接続がない iSCSI ターゲットを検出します。

シナリオの例

iSNS サーバは、ファイバチャネルゾーニング情報と iSCSI アクセス コントロール情報と設定の両方を使用して、ファイバチャネルと iSCSI デバイス全体で均一のアクセス 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 イニシエータだけが、アクセス コントロール情報の両方のセットに基づいてアクセスできるデバイスを検出できます。図 4-48 に、このシナリオの例を示します。

図 4-48 Cisco MDS 環境における iSNS サーバの使用方法

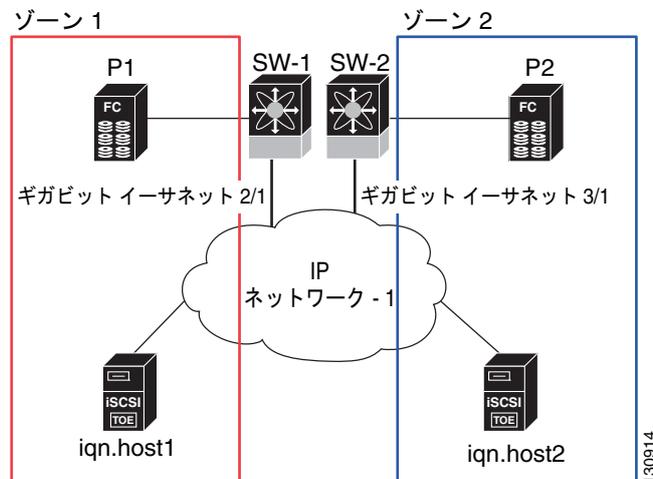


図 4-48 では、iqn.host1 および iqn.host2 が iSCSI イニシエータです。P1 および P2 はファイバチャネルターゲットです。2つのイニシエータは別のゾーンにあります。ゾーン1は iqn.host1 とターゲット P1 から構成され、ゾーン2は iqn.host2 とターゲット P2 から構成されます。iSNS サーバ機能は、SW-1 と SW-2 の両方のスイッチでイネーブルになっています。登録処理は次の方法で実行されます。

1. Initiator iqn.host1 は SW-1、ポート GigabitEthernet2/1 で登録します。
2. Initiator iqn.host2 は SW-2、ポート GigabitEthernet3/1 で登録します。
3. Initiator iqn.host1 は SW-1 に対して iSNS クエリを発行して、すべてのアクセス可能なターゲットを判断します。

4. 次に、iSNS サーバがファイバ チャネル ネーム サーバ (FCNS) に問い合わせ、クエリ送信側からアクセスできる同じゾーンにあるデバイスのリストを取得します。このクエリは P1 だけを生成します。
5. 次に、iSNS サーバは独自のデータベースに問い合わせ、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、仮想ターゲットおよびアクセス コントロール設定、あるいは動的ファイバ チャネル ターゲット インポート機能がイネーブルかディセーブルかなどの iSCSI 設定に基づいています。
6. iSNS サーバはクエリ送信側に応答を送信します。この応答には iSNS サーバが認識しているすべての iSCSI ポータルのリストが含まれています。つまり、iqn.host1 は、SW-1 (Gigabitethernet 2/1) または SW-2 (Gigabitethernet 3/1) 経由で、ターゲット P1 へのログインを選択できます。
7. イニシエータが SW-1 にログインすることを選択し、後からそのポートがアクセスできなくなった場合 (たとえば、Gigabitethernet 2/1 がダウンした場合) は、イニシエータは代わりに SW-2 のポート Gigabitethernet 3/1 経由でターゲット P1 に接続することを選択できます。
8. ターゲットがダウンしているか、ゾーンから削除されている場合は、iSNS サーバは iSNS State Change Notification (SCN) メッセージをイニシエータに送信するため、イニシエータはセッションを削除できます。

iSNS サーバの設定

ここでは、Cisco MDS 9000 ファミリー スイッチの iSNS サーバの設定方法について説明します。

ここで説明する内容は、次のとおりです。

- 「iSNS サーバのイネーブル化」 (P.4-76)
- 「iSNS 設定配布」 (P.4-77)
- 「ESI 再試行カウントの設定」 (P.4-77)
- 「登録期間の設定」 (P.4-77)
- 「iSNS クライアント登録および登録解除」 (P.4-78)
- 「ターゲット検出」 (P.4-78)

iSNS サーバのイネーブル化

iSNS サーバ機能をイネーブルにするには、iSCSI をイネーブルにする必要があります (「iSCSI のイネーブル化」 (P.4-5) を参照)。iSCSI をディセーブルにすると、iSNS が自動的にディセーブルになります。iSNS サーバがスイッチ上でイネーブルになると、対応する iSCSI インターフェイスが起動しているすべての IPS ポートでは、外部 iSNS クライアントからの iSNS 登録とクエリ要求を処理できます。

Fabric Manager を使用して iSNS サーバをイネーブルにする場合は、次の手順に従います。

-
- ステップ 1** [End Devices] > [iSNS] を選択します。
[Information] ペインに iSNS 設定が表示されます。
 - ステップ 2** [Control] タブをクリックして、iSNS サーバ機能の [Command] ドロップダウン メニューから [enable] を選択します。
 - ステップ 3** [Apply Changes] アイコンをクリックして、この変更を保存します。
-



(注) iSNS クライアントからターゲットを検出するときに、VRRP IPv4 アドレスを使用している場合は、[secondary] オプションを使用して、IP アドレスを作成していることを確認します。

iSNS 設定配布

CFS インフラストラクチャを使用して、ファブリック全体の iSNS サーバに iSCSI イニシエータ設定を配布できます。これによって、すべてのスイッチで稼働中の iSNS サーバが、問い合わせ側の iSNS クライアントに対し、ファブリックの任意の場所にある利用可能な iSCSI デバイスのリストを提供できます。CFS については、『Cisco Fabric Manager System Management Configuration Guide』を参照してください。

Fabric Manager を使用して iSNS 設定配布をイネーブルにする場合は、次の手順に従います。

- ステップ 1** [End Devices] > [iSNS] を選択します。
[Information] ペインに iSNS 設定が表示されます。
- ステップ 2** [CFS] タブをクリックして、iSNS の [Admin] ドロップダウン メニューから [enable] を選択します。
- ステップ 3** iSNS の [Global] ドロップダウン メニューから、[enable] を選択します。
- ステップ 4** [Apply Changes] アイコンをクリックして、この変更を保存します。

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、設定した iSNS サーバに情報を登録します。登録時には、クライアントは 60 秒以上の Entity Status Inquiry (ESI; エンティティ ステータス照会) 間隔を示すことができます。クライアントが ESI 間隔をゼロ (0) に設定して登録する場合は、サーバは ESI を使用してクライアントを監視しません。このような場合、明示的に登録解除されるか、iSNS サーバ機能がディセーブルになるまで、クライアントの登録は有効なままです。

ESI 再試行カウントは、iSNS サーバがエンティティ ステータスについて iSNS クライアントに問い合わせる回数です。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にまだ有効であることを示す応答を送信します。設定した再試行回数を超えてもクライアントが応答できない場合は、クライアントはサーバから登録解除されます。

登録期間の設定

iSNS クライアントは、iSNS サーバで登録期間を指定します。iSNS サーバは、この期間が終了するまで、登録をアクティブな状態に保ちます。この期間中に iSNS クライアントからのコマンドがない場合は、iSNS サーバはデータベースからクライアント登録を削除します。

iSNS クライアントが登録期間を指定しない場合は、iSNS サーバはデフォルト値の 0 を取り、登録を無制限にアクティブに保ちます。MDS iSNS サーバで手動で登録期間を設定することもできます。

Fabric Manager を使用して iSNS サーバの登録期間を設定する場合は、次の手順に従います。

- ステップ 1** [End Devices] > [iSNS] を選択します。
[Information] ペインに iSNS 設定が表示されます。
- ステップ 2** [Servers] タブをクリックします。

設定した iSNS サーバが表示されます。

ステップ 3 [ESI NonResponse Threshold] フィールドを ESI 再試行カウント値に設定します。

ステップ 4 [Apply Changes] アイコンをクリックして、この変更を保存します。

iSNS クライアント登録および登録解除

iSNS クライアントは登録されるまで、iSNS サーバに問い合わせできません。

iSNS クライアントの登録解除は明示的に、あるいは (ESI 監視によって) iSNS サーバがクライアントに到達できないことを検出するときに発生します。

iSNS クライアント登録と登録解除を行うと、すべての関連する iSNS クライアントに State Change Notification (SCN) が送信されます。

ターゲット検出

iSCSI イニシエータは、iSNS サーバにクエリを発行して、ターゲットを検出します。サーバはターゲットのリストを検索する *DevGetNext* 要求と、IP アドレスや接続先ポート番号などのターゲットとポータル詳細情報を判定する *DevAttrQuery* をサポートしています。

iSCSI クライアントからクエリ要求を受信すると、iSNS サーバはファイバチャネル ネーム サーバ (FCNS) に問い合わせ、問い合わせ側のイニシエータから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。このクエリの結果は、現在アクティブなゾーニング設定および現在のイニシエータの設定に依存します。iSNS サーバは続いて iSCSI ターゲット設定を使用して、ファイバチャネル ターゲット設定 (仮想ターゲットと動的インポート設定) を同等の iSCSI ターゲットに変換します。この段階では、仮想ターゲットに対して設定されたアクセス コントロールに適用されます。次に、ターゲット詳細に関する応答メッセージが問い合わせのイニシエータに送信されます。

iSNS サーバは、問い合わせ側のイニシエータに、すべての可能なターゲットとポータルを含む包括的な応答を送信します。たとえば、ファイバチャネル ターゲットが別の iSCSI ターゲットとして異なる IPS インターフェイスにエクスポートされる場合は、iSNS サーバはすべての可能な iSCSI ターゲットとポータルのリストで応答します。

ターゲットのリストを最新の状態に保つために、iSNS サーバは、iSCSI ターゲットが到達可能か到達不可能になると、必ず State Change Notification (SCN) をクライアントに送信します。これで、クライアントは、別の iSNS クエリを開始して、アクセス可能なターゲットのリストを再検出できるようになります。次のいずれかが発生すると、iSCSI ターゲットの到達可能性が変わります。

- ターゲットが起動またはダウンした。
- FC ターゲット設定の動的インポートが変更された。
- ゾーンセットが変更された。
- デフォルト ゾーン アクセス コントロールが変更された。
- IPS インターフェイス状態が変更された。
- イニシエータ設定変更により、ターゲットがアクセス可能または不可能になった。

iSNS クラウド検出

IP ネットワークの iSNS サーバを検出するプロセスを自動化するように iSNS クラウド検出を設定できます。

ここで説明する内容は、次のとおりです。

- 「クラウド検出の概要」(P.4-79)
- 「iSNS クラウド検出の設定」(P.4-80)

クラウド検出の概要



(注)

iSNS クラウド検出は、IBM BladeCenter および Cisco Fabric Switch for HP c-Class BladeSystem の Cisco ファブリック スイッチではサポートされていません。

iSNS サーバがクエリ要求を受信すると、iSNS サーバはイニシエータがターゲットに到達できる利用可能なターゲットとポータルのリストで応答します。MDS スイッチ外の IP ネットワーク設定により、イニシエータから到達可能なのがギガビット 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。イニシエータに返されるポータルのセットが到達可能であることを保証するためには、iSNS サーバがそのイニシエータから到達可能な一連のギガビット イーサネット インターフェイスについて認識している必要があります。

iSNS クラウド検出機能では、スイッチ上のインターフェイスを分割された IP クラウドにパーティショニングすることで、イニシエータから到達可能なさまざまなインターフェイスについての情報を iSNS サーバに提供します。この検出では、現在起動しているすべての既知の IPS ポートにメッセージを送信し、応答の有無に基づいて、リモート IPS ポートが同じ IP ネットワークにあるか異なる IP ネットワークにあるかを判断します。

次のイベントの発生時に、クラウド検出が開始されます。

- CLI からの手動要求が CLI からのクラウド検出を開始した。このアクションを実行すると、既存のメンバシップが破壊され、新しいメンバシップが作成されます。
- インターフェイスの自動検出では、正しいクラウドにインターフェイスが割り当てられます。その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シップは増分的に構築され、次のイベント時に開始されます。
 - ギガビット イーサネット インターフェイスが起動した。これは、ローカルとリモートのいずれのギガビット イーサネット インターフェイスも該当します。
 - 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た。
 - ポート上の VRRP 設定が変更された。

iSNS サーバは CFS を使用してすべてのスイッチにクラウドおよびメンバシップ情報を配信します。したがって、クラウドメンバシップ表示は、ファブリックのすべてのスイッチで同じになります。



(注)

CFS 配布が iSNS クラウド検出で正常に動作するためには、ファブリックのすべてのスイッチで Cisco SAN-OS リリース 3.0(1) または NX-OS 4.1(1b) 以上が稼動していなければなりません。

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。ここで説明する内容は、次のとおりです。

- 「iSNS クラウド検出のイネーブル化」(P.4-80)
- 「オンデマンド iSNS クラウド検出の開始」(P.4-80)
- 「自動 iSNS クラウド検出の設定」(P.4-80)

iSNS クラウド検出のイネーブル化

Fabric Manager を使用して iSNS クラウド検出をイネーブルにする場合は、次の手順に従います。

-
- ステップ 1** [End Devices] > [iSNS] を選択します。
[Information] ペインに iSNS 設定が表示されます。
- ステップ 2** [Control] タブをクリックして、クラウド検出機能の [Command] ドロップダウン メニューから [enable] を選択します。
- ステップ 3** [Apply Changes] アイコンをクリックして、この変更を保存します。
-

オンデマンド iSNS クラウド検出の開始

Fabric Manager を使用してオンデマンド iSNS クラウド検出を開始する場合は、次の手順に従います。

-
- ステップ 1** [End Devices] > [iSNS] を選択します。
[Information] ペインに iSNS 設定が表示されます。
- ステップ 2** [Cloud Discovery] タブをクリックして、[Manual Discovery] チェックボックスをオンにします。
- ステップ 3** [Apply Changes] アイコンをクリックして、この変更を保存します。
-

自動 iSNS クラウド検出の設定

Fabric Manager を使用して自動 iSNS クラウド検出をイネーブルにする場合は、次の手順に従います。

-
- ステップ 1** [End Devices] > [iSNS] を選択します。
[Information] ペインに iSNS 設定が表示されます。
- ステップ 2** [Cloud Discovery] タブをクリックして、[AutoDiscovery] チェックボックスをオンにします。
- ステップ 3** [Apply Changes] アイコンをクリックして、この変更を保存します。
-

iSNS クラウド検出配布の設定

Fabric Manager を使用して iSNS クラウド検出 CFS 配布をイネーブルにする場合は、次の手順に従います。

-
- ステップ 1** [End Devices] > [iSNS] を選択します。
[Information] ペインに iSNS 設定が表示されます。
- ステップ 2** [CFS] タブをクリックして、クラウド検出機能の [Admin] ドロップダウン メニューから [enable] を選択します。
- ステップ 3** クラウド検出機能の [Global] ドロップダウン メニューから、[enable] を選択します。
- ステップ 4** [Apply Changes] アイコンをクリックして、この変更を保存します。
-

デフォルト設定

表 4-2 に、iSCSI パラメータのデフォルト設定を示します。

表 4-2 デフォルト iSCSI パラメータ

パラメータ	デフォルト
TCP 接続数	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 回の再送信
PMTU 検出	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	パケット送信なし
TCP 輻輳ウィンドウの監視	イネーブル
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 へのターゲット ファイバ チャンネル	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、PortChannel インターフェイス、および PortChannel サブインターフェイスでアドバタイズ
仮想ファイバ チャンネル ホストへの iSCSI ホスト マッピング	動的マッピング

表 4-2 デフォルト iSCSI パラメータ (続き)

パラメータ	デフォルト
動的 iSCSI イニシエータ	VSAN 1 のメンバー
イニシエータの識別	iSCSI ノード名
静的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 イニシエータが要求を送信するときに自動的にイネーブル。この機能は store-and-forward モードでは設定および使用できません。
iSNS 登録間隔	60 秒 (設定不可)
iSNS 登録間隔の再試行	3
ファブリック配信	ディセーブル

表 4-3 に、iSLB パラメータのデフォルト設定を示します。

表 4-3 デフォルト iSLB パラメータ

パラメータ	デフォルト
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



CHAPTER 5

IP サービスの設定

Cisco MDS 9000 ファミリー スイッチは、イーサネットとファイバ チャンネル 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 ファミリー スイッチは、Network Management System (NMS; ネットワーク管理システム) に関する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 チャンネル 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 チャンネル上で 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 チャンネル 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 チャンネル 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 Virtual Router Redundancy Protocol (VRRP; 仮想ルータ冗長プロトコル) 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) IPv6 の設定については、第 8 章「ギガビット イーサネット インターフェイスの IP バージョン 6 (IPv6) の設定」を参照してください。

この章の内容は、次のとおりです。

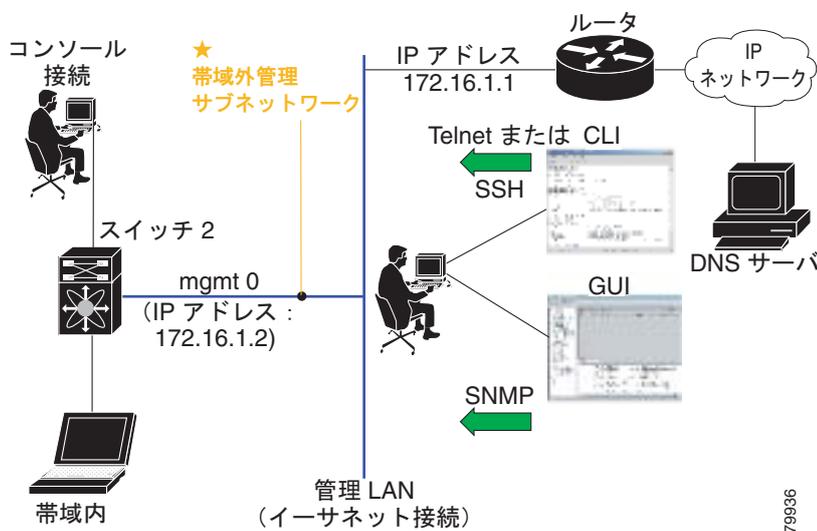
- 「トラフィック管理サービス」(P.5-2)
- 「管理インターフェイスの設定」(P.5-2)
- 「デフォルト ゲートウェイ」(P.5-3)
- 「IPv4 デフォルト ネットワークの設定」(P.5-6)
- 「IPFC」(P.5-7)
- 「IPv4 スタティック ルート」(P.5-8)
- 「オーバーレイ VSAN」(P.5-8)
- 「複数の VSAN の設定」(P.5-10)
- 「仮想ルータ冗長プロトコル」(P.5-11)

- 「DNS サーバの設定」(P.5-15)
- 「デフォルト設定」(P.5-15)

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 プロトコルが稼動する 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、帯域内管理を実行できます (図 5-1 を参照してください)。

図 5-1 スイッチへのアクセスの管理



管理インターフェイスの設定

スイッチ上の管理インターフェイスでは、同時に複数の Telnet または SNMP セッションが利用できます。スイッチは、管理インターフェイスを介してリモートで設定できますが、スイッチにアクセスできるようにするには、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クス長を設定する必要があります。IPv6 アドレスの設定については、第 8 章「ギガビットイーサネットインターフェイスの IP バージョン 6 (IPv6) の設定」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 管理イーサネット インターフェイスが接続されるイーサネット スイッチのポートは、スイッチポートではなく、ホストポート（アクセスポートとも呼ばれます）として設定します。（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はディセーブルにしてください。このようにすることで、イネーブルの場合に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遅延による MDS 管理ポートの遅延を避けることができます。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。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。

Device Manager を使用して IPv6 用に mgmt0 イーサネット インターフェイスを設定する手順は、次のとおりです。

- ステップ 1 [Interface] > [Mgmt] > [Mgmt0] を選択します。
- ステップ 2 説明を入力します。
- ステップ 3 インターフェイスの管理状態を選択します。
- ステップ 4 [CDP] チェックボックスをオンにして、CDP をイネーブルにします。
- ステップ 5 IP アドレス マスクを入力します。
- ステップ 6 [Apply] をクリックして、変更を適用します。

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。

ここで説明する内容は、次のとおりです。

- 「デフォルト ゲートウェイの概要」 (P.5-3)
- 「デフォルト ゲートウェイの設定」 (P.5-4)

デフォルト ゲートウェイの概要

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。



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。

デフォルト ゲートウェイの設定

Device Manager を使用して IP ルートを設定する手順は、次のとおりです。

- ステップ 1** [Switches] > [Interfaces] > [Management] を選択して、[Physical Attributes] ペインで [IP] を選択します。
- ステップ 2** [Information] ペインで [Route] タブをクリックします。
- 図 5-2 に示すように、各 IP ルートのスイッチ名、宛先、マスク、ゲートウェイ、メトリック、インターフェイス、およびアクティブ ステータスを示す [IP Route] ウィンドウが表示されます。

図 5-2 複数のスイッチの IP ルート

Switch	Destination, Mask, Gateway	Metric	Interface	Active
sw172-22-46-221	default, 0, 172.22.46.1	1	mgmt0	true
sw172-22-46-182	default, 0, 172.22.46.1	0	mgmt0	true
sw172-22-46-224	default, 0, 172.22.46.1	0	mgmt0	true
sw172-22-47-167	default, 0, 172.22.46.1	0	mgmt0	true
sw172-22-47-132	default, 0, 172.22.46.1	0	mgmt0	true
sw172-22-46-222	default, 0, 172.22.46.1	0	mgmt0	true
sw172-22-46-225	default, 0, 172.22.46.1	0	mgmt0	true
sw172-22-46-223	default, 0, 172.22.46.1	1	mgmt0	true
sw172-22-46-174	default, 0, 172.22.46.1	1	mgmt0	true
sw172-22-47-133	default, 0, 172.22.46.1	0	mgmt0	true
sw172-22-46-233	default, 0, 172.22.46.1	0	mgmt0	true

- ステップ 3** [Create Row] アイコンをクリックして、新しい IP ルートを追加します。
- 図 5-3 のようなダイアログボックスが表示されます。

図 5-3 [User-Defined Command] ダイアログボックス

Switch: sw-dc4-i-151
 RouteDest: 10.1.1.0
 Mask: 24
 Gateway: 10.1.1.2
 Metric: 1
 Interface: cpp1/1/1

Buttons: Create, Close

Success.

- ステップ 4** このウィンドウのフィールドに入力します。
- [Switch] フィールドにスイッチ名を入力します。
 - [Routedest] および [Mask] フィールドに宛先ネットワーク ID およびサブネット マスクを入力し、スタティック ルートを設定します。
 - [Gateway] フィールドにシードスイッチの IP アドレスを入力し、デフォルト ゲートウェイを設定します。
 - [Metric] および [Interface] フィールドを設定します。



(注) Cisco NX-OS リリース 4.2(1) 以降の場合、新しい IP ルートを作成するときに CPP インターフェイスを選択することもできます。

ステップ 5 [Create] アイコンをクリックします。

Device Manager を使用して IP ルートの設定またはデフォルト ゲートウェイの識別を行う手順は、次のとおりです。

ステップ 1 [IP] > [Routes] を選択します。

[IP Routes] ウィンドウが表示されます。

ステップ 2 [Create] をクリックして、スイッチの新しい IP ルートを作成、またはデフォルト ゲートウェイを識別します。

図 5-4 のようなダイアログボックスが表示されます。

図 5-4 [User-Defined Command] ダイアログボックス



ステップ 3 このウィンドウのフィールドに入力します。

- [Switch] フィールドにスイッチ名を入力します。
- [Routedest] および [Mask] フィールドに宛先ネットワーク ID およびサブネット マスクを入力し、スタティック ルートを設定します。
- [Gateway] フィールドにシード スイッチの IP アドレスを入力し、デフォルト ゲートウェイを設定します。
- [Metric] および [Interface] フィールドを設定します。



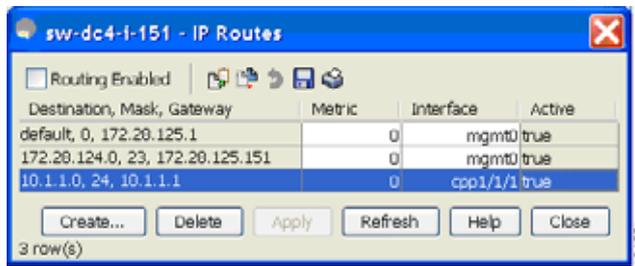
(注) Cisco NX-OS リリース 4.2(1) 以降の場合、新しい IP ルートを作成するときに CPP インターフェイスを選択することもできます。

CPP インターフェイスを選択した場合、スイッチは、入力 CPP により割り当てられる IP アドレスおよびマスクを使用して IP ルート プレフィクスを生成します。

ステップ 4 [Create] をクリックして IP ルートを追加します。

新しい IP ルートが作成されます (図 5-5 を参照してください)。

図 5-5 [IP Routes] ウィンドウ



(注) スイッチにより生成される CPP インターフェイスの IP ルートを削除することはできません。CPP インターフェイスの IP ルートを削除しようとすると、SNMP により次に示すエラー メッセージが表示されます。

```
ip: route type not supported.
```

IPv4 デフォルト ネットワークの設定

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)。



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 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 IP 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、必ず、すべてのエントリに IPv4 アドレスを設定してください。

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このほかのスイッチも、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 アドレスを設定する必要があります (図 5-6 を参照してください)。

図 5-6 オーバーレイ VSAN 機能

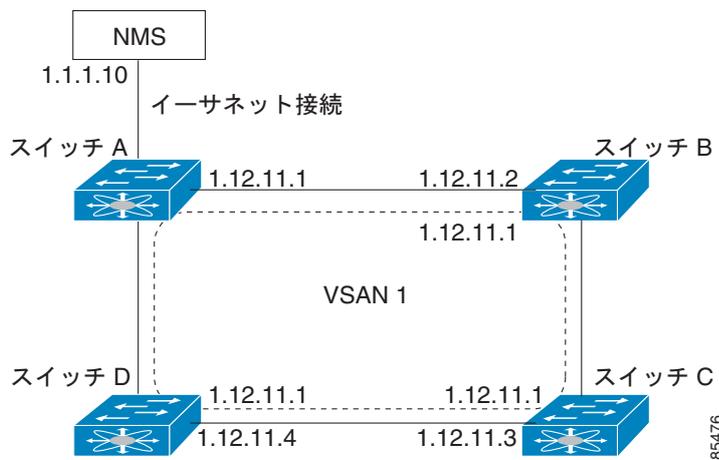


図 5-1 で、スイッチ A の IPv4 アドレスは 1.12.11.1、スイッチ B の IPv4 アドレスは 1.12.11.2、スイッチ C の IPv4 アドレスは 1.12.11.3、スイッチ D の IPv4 アドレスは 1.12.11.4 です。スイッチ A はイーサネット接続されたゲートウェイ スイッチです。NMS は IPv4 アドレス 1.1.1.10 を使用して、ゲートウェイ スイッチに接続しています。オーバーレイされた VSAN 1 内の任意のスイッチに転送されるフレームは、ゲートウェイ スイッチを通してルーティングされます。他のスイッチにゲートウェイ スイッチの IPv4 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。

IPFC

IPFC は、ファイバチャネル インターフェイス経由の IP 転送または (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なく) 帯域内スイッチ管理を提供します。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。



(注)

Cisco MDS 9000 ファミリー スイッチで IPv6 を設定する方法については、第 8 章「ギガビットイーサネット インターフェイスの IP バージョン 6 (IPv6) の設定」を参照してください。

IPFC 設定時の注意事項

IPFC を設定する場合は、次の注意事項に従ってください。

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。

IPv4 スタティック ルート

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。



(注) 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、[第 8 章「ギガビットイーサネット インターフェイスの IP バージョン 6 \(IPv6\) の設定」](#)を参照してください。

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。

オーバーレイ VSAN

ここでは、オーバーレイ VSAN およびオーバーレイ VSAN の設定方法について説明します。

ここで説明する内容は、次のとおりです。

- [「オーバーレイ VSAN の概要」\(P.5-8\)](#)
- [「オーバーレイ VSAN の設定」\(P.5-9\)](#)

オーバーレイ VSAN の概要

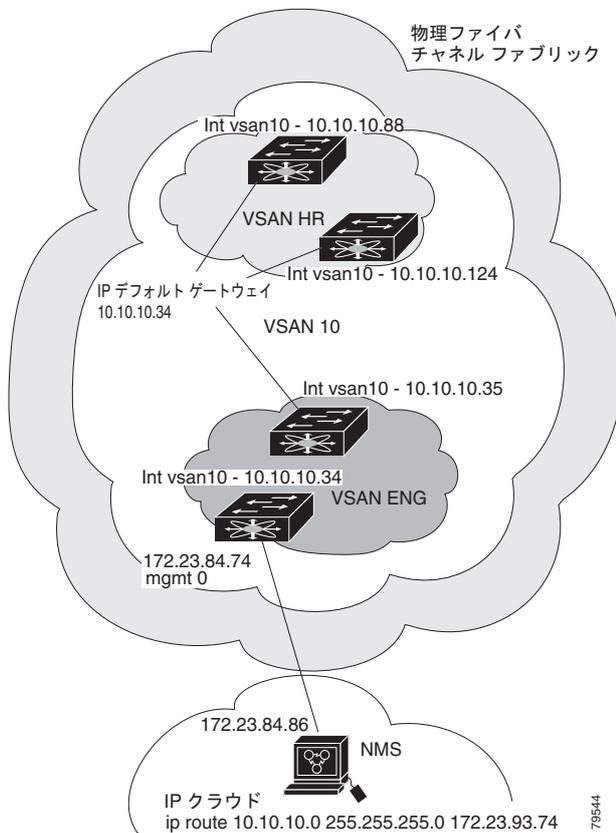
VSAN では、個別のファブリック サービス インスタンスを実行する複数の論理 SAN を 1 つの大規模な物理ネットワーク上でオーバーレイすることにより、より大規模な SAN を構成できます。このようなファブリック サービスの分離によって、ファブリックの再構成やエラー状態が個々の VSAN 内に限定されるため、ネットワークの安定性が向上します。また、物理的に分離された SAN と同じように、各 VSAN を隔離することができます。トラフィックが VSAN 境界を通過したり、デバイスが複数の VSAN に属したりすることはできません。VSAN ごとにファブリック サービスのインスタンスが個別に実行されるため、各 VSAN には独自のゾーン サーバが設定され、VSAN 機能を使用しなくても SAN とまったく同じ方法でゾーンを設定できます。

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。

- ステップ 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。
- ステップ 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。
- ステップ 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。
- ステップ 4** 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 アドレスを設定します (図 5-7 を参照してください)。

図 5-7 オーバーレイ VSAN の設定例



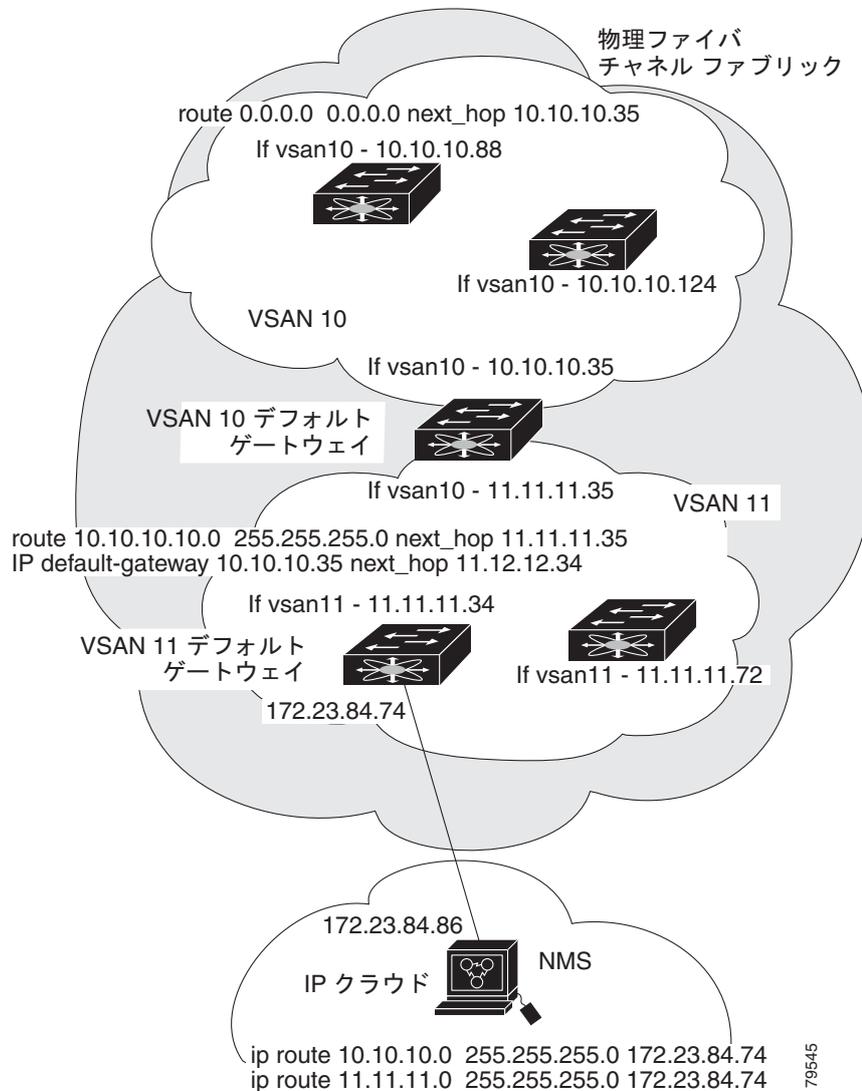
複数の VSAN の設定

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することができます。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する必要があります。

複数の VSAN を設定する手順は、次のとおりです。

- ステップ 1** ファブリック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。
- ステップ 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。
- ステップ 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。
- ステップ 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(図 5-8 を参照してください)。

図 5-8 複数の VSAN の設定例



仮想ルータ冗長プロトコル

Cisco MDS 9000 ファミリー スイッチは、仮想ルータ冗長プロトコル (VRRP) 機能の RFC 2338 標準に準拠しています。ここでは、VRRP 機能について詳細に説明します。

ここで説明する内容は、次のとおりです。

- 「VRRP の概要」(P.5-11)
- 「VRRP の設定」(P.5-13)

VRRP の概要

VRRP を使用すると、NMS に接続されているゲートウェイ スイッチへの冗長な代替パスが確立されます。VRRP には次の特性および利点があります。

- VRRP は再起動可能なアプリケーションです。
- VRRP マスターに障害が発生すると、アドバタイズが 3 回行われるまでの間に、VRRP バックアップが処理を引き継ぎます。
- VRRP over Ethernet、VRRP over VSAN、およびファイバ チャネルの機能は、RFC 2338 および draft-ietf-vrrp-ipv6 の定義に従って実装されます。
- Virtual Router (VR; 仮想ルータ) は一意の仮想ルータ IP、仮想ルータ MAC、および VR ID によって、各 VSAN、およびイーサネット インターフェイスにマッピングされます。
- 別の仮想ルータ IP マッピングを使用することにより、VR ID を複数の VSAN で再利用することができます。
- IPv4 および IPv6 の両方がサポートされています。
- 管理インターフェイス (mgmt 0) は仮想ルータ グループを 1 つだけサポートしています。他のすべてのインターフェイスは、IPv4 と IPv6 を合わせて、最大 7 つの仮想ルータ グループをサポートしています。各 VSAN には最大で 255 個の仮想ルータ グループを割り当てることができます。
- VRRP セキュリティには、認証なし、単純なテキスト認証、および MD5 認証の 3 つのオプションがあります。



(注) IPv6 を使用している場合は、インターフェイスに IPv6 アドレスを設定するか、またはインターフェイスで IPv6 をイネーブルにする必要があります。IPv6 の詳細については、[第 8 章「ギガビットイーサネット インターフェイスの IP バージョン 6 \(IPv6\) の設定」](#)を参照してください。

[図 5-9](#) で、スイッチ A は VRRP マスター スイッチ、スイッチ B は VRRP バックアップ スイッチです。両方のスイッチに、IP アドレスと VRRP のマッピングが設定されています。その他のスイッチでは、スイッチ A がデフォルト ゲートウェイとして設定されます。スイッチ A に障害が発生すると、スイッチ B が自動的にマスターになり、ゲートウェイ機能を引き継ぐため、他のスイッチのルーティング設定を変更する必要はありません。

図 5-9 VRRP の機能

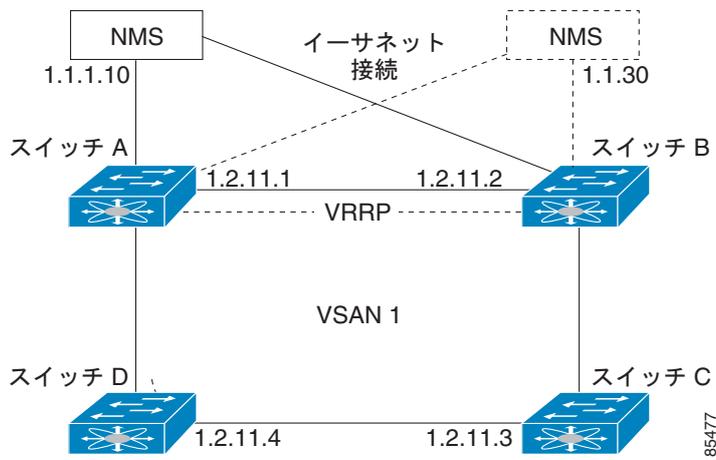
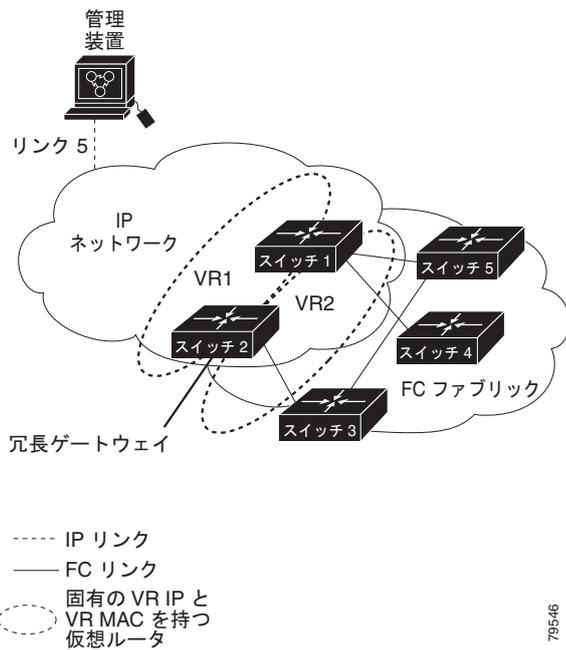


図 5-10 のファブリック例では、複数のインターフェイスタイプにまたがる仮想ルータを設定できないため、2 つの仮想ルータ グループ (VR 1 および VR 2) が存在します。スイッチ 1 とスイッチ 2 の両方で、イーサネット インターフェイスは VR 1 内に、FC インターフェイスは VR 2 内にあります。各仮想ルータは、VSAN インターフェイスおよび VR ID によって一意に識別されます。

図 5-10 冗長ゲートウェイ



VRRP の設定

ここでは VRRP を設定する方法について説明します。ここで説明する内容は、次のとおりです。

- 「仮想ルータの追加および削除」(P.5-13)
- 「仮想ルータの起動」(P.5-13)
- 「仮想ルータ IP アドレスの追加」(P.5-13)
- 「仮想ルータのプライオリティの設定」(P.5-14)
- 「アダプタイズ パケットのタイム インターバルの設定」(P.5-14)
- 「プライオリティのプリエンプトの設定またはイネーブル化」(P.5-14)
- 「仮想ルータの認証の設定」(P.5-14)
- 「インターフェイスのステート追跡に基づいたプライオリティ」(P.5-15)

仮想ルータの追加および削除

すべての VRRP の設定は、VRRP が稼動するファブリック内のスイッチ間で複製する必要があります。



(注)

ギガビット イーサネット ポートに設定できる VRRP グループの総数は、メイン インターフェイスとサブインターフェイスを合わせて、7 グループまでです。この制限は、IPv4 グループおよび IPv6 グループの両方に適用されます。

仮想ルータの起動

デフォルトで、仮想ルータは常にディセーブルです。VRRP を設定できるのは、この状態がイネーブルの場合だけです。VR をイネーブルにする前に、少なくとも 1 つの IP アドレス (IPv4 または IPv6) を設定してください。

仮想ルータ IP アドレスの追加

仮想ルータには、1 つの仮想ルータ IP アドレスを設定できます。設定された IP アドレスがインターフェイス IP アドレスと同じである場合、このスイッチは自動的に IP アドレスを所有します。IPv4 アドレスまたは IPv6 アドレスのいずれかを設定できます。

VRRP 仕様に従うと、仮想ルータはパケットを転送するネクスト ホップ ルータであるため、マスター VRRP ルータは仮想ルータの IP アドレスへ送信されたパケットを削除します。ただし、MDS スイッチでは、アプリケーションが、仮想ルータの IP アドレスへ送信されたパケットを受け付け、アプリケーションへ配信することを要求する場合があります。仮想ルータ IPv4 アドレスの **secondary** オプションを使用すると、VRRP ルータは、マスターである場合、これらのパケットを受け入れます。

Device Manager で仮想ルータの IP アドレスを管理する場合は、次の手順を実行します。

- ステップ 1** [IP] > [VRRP] を選択します。[VRRP] ダイアログボックスに [Operations] タブが表示されます。
- ステップ 2** [VRRP] ダイアログボックスの [IP Addresses] タブをクリックします。

- ステップ 3** 新しい VRRP エントリを作成するには、[Create] をクリックします。[Create VRRP IP Addresses] ウィンドウが表示されます。
- ステップ 4** このウィンドウのフィールドに入力し、新しい VRRP IP アドレスを作成して、[OK] または [Apply] をクリックします。

仮想ルータのプライオリティの設定

仮想ルータのプライオリティには、1 ~ 254 を割り当てることができます。1 が最低プライオリティ、254 が最高プライオリティです。セカンダリ IP アドレスを持つスイッチのデフォルト値は 100、プライマリ IP アドレスを持つスイッチのデフォルト値は 255 です。

アドバタイズ パケットのタイム インターバルの設定

IPv4 を使用するインターフェイスでは、アドバタイズ パケットのタイム インターバルの有効範囲は、1 ~ 255 秒です。デフォルト値は 1 秒です。スイッチにプライマリ IP アドレスが設定されている場合は、この期間を指定する必要があります。

プライオリティのプリエンプトの設定またはイネーブル化

プライオリティが高いバックアップ仮想ルータが、プライオリティの低いマスター仮想ルータをプリエンプトできるようにします。



(注) 仮想 IP アドレスがインターフェイスの IP アドレスでもある場合、プリエンプトは暗黙的に適用されません。



(注) VRRP のプリエンプトは、IP ストレージの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ません。

仮想ルータの認証の設定

VRRP セキュリティには、単純なテキスト認証、MD5 認証、および認証なしの 3 つのオプションがあります。

- 単純なテキスト認証の場合は、同じ仮想ルータに参加するすべてのスイッチで、1 ~ 8 文字の一意のパスワードを使用します。このパスワードは、他のセキュリティ パスワードと異なるものに設定する必要があります。
- MD5 認証の場合は、同じ仮想ルータに参加するすべてのスイッチで、16 文字の一意の鍵を使用します。この秘密鍵は、同じ仮想ルータ内のすべてのスイッチで共有されます。
- デフォルトのオプションは、認証なしです。

VRRP サブモードで認証オプションを使用して鍵を設定したり、コンフィギュレーション ファイルを使用して鍵を配布したりすることができます。このオプションで割り当てられた Security Parameter Index (SPI; セキュリティ パラメータ インデックス) 設定は、VSAN ごとに一意でなければなりません。



(注) すべての VRRP 設定を複製する必要があります。



(注) VRRP ルータ認証は、IPv6 には適用されません。

インターフェイスのステート追跡に基づいたプライオリティ

インターフェイスのステート追跡機能では、スイッチ内の他のインターフェイスのステートに基づいて、仮想ルータのプライオリティが変更されます。追跡対象のインターフェイスがダウンすると、プライオリティは仮想ルータのプライオリティ値に戻ります（「[仮想ルータのプライオリティの設定](#)」(P.5-14) を参照してください)。追跡対象のインターフェイスが起動すると、仮想ルータのプライオリティはインターフェイスのステート追跡機能の値に戻ります。指定された VSAN インターフェイスまたは管理インターフェイス (mgmt 0) のいずれかのステートを追跡できます。インターフェイスのステート追跡機能は、デフォルトではディセーブルです。



(注) インターフェイス追跡機能を使用するには、インターフェイスでプリエンプトをイネーブルにする必要があります。「[プライオリティのプリエンプトの設定またはイネーブル化](#)」(P.5-14) を参照してください。

DNS サーバの設定

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 サーバは、次のいずれかの場合、2 回試行された後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
- 外的要因により（制御不可能な理由により）DNS サーバに到達できない



(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 サーバが正しく設定されていて、到達可能であるかを確認してください。

デフォルト設定

表 5-1 に、DNS 機能のデフォルト設定を示します。

表 5-1 DNS のデフォルト設定

パラメータ	デフォルト
ドメインルックアップ	ディセーブル
ドメイン名	ディセーブル
ドメイン	なし

表 5-1 DNS のデフォルト設定 (続き)

パラメータ	デフォルト
ドメイン サーバ	なし
最大ドメイン サーバ	6

表 5-2 に、VRRP 機能のデフォルト設定を示します。

表 5-2 VRRP のデフォルト設定

パラメータ	デフォルト
仮想ルータ状態	ディセーブル
VSAN 当たりの最大グループ数	255
ギガビットイーサネットポート当たりの最大グループ数	7
プライオリティのプリエンプト	ディセーブル
仮想ルータのプライオリティ	セカンダリ IP アドレスを持つスイッチは 100 プライマリ IP アドレスを持つスイッチは 255
プライオリティ インターフェイス追跡機能	ディセーブル
アドバタイズ インターバル	IPv4 は 1 秒 IPv6 は 100 センチ秒



CHAPTER 6

IP ストレージの設定

Cisco MDS 9000 ファミリの IP Storage (IPS; IP ストレージ) 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して、ファイバチャネル Storage Area Network (SAN; ストレージエリアネットワーク) の到達距離を延長します。スイッチは Fibre Channel over IP (FCIP) を使用して各 SAN アイランドを接続し、iSCSI プロトコルを使用して 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 および iSCSI 機能は IPS モジュール固有であり、Cisco MDS 9200 スイッチまたは Cisco MDS 9500 ディレクタで使用できます。

Cisco MDS 9216I、スイッチおよび 14/2 Multiprotocol Services (MPS-14/2) モジュールを使用すると、ファイバチャネル、FCIP、および iSCSI 機能を使用できます。MPS-14/2 モジュールは、Cisco MDS 9200 シリーズまたは Cisco MDS 9500 シリーズのどのスイッチでも使用できます。

この章の内容は、次のとおりです。

- 「サービス モジュール」 (P.6-1)
- 「サポートされているハードウェア」 (P.6-3)
- 「IPv4 のギガビット イーサネット インターフェイスの設定」 (P.6-4)
- 「ギガビット イーサネットのハイアベイラビリティの設定」 (P.6-8)
- 「Cisco Discovery Protocol (CDP) の設定」 (P.6-11)
- 「デフォルト設定」 (P.6-11)

サービス モジュール

IP ストレージ サービス モジュール (IPS モジュール) および MPS-14/2 モジュールを使用すると、FCIP および iSCSI 機能が使用可能になります。これらのモジュールは Cisco MDS 9000 ファミリーと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機能をすべてサポートします。現在、次のタイプのストレージ サービス モジュールが、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。

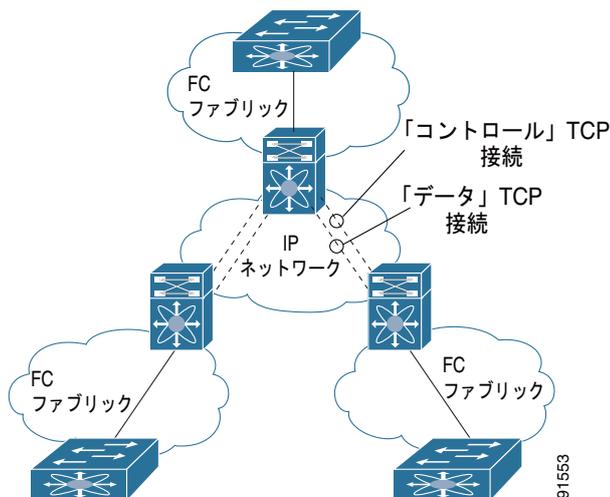
- 4 ポートのホットスワップ可能な IPS モジュール (IPS-4) : 4 つのギガビット イーサネット ポートを備えています。
- 8 ポートのホットスワップ可能な IPS モジュール (IPS-8) : 8 つのギガビット イーサネット ポートを備えています。

- MPS-14/2 モジュール：14 のファイバチャネルポート（ポート番号 1 ～ 14）と 2 つのギガビットイーサネットポート（ポート番号 1 および 2）を備えています。

これらのモジュールのギガビットイーサネットポートは、FCIP プロトコルまたは iSCSI プロトコルをサポートするように設定できます。また、FCIP と iSCSI の両方のプロトコルを同時にサポートするように設定することもできます。

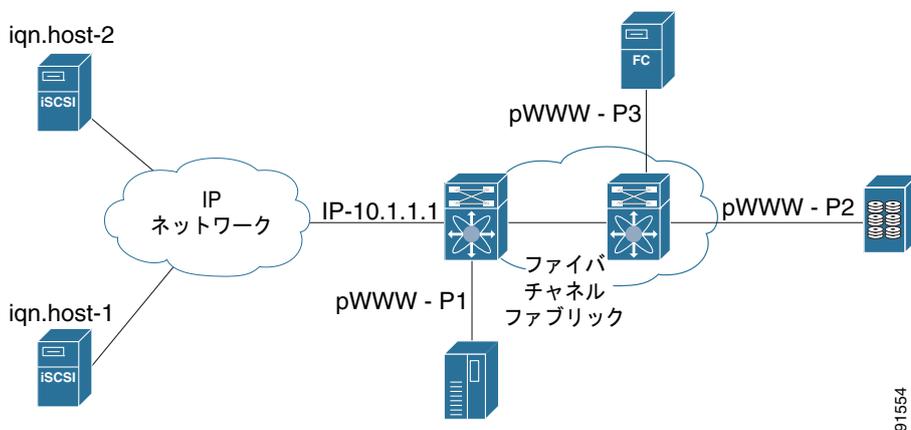
- FCIP：IP ネットワークを介して、2 台の Cisco MDS 9000 ファミリスイッチ間で、またはその他の FCIP 標準準拠のデバイス間で、ファイバチャネルフレームを透過的に転送します。図 6-1 に、IPS モジュールを使用する FCIP の例を示します。

図 6-1 FCIP の例



- iSCSI：IPS モジュールは、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アクセスを可能にします。IP ホストは SCSI コマンドを iSCSI Protocol Data Unit (PDU; プロトコルデータユニット) にカプセル化し、TCP/IP 接続を介して Cisco MDS 9000 ファミリスイッチ IPS ポートに送信します。この時点で、コマンドは IP ネットワークからファイバチャネルネットワークにルーティングされて、宛先に転送されます。図 6-2 に、IPS モジュールが使用される iSCSI の例を示します。

図 6-2 iSCSI の例



モジュール ステータスの確認

Fabric Manager を使用してモジュールのステータスを確認する手順は、次のとおりです。

-
- ステップ 1** [Fabric] ペインでスイッチを選択します。
- ステップ 2** [Switches] フォルダを開き、[Physical Attributes] ペインで [Hardware] を選択します。
[Information] ペインに、スイッチのすべてのモジュールのステータスが表示されます。
-

IPS モジュールのアップグレード



注意

IPS モジュールのソフトウェア アップグレードは中断を伴います。NX-OS ソフトウェアでは、スイッチに搭載されたファイバチャネル モジュールおよびスイッチ自体のソフトウェアの場合、アップグレードで中断は発生しません。

IPS モジュールはローリング アップグレード インストール メカニズムを使用するため、特定のスイッチ内の各モジュールは順にアップグレードする必要があります。安定した状態を確保するために、スイッチの IPS モジュールをアップグレードしてから次の IPS モジュールをアップグレードするまでに 5 分間の間隔が必要です。

MPS-14/2 モジュールのアップグレード



注意

MPS-14/2 モジュールのソフトウェア アップグレードは部分的な中断を伴います。NX-OS ソフトウェアでは、スイッチに搭載されたファイバチャネル モジュールおよびスイッチ自体のソフトウェアの場合、アップグレードで中断は発生しません。

MPS-14/2 モジュールは、14 のファイバチャネル ポート（アップグレード時に中断しない）と 2 つのギガビットイーサネット ポート（アップグレード時に中断する）を備えています。MPS-14/2 モジュールは、2 つのギガビットイーサネット ポートに対してローリング アップグレード インストール メカニズムを使用するため、特定のスイッチ内の各モジュールは順にアップグレードする必要があります。安定した状態を確保するために、スイッチの MPS-14/2 モジュールをアップグレードしてから次のモジュールをアップグレードするまでに 5 分間の間隔が必要です。

サポートされているハードウェア

次のハードウェアを 1 つ以上使用して、FCIP および iSCSI 機能を設定できます。

- IPS-4 または IPS-8 モジュール（詳細については、『Cisco MDS 9200 Series Hardware Installation Guide』または『Cisco MDS 9500 Series Hardware Installation Guide』を参照してください）
- MPS-14/2 モジュール（詳細については、『Cisco MDS 9200 Series Hardware Installation Guide』または『Cisco MDS 9500 Series Hardware Installation Guide』を参照してください）



(注) MPS-14/2 モジュールおよび Cisco MDS 9216i 統合型スーパーバイザ モジュールでは、ファイバチャネルポートとギガビットイーサネットポートでポート番号が異なります。ファイバチャネルポートはポート番号 1 ~ 14 で、ギガビットイーサネットポートはポート番号 1 および 2 です。

- Cisco MDS 9216i スイッチ (詳細については、『Cisco MDS 9200 Series Hardware Installation Guide』を参照してください)

IPv4 のギガビットイーサネットインターフェイスの設定

FCIP および iSCSI はいずれもネットワーク接続に TCP/IP を使用します。各 IPS モジュールまたは MPS-14/2 モジュールでは、接続は、適切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形式で提供されます。ここでは、FCIP および iSCSI で使用できるように IP を設定する手順について説明します。



(注) FCIP の設定については、第 2 章「FCIP の設定」を参照してください。iSCSI の設定については、第 4 章「iSCSI の設定」を参照してください。

新しいポートモード (IPS) は、各 IPS モジュールまたは MPS-14/2 モジュールのギガビットイーサネットポートに定義されています。IP ストレージポートは、暗黙的に IPS モードに設定されるため、iSCSI および FCIP ストレージ機能を実行するためだけに使用できます。IP ストレージポートは、イーサネットフレームのブリッジまたは他の IP パケットのルートは実行しません。

各 IPS ポートは、ファイバチャネル SAN のシングル仮想ファイバチャネルホストを表します。この IPS ポートに接続されるすべての iSCSI ホストは、シングルファイバチャネルホストを介して結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を必要とする大規模な 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) MPS-14/2 モジュールで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。



(注) ギガビットイーサネットインターフェイスで IPv6 を設定するには、『Cisco Fabric Manager Security Configuration Guide』を参照してください。



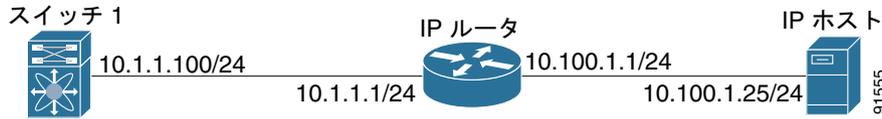
ヒント

IPS モジュールまたは 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。

ギガビットイーサネットの基本設定

図 6-3 に、基本的なギガビットイーサネット IP バージョン 4 (IPv4) 設定の例を示します。

図 6-3 ギガビットイーサネット IPv4 の設定例



(注)

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はディセーブルにしてください。これにより、スパニングツリー設定がイネーブルの場合に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のために発生す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。

図 6-3 のシナリオのギガビットイーサネットインターフェイスを設定する手順は、次のとおりです。

- ステップ 1** Fabric Manager から、[Physical Attributes] ペインで [Switches] > [Interfaces] > [Gigabit Ethernet] を選択します。[Information] ペインにギガビットイーサネットの設定が表示されます。
Device Manager で、設定するギガビットイーサネットポートを右クリックして、[Configure...] を選択します。ギガビットイーサネットの設定ダイアログボックスが表示されます。
- ステップ 2** Fabric Manager の場合、[General] タブをクリックします。または、Device Manager の場合、[GigE] タブをクリックして、インターフェイスの通常の設定オプションを表示します。
- ステップ 3** インターフェイスの説明および Maximum Transmission Unit (MTU; 最大伝送ユニット) 値を設定します。[MTU] フィールドの有効な値は 576 ~ 9000 です。
- ステップ 4** このインターフェイスを CDP に参加させる場合は、[Admin] を [up] または [down] に設定し、[CDP] チェックボックスをオンにします。
- ステップ 5** [IpAddress/Mask] にこのインターフェイスの IP アドレスおよびサブネットマスクを設定します。
- ステップ 6** Fabric Manager で、これらの変更を保存する場合は、[Apply Changes] をクリックします。変更を廃棄する場合は、[Undo Changes] をクリックします。
Device Manager で、これらの変更を保存する場合は、[Apply] をクリックします。変更を保存せずにギガビットイーサネットの設定ダイアログボックスを閉じる場合は、[Close] をクリックします。

インターフェイスの説明の設定

任意のインターフェイスのスイッチポートの説明の設定の詳細については、『Cisco Fabric Manager Interfaces Configuration Guide』を参照してください。

ビーコン モードの設定

任意のインターフェイスのビーコン モードの設定の詳細については、『Cisco Fabric Manager Interfaces Configuration Guide』を参照してください。

自動ネゴシエーションの設定

デフォルトでは、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されています。特定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イネーブルまたはディセーブルにすることができます。自動ネゴシエーションがイネーブルの場合、ポートはスピードまたはポーズ方式、およびリンク パートナーに基づいた受信信号のデュプレックスを自動的に検出します。自動ネゴシエーション機能を使用して、リンク アップ状態を検出することもできます。

MTU フレーム サイズの設定

ポートで大規模な（またはジャンボ）フレームを転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 最大伝送ユニット（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。ポートのジャンボフレームを設定することで、MTU サイズを 9000 バイトまで増加できます。



(注)

最小 MTU サイズは 576 バイトです。



ヒント

MTU を変更すると中断が生じます。ソフトウェアで MTU サイズの変更が検出されると、すべての FCIP リンクおよび iSCSI セッションはフラップします。

無差別モードの設定

特定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またはディセーブルにすることができます。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。

ギガビットイーサネットの VLAN について

仮想 LAN (VLAN) は、物理 LAN ネットワークに複数の仮想レイヤ 2 ネットワークを作成します。VLAN は、トラフィックの分離、セキュリティ、ブロードキャスト コントロールを提供します。

ギガビットイーサネットポートは、IEEE 802.1Q VLAN カプセル化でイーサネットフレームを自動的に認識します。複数の VLAN からのトラフィックを 1 つのギガビットイーサネットポートで受信する必要がある場合、各 VLAN に 1 つずつ、サブインターフェイスを設定します。

IPS モジュールまたは MPS-14/2 モジュールがシスコ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 1 つの IPS ポートで受信する必要がある場合、イーサネットスイッチで次の要件を満たしている必要があります。

- IPS モジュールまたは MPS-14/2 モジュールに接続される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設定されている。

- カプセル化がデフォルトの ISL ではなく 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 (*slot-number / port-numberVLAN-ID*) を作成します。

インターフェイスのサブネットの要件

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 (mgmt 0) は、設定に応じて同じサブネットまたは異なるサブネットに設定できます (表 6-1 を参照してください)。

表 6-1 インターフェイスのサブネットの要件

インターフェイス 1	インターフェイス 2	同じサブネットの設定	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	可	2つのメジャーインターフェイスを同じサブネットまたは異なるサブネットに設定できます。
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	可	同じ VLAN ID の2つのサブインターフェイスを同じサブネットまたは異なるサブネットに設定できます。
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	不可	異なる VLAN ID の2つのサブインターフェイスを同じサブネットに設定することはできません。
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	不可	サブインターフェイスをメジャーインターフェイスと同じサブネットに設定することはできません。
mgmt0	ギガビットイーサネット 1/1.100	不可	mgmt0 インターフェイスを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することはできません。
mgmt0	ギガビットイーサネット 1/1	不可	



(注) 表 6-1 の設定要件はイーサネット PortChannel にも適用されます。

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。



(注) 接続に失敗した場合は、次の点を確認し、IP ホストに対して再度 PING を実行してください。

- 宛先 (IP ホスト) の IP アドレスが正しく設定されている
- ホストがアクティブである (電源が投入されている)
- IP ルートが正しく設定されている
- 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の IPv4-ACL に関する注意事項



ヒント

IPv4-ACL がギガビットイーサネットインターフェイスにすでに含まれている場合、このインターフェイスをイーサネット PortChannel グループに追加することはできません。

ギガビットイーサネットインターフェイスの IPv4-ACL を設定する場合、次の注意事項に従ってください。

- Transmission Control Protocol (TCP; 伝送制御プロトコル) または Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) だけを使用します。



(注) User Datagram Protocol (UDP; ユーザデータグラムプロトコル) および HTTP などのそ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のルールを含む 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できますが、そのルールの効果はありません。

- インターフェイスをイネーブルにする前に IPv4-ACL をインターフェイスに適用します。これにより、トラフィックフローが開始される前に、フィルタが正常であることを確認できます。
- 次の条件に注意してください。
 - **log-deny** オプションを使用する場合、毎秒最大 50 のメッセージが記録されます。
 - ギガビットイーサネット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。
 - IPv4-ACL ルールが既存の TCP 接続に適用される場合、ルールは無視されます。たとえば、A と B の間に既存の TCP 接続があり、発信元を A、宛先を B とするすべてのパケットの削除を指定する IPv4-ACL がその後で適用された場合、このルールの効果はありません。

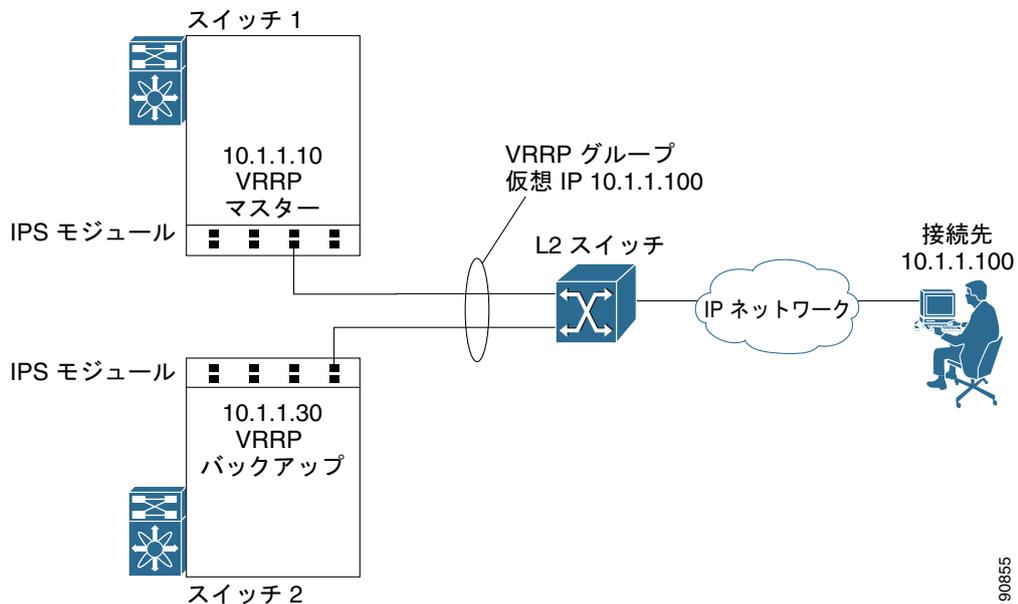
ギガビットイーサネットのハイ アベイラビリティの設定

Virtual Router Redundancy Protocol (VRRP; 仮想ルータ冗長プロトコル) およびイーサネット PortChannel 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ギガビットイーサネット機能です。

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、ギガビットイーサネット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 アドレスを代替ギガビットイーサネット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 (図 6-4 を参照してください)。

図 6-4 VRRP の例



90855

図 6-4 では、VRRP グループのメンバーは、すべて IP ストレージギガビットイーサネット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 つ以上設定できます。

- 同じ IPS モジュールまたは MPS-14/2 モジュールの 1 つ以上のインターフェイス
- 1 台のスイッチの IPS モジュールまたは MPS-14/2 モジュールのインターフェイス
- 複数のスイッチの IPS モジュールまたは MPS-14/2 モジュールのインターフェイス
- ギガビットイーサネットサブインターフェイス
- イーサネット PortChannel および PortChannel サブインターフェイス

ギガビットイーサネットインターフェイスに対する VRRP の設定



(注)

VRRP の **preempt** オプションは、IPS の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ません。ただし、仮想 IPv4 アドレスがインターフェイスの IPv4 アドレスでもある場合、プリエンプトは暗黙的に適用されます。



(注)

IPFC VSAN インターフェイスにセカンダリ VRRP IPv6 アドレスを設定する場合、Cisco リリース 3.0(1) 以前のリリースにダウングレードする前に、セカンダリ VRRP IPv6 アドレスを削除する必要があります。これは IPv6 アドレスを設定する場合にだけ必要です。

イーサネット PortChannel の集約の概要

イーサネット PortChannel は、複数の物理ギガビットイーサネットインターフェイスを単一の論理イーサネットインターフェイスに集約したものです。これにより、リンク冗長性が確保され、場合によっては集約帯域幅およびロードバランシング効率が高まります。

MDS スイッチのギガビットイーサネットポートに接続されたイーサネットスイッチでは、IP アドレス、IP アドレスと UDP/TCP ポート番号、または MAC アドレスに基づいてロードバランシングを実行できます。このロードバランシング方式では、1 つの TCP 接続からのデータトラフィックは、必ずイーサネット PortChannel の同じ物理ギガビットイーサネットポート上で伝送されます。MDS に着信するトラフィックに対して、イーサネットスイッチは、IP アドレス、送信元/宛先 MAC アドレス、または IP アドレスとポートに基づいてロードバランシングを実行できます。1 つの TCP 接続からのデータトラフィックは、常に同じ物理リンク上で伝送されます。両方のポートを発信方向で使用するには、複数の TCP 接続が必要です。

1 つの FCIP リンクのすべての FCIP 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 FCIP リンクの集約帯域幅は 1 Gbps になります。



(注)

シスコイーサネットスイッチの PortChannel は、デフォルトの 802.3ad プロトコルとしてではなく、スタティック PortChannel として設定する必要があります。

イーサネット PortChannel が集約できるのは、指定された IPS モジュール上で相互に隣接する 2 つの物理インターフェイスだけです (図 6-5 を参照してください)。



(注)

PortChannel メンバーは、ポート 1 と 2、ポート 3 と 4、ポート 5 と 6、またはポート 7 と 8 のいずれかの組み合わせでなければなりません。

図 6-5 イーサネット PortChannel の例

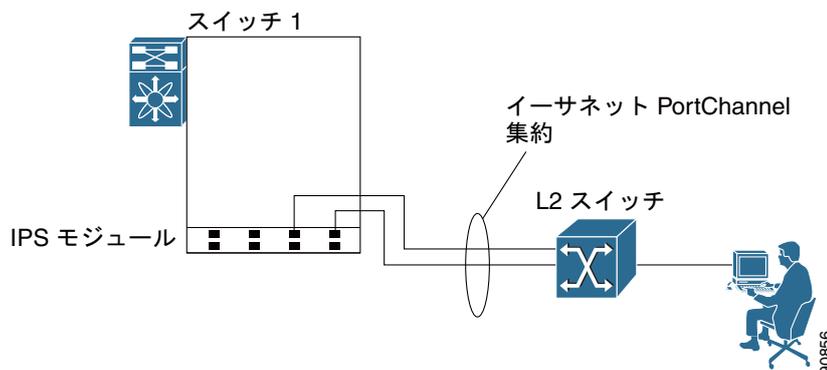


図 6-5 で、スロット 9 のギガビットイーサネットポート 3 および 4 は、イーサネット PortChannel に集約されます。イーサネット PortChannel は、MPS-14/2 モジュールおよび 9216i IPS モジュールではサポートされていません。



(注)

PortChannel インターフェイスは、ギガビットイーサネットおよびファイバチャネル用に設定することができます。ただし、PortChannel メンバシップに基づいて、ギガビットイーサネットパラメータまたはファイバチャネルパラメータだけが適用できます。

イーサネット PortChannel の設定

『Cisco Fabric Manager Interfaces Configuration Guid』で指定された PortChannel 設定は、イーサネット PortChannel 設定にも適用されます。



(注)

次のいずれかの場合は、ギガビットイーサネットインターフェイスを PortChannel に追加できません。

- インターフェイスにすでに IP アドレスが割り当てられている場合
- このインターフェイスにサブインターフェイスが設定されている場合
- インターフェイスに IPv4-ACL ルールが適用されていて、PortChannel には IPv4-ACL ルールが適用されていない場合

Cisco Discovery Protocol (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 モジュールまたは 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でサポートされています。

『Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide』を参照してください。

デフォルト設定

表 6-2 に、IP ストレージ サービス パラメータのデフォルト設定を示します。

表 6-2 ギガビットイーサネットのデフォルトパラメータ

パラメータ	デフォルト
IPS コア サイズ	部分



CHAPTER 7

ギガビットイーサネットインターフェイスの IP バージョン 4 (IPv4) の設定

Cisco MDS 9000 ファミリーは、ギガビットイーサネットインターフェイスの 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 機能を設定する方法について説明します。

この章の内容は、次のとおりです。

- 「IPv4 の概要」 (P.7-1)
- 「IPv4 の基本的なギガビットイーサネットの設定」 (P.7-2)
- 「VLAN」 (P.7-5)
- 「IPv4-ACL」 (P.7-6)
- 「デフォルト設定」 (P.7-7)

IPv4 の概要

FCIP および iSCSI はいずれもネットワーク接続に TCP/IP を使用します。各 IPS モジュールまたは MPS-14/2 モジュールでは、接続は、適切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形式で提供されます。ここでは、FCIP および iSCSI で使用できるように IP を設定する手順について説明します。



(注)

FCIP の設定については、第 2 章「FCIP の設定」を参照してください。iSCSI の設定については、第 4 章「iSCSI の設定」を参照してください。

新しいポートモード (IPS) は、各 IPS モジュールまたは MPS-14/2 モジュールのギガビットイーサネットポートに定義されています。IP ストレージポートは、暗黙的に IPS モードに設定されるため、iSCSI および FCIP ストレージ機能を実行するためだけに使用できます。IP ストレージポートは、イーサネットフレームのブリッジまたは他の IP パケットのルートは実行しません。

各 IPS ポートは、ファイバチャネル SAN のシングル仮想ファイバチャネルホストを表します。この IPS ポートに接続されるすべての iSCSI ホストは、シングルファイバチャネルホストを介して結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) MPS-14/2 モジュールで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。



(注) ギガビットイーサネットインターフェイスで IPv6 を設定するには、「IPv6 アドレッシングの設定および IPv6 ルーティングのイネーブル化」(P.8-11) を参照してください。



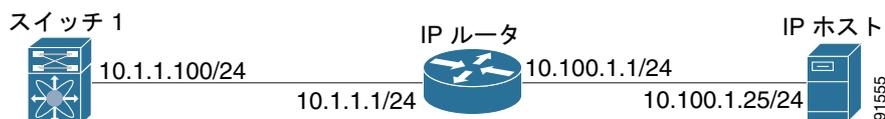
ヒント

IPS モジュールまたは 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に設定しないでください。これらは、別のスタンドアロンハブやスイッチまたは別の VLAN のいずれかを使用して、異なるブロードキャストドメインに設定してください。

IPv4 の基本的なギガビットイーサネットの設定

図 7-1 に、基本的なギガビットイーサネット IP バージョン 4 (IPv4) 設定の例を示します。

図 7-1 ギガビットイーサネット IPv4 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の場合に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のために発生す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。

Fabric Manager 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設定する手順は、次のとおりです。

- ステップ 1 [Switches] > [Interfaces] > [Ethernet] > [IPS] を展開します。
[Information] ペインにギガビットイーサネットの設定が表示されます。
- ステップ 2 [IP Addresses] タブをクリックします。
- ステップ 3 [Create Row] タブをクリックします。
[Create Gigabit Ethernet Interface] ダイアログボックスが表示されます。
- ステップ 4 ギガビットイーサネットインターフェイスを作成するスイッチを選択します。
- ステップ 5 インターフェイスを入力します。たとえば、スロット 2、ポート 2 の場合 2/2 です。

ステップ 6 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 7 これらの変更を保存するには、[Create] をクリックします。変更を保存せずに終了するには、[Close] をクリックします。

ここで説明する内容は、次のとおりです。

- 「インターフェイスの説明の設定」 (P.7-3)
- 「ビーコン モードの設定」 (P.7-3)
- 「自動ネゴシエーションの設定」 (P.7-3)
- 「MTU フレーム サイズの設定」 (P.7-4)
- 「無差別モードの設定」 (P.7-4)

インターフェイスの説明の設定

任意のインターフェイスのスイッチ ポートの説明の設定の詳細については、『Cisco Fabric Manager Interfaces Configuration Guide』を参照してください。

ビーコン モードの設定

任意のインターフェイスのビーコン モードの設定の詳細については、『Cisco Fabric Manager Interfaces Configuration Guide』を参照してください。

自動ネゴシエーションの設定

デフォルトでは、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されています。特定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イネーブルまたはディセーブルにすることができます。自動ネゴシエーションがイネーブルの場合、ポートはスピードまたはポーズ方式、およびリンク パートナーに基づいた受信信号のデュプレックスを自動的に検出します。自動ネゴシエーション機能を使用して、リンク アップ状態を検出することもできます。

Fabric Manager を使用して自動ネゴシエーションを設定する手順は、次のとおりです。

ステップ 1 [Switches] > [Interfaces] > [Ethernet] > [IPS] を展開します。

[Information] ペインにギガビットイーサネットの設定が表示されます。

ステップ 2 [General] タブで、特定のスイッチの [Auto Negotiate] オプションをイネーブルまたはディセーブルにすることができます。

ステップ 3 [Apply Changes] をクリックします。

MTU フレーム サイズの設定

ポートで大規模な（またはジャンボ）フレームを転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 Maximum Transmission Unit (MTU; 最大伝送ユニット) 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。ポートのジャンボ フレームを設定することで、MTU サイズを 9000 バイトまで増加できます。



(注)

最小 MTU サイズは 576 バイトです。



ヒント

MTU を変更すると中断が生じます。ソフトウェアで MTU サイズの変更が検出されると、すべての FCIP リンクおよび iSCSI セッションはフラップします。

Fabric Manager を使用して MTU フレーム サイズを設定する手順は、次のとおりです。

-
- ステップ 1** [Switches] > [Interfaces] > [Ethernet] > [IPS] を展開します。
[Information] ペインにギガビットイーサネットの設定が表示されます。
- ステップ 2** [General] タブの [Mtu] カラムで、特定のスイッチの MTU フレーム サイズを設定する新しい値を入力できます。たとえば、3000 バイトを入力できます。デフォルトは 1500 バイトです。
- ステップ 3** [Apply Changes] をクリックします。
-

無差別モードの設定

特定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またはディセーブルにすることができます。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。

Fabric Manager を使用して無差別モードを設定する手順は、次のとおりです。

-
- ステップ 1** [Switches] > [Interfaces] > [Ethernet] > [IPS] を展開します。
[Information] ペインにギガビットイーサネットの設定が表示されます。
- ステップ 2** [General] タブで、特定のスイッチの [Promiscuous Mode] オプションをイネーブルまたはディセーブルにすることができます。
- ステップ 3** [Apply Changes] をクリックします。
-

VLAN

ここでは、Cisco MDS NX-OS での Virtual LAN (VLAN; 仮想 LAN) サポートについて説明します。ここで説明する内容は、次のとおりです。

- 「ギガビットイーサネットの VLAN について」(P.7-5)
- 「VLAN サブインターフェイスの設定」(P.7-5)
- 「インターフェイスのサブネットの要件」(P.7-6)

ギガビットイーサネットの VLAN について

仮想 LAN (VLAN) は、物理 LAN ネットワークに複数の仮想レイヤ 2 ネットワークを作成します。VLAN は、トラフィックの分離、セキュリティ、ブロードキャスト コントロールを提供します。

ギガビットイーサネットポートは、IEEE 802.1Q VLAN カプセル化でイーサネットフレームを自動的に認識します。複数の VLAN からのトラフィックを1つのギガビットイーサネットポートで受信する必要がある場合、各 VLAN に1つずつ、サブインターフェイスを設定します。



(注)

IPS モジュールまたは MPS-14/2 モジュールがシスコ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1つの IPS ポートで受信する必要がある場合、イーサネットスイッチで次の要件を満たしている必要があります。

- IPS モジュールまたは MPS-14/2 モジュールに接続される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設定されている。
- カプセル化がデフォルトの ISL ではなく 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設定

Device Manager を使用して VLAN サブインターフェイス (VLAN ID) を設定する手順は、次のとおりです。

- ステップ 1** [Interface] > [Ethernet and iSCSI] を選択します。
- ステップ 2** [Sub Interfaces] タブをクリックします。
- ステップ 3** 802.1Q が使用されるギガビットイーサネットサブインターフェイスを選択します。
- ステップ 4** [Edit IP Address] ボタンをクリックします。
- ステップ 5** ギガビットイーサネットインターフェイスの IPv4 アドレスおよびサブネットマスクを入力します。
- ステップ 6** [Create] をクリックして変更を保存するか、[Close] をクリックします。

インターフェイスのサブネットの要件

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 (mgmt 0) は、設定に応じて同じサブネットまたは異なるサブネットに設定できます (表 7-1 を参照してください)。

表 7-1 インターフェイスのサブネットの要件

インターフェイス 1	インターフェイス 2	同じサブネットの設定	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	可	2 つのメジャー インターフェイスを同じサブネットまたは異なるサブネットに設定できます。
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	可	同じ VLAN ID の 2 つのサブインターフェイスを同じサブネットまたは異なるサブネットに設定できます。
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	不可	異なる VLAN ID の 2 つのサブインターフェイスを同じサブネットに設定することはできません。
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	不可	サブインターフェイスをメジャー インターフェイスと同じサブネットに設定することはできません。
mgmt0	ギガビットイーサネット 1/1.100	不可	mgmt0 インターフェイスを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することはできません。
mgmt0	ギガビットイーサネット 1/1	不可	



(注) 表 7-1 の設定要件はイーサネット PortChannel にも適用されます。

IPv4-ACL

ここでは、IPv4 Access Control List (IPv4-ACL; IPv4 アクセス コントロール リスト) の注意事項、およびこれら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方法について説明します。



(注) IPv4-ACL の作成については、『Cisco Fabric Manager Security Configuration Guide』を参照してください。

ギガビットイーサネット IPv4-ACL 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 IPv4-ACL を設定する場合、次の注意事項に従ってください。

- Transmission Control Protocol (TCP; 伝送制御プロトコル) または Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) だけを使用します。



(注) User Datagram Protocol (UDP; ユーザ データグラム プロトコル) および HTTP などのそ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のルールを含む 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できますが、そのルールの効果はありません。

- インターフェイスをイネーブルにする前に IPv4-ACL をインターフェイスに適用します。これにより、トラフィックフローが開始される前に、フィルタが正常であることを確認できます。
- 次の条件に注意してください。
 - **log-deny** オプションを使用する場合、毎秒最大 50 のメッセージが記録されます。
 - **established** オプションは、このオプションを含む IPv4-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場合は無視されます。
 - IPv4-ACL ルールが既存の TCP 接続に適用される場合、ルールは無視されます。たとえば、A と B の間に既存の TCP 接続があり、発信元を A、宛先を B とするすべてのパケットの削除を指定する IPv4-ACL がその後で適用された場合、このルールの効果はありません。



ヒント

IPv4-ACL がギガビットイーサネットインターフェイスにすでに含まれている場合、このインターフェイスをイーサネット PortChannel グループに追加することはできません。IPv4-ACL の設定については、『Cisco Fabric Manager Security Configuration Guide』を参照してください。

デフォルト設定

表 7-2 に、IPv4 パラメータのデフォルト設定を示します。

表 7-2 デフォルトの IPv4 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	ディセーブル



CHAPTER 8

ギガビットイーサネットインターフェイスの IP バージョン 6 (IPv6) の設定

IP バージョン 6 (IPv6) は、Cisco MDS NX-OS の IP Version 4 (IPv4; IP バージョン 4) のものより優れたアドレッシング機能を提供します。IPv6 のアーキテクチャでは、既存の IPv4 ユーザは、エンドツーエンドセキュリティ、Quality of Service (QoS) およびグローバルで一意的なアドレスなどのサービスを提供しつつ、IPv6 に簡単に移行できます。

この章の内容は、次のとおりです。

- 「IPv6 の概要」 (P.8-1)
- 「IPv6 用の基本的な接続の設定」 (P.8-11)
- 「IPv6 スタティック ルートの設定」 (P.8-13)
- 「ギガビットイーサネット IPv6-ACL の注意事項」 (P.8-14)
- 「IPv4 から IPv6 への移行」 (P.8-14)
- 「デフォルト設定」 (P.8-15)



(注) IP アドレッシングを使用する Cisco NX-OS 機能については、本書の該当する章で、IPv6 アドレッシングサポートに関するこれらの機能の説明を参照してください。



(注) 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) を設定するには、第 7 章「ギガビットイーサネットインターフェイスの IP バージョン 4 (IPv4) の設定」を参照してください。

IPv6 の概要

IPv6 の IPv4 に対する機能強化は次のとおりです。

- ネットワークの拡張、およびグローバルな到達可能性の提供が可能になる。
- プライベートアドレスおよび Network Address Translation (NAT; ネットワークアドレス変換) が必要ない。
- アドレスの自動設定が簡単になる。

ここでは、Cisco MDS NX-OS での IPv6 機能について説明します。ここで説明する内容は、次のとおりです。

- 「一意なアドレスに対する拡張 IPv6 アドレス領域」 (P.8-2)
- 「IPv6 アドレスのフォーマット」 (P.8-2)
- 「IPv6 アドレス プレフィックスのフォーマット」 (P.8-3)
- 「IPv6 アドレス タイプ : ユニキャスト」 (P.8-3)
- 「IPv6 アドレス タイプ : マルチキャスト」 (P.8-5)
- 「IPv6 のインターネット制御メッセージプロトコル (ICMP)」 (P.8-6)
- 「IPv6 Path MTU Discovery」 (P.8-7)
- 「IPv6 近隣探索」 (P.8-7)
- 「ルータの検出」 (P.8-9)
- 「IPv6 ステートレス自動設定」 (P.8-9)
- 「IPv4 と IPv6 の二重プロトコルスタック」 (P.8-10)

一意なアドレスに対する拡張 IPv6 アドレス領域

IPv6 は、ネットワーク アドレス ビット数を 32 ビット (IPv4) から 128 ビットに 4 倍にすることで、アドレス領域を拡張します。これにより、さらに多くのグローバルで一意な IP アドレスを使用できます。IPv6 アドレスは、グローバルで一意になることで、ネットワーク デバイスのグローバルな到達可能性およびエンドツーエンドセキュリティや、さらに多くのアドレスが要求されるアプリケーションやサービスに重要な機能が実現されます。

IPv6 アドレスのフォーマット

IPv6 アドレスは、フォーマット x:x:x:x:x:x によりコロン (:) で区切った一連の 16 ビット 16 進数フィールドとして表されます。IPv6 アドレスの例は次のとおりです。

```
2001:0DB8:7654:3210:FEDC:BA98:7654:3210
```

```
2001:0DB8:0:0:8:800:200C:417A
```

通常、IPv6 アドレスには、連続するゼロの 16 進数フィールドが含まれます。IPv6 アドレスを使いやすくするため、2 つのコロン (::) を使用して、IPv6 アドレスの先頭、中間、末尾で連続するゼロの 16 進数フィールドを圧縮できます (2 つのコロンは連続するゼロの 16 進数フィールドを表します)。

表 8-1 に、圧縮された IPv6 アドレスのフォーマットを示します。



(注) 2 つのコロン (::) は IPv6 アドレスで一度だけ使用でき、最も長い連続するゼロの 16 進数フィールドを表すことができます。



(注) IPv6 アドレスの 16 進数文字は大文字と小文字が区別されません。

表 8-1 圧縮された IPv6 アドレスのフォーマット

IPv6 アドレスのタイプ	通常のフォーマット	圧縮されたフォーマット
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 プレフィックスのフォーマット

IPv6 アドレス プレフィックス (フォーマット *ipv6-prefix/prefix-length*) を使用して、アドレス領域全体のビット単位の連続ブロックを表すことができます。*ipv6-prefix* は、コロンで囲まれた 16 ビット値を使用して 16 進数で指定されます。*prefix-length* は、アドレスの連続する高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

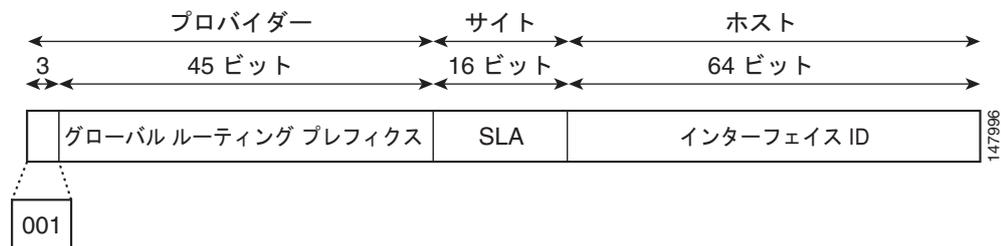
IPv6 ユニキャストアドレスは、シングルノードのシングルインターフェイスの ID です。ユニキャストアドレスに送信されるパケットは、そのアドレスで示されるインターフェイスに配信されます。Cisco MDS NX-OS は、次の IPv6 ユニキャストアドレスタイプをサポートします。

- グローバルアドレス
- リンクローカルアドレス

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 により定義されます。図 8-1 に、グローバルアドレスの構造を示します。

図 8-1 グローバルアドレスのフォーマット



プレフィックス 2000::/3 (001) から E000::/3 (111) のアドレスには、Extended Universal Identifier (EUI) -64 フォーマットの 64 ビットインターフェイス ID が必要です。Internet Assigned Numbers Authority (IANA; インターネット割り当て番号局) は、範囲 2000::/16 の IPv6 アドレス領域をリージョナルレジストリに割り当てます。

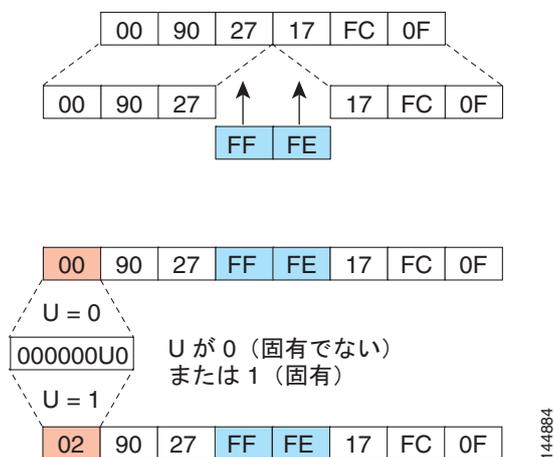
集約可能グローバルアドレスは、通常、48 ビットグローバルルーティングプレフィックスおよび 16 ビットサブネット ID または Site-Level Aggregator (SLA) で構成されます。IPv6 集約可能なグローバルユニキャストアドレスフォーマット文書 (RFC 2374) では、グローバルルーティングプレフィックスには、Top-Level Aggregator (TLA) および Next-Level Aggregator (NLA) という他の 2 つの階層構造のフィールドが含まれるとされていました。TLS フィールドおよび NLA フィールドはポリシーベースであるため、IETF は、これらのフィールドを RFC から削除することを決定しました。この変更以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上の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、16 ビットサブネットフィールドであるサブネット ID を使用して、独自のローカルアドレス階層を作成したり、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 65,535 の個々のサブネットをサポートできるという点で異なります。

インターフェイス ID で、リンク上のインターフェイスが識別されます。インターフェイス ID はリンク上で一意でなければなりません。また、これより広い範囲で一意な場合もあります。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レイヤアドレスと同じか、リンクレイヤアドレスに基づいているため、グローバルで一意なインターフェイス ID になります。集約可能なグローバルユニキャストアドレス タイプおよびその他の 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 ビットの変更済み EUI-64 フォーマットでなければなりません。

Cisco MDS NX-OS は、IEEE 802 インターフェイス タイプ (たとえば、ギガビット イーサネット インターフェイス) をサポートします。この場合、最初の 3 オクテット (24 ビット) がそのインターフェイスの 48 ビット リンクレイヤアドレス (MAC アドレス) の **Organizationally Unique Identifier** (OUI; 組織固有識別子)、4 番目と 5 番目のオクテット (16 ビット) が FFFE の固定 16 進数値、そして、最後の 3 オクテット (24 ビット) が MAC アドレスの最後の 3 オクテットです。インターフェイス ID の構築は、最初のオクテットの 7 番目のビットである **Universal/Local (U/L) ビット** に値 0 または 1 を設定して完了します。ゼロはローカルに管理されている ID を表し、1 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 を参照してください)。

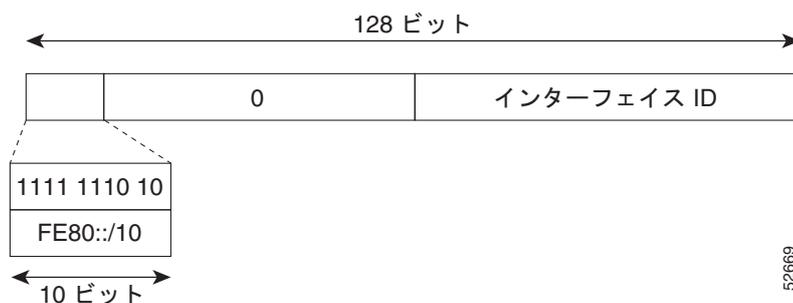
図 8-2 インターフェイス ID フォーマット



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、変更済み EUI-64 フォーマットのインターフェイス ID を使用するインターフェイスで自動的に設定される IPv6 ユニキャスト アドレスです。リンクローカル アドレスは近隣探索プロトコルおよびステートレス自動設定処理で使用されます。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。図 8-3 に、リンクローカル アドレスの構造を示します。

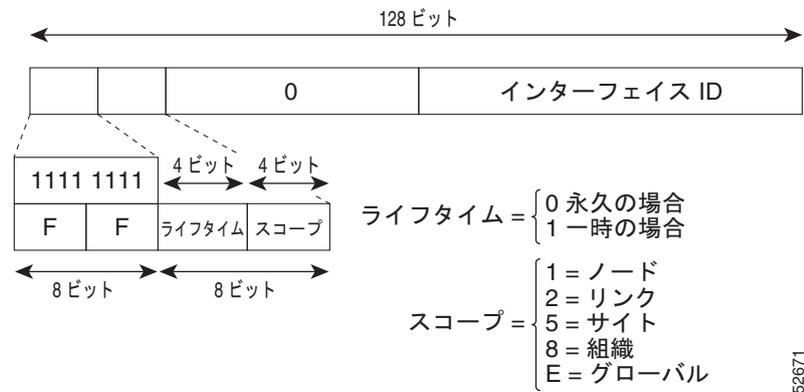
図 8-3 リンクローカル アドレスのフォーマット



IPv6 アドレス タイプ: マルチキャスト

IPv6 マルチキャスト アドレスとは、FF00::/8 (1111 1111) というプレフィクスを持つ IPv6 アドレスです。IPv6 マルチキャスト アドレスは、通常、異なるノードに属するインターフェイス一式の ID 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。プレフィクスに続く 2 番目のオクテットで、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、または組織のスコープ、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、または E です。たとえば、FF02::/16 というプレフィクスを持つマルチキャスト アドレスは、リンク スコープを持つ永久マルチキャスト アドレスです。図 8-4 に、IPv6 マルチキャスト アドレスのフォーマットを示します。

図 8-4 IPv6 マルチキャスト アドレスのフォーマット

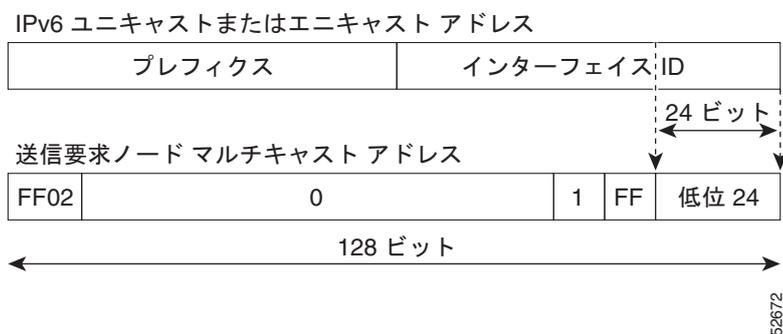


IPv6 ホストは、(受信パケットの宛先となる) 次のマルチキャスト グループに加入する必要があります。

- 全ノード マルチキャスト グループ FF02::1
- ユニキャスト アドレスの低位 24 ビットに連結された送信要求ノード マルチキャスト グループ FF02:0:0:0:1: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ユニキャスト アドレスごとに、関連付けられた送信要求ノード マルチキャスト グループに加入する必要があります。IPv6 送信要求ノード マルチキャスト アドレスには、対応する IPv6 ユニキャスト アドレスの低位 24 ビットに連結されたプレフィクス FF02:0:0:0:1:FF00:0000/104 があります (図 8-5 を参照してください)。たとえば、IPv6 アドレス 2037::01:800:200E:8C6C に対応する送信要求ノード 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 8-5 IPv6 送信要求ノードマルチキャストアドレスのフォーマット



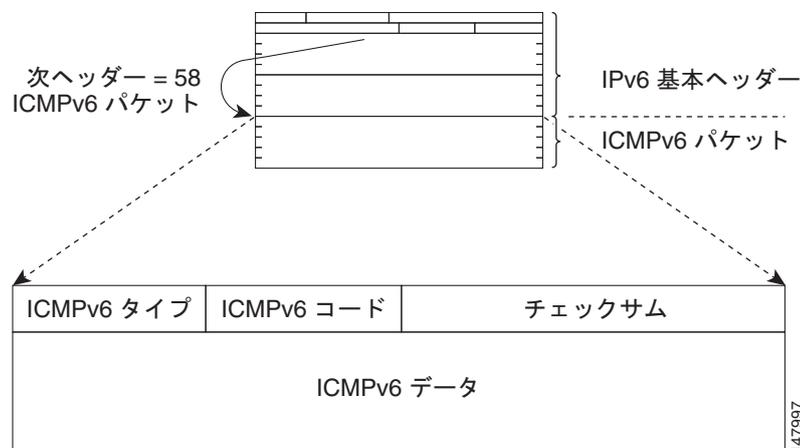
(注) IPv6 にはブロードキャストアドレスはありません。IPv6 マルチキャストアドレスがブロードキャストアドレスの代わりに使用されます。

IPv6 のインターネット制御メッセージ プロトコル (ICMP)

IPv6 のインターネット制御メッセージプロトコル (ICMP) は IPv4 の ICMP と同様に機能します。ICMP は、ICMP 宛先到達不能メッセージなどのエラーメッセージ、および ICMP エコー要求と応答要求などの情報メッセージを生成します。また、IPv6 の ICMP パケットは IPv6 近隣探索処理、Path MTU Discovery、IPv6 の Multicast Listener Discovery (MLD) プロトコルに使用されます。MLD は、IPv4 の Internet Group Management Protocol (IGMP; インターネットグループ管理プロトコル) のバージョン 2 に基づいています。

基本 IPv6 パケットヘッダーの次ヘッダーフィールドの 58 という値は、IPv6 ICMP パケットであることを示します。IPv6 の ICMP パケットは、すべての拡張ヘッダーの後に続く、ICMP パケット中の最後の情報部分であるという点で、トランスポートレイヤパケットに似ています。IPv6 ICMP パケットでは、ICMPv6 タイプフィールドと ICMPv6 コードフィールドに、ICMP メッセージタイプなどの IPv6 ICMP パケット情報が示されます。チェックサムフィールドの値は送信側で計算され、受信側により、IPv6 ICMP パケット内および IPv6 疑似ヘッダー内のフィールドでチェックされます。ICMPv6 データフィールドには、IP パケット処理に関するエラーまたは診断情報が含まれます。図 8-6 に、IPv6 ICMP パケットヘッダーのフォーマットを示します。

図 8-6 IPv6 ICMP パケットヘッダーのフォーマット



IPv6 Path MTU Discovery

IPv4 の場合と同様に、ホストが動的に、データパス上のすべてのリンクの MTU サイズの差を検出し、それに合わせて調整できるように、IPv6 で Path MTU Discovery を使用できます。ただし、IPv6 では、データパス上のリンクのパス MTU が小さすぎてパケットを処理できない場合は、パケットの送信元によりフラグメンテーションが処理されます。IPv6 ホストにパケットのフラグメンテーションを処理させると、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 は 68 オクテットです。つまり、データパス上のすべてのリンクの MTU サイズは、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。

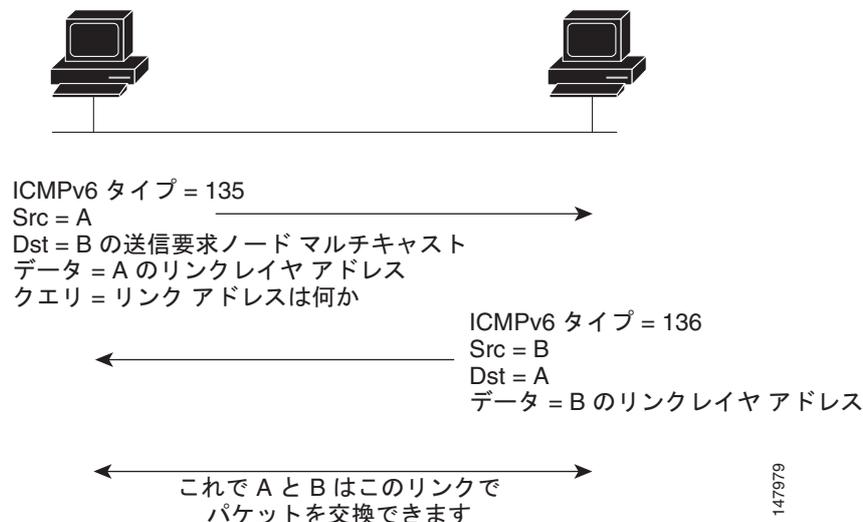
IPv6 近隣探索

IPv6 近隣探索プロセスは、ICMP メッセージおよび送信要求ノード マルチキャストアドレスを使用して、同じネットワーク上のネイバーのアドレス（ローカルリンク）を決定し、ネイバーの到達可能性を検証して、ネイバー ルータを追跡します。

IPv6 ネイバー送信要求メッセージおよびアドバタイズメント 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レイヤアドレスを決定するときに、ローカルリンクで送信されます（図 8-7 を参照してください）。ノードが別のノードのリンクレイヤアドレスを決定する場合、ネイバー送信要求メッセージの送信元アドレスは、ネイバー送信要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レイヤアドレスも含まれます。

図 8-7 IPv6 近隣探索：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、宛先ノードは返信として、ICMP パケット ヘッダーのタイプフィールドの値が 136 のネイバー アドバタイズメント メッセージをローカル リンクで送信します。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 (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レイヤ 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は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により、ネイバーのリンクレイヤ アドレスが認識された後に、ネイバーの到達可能性が確認できます。ノードは、ネイバーの到達可能性を確認するときに、ネイバー送信要求メッセージの宛先アドレスを、ネイバーのユニキャスト アドレスとして使用します。

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レイヤ アドレスが変更されたときにも送信されます。変更があったときのネイバー アドバタイズメントの宛先アドレスは、全ノード 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より、ネイバーのリンクレイヤ アドレスが認識された後に、ネイバーの到達可能性が確認できます。ネイバー到達不能検出により、ネイバーの障害またはネイバーへの転送パスの障害が特定されます。また、この検出は、ホストと近隣ノード (ホストまたはルータ) の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。

ネイバーは、そのノードから受諾の確認応答 (以前にそのノードに送信されたパケットが受信され、処理されたことを示す) が返されると、到達可能と見なされます。受諾の確認応答は、接続が動作中 (宛先に到達中) であることを示す Transmission Control Protocol (TCP; 伝送制御プロトコル) 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は、送信元ノードのネクストホップ ネイバーにも到達しています。順調に進んでいることで、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 リンクにない宛先の場合は、順調に進んでいることで、ファーストホップ ルータが到達可能であることがわかります。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かどうかを確認します。ネイバーから返信された送信要求ネイバー 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確認応答です (値 1 が設定された送信要求フラグを持つネイバー アドバタイズメント メッセージは、ネイバー送信要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が返信された場合は、送信元ノードから宛先ノードまでの片道のパスだけが確認されています。送信要求ネイバー アドバタイズメント メッセージは、往復のパスがいずれも機能していることを示します。



(注)

0 という値が設定された送信要求フラグを持つネイバー 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 アドレスをインターフェイスに割り当て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処理でも使用されます。新規のリンクローカル IPv6 アドレスに対しては、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（新規アドレスは、重複アドレス検出の実行中は一時的なアドレスのままです）。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 アドレスがメッセージ本文に含まれるネイバー送信要求メッセージを送信します。そのアドレスがすでに他のノードによって使用されている場合、ノードは、一時的リンクローカル 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信します。他のノードが同時に、同じアドレスが一意であることを確認している場合は、そのノードも、ネイバー送信要求メッセージを返信します。ネイバー送信要求メッセージの返信としてのネイバー アドバタイズメントメッセージも、同じ一時的アドレスを確認中の他のノードからのネイバー送信要求メッセージも受信しない場合、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 アドレスが一意であると判断し、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。

ルータの検出

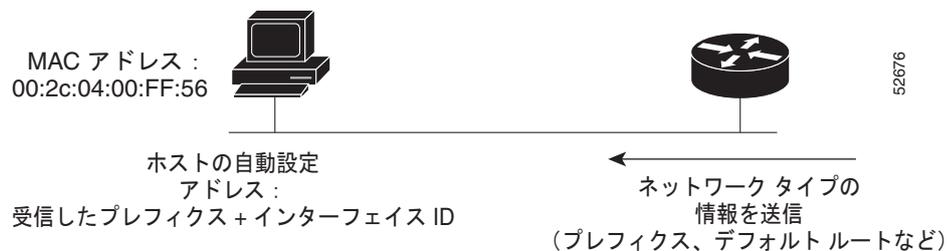
ルータの検出では、ルータ送信要求およびルータ アドバタイズの両方を実行します。ホストは、全ルータのマルチキャストアドレスにルータ送信要求を送信します。ルータは、送信要求または非送信要求に対して、デフォルトのルータ情報および MTU やホップ制限などの追加パラメータを含むルータ アドバタイズを送信します。

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には、インターフェイスの ID およびリンクローカルプレフィクス FE80::/10 から自動的に設定されるリンクローカルアドレスが必要です。リンクローカルアドレスを使用すると、ノードはリンク上の他のノードと通信できます。さらに、リンクローカルアドレスを使用して、ノードを設定することができます。

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 サーバなどのサーバ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、Router Advertisement (RA; ルータ アドバタイズ) メッセージで、任意のサイトローカルプレフィクスやグローバルプレフィ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 メッセージには、定期的に送信されるメッセージと、システム起動時にホストが送信す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メッセージがあります（図 8-8 を参照してください）。

図 8-8 IPv6 ステートレス自動設定

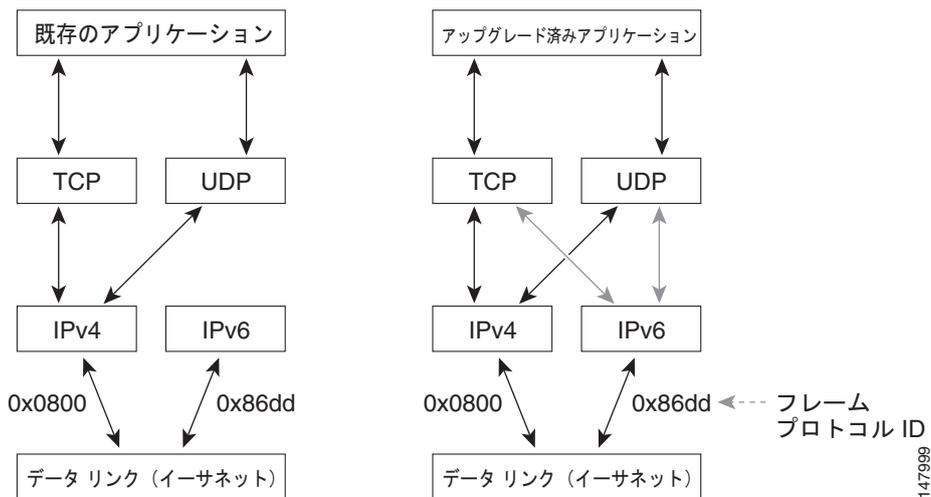


リンク上のノードは、RA メッセージに含まれるプレフィクス（64 ビット）にそのインターフェイス ID（64 ビット）を追加して、自動的にサイトローカルおよびグローバル IPv6 アドレスを設定できます。ノードによって設定された 128 ビットの IPv6 アドレスは、リンクでの一意性を保証するために、重複アドレス検出の対象になります。RA メッセージでアドバタイズされるプレフィクスがグローバルに一意である場合、ノードによって設定された IPv6 アドレスもグローバルに一意であることが保証されます。ホストはシステム起動時に ICMP パケットヘッダーのタイプフィールドの値が 133 のルータ送信要求メッセージを送信するため、スケジュールされた次の RA メッセージを待たずにただち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。この方法を使用すると、ノード上で稼動するアプリケーションを段階的にアップグレードできます。ノード上で稼動するアプリケーションは、IPv6 プロトコル スタックを利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（図 8-9 を参照してください）。

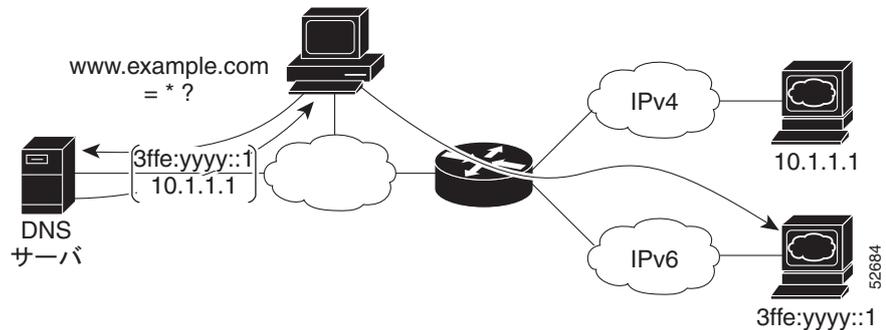
図 8-9 IPv4 と IPv6 の二重プロトコル スタック



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。アプリケーションは新しい API へアップグレードできます。また、引き続き、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。

図 8-10 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名 `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で選択されます）、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 8-10 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



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。各作業には、必須またはオプションの指定があります。ここで説明する内容は、次のとおりです。

- 「IPv6 アドレッシングの設定および IPv6 ルーティングのイネーブル化」(P.8-11)
- 「IPv4 および IPv6 プロトコルアドレスの設定」(P.8-13)

IPv6 アドレッシングの設定および IPv6 ルーティングのイネーブル化

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 アドレスは、RFC 2373 に記述されているように、コロンで囲んだ 16 ビット値を使用して 16 進数で指定する必要があります。

IPv6 プレフィックスは、RFC 2373 に記述されているように、コロンで囲んだ 16 ビット値を使用して 16 進数で指定する必要があります。

IPv6 プレフィックス長アドレスの連続する高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 進値です。10 進値の前にスラッシュ記号を付ける必要があります。

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、自動的にリンクローカルアドレスが設定され、そのインターフェイスで 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、自動的にそのリンクに必要な次のマルチキャストグループに参加します。

- 送信要求ノードマルチキャストグループ FF02:0:0:0:1: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、近隣探索プロセスで使用されます。

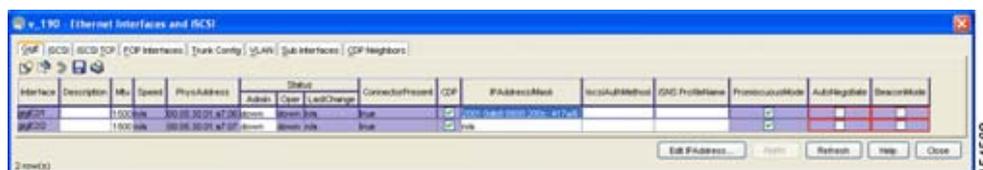


(注) 各インターフェイスには IPv6 アドレス (スタティックおよび自動設定) を最大 8 つまで設定できます。ただし、管理 (mgmt 0) インターフェイスには、スタティック IPv6 アドレスを 1 つだけ設定できません。

Device Manager を使用してインターフェイスの IPv6 アドレスを設定する手順は、次のとおりです。

- ステップ 1** [Interfaces] > [Gigabit Ethernet and iSCSI] を選択します。
[Gigabit Ethernet Configuration] ダイアログボックスが表示されます (図 8-11 を参照してください)。

図 8-11 Device Manager でのギガビットイーサネットの設定

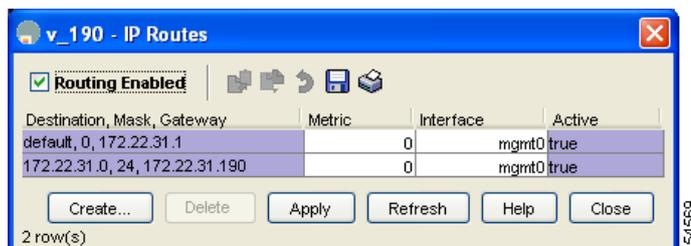


- ステップ 2** 設定する [IP Address] をクリックして、[Edit IP Address] をクリックします。
[IP Address] ダイアログボックスが表示されます。
- ステップ 3** [Create] をクリックし、IPv6 フォーマット (たとえば、2001:0DB8:800:200C::417A/64) を使用して、
[IP Address/Mask] フィールドを設定します。
- ステップ 4** これらの変更を保存するには、[Create] をクリックします。変更を保存せずに終了するには、[Close] をクリックします。

Device Manager を使用して IPv6 ルーティングをイネーブルにする手順は、次のとおりです。

- ステップ 1** [IP] > [Routing] を選択します。[IP Routing Configuration] ダイアログボックスが表示されます (図 8-12 を参照してください)。

図 8-12 Device Manager での IP ルーティングの設定



- ステップ 2** [Routing Enabled] チェックボックスをオンにします。
- ステップ 3** これらの変更を保存するには、[Apply] をクリックします。変更を保存せずに終了するには、[Close] をクリックします。
-

IPv4 および IPv6 プロトコル アドレスの設定

シスコ ネットワーク 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。

Device Manager を使用して、IPv4 および IPv6 プロトコル スタックの両方をサポートするようにシスコ ネットワーク デバイスのインターフェイスを設定する手順は、次のとおりです。

- ステップ 1** [Interfaces] > [Gigabit Ethernet and iSCSI] を選択します。
[Gigabit Ethernet Configuration] ダイアログボックスが表示されます。
- ステップ 2** 設定する [IP Address] フィールドをクリックして、[Edit IP Address] をクリックします。
[IP Address] ダイアログボックスが表示されます。
- ステップ 3** [Create] をクリックし、IPv4 または IPv6 フォーマットを使用して、[IP Address/Mask] フィールドを設定します。
- ステップ 4** これらの変更を保存するには、[Create] をクリックします。変更を保存せずに終了するには、[Close] をクリックします。
-

IPv6 スタティック ルートの設定

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。ここで説明する内容は、次のとおりです。

- [「IPv6 スタティック ルートの設定」 \(P.8-13\)](#)

IPv6 スタティック ルートの設定

IPv6 スタティック ルートを手動で設定し、2 台のネットワーク デバイス間の明示的なパス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ため、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。

Device Manager を使用して IPv6 スタティック ルートを設定する手順は、次のとおりです。

- ステップ 1** [IP] > [Routing] を選択します。
[IP Routing Configuration] ダイアログボックスが表示されます
- ステップ 2** [Create] をクリックします。
[Create IP Route] ダイアログボックスが表示されます。
- ステップ 3** [Dest] フィールドに IPv6 宛先アドレスを設定します。
- ステップ 4** [Mask] フィールドに IPv6 サブネット マスクを設定します。

- ステップ 5** [Gateway] フィールドに IPv6 デフォルト ゲートウェイを設定します。
- ステップ 6** (任意) [Metric] フィールドに必要なルート トリックを設定します。
- ステップ 7** [Interface] ドロップダウン メニューからインターフェイスを選択します。
- ステップ 8** これらの変更を保存するには、[Create] をクリックします。変更を保存せずに終了するには、[Close] をクリックします。

ギガビットイーサネット IPv6-ACL の注意事項



ヒント

IPv6-ACL がギガビットイーサネット インターフェイスにすでに含まれている場合、このインターフェイスをイーサネット PortChannel グループに追加することはできません。IPv6-ACL の設定については、『Cisco Fabric Manager Security Configuration Guide』を参照してください。

ギガビットイーサネット インターフェイスの IPv6-ACL を設定する場合、次の注意事項に従ってください。

- 伝送制御プロトコル (TCP) または Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) だけを使用します。



(注)

User Datagram Protocol (UDP; ユーザ データグラム プロトコル) および HTTP などのそ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のルールを含む 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できますが、そのルールの効果はありません。

- インターフェイスをイネーブルにする前に IPv6-ACL をインターフェイスに適用します。これにより、トラフィック フローが開始される前に、フィルタが正常であることを確認できます。
- 次の条件に注意してください。
 - **log-deny** オプションを使用する場合、毎秒最大 50 のメッセージが記録されます。
 - **established** オプションは、このオプションを含む IPv6-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場合は無視されます。
 - IPv6-ACL ルールが既存の TCP 接続に適用される場合、ルールは無視されます。たとえば、A と B の間に既存の TCP 接続があり、発信元を A、宛先を B とするすべてのパケットの削除を指定する IPv6-ACL がその後で適用された場合、このルールの効果はありません。

IPv6-ACL のインターフェイスへの適用については、『Cisco Fabric Manager Security Configuration Guide』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。ただし、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シスコ ルータを設定する方法の詳細については、『Cisco IOS IPv6 Configuration Guide』の「Implementing Tunneling for IPv6」の章を参照してください。

デフォルト設定

表 8-2 に、IPv6 パラメータのデフォルト設定を示します。

表 8-2 デフォルトの 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 (近隣探索ディセーブル)
到達可能性時間	1000 ミリ秒
再送信時間	30000 ミリ秒
IPv6-ACL	なし



INDEX

A

AAA 認証

設定 [4-30, 4-31](#)

ACL

iSCSI 用の設定 [4-28](#)

ACL ベースのアクセス コントロール

iSCSI 用の設定 [4-28](#)

B

B ポート

SAN 拡張機能 [2-24](#)

設定 [2-25](#)

相互運用性モード [2-23](#)

C

CDP

設定

CFS

iSLB 設定の配信 [4-49](#)

CHAP 応答 [4-33](#)

CHAP 認証 [4-30, 4-45, 4-61](#)

CHAP 認証確認 [4-33](#)

CHAP ユーザ名 [4-32](#)

Cisco Discovery Protocol。「CDP」を参照

Cisco Transport Controller。「CTC」を参照

CTC

起動 [2-17](#)

説明 [2-17](#)

CWM

FCIP プロファイルでの設定 [2-19](#)

D

DNS

デフォルト設定 [5-15](#)

DNS サーバ

設定 [5-15](#)

DSCP

設定 [2-26](#)

E

ELP

Device Manager による確認 (手順) [2-17](#)

Entity Status Inquiry。「ESI」を参照

ESI

未応答回数のしきい値 [4-77](#)

ESI リトライ回数 [4-77](#)

Extended Link Protocol。「ELP」を参照

E ポート

設定 [2-26](#)

F

FCIP [4-1](#)

ELP の確認 (手順) [2-17](#)

FCIP ウィザードによる設定 [2-8 ~ 2-15](#)

IPS モジュール [2-2](#)

IP ストレージ サービスのサポート [6-1](#)

MPS-14/2 モジュール [2-2](#)

VE ポート [2-2](#)

VRRP [2-6](#)

圧縮 [2-34](#)

イネーブル化 [2-8](#)

- インターフェイスの確認 (手順) [2-17](#)
 - 書き込みアクセラレーション [2-27](#)
 - 仮想 ISL [2-2](#)
 - ギガビット イーサネット ポート [6-4, 7-1](#)
 - 詳細機能 [2-27](#)
 - 設定 [2-8](#)
 - タイム スタンプ [2-22](#)
 - テープ アクセラレーション [2-29](#)
 - デフォルト パラメータ [2-36](#)
 - トランク ステータスの確認 (手順) [2-17](#)
 - ハイ アベイラビリティ [2-4](#)
 - パケットの廃棄 [2-22](#)
 - リンク障害 [2-5](#)
 - FCIP TCP パラメータ
 - CWM の設定 [2-19](#)
 - PMTU の設定 [2-19](#)
 - SACK の設定 [2-19](#)
 - ウィンドウ管理の設定 [2-19](#)
 - キープアライブ タイムアウトの設定 [2-18](#)
 - 最小再送信タイムアウトの設定 [2-18](#)
 - 最大再送信回数 の設定 [2-19](#)
 - 最大ジッタの設定 [2-20](#)
 - バッファ サイズの設定 [2-20](#)
 - FCIP 圧縮
 - 設定 (手順) [2-12](#)
 - 説明 [2-34](#)
 - FCIP インターフェイス
 - QoS の設定 [2-26](#)
 - 作成 [2-21](#)
 - 詳細機能の設定 [2-21 ~ 2-26](#)
 - パラメータ [2-4](#)
 - ピアの設定 [2-21](#)
 - FCIP 書き込みアクセラレーション
 - 設定 [2-29](#)
 - 設定 (手順) [2-12](#)
 - 説明 [2-27](#)
 - FCIP テープ アクセラレーション
 - 設定 [2-34](#)
 - 説明 [2-29, 2-34](#)
 - FCIP ピア
 - IP アドレスの設定 [2-21](#)
 - FCIP プロファイル
 - TCP パラメータの設定 [2-18](#)
 - 作成 [2-15](#)
 - 説明 [2-4](#)
 - FCIP リンク
 - B ポート相互運用性モード [2-23](#)
 - IP 接続の開始 [2-22](#)
 - QoS の設定 [2-26](#)
 - TCP 接続 [2-3](#)
 - エンドポイント [2-3](#)
 - 作成 [2-16](#)
 - 設定 [2-15](#)
 - 説明 [2-3](#)
 - ピアの設定 [2-21](#)
 - FCP
 - ルーティング要求 [4-4](#)
 - FC 論理インターフェイス テーブル [4-23](#)
 - Fibre Channel over IP。「FCIP」を参照
 - FSPF
 - ロード バランシング (例) [2-5](#)
-
- ## H
- HA ソリューションの例 [4-55](#)
 - HBA ポート [4-17, 4-22](#)
-
- ## I
- ICMP
 - IPv6 [8-6](#)
 - ICMP パケット
 - IPv6 ヘッダー フォーマット、図 [8-6](#)
 - Internet Storage Name Service。「iSNS」を参照
 - IPFC
 - 設定時の注意事項 [5-8](#)
 - 説明 [5-7](#)
 - IPsec

- FCIP ウィザードによる設定 (手順) [2-9](#)
- IPS ポート [4-10](#)
 - 複数の接続 [4-57](#)
 - モード [7-1](#)
- IPS ポート モード
 - 説明 [6-4](#)
- IPS モジュール
 - CDP のサポート [6-11](#)
 - FCIP [2-2](#)
 - サポートされる機能 [6-1](#)
 - ソフトウェア アップグレード [6-3](#)
 - ポート モード [6-4, 7-1](#)
- IPv4
 - IPv6 への移行 [8-14](#)
 - ギガビット イーサネット インターフェイスの設定 [7-2](#)
 - 説明 [7-1](#)
 - デフォルト設定 [7-7](#)
- IPv4-ACL
 - ギガビット イーサネット インターフェイスのガイドライン [7-7](#)
- IPv4 アドレス
 - IPv4 および IPv6 のプロトコル スタックの設定 [8-13](#)
 - IPv6 プロトコル スタック [8-10](#)
- IPv4 デフォルト ゲートウェイ
 - スタティック ルート (ヒント) [5-6](#)
 - 設定 [5-4](#)
 - 説明 [5-3](#)
- IPv4 デフォルト ネットワーク
 - 説明 [5-6](#)
- IPv6
 - ICMP [8-6](#)
 - IPv4 アドレスおよび IPv6 アドレスの設定 [8-13](#)
 - IPv4 および IPv6 のデュアル プロトコル スタック [8-10](#)
 - IPv4 および IPv6 のデュアル プロトコル スタック アプリケーション、図 [8-11](#)
 - IPv4 および IPv6 のデュアル プロトコル スタック 技術、図 [8-10](#)
 - IPv4 からの移行 [8-14](#)
 - IPv4 経由の拡張 [8-1](#)
 - IPv6-ACL のガイドライン [8-14](#)
 - Path MTU Discovery [8-7](#)
 - アドレス タイプ [8-3](#)
 - アドレッシングの設定 [8-11](#)
 - 管理インターフェイスの設定 [5-3](#)
 - 近隣探索 [8-7](#)
 - スタティック ルート [8-13](#)
 - ステートレス自動設定 [8-9](#)
 - 説明 [8-1 ~ 8-10](#)
 - デフォルト設定 [8-15](#)
 - ルータ アドバタイズメント メッセージ [8-9](#)
 - ルータ検出 [8-9](#)
 - ルーティングのイネーブル化 [8-11](#)
- IPv6-ACL
 - IPv6 のガイドライン [8-14](#)
- IPv6 アドレス
 - IPv4 および IPv6 のプロトコル スタックの設定 [8-13](#)
 - 設定 [8-11](#)
 - フォーマット [8-2](#)
 - プレフィクス フォーマット [8-3](#)
 - マルチキャスト タイプ [8-5](#)
 - ユニキャスト タイプ [8-3](#)
 - リンクローカル タイプ [8-4](#)
- IPv6 近隣探索
 - アドバタイズメント メッセージ [8-7](#)
 - 説明 [8-7](#)
 - 送信要求メッセージ [8-7](#)
 - ネイバー送信要求メッセージ、図 [8-7](#)
- IPv6 スタティック ルート
 - 設定 [8-13](#)
- IPv6 ルーティング
 - イネーブル化 [8-11](#)
- IP ストレージ サービス
 - デフォルト パラメータ [6-11](#)
- IP ストレージ サービス モジュール。「IPS モジュール」を参照

- IP 接続
 - アクティブ モード [2-22](#)
 - 開始 [2-22](#)
 - パッシブ モード [2-22](#)
- IQN
 - フォーマット [4-10](#)
- iSCSI
 - AAA 認証の設定 [4-30, 4-31](#)
 - ACL の設定 [4-28](#)
 - CHAP 認証に特定のユーザ名を使用させるようにイニシエータを制限する [4-32](#)
 - Device Manager 内のターゲット [4-11](#)
 - Fabric Manager のテーブル [4-21](#)
 - GW フラグ、iSCSI
 - ゲートウェイ デバイス [4-18](#)
 - IPS モジュールのサポート [6-2](#)
 - IQN [4-16](#)
 - iSCSI インターフェイスの VSAN メンバシップ [4-24, 4-25](#)
 - iSCSI ウィザードの使用 (手順) [4-7 ~ 4-9](#)
 - MPS-14/2 モジュールのサポート [6-2](#)
 - PortChannel ベースのハイ アベイラビリティ [4-60](#)
 - PortChannel ベースのハイ アベイラビリティ、イーサネット PortChannel ベースのハイ アベイラビリティ [4-60](#)
 - VRRP の設定 [4-59](#)
 - VSAN メンバシップ [4-24](#)
 - VSAN メンバシップの例 [4-25](#)
 - WWN 競合の確認 [4-21](#)
 - アクセス コントロール [4-26 ~ 4-30](#)
 - アクセス コントロールの実行 [4-29](#)
 - イニシエータ ターゲット [4-8](#)
 - イニシエータのアイドル タイムアウト
 - iSCSI、イニシエータのアイドル タイムアウト
 - Fabric Manager による設定 [4-18](#)
 - イニシエータのゾーンデータベースへの追加 [4-27](#)
 - イニシエータ名 [4-32](#)
 - イネーブル化 [4-5](#)
 - エラー [4-17](#)
 - 仮想ターゲットの作成 [4-12](#)
 - ギガビットイーサネット ポート [6-4, 7-1](#)
 - 検出フェーズ [4-29](#)
 - 互換ドライバ [4-2](#)
 - 詳細 VSAN メンバシップ [4-26](#)
 - スタティック マッピングされたイニシエータ [4-38](#)
 - セッション作成 [4-30](#)
 - セッション制限
 - 設定 [4-2, 4-4, 4-60](#)
 - ゾーン名 [4-9](#)
 - ターゲットの LUN マッピング [4-67](#)
 - デフォルト パラメータ [4-81](#)
 - ドライバ [4-2](#)
 - トランスペアレント イニシエータ モード [4-17](#)
 - トランスペアレント モード イニシエータ [4-63](#)
 - ファイバチャネル ターゲット [4-9, 4-16](#)
 - 複数の IPS ポート [4-57](#)
 - プロトコル [4-2](#)
 - マルチパス ソフトウェアを使用していないホストでの HA [4-55](#)
 - 要求と応答 [4-4](#)
 - ルーティング [4-2](#)
 - ルーティング モードのチャート、iSCSI のルーティング モードのチャート [4-36](#)
 - ローカル認証を使用するユーザ [4-32](#)
 - ログインリダイレクト [4-39](#)
 - iscsi-gw [4-23](#)
 - iSCSI LU [4-10](#)
 - iSCSI イニシエータ
 - WWN 割り当て [4-19](#)
 - アイドル タイムアウト [4-18](#)
 - 固定 IP アドレス マッピングの設定 [4-20](#)
 - スタティック マッピング [4-19](#)
 - スタティック マッピング (手順) [4-20](#)
 - ダイナミック WWN マッピングをスタティックにする [4-21](#)
 - ダイナミック マッピング [4-19](#)
 - トランスペアレント モード [4-17](#)
 - プロキシモード [4-22](#)
 - iSCSI インターフェイス
 - QoS の設定 [4-35](#)

- TCP 調整パラメータの設定 [4-34](#)
- VSAN メンバシップ [4-25](#)
 - 作成 [4-6](#)
 - 作成、iSCSI
 - インターフェイスの作成 [4-6](#)
 - 設定 [4-16](#)
 - リスナー ポートの設定 [4-34](#)
 - リスナー ポートの設定、iSCSI
 - リスナー ポート [4-34](#)
 - ルーティング モードの設定 [4-35](#)
 - ルーティング モードの設定、iSCSI [4-35](#)
- iSCSI サーバ ロード バランシング [4-37](#)
- iSCSI サーバ ロード バランシング。「iSLB」を参照
- iSCSI セッション
 - 認証、iSCSI
 - セッション認証、認証
 - iSCSI セッション [4-30](#)
- iSCSI ターゲット
 - アドバタイジング [4-14](#)
 - スタティック インポート [4-12](#)
 - スタティック インポート、スタティック マッピング、iSCSI ターゲット
 - スタティック マッピング [4-12](#)
 - セカンダリ アクセス [4-55](#)
 - ダイナミック インポート [4-10](#)
 - ダイナミック マッピング [4-10](#)
 - 透過的なフェールオーバー
 - 例 [4-14](#)
- iSCSI デバイス
 - VSAN のメンバシップの例 [4-25](#)
- iSCSI 認証
 - RADIUS の設定 (手順) [4-33](#)
 - イニシエータに対する制限 [4-32](#)
 - 外部 RADIUS サーバ [4-62](#)
 - グローバル上書き [4-31](#)
 - シナリオ [4-60](#)
 - 設定 [4-30, 4-45](#)
 - セットアップのガイドライン [4-60](#)
 - メカニズム [4-31](#)
 - ローカル認証 [4-32](#)
- iSCSI ハイ アベイラビリティ
 - 設定 [4-53 ~ 4-60](#)
- iSCSI プロトコル [4-1](#)
- iSCSI ベースのアクセス コントロール [4-28](#)
- iSCSI ホスト
 - VSAN メンバシップ [4-24](#)
 - イニシエータの識別 [4-16](#)
 - イニシエータ プレゼンテーション モード [4-17](#)
- iSLB
 - CFS を使用した設定の配信 [4-49](#)
 - Device Manager による設定 [4-39](#)
 - VRRP の設定 [4-49](#)
 - VSAN メンバシップ [4-43](#)
 - イニシエータおよびターゲットの設定 [4-43](#)
 - イニシエータの WWN 割り当て [4-37](#)
 - 最大イニシエータ数 [4-38](#)
 - 自動ゾーン分割 [4-50](#)
 - スタティック イニシエータ設定、イニシエータ設定
 - スタティック iSLB [4-38](#)
 - 設定 [4-37](#)
 - 設定の制限 [4-38](#)
 - 設定の配信 [4-49, 4-50](#)
 - 設定配信のイネーブル化 [4-51](#)
 - 設定変更のコミット
 - iSLB [4-52](#)
 - 前提条件の設定 [4-39](#)
 - ゾーン セットのアクティブ化に失敗する [4-45](#)
 - ゾーンのアクティブ化 [4-43, 4-45](#)
 - ゾーンの設定 [4-43, 4-45](#)
 - ダイナミック イニシエータ マッピング [4-42](#)
 - デフォルト設定 [4-82](#)
 - ロード バランシング アルゴリズム [4-48](#)
- iSLB、CFS 配信の設定された [4-38](#)
- iSLB イニシエータ [4-39](#)
 - VSAN メンバシップ [4-43](#)
 - WWN の割り当て [4-42](#)
 - 設定 [4-42 ~ 4-46](#)
 - ゾーンのアクティブ化 [4-45](#)

ゾーンの設定 **4-45**

ダイナミック イニシエータ マッピング **4-42**

ロード バランシング メトリックの設定 **4-43**

iSLB イニシエータ ターゲット

説明 **4-43**

ゾーンのアクティブ化 **4-45**

ゾーンの設定 **4-45**

iSLB 自動ゾーン機能 **4-39**

iSLB セッション

IPS ポートあたりの最大数、iSLB
IPS ポートあたりの最大セッション数 **4-38**

認証 **4-45**

認証、iSLB
セッション認証 **4-45**

iSNS

ESI **4-77**

クライアント登録 **4-78**

クラウド検出 **4-79**

サーバの設定 **4-76 ~ 4-78**

設定 **4-78**

説明 **4-72**

iSNS クラウド検出

CFS 配信 **4-81**

イネーブル化 **4-80**

オンデマンドで開始 **4-80**

自動 **4-80**

説明 **4-79**

iSNS サーバ

ESI リトライ回数の設定 **4-77**

イネーブル化 **4-76**

設定の配信 **4-77**

例のシナリオ **4-75**

iSNS プロファイル
作成 **4-73**

L

LU **4-10**

LUN **4-10**

ストレージ ポート フェールオーバー用の
trespass **4-57**

マッピングと割り当て **4-22**

明示的なアクセス コントロール **4-22**

LUN マッピング **4-56**

iSCSI **4-67**

M

MD5 認証
VRRP **5-14**

mgmt0 インターフェイス
ローカル IPv4 ルーティング **5-7**

MPS-14/2 モジュール **4-1, 4-2, 4-3, 4-6, 4-22, 4-29**

CDP のサポート **6-11**

FCIP **2-2**

サポートされる機能 **6-1**

ソフトウェア アップグレード **6-3**

ポート モード **6-4, 7-1**

MTU

IPv6 のパス検出 **8-7**

サイズの設定
フレーム サイズの設定 **7-4**

MTU フレーム サイズ
ギガビット イーサネット インターフェイスの設
定 **6-6**

Multiprotocol Services モジュール。「MPS-14/2 モジュー
ル」を参照

N

None 認証 **4-30**

NTP
タイムスタンプ オプション **2-23**

P

Path MTU。「PMTU」を参照

PDU **4-35**

PMTU

FCIP プロファイルでの設定 **2-19**

PortChannel

FCIP ハイ アベイラビリティのための設定 **2-5**

IQN フォーマット **4-10**

インターフェイス **4-14**

サブインターフェイス **4-14**

冗長性 **2-7**

メンバーの組み合わせ **6-10**

ロード バランシング (例) **2-5**

pWWN

ダイナミックをスタティックに変換 **4-21**

Q

QoS

DSCP 値 **2-26**

QoS 値

設定 **4-35**

R

RADIUS **4-62**

AAA 認証 **4-30, 4-45**

iSCSI RADIUS サーバの設定、iSCSI

RADIUS サーバの設定 **4-33**

RSCN **4-18**

S

SACK

FCIP プロファイルでの設定 **2-19**

SAN 拡張チューナー

設定 **3-3**

説明 **3-1**

調整ガイドライン **3-2**

データ パターン **3-3**

デフォルト設定 **3-7**

ライセンス要件 **3-3**

SCSI

ルーティング要求 **4-2**

Selective Acknowledgment。「SACK」を参照

SPI

仮想ルータの設定 **5-14**

T

TACACS+

AAA 認証 **4-45**

TCP 接続

FCIP プロファイル **2-4**

TCP 調整パラメータ **4-34**

TCP パラメータ

FCIP プロファイルでの設定 **2-18**

V

VE ポート

FCIP **2-2**

説明 **2-2**

VLAN

ギガビット イーサネット サブインターフェイスの設定 **7-5**

説明 **6-6, 7-5**

VR ID

説明 **5-11**

マッピング **5-11**

VRRP **4-37**

IQN フォーマット **4-10**

iSCSI パラメータ変更の影響 **4-48**

iSLB **4-46**

iSLB 用の設定 **4-49**

MD5 認証 **5-14**

アドバタイズメント タイム インターバルの設定 **5-14**

仮想ルータの開始 **5-13**

仮想ルータの設定 **5-13**

ギガビット イーサネット インターフェイス選択のアルゴリズム **4-48**

ギガビット イーサネット インターフェイス用の設定 **6-9**

グループ メンバー **6-9**

セキュリティ認証 **5-14**

説明 **5-11, 6-8**

デフォルト設定 **5-16**

バックアップ スイッチ **5-11**

平文認証 **5-14**

プライオリティの設定 **5-14**

プライオリティ プリエンプション **5-14**

プライマリ IP アドレス **5-13**

マスター スイッチ **5-11**

VRRP (iSCSI ログイン リダイレクトを使用する場合) **4-39**

VRRP グループ **4-25**

VSAN

IPv4 スタティック ルーティング **5-8**

iSCSI デバイスのメンバシップの例 **4-25**

iSLB **4-43**

iSLB イニシエータ **4-43**

VRRP **5-11**

VSAN 間のトラフィック ルーティング **5-1**

オーバーレイされたルート **5-8**

ゲートウェイ スイッチ **5-6**

複数の IPv4 サブネットの設定 **5-10**

VSAN メンバシップ

iSCSI インターフェイス **4-25**

iSCSI ホスト **4-24**

iSCSI ホスト、iSCSI

ホストの VSAN メンバシップ **4-24**

W

WWN

スタティック バインディング **4-22**

あ

アクセス コントロール

iSCSI **4-28**

実行、iSCSI

アクセス コントロールの実行 **4-29**

アクセス コントロール、ゾーン分割ベースのアクセス コントロール、iSCSI

ゾーン分割ベースのアクセス コントロール **4-29**

アダプタイズ対象インターフェイス **4-14**

アダプタイズメント パケット

タイム インターバルの設定 **5-14**

い

イーサネット PortChannel

iSCSI **4-60**

ギガビット イーサネット インターフェイスの追加 **6-11**

冗長性 **2-6**

設定 **6-11**

説明 **6-10**

一時的な障害 **4-18**

イニシエータ

スタティック マッピングされた iSCSI **4-38**

インターネット制御メッセージ プロトコル。「ICMP」を参照

インバンド管理

IPFC **5-7**

う

ウィンドウ管理

FCIP プロファイルでの設定 **2-19**

お

オートネゴシエーション

ギガビット イーサネット インターフェイスの設定 **6-6, 7-3**

オーバーレイ VSAN

- 設定 [5-9](#)
- 説明 [5-8](#)

か

外部 RADIUS サーバ

- CHAP [4-62](#)

仮想 E ポート。「VE ポート」を参照

仮想 ISL

- 説明 [2-2](#)

仮想 LAN。「VLAN」を参照

仮想ファイバ チャンネル ホスト [4-3](#)

仮想ルータ

- 開始 [5-13](#)
- 削除 [5-13](#)
- 追加 [5-13](#)
- デフォルト設定 [5-16](#)
- 認証 [5-14](#)

プライオリティの設定 [5-14](#)

プライマリ IP アドレスの追加 [5-13](#)

仮想ルータ ID。「VR ID」を参照

仮想ルータ冗長プロトコル。「VRRP」を参照

仮想ルータ冗長プロトコル、プロトコル

仮想ルータ冗長性 [4-37](#)

カットスルー ルーティング モード [4-36, 4-37](#)

管理インターフェイス

- IPv6 用の設定 [5-3](#)
- 設定 [5-3](#)

き

キープアライブ タイムアウト

- FCIP プロファイルでの設定 [2-18](#)

ギガビット イーサネット

- IPv4 設定例 [6-5](#)

ギガビット イーサネット インターフェイス

- IPv4-ACL のガイドライン [7-7](#)
- IPv4 の設定 [7-2](#)

IPv6 アドレスの設定 [8-12](#)

MTU フレーム サイズの設定 [6-6, 7-4](#)

VRRP の設定 [6-9](#)

オートネゴシエーションの設定 [6-6, 7-3](#)

サブインターフェイス [6-7, 7-6](#)

サブネットの要件 [6-7, 7-6](#)

設定 [6-4 ~ 6-11](#)

デフォルト パラメータ [7-7](#)

ハイ アベイラビリティの設定 [6-8 ~ 6-11](#)

無差別モードの設定 [6-6, 7-4](#)

ギガビット イーサネット インターフェイスの例 [4-57](#)

ギガビット イーサネット サブインターフェイス

VLAN の設定 [7-5](#)

く

クラウド検出。「iSNS クラウド検出」を参照

さ

最小再送信タイムアウト

FCIP プロファイルでの設定 [2-18](#)

最大再送信回数

FCIP プロファイルでの設定 [2-19](#)

サブネット

要件 [6-7, 7-6](#)

差別化サービス コード ポイント。「DSCP」を参照

し

ジッタ

FCIP プロファイルでの予測最大値の設定 [2-20](#)

自動生成された iSCSI ターゲット、iSCSI

自動生成されたターゲット [4-30](#)

ジャンボ フレーム。「MTU」を参照

冗長性

VRRP [2-6](#)

イーサネット PortChannel [2-6, 2-7](#)

ファイバチャネル PortChannel [2-7](#)

す

スイッチオーバー

VRRP [2-6](#)

スイッチ管理

インバンド [5-7](#)

スタティック iSLB イニシエータ

変換 [4-42](#)

スタティック WWN マッピング [4-27](#)

スタティック インポートされた iSCSI ターゲット [4-55](#)

スタティック マッピング [4-42](#)

スタティック マッピングされた iSCSI ターゲット、iSCSI

スタティック マッピングされたターゲット [4-30](#)

ストア アンド フォワード ルーティング モード [4-36,](#)
[4-37](#)

せ

セキュリティ パラメータ インデックス。「SPI」を参照

そ

相互 CHAP 認証

iSCSI 用の設定 [4-33](#)

iSLB 用の設定 [4-46](#)

ゾーン

iSLB [4-43, 4-45](#)

iSLB 用の設定とアクティブ化 [4-43](#)

ゾーン分割ベースのアクセス コントロール

iSCSI 用の設定 [4-27](#)

iSCSI 用の設定、iSCSI

ゾーン分割ベースのアクセス コントロールの設
定 [4-27](#)

た

ターゲット検出 [4-78](#)

ダイナミック iSCSI イニシエータ

スタティックへの変換、iSCSI

ダイナミック イニシエータのスタティックへの変
換 [4-21](#)

変換 [4-42](#)

ダイナミック マッピング [4-10, 4-42](#)

ダイナミック マッピング、iSCSI

ダイナミック マッピング、iSCSI

スタティック マッピング [4-9](#)

ち

遅延

転送 [4-35](#)

て

デフォルト ゲートウェイ。「IPv4 デフォルト ゲートウェイ」を参照

デフォルト ネットワーク。「IPv4 デフォルト ネットワーク」を参照

と

ドライバ

iSCSI [4-2](#)

トラブルシューティング

CTC [2-17](#)

トランキング モード

FCIP インターフェイス [2-4](#)

トランスペアレント イニシエータ モード [4-17](#)

トランスペアレント イニシエータ モード、iSCSI

トランスペアレント イニシエータ モード [4-22](#)

に

認証

CHAP オプション [4-61](#)

Device Manager によるローカルの設定 [4-32](#)

iSCSI セットアップ **4-60**
 iSLB イニシエータの制限、イニシエータ認証
 制限、iSLB
 iSLB イニシエータの制限 **4-46**
 MD5 **5-14**
 相互 CHAP、相互 CHAP 認証 **4-33**
 平文 **5-14**
 メカニズム **4-31**
 ローカル **4-32**
 「MD5 認証」も参照
 「平文認証」も参照

は

ハイ アベイラビリティ
 VRRP **2-6, 4-59**
 VRRP、VRRP ベースのハイ アベイラビリティ
 ティ **4-59**
 イーサネット PortChannel **2-6, 4-60**
 ファイバ チャンネル PortChannel **2-7**
 パケット
 FCIP での廃棄 **2-22**
 パススルー ルーティング モード **4-35, 4-37**
 バッファ サイズ
 FCIP プロファイルでの設定 **2-20**

ふ

ファイバ チャンネル **4-1**
 iSCSI ターゲット **4-9 ~ 4-16**
 ファイバ チャンネル ゾーン分割ベースのアクセス コント
 ロール **4-29**
 ファイバ チャンネル ターゲット
 ダイナミック インポート **4-11**
 ダイナミック マッピング **4-11**
 ファブリックのロック
 解除 **4-52**
 負荷メトリック **4-43**
 複数の VSAN

設定 **5-10**
 輻輳ウィンドウ監視。「CWM」を参照
 ブリッジ ポート。「B ポート」を参照
 フレーム
 MTU サイズの設定 **6-6, 7-4**
 プロキシ イニシエータ
 設定、iSCSI
 プロキシ イニシエータの設定 **4-23**
 プロキシ イニシエータ モード **4-17, 4-27**
 設定 **4-22**
 ゾーン分割 **4-24**
 プロキシ イニシエータ モード、iSCSI
 プロキシ イニシエータ モード **4-22**
 プロトコル **4-1**
 VRRP **4-10**

ほ

ポート
 仮想 E **2-2**
 ポート モード
 IPS **6-4, 7-1**

ま

マージ ステータスの矛盾、iSLB
 マージ ステータスの矛盾、CFS
 マージ ステータスの矛盾 **4-53**
 マルチキャスト アドレス
 IPv6 送信要求ノードフォーマット、図 **8-6**
 IPv6 フォーマット、図 **8-5**
 ブロードキャスト アドレスに対する IPv6 の代替手
 段 **8-6**
 マルチパス ソフトウェアの例 **4-54**

む

無差別モード

ギガビット イーサネット インターフェイスの設定 [6-6, 7-4](#)

め

明示的なファブリック ログアウト [4-18](#)

り

リンク冗長性

イーサネット PortChannel 集約 [6-10](#)

リンクローカル アドレス

説明 [8-4](#)

フォーマット、 [8-4](#)

る

ルータ検出

IPv6 [8-9](#)

ろ

ロード バランシング [4-37, 4-39](#)

FSPF (例) [2-5](#)

PortChannel (例) [2-5](#)

重み付け [4-43](#)

ロック、ファブリックの [4-51](#)